

# NetScaler Gateway 11.0

Sep 16, 2015

## Key Features

[NetScaler Gateway Architecture](#)

[How User Connections Work](#)

## Common Deployments

[Deploying in the DMZ](#)

[Deploying in the Secure Network](#)

## What's New

## Known Issues

## Client Software Requirements

[NetScaler Gateway Plug-in System Requirements](#)

[Endpoint Analysis Requirements](#)

## Compatibility With Citrix Products

## Licensing

[NetScaler Gateway License Types](#)

[Obtaining Your Platform or Universal License Files](#)

[To install a license on NetScaler Gateway](#)

[Verifying Installation of the Universal License](#)

## Upgrading

## Before Getting Started

[Planning for Security](#)

[Prerequisites](#)

[Pre-Installation Checklist](#)

## Installing the System

[Configuring NetScaler Gateway](#)

[Using the Configuration Utility](#)

[Policies and Profiles on NetScaler Gateway](#)  
[Viewing NetScaler Gateway Configuration Settings](#)  
[Configuring the NetScaler Gateway by Using Wizards](#)  
[Configuring the Host Name and FQDN on NetScaler Gateway](#)  
[Installing and Managing Certificates](#)  
[Testing Your NetScaler Gateway Configuration](#)  
[Creating Virtual Servers](#)  
[Configuring IP Addresses on NetScaler Gateway](#)  
[Resolving DNS Servers Located in the Secure Network](#)  
[Configuring DNS Virtual Servers](#)  
[Configuring Name Service Providers](#)  
[Configuring Server-Initiated Connections](#)  
[Configuring Routing on NetScaler Gateway](#)  
[Configuring Auto Negotiation](#)

## [Configuring Authentication and Authorization](#)

[Configuring Default Global Authentication Types](#)  
[Configuring Authentication Without Authorization](#)  
[Configuring Authorization](#)  
[Disabling Authentication](#)  
[Configuring Authentication for Specific Times](#)  
[How Authentication Policies Work](#)  
[Configuring Local Users](#)  
[Configuring Groups](#)  
[Configuring LDAP Authentication](#)  
[Configuring Client Certificate Authentication](#)  
[Configuring RADIUS Authentication](#)  
[Configuring SAML Authentication](#)  
[Configuring TACACS+ Authentication](#)  
[Configuring Multifactor Authentication](#)  
[Configuring Single Sign-On](#)  
[Configuring One-Time Password Use](#)  
[nFactor for Gateway Authentication](#)

## Configuring the VPN User Experience

How User Connections Work with the NetScaler Gateway Plug-in

Choosing the User Access Method

Deploying NetScaler Gateway Plug-ins for User Access

Selecting the NetScaler Gateway Plug-in for Users

Integrating the NetScaler Gateway Plug-in with Citrix Receiver

Customizing the User Portal

Configuring Clientless Access

Configuring the Client Choices Page

Configuring Access Scenario Fallback

Configuring Connections for the NetScaler Gateway Plug-in

How a Traffic Policy Works

Configuring Session Policies

Configuring Endpoint Policies

Creating Advanced Endpoint Analysis Scans

Managing User Sessions

## Configuring Unified Gateway

Unified Gateway FAQ

## Deploying in a Double Hop DMZ

Deploying NetScaler Gateway in a Double-Hop DMZ

How a Double-Hop Deployment Works

Communication Flow in a Double-Hop DMZ Deployment

Preparing for a Double-Hop DMZ Deployment

Installing and Configuring Netscaler Gateway in a Double-Hop DMZ

## Using High Availability

How High Availability Works

Configuring Settings for High Availability

Configuring Communication Intervals

Synchronizing NetScaler Gateway Appliances

Synchronizing Configuration Files in a High Availability Setup

Configuring Command Propagation

Configuring Fail-Safe Mode

Configuring the Virtual MAC Address

Configuring High Availability Pairs in Different Subnets

Configuring Route Monitors

Configuring Link Redundancy

Understanding the Causes of Failover

Forcing Failover from a Node

## Using Clustering

Configuring Clustering

## Maintaining and Monitoring the System

## Integrating with Citrix Products

## How Users Connect to Applications, Desktops, and ShareFile

## Deploying with XenMobile App Edition, XenApp, and XenDesktop

## Accessing XenApp and XenDesktop Resources with the Web Interface

Integrating NetScaler Gateway with XenApp or XenDesktop

Establishing a Secure Connection to the Server Farm

Deploying with the Web Interface

Setting Up a Web Interface Site to Work

Configuring Communication with the Web Interface

Configuring Additional Web Interface Settings on NetScaler Gateway

Configuring Access to Applications and Virtual Desktops in the Web Interface

Configuring SmartAccess

Configuring SmartControl

Configuring Single Sign-On to the Web Interface

Allowing File Type Association

## Integrating with App Controller or StoreFront

How NetScaler Gateway and App Controller Integrate

Creating Policies with the Quick Configuration Wizard

Configuring NetScaler Gateway and App Controller

[Configuring Session Policies and Profiles for App Controller and StoreFront](#)

[Configuring Custom Clientless Access Policies for Receiver](#)

[Configuring Custom Clientless Access Policies for Receiver for Web](#)

[Using WebFront to Integrate with StoreFront](#)

## Configuring Settings for Your XenMobile Environment

[To configure load balancing servers for XenMobile MDM Edition](#)

[To configure load balancing servers for Microsoft Exchange with Email Security Filtering](#)

[To configure XenMobile NetScaler Connector \(XNC\) ActiveSync Filtering](#)

[To configure ShareFile settings](#)

[Allowing Access from Mobile Devices with Worx Apps](#)

[To configure NetScaler Gateway settings](#)

## Optimizing Network Traffic with CloudBridge

[Stateless RDP Proxy](#)

# Key Features

Aug 19, 2015

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 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.

The key features of NetScaler Gateway are:

- Authentication
- Termination of encrypted sessions
- Access control (based on permissions)
- Data traffic relay (when the preceding three functions are met)
- Support for multiple virtual servers and 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, as well as 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 works with 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.

|  |  |
|--|--|
| <a href="#">NetScaler Gateway Appliances</a> | Provides information about NetScaler Gateway appliances and the appliance installation instructions.   |
| <a href="#">Pre-Installation Checklist</a>   | Provides planning information to review and a list of tasks to complete before you install NetScaler Gateway in your network.  |
| <a href="#">Common Deployments</a>           | Provides information about deploying the NetScaler Gateway in the network DMZ, in a secure network without a DMZ, and with additional appliances to support load balancing and failover. Also provides information about deploying NetScaler Gateway with Citrix XenApp and Citrix XenDesktop. |
| <a href="#">Licensing</a>                    | Provides information about installing licenses on the appliance. Also provides information about installing licenses on multiple NetScaler Gateway appliances.   |



# NetScaler Gateway Architecture

Nov 04, 2014

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 accounting. 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](#). Accounting 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 accounting, see [Configuring Auditing on NetScaler Gateway](#).
- User connections. Users can log on to NetScaler Gateway by using the following access methods:
  - The NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in is not installed, they can log on by using a web browser to download and install the plug-in. If users have Citrix Receiver installed, users log on with the NetScaler Gateway Plug-in from Receiver. When Receiver and the NetScaler Gateway Plug-in are installed on the user device, Receiver adds the NetScaler Gateway Plug-in automatically.
  - The NetScaler Gateway Plug-in for Mac OS X that allows users running Mac OS X to log on. It has the same features and functions as the NetScaler Gateway Plug-in for Windows. You can provide endpoint analysis support for this plug-in version by installing NetScaler Gateway 10.1, Build 120.1316.e.
  - The NetScaler Gateway Plug-in for Java that enables Mac OS X, Linux, and optionally, Windows users to log on by using a web browser.
  - Receiver that allows user connections to published applications and virtual desktops in a server farm by using the Web Interface or Citrix StoreFront.
  - Receiver, Worx Home, WorxMail, and WorxWeb that allows users access to web and SaaS applications, iOS and Android mobile apps, and ShareFile data hosted in App Controller.
  - 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 web sites.



- Virtual adapter. The NetScaler Gateway virtual adapter provides support for applications that require IP spoofing. The virtual adapter is installed on the user device when the NetScaler Gateway Plug-in is installed. When users connect to the internal network, the outbound connection between NetScaler Gateway and internal servers use the intranet IP address as the source IP address. The NetScaler Gateway Plug-in 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 local area network (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 needs to 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

Mar 25, 2014

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:

- NetScaler Gateway Plug-in
- Citrix Receiver
- WorxMail and WorxWeb
- Android and iOS mobile devices

The NetScaler Gateway Plug-in 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 Mac OS 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 needs to 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 his or her credentials. You can use Advanced Endpoint Analysis on a Mac OS 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 NetScaler Gateway Plug-in for Windows or NetScaler Gateway Plug-in for Mac OS X. If you are using the Network Gateway Plug-in for Java, the user device is also initialized with a list of preconfigured resource IP addresses and port numbers.
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 NetScaler Gateway Plug-in 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 XenMobile App Edition 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 App Controller. A user can connect with the NetScaler Gateway Plug-in through clientless access, or by using Citrix Receiver or WorxHome. For more information about App Controller, see [Installing App Controller](#).

Users can connect with Receiver to access their Windows-based applications and virtual desktops. Users can also access applications from App Controller. To connect from a remote location, users also install the NetScaler Gateway Plug-in on their device. Receiver automatically adds the NetScaler Gateway Plug-in to its list of plug-ins. When users log on to Receiver, they can also log on to the NetScaler Gateway Plug-in. You can also configure NetScaler Gateway to perform single sign-on to the NetScaler Gateway Plug-in when users log on to Receiver.

Users can connect from an iOS or Android device by using Worx Home. Users can access their email by using WorxMail and connect to web sites 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 Micro VPN automatically. In addition, WorxMail and WorxWeb use Micro VPN to establish connections through NetScaler Gateway. You do not have to configure Micro VPN on NetScaler Gateway.

# Common Deployments

Mar 05, 2015

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 resources 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 XenApp, XenDesktop, StoreFront, and XenMobile Server to allow users to access their Windows, web, mobile, and SaaS applications. If your deployment includes XenApp, StoreFront, or XenDesktop 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 XenDesktop or XenMobile App Edition.

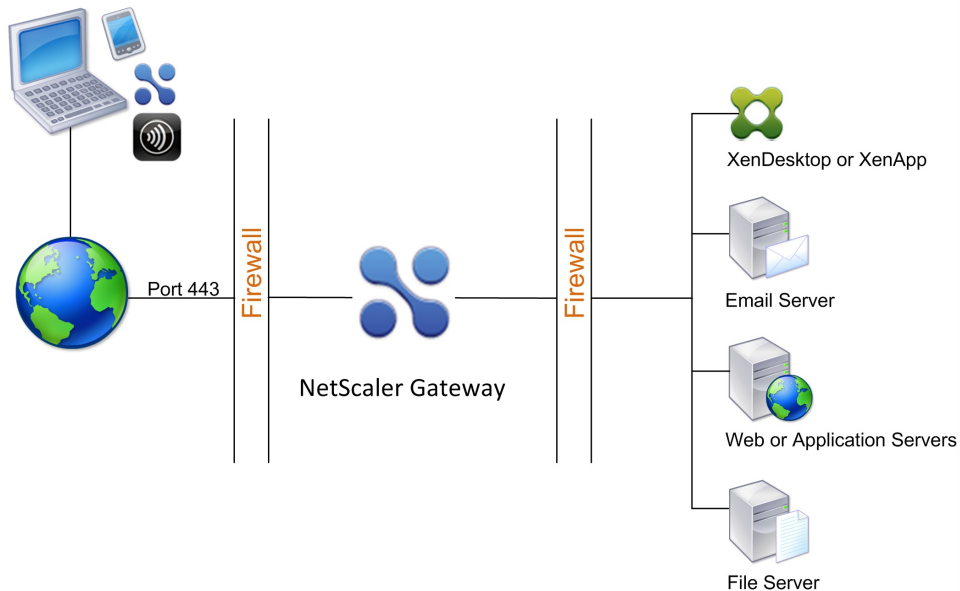
For more information about expanding your NetScaler Gateway installation with these and other supported Citrix solutions, see [Integrating with Citrix Products](#).

# Deploying in the DMZ

Jan 14, 2014

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 NetScaler Gateway Plug-in or Citrix Receiver.

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.

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.

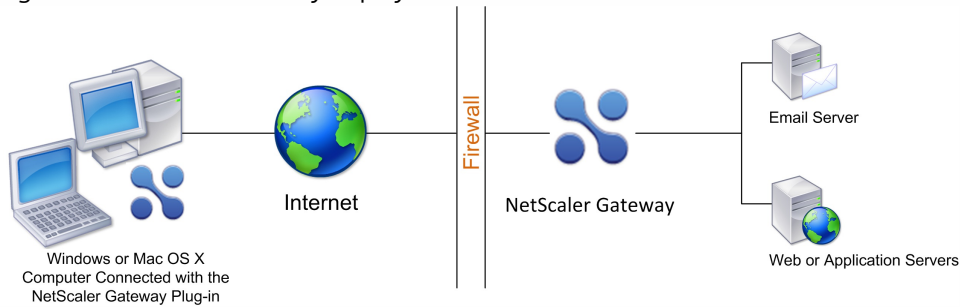
For example, if you authorize external users to access a web server in the internal network, and this server listens for HTTP connections on port 80, you must allow HTTP on port 80 through the second firewall. NetScaler Gateway establishes the connection through the second firewall to the HTTP server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

# Deploying in the Secure Network

Jan 14, 2014

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, however, 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, NetScaler Gateway Plug-in 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.

# What's New

Dec 30, 2015

## Access Insight

New in this release is a metric for measuring layer 7 latency for Insight that actively monitors a network disruption at a configurable granular level. The following are new features in this release.

- Live latency monitoring to catch spikes.
- Notifications sent out to the Insight Center if the latency exceeds the minimum observed latency. (These notifications are sent out if the latency exceeds the minimum observed latency by a configurable threshold factor for a configurable interval of time. The interval of time is used to filter out any outliers from being reported).
- Run time configurable
- Flexibility to configure different connections to have different parameters depending on certain “rules”.

New in this release is the HDX Insight feature. It reports the details about the ICA session. The NetScaler appliance examines the ICA packet, and generates Appflow records, which exports information records, that help uncover issues.

## Gateway

The Dual-Hop enhancement enables next-hop requests to be distributed among several available NetScaler appliances. The Dual-Hop feature expands the capability to load balance across any next-hop server, so that if one next-hop server is unavailable, connections can be re-established using another available server. This enhancement supports the below configurations:

- Creates a LB virtual server on DMZ NetScaler for the next-hop targets, and allow this LB to be added as a Next-Hop Server.
- Specifies a next-hop server as an FQDN name so a GSLB solution could be used.

New in this release, NetScaler administrators can assign RDP capabilities through the NetScaler Gateway configuration. The following are configurable as part of the RDP client profile:

- Redirection of ClipBoard
- Redirection of Printers
- Redirection of Disk Drives

The VPN plugin was enhanced to acknowledge the intranet application protocol flag. ICMP blocking can be configured to separate intranet applications for UDP and TCP.

The NetScaler appliance was enhanced to provide a verbose log of Passed/Failed EPA scans. The verbose log provides an easy to read reason for failures on the client machine.

## Auth

The NetScaler appliance has been enhanced to provide SAML authentication to an application by activating the SAML Identity Provider (IdP) and/or the SAML Service Provider (SP). If the system time on NetScaler SAML IdP and the peer SAML SP is not in sync, either party may invalidate the messages.

Duration can be setup for valid assertions. This duration, called the "skew time," specifies the number of minutes that the message will be accepted. The skew time can be configured on the SAML SP and the SAML IdP.

If used as a SAML Identity Provider (IdP), the NetScaler appliance can be setup to serve assertions to pre-configured SAML Service Providers (SP) or those trusted by the IdP. The SAML IdP must have the service provider ID (or issuer name) of the relevant SAML SPs.

If used as a SAML Identity Provider (IdP), the NetScaler appliance now supports redirect bindings (in addition to POST binding).

If used as a SAML SP, the NetScaler appliance can now extract multi-valued attributes from a SAML assertion.

In the SAML Service Provider (SP) module, names of the attributes that can be extracted from an incoming SAML assertion can be up to 127 bytes long. The previous limit was 63 bytes.

### Framehawk Virtual Channel

NetScaler Gateway now supports the new UDP-based Framehawk virtual channel.  
[# 587560]

### Windows 10

NetScaler Gateway now supports Windows 10.  
[# 579428]



## NetScaler with Unified Gateway

This feature extends NetScaler Gateway connectivity with access to any web application through a single URL, along with seamless single sign-on and sign-off. Single URL access can be configured for:

- Internal organizational web applications
- Software as a Service applications, including SAML based single sign-on when available
- Outlook Web Access and SharePoint as clientless applications
- Load balanced applications served through NetScaler load balancing virtual servers
- XenApp and XenDesktop published resources.

The feature can be configured and managed with the Unified Gateway wizard in the NetScaler configuration utility. [#00552862, #0438356, #0519875, #0519875]

## SmartControl

SmartControl allows policy-based management decisions for ICA connections through the VPN. SmartControl policies can be applied at the session level to control user's ICA environment and to further manage ICA connections with SmartGroup sorting decisions. [#0525947]

## Portal Customization and EULA

The Portal Customization options have been expanded to allow end-to-end customization of the VPN user portal. Administrators can apply themes to their VPN portal design or use themes as a foundation for their own customization or branding. An option to present VPN users an End User License Agreement (EULA) has also been added to the portal design. Portal themes and EULAs can be bound to a VPN virtual server or specified as global VPN parameters. [#0489467]

## New and Updated Gateway Clients

NetScaler Gateway release 11.0 adds new plug-in clients for the following operating systems:

- Android 4.1 or later  
Please find the playstore link for CitrixVPN app here:  
<https://play.google.com/store/apps/details?id=com.citrix.CitrixVPN&hl=en>
- iOS 7 or later
- Linux (Ubuntu 12.04 and 14.04)

Each of these clients provides full SSL VPN tunnel functionality through NetScaler Gateway and supports all authentication methods available in NetScaler Gateway.

Additionally, the Mac OS and Windows plug-ins have been refreshed and updated for the 11.0 release, including OS X 10.10 (Yosemite) support for the Mac OS X plug-in. [#0495767, #0520483]

## NetScaler Gateway Plug-in Upgrade Control

The NetScaler Gateway client plug-ins are no longer coupled to the NetScaler release versioning. Settings for version requirement per client OS type can be configured globally and within session policies. [#0236620]

## Plug-in Icon Decoupling from Citrix Receiver

The desktop client plug-ins icons can now be configured to operate independently from Native Citrix Receiver clients. Settings to manage Receiver integration with the NetScaler Gateway Plug-ins can be configured globally and within session

policies. [#0406312]

### **Disabling Automatic Update for the Windows Gateway Client and EPA Plug-ins**

This enhancement adds an option in client Endpoint Analysis (EPA) to prevent automatic client updates by disabling the "EnableAutoUpdate" registry key. [#236620]

### **Striped Cluster for NetScaler Gateway in ICA Proxy Mode**

This feature allows administrators to deploy NetScaler Gateway with XenApp and XenDesktop in a striped cluster configuration. Administrators can use existing Gateway configurations and scale seamlessly in a cluster deployment without having to restrict the VPN configuration to a single node.

Note that this feature is limited to ICA Proxy basic-mode virtual servers and does not support SmartAccess. [#0490329]

### **Clientless VPN support for Outlook Web Access 2013 and SharePoint 2013**

NetScaler Gateway has improved support for access to Outlook Web Access 2013 and SharePoint 2013 through Clientless VPN (CVPN) sessions. [#0494995]

### **WebFront**

WebFront is an alternative integration point for XenApp and XenDesktop deployments served by StoreFront. Resident on NetScaler, WebFront uses caching and packet flow optimization in the distribution of user stores. These techniques improve end user experience for Receiver for Web users and speed up single sign-on for native Receiver users. In the NetScaler configuration utility, the WebFront feature is on the Configuration tab at System > WebFront. [#0497619, #0497625]

### **ICA Proxy Connection Termination after Session Time Out**

Automatic session timeout can be enabled for ICA connections as a VPN parameter. Enabling this parameter forces active ICA connections to time out when a VPN session closes. [#0358672]

### **Support for Common Gateway Protocol (CGP) over WebSockets**

NetScaler Gateway virtual servers have improved intelligence for handling CGP traffic destined for the common CGP port, 2598, over WebSockets. This enhancement allows Receiver for HTML5 user sessions through NetScaler Gateway to support Session Reliability. [#0519889]

### **SPNEGO Encapsulation for Kerberos Tickets**

NetScaler now uses SPNEGO encapsulation on Kerberos tickets that are sent to back-end web applications and servers. [#404899]

### **Cross Domain Kerberos Constrained Delegation**

This enhancement adds support for cross-domain Kerberos constrained delegation when both the user and the service realm have a two-way shortcut trust. That is, if the user and service belong to different domains/realms, constrained delegation fails. However, if a user logs on with a user name and password, Kerberos Single Sign-On works for cross-domain access, because the NetScaler Gateway appliance does Kerberos impersonation with the user password. NetScaler Gateway currently does not otherwise support cross-domain constrained delegation. [#444387]

# Known Issues

Jul 14, 2015

The following is a list of known issues in this release. **Read the list carefully before installing the product.**

- A seamless Single Sign-On (SSO) to the same URL domain fails when a plug-in is launched in native mode.  
[# 544325]
- When set in the Authentication Profile of a load balancing virtual server that is behind a Unified Gateway, the Authentication Domain parameter will cause single sign-on to fail when the authentication is performed by a traffic manager in a different traffic domain.  
[# 574194]
- Sometimes the homepage shows up blank on chrome browser. Refreshing the page solves the issue.  
[# 574173]
- When a VPN works as a SAML SP in a two-factor case, and if the Get /vpn/index after /cgi/samlauth comes to the same core, NetScaler resends the SAML Auth request.  
Intermittent issues appear in multi-core systems. It works normally if both requests go to different cores.  
[# 576414]
- The NetScaler Gateway URL cannot be added to a Store with Receiver for Windows if only the SHA 384 cipher is enabled in the Receiver OS.  
[# 571340]
- In the EULA and native client, the French characters, 'œ' and 'Œ', do not render properly.  
[# 571674]
- In a double hop setup, when SSL relay is enabled for XenApp and XenDesktop, the XenApp or XenDesktop resource launch fails. The builds affected: 10.1-118.X to 10.5-55.8.  
[# 550877]
- Smart Control does not work for applications that have SSL relay enabled on the server with few ICAPOLICY rules.  
[# 570437]
- Customized pages are not loaded successfully in Internet Explorer. This is a known limitation of the browser. To get the customized page in IE, open developer tools by pressing F12. Browse to the NetScaler Gateway URL, and access the customized WebFront site. Customized pages are successfully loaded in Chrome.  
[# 570161]
- When accessing SharePoint 2007 through Clientless VPN, the VPN session terminates, and some URL requests are not rewritten in Clientless VPN mode.  
[# 567887]
- When exiting Receiver for Windows, the NetScaler Gateway plug-in exits also even when icon decoupling is enabled.  
[# 566871]
- If a user adds multiple personal bookmarks with the same URL or fileshare address, but each bookmark has a different name, then deleting one bookmark will delete all of bookmarks with the same address.  
[# 558903]

- The NetScaler Gateway client plug-ins will not decouple immediately for previously installed clients after the 'Show VPN Plugin-in icon with Receiver' option is enabled. Users need to exit the plugin process and restart to complete the decoupling.  
[# 558799]
- Web applications do not show the complete name of the bookmark. The VPN URL supports 32 characters, but the portal homepage only supports 8~11 characters.  
[# 572731]
- Currently, the EULA feature in portal does not work for certificate authorization. It only works for authentication. EULA works fine in other scenarios.  
[# 556111]
- When customizing a portal theme according to previous processes, for example using the command "vpn parameter UITHEME CUSTOM", the administrator needs to copy the CSS files in the NetScaler shell. Because of the design changes for Portal customization in NetScaler Gateway 11.0, copying the CSS files is required. Complete the steps described in the documentation page at:

<http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-connect-users-wrapper-con/ng-connect-users-cr-integration-con/ng-connect-custom-theme-page-tsk.html>

The following changes to the steps are needed:

After step 3,

4) At command prompt, type "cd /var/netscaler/logon/themes/ "

If you want to customize the Greenbubble theme, then

"cp -r Greenbubble Custom"

Or if you want to customize the Default theme, then

"cp -r Default Custom"

Now, you can make changes to files under "/var/netscaler/logon/themes/Custom"

Make edits to css/base.css

Copy a custom logo to the /var/ns\_gui\_custom/ns\_gui/vpn/media folder

Make changes to labels in files present in resources/ directory. These correspond to different languages.

Note: You can use WinSCP to transfer the files.

If changes to html pages or javascript files are also needed, then edits in "/var/ns\_gui\_custom/ns\_gui/" would be needed.

After all changes are done to files in "/var/ns\_gui\_custom/ns\_gui"

At command prompt, type

"tar -cvzf /var/ns\_gui\_custom/customtheme.tar.gz /var/ns\_gui\_custom/ns\_gui/\*"

5. Use the configuration utility to switch to the custom theme.

The previous Step 5 is not required in NetScaler Gateway 11.0. Once changes are made to one appliance, they propagate to all appliances in HA or cluster configurations.

[# 556317]

- When authprofile and authentication are configured to enable load balancing, the NetScaler appliance displays the /VPN/ Index page when it should display the HTTP Error 401- unauthorized access message. This happens intermittently when forms authentication enabled load balancing is modified for 401 authentication.  
[# 575652]
- An internet connection is required for publisher verification for the NetScaler Gateway plug-in for Windows. If not connected to the internet when downloading the plug-in from the NetScaler Gateway, the error 'Publisher AGEE\_setup.exec couldn't be verified' is seen.  
[# 553463, 558963]
- The pop-up messages for NetScaler Gateway Plug-in for Windows appear behind the active applications (such as browsers) on Windows 8.  
[# 511757]
- If two-factor authentication is configured with client certificates and LDAP and if 'Deny SSL Renegotiation' is set to 'All', user connections fail. The 'Deny SSL Renegotiation' parameter must be set to 'No'.  
To configure Deny SSL Renegotiation
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand Traffic Management and then expand SSL.
  2. In the details pane, under Settings, click 'Change advanced SSL settings'.
  3. Select 'No' for 'Deny SSL Renegotiation' and then click OK.  
[# 480009]
- A selected certificate does not get saved when SSL renegotiation with two-factor authentication is enabled. The certificate does get saved when certificate authentication is enabled.  
[# 574649]
- Audio over UDP is not supported with ICA sessiontimeout enabled or with Smart Control.  
[# 572850]
- On Android 4.4.2. devices, after frequent network changes, the VPN session may disconnect. Until the device is rebooted, a new VPN session can not be established. Upgrading the Android version resolves the problem.  
[# 575105]
- If an invalid certificate is selected as part of login, when certificate Authentication is optional, and two factor authentication is ON, the login fails as expected. But an app saves the certificate, though login failed. The user has to manually delete the saved certificate from the EditConnection Page to retry with a valid/no certificate.  
[# 575047]
- Android devices prior to version 5.0, SSL renegotiation fails when TLS1.2 is enabled.  
[# 574640]
- After login is successful from browser, the VIP URL changes to "localvip:8080".  
[# 576221]

- The Client and EPA Plug-ins don't work with the latest Chrome versions as support for NPAPI is disabled by default. The support will be deprecated entirely in Chrome version 45 in September 2015.  
From Chrome version 42, all NPAPI plugins will appear as if they are not installed. This will affect customers upgrading from 10.5 to 11.0. This is also applicable to customers who upgrade from 11.0 Beta builds and later Release builds. Affected customers will see a download prompt even though the VPN or EPA plugin is installed.  
Work Around:  
There is no work around to enable NPAPI for Chrome on Linux.  
Users need to use a browser which allows NPAPI (e.g. Firefox).  
More about NPAPI deprecation in Chrome browsers can be found at:  
<https://support.google.com/chrome/answer/6213033?hl=en>  
[# 574355]
- The plug-in crashes when VPN logout is performed from browser.  
[# 576215]
- An unintentional automatic Linux exit happens under the following conditions:
  - \* The NetScaler appliance is configured for dual, certificate authentication and LDAP authentication.
  - \* The subject field of the client certificate doesn't contain an email attribute value.
 [# 571281]
- The Linux NetScaler Gateway client fails to launch its system tray icon after installation in Ubuntu 14.04.  
Root cause: Ubuntu has turned off whitelisting since version 13.10.  
Steps to fix:  
sudo apt-add-repository ppa:gurqn/systray-trusty  
sudo apt-get update  
sudo apt-get upgrade  
Then logoff and log in again.  
References:  
<http://ubuntuforums.org/showthread.php?t=2217458>  
<http://askubuntu.com/questions/456950/system-tray-icons-disappeared-after-installing-ubuntu-14-04>  
<https://launchpad.net/~gurqn/+archive/ubuntu/systray-trusty>  
[# 528843]
- During login, the icon present in the dock is changed to the previous version's icon. After the login process is finished, the icon changes to the new icon.  
Workaround: Quit the plugin and restart it. The new icon shows normally during the login process.  
[# 574428]
- The NetScaler appliance is not able to connect a Mac computer to the VPN if only SSLv2 is enabled.  
[# 574149]
- The NetScaler Gateway Client icon in Launchpad is not updated with the new client installation. Launchpad continues to show the previous Black Lock icon even though the new Blue Lock icon is shown elsewhere in the Finder. This happens because the Finder caches application icons and their aliases. As a result, the Launcher does not update the alias icon when the application's icon has been changed.  
Workaround - Clear the Finder's icon cache using following article's instructions:  
<http://apple.stackexchange.com/questions/151549/symbolic-link-icons-dont-update> (requires reboot) OR modify the application alias name in /Applications/Citrix by adding few spaces (minimum two).

[# 573907]

- The Mac OS Endpoint Analysis (EPA) client only supports TLS1.0 and thus cannot perform EPA if the server has only TLS1.1/1.2 enabled.

There is no workaround for this problem, but a customer can still perform EPA with the Mac VPN plugin. EPA from a browser will not be available if TLS1.0 is not enabled.

[# 572969]

- When you navigate to Settings > Options > Account in an Outlook Web Access browser, the account information does not appear. This issue occurs on IE 10 and IE 11 browsers.

[# 571714]

- On the Unified Gateway Dashboard, the ICA sessions counter increases when a Full VPN session is established. Although the ICA sessions counter is not configured to collect ICA data, the ICA sessions counter increases.

[# 573301]

- When the HTTP/2 Protocol is used to access the VPN with external authentication, the transaction will not go through. Ensure HTTP/2 is disabled in nshttp\_default\_strict\_profile.

[# 574742]

- Endpoint analysis (EPA) does not start a security scan on the user's device, and the VPN session does not launch with the proxy configured on a Chrome browser.

[# 575527]

- If StoreFront has been configured as WIHome parameter, then accessing the Store Apps in Applications tab in the homepage over Full vpn mode with Windows does not work and an error message "Cannot complete your request" is returned.

[# 575993]

- After setting a netprofile to the virtual server, unbind and rebind the SSL cert-key pair bound to the virtual server to connect with DTLS. If this is not done, the DTLS connection handshake between the client and the NetScaler Gateway appliance fails. After rebinding the SSL certkey pair, the handshake is accepted and the netprofile is honored.

[# 555018]

- Applicable only for Mac and Linux VPN clients

Chrome is phasing out NPAPI support. From Chrome version 42+ all NPAPI plugins will appear as if they are not installed. This will affect all existing customers. Affected customers will see a download prompt even though the VPN plugin is installed.

Workaround: Google has announced that Chrome will stop supporting NPAPI completely in version 45.

Until then, you can enable NPAPI as follows:

1) In the Chrome URL bar, type:

Chrome://flags

2) Enable the "Enable NPAPI" option.

3) Restart Chrome.

For more information about NPAPI deprecation, see <https://support.google.com/chrome/answer/6213033?hl=en>

[# 572447, 574353, 575609]

- When using the Smart Control configuration, the ICASESSIONTIMEOUT feature is always enabled. There is not an option to disable it.

[# 572386]

- The Unified Gateway wizard does not support the creation of two Intranet Application type seamless SSO URLs using same LB with different site relative string.  
[# 576055]
- Two NSC\_AAAC cookies are seen when a request is sent by a Client to the VIP. The value is the same for both cookies. One cookie is for FQDN; the other cookie is for the domain.  
Two NSC\_AAAC cookies are no longer seen after the version 11.0 beta.  
[# 540590, 539586]
- When Unified Gateway is deployed with seamless SSO enabled for virtual server authentication, then the authentication servers and policy realms bound at the authentication virtual server will be ignored. Instead, those authentication policies at Gateway are utilized for authentication. Authentication policies at the authentication virtual server are used when step-up authentication is configured using authentication profiles. Increasing the authentication profile's "authentication level" is the method used to step-up authentication.  
[# 540526]
- Certificate based authentication fails for devices running Android versions before 5.0. This is applicable if only TLSv1.2 is enabled on server.  
[# 572098]
- When the maxAAUsers parameter is UNSET on a VPN virtual server, NetScaler Gateway does not update the value to previously set value. Due to this, numbers of users allowed on a vpn virtual server cannot be increased by applying an UNSET operation. Administrators need to configure a SET operation as a workaround.  
For example, if the administrator configures 10 as the maxAAUsers value, then issues a SET operation for 5, if he issues another UNSET, the number of allowed users does not go back to 10 users.  
[# 576063]



# Client Software Requirements

Jul 14, 2015

This section describes the system requirements for the Citrix NetScaler Gateway client software.

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

If you configure endpoint policies on NetScaler Gateway, when users log on, NetScaler Gateway downloads and installs the Endpoint Analysis Plug-in on the user device automatically.

# NetScaler Gateway Plug-in System Requirements

Aug 24, 2015

The NetScaler Gateway Plug-in establishes a connection from the user device to the NetScaler Gateway appliance. The NetScaler Gateway Plug-in is distributed as a desktop application for Microsoft Windows or Mac OS X. The NetScaler Gateway Plug-in is downloaded and installed automatically when users enter the secure Web address of the NetScaler Gateway appliance and a logon point in a Web browser.

The NetScaler Gateway Plug-in has been validated on the following operating systems and Web browsers.

| <b>Operating System</b>   | <b>Supported Browsers</b>  |
|---|--|
| <b>Mac OS X (10.10, 10.9, and 10.8)</b>   | Safari 7.1 or later<br>Google Chrome Release 30 or later<br>Mozilla Firefox Release 30 or later                |
| <b>Windows 10 Enterprise</b>  | Internet Explorer 11<br>Google Chrome Release 30 or later<br>Mozilla Firefox Release 24 or later               |
| <b>Windows 8.1 Pro</b><br><b>Windows 8.1 Enterprise</b>   | Internet Explorer 11<br>Google Chrome Release 30 or later<br>Mozilla Firefox Release 24 or later               |
| <b>Windows 8 Pro</b><br><b>Windows 8 Enterprise</b>   | Internet Explorer 9 and 10<br>Google Chrome Release 30 or later<br>Mozilla Firefox Release 24 or later         |
| <b>Windows 7 Home Basic Edition</b><br><b>Windows 7 Home Premium Edition</b><br><b>Windows 7 Professional Edition</b><br><b>Windows 7 Enterprise Edition</b><br><b>Windows 7 Ultimate Edition</b>                 | Internet Explorer 8, 9, 10, and 11<br>Google Chrome Release 30 or later<br>Mozilla Firefox Release 24 or later |
| <b>Windows Vista Home Basic Edition</b><br><b>Windows Vista Home Premium Edition</b><br><b>Windows Vista Enterprise Edition</b><br><b>Windows Vista Business Edition</b><br><b>Windows Vista Ultimate Edition</b> | Internet Explorer 7, 8 and 9<br>Mozilla Firefox Release 9 and 10   |

# Endpoint Analysis Requirements

Jun 30, 2015

When NetScaler Gateway installs the Endpoint Analysis Plug-in on the user device, the plug-in scans the user device for the endpoint security requirements that you configured on NetScaler Gateway. The requirements include information, such as the operating system, antivirus, or web browser versions.

When Windows users connect to NetScaler Gateway using the browser for first time, the portal requests the installation of the Endpoint Analysis Plug-in. On subsequent log on attempts, the plug-in checks the upgrade control configuration to decide if the client EPA plug-in upgrade is necessary. If it is necessary, the user will receive a prompt to download and install the newer End-Point Analysis Plug-in. The Endpoint Analysis Plug-in for Windows is installed as a Windows 32-bit application. No special privileges are required to install or use it.

For Mac OS X, the user is required to install the Endpoint Analysis Plug-in. The plug-in for Mac OS X is installed as a 32-bit application. No special privileges are necessary to install it. On subsequent log on attempts, if the plug-in versions do not match, the user will be prompted to download and install the plug-in.

To use the Endpoint Analysis Plug-in, the following software is required on the user device:

- Windows XP, Windows Vista, Windows 7, Windows 8 or Windows 10 with all service packs and critical updates installed.
- Mac OS X versions 10.8, 10.9, and 10.10.
- Internet Explorer with cookies enabled. The minimum required version is 7.0.
- Firefox with the Endpoint Analysis Plug-in enabled. The minimum required version is 3.0.
- Google Chrome

Important: In case of Pre-Authentication EPA, if a user does not install the Endpoint Analysis Plug-in on the user device or chooses to skip the scan, the user cannot log on with the NetScaler Gateway Plug-in. In case of Post-Authentication EPA, the user can access resources for which a scan is not required by using either clientless access or by using Citrix Receiver.

# Compatibility with Citrix Products

Aug 27, 2015

The following table provides the Citrix products and versions with which NetScaler Gateway 11.0 is compatible.

Note: NetScaler Gateway features are available on NetScaler VPX.

| Citrix product      | Release version  |
|---------------------|--|
| CloudBridge         | 5.6 through 7.4  |
| NetScaler Platforms | All current MPX models including FIPS compliant appliances |
| NetScaler           | 10.1, 10.5, and 11.0                                       |
| NetScaler VPX       | 10.1   |
| StoreFront          | 2.5, 2.6, and 3.0  |
| VDI-in-a-Box        | 5.2, 5.3, and 5.4  |
| Web Interface       | 5.4  |
| XenApp              | 6.5  |
| XenDesktop          | 7.5 and 7.6  |
| XenMobile           | 9.0 and 10.0   |

NetScaler Gateway 11.0 supports the following versions of Citrix client software:

| Receiver or Plug-in                    | Minimum Supported Version |
|--|---------------------------|
| NetScaler Gateway Plug-in for Mac OS X | 3.0.1                     |
| NetScaler Gateway Plug-in for Windows  | 10.1                      |
| Receiver for Android                   | 3.4 and 3.5               |

| Receiver for iOS<br>Receiver or Plug-in | 5.8<br>Minimum Supported Version |
|---|----------------------------------|
| Receiver for Mac                        | 11.8.x                           |
| Receiver for Windows                    | 4.0                              |
| Worx Home for iOS                       | 9.0.2                            |
| Worx Home for Android                   | 9.0.1                            |
| WorxMail for iOS                        | 9.0.2                            |
| WorxWeb for iOS                         | 9.0.2                            |
| WorxMail for Android                    | 9.0.1                            |
| WorxWeb for Android                     | 9.0.1                            |

# Licensing

Jul 09, 2015

Before you can deploy Citrix NetScaler Gateway to support user connections, the appliance must be properly licensed.

**Important:** 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 need to reinstall NetScaler Gateway appliance software and do not have a backup of the configuration, you will 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

Jul 09, 2015

NetScaler Gateway requires a Platform license. The Platform license allows an unlimited amount of connections to XenApp, XenDesktop, or StoreFront by using ICA proxy. To allow VPN connections to the network from the NetScaler Gateway Plug-in, a SmartAccess logon point, or Worx Home, WorxWeb, or WorxMail, 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 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 will need the original license files.

The Platform license allows unlimited user connections to published applications on XenApp or virtual desktops from XenDesktop. 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 web site](#).

The Universal license limits the number of concurrent user sessions to the number of licenses you purchase.

The Universal license supports the following features:

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

If you purchase 100 licenses, you can have 100 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 you terminate the session. 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 Authorization Code (LAC) in e-mail.
- You use the Setup Wizard to configure NetScaler Gateway with the host name.

- You allocate the NetScaler Gateway licenses from the Citrix web site. Use the host name to bind the licenses to the appliance during the allocation process.
- You install the license file on NetScaler Gateway.

The Express license is used with the NetScaler VPX and allows for up to five concurrent user connections by using Receiver or the NetScaler Gateway Plug-in. The Express license is available for the VPX appliance and expires after one year. Users can connect to either Basic or SmartAccess virtual servers.

For more information about the system requirements for NetScaler VPX, see [Getting Started with Citrix NetScaler VPX](#). To download the appliance, see [NetScaler VPX Release 10.1](#).

After you download NetScaler VPX, from the NetScaler VPX web site, you acquire a license key, and then you activate and download your license file. You will need to provide the host name of your Citrix License Server or the host name of the NetScaler appliance.

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



# Obtaining Your Platform or Universal License Files

Apr 29, 2013

After you install NetScaler Gateway, you are ready to obtain your Platform or Universal license files from Citrix. You log on to the Citrix web site 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.

**Important:** You must install licenses on NetScaler Gateway. The appliance does not obtain licenses from Citrix License Server.

To obtain your licenses, go to the [Activate, upgrade and manage Citrix licenses](#) web page. On this page, you can get your new license and activate, upgrade, and manage Citrix licenses.

# To install a license on NetScaler Gateway

Jun 26, 2014

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 at a later date, you allocate an additional 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 need to restart NetScaler Gateway. Click Reboot.

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 amount of users and then click OK.

The number in this field corresponds to the number of licenses contained within the license file. This number should 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.

# Verifying Installation of the Universal License

Apr 29, 2013

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

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

# Before Getting Started

Jul 08, 2015

Before you install Citrix NetScaler Gateway, you should 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 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 works with the following Citrix products:

- XenMobile
- XenApp
- XenDesktop
- StoreFront
- Web Interface
- CloudBridge

For more information about deploying NetScaler Gateway, see [Common Deployments](#) and [Integrating With Citrix 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 NetScaler Gateway Plug-in, requiring users to log on with Citrix Receiver, Worx Home, 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.

# Planning for Security

May 29, 2013

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

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 Citrix 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 XenApp 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.

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 should 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 the authentication types in the preceding list, 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.

# Prerequisites

Jun 24, 2013

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 NetScaler Gateway Plug-in from the Citrix web site 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.

# Pre-Installation Checklist

Mar 25, 2014

The checklist consists of a list of tasks and planning information you should 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 the Model MPX Appliance](#) and [Installing NetScaler Gateway](#).

|  |  |
|--|--|
| Ensure that user devices meet the installation prerequisites described in <a href="#">NetScaler Gateway Plug-in System Requirements</a> .                      |  |
| Identify the mobile devices with which users connect.<br><br>Note: If users connect with an iOS device, you need to enable Secure Browse in a session profile. |  |

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.<br><br>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 <a href="#">Citrix web site</a> .  |  |
| Generate a Certificate Signing Request (CSR) and send to a Certificate Authority (CA). Enter the date you send the CSR to the CA.   |  |
| Write down the system IP address and subnet mask.   |  |
| Write down the mapped IP address and subnet mask.   |  |
| Write down the subnet IP address and subnet mask (optional).  |  |
| Write down the administrator password.<br><br>The default password that comes with NetScaler Gateway is nsroot.   |  |

|  |  |
|--|--|
| <p>Write down the port number.</p> <p>This is the port 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.</p> |  |
| <p>Write down the default gateway IP address.</p>  |  |
| <p>Write down the DNS server IP address and port number.</p> <p>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.</p>                                     |  |
| <p>Write down the first virtual server IP address and host name.</p>   |  |
| <p>Write down the second virtual server IP address and host name (if applicable).</p>  |  |
| <p>Write down the WINS server IP address (if applicable).</p>  |  |

|   |  |
|---|--|
| <p>Write down the internal networks that users can access through NetScaler Gateway.</p> <p>Example: 10.10.0.0/24</p> <p>Enter all internal networks and network segments that users need access to when they connect through NetScaler Gateway by using the NetScaler Gateway Plug-in.</p> |  |
|---|--|

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.

|   |  |
|---|--|
| <p>Write down the NetScaler Gateway software version number.</p> <p>The version number must be the same on both NetScaler Gateway appliances.</p> |  |
| <p>Write down the administrator password (nsroot).</p> <p>The password must be the same on both appliances.</p>                                   |  |
| <p>Write down the primary NetScaler Gateway IP address and ID.</p>  |  |



|   |  |
|---|--|
| 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.<br><br>You must install the same Universal license on both appliances. |  |
| Write down the RPC node password.   |  |

NetScaler Gateway supports several different authentication and authorization types that can be used in a variety of 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.<br><br>If you allow unsecure connections to the LDAP server, the default is port 389. If you encrypt connections to the LDAP server with SSL, the default is port 636.  |  |
| Write down the security type.<br><br>You can configure security with or without encryption.   |  |
| Write down the administrator bind DN.<br><br>If your LDAP server requires authentication, enter the administrator DN that NetScaler Gateway should use to authenticate when making queries to the LDAP directory. An example is <code>cn=admin, cn=Users, dc=ace, dc=com</code> . |  |
| Write down the administrator password.<br><br>This is the password associated with the administrator bind DN.   |  |
| Write down the Base DN.<br><br>DN (or directory level) under which users are located; for example, <code>ou=users, dc=ace, dc=com</code> .  |  |
| Write down the server logon name attribute.<br><br>Enter the LDAP directory person object attribute that specifies a user's logon name. The default is  |  |

|   |  |
|---|--|
| <p>sAMAccountName. If you are not using Active Directory, common values for this setting are cn or uid.</p> <p>For more information about LDAP directory settings, see <a href="#">Configuring LDAP Authentication</a>.</p>   |  |
| <p>Write down the group attribute.</p> <p>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.</p> |  |
| <p>Write down the subattribute name.</p>  |  |

## 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.

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

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

|  |  |
|--|--|
| <p>Obtain and install on NetScaler Gateway a secure IdP certificate.</p> |  |
| <p>Write down the redirect URL.</p>                                      |  |
| <p>Write down the user field.</p>  |  |
| <p>Write down the signing certificate name.</p>                          |  |

|  |  |
|--|--|
| Write down the SAML issuer name.             |  |
| Write down the default authentication group. |  |

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 XenApp or XenDesktop in the secured network on these ports.  |  |
| Write down the authentication ports.<br><br>Open only the port appropriate for your NetScaler Gateway configuration. <ul style="list-style-type: none"> <li>• For LDAP connections, the default is TCP port 389.</li> <li>• For a RADIUS connection, the default is UDP port 1812.</li> </ul> |  |
| Write down the XenApp or XenDesktop ports.<br><br>If you are using NetScaler Gateway with XenApp or XenDesktop, open TCP port 1494. If you enable session reliability, open TCP port 2598 instead of 1494.<br><br>Citrix recommends keeping both of these ports open.                         |  |

Complete the following tasks if you are deploying NetScaler Gateway to provide access to XenApp or XenDesktop through the Web Interface or StoreFront. The NetScaler Gateway Plug-in 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). |  |

Complete the following tasks if you deploy App Controller in your internal network. If users connect to App Controller 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 App Controller.                         |  |
| Identify web, SaaS, and mobile iOS or Android applications users can access. |  |

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

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

|  |  |
|--|--|
| <p>Complete the items in the NetScaler Gateway Basic Network Connectivity section of this checklist for this NetScaler Gateway.</p> <p>When completing those items, note that Interface 0 connects this NetScaler Gateway to the Internet and Interface 1 connects this NetScaler Gateway to NetScaler Gateway in the second DMZ.</p>  |  |
| <p>Configure the second DMZ appliance information on the primary appliance.</p> <p>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.</p>    |  |
| <p>Write down the connection protocol and port between appliances.</p> <p>To configure NetScaler Gateway as the first hop in the double DMZ, you must specify the connection protocol and 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.</p> |  |

#### 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, note that Interface 0 connects this NetScaler Gateway to NetScaler Gateway in the first DMZ. Interface 1 connects this NetScaler Gateway to the secured network.

# Upgrading

Jan 22, 2014

You can upgrade the software that resides on NetScaler Gateway when new releases are made available. You can check for updates on the Citrix web site. 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 [Citrix Support](#) web site.

For information about the latest NetScaler Gateway maintenance release, see the [Citrix Knowledge Center](#).

1. Go to the [Citrix web site](#).
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.

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.

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.

# Installing the System

Jul 07, 2015

When you receive your Citrix NetScaler Gateway appliance, you unpack the appliance and prepare the site and rack. After you determine that the location where you will 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. For detailed appliance installation instructions, see [Installing the NetScaler Gateway Appliance](#).

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. See [NetScaler Gateway Virtual Appliances](#) for instructions on obtaining and installing a VPX image.

Citrix recommends using the [NetScaler Gateway Pre-Installation Checklist](#) 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 as well as an appliance.



# Configuring NetScaler Gateway

Mar 04, 2015

After you configure the base network settings on Citrix 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 need to 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 fails, 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

Jan 16, 2014

The configuration utility allows you to configure most of the NetScaler Gateway settings. You use a web browser to access 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 App Controller. 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](#)

# Policies and Profiles on NetScaler Gateway

Nov 11, 2014

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 are met. Each policy has a unique name and can have a profile bound to the policy.

For more information about policies with NetScaler Gateway, see the following topics:

# How Policies Work

May 30, 2013

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 should 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 amount of time users can stay logged on.

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

- The name of the virtual server that is configured on the appliance. The name is sent to XenApp 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 work with XenMobile App Edition, see [Configuring Settings for Your XenMobile Environment](#).

For more information about configuring NetScaler Gateway to work with Citrix XenApp and XenDesktop, see [Accessing XenApp and XenDesktop Resources with the Web Interface](#) and [Integrating with App Controller or StoreFront](#).

For more information about preauthentication policies, see [Configuring Endpoint Polices](#).

# Setting the Priorities of Policies

Apr 29, 2013

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.

# Configuring Conditional Policies

Jan 22, 2014

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 NetScaler Gateway Plug-in 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 a wide area network (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.

# Creating Policies on NetScaler Gateway

Jan 22, 2014

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 App Controller 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

May 30, 2013

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
- Client security expressions that define the software, files, processes, or registry values that must be installed and running on the user device
- Network-based expressions that restrict access based on network settings

NetScaler Gateway can also be used as a Citrix 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.

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



# Creating Simple and Compound Expressions

May 02, 2013

Simple expressions check for a single condition. An example of a simple expression is:

```
REQ.HTTP.URL == HTTP://www.mycompany.com
```

Compound expressions check for multiple conditions. You create compound expressions by connecting to one or more expression names using the logical operators && and |. You can use the symbols to group the expression in the order of evaluation.

Compound expressions can be categorized as:

- **Named expressions.** As an independent entity, a named expression can be reused by other policies and are part of the policy. You configure named expressions at the system level in the configuration utility. You can use a predefined named expression in the policy or create one of your own.
- **Inline expressions.** An inline expression is one that you build within the policy that is specific to the policy.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand AppExpert and then click Expressions.
2. In the details pane, click Add.
3. In the Create Policy Expression dialog box, in Expression Name, type a name for the expression.
4. To create an expression, click Add.
5. Do one of the following:
  1. In Frequently Used Expression, select an expression from the list, click OK, click Create and then click Close.
  2. Under Construct Expression, select the parameters for the expression string, click OK, click Create and then click Close.

# Adding Custom Expressions

Nov 11, 2014

If you are creating a policy, you can create a custom expression while configuring the policy. For example, you are creating a session profile to allow users to log on with the NetScaler Gateway Plug-in, set a time limit for the session, and allow single sign-on with Windows. After you create the session profile, in the Create Session Policy dialog box, you can create the expression. The following example shows an expression that checks for a process and antivirus application:

```
CLIENT.APPLICATION.PROCESS(ccapp.exe)EXISTS -frequent 5 &&  
CLIENT.APPLICATION.AV(Symantec).VERSION==14.20.0.29 -freshness 5 && ns_true
```

# Using Operators and Operands in Policy Expressions

May 15, 2013

An

— *operator*

is a symbol that identifies the operation— mathematical, Boolean, or relational, for example— that manipulates one or more objects, or

— *operands*

. The first section in this topic defines the operators you can use and provides a definition. The second section lists the operators you can use with specific qualifiers, such as method, URL and query.

This section defines the operators that you can use when creating a policy expression and provides a description of the operator.

## **==, !=, EQ, NEQ**

These operators test for exact matches. They are case-sensitive (“cmd.exe” is NOT EQUAL to “cMd.exe”). These operators are useful for creating permissions to allow particular strings that meet an exact syntax, but to exclude other strings.

## **GT**

This operator is used for numerical comparisons; it is used on the length of the URLs and query strings.

## **CONTAINS, NOTCONTAINS**

These operators perform checks against the specified qualifier to determine if the specified string is contained in the qualifier. These operators are not case-sensitive.

## **EXISTS, NOTEXISTS**

These operators check for the existence of particular qualifier. For example, these operators can be applied to HTTP headers to determine if a particular HTTP header exists or if the URL Query exists.

## **CONTENTS**

This operator checks if the qualifier exists and if it has contents (that is, whether or not a header exists and has a value associated with it, no matter what the value).

This section shows the parameters you can use for operators and operands. Each item starts with the qualifier and then lists the associated operator and operand, describes the action that the expression will carry out, and provides an example.

### **Method**

Operator: EQ, NEQ

Operands: Required:

- Standard HTTP methods
- Supported methods
- GET, HEAD, POST, PUT, DELETE OPTIONS, TRACE, CONNECT

Actions: Verifies the incoming request method to the configured method.

Example: Method EQ GET

## URL

Operator: EQ, NEQ

Operands: Required: URL (Format: /[prefix][\*][.suffix])

Actions: Verifies the incoming URL with the configured URL.

Example:

URL EQ /foo\*.asp

URL EQ /foo\*

URL EQ /\*.asp

URL EQ /foo.asp

Operator: CONTAINS, NOTCONTAINS

Operands: Required: Any string (in quotes)

Actions: Verifies the incoming URL for the presence of the configured pattern. (Includes URL and URL query.)

Example: URL CONTAINS 'ZZZ'

## URL LEN

Operator: GT

Operands: Required: Length (as an integer value)

Actions: Compares the incoming URL length with the configured length. (Includes URL and URL query.)

Example: URLLEN GT 60

## URL QUERY

Operator: CONTAINS, NOTCONTAINS

Operands: Required: Any string (in quotes).

Optional: Length and offset

Actions:

Verifies the incoming URL query for the presence of the configured pattern.

Used similarly to CONTENTS.

If no option is specified, the whole URL query after the pattern is used.

If options are present, only the length of the query after the pattern is used.

The offset is used to indicate from where to start the search for the pattern.

Example: URLQUERY CONTAINS 'ZZZ'

## URL QUERY LEN

Operator: GT

Operands: Required: Length (as an integer value)

Actions: Compares the incoming URL query length with the configured length.

Example: URLQUERYLN GT 60

## URL TOKENS

Operator: EQ, NEQ

Operands: Required: URL tokens (Supported URL tokens =, +, %, !, &, ?).

Actions: Compares the incoming URL for the presence of configured tokens. A backward slash (\) must be entered in front of the question mark.

Example: URLTOKENS EQ '% , +, &, \?'

## VERSION

Operator: EQ, NEQ

Operands: Required: Standard HTTP versions. Valid HTTP version strings HTTP/1.0, HTTP/1.1

Actions: Compares the incoming request's HTTP version with the configured HTTP version.

Example: VERSION EQ HTTP/1.1

Header

Operator: EXISTS, NOTEXISTS

Operands: None

Actions: Examines the incoming request for the presence of the HTTP header.

Example: Header Cookie EXISTS

Operator: CONTAINS, NOTCONTAINS

Operands: Required: Any string (in quotes).

Optional: Length and offset

Actions: Verifies the incoming request for the presence of a configured pattern in the specific header. Used similarly to CONTENTS. If no option is specified, the whole HTTP header value after the pattern is used. If options are present, only the length of the header after the pattern is used. The offset is used to indicate from where to start the search for the pattern.

Example: Header Cookie CONTAINS "&sid"

Operator: CONTENTS

Operands: Optional: Length and offset

Actions: Uses the contents of the HTTP header. If no option is specified, the whole HTTP header value is used. If options are present, only the length of the header starting from the offset is used.

Example: Header User-Agent CONTENTS

## SOURCEIP

Operator: EQ, NEQ

Operands: Required: IP address

Optional: Subnet mask

Actions: Verifies the source IP address in the incoming request against the configured IP address. If the optional subnet mask is specified, the incoming request is verified against the configured IP address and subnet mask.

Example: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

## DESTIP

Operator: EQ, NEQ

Operands: Required: IP address

Optional: Subnet mask

Actions: Verifies the destination IP address in the incoming request against the configured IP address. If the optional

subnet mask is specified, the incoming request is verified against the configured IP address and subnet mask.

Example: Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

#### **SOURCEPORT**

Operator: EQ, NEQ

Operands: Required: Port number

Optional: Port range

Actions: Verifies the source port number in the incoming request against the configured port number.

Example: SOURCEPORT EQ 10-20

#### **DESTPORT**

Operator: EQ, NEQ

Operands: Required: Port number

Optional: Port range

Actions: Verifies the destination port number in the incoming request against the configured port number.

Example: DESTPORT NEQ 80

#### **CLIENT.SSL.VERSION**

Operator: EQ, NEQ

Operands: Required: SSL version

Actions: Checks the version of the SSL or TLS version used in the secure connection.

Example: CLIENT.SSL.VERSION EQ SSLV3

#### **CLIENT.CIPHER.TYPE**

Operator: EQ, NEQ

Operands: Required: Client cipher type

Actions: Checks for the type of the cipher being used (export or non-export).

Example: CLIENT.CIPHER.TYPE EQ EXPORT

#### **CLIENT.CIPHER.BITS**

Operator: EQ, NEQ, GE, LE, GT, LT

Operands: Required: Client cipher bits

Actions: Checks for the key strength of the cipher being used.

Example: CLIENT.CIPHER.BITS GE 40

#### **CLIENT.CERT**

Operator: EXISTS, NOTEXISTS

Operands: none

Actions: Checks whether or not the client sent a valid certificate during the SSL handshake.

Example: CLIENT.CERT EXISTS

#### **CLIENT.CERT.VERSION**

Operator: EQ, NEQ, GE, LE, GT, LT

Operands: Client certificate version

Actions: Checks the version of the client certificate.

Example: CLIENT.CERT.VERSION EQ 2

### **CLIENT.CERT.SERIALNUMBER**

Operator: EQ, NEQ

Operands: Required: Client certificate serial number

Actions: Checks the serial number of the client certificate. The serial number is treated as a string.

Example: CLIENT.CERT.SERIALNUMBER EQ 2343323

### **CLIENT.CERT.SIGALGO**

Operator: EQ, NEQ

Operands: Required: Client certificate signature algorithm.

Actions: Checks the signature algorithm used in the client certificate.

Example: CLIENT.CERT.SIGALGO EQ md5WithRSAEncryption

### **CLIENT.CERT.SUBJECT**

Operator: CONTAINS, NOTCONTAINS

Operands: Required: Client certificate subject

Optional: Length, offset

Actions: Checks the subject field of the client certificate.

Example: CLIENT.CERT.SUBJECT CONTAINS CN= Access\_Gateway

### **CLIENT.CERT.ISSUER**

Operator: CONTAINS, NOTCONTAINS

Operands: Required: Client certificate issuer

Optional: Length, offset

Actions: Checks the issuer field of the client certificate.

Example: CLIENT.CERT.ISSUER CONTAINS O=VeriSign

### **CLIENT.CERT.VALIDFROM**

Operator: EQ, NEQ, GE, LE, GT, LT

Operands: Required: Date

Actions: Checks the date from which the client certificate is valid.

Valid date formats are:

Tue, 05 Nov 1994 08:12:31 GMT

Tuesday, 05-Nov-94 08:12:31 GMT

Tue Nov 14 08:12:31 1994

Example: CLIENT.CERT.VALIDFROM GE 'Tue Nov 14 08:12:31 1994'

### **CLIENT.CERT.VALIDTO**

Operator: EQ, NEQ, GE, LE, GT, LT

Operands: Required: Date

Actions: Checks the date until which the client certificate is valid.

Valid date formats are:

Tue, 05 Nov 1994 08:12:31 GMT

Tuesday, 05-Nov-94 08:12:31 GMT

Tue Nov 14 08:12:31 1994

Example: CLIENT.CERT.VALIDTO GE 'Tue Nov 14 08:12:31 1994'



# Viewing NetScaler Gateway Configuration Settings

May 19, 2013

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.

# Saving the NetScaler Gateway Configuration

Feb 21, 2014

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.

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

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.

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.

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.

# Clearing the NetScaler Gateway Configuration

Sep 06, 2013

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.

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.

# Configuring the NetScaler Gateway by Using Wizards

Mar 25, 2014

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 Setup Wizard helps you configure basic NetScaler Gateway settings for the first time.
- XenMobile Integrated Configuration helps you configure your NetScaler Gateway and XenMobile environment.
- The Quick Configuration wizard helps you configure the correct policies, expressions, and settings for connections to XenMobile App Edition, StoreFront, and the Web Interface.
- The NetScaler Gateway wizard helps you configure NetScaler Gateway-specific settings.
- The Published Applications wizard helps you configure settings for user connections by using Citrix Receiver.

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.

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 web site. For more information, see [Licensing NetScaler Gateway](#).

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

The Integrated XenMobile 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 XenMobile Configuration, see [Configuring Settings for Your XenMobile Environment](#).

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 XenApp and XenDesktop, with the ability to configure multiple instances of the Secure Ticket Authority (STA)
- XenMobile App Edition only
- StoreFront only
- XenMobile App Edition 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
- XenMobile and XenApp/XenDesktop

NetScaler Gateway supports user connections directly to XenMobile App Edition, 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 XenMobile App Edition, StoreFront, and Web Interface settings:

- Session policies, including policies and profiles for Receiver, Receiver for Web, NetScaler Gateway Plug-in, and Program Neighborhood Agent
- Clientless access
- LDAP and RADIUS authentication

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

You use the Published Applications wizard to configure NetScaler Gateway to connect to servers running XenApp or XenDesktop 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](#).

# Configuring NetScaler Gateway with the First-time Setup Wizard

Sep 18, 2013

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.

You must 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. You must 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 activation code (LAC) 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 additional settings.

# Configuring Settings with the Quick Configuration Wizard

Mar 18, 2014

You can configure settings in NetScaler Gateway to enable communication with App Controller, 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, App Controller, 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 App Controller 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 App Controller.

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)
- App Controller, 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 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 additional virtual servers and settings.

**Important:** If you use the Quick Configuration wizard to configure an additional NetScaler Gateway virtual server, you must use an 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:
  1. If the appliance is licensed for NetScaler Gateway only, click the Home tab.
  2. 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:
  1. In Name, type a name for the virtual server.
  2. In IP address, type the IP address for the virtual server.
  3. In Port, type the port number. The default port number is 443.
  4. 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:
  1. Click Choose Certificate and then in Certificate, select the certificate.
  2. Click Install Certificate and then in Choose Certificate and in Choose Key, click Browse to navigate to the certificate and private key.
  3. 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:
  1. In Primary Authentication, select LDAP, RADIUS, or Cert.
  2. 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.
  3. 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 XenMobile (App Controller) or XenApp / XenDesktop (StoreFront or Web Interface) settings.

## Configuring Enterprise Store Settings

NetScaler Gateway supports user access to web, SaaS, and mobile apps and ShareFile only through App Controller. 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:

- App Controller only
- StoreFront only
- App Controller 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 XenMobile or XenApp/XenDesktop 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 XenMobile. 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 XenApp / XenDesktop.
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 XenApp or virtual desktops from XenDesktop.
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 App Controller only

1. Click XenMobile.
2. In App Controller FQDN, enter the FQDN for App Controller.
3. Click Done.

## To configure Web Interface settings

1. In the Quick Configuration wizard, click XenApp / XenDesktop.
2. In Deployment Type, select Web Interface and then configure the following:
  1. In XenApp Site URL, type the complete IP address or FQDN of the Web Interface.
  2. In XenApp Services Site URL, type the complete IP address or FQDN of the Web Interface with the PNAgent Path. You can enter the default path or enter your own path.
  3. In Single Sign-on Domain, enter the domain to use.

4. In STA URL, type the complete IP address or FQDN of the server running the STA.
3. Click Done.

# Configuring Settings by Using the NetScaler Gateway Wizard

May 30, 2013

After you run the Setup Wizard, you can run the NetScaler Gateway wizard to configure additional 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 CA. 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.

# Configuring the Host Name and FQDN on NetScaler Gateway

Jan 22, 2014

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.

# Installing and Managing Certificates

Jan 21, 2014

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 CA. 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.

# Creating a Certificate Signing Request

Jan 22, 2014

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](#).

To 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.

To create a CSR in the configuration utility

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

1. In the configuration utility, on the Configuration tab, in the navigation pane, click SSL.
2. In the details pane, under SSL Certificates, click Create CSR (Certificate Signing Request).
3. 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.

# Installing the Signed Certificate on NetScaler Gateway

Jan 22, 2014

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.

To pair the signed certificate with a private key

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 and then click Certificates.
3. In the details pane, click Install.
4. In Certificate-Key Pair Name, type the name of the certificate.
5. In Certificate File Name, select the drop-down box in Browse and then click Appliance.
6. Navigate to the certificate, click Select and then click Open.
7. In Private Key File Name, select the drop-down box in Browse and then 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`.
8. Choose the private key and then click Open.
9. If the certificate is PEM-format, in Password, type the password for the private key.
10. If you want to configure notification for when the certificate expires, select Notifies When Expires.
11. In Notification Period, type the number of days, click Create and then click Close.

To bind the certificate and private key to a virtual server

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 and then click 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.

To unbind test certificates from the virtual server

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 and then click 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.



# Configuring Intermediate Certificates

Jan 22, 2014

An

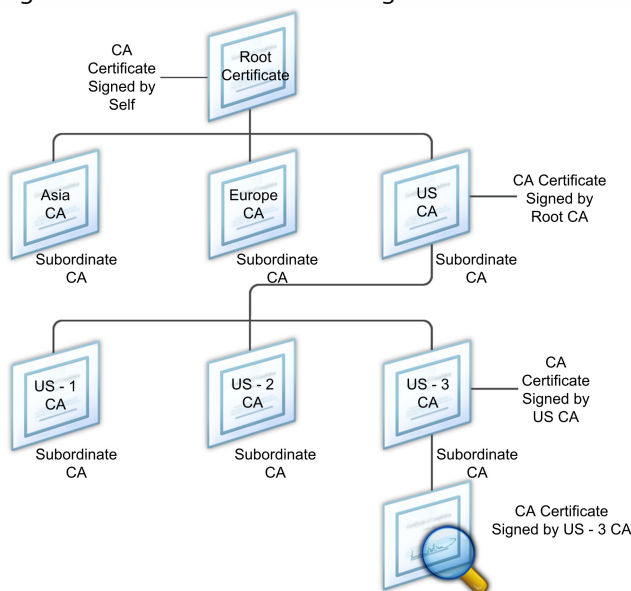
— *intermediate certificate*

is a certificate that goes between NetScaler Gateway (the server certificate) and a root certificate (usually 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 CA. 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 CA. The CAs that are directly subordinate to the root CA have CA certificates signed by the root CA. 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 CA. If a user or server certificate is signed by an intermediate CA, 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 CA, in that order. The intermediate CA's certificate is followed by the certificate of its CA. This listing continues until the last certificate in the list is for a root CA. Each certificate in the chain attests to the identity of the previous certificate.

Figure 2. A typical digital certificate chain



## To 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 drop-down box, 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.

## To 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.

# Using Device Certificates for Authentication

Jul 17, 2015

A device certificate verifies that a user device is allowed to connect to the internal network. NetScaler Gateway supports device certificates that enable you to bind the device identity to a public key.

Note: You must install NetScaler Gateway 10.1, Build 120.1316.e or newer to configure device certificates.

You can use any of the following as the device identity:

- MAC address of the network interface card installed on the device
- Device identifier
- Identification that is unique to the device

When users log on, you can require only the device certification as part of the authentication process. You can also require the device certificate when using pre-authentication or advanced endpoint analysis policies.

NetScaler Gateway needs to verify 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 the log on to NetScaler Gateway.

If you install two or more device certificates on NetScaler Gateway, users need to 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.

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 web site.
- [Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority](#) on the Microsoft System Center web site.
- [How to request a certificate from a Microsoft Certificate Authority using DCE/RPC and the Active Directory Certificate profile payload](#) on the Apple support web site.
- [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 web site.

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](#). After you install the certificate, you bind the certificate to the virtual server.

## To enable and bind device certificates on a virtual server

After you install device certificates on NetScaler Gateway, you need to enable the certificates for the relevant virtual server to activate them in your configuration.

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 Edit.
3. In the main VPN Virtual Server details pane, click the pencil icon then expand More.
4. Select Enable Device Certificate.
5. In the selection dialog that appears, select Add then click a device certificate to enable. Click the plus icon next to the

chosen device certificate and then click OK.

# Importing and Installing an Existing Certificate

Jul 09, 2015

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. In some cases, 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 new 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. For more information about replacing the Secure Gateway, see [Replacing the Secure Gateway with NetScaler Gateway](#).

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) file.
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. Follow the same steps above to create the DSA private key.

# Certificate Revocation Lists

Feb 27, 2014

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
- Day(s): Maximum 31

1. In the configuration utility, on the Configuration tab, expand SSL and then click on 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 just 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 configuration utility

A CRL is generated and published by a CA periodically or, in some cases, 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 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. This 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 should 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 CRL refresh should be performed. The option is not available if interval is set to DAILY.

##### **Time**

The exact time in 24-hour format when the CRL refresh should 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
  - Day(s)
  - Time
5. Click Create. In the CRL pane, select the CRL that you just configured and verify that the settings that appear at the bottom of the screen are correct.

# Monitoring Certificate Status with OCSP

Apr 27, 2013

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.

# Configuring OSCP Certificate Status

May 27, 2013

Configuring 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 OSCP

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 OSCP 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 needs to 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 OSCP 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.

# Testing Your NetScaler Gateway Configuration

Jan 22, 2014

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 NetScaler Gateway Plug-in.

After you install and then successfully connect with the NetScaler Gateway Plug-in, the Access Interface appears. The Access Interface is the default home page for NetScaler Gateway.

## Creating a new user account by using the configuration utility

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 may 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.

# Creating Virtual Servers

May 07, 2015

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 additional 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 App Controller, StoreFront or the Web Interface in your environment, you can use the Quick Configuration wizard to create the virtual server and all of 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 additional virtual servers

Jan 22, 2014

You can add, modify, enable or disable, and remove virtual servers by using the virtual server node in the navigation pane of the configuration utility 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](#).

To create a virtual server by using the configuration utility

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 Add.
3. Configure the settings you want, click Create and then click Close.

# Configuring Connection Types on the Virtual Server

Mar 20, 2014

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

- Connections with Citrix Receiver only to XenApp or XenDesktop without SmartAccess, endpoint analysis, or network layer tunneling features.
- Connections with the NetScaler Gateway Plug-in and SmartAccess, which allows the use of SmartAccess, endpoint analysis, and network layer tunneling functions.
- Connections with Worx Home 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. 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 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 Worx Home, the NetScaler Gateway Plug-in 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.

# Configuring a Listen Policy for Wildcard Virtual Servers

Jan 22, 2014

You can configure NetScaler Gateway virtual servers to restrict the ability for a virtual server to listen on a specific virtual local area network (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 *.  |
| 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 listen 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 should listen. The rule is:<br><b>CLIENT.VLAN.ID.EQ (&lt;ipaddressat&gt;)</b><br><br>For <ipaddressat>, substitute the ID number assigned to the VLAN.   |

To create a wildcard virtual server with a listen policy

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 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.

# Configuring IP Addresses on NetScaler Gateway

Sep 16, 2013

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. This is similar to the mapped IP (MIP) address.

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.** NetScaler Gateway uses the SNIP address.
- **File transfers from the home page.** NetScaler Gateway uses the SNIP address.
- **DNS and WINS queries.** NetScaler Gateway uses either the MIP address or SNIP address.
- **Network traffic to resources in the secure network.** NetScaler Gateway uses the MIP address, the SNIP address, or IP pooling, depending on the configuration on NetScaler Gateway.
- **ICA proxy setting.** NetScaler Gateway uses the MIP address or SNIP address.

# Changing or Deleting Mapped IP Addresses

Jan 22, 2014

NetScaler Gateway supports one mapped IP address. If you configure one mapped IP address on the appliance, you cannot change or delete the address. If you need to change the mapped IP address, you first create a new mapped IP address and then delete the original mapped IP address.

You can use either the Setup Wizard or the Network node in the configuration utility to configure additional mapped IP addresses.

## To create a new mapped 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 Mapped IP and then click Create.

## To delete a mapped 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 the mapped address and then click Remove.

# Configuring Subnet IP Addresses

Jan 22, 2014

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 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.

# Configuring IPv6 for User Connections

Jan 21, 2014

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 Receiver. User connections with the NetScaler Gateway Plug-in are not supported with IPv6.

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

- XenApp and Web Interface. When you configure IPv6 for user connections and if there is a mapped IP address that uses IPv6, XenApp 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.

# Resolving DNS Servers Located in the Secure Network

May 19, 2013

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.

# Configuring DNS Virtual Servers

May 19, 2013

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. You must 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 Citrix eDocs.

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.

# Configuring Name Service Providers

Jan 22, 2014

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 additional 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. For more information, see [Resolving DNS Servers Located in the Secure Network](#).

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.



# Configuring Server-Initiated Connections

May 28, 2013

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 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 could be logged on to NetScaler Gateway at that time:

```
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 below.

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 through the use of 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 gets 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 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.

# Configuring Routing on NetScaler Gateway

Jan 22, 2014

To provide access to internal network resources, NetScaler Gateway must be capable of routing 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 may 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 (BGP)

## Configuring a Static Route

When setting up communication with another host or network, you may 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.

# Configuring Auto Negotiation

Jan 22, 2014

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.

# Authentication and Authorization

May 07, 2015

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, as well as 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

Jul 31, 2015

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

May 27, 2013

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

May 03, 2013

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

May 07, 2015

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:

```
REQ.IP.DESTIP==10.3.0.0 -netmask 255.255.0.0
```

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 LDAP, RADIUS, 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.

## To configure an authorization policy

1. In the configuration utility, on the Configuration tab, expand 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. Click Done when your expression is complete.
7. Click Create.

## To bind an authorization policy to a user by using the configuration utility

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, select a user and then click Open.
3. On the Authorization tab, click Insert Policy.
4. Under Policy Name, double-click the policy.

5. Under Priority, set the priority number and then click OK.

#### To bind an authorization policy to a group by using the configuration utility

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. On the Authorization tab, click Insert Policy.
4. Under Policy Name, double-click the policy.
5. Under Priority, set the priority number and then click OK.

# Setting Default Global Authorization

May 10, 2013

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

Jan 24, 2014

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

Jan 24, 2014

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.
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

Jan 22, 2014

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 policies 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

Jan 22, 2014

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

Jan 22, 2014

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 configuration utility

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 configuration utility

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

Jan 22, 2014

By default, authentication policies 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

Jan 22, 2014

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

Jan 22, 2014

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.

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.

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

Jan 22, 2014

You can add users to a group either during creation of the group or at a later time. You can add users to multiple groups so users can inherit the policies and settings that are bound to those groups.

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 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

May 01, 2013

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](http://www.homepage1.com). Group2 is bound with a session policy configured with home page [www.homepage2.com](http://www.homepage2.com). When these policies are bound to respective groups without a priority number or with 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](http://www.homepage1.com), you can ensure that users who belong to both the groups will always receive the home page [www.homepage1.com](http://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.

# Configuring LDAP Authentication

Feb 24, 2014

You can configure the NetScaler Gateway to authenticate user access with one or more LDAP servers.

LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on 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 use 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 of 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,<br>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

Jan 23, 2014

1. In the configuration utility, on the Configuration tab, expand 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:

1. In Base DN (location of users), type the base DN under which users are located.

The base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of syntax for base DN are:

```
ou=users,dc=ace,dc=com
```

```
cn=Users,dc=ace,dc=com
```

2. In Administrator Bind DN, type the administrator bind DN for queries to the LDAP directory.

Examples for 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 required, 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.

3. In Administrator Password and Confirm Administrator Password, type the administrator password for the LDAP server.
10. To retrieve additional LDAP settings automatically, click Retrieve Attributes.  
When you click Retrieve Attributes, the fields under Other Settings populate automatically. If you don't want to do this, 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 should look for user logon names for the LDAP server that you are configuring. The default is `samAccountName`.
12. 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.
13. In Security Type, select the security type and then click Create.
14. 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.

Note: If you select PLAINTEXT or TLS for security, use port number 389. If you select SSL, use port number 636.

# Determining Attributes in Your LDAP Directory

May 02, 2013

If you need help 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 Web site](#). 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 need to 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

Jan 23, 2014

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 that will and will not work with NetScaler Gateway authorization, 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

May 03, 2013

LDAP servers that evaluate group memberships from group objects work with 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 work with NetScaler Gateway group extraction.

For example, in IBM Directory Server, all group memberships, including the static, dynamic, and nested groups, can be returned through the use of the `ibm-allGroups` attribute. In Sun ONE, all roles, including managed, filtered, and nested, are calculated through the use of the `nsRole` attribute.

# How LDAP Group Extraction Works from the Group Object Indirectly

May 03, 2013

LDAP servers that evaluate group memberships from group objects indirectly will not work 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 will not work with NetScaler Gateway group extraction. For this type of LDAP server, group membership searches are performed by locating the user in the member list of groups.

# LDAP Authorization Group Attribute Fields

May 03, 2013

The following table contains examples of LDAP group attribute fields:

|                                      |                 |
|--------------------------------------|-----------------|
| Microsoft Active Directory Server    | memberOf        |
| Novell eDirectory                    | groupMembership |
| IBM Directory Server                 | ibm-allGroups   |
| Sun ONE directory (formerly iPlanet) | nsRole          |

# To configure LDAP authorization

Jan 24, 2014

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

Feb 28, 2014

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.

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, such as `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 could 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

Feb 27, 2014

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 App Controller or the Web Interface in multiple domains, the domains do not need to trust each other.

# Creating Session Policies for Group Extraction

Feb 26, 2014

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.
- 
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:
    1. Next to ICA Proxy, click Override Global and then select ON.
    2. Next to Web Interface Address, click Override Global and then type the Web address of the Web Interface.
    3. 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 ChiId.
  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.

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

May 10, 2013

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 Active Directory.

Create the authentication profiles first and then create the authentication policy.

1. In the configuration utility, on the Configuration tab, expand NetScaler 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.

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

May 10, 2013

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.

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 Active Directory. Group names are also case-sensitive and the case must match the case you entered in 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.
- 
1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
  2. In the configuration utility, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
  3. In the details pane, click a virtual server and then click Open.
  4. On the Authentication tab, click Primary, under Policy Name, double-click Insert Policy and then select the first authentication policy.
  5. Under Policy Name, click Insert Policy, double-click the second authentication policy and then click OK.

# Configuring Client Certificate Authentication

Jan 23, 2014

Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. Client certificate authentication can also be used with another authentication type, such as LDAP or RADIUS, to provide two-factor authentication.

To authenticate users based on the client-side certificate attributes, client authentication should be enabled on the virtual server and the client certificate should 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. If the user does not provide a valid certificate during the Secure Sockets Layer (SSL) handshake or if 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.

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 using the client certificate.
4. In Default Authentication Type, select Cert.
5. In User Name Field, select the type of certificate field that holds the user names.
6. In Group Name Field, select the type of the certificate field that holds the group name.
7. In Default Authorization Group, type the name of the default group and then click OK.

If client certificate authentication is enabled on NetScaler Gateway, users are authenticated based on certain attributes of the client certificate. After authentication is completed successfully, the user name or the user and group name of the user are extracted from the certificate and any policies specified for that user are applied.

# Configuring and Binding a Client Certificate Authentication Policy

Jan 23, 2014

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.

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. 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.

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.

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.

# Configuring Two-Factor Client Certificate Authentication

Jan 23, 2014

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

Jun 24, 2014

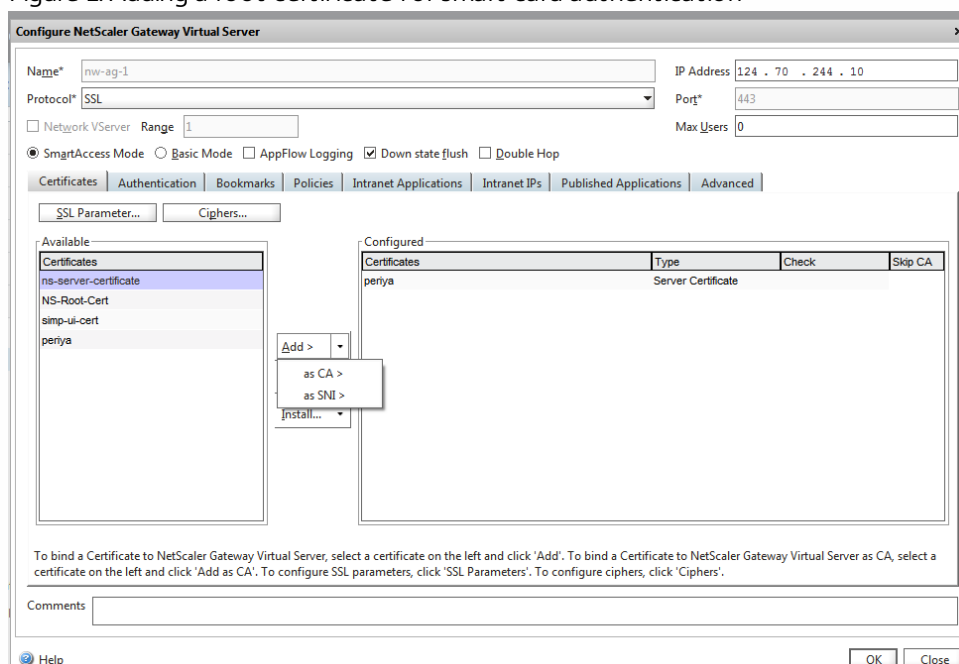
You can configure NetScaler Gateway to use a cryptographic smart card to authenticate users.

To configure a smart card to work 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 **as CA** from the Add drop-down box, as shown in the following figure.

Figure 1. Adding a root certificate for smart card authentication



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 public key infrastructure. Private keys are protected by hardware controls and never leave the smart card. Your users get the convenience 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 XenDesktop and XenApp. Smart card users logging on to StoreFront can also access applications provided by App Controller. However, users must authenticate again to access App Controller web applications that use client certificate authentication.

For more information, see [Use smart cards with StoreFront](#) in the StoreFront documentation.

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) at two different times: when logging on and when trying to start a published resource. This situation occurs if the web browser and Citrix Receiver are using the same virtual server that is configured to use client certificates. Citrix Receiver 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 click SSL.
2. In the main panel, click Change advanced SSL settings.
3. From the Deny SSL Renegotiation menu, select NO.

1. Connect the smart card to the user device.
2. Open your web browser and log on to NetScaler Gateway.

# Configuring a Common Access Card

May 10, 2013

The United States Department of Defense uses common access cards for identification and authentication.

To configure a common access card

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. On the Servers tab, click Add.
3. In Name, type a name.
4. In Authentication Type, select Cert.
5. In User Name Field, type `SubjectAltName:PrincipalName` and then click Create.
6. On the Policies tab, create a policy that uses this server and then bind the policy to the virtual server.

# Configuring RADIUS Authentication

May 27, 2013

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 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 work 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. This should 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

Jan 23, 2014

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

May 02, 2013

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

Jan 23, 2014

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 (also called RADIUS Attribute 8 Framed-IP-Address in Access Requests) that is assigned to the user. 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

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, 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

May 10, 2013

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 CTXSUserGroups=

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 CTXUserGroups=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 CTXUserGroups= groupname. If two groups are defined, such as sales and finance, the attribute value is CTXUserGroups=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

Apr 07, 2015

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

Jun 27, 2014

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. 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        |
| Acct-Terminate-Cause | Reason for account termination (see below). |           | X        |

**Table 2. 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<br>LOGOUT_SESSN_MAXLICRCHD<br>LOGOUT_SESSN_CLISECCHK_FAILED<br>LOGOUT_SESSN_PREAUTH_CHANGED<br>LOGOUT_SESSN_COOKIE_MISMATCH<br>LOGOUT_SESSS_DHT<br>LOGOUT_SESSS_2FACTOR_FAIL | RAD_TERM_NAS_REQUEST     |

| NetScaler Logout Method  | RADIUS Termination Cause |
|--------------------------|--------------------------|
| LOGOUT_SESSN_ICALIC      |                          |
| LOGOUT_SESSN_INTERNALERR | RAD_TERM_NAS_ERROR       |
| Other                    |                          |

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

Mar 05, 2014

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, that 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 relying party. The relying party simply sends the information back so that when the sending party gets the assertion along with RelayState, the sending party knows what to do next. Citrix recommends that you encrypt or obfuscate RelayState.

## 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 AD FS server to work 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 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 Relying 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 Relying 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-ADFWRelyingPartyTrust - SigningCertificateRevocationCheck None-TargetName NetScaler`

After you configure the settings, verify the relying party data before you complete the Relying 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 Relying Party Trust Wizard, select the configured trust and then edit the properties. You need to do the following:

- Set the secure hash algorithm to SHA-1.  
Note: Citrix 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 should be the following:  
`=> issue(Type = "logoutURL", Value = "https://<adfs.fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"]`

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.
- Citrix recommends that you configure actual user names instead of opaque strings.
- SAML cannot be bound as the secondary authentication type.



# To configure SAML authentication

Mar 18, 2014

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.
5. Next to Server, click New.
6. In Name, type a name for the server profile.
7. 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](#).
8. In Redirect URL, enter the URL of the authentication Identity Provider (IdP).  
This is the URL for user logon to the SAML server. This is the server to which NetScaler Gateway redirects the initial request.
9. In User Field, enter the user name to extract.
10. In Signing Certificate Name, select the private key for the certificate you selected in Step 9.  
This is the certificate that is bound to the AAA 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 SAML 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 Default authentication group, enter the group name.
13. To enable two-factor authentication, in Two Factor, click ON.
14. Disable Reject Unsigned Assertion. Enable this setting only if the SAML or IDP server is signing the SAML response.
15. Click Create and then click Close.
16. 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.

# Configuring TACACS+ Authentication

Jan 23, 2014

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

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, type a name for the policy.
5. Next to Server, click New.
6. In Name, type a name for the server.
7. Under Server, type the IP address and port number of the TACACS+ server.
8. Under TACACS server information, in TACACS Key and Confirm TACACS key, type the key.
9. In Authorization, select ON 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.

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](#).

# Configuring Multifactor Authentication

Jan 23, 2014

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 policies. 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

Jan 23, 2014

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 to 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 could 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

Mar 19, 2014

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

Jan 23, 2014

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 should 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 and then click 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

Jan 24, 2014

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 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.

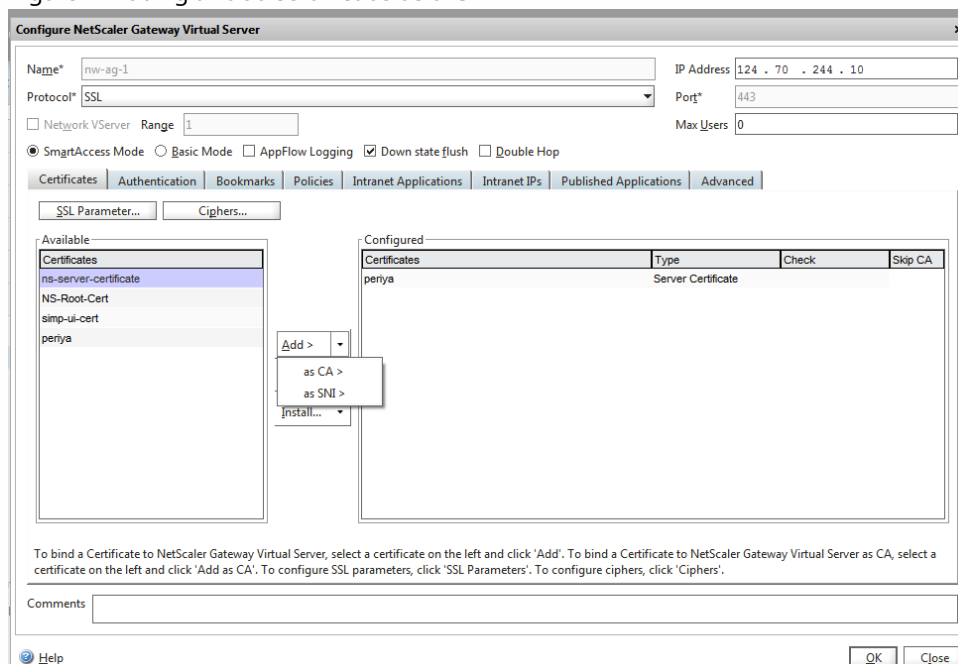
1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, click Install.
3. In Certificate - Key Pair Name, type a name for the certificate.
4. In Certificate File Name, click Browse and in the drop-down box, select 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.

Note: If you are adding a root certificate for smart card authentication, you must select as CA from the Add drop-down 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 drop down box, click as 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.

After configuring the client certificate, test the authentication by logging on to NetScaler Gateway with the NetScaler Gateway Plug-in. 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 could 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

Feb 05, 2014

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

Feb 05, 2014

Users open a connection by starting the NetScaler Gateway Plug-in from the desktop. You can specify that the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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

Feb 05, 2014

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 NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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

Feb 05, 2014

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

Feb 05, 2014

If users connect to servers running Citrix XenApp 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.

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 XenApp, see [Providing Access to Published Applications and Virtual Desktops Through the Web Interface](#).

# Configuring One-Time Password Use

Jan 22, 2014

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 NetScaler Gateway Plug-in and NetScaler Gateway is interrupted and then restored.

An attempt to reauthenticate can also occur when connections are configured to use Citrix Receiver 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

May 29, 2013

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

Feb 28, 2014

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 logon. This password return with 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 of the allowed network resources in the internal network, including App Controller, 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. You must configure the RADIUS server to return the user single sign-on password in a vendor-specific attribute value pair. In an 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 \(IANA\) web site](#). 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.

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

Jul 12, 2011

The SafeWord product line helps to provide secure authentication through the use of a token-based passcode. After users enter a passcode, it is immediately 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 work with the Citrix Web Interface. Authentication does not have to be configured on Access Gateway and can be handled by the Citrix Web Interface. 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

May 02, 2013

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 work with the 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

May 04, 2017

## Introduction

nFactor authentication enables a whole new set of possibilities with respect to authentication. Administrators using nFactor enjoy authentication, authorization, and auditing (AAA) 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.

## Use-cases

nFactor authentication enables dynamic authentication flows based on the user profile. In some cases, these could be simple flows to be intuitive to the user. In other cases, they could be coupled with securing active directory or other authentication servers. The following are some requirements specific to Gateway:

### 1. Dynamic username and password selection

Traditionally, Citrix clients (including Browsers and Receivers) use the active directory (AD) password as the first password field. The second password is usually reserved for the One-Time-Password (OTP). However, in order 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 login, user's access levels vary on NetScaler 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

In some cases, different pairs of authentication policies are used to authenticate different sets of users. Providing pair policies increases effective authentication. Dependent policies could be made from one flow. In this manner, independent sets of policies become flows of their own that increase efficiency and reduce complexity.

## Clients Support

The following table details configuration details.

| Client           | nFactor Support | Authentication Policy Bind Point | EPA |
|------------------|-----------------|----------------------------------|-----|
| Browsers         | Yes             | Auth                             | Yes |
| Citrix Receivers | No              | VPN                              | N   |
| Gateway Plug in  | No              | VPN                              | Yes |

## Authentication Response Handling

The NetScaler Gateway callback registers handle authentication responses. AAA (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.

## Command Line Configuration

The Gateway virtual server needs an authentication virtual server named as an attribute. This the only configuration required for this model.

```
>add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

The authnVsName is the name of authentication virtual server. This virtual server is should 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, as well as rfWeb clients, are modeled on responses sent by Gateway. For example, a 302 response to /vpn/index.html is expected for many clients. Also, these clients depend on various Gateway cookies such as "pwcount", "NSC\_CERT", etc.

## End Point Analysis (EPA)

Since the AAA subsystem does not support EPA for nFactor; yet, the Gateway virtual server performs EPA. After EPA, the login credentials are sent to the authentication virtual server using the aforementioned API. Once authentication is complete, Gateway continues to the post authentication 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 password(s) obtained are used for these factors. However, with nFactor the number of factors that could be configured is practically unlimited. Passwords obtained from the Gateway client are reused (as per configuration) for configured factors. Care must be taken such that one-time-password (OTP) should not be reused multiple times. Likewise, administrator must ensure that password reused at a factor is indeed applicable to that factor.

## Defining Citrix Clients

The configuration option is provided to help NetScaler determine browser clients vs. thick clients such as Receiver.

A pattern set, `ns_vpn_client_useragents`, is provided for the administrator in order to configure patterns for all Citrix clients.

Likewise, binding the “Citrix Receiver” string to the above patset to ignore all Citrix clients that have “Citrix Receiver” in the User-Agent.

## Restricting nFactor for Gateway

nfactor for Gateway authentication will not happen if the following conditions are present.

1. The `authnProfile` is not set at NetScaler Gateway.
2. Advanced authentication policies are not bound to authentication vserver and the same authentication vserver is mentioned in `authnProfile`.
3. The User-Agent string in 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 aforementioned patset, requests coming from those user-agents do not participate in the nFactor flow. For example, the command below restricts configuration for all browsers (assuming all browsers contain “Mozilla” in the user-agent string):

- o 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, etc. of the form. This includes the labels of the form itself. A customer can provide success/failure message that describe the form presented at a given point.

# 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 required.

Also, most single factor use cases with few customizations do not need loginSchema(s) configuration.

The administrator is advised to check documentation for additional configuration options that enable NetScaler to discover the factors. Once the user submits the credentials, the administrator can configure more than one factor in order 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 could be a “nextFactor” configured as a “passthrough”. A “passthrough” implies that the NetScaler should 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. Please see <https://docs.citrix.com/en-us/netscaler/11/security/aaa-tm/multi-factor-nfactor-authentication.html>.

## Username Password Expressions

In order 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 username/password that user presents. These are advanced policy expressions and can be used to override the user input as well.

## GUI Configuration

The following topics are described in this section:

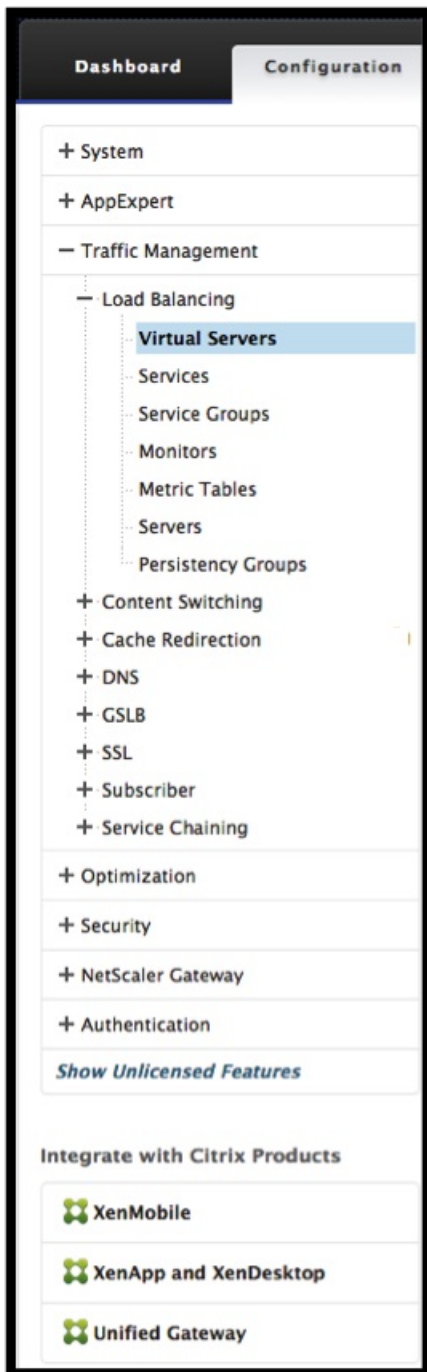
- o Create a Virtual Server
- o Create Authentication Virtual Server
- o Create Authentication CERT Profile
- o Create an Authentication Policy
- o Add an LDAP authentication server
- o Add an LDAP authentication policy



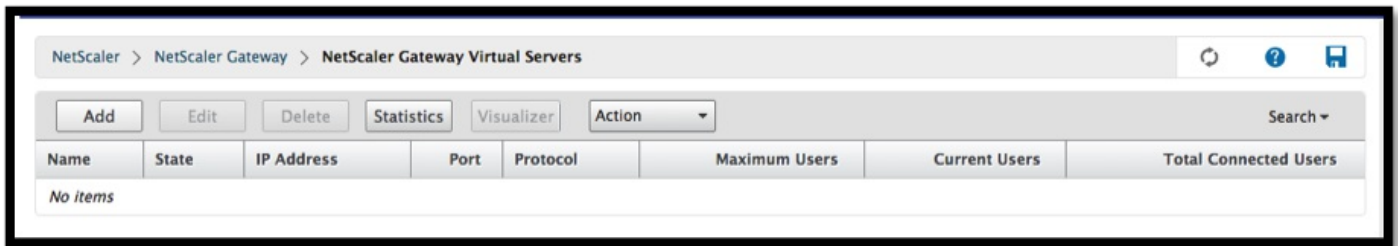
- o Add a Radius authentication server
- o Add a Radius Authentication Policy
- o Create an Authentication Login Schema
- o Create a Policy Label

## Create a Virtual Server

1. Go to NetScaler Gateway -> Virtual Servers.



- Click on the **Add** button to create a Load Balancing Virtual server.



- Enter the following information.

|  |  |
|--|--|
| Enter the Name of the virtual server.            | <p>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.</p> <p>The following requirement applies only to the NetScaler CLI:<br/>If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').</p> |
| 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.<br>Range 1 - 65535.   |
| Enter the Authentication Profile.                | Authentication Profile entity on virtual server. This entity can be used to offload authentication to AAA vserver for multi-factor (nFactor) authentication  |
| Enter the RDP Server Profile.                    | Name of the RDP server profile associated with the vserver.  |

|                                       |   |
|---------------------------------------|---|
| 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<br>Min = 1<br>Max = 255  |
| Enter the Failed Login Timeout.       | Number of minutes an account will be locked if user exceeds maximum permissible attempts<br><br>Min = 1   |
| Enter the Windows EPA Plugin Upgrade. | Option to set plugin upgrade behavior for Win   |
| Enter the Linux EPA Plugin Upgrade.   | Option to set plugin upgrade behavior for Linux   |
| Enter the MAC EPA Plugin Upgrade      | Option to set plugin upgrade behavior for Mac   |
| Login Once                            | This option enables/disables seamless SSO for this vserver.   |
| ICA Only                              | <p>- When set to ON, it implies Basic mode where the user can log on using either Citrix Receiver or a browser and get access to the published apps configured at the XenApp/XenDesktop environment pointed out by the Wihome parameter. Users are not allowed to connect using the NetScaler Gateway Plug-in 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.</p> <p>- When set to OFF, it implies Smart Access mode where the user can log on using either Citrix Receiver or a browser or a NetScaler Gateway Plug-in. 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 CVPN. The numbers of users that can log in and access the resources are limited by the CCU licenses in this mode.</p> |

|                             |   |
|-----------------------------|---|
| 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.  |
| 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. |
| Range                       |   |
| DTLS                        | This option starts/stops the turn service on the vserver  |
| 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 device certificate check as a part of EPA is on or off.   |
| Click OK                    |   |

### VPN Virtual Server

**Basic Settings**

Name\*  
Mercury

IP Address Type\*  
IP Address

IP Address\*  
10 . 217 . 28 . 164  IPv6

Port\*  
443

Authentication Profile  
[Dropdown] + [Edit] [Help]

RDP Server Profile  
[Dropdown]

Maximum Users  
0

Max Login Attempts  
75

Failed Login Timeout  
[Text Box]

Windows EPA Plugin Upgrade  
[Dropdown]

Linux EPA Plugin Upgrade  
[Dropdown]

Mac EPA Plugin Upgrade  
[Dropdown]

Login Once

ICA Only  
 Enable Authentication  
 Double Hop  
 Down State Flush  
 Range  
 1

DTLS  
 AppFlow Logging  
 ICA Proxy Session Migration  
 State  
 Enable Device Certificate

Comments  
[Text Box]

▲ Less

OK Cancel

4. Select the **No Server Certificate** section of the page.

### VPN Virtual Server

**Basic Settings**

|                        |               |                             |       |
|------------------------|---------------|-----------------------------|-------|
| Name                   | Mercury2      | Maximum Users               | 0     |
| IPAddress              | 10.217.164.28 | Max Login Attempts          | 75    |
| Port                   | 443           | Failed Login Timeout        | 3     |
| State                  | -             | ICA Only                    | true  |
| Authentication Profile | -             | Enable Authentication       | true  |
| RDP Server Profile     | -             | Windows EPA Plugin Upgrade  | -     |
| Login Once             | false         | Linux EPA Plugin Upgrade    | -     |
| Double Hop             | false         | Mac EPA Plugin Upgrade      | -     |
| Down State Flush       | false         | ICA Proxy Session Migration | false |
| DTLS                   | true          | Enable Device Certificate   | false |
| AppFlow Logging        | false         |                             |       |

**Certificates**

- No Server Certificate >
- No CA Certificate >

[Continue](#)

5. Click > to Select the Server Certificate.

### Server Certificate Binding

Select Server Certificate\*

Click to select > +

Server Certificate for SNI

[Bind](#) [Close](#)

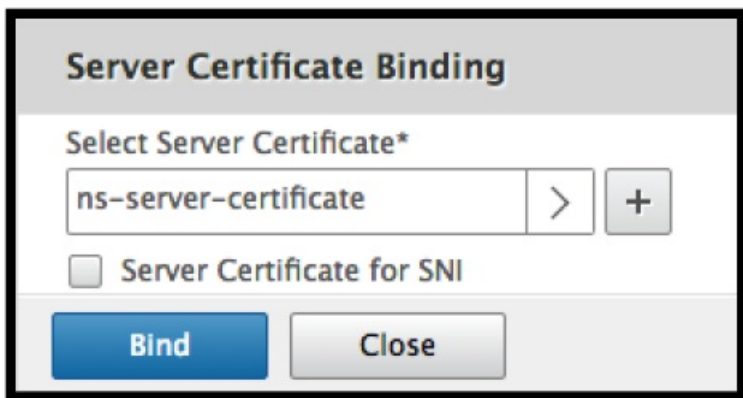
6. Select the SSL Certificate and click the **Select** button.

### SSL Certificates

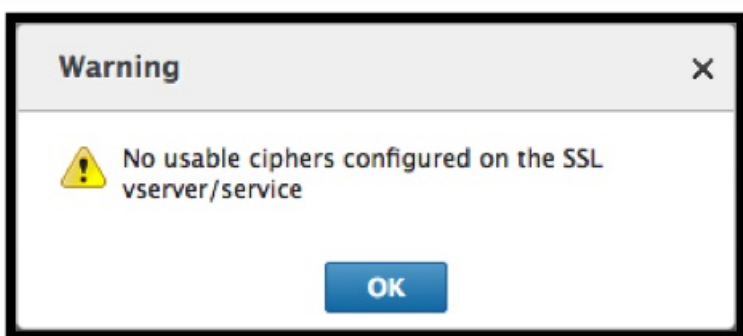
[Select](#) | [Install](#) | [Update](#) | [Delete](#) | Action ▾

| Name                  |
|-----------------------|
| ns-server-certificate |

7. Click **Bind**.



8. If you see a warning about **No usable ciphers**, click **OK**



9. Click the **Continue** button.

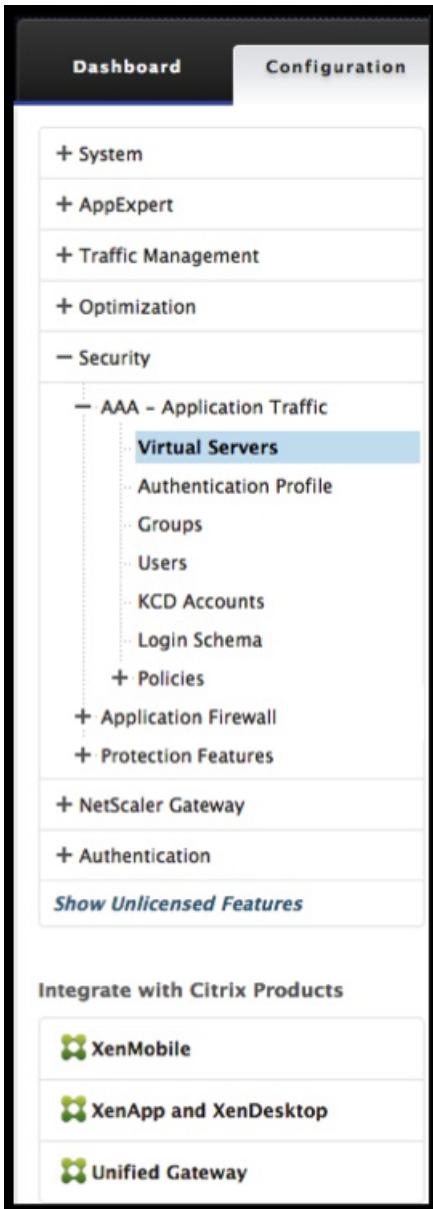


10. In the Authentication section, click the + icon in the top right.

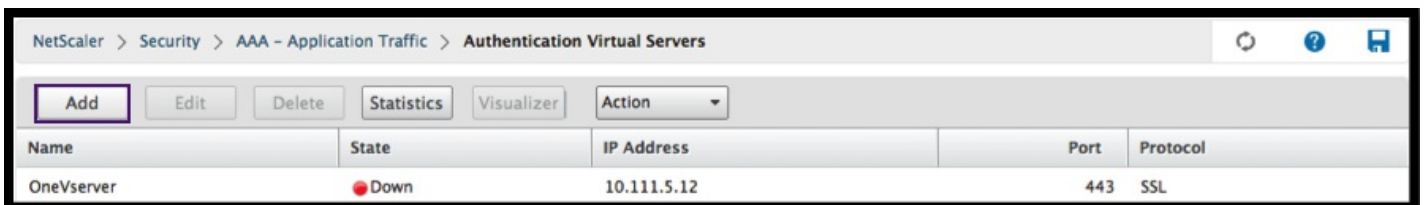


## Create Authentication Virtual Server

1. Go 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 mandatory fields are indicated by an \* to the right of the setting name.



- a) Enter the **Name** for the new authentication virtual server.
- b) Enter the **IP Address Type**. The IP Address Type can be configured as Non-addressable.
- c) Enter the **IP Address**. The IP Address can be zero.
- d) Enter the **Protocol** type of the authentication virtual server.
- e) Enter the **TCP Port** on which the virtual server accepts connections.
- f) Enter the **domain** of the authentication cookie set by Authentication virtual server.
- g) Click **OK**.

# Authentication Virtual Server

## Basic Settings

Name\*

OneVserver

(a)

IP Address Type\*

IP Address

(b)

IP Address\*

10 . 111 . 5 . 12

(c)

IPv6

Protocol

SSL

(d)

Port\*

443

(e)

Authentication Domain

(f)

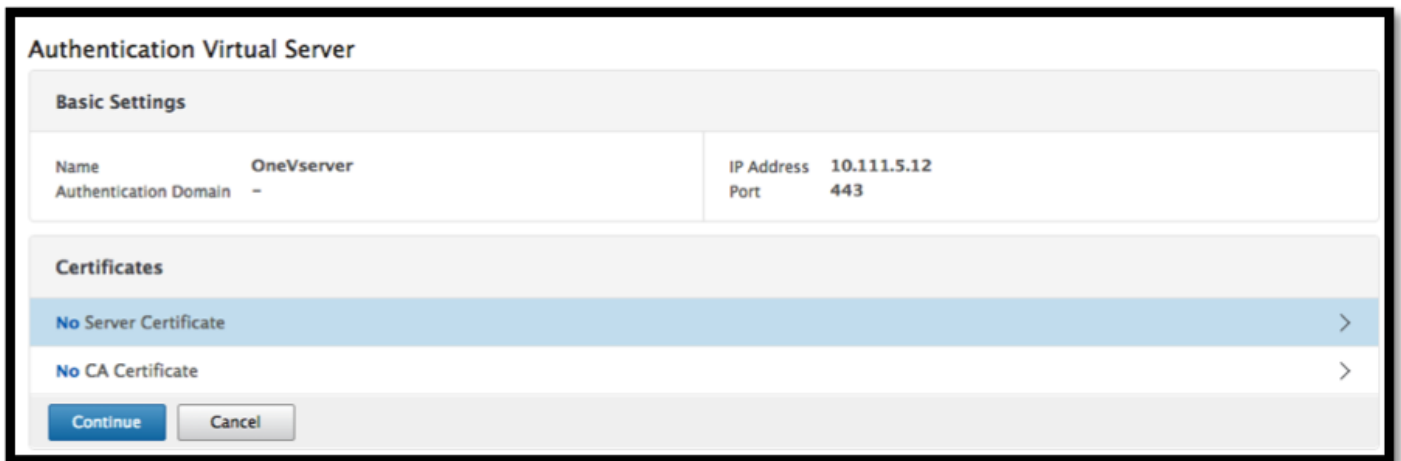
▶ More

(g)

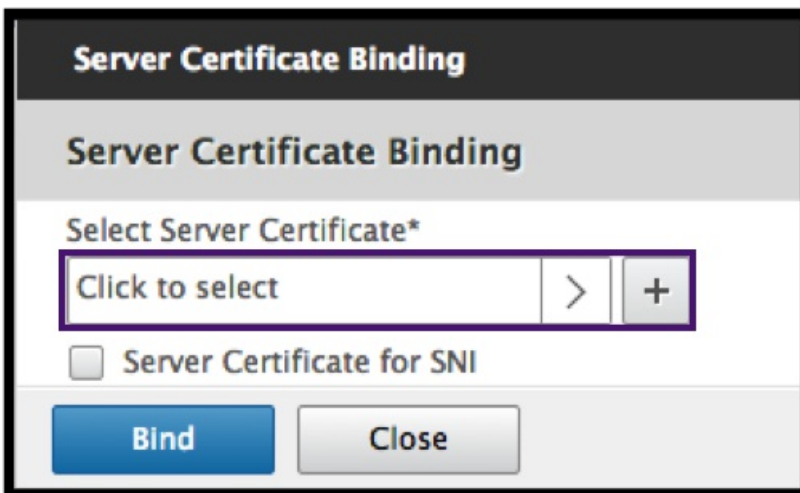
OK

Cancel

4. Click on the **No Server Certificate**.

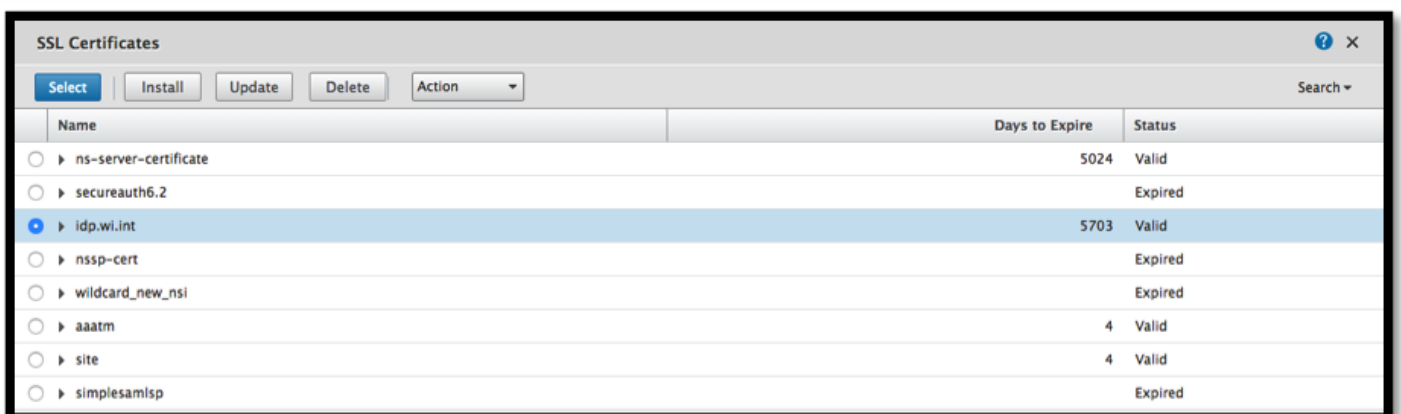


5. Select the desired Server Certificate from the pull down.



6. Choose the desired SSL Certificate and click the **Select** button.

**Note:** The Authentication virtual server does not need a certificate bound to it.



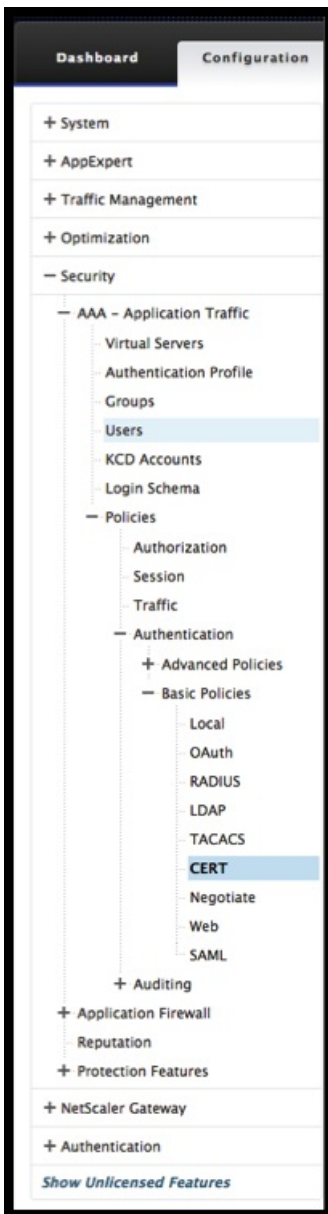
7. Configure the **Server Certificate Binding**.

- o Check the **Server Certificate for SNI** box to bind the Certkey(s) used for SNI processing.
- o Click the **Bind** button.



## Create Authentication CERT Profile

1. Go 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 mandatory fields are indicated by an \* to the right of the setting name.

- o **Name** - Name for the client cert authentication server profile (action).

- o **Two factor** – In this instance the two-factor option is NOOP.
- o **User Name Field** – enter the client-cert field from which the username is extracted. Must be set to either ""Subject"" or ""Issuer"" (include both sets of double quotation marks).
- o **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).
- o **Default Authentication Group** - This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
- o Click **Create**.

**Create Authentication CERT Profile**

Name\*  
 ? (a)

Authentication Type  
 CERT

Two Factor  
 ON  OFF (b)

User Name Field  
 (c)

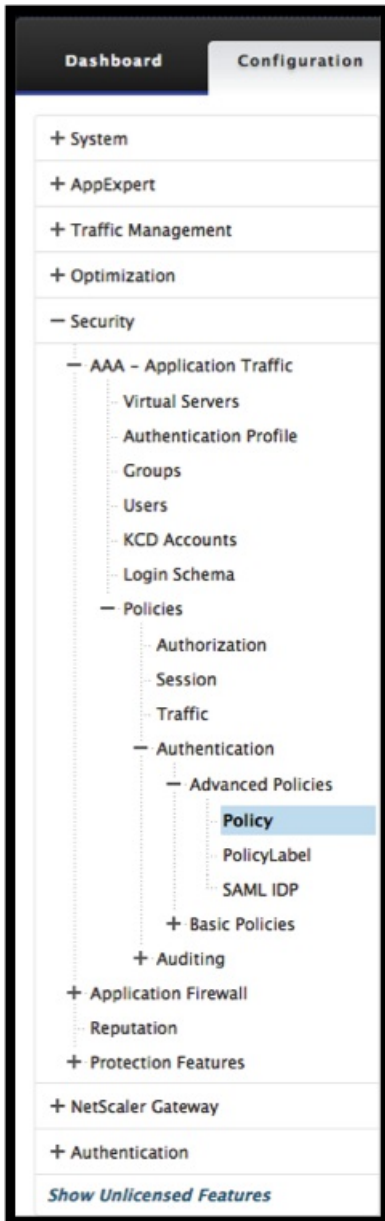
Group Name Field  
 (d)

Default Authentication Group  
 (e)

(f)

# Create an Authentication Policy

1. Go to Security -> AAA – Application Traffic -> Policies -> Authentication -> Advanced Policies -> Policy



2. Select the **Add** button

NetScaler > Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policies

Buttons: Add, Edit, Delete, Rename

Search

| Name       | Expression                                  | Request Server |
|------------|---|----------------|
| ldap       | true  | ldap-new       |
| cer        | true  | cert           |
| local      | true  | LOCAL          |
| ldap1      | true  | ldap-new1      |
| no_ldap    | http.req.user.is_member_of("group1")        | NO_AUTHN       |
| no_cert    | http.req.user.is_member_of("Domain Admins") | NO_AUTHN       |
| tac        | true  | tac            |
| radius     | true  | radius         |
| samlInf    | true  | shibboleth     |
| nopol      | true  | NO_AUTHN       |
| shibboleth | true  | shibboleth     |
| secure     | true  | secureauth_idp |
| web        | true  | webAuth2       |

3. Complete the following information to Create Authentication Policy. The mandatory fields are indicated by an \* to the right of the setting name.

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 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 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.

g) Click **Create**

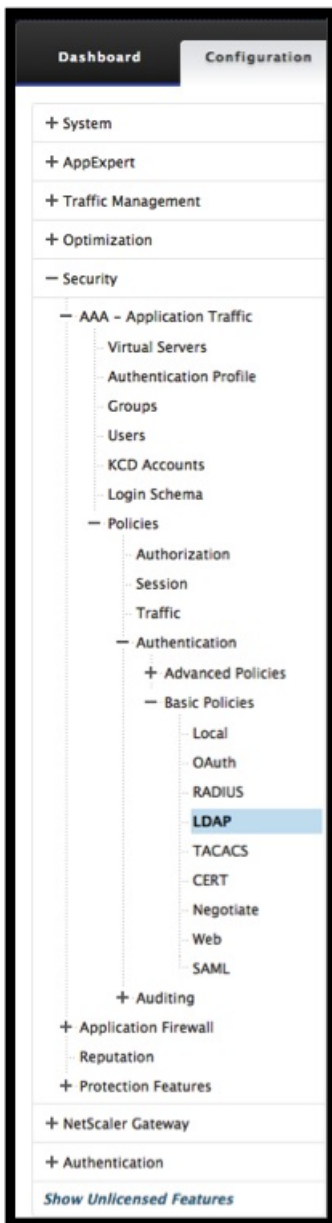


The screenshot shows the 'Create Authentication Policy' dialog box. It contains the following fields and controls:

- Name\***: A text input field containing 'Policy1', marked with callout 'a'.
- Action Type\***: A dropdown menu showing 'CERT', marked with callout 'b'.
- Action\***: A dropdown menu showing 'Profile1' with '+' and edit icons, marked with callout 'c'.
- Log Action**: A dropdown menu with '+' and edit icons, marked with callout 'd'.
- Expression\***: An 'Expression Editor' section with callout 'e'. It includes dropdowns for 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions', a 'Clear' button, and a text area containing 'true'. A green 'G' icon and 'Evaluate' button are at the bottom right of the editor.
- Comments**: A text input field marked with callout 'f'.
- Buttons**: 'Create' and 'Close' buttons at the bottom left, with 'Create' marked by callout 'g'.

## Add an LDAP Authentication Server

1. Go to Security -> AAA – Application Traffic -> Policies -> Authentication -> Basic Policies -> LDAP.



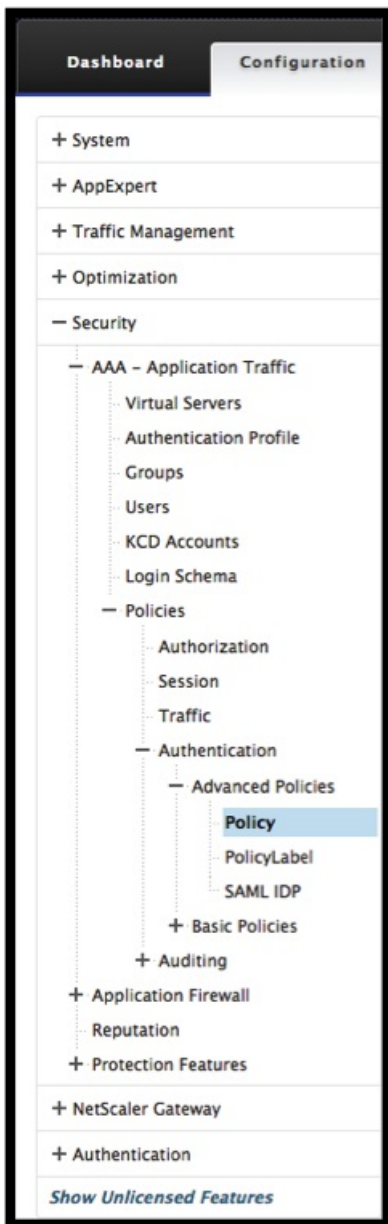
2. Add an LDAP server by selecting the **Server** tab and selecting the **Add** button.

The screenshot shows the 'Servers' tab in the Citrix NetScaler interface. The 'Add' button is highlighted with a red box. Below the buttons is a table with the following data:

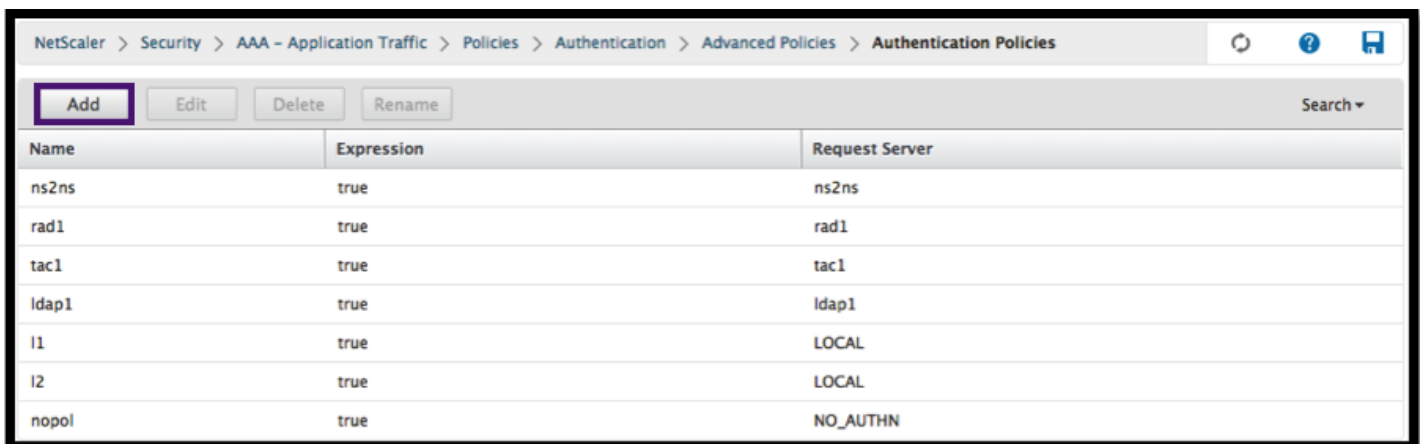
| Name       | Server Name | IP Address    | Port | Server Type | Time-out (seconds) |
|------------|-------------|---------------|------|-------------|--------------------|
| ldap1      |             | 10.217.28.180 | 389  | AD          | 3                  |
| ldap-dummy |             | 10.217.1.3    | 389  | AD          | 3                  |

## 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 Authentication Policy. The mandatory fields are indicated by an \* to the right of the setting name.

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 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.

g) Click **Create**

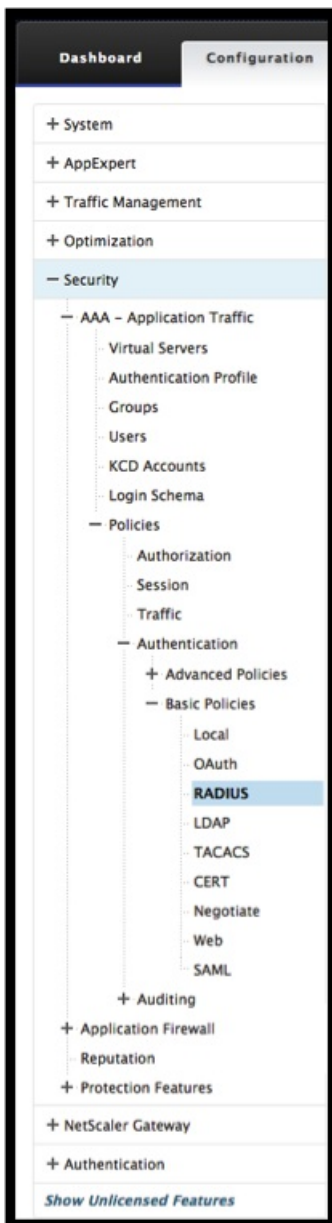
The screenshot shows the 'Create Authentication Policy' form. The fields are as follows:

- Name\***: ldap2 (marked with a circled 'a')
- Action Type\***: LDAP (marked with a circled 'b')
- Action\***: ldap1 (marked with a circled 'c')
- Log Action**: (empty, marked with a circled 'd')
- Expression\***: true (marked with a circled 'e'). The Expression Editor shows 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions' dropdowns, and an 'Evaluate' button.
- Comments**: (empty, marked with a circled 'f')

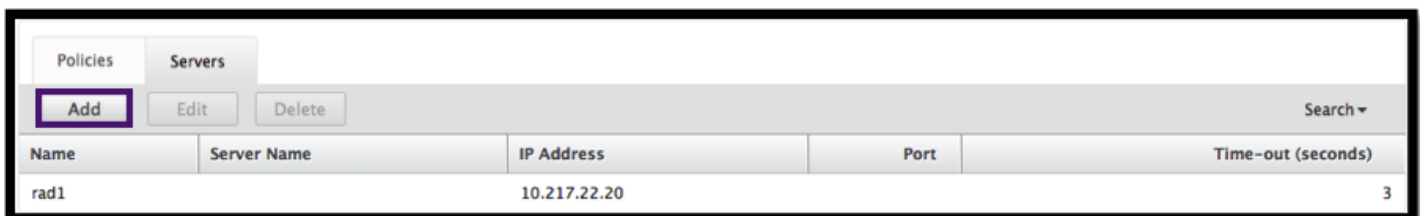
At the bottom, there are 'Create' and 'Close' buttons (marked with a circled 'g').

## Add a Radius Authentication Server

1. Go 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 mandatory fields are indicated by an \* to the right of the setting name.

- Enter a **Name** for the Radius Action
- 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 a number of seconds. This is the value that the NetScaler appliance waits for a response from the RADIUS server.
- 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.**
- g) Click **Create**

**Create Authentication RADIUS Server**

Name\*  
rad2 (a)

Server Name  Server IP

IP Address\* (b)  
10 . 220 . 25 . 10  IPv6

Port\*  
2000 (c)

Time-out (seconds)  
5 (d)

Secret Key\*  
..... (e)

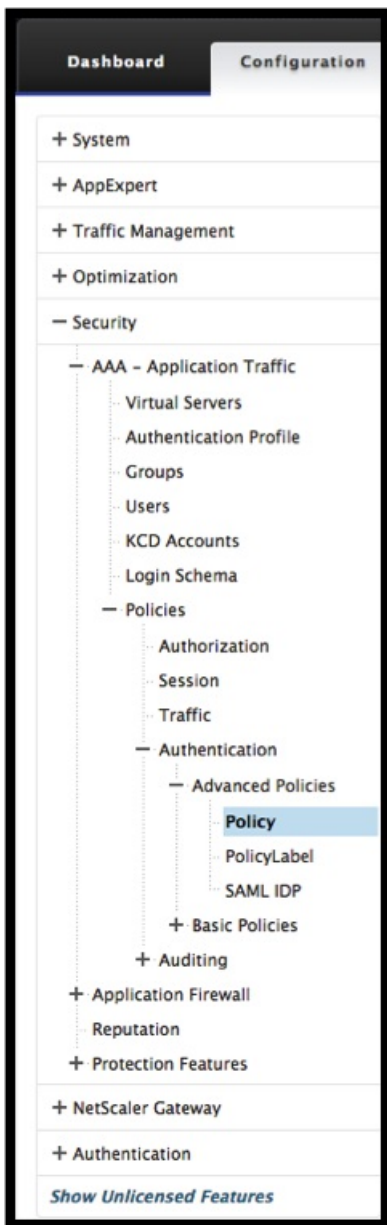
Confirm Secret Key\*  
..... (f)

▶ More (g)

**Create** Close

## Add a Radius Authentication Policy

1. Go to Security -> AAA – Application Traffic -> Policies -> Authentication -> Advanced Policies -> Policy.



2. Click **Add** to create an Authentication Policy.

NetScaler > Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policies

Buttons: Add (highlighted), Edit, Delete, Rename

Search

| Name  | Expression | Request Server |
|-------|------------|----------------|
| ns2ns | true       | ns2ns          |
| rad1  | true       | rad1           |
| tac1  | true       | tac1           |
| ldap1 | true       | ldap1          |
| l1    | true       | LOCAL          |
| l2    | true       | LOCAL          |
| nopol | true       | NO_AUTHN       |

3. Complete the following information to Create Authentication Policy. The mandatory fields are indicated by an \* to the right of the setting name.

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 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 messagelog 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.

g) Click **OK**

The screenshot shows the 'Configure Authentication Policy' dialog box. It contains the following fields and controls:

- Name:** A text input field containing 'rad1'. A circled 'a' is next to it.
- Action Type:** A dropdown menu with 'RADIUS' selected. A circled 'b' is next to it.
- Action\*:** A dropdown menu with 'rad1' selected, followed by '+' and edit icons. A circled 'c' is next to it.
- Log Action:** A dropdown menu, followed by '+' and edit icons. A circled 'd' is next to it.
- Expression:** A section with 'Expression Editor' on the right. It includes dropdowns for 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions', a 'Clear' button, and a text area containing 'true'. An 'Evaluate' button is at the bottom right. A circled 'e' is next to the 'Expression' label.
- Comment:** A text input field. A circled 'f' is next to the 'Comment' label.
- Buttons:** 'OK' and 'Close' buttons at the bottom. A circled 'g' is next to the 'OK' button.

4. Verify that your Authentication Policy is listed.



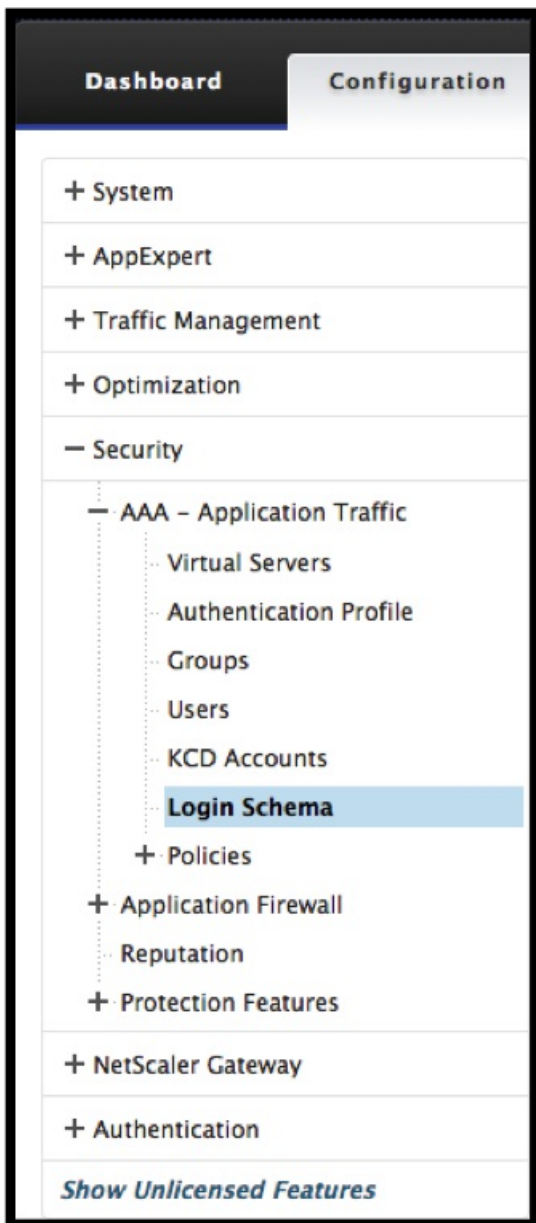
NetScaler > Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policies

Search ▾

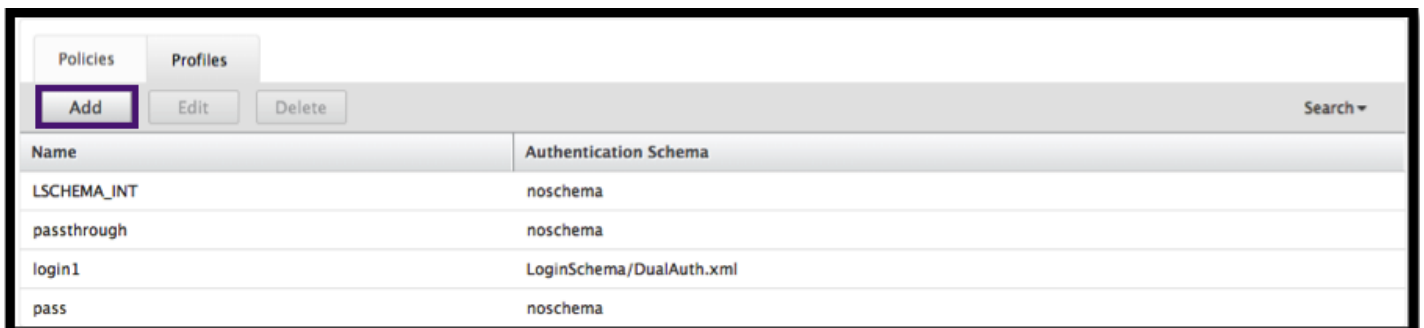
| Name   | Expression | Request Server |
|--------|------------|----------------|
| ns2ns  | true       | ns2ns          |
| rad1   | true       | rad1           |
| tac1   | true       | tac1           |
| ldap1  | true       | ldap1          |
| l1     | true       | LOCAL          |
| l2     | true       | LOCAL          |
| nopol  | true       | NO_AUTHN       |
| radius | true       | LOCAL          |

## Create an Authentication Login Schema

1. Go to Security -> AAA – Application Traffic -> Login Schema.



2. Select the Profiles tab and Click the **Add** button.



3. Complete the following fields to Create Authentication Login Schema:

a) Enter **Name** – this is the name for the new login schema.

- b) Enter **Authentication Schema** - this is the name of the file for reading authentication schema to be sent for Login Page UI. This file should contain xml definition of elements as per Citrix Forms Authentication Protocol to be able to render login form. If administrator does not want to prompt users for additional credentials but continue with previously obtained credentials, then "noschema" can be given as argument. Please note that this applies only to loginSchemas that are used with user-defined factors, and not the virtual server factor
- c) Enter **User Expression** - this is the expression for username extraction during login
- d) Enter **Password Expression** - this is the expression for password extraction during login
- e) Enter **User Credential Index** - this is the index at which user entered username should be stored in session.
- f) Enter **Password Credential Index** - this is the index at which user entered password should be stored in session.
- g) Enter **Authentication Strength** - this is the weight of the current authentication.
- h) Click **Create**

The screenshot shows the 'Create Authentication Login Schema' dialog box. It contains the following fields and controls:

- Name\***: A text input field containing 'login2', annotated with a circled 'a'.
- Authentication Schema\***: A dropdown menu showing 'LoginSchema/DualAuth.xml' and a 'Browse' button, annotated with a circled 'b'.
- User Expression**: An 'Expression Editor' section with dropdowns for 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions', a 'Clear' button, and a text area. It is annotated with a circled 'c'.
- Password Expression**: An 'Expression Editor' section with dropdowns for 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions', a 'Clear' button, and a text area. It is annotated with a circled 'd'.
- User Credential Index**: A text input field containing '4', annotated with a circled 'e'.
- Password Credential Index**: A text input field containing '3', annotated with a circled 'f'.
- Authentication Strength**: A text input field containing '0', annotated with a circled 'g'.
- Create** and **Close** buttons at the bottom, with the 'Create' button annotated with a circled 'h'.

4. Verify that your Login Schema Profile is listed.

NetScaler > Security > AAA – Application Traffic > Login Schema > Profiles

Policies Profiles

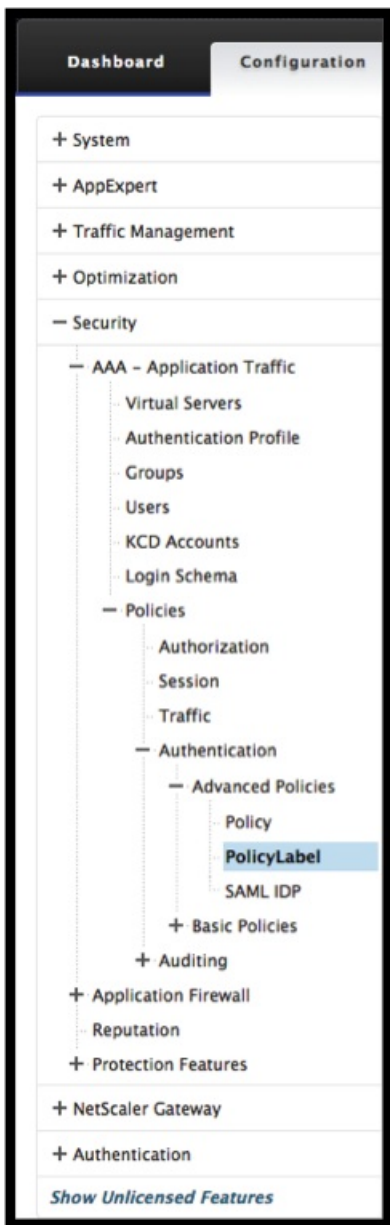
Add Edit Delete Search ▾

| Name        | Authentication Schema    |
|-------------|--------------------------|
| login2      | LoginSchema/DualAuth.xml |
| LSHEMA_INT  | noschema                 |
| passthrough | noschema                 |
| login1      | LoginSchema/DualAuth.xml |
| pass        | noschema                 |

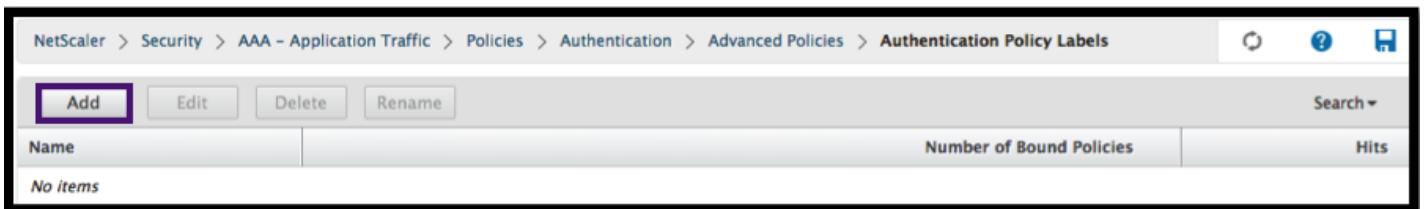
## Create a Policy Label

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. Go to Security -> AAA – Application Traffic -> Policies -> Authentication -> Advanced Policies -> Policy Label.



2. Click the **Add** button.



3. Complete the following fields to Create Authentication Policy Label:
- Enter the **Name** for the new authentication policy label.
  - Enter the **Login Schema** associated with authentication policy label.
  - Click **Continue**.

**Create Authentication Policylabel**

Name\*  
 ? a

Login Schema\*  
 + ✎ b

Comment

Continue Cancel

4. Select a **Policy** from the drop-down menu.

**Create Authentication Policylabel**

|                      |                             |
|----------------------|-----------------------------|
| Name<br>PolicyLabel1 | Login Schema<br>LSCHEMA_INT |
|----------------------|-----------------------------|

**Policy Binding**

Select Policy\*  
 > + ✎

**Binding Details**

Priority\*

Goto Expression\*

Select Next Factor  
 > + ✎

Bind Close

5. Choose the desired **Authentication Policy** and click the **Select** button.

| Authentication Policies                    |            |                 |
|--|------------|-----------------|
| Name                                       | Expression | Request Server  |
| <input type="radio"/> rad-new              | true       | rad-new         |
| <input checked="" type="radio"/> rad_22_20 | true       | rad_22_20       |
| <input type="radio"/> ldap-new             | true       | ldap-new        |
| <input type="radio"/> tac-new              | true       | tac-new         |
| <input type="radio"/> local                | true       | LOCAL           |
| <input type="radio"/> webAuth              | true       | webAuth         |
| <input type="radio"/> ldap-extraction      | true       | ldap-extraction |

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.

### Create Authentication Policylabel

|                             |                                   |
|-----------------------------|-----------------------------------|
| Name<br><b>PolicyLabel1</b> | Login Schema<br><b>LSHEMA_INT</b> |
|-----------------------------|-----------------------------------|

#### Policy Binding

Select Policy\*  
rad\_22\_20 > + ✎

► More

#### Binding Details

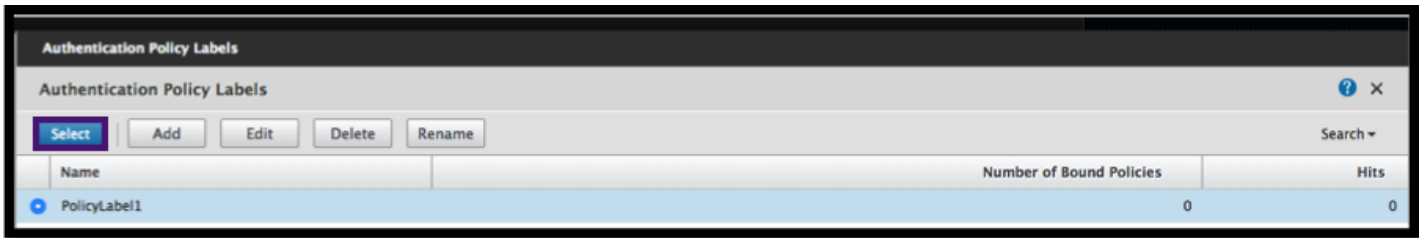
Priority\*  
100 a

Goto Expression\*  
NEXT b

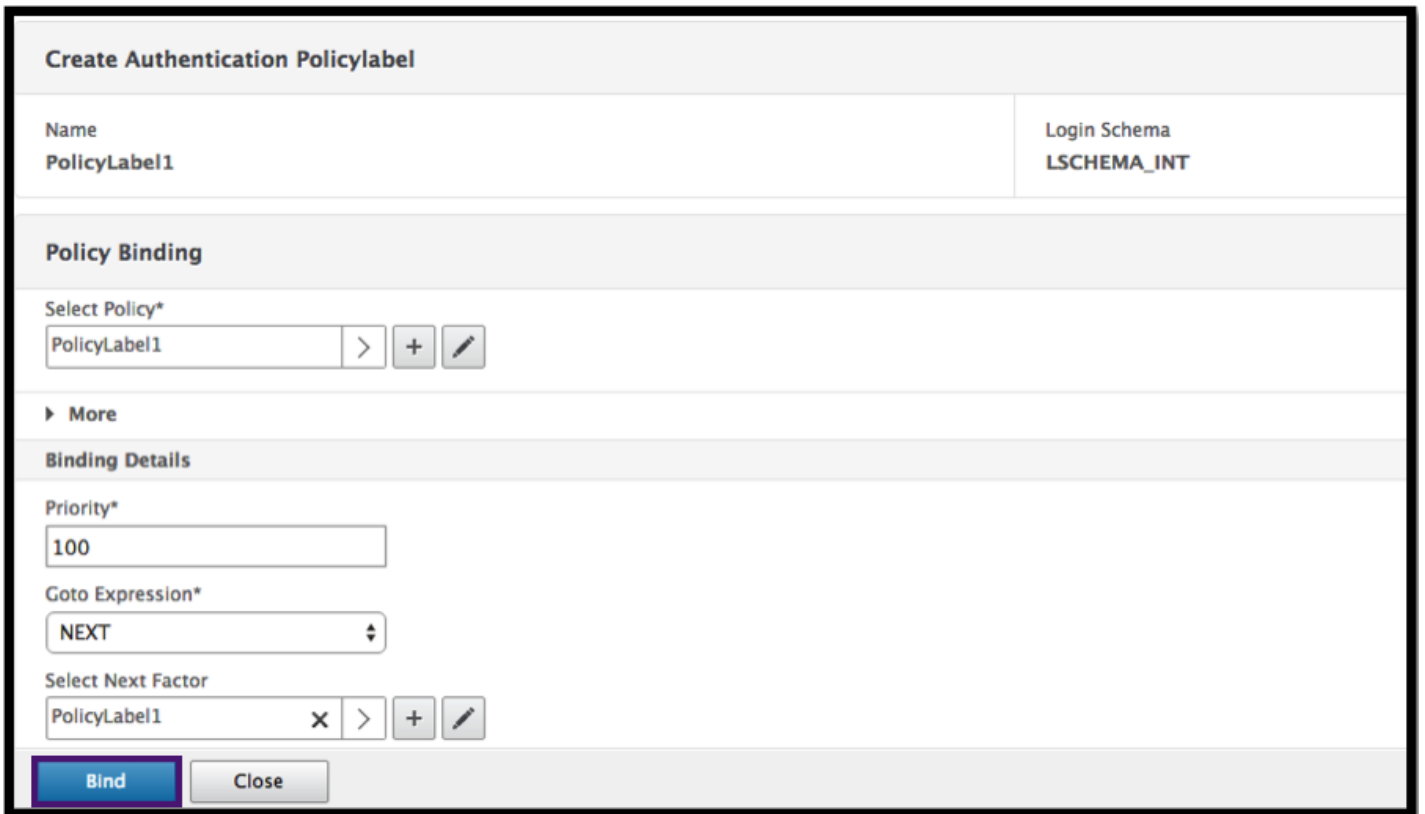
Select Next Factor  
Click to select > + ✎

**Bind** Close

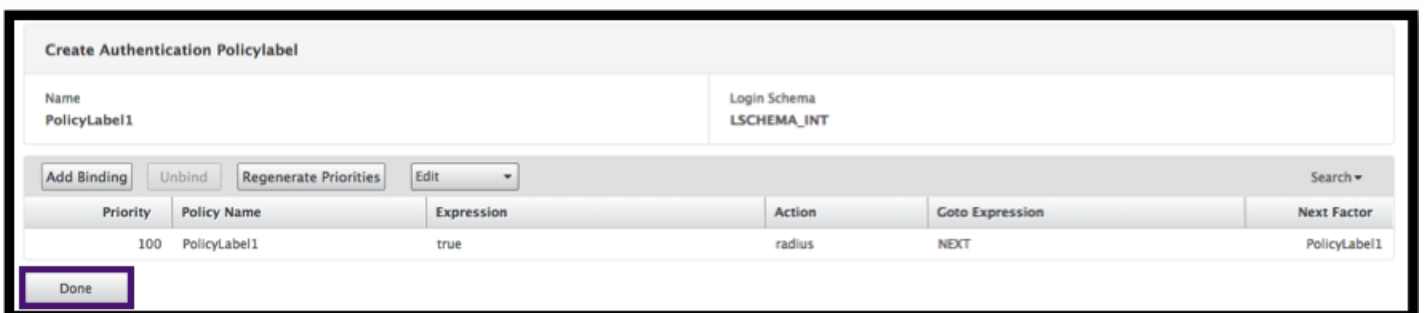
7. Select the desired Authentication Policy and click the **Select** button.



8. Click the **Bind** button.



9. Click **Done**.



10. Review the Authentication Policy Label.



NetScaler > Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policy Labels

Refresh Help Save

Add Edit Delete Rename Search ▾

| Name         | Number of Bound Policies | Hits |
|--------------|--------------------------|------|
| PolicyLabel1 | 0                        | 0    |

# Configuring the VPN User Experience

Jul 06, 2015

Users can use the following methods to connect to your organization's network resources through NetScaler Gateway:

- Citrix Receiver that contains all Citrix plug-ins installed on the user device.
- Receiver for Web that allows user connections to applications, desktops, and ShareFile by using a Web browser.
- Worx Home to allow users to access WorxMail, WorxWeb and mobile apps from their iOS and Android devices.
- NetScaler Gateway Plug-in for Windows, Mac OS X, or Linux.
- NetScaler Gateway App for iOS and Android.
- NetScaler Gateway Plug-in for Java.
- Clientless access that provides users with the access they need without installing user software.
- Interoperability with Citrix Repeater Plug-in.

If users install the NetScaler Gateway Plug-in and then install Receiver from XenApp 6.5 for Windows Server 2008 (including Feature Pack and Feature Pack 2), XenDesktop 7.0 or newer, Receiver automatically adds the NetScaler Gateway Plug-in. Users can connect with the NetScaler Gateway Plug-in from a web browser or from Receiver.

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 XenMobile Worx apps for iOS and Android mobile devices. NetScaler Gateway contains Secure Browse that allows connections to NetScaler Gateway from iOS mobile devices that establishes the Micro VPN tunnel. Android devices that connect with Worx Home 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 Worx apps, you must configure DNS settings on NetScaler Gateway. For details, see [Supporting DNS Queries by Using DNS Suffixes for Android Devices](#).

# How User Connections Work with the NetScaler Gateway Plug-in

Feb 03, 2014

NetScaler Gateway operates as follows:

- When users attempt to access network resources across the VPN tunnel, the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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.

# Establishing the Secure Tunnel

Feb 03, 2014

When users connect with the NetScaler Gateway Plug-in, Worx Home, or Citrix Receiver, 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 NetScaler Gateway Plug-in, Worx Home, or Receiver describing the networks to be secured and containing an IP address if you enable address pools.

When the NetScaler Gateway Plug-in 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. Receiver must support the NetScaler Gateway Plug-in to establish the connection through the secure tunnel when users log on.

Worx Home, Worx 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 NetScaler Gateway Plug-in 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.

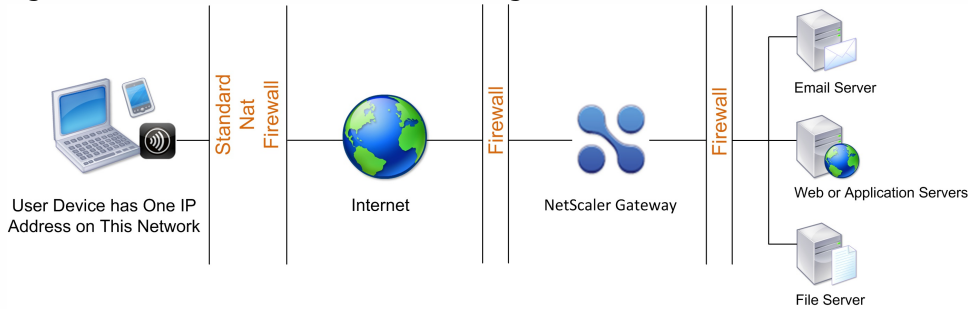
Locally, on the user device, all connection-related traffic, such as SYN-ACK, PUSH, ACK, and FIN packets, is recreated by the NetScaler Gateway Plug-in to appear from the private server.

# Operation Through Firewalls and Proxies

Jan 31, 2014

Users of the NetScaler Gateway Plug-in are sometimes located inside another organization's firewall, as shown in the following figure:

Figure 1. Connection from user device through two internal firewalls



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.

# NetScaler Gateway Plug-in Upgrade Control

Sep 16, 2015

## Overview

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 user interface:

- At the Global Settings
- At the Session Profile level

For each client type, NetScaler Gateway allows the following three options to control plug-in upgrade behavior:

a. **Always**

The plug-in always gets upgraded whenever the end user's plug-in version doesn't match with the plug-in shipped with NetScaler. This is the default behavior. Choose this option if you don't want multiple plug-in versions running in your enterprise.

b. **Essential** (and security)

The plug-in only upgraded when it is deemed necessary. Upgrades are deemed necessary in following two circumstances

1. Installed Plug-in is incompatible with current NetScaler version.
2. Installed Plug-in needs to be updated for necessary security fix.

You should 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

c. **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

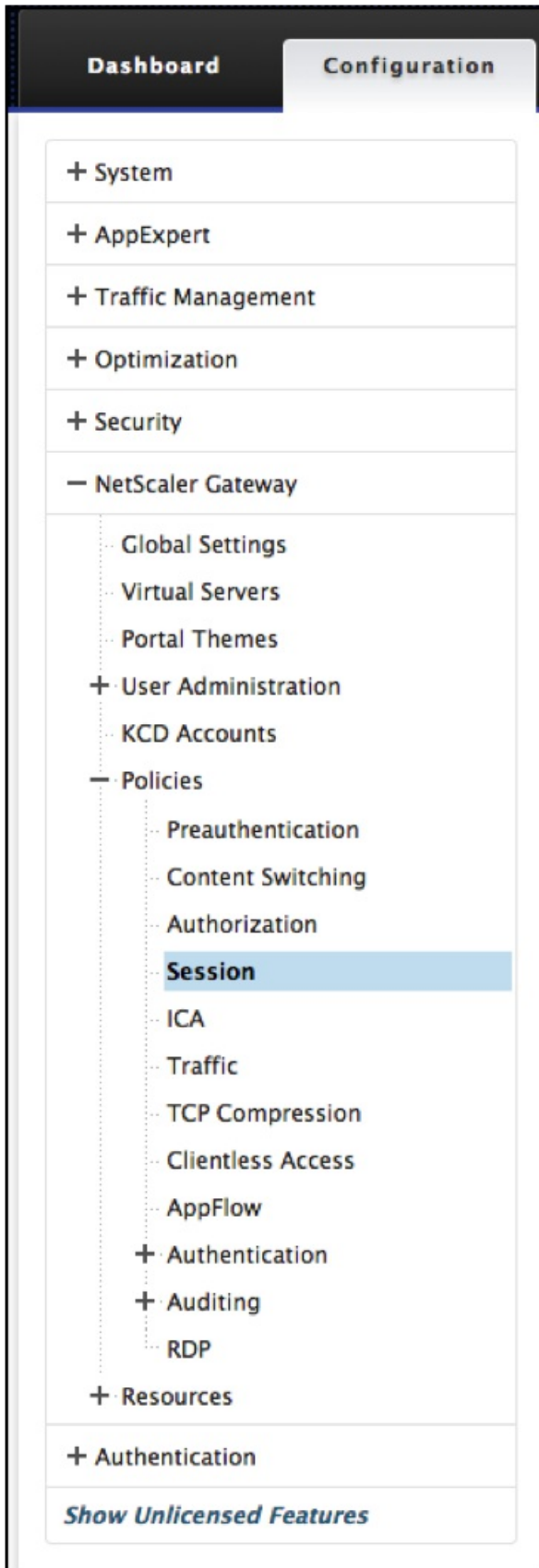
NetScaler Gateway supports EPA plug-ins for Windows and Mac operating systems. To support EPA plug-in upgrade control at the Vserver level, NetScaler Gateway supports two Vserver parameters named windowsEPAPuginUpgrade and macEPAPuginUpgrade.

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 Gateway>Policies>Session.



2. Select the desired session policy, and then click **Edit**.



| Session Policies     |  | Session Profiles |                 |          |
|----------------------|--|------------------|-----------------|----------|
| Name                 | Expression   | Action           | Globally Bound? | Priority |
| SETVPNPARAMS_POL     | ns_true  | SETVPNPARAMS_ACT | ✗               | -NA-     |
| 10.207.27.15_443_POL | NS_TRUE  | 10.207.27.15_443 | ✗               | -NA-     |
| test2                | CLIENT.APPLICATION(MAC-FIREWALL_1003_VERSION_<_... | test 2           | ✗               | -NA-     |

3. Click the + icon.

### Configure NetScaler Gateway Session Policy

Name

Action\*  
 +

Expression\* OPSWAT EPA Editor Expression Editor

NS\_TRUE

4. Select the **Client Experience** tab.

Name\*  ?

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration
Client Experience
Security
Published Applications
Remote Desktop

Override Global

DNS Virtual Server

WINS Server IP

Kill Connections\*

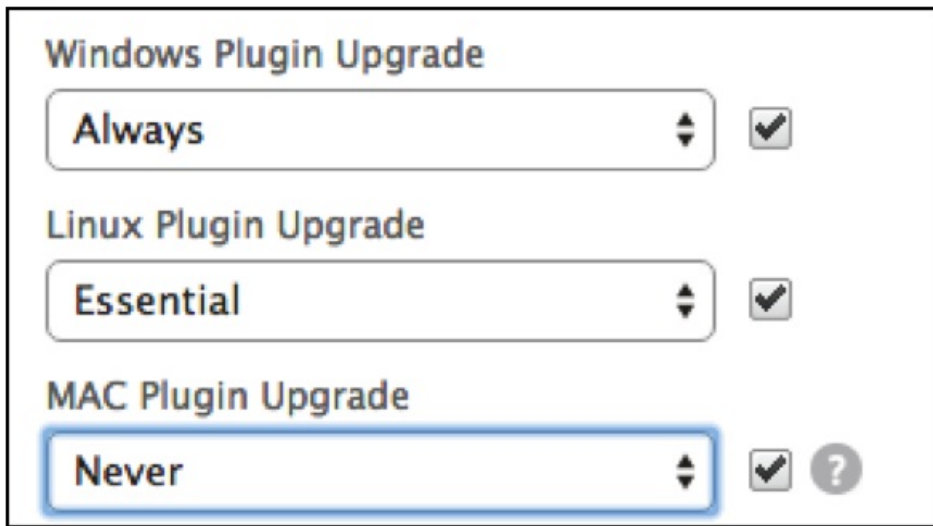
**Advanced Settings**

5. These dialog boxes options affect the upgrade behavior.

- Always
- Essential
- Never

The default is Always.

6. Select the check box to the right of each option. Select the frequency to apply the upgrade behavior.

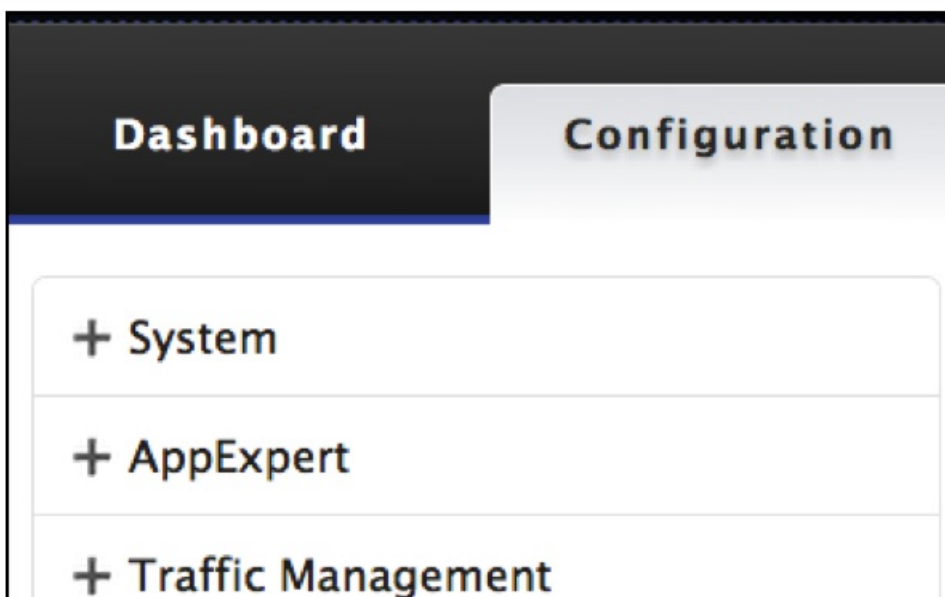


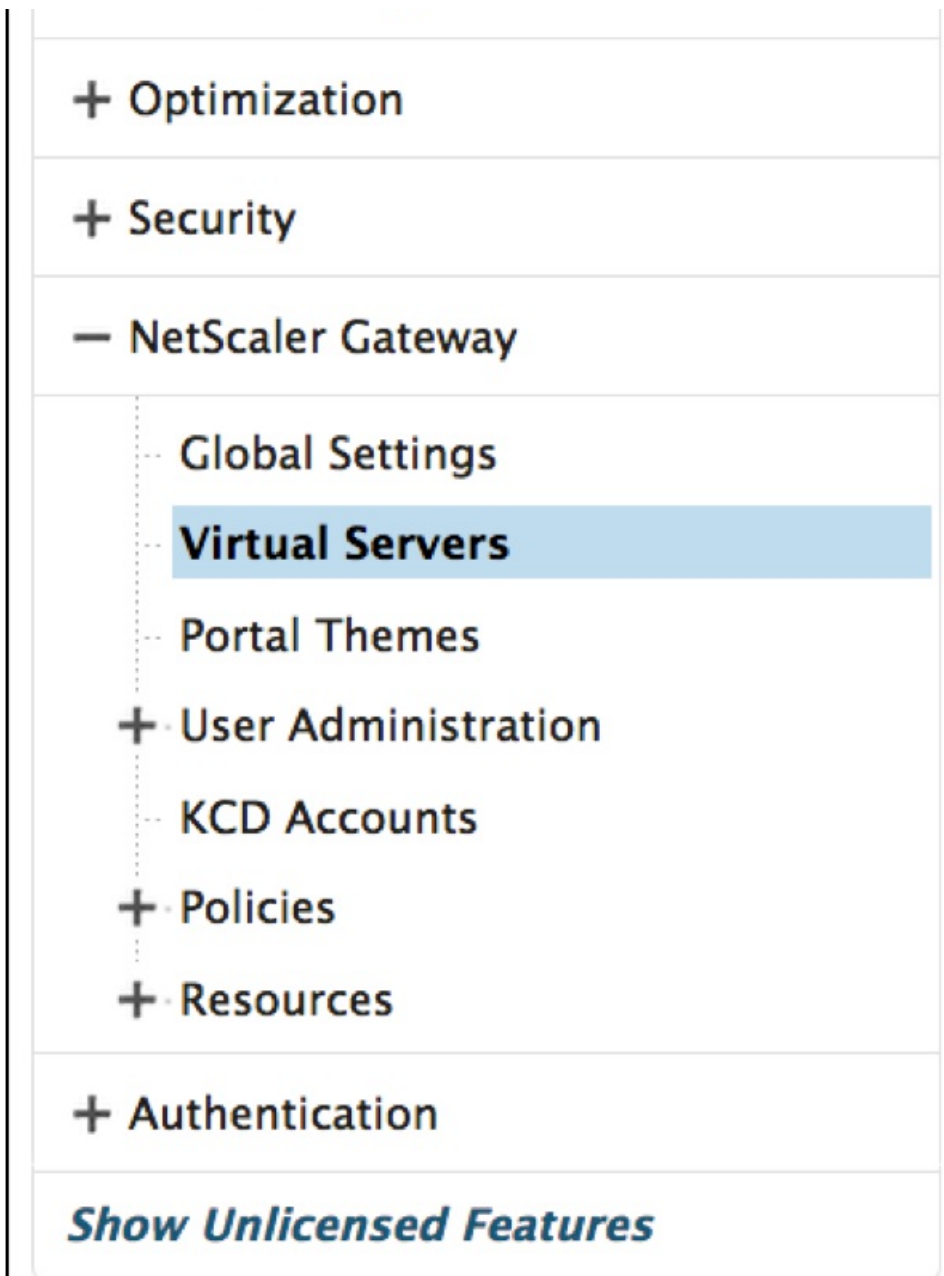
The screenshot shows a configuration dialog box with three sections: "Windows Plugin Upgrade", "Linux Plugin Upgrade", and "MAC Plugin Upgrade". Each section has a dropdown menu and a checkbox. The "Windows Plugin Upgrade" dropdown is set to "Always" and the checkbox is checked. The "Linux Plugin Upgrade" dropdown is set to "Essential" and the checkbox is checked. The "MAC Plugin Upgrade" dropdown is set to "Never" and the checkbox is checked. A question mark icon is visible next to the "MAC Plugin Upgrade" checkbox.

## 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.

| <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Statistics"/> <input type="button" value="Visualizer"/> <input type="button" value="Action"/> |                                       |              |      |          |               |               | Search ▾ |
|--|---------------------------------------|--------------|------|----------|---------------|---------------|----------|
| Name   | State                                 | IP Address   | Port | Protocol | Maximum Users | Current Users |          |
| Vulcan   | <span style="color:red">●</span> Down | 10.207.27.24 | 443  | SSL      | 0             | 0             |          |
| Twilight   | <span style="color:green">●</span> Up | 10.127.27.80 | 443  | SSL      | 0             | 0             |          |
| Dolphin  | <span style="color:green">●</span> Up | 10.208.28.24 | 443  | SSL      | 0             | 0             |          |
| Quicksilver  | <span style="color:green">●</span> Up | 20.20.15.9   | 443  | SSL      | 0             | 0             |          |
| Quicksilver2   | <span style="color:green">●</span> Up | 20.20.15.8   | 443  | SSL      | 0             | 0             |          |
| Minerva  | <span style="color:green">●</span> Up | 20.20.20.3   | 443  | SSL      | 0             | 0             |          |
| Pluto  | <span style="color:green">●</span> Up | 15.15.9.7    | 443  | SSL      | 0             | 0             |          |
| Penquin  | <span style="color:red">●</span> Down | 2.3.4.3      | 443  | SSL      | 0             | 0             |          |
| UG_VPN_UG-Virtual-Server-1   | <span style="color:green">●</span> Up | 0.0.0.0      | 0    | SSL      | 0             | 0             |          |

3. Click the **pencil** icon.

### VPN Virtual Server

Basic Settings

✎

Help >

|  |  |   |
|--|--|---|
| <p>Name <b>Quicksilver</b></p> <p>IPAddress <b>20.20.15.9</b></p> <p>Port <b>443</b></p> <p>State <span style="color:green">●</span> <b>Up</b></p> <p>RDP Server Profile <b>-</b></p> <p>Login Once <b>false</b></p> <p>Double Hop <b>false</b></p> <p>Down State Flush <b>true</b></p> <p>DTLS <b>false</b></p> <p>AppFlow Logging <b>false</b></p> | <p>Maximum Users <b>0</b></p> <p>Max Login Attempts <b>-</b></p> <p>Failed Login Timeout <b>-</b></p> <p>ICA Only <b>false</b></p> <p>Enable Authentication <b>true</b></p> <p>Windows EPA Plugin Upgrade <b>-</b></p> <p>Linux EPA Plugin Upgrade <b>-</b></p> <p>Mac EPA Plugin Upgrade <b>-</b></p> <p>ICA Proxy Session Migration <b>false</b></p> <p>Enable Device Certificate <b>false</b></p> | <p><b>Advanced Settings</b></p> <ul style="list-style-type: none"> <li><a href="#">+ Content Switching Policies</a></li> <li><a href="#">+ SSL Profile</a></li> <li><a href="#">+ SSL Ciphers</a></li> <li><a href="#">+ SSL Policies</a></li> <li><a href="#">+ Intranet IP Addresses</a></li> <li><a href="#">+ Intranet Applications</a></li> <li><a href="#">+ Published Applications</a></li> <li><a href="#">+ Portal Themes</a></li> <li><a href="#">+ EULA</a></li> </ul> |
|--|--|---|

**Certificates**

✎

- 1 Server Certificate
>
- No CA Certificate
>

**Authentication**

+

- Primary Authentication
>
- 1 Local Policy
>

4. Click **More**

## VPN Virtual Server

### Basic Settings

Name  
Quicksilver

IP Address Type  
IP Address

IPAddress\*  
20 . 20 . 15 . 9  IPv6

Port  
443

▶ More

OK Cancel

5. The dialog boxes that appear affect the upgrade behavior. The options available are

- Always
- Essential
- Never

# VPN Virtual Server

**Basic Settings**

Name  
Quicksilver

IP Address Type  
IP Address

IPAddress\*  
20 . 20 . 15 . 9  IPv6

Port  
443

RDP Server Profile

Maximum Users  
0

Max Login Attempts

Failed Login Timeout

Windows EPA Plugin Upgrade  
Always

Linux EPA Plugin Upgrade  
Essential

Mac EPA Plugin Upgrade  
Never

# Requirements

Windows EPA and VPN plug-in => version should be greater than 11.0.0.0

Mac EPA plug-in => version should be greater than 3.0.0.31

Mac VPN plug-in => version should be greater than 3.1.4 (357)

If NetScaler is upgraded to 11.0 release, all previous VPN (and EPA) plug-ins will upgrade to the latest version irrespective of upgrade control configuration. For subsequent upgrades, they will respect the above upgrade control configuration.



# Choosing the User Access Method

Feb 03, 2014

You can configure NetScaler Gateway to provide user connections through the following scenarios:

- User connections by using Citrix Receiver. Receiver works with StoreFront or the Web Interface to provide users with access to published applications or virtual desktops in a server farm. Receiver is software that uses the ICA network protocol to establish user connections. Users install Receiver on the user device. When users install Receiver on their Windows-based or Mac-based computer, Receiver subsumes all plug-ins, including the NetScaler Gateway Plug-in for user connections. NetScaler Gateway also supports connections from Receiver for Android and Receiver for iOS. Users can connect to their virtual desktops and Windows-based, web, mobile, and SaaS applications through App Controller, StoreFront, or the Web Interface.
- User connections with Worx Home. Users can connect to mobile, web, and SaaS applications configured in App Controller. Users install Worx Home on their mobile device (Android or iOS). When users log on to Worx Home, they can install WorxMail and WorxWeb, along with any other mobile app you installed in App Controller. Worx Home, WorxMail, and WorxWeb use Micro VPN technology to establish connections through NetScaler Gateway.
- User connections by using the NetScaler Gateway Plug-in as a standalone application. The NetScaler Gateway Plug-in 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 Web sites.
- User connections by using clientless access. Clientless access provides users with the access they need without requiring installation of software, such as the NetScaler Gateway Plug-in or Receiver, 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 XenApp, virtual desktops from Citrix XenDesktop, 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 NetScaler Gateway Plug-in to StoreFront or the Web Interface, by using Receiver, if the user device does not pass the initial endpoint analysis scan. If users log on to NetScaler Gateway through Receiver, the preauthentication scan does not work. Post-authentication scans do work when NetScaler Gateway establishes the VPN tunnel.

Users can download and install the NetScaler Gateway Plug-in 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 Merchandising Server.



# Deploying NetScaler Gateway Plug-ins for User Access

Feb 27, 2014

NetScaler Gateway comes with the following plug-ins for user access:

- NetScaler Gateway Plug-in for Windows
- NetScaler Gateway Plug-in for Mac
- NetScaler Gateway Plug-in for Java

When users log on to NetScaler Gateway for the first time, they download and install the NetScaler Gateway Plug-in from a web page. Users log on by clicking the NetScaler Gateway icon in the notification area on a Windows-based computer. On a Mac OS X computer, users can log on from the Dock or the Applications menu. If you upgrade NetScaler Gateway to a new software version, the NetScaler Gateway Plug-in updates automatically on the user device.

The NetScaler Gateway Plug-in for Java can be used on any user device that supports Java. The NetScaler Gateway Plug-in for Java supports most TCP-based applications, but provides only some of the features of the NetScaler Gateway Plug-in for Windows or NetScaler Gateway Plug-in for Mac OS X. The NetScaler Gateway Plug-in for Java provides limited access to the network resources you define. For more information about the Java plug-in, see [Connecting with the NetScaler Gateway Plug-in for Java](#).

You can also deploy the NetScaler Gateway Plug-in with Citrix Receiver Updater. When users install Receiver Updater, it automatically adds all user plug-ins installed on the user device to Receiver. Users log on to the NetScaler Gateway Plug-in with Receiver by opening Receiver and then right-clicking the NetScaler Gateway Plug-in and then clicking Logon. If you upgrade the NetScaler Gateway appliance to a new version, the NetScaler Gateway Plug-in within Receiver upgrades automatically to the new version.

You can deploy the NetScaler Gateway Plug-in 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 include:

- 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 additional 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 NetScaler Gateway Plug-in from Active Directory](#).

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.

# Selecting the NetScaler Gateway Plug-in for Users

Feb 03, 2014

When you configure NetScaler Gateway, you can choose how users log on. Users can log on with one of the following plug-ins:

- NetScaler Gateway Plug-in for Windows
- NetScaler Gateway Plug-in for Mac OS X
- NetScaler Gateway Plug-in for Java

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/Mac OS X or Java as the plug-in type. When users log on, they receive the plug-in as defined globally or in the session profile and policy. You must create separate profiles for the plug-in type. You can only choose either Windows/Mac OS X or Java in the session profile. To configure the NetScaler Gateway Plug-in for Java, see [Connecting with the NetScaler Gateway Plug-in for Java](#).

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/Mac OS X and then click OK.

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 new 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 new 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/Mac OS X.
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.

If you are configuring the NetScaler Gateway Plug-in 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.

# Installing the NetScaler Gateway Plug-in for Windows

Feb 03, 2014

When users log on to NetScaler Gateway, they download and install the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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 might need to 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 NetScaler Gateway Plug-in 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 an 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 NetScaler Gateway Plug-in from Receiver or by using a web browser. Provide instructions to users about how to log on with the NetScaler Gateway Plug-in through Receiver or a web browser.

Because users work with files and applications as if they were 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 NetScaler Gateway Plug-in on their computer.

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 NetScaler Gateway Plug-in connects and displays a message in the notification area on a Windows-based computer.

If you want users to connect with the NetScaler Gateway Plug-in 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.

To configure the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in for logon.

Note: If users open the Configure NetScaler Gateway dialog box from within Receiver, the Options tab is not available.

# Deploying the NetScaler Gateway Plug-in from Active Directory

Jan 31, 2014

If users do not have administrative privileges to install the NetScaler Gateway Plug-in on the user device, you can deploy the plug-in for users from Active Directory.

When you use this method to deploy the NetScaler Gateway Plug-in, 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 NetScaler Gateway Plug-in package by using a Group Policy Object.

Note: Distribution of the NetScaler Gateway Plug-in from Active Directory is only supported on Windows XP, Windows Vista, Windows 7, and Windows 8.

You can download the MSI package from the configuration utility or from the Citrix web site.

1. In the configuration utility, click Downloads.
2. Under NetScaler Gateway Plugin, click Download NetScaler Gateway Plugin for Windows and then save the file `nsvpnc_setup.exe` to your Windows server.  
Note: If the File Download dialog box does not appear, press the CTRL key when you click the link Download NetScaler Gateway Plugin 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`.
4. Save the extracted file to a folder on the Windows server.

After you extract the file, you 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 NetScaler Gateway Plug-in, Citrix recommends assigning the package to the user device. The MSI package is designed to be 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 Microsoft Internet Security and Acceleration (ISA) Server.

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 a 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 NetScaler Gateway Plug-in.
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 NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in is installing.



# Upgrading and Removing the NetScaler Gateway Plug-in by Using Active Directory

May 30, 2013

Each release of the NetScaler Gateway Plug-in is packaged as a full product installation, instead of as a patch. When users log on and the NetScaler Gateway Plug-in detects a new version of the plug-in, the plug-in upgrades automatically. You can also deploy the NetScaler Gateway Plug-in to upgrade by using Active Directory.

To do so, create a new distribution point for the NetScaler Gateway Plug-in. Create a new 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 NetScaler Gateway Plug-in is updated.

To remove the NetScaler Gateway Plug-in 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.

# Troubleshooting the NetScaler Gateway Plug-in Installation Using Active Directory

May 08, 2013

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 should 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 of 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 Active Directory.

To troubleshoot other installation issues for managed software, Citrix recommends using a group policy to enable Windows Installer Logging.

# Connecting with the NetScaler Gateway Plug-in for Java

Feb 05, 2014

The NetScaler Gateway Plug-in for Java can be used on any user device that supports Java.

Note: Java Runtime Environment (JRE) Version 1.4.2 up to the most recent version of JRE is required for the following operating systems and web browsers.

- Mac OS X
- Linux
- Windows XP (all versions), Windows Vista, Windows 7, and Windows 8
- Internet Explorer
- Firefox
- Safari 1.2 up to the most recent version of the web browser

The NetScaler Gateway Plug-in for Java supports most TCP-based applications, but provides only some of the features of the NetScaler Gateway Plug-in for Windows or NetScaler Gateway Plug-in for Mac OS X.

Users do not require administrative privileges on the user device to use the NetScaler Gateway Plug-in for Java. For security reasons, you might want to require using this plug-in version for a particular virtual server, group, or user, regardless of which user device is used.

To configure NetScaler Gateway to install the NetScaler Gateway Plug-in for Java on user devices, configure a session policy and then bind it to the virtual server, group, or user.

If users log on from a computer running Windows 7, the proxy server information is not set automatically in Internet Explorer. Users must manually configure the proxy server on the computer running Windows 7.

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.
3. Select a session profile and then click Open.
4. On the Client Experience tab, next to Plug-in Type, click Override Global, select Java and then click OK.

After creating the session policy, create an intranet application to define the interception mode for users who log on with the NetScaler Gateway Plug-in for Java.

1. In the configuration utility, 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.
4. Click Proxy.
5. In Destination IP Address, type the IP address.
6. In Destination Port, type the port number.
7. In Source IP Address, type the IP address.

8. In Source Port, type the port number, click Create and then click Close.

If you do not specify a source IP address and port number, NetScaler Gateway automatically uses 127.0.0.1 for the IP address and 0 for the port.

When users log on using the NetScaler Gateway Plug-in for Java on a computer running Windows Vista, Windows 7, or Windows 8, network traffic for TCP intranet applications is not tunneled. The HOSTS file is not updated automatically on computers running Vista and Windows 7. You must add the intranet applications manually to the HOSTS file.

On a Windows-based computer, you can edit the HOSTS file in Notepad or another text editor. If you edit the HOSTS file in Notepad, you must run Notepad as an administrator. Add the mapping entries for the intranet application for the NetScaler Gateway Plug-in for Java and then save the file.

- 
- 
- 
- 
- 
- 
- 
- 

- 
- 
- 
- 

- 
-



- 
- 
  
- 
- 
- 
- 
-





- 
- 
- 

- 
- 

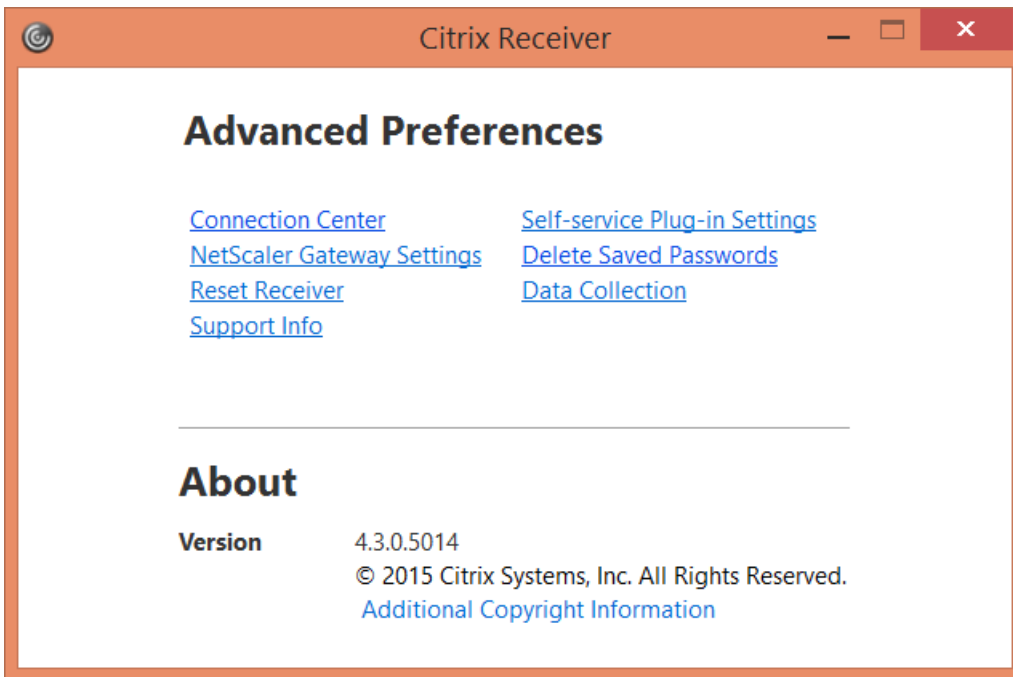
- 

- 

- 

-





**Advanced Settings**

General

Client Options

Client Cleanup

Proxy

Login Script

Logout Script

Client Debug\*

Split DNS\*

Application Token Timeout (secs)

MDX Token Timeout (mins)

- Local LAN Access
- Allow access to private network IP addresses only
- Client Choices ?
- Show VPN Plugin-in icon with Receiver

OK

Close

- 
- 
- 
- 
- 

```
enable ns feature IPv6PT
enable ns mode USNIP
```

```
set dns parameter -resolutionOrder
AAAAThenAQuery
AThenAAAAQuery
OnlyAAAAQuery
OnlyAQuery
```

```
set vpn parameter -wihome http://<XD_domain>/Citrix/StoreWeb
```

```
set vpn parameter -wihome http://storefront.domain.com/Citrix/StoreWeb
```

```
vpn parameter -wihome http://[1000:2000::3000]/Citrix/StoreWeb
```

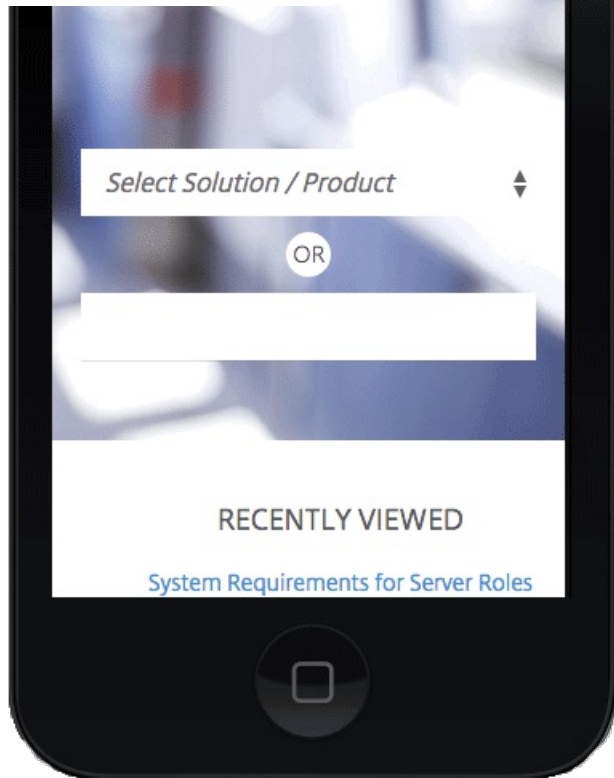


- 
- 
-





mentation



- 
- 
- 
- 

Figure 1: Caxton Theme



Figure 2: Greenbubble Theme

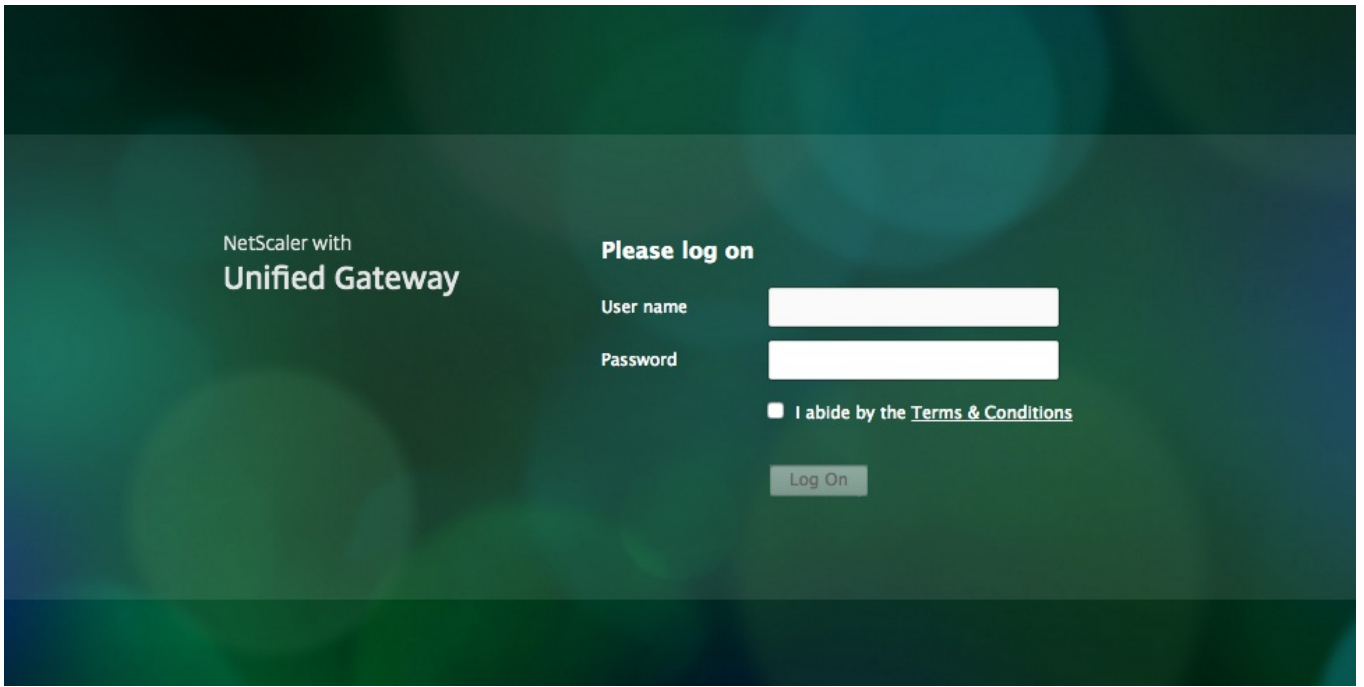


Figure 3: X1 Theme

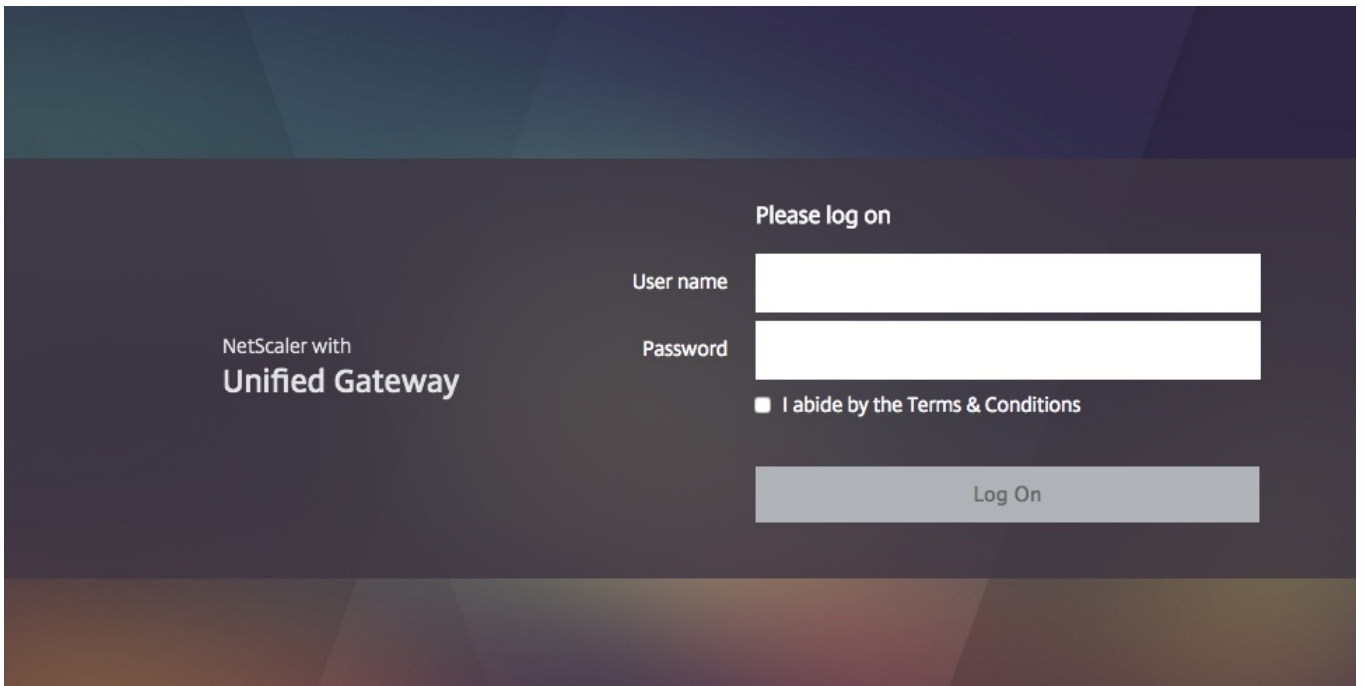




Figure 4: Portal Theme interface



← Back

### Portal Theme

| Portal Theme  |           |
|---|-----------|
| Theme Name  | MainTheme |
| Template Theme  | X1        |
| <a href="#">Click to bind and view configured theme</a> |           |

| Advanced Settings     |
|-----------------------|
| + Login Page          |
| + EPA Page            |
| + EPA Error Page      |
| + Post EPA Page       |
| + VPN Connection Page |
| + Portal Home Page    |

| Look & Feel                              |                                |
|--|--------------------------------|
| <b>Home Page</b>                         |                                |
| Body Background Color                    | -                              |
| Navigation Pane Background Color         | rgb<br>a(0, 0, 0, 0.15)        |
| Navigation Pane Font Color               | rgba(255, 255, 255, 0.7)       |
| Navigation Selected Tab Background Color | #315a68                        |
| Navigation Selected Tab Font Color       | ffffff                         |
| Content Pane Background Color            | -                              |
| Button Background Color                  | #02a1c1                        |
| Content Pane Font Color                  | #dcdcdc                        |
| Content Pane Title Font Color            | #dcdcdc                        |
| Bookmarks Description Font Color         | #dcdcdc                        |
| Show Enterprise Websites Section         | true                           |
| Show Personal Websites Section           | true                           |
| Show Enterprise File Shares Section      | true                           |
| Show Personal File Shares Section        | true                           |
| <b>Other Pages</b>                       |                                |
| Background Image                         | X1-bg-img.jpg                  |
| Header Background Color                  | #f4f5f6                        |
| Header Font Color                        | -                              |
| Header Border-Bottom Color               | -                              |
| Header Logo                              | logo-unifiedgateway_header.png |
| Center Logo                              | ns_gateway_logo_center.png     |
| Watermark Image                          | -                              |
| Form Font Size                           | 14px                           |
| Form Font Color                          | ffffff                         |
| Button Color                             | #02a1c1                        |
| Button Hover Image                       | #02a1c1                        |
| Form Title Font Size                     | 16px                           |
| Form Title Font Color                    | ffffff                         |
| Form Background Color                    | rgba(63, 54, 67, 0.8)          |
| EULA Title Font Size                     | 20px                           |

| Language         |
|------------------|
| Language English |

Done

Figure 5: The Color Picker

**Look & Feel**

Use the controls here to customize the attributes that define the look and feel for portal pages.

**Home Page**

Modify the portal page properties here. Refer to the 'Attributes Legend' link below to see where the attributes are applied.

**Attribute Legend**

Body Background Color

Navigation Pane Background Color

Navigation Pane Font Color

Navigation Selected Tab Background Color

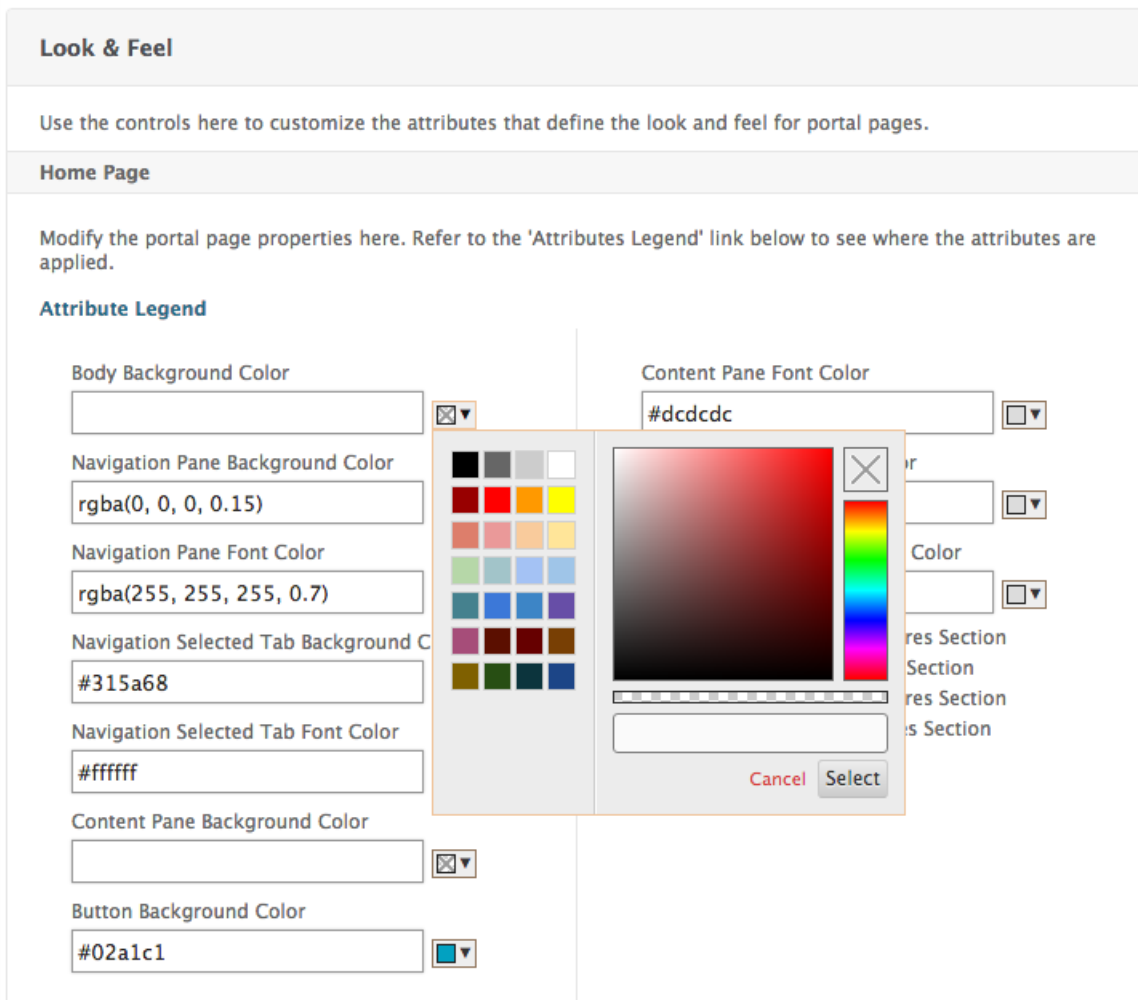
Navigation Selected Tab Font Color

Content Pane Background Color

Button Background Color

Content Pane Font Color

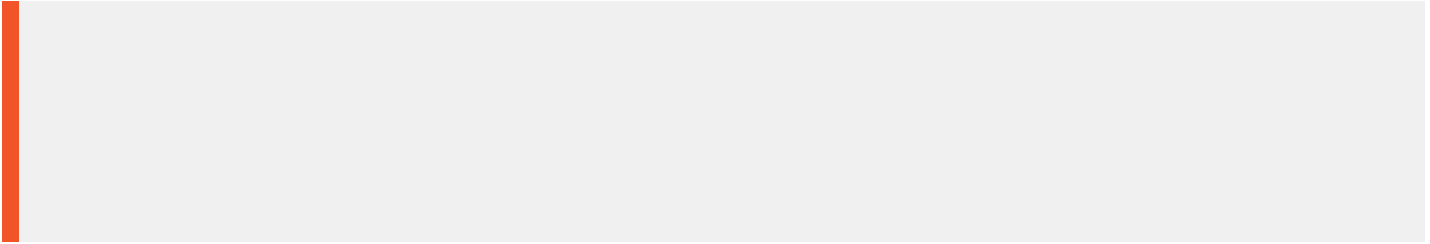
**Color Picker**







- 
- 
- 
- 
- 
- 







- 

- 

- 

- 

-

- 
- 
-



- 
- 
-

- 
- 
- 

- 
- 
- 

-





- 
- 

- 
-





- 
- 
-

- 
- 
-



# Saving User Settings for Clientless Access Through Web Interface

Feb 05, 2014

When users log on and log off from the Web Interface by using clientless access, NetScaler Gateway does not forward the client-consumed cookie set from the previous session, even if the cookies are persistent when users log on multiple times. You can use the configuration utility or command line to bind cookies to a pattern set of client cookies to preserve Web Interface settings between sessions.

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies and then click Clientless Access.
2. In the right pane, on the Policies tab, click Add.
3. In the Create Clientless Access Policy dialog box, in Name, type a name for the policy.
4. Next to Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Cookies tab, in Client Cookies, select `ns_cvpn_default_client_cookies` and then click Modify.
7. In the Configure Pattern Set dialog box, under Specify Pattern, in Pattern, enter the following parameters:
  - `WIUser` and then click Add.
  - `WINGDevice` and then click Add.
  - `WINGSession` and then click Add.
8. Click OK and then click Create.
9. In the Create Clientless Access Policy dialog box, in Expression, type `true`, click Create and then click Close.

1. Log on to the NetScaler Gateway command line by using a Secure Shell (SSH) connection, such as PuTTY.
2. At the command prompt, type `shell`.
3. At the command prompt, enter the following commands:
  - `bind policy patset ns_cvpn_default_client_cookies WIUser` and then press ENTER.
  - `bind policy patset ns_cvpn_default_client_cookies WINGDevice` and then press ENTER.
  - `bind policy patset ns_cvpn_default_client_cookies WINGSession` and then press ENTER.



# Configuring the Client Choices Page

Feb 05, 2014

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:

- NetScaler Gateway Plug-in for Windows
- NetScaler Gateway Plug-in for Mac OS X
- NetScaler Gateway Plug-in for Java
- 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 NetScaler Gateway Plug-in for Windows silently upgrades or downgrades to the version on the appliance. If users connect by using the NetScaler Gateway Plug-in 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, web sites, and use Outlook Web Access.

If users select the NetScaler Gateway Plug-in for Java, the plug-in starts and users are logged on. The choices page does not appear.

Secure Browse allows users to connect through NetScaler Gateway from an iOS device. If you enable Secure Browse, when users log on by using Worx Home, Secure Browse disables the client choices page.

# Showing the Client Choices Page at Logon

Feb 05, 2014

When you enable the client choices option, users can log on with the NetScaler Gateway Plug-in, the Web Interface, Receiver or clientless access from one web page after successful authentication to NetScaler Gateway. When log on is successful, icons appear in the web page from which users can choose the method to establish a connection. You can also configure the NetScaler Gateway Plug-in for Java to appear on the choices page.

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 are treated the same as user devices that pass the endpoint scan.

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, click Client Choices and then click OK.

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 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.
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.

# Configuring Client Choices Options

Feb 05, 2014

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 NetScaler Gateway Plug-in, 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.

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 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 NetScaler Gateway Plug-in, StoreFront, and clientless access.

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.
4. On the Client Experience tab, do the following:
  1. Next to Home Page, click Override Global and then clear Display Home Page. This disables the Access Interface.
  2. Next to Clientless Access, click Override Global and then select OFF.
  3. Next to Plug-in Type, click Override Global and then select Windows/Mac OS X.
  4. 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:
  1. Next to ICA Proxy, click Override Global and then select OFF.
  2. Next to Web Interface Address, click Override Global and then type the Web address of StoreFront, such as `http://ipAddress/Citrix/`.
  3. Next to Web Interface Portal Mode, click Override Global and then select COMPACT.
  4. 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 NetScaler Gateway Plug-in 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 XenApp choice does not appear on the choices page.

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.

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.

# Configuring Access Scenario Fallback

Feb 05, 2014

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 NetScaler Gateway Plug-in to the Web Interface or StoreFront by using Citrix Receiver 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 or not 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 is enabled, users can log on to the Web Interface or StoreFront by using Receiver 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.

# Creating Policies for Access Scenario Fallback

Feb 05, 2014

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 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 NetScaler Gateway Plug-in or the Citrix Receiver 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 and 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 NetScaler Gateway Plug-in and the Web Interface home page takes precedence for Web Interface users. The Receiver home page takes precedence for StoreFront.

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.

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.

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.

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.

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 twice.

# Configuring Connections for the NetScaler Gateway Plug-in

May 09, 2013

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.



# Configuring the Number of User Sessions

May 10, 2013

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.

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.

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.

# Configuring Time-Out Settings

Feb 05, 2014

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 will close. If the session closes, the user must log on again.

There are three time-out options:

- **Forced time-out.** If you enable this setting, NetScaler Gateway disconnects the session after the time-out interval elapses regardless of what the user is doing. There is no action the user can take to prevent the disconnection from occurring when the time-out interval elapses. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Receiver, Worx Home, or through a web browser. The default setting is 30 minutes. If you set this value to zero, the setting is disabled.
- **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 NetScaler Gateway Plug-in, Receiver, Worx Home, or through a web browser. The default time-out setting is 30 minutes. If you set this value to zero, the setting is disabled.
- **Idle session time-out.** The duration after which the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in only. The default setting is 30 minutes. If you set this value to zero, the setting is disabled.

Note: 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.

You can enable any of these settings by entering a value between 1 and 65536 to specify a number of 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.

# Configuring Forced Time-Outs

Feb 05, 2014

A forced time-out disconnects the NetScaler Gateway Plug-in automatically after a specified amount of time. You can configure a forced time-out globally or as part of a session 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 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.

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.

# Configuring Session or Idle Time-Outs

Feb 05, 2014

You can use the configuration utility 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.

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, 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.
  
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, 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.
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.

# Connecting to Internal Network Resources

Feb 05, 2014

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 NetScaler Gateway Plug-in for Windows, set the interception mode to transparent. If you are using the NetScaler Gateway Plug-in 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.

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.

# Configuring Split Tunneling

Feb 05, 2014

You can enable

— *split tunneling*

to prevent the NetScaler Gateway Plug-in from sending unnecessary network traffic to NetScaler Gateway.

When you do not enable split tunneling, the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in sends only traffic destined for networks protected by NetScaler Gateway through the VPN tunnel. The NetScaler Gateway Plug-in does not send network traffic destined for unprotected networks to NetScaler Gateway.

When the NetScaler Gateway Plug-in starts, it obtains the list of intranet applications from NetScaler Gateway. The NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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 Receiver, 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 NetScaler Gateway Plug-in, 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.

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.

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 NetScaler Gateway Plug-in sends traffic to NetScaler Gateway, but access to the resource is denied.

# Configuring Client Interception

Feb 05, 2014

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 in order for client interception to occur.

You can configure intranet applications by using the configuration utility. 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 App Controller and your Exchange server. If you do not enable split tunneling, you do not need to configure the App Controller and Exchange IP addresses in Intranet Applications.



# Configuring Intranet Applications for the NetScaler Gateway Plug-in

Feb 05, 2014

You create intranet applications for user access to resources by defining the following:

- Access to one IP address and subnet mask
- Access to a range of IP addresses

When you define an intranet application on NetScaler Gateway, the NetScaler Gateway Plug-in 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:

- Intranet applications do not need to be defined if the following conditions are met:
  - Interception mode is set to transparent
  - Users are connecting to NetScaler Gateway with the NetScaler Gateway Plug-in for Windows
  - Split tunneling is disabled
- If users connect to NetScaler Gateway by using the NetScaler Gateway Plug-in for Java, you must define intranet applications. The NetScaler Gateway Plug-in for Java intercepts traffic only to network resources defined by intranet applications. If users connect with this plug-in, set the interception mode to proxy.

When configuring an intranet application, you must select an interception mode that corresponds to the type of plug-in software used to make connections.

Note: You cannot configure an intranet application for both proxy and transparent interception. To configure a network resource to be used by both the NetScaler Gateway Plug-in for Windows and NetScaler Gateway Plug-in for Java, configure two intranet application policies and bind the policies to the user, group, virtual server, or NetScaler Gateway global.

1. In the configuration utility, 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.

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. In the configuration utility, 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.

# Configuring Intranet Applications for the NetScaler Gateway Plug-in for Java

Feb 05, 2014

If users connect with the NetScaler Gateway Plug-in for Java, you must configure an intranet application and set the interception mode to proxy. The NetScaler Gateway Plug-in for Java intercepts traffic by using the user device loopback IP address and port number specified in the profile.

If users are connecting from a Windows-based device, the NetScaler Gateway Plug-in for Java attempts to modify the HOST file by setting the application HOST name to access the loopback IP address and port specified in the profile. Users must have administrative privileges on the user device for HOST file modification.

If users are connecting from a non-Windows device, you must configure applications manually by using the source IP address and port values specified in the intranet application profile.

1. In the configuration utility, 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. Click Proxy.
5. In Destination IP Address and Destination Port, type the destination IP address and port.
6. Under Source IP Address and Source Port, type the source IP address and port.  
Note: You should set the source IP address to the loopback IP address of 127.0.0.1. If you do not specify an IP address, the loopback IP address is used. If you do not enter a port value, the destination port value is used.

# Configuring Name Service Resolution

May 14, 2013

During installation of NetScaler Gateway, you can use the NetScaler Gateway wizard to configure additional 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 at that time. You can add additional 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 additional DNS server on NetScaler Gateway, create a virtual server that acts as a DNS server for name resolution.

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.

# Enabling Proxy Support for User Connections

Feb 04, 2014

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.

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 Proxy tab, under Proxy Settings, select On.
5. For the protocols, type the IP address and port number and then click OK.

Note: If you select Appliance, 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. After the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user's network.

You can configure one proxy server to support all of the protocols that NetScaler Gateway uses. This setting provides one IP address and port combination for all of the protocols.

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 Proxy tab, under Proxy Settings, select On.
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.

When you configure NetScaler Gateway as a proxy server, unsecure and secure HTTP are the only supported protocols.

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 Proxy tab, under Proxy Settings, select Appliance.
5. For the protocols, type the IP address and port number and then click OK.

# Configuring Address Pools

May 14, 2013

In some situations, users who connect with the NetScaler Gateway Plug-in 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. A remote user can be addressed by an IP address on the internal network. 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 need to 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.



# Configuring Address Pools

Feb 05, 2014

You use the configuration utility to configure address pools at the level to which you want to bind the policy. For example, if you want to create an address pool for a virtual server, configure the intranet IP addresses on that node. After you configure the address pool, the policy is bound to the entity where it is configured. You can also create an address pool and bind it globally on NetScaler Gateway.

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 you want to add to the pool and then click OK.
- 
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 you want to add to the pool and then click OK.

# Defining Address Pool Options

Feb 05, 2014

You can use a session policy or the global NetScaler Gateway settings to control whether or not 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 and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- **Spillover.** When you configure address pools and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- **Off.** Address pools are not configured.

## To configure 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.

## Configuring the Transfer Login Page

If a user does not have an intranet IP address available and then tries to establish another session with NetScaler Gateway, the Transfer Login page appears. The Transfer Login page allows users to replace their existing NetScaler Gateway session with a new session.

The Transfer Login 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 Login 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 Login page appears and the user can choose to replace an existing session with a new session.

Note: If the user does not have an assigned IP address available and a new session cannot be established by using the Transfer Login page, the user receives an error message.

The Transfer Login page appears only if you configure address pools and disable spillover.

## Configuring 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.

# Supporting VoIP Phones

May 11, 2013

When you install NetScaler Gateway as a standalone appliance and users connect with the NetScaler Gateway Plug-in, NetScaler Gateway supports two-way communication with Voice over IP (VoIP) softphones.

Real-time applications, such as voice and video, are implemented over User Datagram Protocol (UDP). Transmission Control Protocol (TCP) is not appropriate for real-time traffic due to the delay introduced by acknowledgments and retransmission of lost packets. It is more important to deliver packets in real time than to ensure that all packets are delivered. However, with any tunneling technology over TCP, such real-time performances cannot be met.

NetScaler Gateway supports the following VoIP softphones.

- 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 NetScaler Gateway Plug-in and one of the supported softphones on the same user device. When the VoIP traffic is sent over the secure tunnel, the following softphone features are supported:

- Outgoing calls that are placed from the IP softphone
- Incoming calls that are placed to the IP softphone
- Bidirectional voice traffic

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.

# Configuring Application Access for the NetScaler Gateway Plug-in for Java

May 11, 2013

You can configure the access level and the applications users are allowed to access in the secure network. If users are logged on by using the NetScaler Gateway Plug-in for Java, in the Secure Access Remote Session dialog box, users can click Applications. The Intranet Applications dialog box appears and lists all of the applications the user is authorized to access.

When users are connected with the NetScaler Gateway Plug-in for Java, you can configure one of two methods that allow users to access applications.

- HOSTS File Modification method
- SourceIP and SourcePort method

## Accessing Applications by Using the HOSTS File Modification Method

When you use the HOSTS File Modification method, the NetScaler Gateway Plug-in for Java adds an entry that corresponds to the applications that the you configure in the HOSTS file. To modify this file on a Windows-based device, you must be logged on as an administrator or have administrator privileges. If you are not logged on with administrator privileges, manually edit the HOSTS file and add the appropriate entries.

Note: On a Windows-based computer, the HOSTS file is located in the following directory path:

%systemroot%\system32\drivers\etc. On a Macintosh or Linux computer, the HOSTS file is located at /etc/hosts.

For example, you want to use Telnet to connect to a computer in the secure network. You use the remote computer to work both within your secure network and remotely—for example, from home. The IP address should be the localhost IP address, 127.0.0.1. In the HOSTS file, you add the IP address and the application name, such as:

```
127.0.0.1 telnet1
```

When the HOSTS file is edited and saved on the user device, you test your connection. You can test your connection by opening a command prompt and using Telnet to connect. If users are employing a user device that is not within the secure network, log on to NetScaler Gateway before starting Telnet.

To connect to a computer in the secure network

1. Start a Telnet session using the available software for your computer.
2. From a command prompt, type: `Open telnet`  
The logon prompt of the remote computer appears.

## Accessing Applications by Using the SourceIP and SourcePort Method

If users need to access an application in the secure network and do not have administrative rights on the user device, configure the HOSTS file by using the source IP address and port number that is located in the Intranet Applications dialog box.

To open the Intranet Applications dialog box and locate the IP address and port number

1. When users log on with the plug-in, in the Secure Remote Access dialog box, click Applications.
2. Find the application in the list and note the SourceIP address and SourcePort number.

When you have the IP address and port number, start a Telnet session to connect to the computer in the remote network.

# Configuring the Access Interface

Feb 05, 2014

NetScaler Gateway includes a default home page that is a web 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 web sites, 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 web sites 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.

# Replacing the Access Interface with a Custom Home Page

Feb 05, 2014

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.

## To 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.

## To 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.



# Changing the Access Interface

May 14, 2013

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.

# Creating and Applying Web and File Share Links

Feb 05, 2014

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 and File Shares panes under Enterprise Web Sites and Enterprise File Shares. If users add their own links, these links appear under Personal Web Sites and Personal File Shares.

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, click Create and then click Close.

If you enable clientless access, you can make sure that requests to web sites go through NetScaler Gateway. For example, you added a bookmark for

— <http://www.agexternal.com>

. In the Create Bookmark dialog box, select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, web site requests go from the user device to NetScaler Gateway and then to the web site. When you clear the check box, requests go from the user device to the web site. This check box is only available if you enable clientless access.

To bind bookmarks 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 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 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. The links are organized on the page according to type, as web site links or as file share links.

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.

# Configuring User Name Tokens in Bookmarks

Mar 18, 2014

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.

# How a Traffic Policy Works

May 02, 2013

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 need to enable or disable single sign-on for certain applications.
- Identifying situations where you want to use other HTTP features for NetScaler Gateway Plug-in traffic.
- Defining the file extensions that are used with file type association.

# Creating a Traffic Policy

Jan 22, 2014

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.

## To configure a traffic policy

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, 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 Branch Repeater, 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.

# Configuring Form-Based Single Sign-On

May 30, 2013

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](#).

To configure form-based 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 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 Field, type the name of the attribute for the user name field.
6. In Password Field, 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 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.

# Configuring SAML Single Sign-On

Jan 22, 2014

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.

To 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.



# Binding a Traffic Policy

Feb 28, 2014

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.

To bind a traffic policy globally by using the configuration utility

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.

# Removing Traffic Policies

Jan 22, 2014

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.

To unbind a traffic policy by using the configuration utility

1. In the configuration utility, in the navigation pane, do one of the following:
  - 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.

To remove a traffic policy by using the configuration utility

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, on the Policies tab, select the traffic policy and then click Remove.

# Configuring Session Policies

Jan 22, 2014

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 NetScaler Gateway Plug-in for Windows or the NetScaler Gateway Plug-in for Mac. You can also configure settings to require users to log on with Citrix Receiver or Work Home. 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 new 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 App Controller 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.

## 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. 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.

# Creating a Session Profile

Jan 22, 2014

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.

## Configuring 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

## Configuring 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 (NetScaler Gateway Plug-in for Windows, NetScaler Gateway Plug-in for Mac OS X, or NetScaler Gateway Plug-in for Java)
- Split tunneling
- Session and idle time-out settings
- Clientless access
- Clientless access URL encoding
- Plug-in type (Windows, Mac, or Java)
- 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 NetScaler Gateway Plug-in](#).

## Configuring 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](#).

#### Configuring XenApp and XenDesktop 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 XenApp or XenDesktop:

- ICA proxy, which are client connections using Citrix Receiver
- Web Interface address
- Web Interface portal mode
- Single sign-on to the server farm domain
- Receiver 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 configuration utility

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 configuration utility

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 new 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:
  1. Click Create and then click Close to create the policy.
  2. Click OK and then click Close to modify the policy.

# Binding Session Policies

Jan 22, 2014

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

To bind a session policy by using the configuration utility

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then do one of the following:
  1. Click Virtual Servers.
  2. Expand User Administration and then click AAA Groups.
  3. Expand User Administration and then click AAA Users.
2. Depending on your selection in Step 1, click the Policies tab in one of the following dialog boxes:
  - Create NetScaler Gateway Virtual Server
  - Configure AAA Group
  - Configure AAA Users
3. Click Session to add the session policy.
4. Click Insert Policy, select the session policy and then click OK.

# Configuring Endpoint Polices

May 06, 2013

— *Endpoint analysis*

is a process that scans a user device and detects information, such as the presence and version level of an operating system, and of antivirus, firewall, or web browser software. You can use endpoint analysis to verify that the user device meets your requirements before allowing it to connect to your network or remain connected after users log on. You can monitor files, processes, and registry entries on the user device during the user session to ensure that the device continues to meet requirements.

# How Endpoint Policies Work

May 06, 2013

You can configure NetScaler Gateway to check if a user device meets certain security requirements before a user logs on. This is called a

— *preauthentication 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 preauthentication scan, users are not allowed to log on.

If you need to configure additional security requirements that are not used in a preauthentication policy, you 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 items, such as antivirus software or a process, is still true.

When you configure a preauthentication or post-authentication policy, NetScaler Gateway downloads the Endpoint Analysis Plug-in and then runs the scan. Each time a user logs on, the Endpoint Analysis Plug-in runs automatically.

You 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 security expression within a session policy. If the user device fails to meet the requirements of the client security 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 additional checks.

You can incorporate detected information into policies, enabling you to grant different levels of access based upon 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 untrusted computers, you can provide a more restricted level of access that allows users to edit documents on remote servers without downloading them.

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 preauthentication 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 completes before the user session uses a license.
- Compares property values detected on the user device with desired property values listed in your configured scans.
- Produces an output verifying whether or not 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.



# Evaluating User Logon Options

Jan 27, 2014

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 can only have access to the Web Interface or through clientless access.

For example, you want to provide users access by using the NetScaler Gateway Plug-in. 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 NetScaler Gateway Plug-in.

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 NetScaler Gateway Plug-in.
- 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 NetScaler Gateway Plug-in.

# Setting the Priority of Preauthentication Policies

Jan 27, 2014

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 to AAA Global 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 at AAA Global 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.

To change the priority of a preauthentication policy

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 Policies tab, click Pre-authentication.
4. Under Priority, type the priority number for the policy and then click OK.

# Configuring Preauthentication Policies and Profiles

Jan 27, 2014

You can configure NetScaler Gateway to check for client-side security before users are authenticated. This method ensures that the user device establishing a session with NetScaler Gateway conforms to your security requirements. You configure client-side security checks through the use of preauthentication 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 action to allow or deny a process to execute on the user device. For example, the text file, `clienttext.txt`, is running on the user device. When the user logs on to NetScaler Gateway, you can either allow or deny access if the text file is running. If you do not want to allow users to log on if the process is running, configure the profile so the process is stopped 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 of the created 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 a new 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 drop-down list 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 client security string that will be configured on NetScaler Gateway when you select a named expression.

To configure a preauthentication profile globally by using 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 Settings, click Change pre-authentication settings.
3. In the Global Pre-authentication settings dialog box, configure the settings:
  1. In Action, select Allow or Deny.  
Denies or allows users to log on after endpoint analysis occurs.
  2. In Processes to be cancelled, enter the process.  
This specifies the processes to be stopped by the Endpoint Analysis Plug-in.
  3. In Files to be deleted, enter the file name.

This specifies the files to be deleted by the Endpoint Analysis Plug-in.

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 configuration utility

1. 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 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 cancelled, 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.  
Note: If a file is to be deleted or a process stopped, users receive a message asking for confirmation. Steps 5 and 6 are optional parameters.

If you use the configuration utility 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 drop-down list.

# Configuring Endpoint Analysis Expressions

Jan 24, 2014

Preauthentication and client security session policies include a profile and an expression. The policy can have one profile and multiple expressions. To scan a user device for an application, file, process, or registry entry, you create an expression or compound expressions within the policy.

## Types of Expressions

The expression consists of an expression type and the parameters of the expression. Expression types include:

- General
- Client security
- Network based

## Adding Preconfigured Expressions 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.

To add a named expression to a preauthentication policy

1. 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, select a policy and then click Open.
3. Next to Named Expressions, select Anti-Virus, select the antivirus product from the list, click Add Expression, click Create and then click Close.

# Configuring Custom Expressions

Jan 27, 2014

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 client security expressions to refer to commonly used client security strings. This eases the process of configuring preauthentication policies and also in maintaining the configured expressions.

For example, you want to create a custom client security expression for Symantec AntiVirus 10 and make sure that the virus definitions are no more than three days old. Create a new policy and then configure the expression to specify the virus definitions.

The following procedure shows how to create a client security policy in a preauthentication policy. You can use the same steps in a session policy.

To create a preauthentication policy and custom client security expression

1. 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, click Add. The Create Pre-Authentication Policy dialog box opens.
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 Match Any Expression, click Add.
7. In Expression Type, select Client Security.
8. Configure the following:
  1. In Component, select Anti-Virus.
  2. In Name, type a name for the application.
  3. In Qualifier, select Version.
  4. In Operator, select ==.
  5. In Value, type the value.
  6. 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.

# Configuring Compound Expressions

Jan 24, 2014

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_McAfeeviruscan_11 || av_5_sophos_4
```

For more information about compound expressions, see [Configuring Compound Expressions](#).

# Binding Preauthentication Policies

Jan 27, 2014

After you create the preauthentication or client security session policy, bind the policy to the level to which it applies. You can bind the preauthentication policies to virtual servers or globally.

To create and bind a preauthentication policy 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, 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.

To bind a preauthentication policy 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. 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.



# Unbinding and Removing Preauthentication Policies

Jan 27, 2014

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.

To unbind a global preauthentication policy

1. 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, 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.

To unbind a preauthentication policy from 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 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.

To remove a preauthentication policy

1. 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, select a policy and then click Remove.

# Configuring Post-Authentication Policies

May 29, 2013

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.

Note: This functionality works only with the NetScaler Gateway Plug-in. If users log on with Citrix Receiver, the endpoint analysis scan runs at logon only.

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 on the basis of a client security 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 security expression and a client security 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](#).

# Configuring a Post-Authentication Policy

Jan 27, 2014

You use a session policy to configure a post-authentication policy. A simple policy includes a client security expression and a client security message.

To configure a post-authentication 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 Security tab, click Advanced Settings.
7. Under Client Security, click Override Global and then click New.
8. Configure the client security 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.

# Configuring the Frequency of Post-Authentication Scans

May 13, 2013

You can configure NetScaler Gateway to run the post-authentication policy at specified intervals. For example, you configured a client security 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 NetScaler Gateway Plug-in. If users log on with Citrix Receiver, the endpoint analysis scan runs at logon only.

You can set the frequency (in minutes) when you configure the client security 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.

Figure 1. Dialog box for configuring the frequency of post-authentication scans

| Component  | Name*            | Qualifier | Operator | Value* |
|------------|------------------|-----------|----------|--------|
| Anti-Virus | Norton Antivirus | Version   | ==       | 10     |

Frequency (min)  Error Weight  Freshness

OK Close

# Configuring Quarantine and Authorization Groups

May 06, 2013

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 that has access only to your email server and a file share. When user devices pass the security 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 on the basis of a client security expression within the session policy. When the user is a member of a group, NetScaler Gateway applies the session policy based on group membership.

# Configuring Quarantine Groups

Jan 27, 2014

When you configure a quarantine group, you configure the client security expression using the Security Settings - Advanced Settings dialog box within a session profile.

To configure the client security expression for a quarantine 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, 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 security 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, 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. 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, configure the client security 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.

# Configuring Authorization Groups

Jan 27, 2014

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. 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 Security tab, click Advanced Settings.
7. Under Authorization Groups, click Override Global, select a group from the drop-down list, click Add, 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.

After you create the session policy, you can bind it to a user, group, or virtual server.

## To configure a global authorization group

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. Under Authorization Group, select a group from the drop-down list, click Add and then click OK twice.

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 Security Preauthentication Expressions for User Devices

Jan 27, 2014

NetScaler Gateway provides various endpoint security checks during user logon or at other configured times during a session that help in improving security. Only the user devices that pass these security checks are allowed to establish a NetScaler Gateway session.

The following are the types of security 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 security check fails on the user device, no new connections are made until a subsequent check passes (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 security expressions within session policies that are designed to carry out security checks on user devices.



# Configuring Antivirus, Firewall, Internet Security, or Antispam Expressions

Jan 27, 2014

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 is the type of client security, such as antivirus, firewall, or registry entry.
- Name is the name of the application, process, file, registry entry, or operating system.
- Qualifier is 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 is the application version for antivirus, firewall, Internet security, or antispam software on the user device.
- Frequency is how often a post-authentication scan is run, in minutes.
- Error weight assigns a weight 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 security policy to a preauthentication or session policy

1. In the configuration utility, in the navigation pane, do one of the following:
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
  2. 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:
  1. In Component, select the item for which to scan.
  2. In Name, type the name of the application.
  3. In Qualifier, select Version.
  4. In Operator, select the value.
  5. In Value, type the client security string, click OK, click Create and then click Close.

# Configuring Service Policies

Jan 27, 2014

A service is a program that 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:
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
  2. 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:
  1. In Component, select Service.
  2. In Name, type the name of the service.
  3. In Qualifier, leave blank or select Version.
  4. 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.

# Configuring Process Policies

Jan 27, 2014

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:
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
  2. 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:
  1. In Component, select Process.
  2. In Name, type the name of the application.
  3. In Operator, select EXISTS or NOT EXISTS, 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
```

# Configuring Operating System Policies

Feb 24, 2014

When you create a session or preauthentication policy, you can configure client security strings to determine whether or not 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   |
|-------------------------|---------|
| Mac OS 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

1. In the configuration utility, in the navigation pane, do one of the following:
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
  2. 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:
  1. In Component, select Operating System.
  2. In Name, type the name of the operating system.
  3. In Qualifier, do one of the following:
    - Leave blank.
    - Select Service Pack.
    - Select Hotfix.
    - Select Version for Mac OS X only.
  4. Depending on your selection in Step C, 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.
7. Click Create 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.

# Configuring Registry Policies

Jan 27, 2014

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 NetScaler Gateway Plug-in registry key when users log on:

```
CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client_ProductVersion
```

Note: If you are scanning for registry keys and values and you select Advanced Free-Form in the Expression dialog box, 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 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 should 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:
  1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
  2. 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:
  1. In Component, select Registry.
  2. In Name, type the name of the registry key.
  3. In Qualifier, leave blank or select Value.
  4. 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 !=
  5. In Value, type the value as it appears in the registry editor, click OK and then click Close.

# Configuring Compound Client Security Expressions

May 29, 2013

You can combine client security strings to form compound client security 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 security expressions together when you form a compound expression. The use of parentheses improves the understanding and debugging of the client expression.

## Configuring Policies with the AND (&&) Operator

The AND (&&) operator works by combining two client security 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 security check that determines if the user device has Version 7.0 of Sophos AntiVirus installed and running. It also checks if the netlogon 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
```

## Configuring Policies with the OR (| |) Operator

The OR (| |) operator works by combining two security 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 symbols '| |'.

Example:

The following is a client security 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
```

## Configuring Policies Using the NOT (!) Operator

The NOT (!) or the negation operator negates the client security string.

Example:

The following client security 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)
```

- 
- 
  
- 
- 
-

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

- 
- 
- 
- 
- 
- 

- 
- 
- 
- 
- 
- 
- 
- 
-



- 
-

CLIENT.APPLICATION (SCAN-type\_ Product-id\_ Method-name\_ Method-comparator\_ Method-param \_...)

SCAN-type

Product-id

Method-name

Method-comparator

Method-param

client.application(ANTIVIR\_2600\_RTP\_==\_TRUE)

CLIENT.SYSTEM

CLIENT.APPLICATION

|  | ANTIPHI  |
|--|----------|
|  | ANTISPY  |
|  | ANTIVIR  |
|  | BACKUP   |
|  | DEV-CONT |

|  |             |
|--|-------------|
|  |             |
|  | DATA-PREV   |
|  | DESK-SHARE  |
|  | FIREWALL    |
|  | HEALTH      |
|  | HD-ENC      |
|  | IM          |
|  | BROWSER     |
|  | P2P         |
|  | PATCH       |
|  | URL-FILT    |
|  | MAC         |
|  | DOMAIN      |
|  | REG-NUM     |
|  | REG-NON-NUM |

MAC-  
MAC-ANTIVIR      MAC-ANTIPHI

client.application(MAC-ANTIVIR\_2600\_RTP\_==\_TRUE)

|           |  |    |      |
|-----------|--|----|------|
|           |  |    |      |
| VERSION   |  |    |      |
| AUTHENTIC |  |    | TRUE |
| ENABLED   |  |    | TRUE |
| RUNNING   |  |    | TRUE |
| COMMENT   |  | [] |      |

|             |  |                          |   |
|-------------|--|--------------------------|---|
|             |  |                          |   |
| ENABLED-FOR |  | allof<br>anyof<br>noneof | Internet Explorer<br><br>Mozilla Firefox<br><br>Google Chrome |



|  |  |  |                    |
|--|--|--|--------------------|
|  |  |  | Opera              |
|  |  |  | Safari             |
|  |  |  | Safari             |
|  |  |  | Mozilla<br>Firefox |
|  |  |  | Google<br>Chrome   |
|  |  |  | Opera              |

|                     |  |  |      |
|---------------------|--|--|------|
|                     |  |  |      |
| RTP                 |  |  | TRUE |
| SCAN-TIME           |  |  |      |
| VIRDEF-FILE-TIME    |  |  |      |
| VIRDEF-FILE-VERSION |  |  |      |
| ENGINE-VERSION      |  |  |      |

|                  |  |  |  |
|------------------|--|--|--|
|                  |  |  |  |
| LAST-BK-ACTIVITY |  |  |  |

|         |  |  |      |
|---------|--|--|------|
|         |  |  |      |
| ENABLED |  |  | TRUE |

|              |  |  |      |
|--------------|--|--|------|
|              |  |  |      |
| SYSTEM-COMPL |  |  | TRUE |

|          |  |                          |  |
|----------|--|--------------------------|--|
|          |  |                          |  |
| ENC-PATH |  |                          |  |
| ENC-TYPE |  | allof<br>anyof<br>noneof | UNENCRYPTED<br>PARTIAL<br>ENCRYPTED<br>VIRTUAL<br>SUSPENDED<br>PENDING |

|         |  |  |      |
|---------|--|--|------|
|         |  |  |      |
| DEFAULT |  |  | TRUE |

|       |  |  |  |
|-------|--|--|--|
|       |  |  |  |
| SCAN- |  |  |  |

|              |  |                 |                            |
|--------------|--|-----------------|----------------------------|
| TIME         |  |                 |                            |
| MISSED-PATCH |  | anyof<br>noneof | ANY<br>Pre-selected<br>NON |

|      |  |                 |  |
|------|--|-----------------|--|
|      |  |                 |  |
| ADDR |  | anyof<br>noneof |  |

|        |  |                 |  |
|--------|--|-----------------|--|
|        |  |                 |  |
| SUFFIX |  | anyof<br>noneof |  |

|      |  |  |  |
|------|--|--|--|
|      |  |  |  |
| PATH | HKEY_LOCAL_MACHINE<br>HKEY_CURRENT_USER<br>HKEY_USERS<br>HKEY_CLASSES_ROOT |  |  |

|          |                     |  |      |
|----------|---------------------|--|------|
|          | HKEY_CURRENT_CONFIG |  |      |
| REDIR-64 |                     |  | TRUE |
| VALUE    |                     |  |      |

|          |  |  |      |
|----------|--|--|------|
|          |  |  |      |
| PATH     |  |  |      |
| REDIR-64 |  |  | TRUE |
| VALUE    |  |  |      |

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|--|--|--|--|

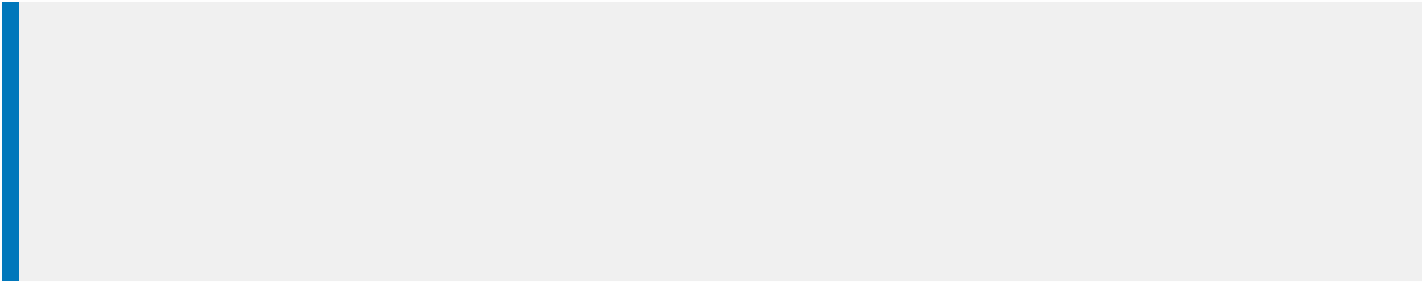


- 
- 
- 
- 
- 
-





- 
- 
- 
- 
-



- 
- 
- 
- 
- 

- 

- 

- 

- 

- 

-



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

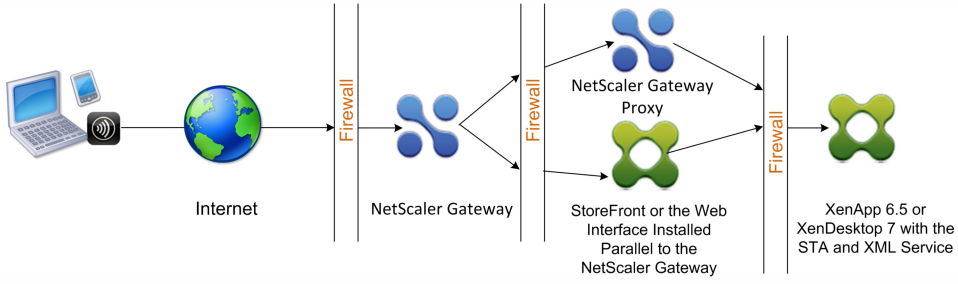
[Redacted]

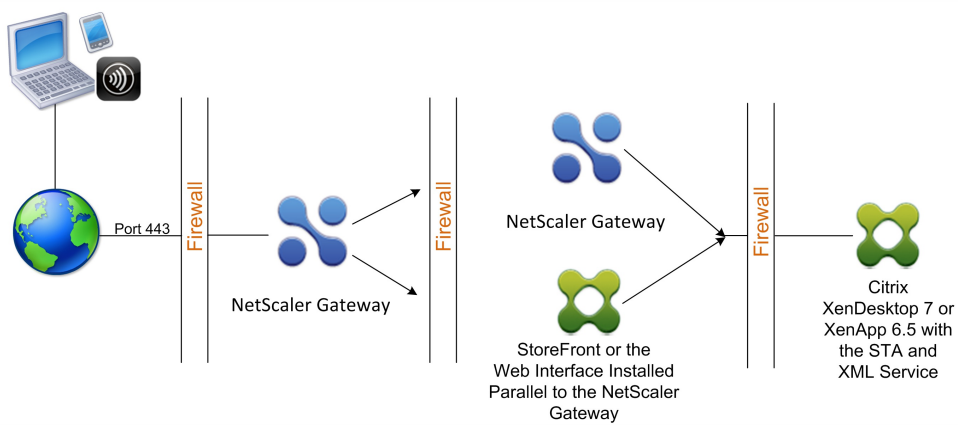
[Redacted]

[Redacted]

[Redacted]



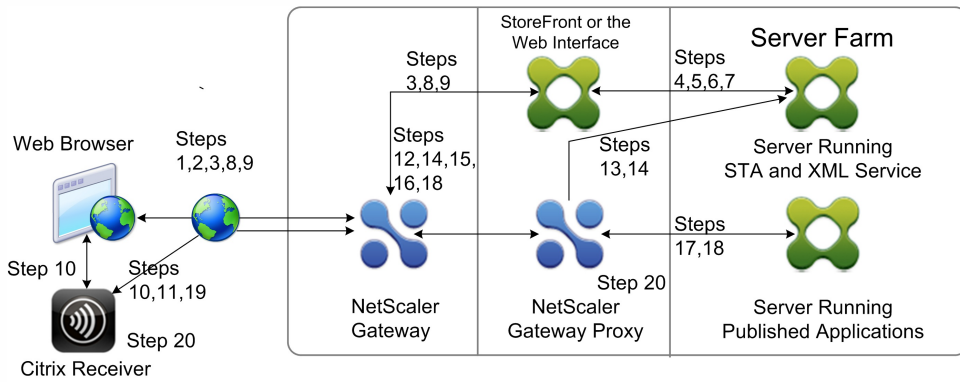


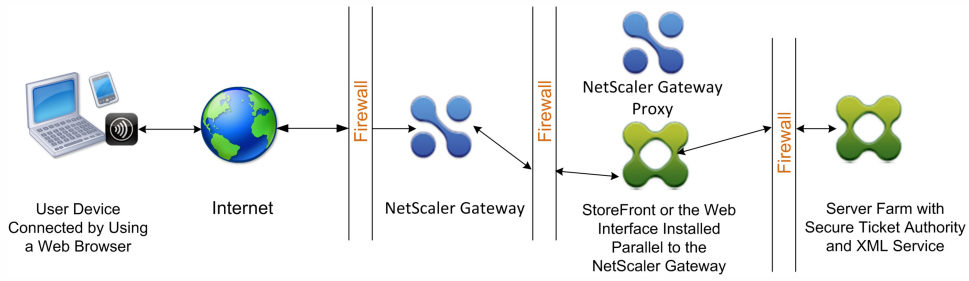




- 
- 
- 
-

- 
- 
- 
- 









- 
- 
- 
- 
- 
-

- 
- 
- 
- 

- 
- 
- 
-

- 
- 
- 
- 
- 
-

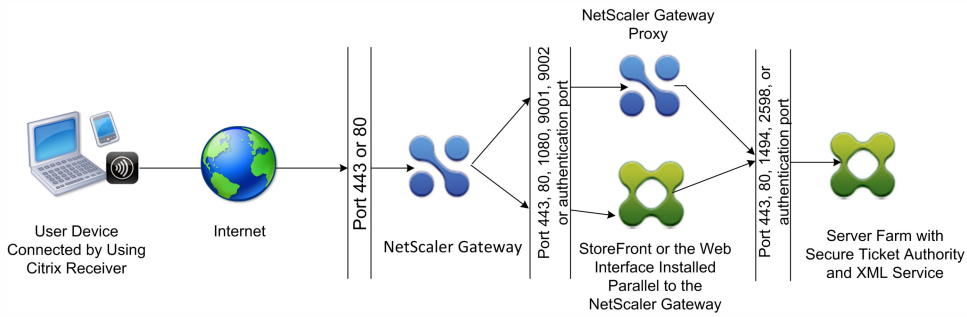








# Opening the Appropriate Ports on the Firewalls



|  |  |
|--|--|
|  |  |
|  |  |
|  |  |

|  |  |
|--|--|
|  |  |
|  |  |



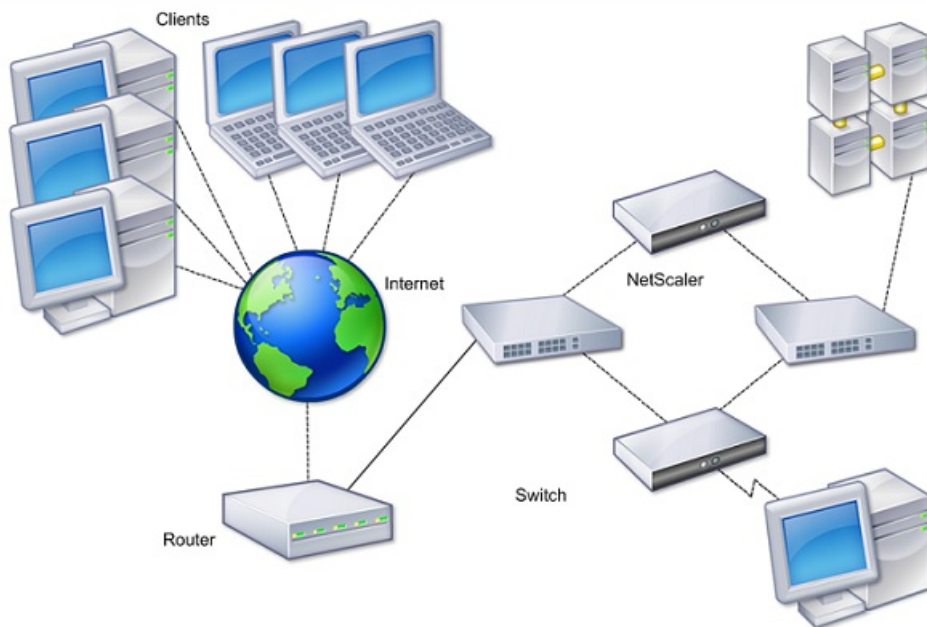
# Managing SSL Certificates in a Double-Hop DMZ Deployment







# Using High Availability





# How High Availability Works

- 
- 
- 

- 
- 

- 

- 

- 

- 

- 

-



# Configuring Settings for High Availability



# Creating or Changing an RPC Node Password

# Configuring the Primary and Secondary Appliances for High Availability



# Configuring Communication Intervals

- 
-

# Synchronizing NetScaler Gateway Appliances

- 
- 

- 
- 

- 
- 
-

# Synchronizing Configuration Files in a High Availability Setup

- 
- 
- 
-

# Configuring Command Propagation

- 
-

# Troubleshooting Command Propagation

- 
- 
-

# Configuring Fail-Safe Mode

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

# Configuring the Virtual MAC Address



# Configuring IPv4 Virtual MAC Addresses

# Creating or Modifying an IPv4 virtual MAC address

# Configuring IPv6 virtual MAC addresses

# Creating or Modifying a Virtual MAC Address for IPv6

- 
-

# Configuring High Availability Pairs in Different Subnets



# Adding a Remote Node

# Configuring Route Monitors

May 30, 2013

You can use route monitors to make the high availability state dependent on the internal routing table, whether or not the table contains any dynamically learned or static routes. In an 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.

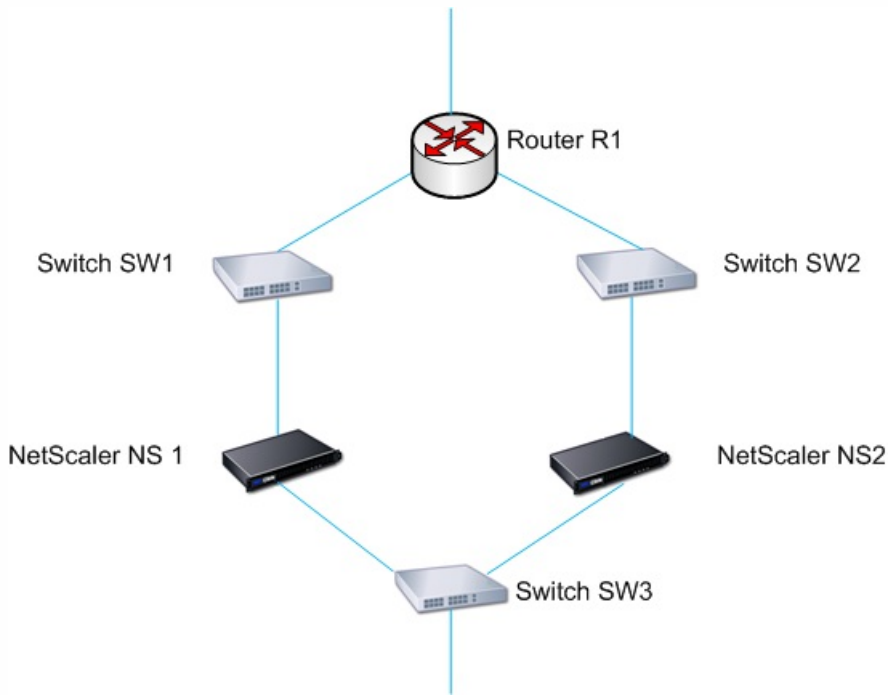
Route monitors are supported on either enabled or disabled Independent Network Configuration settings. The following table shows what occurs with route monitors in a high availability setup and with Independent Network Configuration enabled or disabled.

| 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 of the 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, in order to allow NetScaler Gateway to learn the dynamic routes, which may take up to 180 seconds: <ul style="list-style-type: none"><li>• reboot</li><li>• failover</li><li>• set route6 command for v6 routes</li><li>• set route msr enable/disable command for v4 routes</li><li>• adding a new route monitor</li></ul> | 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 failover 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 route to R1 is down from both NS1 and NS2, failover happens every 180 seconds till one of the appliances is able to reach R1 and restore the connection.

# Adding or Removing Route Monitors

Jan 22, 2014

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.

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.

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

Jan 22, 2014

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 nonfunctional.

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.

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.

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.

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

May 30, 2013

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

May 29, 2013

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

May 29, 2013

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 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."

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

Jan 21, 2014

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.

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

May 30, 2013

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 could 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.

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.

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

Jun 27, 2014

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

You should 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.

# Configuring Clustering

Jun 26, 2014

The primary tasks in setting up NetScaler Gateway clustering are:

1. Decide which NetScaler Gateway appliance or VM will be 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 cluster node group.

Note that multiple methods are available for configuring a NetScaler cluster. The following set of tasks uses the most direct method available in the configuration utility.

Once you have all of the deployment details in order, begin the configuration on the NetScaler Gateway that will be 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.
  1. Enter a Cluster instance ID. This 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.
  2. Enter the Cluster IP address. This will be the cluster's configuration coordinator IP address, which is the management IP address for the cluster.
  3. 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. Wait for system to restart. Once available, log on to the configuration utility at the Cluster IP address configured in step 4b.
8. 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.

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 should be completed before configuring your NetScaler Gateway setup. This way, you

will 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 username 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.

Repeat steps 4 through 9 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.

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. This is required 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 will be the only node bound to the cluster 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.

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.

# Maintaining and Monitoring the System

May 29, 2013

Once you complete configuration of your Citrix 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 web site, you can navigate to the NetScaler Gateway download site and 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 restricts 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

May 28, 2013

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 additional 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 who is assigned to monitor NetScaler Gateway connections and logs and another person who is 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. You must 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 execute 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

Feb 21, 2014

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. You use the configuration utility to create system users, system groups, command policies, and to define permissions.

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 Password and Confirm Password, 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. Under Command Policies, in Action, click Insert.
8. In the Insert Command Policies dialog box, select the command, click OK, click Create and then click close.

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

May 19, 2013

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. If you configure a simple policy, you configure a component on the appliance, such as NetScaler Gateway and authentication. If 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.

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

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 a 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 users or groups you create. You cannot bind a custom command policy to the user nsroot.

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

May 19, 2013

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 two 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 should 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 could 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

Feb 21, 2014

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.

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:
  1. In Name, type the name of the server.
  2. 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

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.

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.

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

Feb 21, 2014

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.                              |

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.

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 NetScaler Gateway Plug-in Logging

May 23, 2013

You can configure the NetScaler Gateway Plug-in to log all errors to text files that are stored on the user device. Users can configure the NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in 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 NetScaler Gateway Plug-in. Users can email the log files to Technical Support.

In the Configuration dialog box, users can set the level of logging for the NetScaler Gateway Plug-in. The logging levels are:

- Record error messages
- Record event messages
- Record NetScaler Gateway Plug-in statistics
- Record all errors, event messages, and statistics

1. On the user device, right-click the NetScaler Gateway icon in the notification area and then click Configure NetScaler Gateway.
2. Click the Trace tab, select the log level and then click OK.

Note: Users must be logged on with the NetScaler Gateway Plug-in to open the Configuration dialog box.

# To monitor ICA connections

Oct 31, 2014

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 XenApp or XenDesktop
  - Port number of the server running XenApp or XenDesktop
1. In the configuration utility, in the navigation pane, click NetScaler Gateway.
  2. In the details pane, under Monitor Connections, click ICA connections to view the monitoring dialog box.



# Integrating with Citrix Products

May 06, 2015

If you are a system administrator responsible for installing and configuring NetScaler Gateway, you can configure the appliance to work with App Controller, StoreFront, and the Web Interface.

Users can connect directly to App Controller from the internal network or from a remote location. When users connect, they can access their web, SaaS, and mobile apps. They can also work with 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 App Controller, 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, App Controller, XenApp, XenDesktop, and the Web Interface reside in the secure network.
- ShareFile is configured in App Controller. For more information about ShareFile, see [ShareFile](#) and [Configuring ShareFile for User Access](#).

How you deploy StoreFront and App Controller depends on the apps you provide to mobile devices. If users have access to MDX apps that are wrapped with the MDX Toolkit, App Controller resides in front of StoreFront in the secure network. If you are not providing access to MDX apps, StoreFront resides in front of App Controller in the secure network.

# How Users Connect to Applications, Desktops, and ShareFile

May 18, 2015

If you have App Controller in your deployment, users can connect in the following ways:

- NetScaler Gateway Plug-in that establishes a full VPN tunnel to resources in the internal network. You create a session profile to select the NetScaler Gateway Plug-in for Windows or the NetScaler Gateway Plug-in for Mac. When users log on by using the plug-in, endpoint analysis scans can run on the user device.  
Note: To allow endpoint analysis scans to run on Mac computers, you must install NetScaler Gateway 10.1, Build 120.1316.e or newer.
- Citrix Receiver to connect to web, SaaS, and Enterprise applications, web links, and documents from ShareFile through App Controller. When users log on with Receiver, NetScaler Gateway routes the connection to App Controller. When Receiver establishes the connection, users' applications and documents appear in Receiver. If users log on with Receiver and connect to App Controller directly, you must enable clientless access in NetScaler Gateway. This deployment does not require StoreFront.
- Receiver to connect to published applications and virtual desktops through StoreFront or the Web Interface. When users log on with Receiver, NetScaler Gateway routes the connection to StoreFront or the Web Interface. When Receiver establishes the connection, user applications and desktops appear in Receiver.
- Worx Home to connect to iOS and Android apps, including WorxMail and WorxWeb, from mobile devices through App Controller. When users log on to Worx Home, they have access to the mobile apps that you configure in App Controller. When NetScaler Gateway establishes the Micro VPN connection, users mobile apps appear in the Worx Home window. Users can start the apps from Worx Home. Some apps require users to download and install the app on the mobile device.

In any of the preceding scenarios, if users want to connect through NetScaler Gateway, they do the following:

- Users log on by using the NetScaler Gateway Plug-in or Receiver. To log on for the first time, users open a web browser and type the fully qualified domain name (FQDN) of NetScaler Gateway or Receiver. Users with mobile devices log on with Worx Home.
- On the logon page, users enter their credentials and are authenticated.
- After authentication, the user session redirects to StoreFront or App Controller depending on your deployment.
- If you deploy both StoreFront and App Controller, NetScaler Gateway contacts the first server in the deployment. For example, if you configure MDX mobile apps in App Controller, you deploy StoreFront behind App Controller. If you are not providing access to MDX mobile apps, you deploy App Controller behind StoreFront.
- All of the users' desktops, documents, and web, SaaS, and Windows-based applications appear in Receiver or Worx Home.

If users need to access other resources in the internal network, such as Exchange, file shares, or internal web sites, they can also log on with the NetScaler Gateway Plug-in. For example, if users want to connect to a Microsoft Exchange server in the network, they start Microsoft Outlook on their computer. The secure connection is made with the NetScaler Gateway Plug-in which connects to NetScaler Gateway. The SSL VPN tunnel is created to the Exchange Server and users can access their email.

Important: Citrix recommends configuring authentication on the NetScaler Gateway virtual server. When you disable authentication in NetScaler Gateway, unauthenticated HTTP requests are sent directly to the servers running the Web

Interface, StoreFront or App Controller in the internal network.

# Deploying with XenMobile App Edition, XenApp, and XenDesktop

Mar 25, 2014

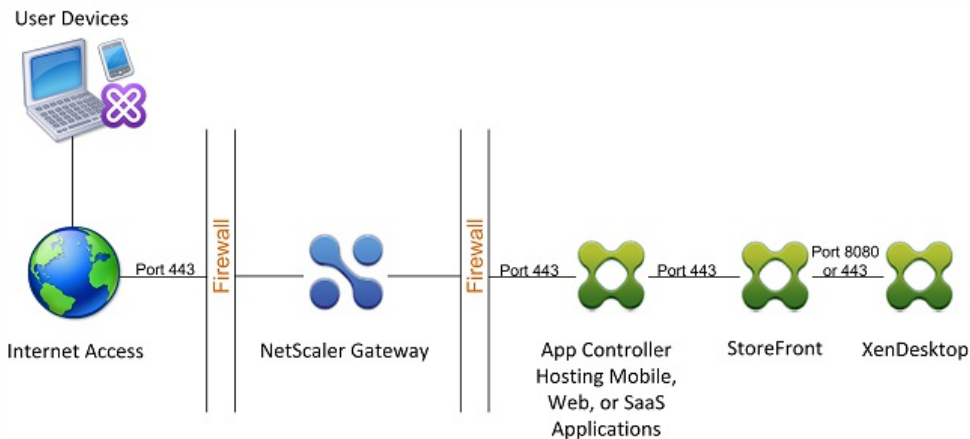
You can have users connect to Windows, web, SaaS, and mobile applications and virtual desktops hosted in your network. You can provide access to your applications and desktops for remote and internal users by using NetScaler Gateway, XenMobile App Edition, and XenApp and XenDesktop. NetScaler Gateway authenticates users and then allows them to access their applications by using Citrix Receiver or Worx Home.

Users connect to their Windows-based apps published in XenApp and virtual desktops published in XenDesktop by using Receiver and StoreFront.

XenMobile App Edition contains App Controller, which allows users to connect to web, SaaS, and MDX applications. App Controller allows you to manage web, SaaS, and MDX applications for single sign-on (SSO), along with ShareFile documents. You install App Controller in the internal network. Remote users connect to App Controller through NetScaler Gateway to access their applications and ShareFile data. Remote users can connect with either the NetScaler Gateway Plug-in, Receiver, or Worx Home to access applications and ShareFile. Users who are in the internal network can connect directly to App Controller by using Receiver. The following figure shows NetScaler Gateway deployed with App Controller and StoreFront.

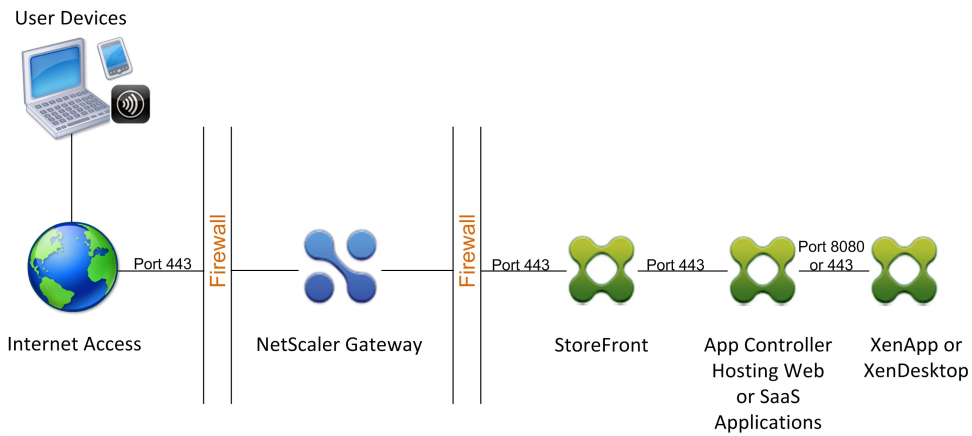
If your deployment provides access to MDX applications from App Controller and access to Windows-based applications from StoreFront, you deploy App Controller in front of StoreFront as shown in the following illustration:

Figure 1. Deploying NetScaler Gateway with App Controller in Front of StoreFront



If your deployment does not provide access to MDX applications, StoreFront resides in front of App Controller, as shown in the following illustration:

Figure 2. Deploying NetScaler Gateway with StoreFront in Front of App Controller



With each deployment, StoreFront and App Controller must reside in the internal network and NetScaler Gateway must be in the DMZ. For more information about deploying App Controller, see [Installing App Controller](#). For more information about deploying StoreFront, see [StoreFront](#).

# Accessing XenApp and XenDesktop Resources with the Web Interface

May 15, 2013

One or more computers running XenApp or XenDesktop creates a server farm. If your enterprise network contains a server farm, you can deploy NetScaler Gateway to provide secure Internet access to published applications or virtual desktops by using the Web Interface.

In such deployments, NetScaler Gateway works with the Web Interface and the Secure Ticket Authority (STA) to provide authentication, authorization, and redirection to published applications hosted on a computer running XenApp or to virtual desktops provided by XenDesktop.

This functionality is achieved by integrating NetScaler Gateway with the Web Interface, XenApp, or XenDesktop. This integration provides advanced authentication and an access control option to the Web Interface. For more information about the Web Interface, see the Web Interface documentation in the Citrix documentation library.

Remote connectivity to a server farm does not require the NetScaler Gateway Plug-in. To access published applications or desktops, users connect by using Citrix Receiver.

# Integrating NetScaler Gateway with XenApp or XenDesktop

Feb 07, 2014

When you configure NetScaler Gateway for user connections, you can include settings for network traffic to XenApp, XenDesktop, or both. To do so, you configure NetScaler Gateway and the Web Interface to communicate with each other.

The tasks for integrating these products include:

- Creating a Web Interface site in the XenApp or XenDesktop farm.
- Configuring settings within the Web Interface to route user connections through NetScaler Gateway.
- Configuring NetScaler Gateway to communicate with the Web Interface and the Secure Ticket Authority (STA).

You can also configure NetScaler Gateway to communicate with a XenApp server farm by deploying NetScaler Gateway in a double-hop DMZ. For more information, see [Deploying NetScaler Gateway in a Double-Hop DMZ](#).

NetScaler Gateway and Web Interface use the STA and Citrix XML Service to establish user connections. The STA and XML Service run on the XenApp or XenDesktop server.

# Establishing a Secure Connection to the Server Farm

Feb 07, 2014

The following example shows how NetScaler Gateway deployed in the DMZ works with the Web Interface to provide a secure, single point-of-access to published resources available in a secure enterprise network.

In this example, all of the following conditions exist:

- User devices from the Internet connect to NetScaler Gateway by using Citrix Receiver.
  - The Web Interface resides behind NetScaler Gateway in the secure network. The user device makes the initial connection to NetScaler Gateway and the connection is passed to the Web Interface.
  - The secure network contains a server farm. One server within this server farm runs the Secure Ticket Authority (STA) and the Citrix XML Service. The STA and the XML Service can run on either XenApp or XenDesktop.
1. A remote user types the address of NetScaler Gateway; for example, <https://www.ag.wxyco.com>, in the address field of a web browser. The user device attempts this SSL connection on port 443, which must be open through the firewall for the connection to succeed.
  2. NetScaler Gateway receives the connection request and users are asked for their credentials. The credentials are passed back through NetScaler Gateway, users are authenticated, and the connection is passed to the Web Interface.
  3. The Web Interface sends the user credentials to the Citrix XML Service running in the server farm.
  4. The XML Service authenticates the user credentials and sends the Web Interface a list of the published applications or desktops the user is authorized to access.
  5. The Web Interface populates a Web page with the list of published resources (applications or desktops) that the user is authorized to access and sends this Web page to the user device.
  6. The user clicks a published application or desktop link. An HTTP request is sent to the Web Interface indicating the published resource that the user clicked.
  7. The Web Interface interacts with the XML Service and receives a ticket indicating the server on which the published resource runs.
  8. The Web Interface sends a session ticket request to the STA. This request specifies the IP address of the server on which the published resource runs. The STA saves this IP address and sends the requested session ticket to the Web Interface.
  9. The Web Interface generates an ICA file containing the ticket issued by the STA and sends it to the Web browser on the user device. The ICA file generated by the Web Interface contains the fully qualified domain name (FQDN) or the Domain Name System (DNS) name of NetScaler Gateway. Note that the IP address of the server running the requested resource is never revealed to users.
  10. The ICA file contains data instructing the web browser to start Citrix Receiver. The user device connects to NetScaler Gateway by using the NetScaler Gateway FQDN or DNS name in the ICA file. Initial SSL/TLS handshaking occurs to establish the identity of NetScaler Gateway.
  11. The user device sends the session ticket to NetScaler Gateway and then NetScaler Gateway contacts the STA for ticket validation.
  12. The STA returns the IP address of the server on which the requested application resides to NetScaler Gateway.
  13. NetScaler Gateway establishes a TCP connection to the server.
  14. NetScaler Gateway completes the connection handshake with the user device and indicates to the user device that the connection is established with the server. All further traffic between the user device and the server is proxied through NetScaler Gateway. The traffic between the user device and NetScaler Gateway is encrypted. The traffic between



NetScaler Gateway and the server can be encrypted independently, but is not encrypted by default.

# Deploying with the Web Interface

Jan 15, 2014

When you deploy NetScaler Gateway to provide secure remote access to XenApp or XenDesktop, NetScaler Gateway works with the Web Interface and the Secure Ticket Authority (STA) to provide access to published applications and desktops hosted in a server farm.

Deploying NetScaler Gateway in the DMZ is the most common configuration when NetScaler Gateway operates with a server farm. In this configuration, NetScaler Gateway provides a secure single point-of-access for the web browsers and Citrix Receiver that access the published resources through the Web Interface. This section covers the basic aspects of about this deployment option.

The configuration of your organization's network determines where you deploy NetScaler Gateway when it operates with a server farm. You have the following two options:

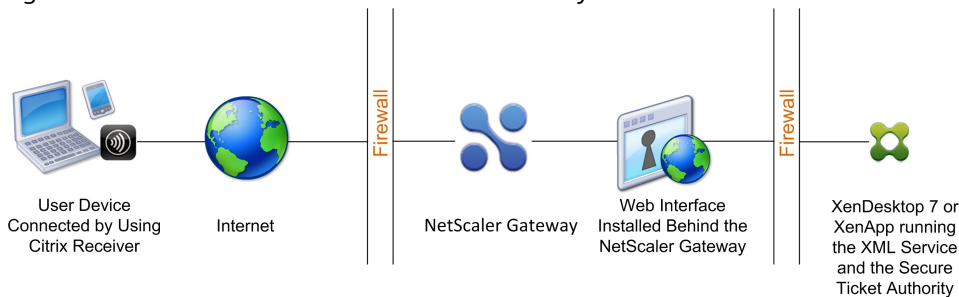
- If your organization protects the internal network with a single DMZ, deploy NetScaler Gateway in the DMZ.
- If your organization protects the internal network with two DMZs, deploy one NetScaler Gateway in each of the two network segments in a double-hop DMZ configuration. For more information, see [Deploying NetScaler Gateway in a Double-Hop DMZ](#).

Note: You can also configure a double-hop DMZ with the second NetScaler Gateway appliance in the secure network.

When you deploy NetScaler Gateway in the DMZ to provide remote access to a server farm, you can implement one of the following three deployment options:

- Deploy the Web Interface behind NetScaler Gateway in the DMZ. In this configuration, as shown in the following figure, both NetScaler Gateway and the Web Interface are deployed in the DMZ. The initial user connection goes to NetScaler Gateway and is then redirected to the Web Interface.

Figure 1. Web Interface Behind NetScaler Gateway in the DMZ



- Deploy NetScaler Gateway parallel to the Web Interface in the DMZ. In this configuration, both NetScaler Gateway and the Web Interface are deployed in the DMZ, but the initial user connection goes to the Web Interface instead of NetScaler Gateway.
- Deploy NetScaler Gateway in the DMZ and deploy the Web Interface in the internal network. In this configuration, NetScaler Gateway authenticates user requests before relaying the request to the Web Interface in the secure network. The Web Interface does not perform authentication, but interacts with the STA and generates an ICA file to ensure that ICA traffic is routed through NetScaler Gateway to the server farm.

The location in which you deploy the Web Interface depends on a number of factors, including:

- Authentication. When users log on, either NetScaler Gateway or the Web Interface can authenticate user credentials. Where you place the Web Interface in your network is a factor that determines, in part, where users authenticate.

- User software. Users can connect to the Web Interface with either the NetScaler Gateway Plug-in or Citrix Receiver. You can limit the resources users can access by using Citrix Receiver only, or give users greater network access with the NetScaler Gateway Plug-in. How users connect, and the resources to which you allow users to connect can help determine where you deploy the Web Interface in your network.

# Deploying the Web Interface in the Secure Network

Jan 15, 2014

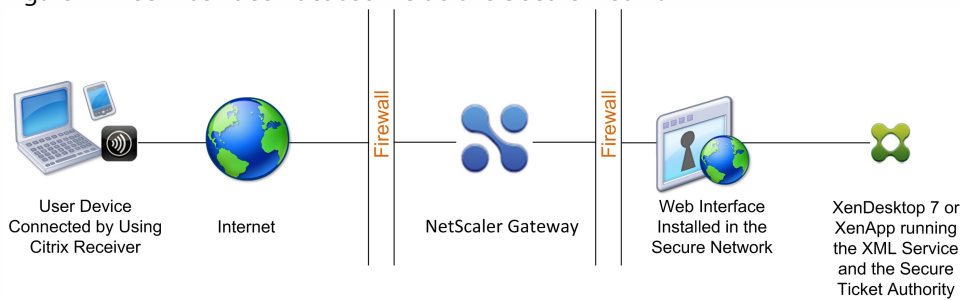
In this deployment, the Web Interface resides in the secure, internal network. NetScaler Gateway is in the DMZ. NetScaler Gateway authenticates user requests before sending the requests to the Web Interface.

When you deploy the Web Interface in the secure network, you must configure authentication on NetScaler Gateway.

If you deploy the Web Interface with Citrix XenDesktop, deploying the Web Interface in the secure network is the default deployment scenario. When the Desktop Delivery Controller is installed, a custom version of the Web Interface is also installed.

**Important:** When the Web Interface is in the secure network, you should enable authentication on NetScaler Gateway. Users connect to NetScaler Gateway, type their credentials, and then connect to the Web Interface. When you disable authentication, unauthenticated HTTP requests are sent directly to the server running the Web Interface. Disabling authentication on NetScaler Gateway is recommended only when the Web Interface is in the DMZ and users connect directly to the Web Interface.

Figure 1. Web Interface Located Inside the Secure Network



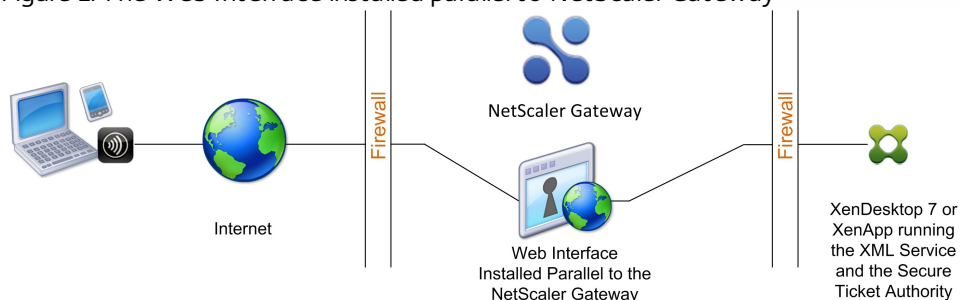
# Deploying the Web Interface Parallel to NetScaler Gateway in the DMZ

Jan 15, 2014

In this deployment, the Web Interface and NetScaler Gateway both reside in the DMZ. Users connect directly to the Web Interface by using a web browser or Citrix Receiver. User connections are first sent to the Web Interface for authentication. After authentication, the connections are routed through NetScaler Gateway. After users log on successfully to the Web Interface, they can access published applications or desktops in the server farm. When users start an application or desktop, the Web Interface sends an ICA file containing instructions for routing ICA traffic through NetScaler Gateway as if it were a server running the Secure Gateway. The ICA file delivered by the Web Interface includes a session ticket produced by the Secure Ticket Authority (STA).

When Citrix Receiver connects to NetScaler Gateway, the ticket is presented. NetScaler Gateway contacts the STA to validate the session ticket. If the ticket is still valid, the user's ICA traffic is relayed to the server in the server farm. The following figure shows this deployment.

Figure 1. The Web Interface installed parallel to NetScaler Gateway



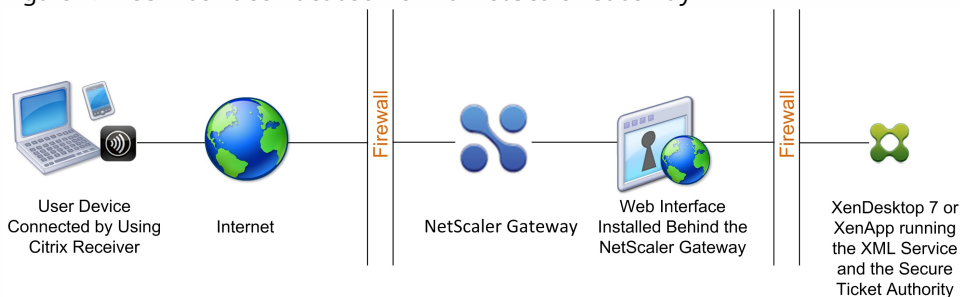
When the Web Interface runs parallel to NetScaler Gateway in the DMZ, you do not need to configure authentication on NetScaler Gateway. The Web Interface authenticates users.

# Deploying the Web Interface Behind NetScaler Gateway in the DMZ

Jan 15, 2014

In this configuration, both NetScaler Gateway and the Web Interface are deployed in the DMZ. When users log on with Citrix Receiver, the initial user connection goes to NetScaler Gateway and is then redirected to the Web Interface. To route all HTTPS and ICA traffic through a single external port and require the use of a single SSL certificate, NetScaler Gateway acts as a reverse web proxy for the Web Interface.

Figure 1. Web Interface Located Behind NetScaler Gateway



When the Web Interface is deployed behind NetScaler Gateway in the DMZ, you can configure authentication on the appliance but it is not required. You can have either NetScaler Gateway or the Web Interface authenticate users because both reside in the DMZ.

# Setting Up a Web Interface Site to Work

May 13, 2013

The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their published applications and desktops through a standard Web browser or through Citrix Receiver.

You can use the Access Management Console to configure Web Interface 5.1 sites and the Web Interface Management console to create Web Interface sites for Versions 5.2, 5.3, and 5.4. You can install the consoles on Windows-based platforms only.

To configure the Web Interface to work with NetScaler Gateway, you need to:

- Create the Web Interface site for the version you are using.
- Configure settings in the Web Interface.
- Configure Web Interface settings on NetScaler Gateway.

# Web Interface Features

May 30, 2013

Before you configure the Web Interface to work with NetScaler Gateway, you need to understand the differences between Citrix XenApp Web sites and XenApp Services sites.

- **XenApp Web sites.** The Web Interface provides functionality to create and manage XenApp Web sites. Users access published resources and streamed applications remotely using a Web browser and a plug-in.
- **XenApp Services sites.** XenApp is a plug-in designed for flexibility and ease of configuration. By using XenApp in conjunction with XenApp Services sites on the Web Interface, you can integrate published resources with users' desktops. Users access remote and streamed applications, and remote desktops and content by clicking icons on their desktop or the Start menu, or by clicking in the notification area of their computer desktop. You can determine the configuration options your users can access and modify, such as audio, display, and logon settings.

Note: If you select this option, access to virtual desktops is not supported.

For more information, see the Web Interface documentation in the Technologies node in the Citrix eDocs library.



# Setting Up a Web Interface Site

May 30, 2013

If you deploy the Web Interface in the secure network and configure authentication on NetScaler Gateway, when users connect to NetScaler Gateway, the appliance authenticates users.

**Important:** Install and configure the Web Interface before you configure NetScaler Gateway. For more information, see the Web Interface documentation in the Technologies node in the Citrix eDocs library.

The steps for creating a Web Interface site include:

- Select how users log on. This can be through a web browser, the NetScaler Gateway Plug-in, or Citrix Receiver. For information, see [Web Interface Features](#).
- Identify where users authenticate from. NetScaler Gateway or the Web Interface.

**Note:** When the Web Interface is in the secure network, you enable authentication on the virtual server on the NetScaler Gateway. When you disable authentication, unauthenticated HTTP requests are sent directly to the server running the Web Interface. Disabling authentication on NetScaler Gateway is recommended only when the Web Interface is in the DMZ and users connect directly to the Web Interface.

Make sure you install a valid server certificate on NetScaler Gateway. For more information about working with certificates, see [Installing and Managing Certificates](#).

**Important:** For the Web Interface to work properly with NetScaler Gateway 10.1, the server running the Web Interface must trust the NetScaler Gateway certificate and be able to resolve the virtual server fully qualified domain name (FQDN) to the correct IP address.

# Creating a Web Interface 5.4 Site

Feb 06, 2014

The Citrix Web Interface Management console is a Microsoft Management Console (MMC) 3.0 snap-in that enables you to create and configure XenApp Web and XenApp Services sites hosted on Microsoft Internet Information Services (IIS). Web Interface site types are shown in the left pane. The central results pane displays the sites available within the site type container selected in the left pane.

The Citrix Web Interface Management console enables you to perform day-to-day administration tasks quickly and easily. The Action pane lists the tasks currently available. Tasks relating to items selected in the left pane are shown at the top and actions available for items selected in the results pane are shown below.

When using the console, your configuration takes effect when you commit your changes using the console. As a result, some Web Interface settings may be disabled if their values are not relevant to the current configuration and the corresponding settings are reset to their default values in `WebInterface.conf`. Citrix recommends that you create regular backups of the `WebInterface.conf` and `config.xml` files for your sites.

The Citrix Web Interface Management console is installed automatically when you install Web Interface for Microsoft Internet Information Services. Run the console by clicking `Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management`.

Note: You must ensure that MMC 3.0 is present on the server on which you install the Web Interface as this is a prerequisite for installation of the Citrix Web Interface Management console. MMC 3.0 is available by default on all the Windows platforms supported for hosting the Web Interface.

You can edit the following configuration files to configure Web Interface sites:

- Web Interface configuration file. The Web Interface configuration file, `WebInterface.conf`, enables you to change many Web Interface properties; it is available on both Microsoft Internet Information Services (IIS) and Java application servers. You can use this file to perform day-to-day administration tasks and customize many more settings. Edit the values in `WebInterface.conf` and save the updated file to apply the changes. For more information about configuring the Web Interface by using `WebInterface.conf`, see the Web Interface documentation in the Technologies node in Citrix eDocs.
- Citrix online plug-in configuration file. You can configure the Citrix online plug-in by using the `config.xml` file on the Web Interface server.

# Configuring Sites By Using the Citrix Web Interface Management Console

Feb 07, 2014

The Citrix Web Interface Management console is a Microsoft Management Console (MMC) 3.0 snap-in that enables you to create and configure XenApp Web and XenApp Services sites hosted on Microsoft Internet Information Services (IIS). Web Interface site types are shown in the left pane. The central results pane displays the sites available within the site type container selected in the left pane.

The Citrix Web Interface Management console enables you to perform day-to-day administration tasks quickly and easily. The Action pane lists the tasks currently available. Tasks relating to items selected in the left pane are shown at the top and actions available for items selected in the results pane are shown below.

When using the console, your configuration takes effect when you commit your changes using the console. As a result, some Web Interface settings may be disabled if their values are not relevant to the current configuration and the corresponding settings are reset to their default values in `WebInterface.conf`. Citrix recommends that you create regular backups of the `WebInterface.conf` and `config.xml` files for your sites.

The Citrix Web Interface Management console is installed automatically when you install Web Interface for Microsoft IIS. Run the console by clicking Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

Note: You must ensure that MMC 3.0 is present on the server on which you install the Web Interface as this is a prerequisite for installation of the Citrix Web Interface Management console. MMC 3.0 is available by default on all the Windows platforms supported for hosting the Web Interface.

# Configuring NetScaler Gateway Settings in the Web Interface 5.4

Feb 07, 2014

To use NetScaler Gateway in your deployment, you must configure the Web Interface support the appliance. To do this, use the Secure Access task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click either XenApp Web Sites or XenApp Services Sites and then select your site in the results pane.
3. In the Action pane, click Secure Access.
4. On the Specify Access Methods page, do one of the following:
  - Click Add to add a new access route.
  - Select an existing route from the list and then click Edit.
5. From the Access method list, select one of the following options:
  - If you want to send the actual address of the Citrix server to NetScaler Gateway, select Gateway Direct.
  - If you want to send the alternate address of the XenApp server to NetScaler Gateway, select Gateway alternate. Note: XenDesktop virtual desktops cannot be accessed if alternate addresses are used.
  - If you want the address given to NetScaler Gateway to be determined by the address translation mappings set in the Web Interface, select Gateway translated.
6. Enter the network address and subnet mask that identify the client network. Use the Move Up and Move Down buttons to place the access routes in order of priority in the User device addresses table and then click Next.
7. If you are not using gateway address translation, continue to Step 10. If you are using gateway address translation, do one of the following on the Specify Address Translations page:
  - Click Add to add a new address translation.
  - Select an existing address translation from the list and then click Edit.
8. In the Access Type area, select one of the following options:
  - If you want NetScaler Gateway to use the translated address to connect to the Citrix server, select Gateway route translation.
  - If you configured a client translated route in the User device addresses table and want both the Citrix client and NetScaler Gateway to use the translated address to connect to the Citrix server, select User device and gateway route translation.
9. Enter the internal and external (translated) ports and addresses for the Citrix server, click OK and then click Next. When NetScaler Gateway connects to the Citrix server, it uses the external port number and address. Ensure that the mappings you create match the type of addressing being used by the server farm.
10. On the Specify Gateway Settings page, specify the fully qualified domain name (FQDN) and port number of the NetScaler Gateway appliance that clients must use. The FQDN must match what is on the certificate installed on the gateway.
11. Select Enable session reliability if you want the Citrix server to keep disconnected sessions open while the client attempts to reconnect automatically.
12. Select Request tickets from two STAs where available if you enabled session reliability and want to use simultaneous ticketing from two Secure Ticket Authority (STA) servers. When you enable this option, the Web Interface obtains

tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If for any reason the Web Interface is unable to contact two STAs, it falls back to using a single STA. Click Next.

13. On the Specify Secure Ticket Authority Settings page, do one of the following:

- Click Add to specify the URL of a STA that the Web Interface can use.
- Select an entry from the list and then click Edit.

Use the Move Up and Move Down buttons to place the STAs in order of priority.

STAs are included with the Citrix XML Service; for example, `http[s]://servername.domain.com/scripts/ctxsta.dll`. You can specify more than one STA for fault tolerance; however, Citrix recommends that you do not use an external load balancer for this purpose.

14. Select Use for load balancing to choose whether or not to enable load balancing between STAs.

Enabling load balancing allows you to evenly distribute connections among servers so that no one server becomes overloaded.

15. Select Bypass failed servers for to specify the length of time that unreachable STAs should be bypassed.

The Web Interface provides fault tolerance among the servers on the STA URLs list so that if a communication error occurs, the failed server is bypassed for the specified time period.

# Creating a Web Interface 5.3 Site

May 28, 2013

When you create a Web Interface 5.3 site, you can require users to log on with either a web browser, Citrix Receiver, or Citrix Desktop Receiver. You can use the Citrix Web Interface Management console to create multiple Web Interface sites.

You can only enable single sign-on with a smart card to the Web Interface with Web Interface 5.3. This version of the Web Interface can run on XenApp 4.5, 5.0, and 6.0.

Web Interface 5.3 runs on the following operating systems:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Note: XenApp 6.0 runs only on Windows Server 2008 R2.

1. Click Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane, select XenApp Web Sites. Users log on to the Web Interface using a Web browser.
3. On the Action menu, click Create Site.
4. Keep the default Internet Information Services (IIS) site and path and then click Next.

The default site path is /Citrix/XenApp or you can specify a path.

Note: If there are any preexisting XenApp Web sites that use the default path, an appropriate increment is added to distinguish the new site.

5. In Specify where user authentication takes place, select one of the following:
  - At Web Interface to have users authenticate using the Web Interface.  
Select this option if the Web Interface is deployed as a standalone server parallel to NetScaler Gateway in the demilitarized zone (DMZ).
  - At Access Gateway to have users authenticate using the NetScaler Gateway appliance.  
If you select this option, NetScaler Gateway authenticates users and initiates single sign-on to the Web Interface if it is configured on the appliance.

Note: If SmartAccess is configured on NetScaler Gateway, this setting enables SmartAccess in XenApp or XenDesktop.

6. Click Next.
7. If you selected At Access Gateway in Step 5, in Authentication service URL, type the Web address to the NetScaler Gateway authentication service URL, such as <https://access.company.com/CitrixAuthService/AuthService.aspx> and then click Next.
8. Under Authentication Options, select how users log on:
  - Explicit. Users log on by using a Web browser.
  - Smart Card. Users log on by using a smart card.
9. Click Next.
10. If you selected Smart Card in Step 8, select one of the following:
  - Prompt users for PIN. Users enter their personal identification number (PIN) when they start a published application or desktop.
  - Enable smart card pass-through. Users do not have to enter their PIN when they start a published application or

desktop.

You receive a summary screen showing your settings. Click Next to create the Web Interface site. When the site is successfully created, you are then prompted to configure the remaining settings in the Web Interface. Follow the instructions in the wizard to complete the configuration.

# Configuring NetScaler Gateway Settings in Web Interface 5.3

Nov 30, 2013

After you create the Web Interface 5.3 site, you can use Citrix Web Interface Management to configure settings for NetScaler Gateway.

1. Click Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of Citrix Web Interface Management, click XenApp Web Sites.
3. In the Action pane, click Secure Access.
4. In the Edit Secure Access Settings dialog box, click Add.
5. In the Add Access Route dialog box, type the user device address, subnet mask, and in Access Method, select Gateway direct, click OK and then click Next. If you do not specify the user device address and subnet mask, the Gateway direct option applies to all user devices. The Gateway direct option is appropriate for user devices connecting from outside of the internal network, whereas the Direct option is appropriate for user devices connecting from within the internal network.
6. In Address (FQDN), type the NetScaler Gateway fully qualified domain name (FQDN). This must be the same FQDN that is used on the NetScaler Gateway certificate.
7. In Port, type the port number. The default is 443.
8. To enable session reliability, click Enable session reliability and then click Next.
9. Under Secure Ticket Authority URLs, click Add.
10. In Secure Ticket Authority URL, type the name of the master server running the XML Service on XenApp, click OK and then click Finish. For example, type `http://xenappsrv01/Scripts/CtxSta.dll`.

After you configure the settings in the Web Interface, you can then configure settings on NetScaler Gateway.



# Adding XenApp and XenDesktop to a Single Site

Feb 07, 2014

If you are running XenApp and XenDesktop, you can add both applications to a single Web Interface site. This configuration allows you to use the same Secure Ticket Authority (STA) server from either XenApp or XenDesktop.

Note: XenDesktop supports the Web Interface. The minimum required version of the Web Interface is 5.0. If you are using Web Interface 5.3 or 5.4, you combine the XenApp and XenDesktop sites by using the Web Interface Management console.

Note: If the server farms are in different domains, you must establish two-way trust between the domains.

1. Click Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane, select XenApp Web Sites.
3. In the Action pane, right-click a site and then click Server Farms.
4. In the Manage Server Farms dialog box, click Add.
5. Complete the settings for the server farm and then click OK twice.

For the best experience when using XenDesktop, change the setting `UserInterfaceBranding` to `Desktops` in the `WebInterface.conf` configuration file.

# Routing User Connections Through NetScaler Gateway

Feb 27, 2014

In XenApp and XenDesktop, you can configure the servers to only accept connections that are routed through NetScaler Gateway. In XenApp 6.5, you configure a policy in Citrix AppCenter to route connections through NetScaler Gateway. In XenDesktop 7.1, you use Citrix Studio to configure the settings.

1. Click Start > Administrative Tools > Citrix > Management Consoles > Citrix AppCenter.
2. Expand Citrix Resources > XenApp > farmName, where farmName is the name of the server farm.
3. Click Policies.
4. In the center pane, click Computer or User and then click New.
5. In the New Policy wizard, in Name, type a name for the policy and then click Next.
6. Under Categories, click Server Settings.
7. Under Settings, next to Connection access control, click Add.
8. In the Add Setting - Connection access control dialog box, in Value, select Citrix Access Gateway connections only and then click OK.
9. Click Next two times and then click Create. XenApp creates the policy.

You can restrict access to a Delivery Group's machines. You can restrict access for users by using SmartAccess that filters user connections made through NetScaler Gateway. You can perform this task in the Policy node in Studio, or through policy settings as described in [Quick reference table](#).

1. In Studio, under Delivery Groups, select the Delivery Group you want to restrict.
2. Click Edit Delivery Group and then click Access policy.
3. On the Access Policy page, select Connections through NetScaler Gateway. Only connections through the NetScaler Gateway are allowed.
4. To choose a subset of those connections, select Connections meeting any of the following filters:
  1. Define the NetScaler Gateway site.
  2. Add, edit, or remove the SmartAccess strings that define the allowed user access scenarios for the Delivery Group. For more information about configuring SmartAccess, see [Configuring SmartAccess on NetScaler Gateway](#).

# Configuring Communication with the Web Interface

May 13, 2013

You can configure NetScaler Gateway to communicate with the Web Interface running on Citrix XenApp and Citrix XenDesktop. To do so, configure a virtual server on NetScaler Gateway. Next, bind a signed server certificate and authentication, session, preauthentication, and post-authentication policies to the virtual server. NetScaler Gateway uses the virtual server IP address to route user connections to the Web Interface.

The Published Applications Wizard allows you to configure NetScaler Gateway to route user connections to the Web Interface. NetScaler Gateway uses the Secure Ticket Authority (STA) for user connections.

# Configuring Policies for Published Applications and Desktops

Feb 08, 2014

To establish communication with XenApp and XenDesktop servers, you need to configure NetScaler Gateway to recognize the servers. You can configure the settings globally or you can use policies that are bound to users, groups, or virtual servers. To configure the Web Interface 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. In the Global NetScaler Gateway Settings dialog box, on the Client Experience tab, do the following:
  1. In Plug-in type, select Java.
  2. In Clientless Access, select Allow.

Note: Perform Step 3 to support VPN-capable Citrix Receiver, such as Receiver for iOS or Receiver for Android. To support mobile Receiver, you must install a minimum of Access Gateway 10, Build 69.6 or Access Gateway 10, Build 71.6014.e. If you are running Access Gateway 9.3, you do not need to perform this step.
4. On the Published Applications tab, next to ICA Proxy, select ON.
5. Next to Web Interface Address, type the Web address of the Web Interface and then click OK.

## To configure a session policy for the Web Interface

You can configure a session policy and bind it to a virtual server to limit access to the Web Interface.

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 the Create Session Policy dialog box, in Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In the Create Session Profile dialog box, in Name, type a name for the profile.
6. On the Client Experience tab, do the following:
  1. Next to Plug-in type, select Override Global and then select Java.
  2. Next to Clientless Access, select Override Global and then select Allow.
7. On the Published Applications tab, next to ICA Proxy, click Override Global and select ON.
8. Next to Web Interface Address, click Override Global, type the Web address of the Web Interface 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 a session policy, bind the policy to a virtual server.

## To bind a session policy 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. On the Policies tab, click Session and then click Insert Policy.
4. Select a session policy from the list, enter the priority number (optional) and then click OK



# Configuring Settings with the Published Applications wizard

May 16, 2013

To configure NetScaler Gateway with the Web Interface, you need the following information:

- IP addresses of servers running XenApp or XenDesktop
- Fully qualified domain name (FQDN) of the server running the Web Interface
- Virtual server configured on NetScaler Gateway
- Session policy configured for SmartAccess
- IP addresses of additional servers running the Web Interface if you are configuring Web Interface failover

To configure Web Interface settings by using the Published Applications 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 Published Applications wizard.
3. Click Next and then follow the instructions in the wizard.

You can configure and activate the Secure Ticket Authority (STA) from within the Published Applications wizard. When you complete the Published Applications wizard, the settings are bound globally.

# Configuring the Secure Ticket Authority on NetScaler Gateway

Feb 17, 2014

The Secure Ticket Authority (STA) is responsible for issuing session tickets in response to connection requests for published applications on XenApp and published desktops on XenDesktop. These session tickets form the basis of authentication and authorization for access to published resources.

You can use any of the following methods to configure the STA on NetScaler Gateway:

- Global settings in the configuration utility
- Published Applications wizard
- Session policy

You can bind the STA globally or to virtual servers. You can also add multiple servers running the STA when you configure a virtual server.

If you are securing communications between the NetScaler Gateway and the STA, make sure a server certificate is installed on the server running the STA.

## To bind the STA globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, click NetScaler Gateway > 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, enter the URL of the STA server, click Create and then click OK.
5. In the STA Server dialog box, in URL, type the IP address or fully qualified domain name (FQDN) of the server running the STA and then click Create.

Note: You can add more than one server running the STA to the list. The STAs that are listed in the Web Interface must match the STAs that are configured on NetScaler Gateway. If you are configuring multiple STAs, do not use load balancing between NetScaler Gateway and the servers running the STA.

## To bind a STA 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. On the Published Applications tab, under Secure Ticket Authority, click Add.
4. In the Configure STA Server dialog box, enter the URL of the STA server and then click Create.
5. Repeat Step 4 to add additional STA servers and then click OK in the Configure NetScaler Gateway Virtual Server dialog box.

# Configuring Additional Web Interface Settings on NetScaler Gateway

May 30, 2013

If you deploy NetScaler Gateway in a Web Interface environment, you can complete the following optional tasks:

- [Configuring Web Interface Failover](#) Configure NetScaler Gateway to failover to a secondary server running the Web Interface.
- [Configuring Smart Card Access with the Web Interface](#) Configure user sessions to log on directly to the Web Interface by using Citrix Receiver and smart card authentication.



# Configuring Web Interface Failover

Feb 17, 2014

You can use the Published Applications Wizard to configure NetScaler Gateway to fail over to a secondary server running the Web Interface.

Web Interface failover allows user connections to stay active if the primary Web Interface fails. When you configure failover, you define a new IP address in addition to the system IP address, mapped IP address, or virtual server IP address. The new IP address must be on the same subnet as the system or mapped IP address.

When you configure Web Interface failover on NetScaler Gateway, any network traffic that is sent to the new IP address is relayed to the primary Web Interface. The virtual server that you select in the Published Applications wizard serves as the network address translation (NAT) IP address. The real IP address is that of the Web Interface. If the primary Web Interface fails, network traffic is sent to the secondary Web Interface.

## To configure Web Interface failover

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 Published applications wizard.
3. Click Next, select a virtual server and then click Next.
4. On the Configure Client Connections page, click Configure Web Interface Failover.
5. Under Primary Web Interface, in Web Interface Server, type the IP address of the primary Web Interface.
6. In Web Interface Server Port, type the port number for the primary Web Interface.
7. In Virtual Server IP, type the new IP address for failover.
8. In Virtual Server Port, enter the port number for the virtual server.
9. Under Backup Web Interface, in Web Interface Server, type the IP address of the server running the Web Interface or select a server from the list.
10. In Web Interface Server Port, type the port number of the Web Interface and then click OK.
11. Click Next and then follow the instructions to complete the wizard.

# Configuring Smart Card Access with the Web Interface

May 30, 2013

When you configure the Web Interface to use smart card authentication, you can configure the following deployment scenarios in order to integrate NetScaler Gateway, depending on how users log on:

- If users log on directly to the Web Interface by using Citrix Receiver and smart card authentication, the Web Interface must be parallel to NetScaler Gateway in the DMZ. The server running the Web Interface must also be a domain member.

In this scenario, both NetScaler Gateway and the Web Interface perform SSL termination. The Web Interface terminates secure HTTP traffic including user authentication, the display of published applications, and the starting of published applications. NetScaler Gateway terminates SSL for incoming ICA connections.

- If users log on with the NetScaler Gateway Plug-in, NetScaler Gateway performs the initial authentication. When NetScaler Gateway establishes the VPN tunnel, users can log on to the Web Interface by using the smart card. In this scenario, you can install the Web Interface behind NetScaler Gateway in the DMZ or in the secure network.

Note: NetScaler Gateway can also use the smart card for authentication by using a client certificate. For more information, see [Configuring Smart Card Authentication](#)

# Configuring Access to Applications and Virtual Desktops in the Web Interface

Feb 05, 2014

You can configure NetScaler Gateway to give users access to published applications and virtual desktops with the NetScaler Gateway Plug-in instead of with Receiver. To configure access to applications and desktops, you change the configuration on NetScaler Gateway from using Receiver only to connect to NetScaler Gateway, to a configuration that enables connections by using the NetScaler Gateway Plug-in with single sign-on to the Web Interface. For example, you configure NetScaler Gateway so that all users connect with the NetScaler Gateway Plug-in and use the Web Interface as the home page. This scenario supports single sign-on to the Web Interface.

In addition to access to applications and desktops, users can also run applications installed on the user device that make network connections through the VPN tunnel.

To start the configuration, use the following guidelines:

- Create a Web Interface site.
- Configure Advanced Access Control settings.
- Configure SmartAccess.
- Configure endpoint analysis on NetScaler Gateway.
- Configure policies and filters on Citrix XenApp and XenDesktop.
- Configure NetScaler Gateway so users log on by using the NetScaler Gateway Plug-in to access published applications and virtual desktops.

For more information, see the following topics in Citrix eDocs:

- [Setting Up a Web Interface Site.](#)
- [How SmartAccess Works for XenApp and XenDesktop](#)
- [Configuring Endpoint Polices](#)
- [Configuring XenApp Policies and Filters](#)
- [To configure policies and filters in XenDesktop 5](#)
- [Configuring NetScaler Gateway to Communicate with the Web Interface](#)

When configuring user logon to XenApp and XenDesktop, you first create a session profile to select the NetScaler Gateway Plug-in for Windows. Then, you create a profile for intranet applications for access to XenApp, XenDesktop, and the Web Interface.

To configure global settings for the NetScaler Gateway Plug-in for access to applications and desktops

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 Published Applications tab, next to ICA Proxy, select OFF.
4. In Web Interface Address, type the URL of the Web Interface site. This becomes the home page for users.
5. In Single Sign-On Domain, type the Active Directory domain name.
6. On the Client Experience tab, next to Plug-in Type, select Windows/Mac OS X and then click OK.

## To configure the intranet application

1. In the configuration utility, 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 application.
4. Click Transparent.
5. In Protocol, select the TCP, UDP, or Any.
6. In Destination Type, select IP Address and Netmask . For example, type 172.16.100.0 and the subnet mask 255.255.255.0 to represent all servers on the 172.16.100.x subnet. The IP address of the Web Interface, XenApp, and all other servers to which users connect must be in one of the subnets defined as an intranet application.  
After you create the intranet application, you can bind it globally or to a virtual server.
7. In IP Address and NetMask, type the IP address and subnet mask that represents your internal network, click Create and then click Close.  
After you create the intranet application, you can bind it globally or to a virtual server.

## To bind an intranet application 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 Applications, click Create mappings to TCP applications in the secure network for the NetScaler Gateway Plug-in for Java.
3. In the Configure VPN Intranet Applications dialog box, click Add.
4. Under Available, select one or more intranet applications, click the arrow to move the intranet applications to Configured and then click OK.

## To bind an intranet application 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. In the Configure NetScaler Gateway Virtual Server dialog box, click the Intranet Applications tab.
4. Under Available Application Name, select the intranet applications, click Add and then click OK.

When users log on with the NetScaler Gateway Plug-in, the VPN tunnel is established and either Receiver or the Web Interface is used as the home page.

# Configuring SmartAccess

May 14, 2013

You can use SmartAccess with XenApp and XenDesktop to intelligently deliver published applications and virtual desktops to users.

SmartAccess allows you to control access to published applications and desktops on a server through the use of NetScaler Gateway session policies. You use preauthentication and post-authentication checks as a condition, along with other conditions, for access to published resources. Other conditions include anything you can control with a XenApp or XenDesktop policy, such as printer bandwidth limits, user device drive mapping, clipboard, audio, and printer mapping. You can apply a XenApp or XenDesktop policy based on whether or not users pass an NetScaler Gateway check.

NetScaler Gateway can deliver XenDesktop by using the same options that are available with Web Interface, ICA proxy access, clientless access, and NetScaler Gateway access.

This functionality is achieved by integrating NetScaler Gateway components with the Web Interface and XenApp or XenDesktop. This integration provides advanced authentication and an access control options to the Web Interface. For more information, see the Web Interface documentation in the Technologies node in the Citrix eDocs library.

Remote connectivity to a server farm does not require the NetScaler Gateway Plug-in. Users can connect with Citrix Receiver. Users can use the NetScaler Gateway Plug-in to log on and receive their published applications and virtual desktops through the Access Interface, which is the default home page for NetScaler Gateway.

# How SmartAccess Works for XenApp and XenDesktop

Feb 17, 2014

To configure SmartAccess, you need to configure NetScaler Gateway settings on the Web Interface and configure session policies on NetScaler Gateway. When you run the Published Applications Wizard, you can select the session policies you created for SmartAccess.

After you configure SmartAccess, the feature works as follows:

1. When a user types the web address of a virtual server in a web browser, any preauthentication policies that you configured are downloaded to the user device.
2. NetScaler Gateway sends the preauthentication and session policy names to the Web Interface as filters. If the policy condition is set to true, the policy is always sent as a filter name. If the policy condition is not met, the filter name is not sent. This allows you to differentiate the list of published applications and desktops and the effective policies on a computer running XenApp or XenDesktop, based on the results of the endpoint analysis.
3. The Web Interface contacts the XenApp or XenDesktop server and returns the published resource list to the user. Any resources that have filters applied do not appear in the user's list unless the condition of the filter is met.

You can configure SmartAccess endpoint analysis on NetScaler Gateway. To configure endpoint analysis, create a session policy that enables the ICA proxy setting and then configure a client security string.

When the user logs on, the endpoint analysis policy runs a security check of the user device with the client security strings that you configured on NetScaler Gateway.

For example, you want to check for a specific version of Sophos Antivirus. In the expression editor, the client security strings appears as:

```
client.application.av(sophos).version == 10.0.2
```

After you configure the session policy, bind it to a user, group, or virtual server. When users log on, the SmartAccess policy check starts and verifies whether or not the user device has Version 10.0.2 or later of Sophos Antivirus installed.

When the SmartAccess endpoint analysis check is successful, the Web Interface portal appears in case of a clientless session; otherwise, the Access Interface appears.

When you create a session policy for SmartAccess, the session profile does not have any settings configured, which creates a null profile. In this case, NetScaler Gateway uses the Web Interface URL configured globally for SmartAccess.

# Configuring XenApp Policies and Filters

Feb 20, 2014

After you create the session policy on NetScaler Gateway, you configure policies and filters on the computer running XenApp that are applied to users according to the endpoint analysis configuration.

To configure XenApp 6.5 policies and filters

1. On the server running XenApp, click Start > Administrative Tools > Citrix > Citrix XenApp. If prompted, configure and run discovery.
2. In the left pane, expand Citrix Resources > XenApp > farmName, where farmName is the name of the server farm.
3. Click Applications.
4. In the center pane, right-click an application and then click Application properties.
5. In the navigation pane, under Properties, click Advanced > Access control.
6. In the right pane, click Any connection that meets any of the following filters and then click Add.
7. In Access Gateway farm, type the name of the NetScaler Gateway virtual server.
8. In Access Gateway filter, type the name of the endpoint session policy and then click OK.
9. In the Application Properties dialog box, clear Allow all other connections and then click OK.

# To configure a session policy for SmartAccess

Feb 17, 2014

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 the Create Session Policy dialog box, in Name, type a name for the policy, such as ValidEndpoint.
4. In Request Profile, click New and in Name, type a name for the profile, such as Null and then click Create.
5. In the Create Session Policy dialog box, create a client security expression, click Create and then click Close.

The client security expression is used to differentiate between valid and invalid endpoints. You can provide different levels of access to published applications or desktops based on the results of endpoint analysis.

After you create the session policy, bind it either globally or to a virtual server.



# Configuring User Device Mapping on XenApp

Feb 28, 2014

You can use NetScaler Gateway filters that are applied to policies on a computer running XenApp. Filters give users access to XenApp capabilities, such as user device drive mapping, printer mapping, or clipboard mapping based on the results of the endpoint analysis.

Citrix Receiver supports the mapping of devices on user devices so users can access external devices within user sessions. User device mapping provides:

- Access to local drives and ports
- Cut-and-paste data transfer between a user session and the local clipboard
- Audio (system sounds and .wav files) playback from the user session

During logon, the user device informs the server of the available user drives and COM ports. In XenApp 6.5, user drives are mapped to the server and use the user device drive letter. These mappings are available only for the current user during the current session. The mappings are deleted when the user logs off and recreated the next time the user logs on.

After enabling the XML Service, you need to configure policies for user device mapping.

To enforce user device mapping policies based on SmartAccess filters, you create the following two policies on the server:

- A restrictive ICA policy that disables user device mapping and applies to all NetScaler Gateway users
  - A full ICA policy that enables user device mapping and applies only to users who fulfill the endpoint analysis session policy
- Note: The filtered non-restrictive ICA policy must be given a higher priority than the restrictive ICA policy, so that when it applies to a user, the non-restrictive policy overrides the policy that disables user device mapping.

You configure restrictive and non-restrictive policies on XenApp 6.5 by using Citrix AppCenter.

# To configure a restrictive policy on XenApp 6.5

Feb 20, 2014

1. Click Start > Administrative Tools > Management Consoles > Citrix AppCenter.
2. In the left pane, expand XenApp, expand the server and then click Policies.
3. In the Policies pane, click the User tab and then click New.
4. In Name, type a name for the policy and then click Next.
5. Under Categories, click All Settings.
6. Under Settings, in Auto connect client drives, click Add.
7. In the Add Setting dialog box, click Disabled, click OK and then click Next.
8. Under Categories, click All Filters.
9. Under Filters, in Access Control, click Add.
10. In the New Filter dialog box, click Add.
11. In Mode, click Deny.
12. In Connection Type, select With Access Gateway.
13. In AG Farm, type the virtual server name.
14. In Access Condition, type or select the session policy name that is configured on NetScaler Gateway, click OK two times, click Next and then click Create to complete the wizard.

# To configure a non-restrictive policy on XenApp 6.5

Feb 20, 2014

1. Click Start > Administrative Tools > Management Consoles > Citrix AppCenter.
2. In the left pane, expand XenApp, expand the server and then click Policies.
3. In the Policies pane, click the User tab and then click New.
4. In Name, type a name for the policy and then click Next.
5. Under Categories, click All Settings.
6. Under Settings, in Auto connect client drives, click Add.
7. Click Enabled, click OK and then click Next.
8. Under Categories, click All Filters.
9. Under Filters, in Access Control, click Add.
10. In the New Filter dialog box, click Add.
11. In Mode, click Allow.
12. In Connection Type, select With Access Gateway.
13. In AG Farm, type the virtual server name.
14. In Access Condition, type or select the session policy name that is configured on NetScaler Gateway, click OK two times, click Next and then click Create to complete the wizard.

# Enabling XenApp as a Quarantine Access Method

May 14, 2013

If you have endpoint analysis configured on NetScaler Gateway, users who pass an endpoint scan can access all the resources that you configure on NetScaler Gateway. You can put users who fail an endpoint scan in a quarantine group. These users can access published applications from XenApp only. Success or failure of the endpoint analysis scan determines the access method available to users.

For example, you create an endpoint analysis scan to check whether or not Notepad is running on the user device when users log on. If Notepad is running, users can log on using the NetScaler Gateway Plug-in. If Notepad is not running, users receive only the list of published applications.

To configure restricted user access, create a quarantine group on NetScaler Gateway. You create the quarantine group within a session profile and then add the profile to a session policy.

# Creating a Session Policy and Endpoint Analysis Scan for a Quarantine Group

Feb 17, 2014

To enable XenApp as a quarantine access method, create a group on NetScaler Gateway that you use as the quarantine group. Then, create a session policy where you select the group.

After you create the session policy, bind the policy to the quarantine group. After you configure the policies and bind them to the group, test the results. For example, for users to successfully log on, Notepad must be running on the user device. If Notepad is running, users can log on by using the NetScaler Gateway Plug-in. If Notepad is not running, users can log on with Citrix Receiver.

For more information about configuring endpoint analysis policies, see [Configuring Endpoint Polices](#).

To create an endpoint analysis scan and add a quarantine 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, on the Policies tab, click Add.
3. In the Create Session Policy dialog box, in Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In the Create Session Profile dialog box, in Name, type a name for the profile.
6. On the Security tab, click Advanced.
7. In the Security Settings - Advanced dialog box, under Client Security, click Override Global and then click New.
8. In the Create Expression dialog box, next to Match Any Expression, click Add.
9. In Expression Type, select Client Security.
10. In Component, select Process.
11. In Name, type notepad.exe, click OK and then click Create.
12. In the Security Settings - Advanced dialog box, in Quarantine Group, select the quarantine group, click Create, click OK and then click Create.
13. In the Create Session Policy dialog box, next to Named Expressions, select True value, click Add Expression, click Create and then click Close.

# Configuring XenDesktop for SmartAccess

May 28, 2013

NetScaler Gateway enables XenDesktop to deliver secure desktops to remote users. XenDesktop can use the SmartAccess capabilities of NetScaler Gateway to intelligently deliver desktops. When you use the Delivery Services Console in XenDesktop to create desktop groups, you then configure policies and filters for access control.

To configure NetScaler Gateway to deliver published desktops, you use the same options that are available with the Web Interface, ICA proxy access, clientless access, and NetScaler Gateway access.

When you create a session policy and configure settings on the Published Applications tab, use the web address for the XenDesktop Web Interface site. After you create the policy, bind it to a virtual server. Then, create a null session profile in which you do not configure settings. The Web Interface configuration is inherited from global settings.

# To configure a session policy for SmartAccess with XenDesktop

Feb 17, 2014

You configure SmartAccess on NetScaler Gateway to access XenDesktop by creating a session policy bound to a virtual server.

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 the Create Session Policy dialog box, in Name, type a name for the policy, such as XenDesktopPolicy.
4. In Request Profile, click New.
5. In the Create Session Profile dialog box, in Name, type a name for the profile, such as XenDesktopProfile.
6. On the Published Applications tab, next to ICA Proxy, click Override Global and then select ON.
7. In Web Interface Address, click Override Global and then type the URL to the XenDesktop Web Interface site.
8. In Single Sign-on Domain, click Override Global, type the domain name and then click Create.
9. In the Create Session Policy dialog box, next to Named Expressions, select True Value, click Add Expression, click Create and then click Close.

You also need to create a null session policy which is bound to the virtual server. The session profile does not contain any configuration, making it a null profile. In the session policy, add the True Value expression and then save the policy.

After you create both session policies, bind both policies to the virtual server.

# To configure policies and filters in XenDesktop 5

May 14, 2013

You can configure settings in XenDesktop 5 by using either the Desktop Studio or the Group Policy Editor. When you configure NetScaler Gateway settings in XenDesktop, use the NetScaler Gateway virtual server name and the session policy name. Then, configure access control to allow connections to meet defined filters. You can also use SmartAccess policies.

1. On the XenDesktop server, click Start > All Programs > Citrix > Desktop Studio.
2. In the left pane, click to expand HDX Policy and then click the User tab in the middle pane.
3. Under Users, click New.
4. In the New Policy dialog box, under Identify your policy and then in Name, type a name.
5. Click Next twice.
6. In the New Policy dialog box, on the filters tab, under Filters, click Access Control and then click Add.
7. In the New Filter dialog box, click Add.
8. In the New Filter Element dialog box, in Connection Type, select With Access Gateway.  
To apply the policy to connections made through NetScaler Gateway without considering NetScaler Gateway policies, leave the default entries in AG farm name and Access condition.
9. If you want to apply the policy to connections made through NetScaler Gateway based on existing NetScaler Gateway policies, do the following:
  1. In AG farm name, type the virtual server name.
  2. In Access condition, type the name of the endpoint analysis policy or session policy.Important: XenDesktop does not validate the NetScaler Gateway virtual server, endpoint analysis policy, or session policy names. Make sure the information is correct.
10. Click OK twice, click Next and then click Create.



# To add the Desktop Delivery Controller as the STA

Feb 17, 2014

To establish ICA connections with XenDesktop, you add the IP address of the Desktop Delivery Controller to the virtual server as the Secure Ticket Authority (STA).

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 Published Applications tab, under Secure Ticket Authority, click Add.
4. In the Configure STA Server dialog box, enter the URL of the STA server, and then click Create.
5. Repeat Step 4 to add additional STA servers and then click OK in the Configure NetScaler Gateway Virtual Server dialog box.

# Configuring SmartControl

Jul 14, 2015

## Overview

Smart Control allows administrators to define granular policies to configure and enforce user environment attributes for XenApp and XenDesktop on NetScaler Gateway. Smart Control allows administrators to manage these policies from a single location, rather than at each instance of these server types.

Smart Control 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.

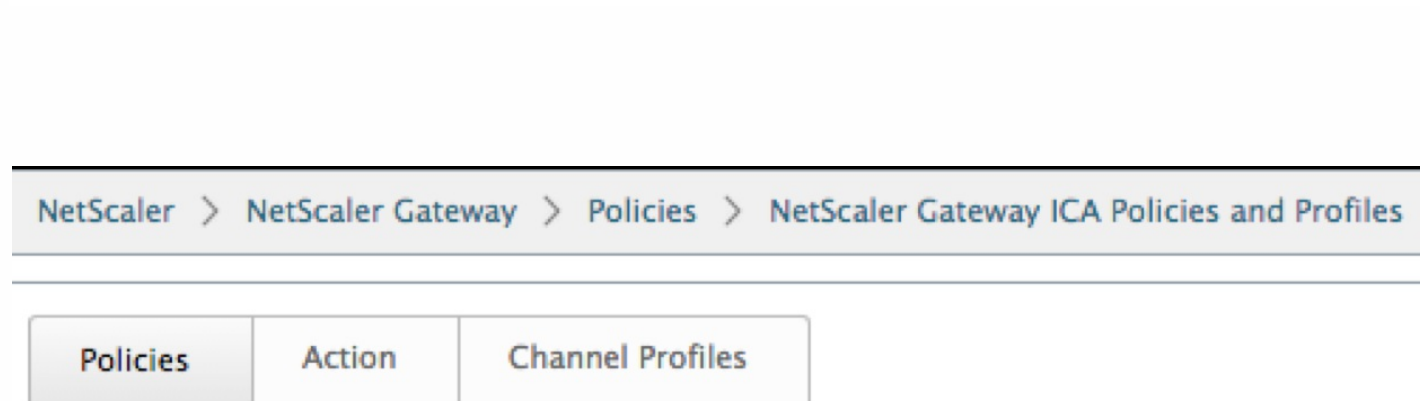
The following table lists the user environment attributes that Smart Control can enforce:

|                            |   |
|----------------------------|---|
| 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. These 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 receiver.   |
| ClientPrinterRedirection   | Specifies the client printers to be mapped to a server when a user logs on to a session.                                      |

## Smart Control Operations

Smart Control operates using the following three tabs:

- [Policies](#)
- [Action](#)
- [Access Profiles](#)



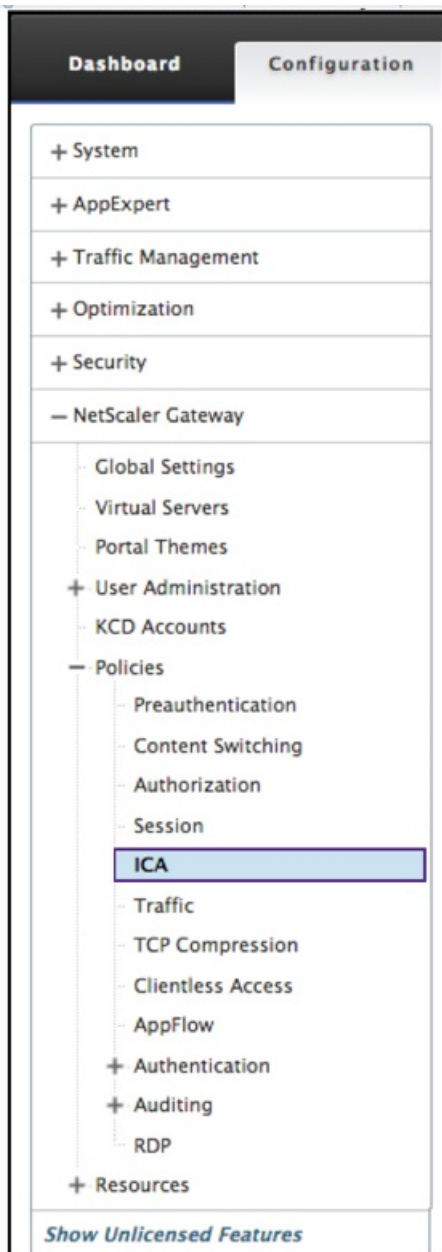
## Policies

An ICA policy specifies an Action, Access Profile, Expression and optionally, a Log Action. The following commands are available from the Policies tab:

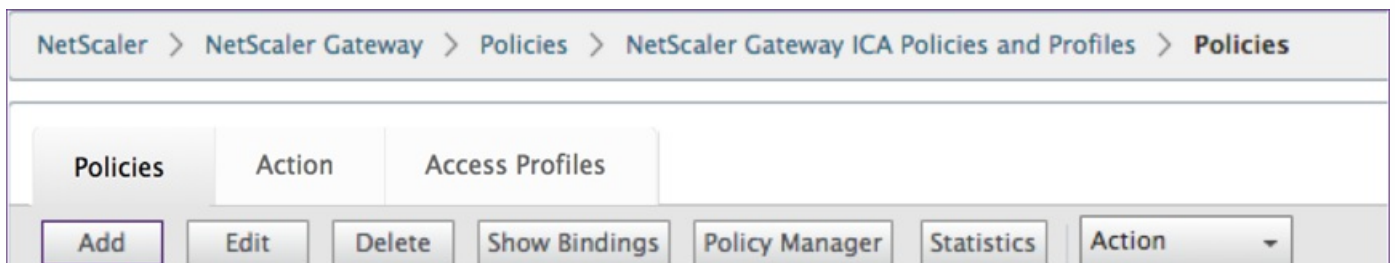
- [Add](#)
- [Edit](#)
- [Delete](#)
- [Show Bindings](#)
- [Policy Manager](#)
- [Action](#)

### Add

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.



2. In the details pane, on the Policies tab, click **Add**.



3. The following screen appears. In the **Name** dialog box, type a name for the policy. This is a required field. All required fields are indicated by an asterisk.

← Back

### Create Policy

Name\*  (3)

Action\*  > + ✎ (4)

Expression\* Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

Press Control+Space to start the expression and then type '.' to get the next set of options (5)

Evaluate

Log Action  ⌵ + ✎ ? (6)

Comments  (7)

Create Close (8)

4. Next to Action do one of the following:

- Click the > icon to select an existing action. For details see [Select an action](#).
- Click the + icon to create a new action. For details see [Create a new action](#).
- The **pencil** icon is disabled.

5. Create an expression. For details see [Expressions](#).

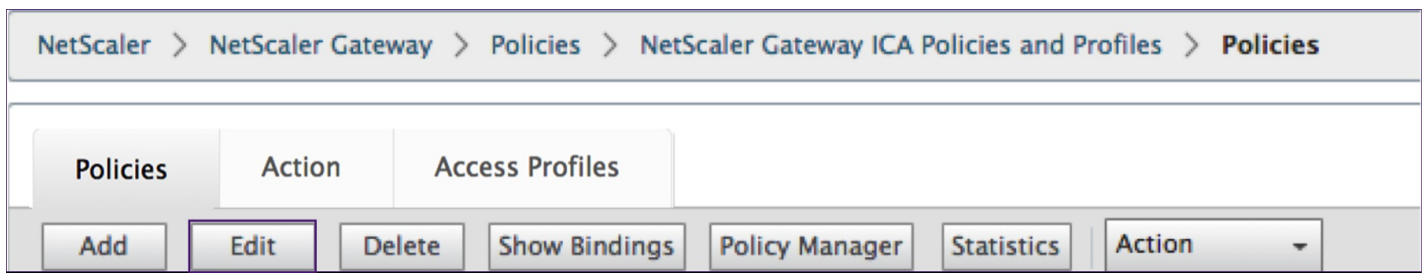
6. Create a **Log Action**. For more details see [Create a Log Action](#).

7. Enter a message into the Comments box. The comment writes to the message log. This field is optional.

8. Click **Create**.

### Edit

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.
2. Select the ICA policy from the list.
3. In the details pane, on the Policies tab, click **Edit**.



4. Verify the policy name.

**Configure Policy**

Name  
policy\_2 (4)

Action\*  
Action\_7 (5)

Expression\*  
CLIENT.TCP.DSTPORT.EQ(2) (6)

Log Action  
AuditMessage1 (7)

Comments  
Watch for unauthorized connections! (8)

OK Close (9)

5. To revise the **Action** do one of the following:

- Click the > icon to revise an existing **Action**. For detail see [Select an action](#).
- Click the + icon to create a new **Action**. For detail see [Create a new action](#).
- Click the pencil icon to revise the [Access Profile](#).

6. Revise the **Expression** as desired. For details see [Expressions](#).

7. To revise the **Log Action** do one of the following:

- Click the + icon to create a new **Log Action**. For details see [Create a Log Action](#).
- Click the pencil icon to configure an Audit Message. For details see [Configure Audit Message Action](#).

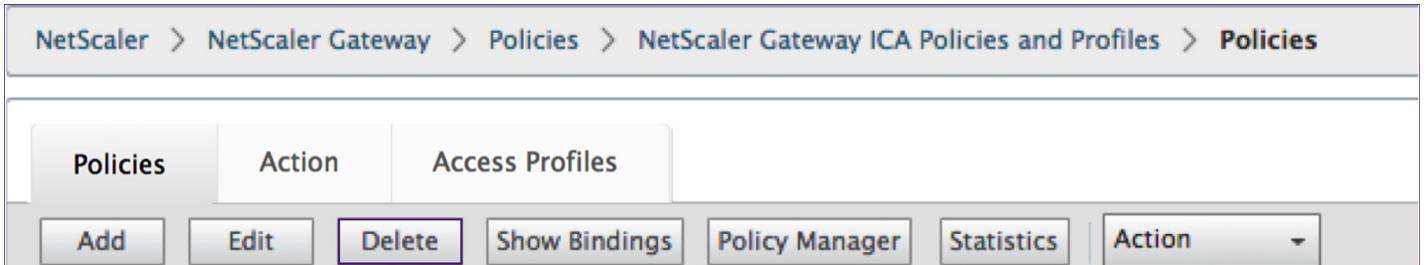
8. Revise the comments as desired.

9. Click **OK**.

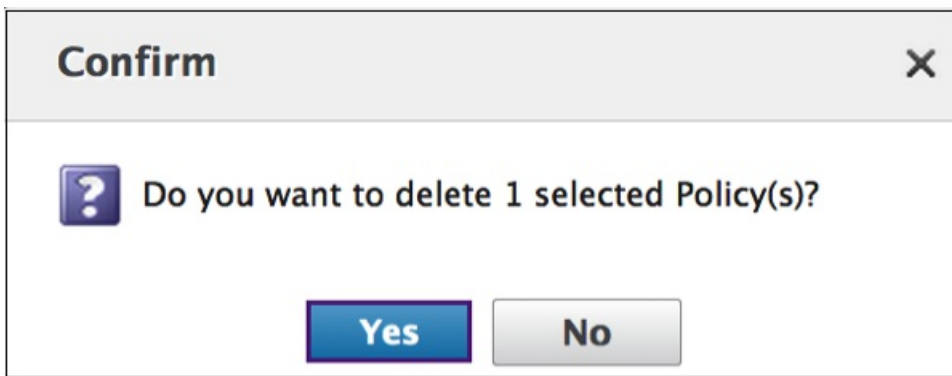
Delete

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.
2. Select the desired ICA policy from the list.

In the details pane, on the Policies tab, click **Delete**.

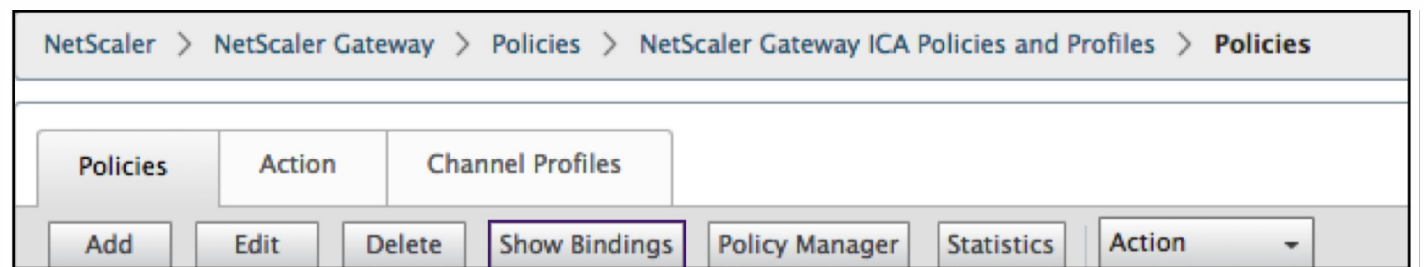


4. Confirm that you want to delete the policy by clicking **Yes**.



### Show Binding

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.
2. Select the ICA policy from the list.
3. In the details pane, on the Policies tab, click **Show Bindings**.



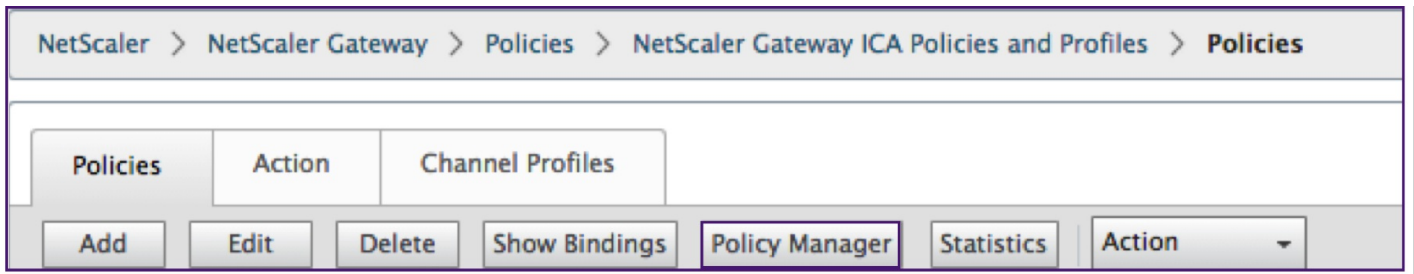
### Policy Manager

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and

then click ICA.

2. Select the desired ICA policy from the list.

3. In the details pane, on the Policies tab, click **Policy Manager**



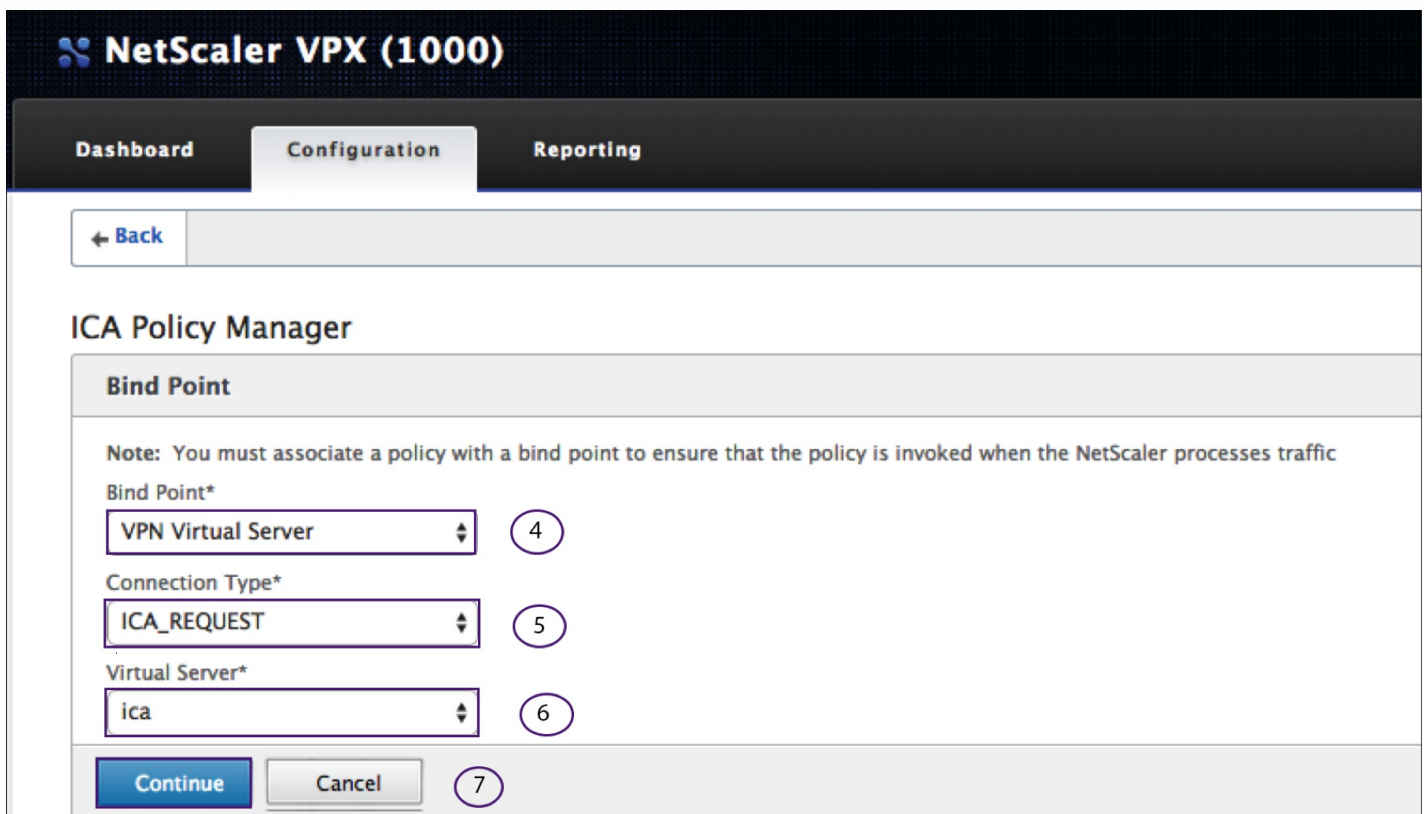
4. From the Bind Point dialog box, select a policy from the drop down menu. These are the following choices:

- Override Global
- VPN Virtual Server
- Cache Redirection Virtual Server
- Default Global

5. From the Connection Type dialog box, select a binding policy from the drop down menu.

6. If you select either the VPN Virtual Server or the Cache Redirection Virtual Server, you connect to the server using the drop down box.

7. Click **Continue**.





## Add Binding

1. After selecting Continue, this screen appears.
2. Select a Policy to attach the Binding.
3. Select Add Binding.

### ICA Policy Manager

**Bind Point** ✎

Bind Point **Override Global**      Connection Type **ICA\_REQUEST**

**Add Binding**   **Unbind**   **Bind NOPOLICY**   **Edit** ▾      Search ▾

| Priority | Policy Name | Expression                         | Action   | Goto Expression |
|----------|-------------|------------------------------------|----------|-----------------|
| ▶ 10     | Policy_5    | HTTP.REQ.USER.NAME.CONTAINS("g,t") | Action_5 | END             |
| ▶ 100    | policy_2    | CLIENT.TCP.DSTPORT.EQ(2)           | Action_7 | END             |
| ▶ 120    | Policy_3    | HTTP.REQ.USER.NAME.CONTAINS("w")   | Action_2 | NEXT            |
| ▶ 130    | Policy_4    | HTTP.REQ.USER.NAME.CONTAINS("4H")  | Action_5 | NEXT            |
| ▶ 140    | Policy_6    | HTTP.REQ.USER.NAME.CONTAINS("k")   | Action_7 | END             |
| ▶ 150    | Policy_7    | CLIENT.IP.DST.EQ(77)               | Action_2 | END             |

**Done**

## Policy Binding

1. After selecting Done, this screen appears.
  - Click the > icon to select an existing policy. For detail see [Select an existing policy](#).
  - Click the + con to create a new policy. For detail see [Create a new policy](#).
  - The **pencil** icon is disabled for this screen.

## Policy Binding

### Policy Binding

Select Policy\*

Click to select > + ✎

### Binding Details

Priority\*

120 ?

Goto Expression\*

NEXT ?

**Bind** Close

## Unbind Policy

1. Select the policy you want to unbind, and click the **Unbind** button.

### ICA Policy Manager

| Priority | Policy Name | Expression                              | Action      | Goto Expression |
|----------|-------------|---|-------------|-----------------|
| ▶ 120    | ica_pol5    | HTTP.REQ.USER.IS_MEMBER_OF("group1")    | ica_act5    | END             |
| ▶ 140    | ica_pol6    | client.IP.DST.BETWEEN(1.1.1.1, 1.2.1.2) | ica_trois_B | END             |
| ▶ 150    | ica_pol4    | client.TCP.DSTPORT.EQ(7)                | ica_act4    | END             |
| ▶ 160    | unus        | HTTP.REQ.USER.IS_MEMBER_OF("floor")     | ica_act1    | NEXT            |

2. Click **Done**
3. Click the **Yes** button on the pop-up screen to confirm that you desire to unbind the selected entity.



## Bind NOPOLICY

1. Select policy that requires NOPOLICY, and click the **Bind NOPOLICY** button.

ICA Policy Manager

Bind Point **Override Global** Connection Type **ICA\_REQUEST**

Add Binding Unbind **Bind NOPOLICY** Edit

| Priority | Policy Name | Expression                              | Action      | Goto Expression |
|----------|-------------|---|-------------|-----------------|
| ▶ 120    | ica_pol5    | HTTP.REQ.USER.IS_MEMBER_OF("group1")    | ica_act5    | END             |
| ▶ 140    | ica_pol6    | client.IP.DST.BETWEEN(1.1.1.1, 1.2.1.2) | ica_trois_B | END             |
| ▶ 150    | ica_pol4    | client.TCP.DSTPORT.EQ(7)                | ica_act4    | END             |
| ▶ 160    | unus        | HTTP.REQ.USER.IS_MEMBER_OF("floor")     | ica_act1    | NEXT            |

Done

2. Click **Done**

## Edit

You can edit from the ICA Policy Manager.

1. Select the policy you want to edit, and select **Edit**.

## ICA Policy Manager

The screenshot shows the ICA Policy Manager interface. At the top, there's a 'Bind Point' section with 'Override Global' selected and 'ICA\_REQUEST' as the connection type. Below this are buttons for 'Add Binding', 'Unbind', 'Bind NOPOLICY', and 'Edit'. A search bar is on the right. The main table has columns for Priority, Policy Name, Expression, Action, and Goto Expression. The row for 'policy5' is highlighted. A 'Done' button is at the bottom left.

| Priority | Policy Name | Expression                          | Action   | Goto Expression |
|----------|-------------|-------------------------------------|----------|-----------------|
| ▶ 100    | policy1     | CLIENT.IP.SRC.EQ(9)                 | action1  | END             |
| ▶ 120    | policy2     | CLIENT.IP.SRC.EQ(12)                | action2  | END             |
| ▶ 150    | policy5     | HTTP.REQ.USER.IS_MEMBER_OF("list")  | Action_5 | END             |
| ▶ 160    | policy3     | HTTP.REQ.USER.IS_MEMBER_OF("Table") | action3  | END             |

2. You have the option to make the following edits: [Edit Binding](#), [Edit Policy](#), [Edit Action](#).

The screenshot shows the ICA Policy Manager interface with a context menu open over the 'Policy\_5' row. The menu options are 'Select Action', 'Edit Binding', 'Edit Policy', and 'Edit Action'. The table has columns for Priority, Policy Name, Expression, Action, and Goto Expression. The 'Policy\_5' row is highlighted. A 'Done' button is at the bottom left.

| Priority | Policy Name | Expression                         | Action   | Goto Expression |
|----------|-------------|------------------------------------|----------|-----------------|
| ▶ 10     | Policy_5    | HTTP.REQ.USER.NAME.CONTAINS("g.t") | Action_5 | END             |
| ▶ 100    | policy_2    | CLIENT.TCP.DSTPORT.EQ(2)           | Action_7 | END             |
| ▶ 120    | Policy_3    | HTTP.REQ.USER.NAME.CONTAINS("w")   | Action_2 | NEXT            |
| ▶ 130    | Policy_4    | HTTP.REQ.USER.NAME.CONTAINS("4H")  | Action_5 | NEXT            |
| ▶ 140    | Policy_6    | HTTP.REQ.USER.NAME.CONTAINS("k")   | Action_7 | END             |
| ▶ 150    | Policy_7    | CLIENT.IP.DST.EQ(77)               | Action_2 | END             |

For more information see [Edit Binding](#), [Edit Policy](#), [Edit Action](#).

## Edit Binding

- 1.. With the policy selected, click **Edit Binding**.
2. Verify that you are editing the desired policy. This Policy Name is not editable.

**Policy Binding**

**Policy Binding**

Policy Name  
ica\_pol8

► More

**Binding Details**

Priority\*  
110

Goto Expression\*  
END

Bind Close

3. Set the Priority as desired.
4. Set Goto Expression as desired.
5. Click the **Bind** button.

## Edit Policy

1. With the policy selected, click **Edit Policy**.
2. Verify the policy Name to ensure you are editing the desired policy. This field is not editable.

**Configure Policy**

Name  
policy2

Action\*  
action2

Expression\* Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

CLIENT.IP.SRC.EQ(12) Evaluate

Log Action  
message

Comments  
Inspect the IP Source!

OK Close

3. To revise the Action policy, do one of the following:

- Click the > icon to select an existing Action. For details see [Select an action](#).
- Click the + icon to create an action. For details see [Create a new action](#).
- Click the **pencil** icon to revise the Access Profile. For details see [Select an existing Access Profile](#).

4. Revise the Expression as desired. For more details see [Expressions](#).

5. Select the desired type of message from the drop down menu. To create a Log Action, do one of the following:

- Click the + icon to create an action. For details see [Create a Log Action](#).
- Click the **pencil** icon to revise the Configure Audit Message Action. For details see [Configure Audit Message Action](#).

6. Enter Comments about the ICA Policy.

7. Click **OK** when the edit is complete.

## Edit Action

1. With the policy selected, click **Edit Action**.

2. Verify the Action Name to confirm you are editing the desired Action. This field is not editable.

3. Next to Access Profile do one of the following:

- Click the > icon to select a different Access Profile. For detail see [Configure Action](#).
- Click the + icon to select a new Channel Profile. [Create a Access Profile](#).
- Click the pencil icon to revise the Access Profile. For details see [Select an existing Access Profile](#).

4. Click **OK**.

**Configure Action**

Name  
Action\_1 ②

Access Profile\*  
Profile1 > + ✎ ③

④  
OK Close

## Action

The Policies>Action commands are used to rename the action.

1. Select the desired ICA Action from the list.
2. On the ICA Policies tab, click Action. Select Rename from the drop-down menu.

| Name     | Action   | Expression                         | Hits | Active |
|----------|----------|------------------------------------|------|--------|
| policy_1 | Action_1 | CLIENT.TCP.DSTPORT.EQ(1)           | 0    | ✓      |
| policy_2 | Action_7 | CLIENT.TCP.DSTPORT.EQ(2)           | 0    | ✓      |
| Policy_3 | Action_2 | HTTP.REQ.USER.NAME.CONTAINS("w")   | 0    | ✓      |
| Policy_4 | Action_5 | HTTP.REQ.USER.NAME.CONTAINS("4H")  | 0    | ✓      |
| Policy_5 | Action_5 | HTTP.REQ.USER.NAME.CONTAINS("g.t") | 0    | ✓      |
| Policy_6 | Action_7 | HTTP.REQ.USER.NAME.CONTAINS("k")   | 0    | ✓      |
| Policy_7 | Action_2 | CLIENT.IP.DST.EQ(77)               | 0    | ✓      |

3. Rename the action.

← Back

**Rename Action**

Name\*

ica\_action20

OK Close

4. Click **OK**

## Action

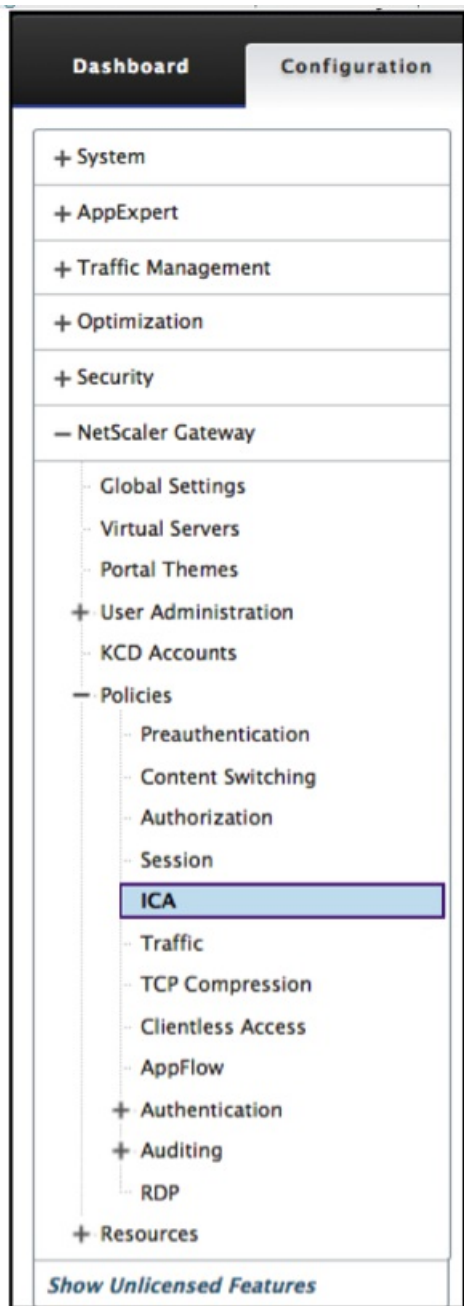
An Action connects a policy with an Access Profile. The following commands are available from the Policies tab:

- [Add](#)
- [Edit](#)
- [Delete](#)
- [Action](#)

### Add

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.





2. In the details pane, on the Action tab, click **Add**.

NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Action

Policies | Action | Access Profiles

Add | Edit | Delete | Action | Search

| Name     | Access Profile |
|----------|----------------|
| action1  | Profile1       |
| action2  | Profile2       |
| action3  | Profile1       |
| action7  | Profile1       |
| Action_5 | Profile1       |
| Action_4 | Profile_X      |
| Action9  | Profile9       |

3. In Name, type a name for the **Action**.

4. Next to Access Profile do one of the following:

- Click the > icon to select an existing Access Profile. For detail see [Select an existing Access Profile](#).
- Click the + icon to create a new Access Profile. For detail see [Create a Access Profile](#).
- The pencil icon is disabled for this screen.

5. Click **Create**.

**Create Action**

Name\*  ③

Access Profile\*  > + ✎ ④

⑤

Edit

1. Select the desired ICA policy from the list.

NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Action

Policies | **Action** | Access Profiles

Add | **Edit** | Delete | Action ▾ | Search ▾

| Name     | Access Profile |
|----------|----------------|
| action1  | Profile1       |
| action2  | Profile2       |
| action3  | Profile1       |
| action7  | Profile1       |
| Action_5 | Profile1       |
| Action_4 | Profile_X      |
| Action9  | Profile9       |

2. In the details pane, on the Action tab, click **Edit**.

## Configure Action

3. Verify the Action Name to confirm you are editing the desired Action. This field is not editable.

4. Next to Access Profile do one of the following:

- Click the > to select an existing Access Profile. For detail see [Select an existing Access Profile](#).
- Click the + to create a new Access Profile. For detail see [Create a Access Profile](#).
- Click the pencil icon to [Configure Access Profile](#).

5. Click **OK**.

### Configure Action

Name

Action\_1

3

Access Profile\*

Profile1

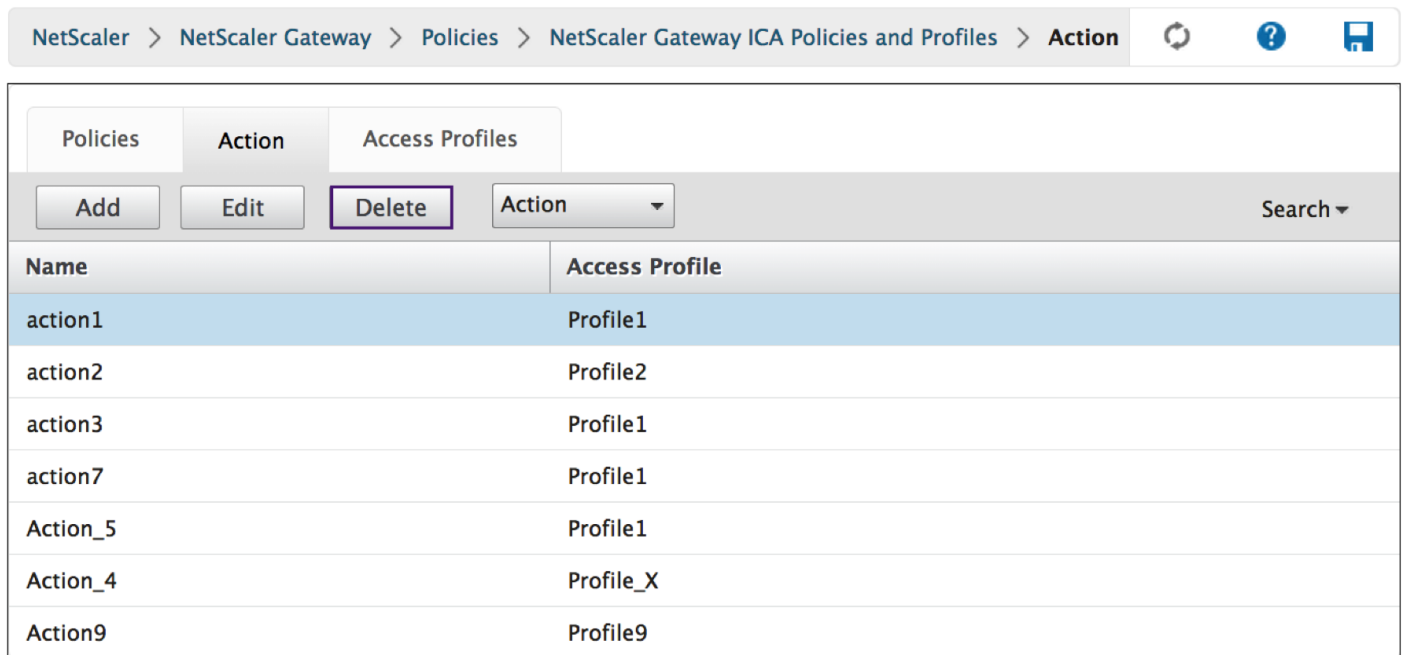
>
+
✎

4

5
OK
Close

## Delete

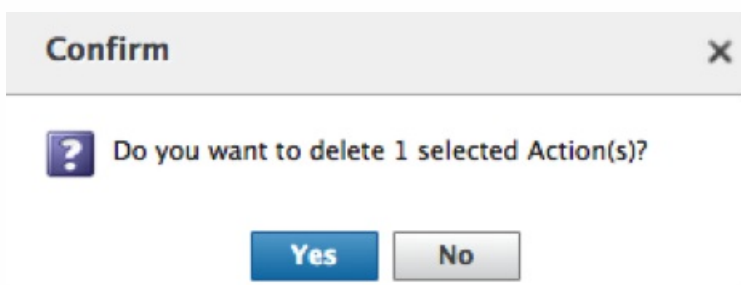
1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Action and then click ICA.
2. Select the desired ICA Action from the list.
3. In the details pane, on the Action tab, click Delete.



The screenshot shows the NetScaler configuration utility interface. The breadcrumb navigation is: NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Action. The interface has three tabs: Policies, Action (selected), and Access Profiles. Below the tabs are buttons for Add, Edit, Delete (highlighted with a purple border), and an Action dropdown menu. A search field is on the right. Below these is a table with two columns: Name and Access Profile.

| Name     | Access Profile |
|----------|----------------|
| action1  | Profile1       |
| action2  | Profile2       |
| action3  | Profile1       |
| action7  | Profile1       |
| Action_5 | Profile1       |
| Action_4 | Profile_X      |
| Action9  | Profile9       |

4. Confirm the Action you want to delete the policy by clicking **Yes**.



The screenshot shows a 'Confirm' dialog box with a close button (X) in the top right corner. The main text reads: '? Do you want to delete 1 selected Action(s)?'. At the bottom, there are two buttons: 'Yes' (highlighted in blue) and 'No'.

## Action

The ICA Action>Action commands are used to rename the action.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Action and then click ICA.
2. Select the desired ICA Action from the list.
3. In the details pane, on the Action tab, click **Action**.

| ICA Policies |                           | ICA Action   | Access Profiles |
|--------------|---------------------------|--|-----------------|
| Add          |                           | Edit   | Delete          |
|              |                           | Action <span style="border: 1px solid black; border-radius: 50%; padding: 2px;">3</span> |                 |
| Name         | ICA Access Profile        |  |                 |
| Action_1     | default_ica_accessprofile |  |                 |
| Action_2     | Profile_2                 |  |                 |
| Action_3     | Profile_4                 | <span style="border: 1px solid black; border-radius: 50%; padding: 2px;">2</span>        |                 |
| Action_7     | Profile_7                 |  |                 |
| Action_5     | Profile_5                 |  |                 |

4. Select Action>Rename from the drop-down menu.

5. Rename the action.

← Back

**Rename Action**

Name\*

OK
Close

6. Click **OK**

## Access Profiles

An ICA profile defines the settings for user connections.

Access profiles specify the actions that are applied to a user's XenApp or XenDesktop environment ICA if the user device

meets the policy expression conditions. You can use the configuration utility 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 independently of 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. The following commands are available from the Policies tab:

- [Add](#)
- [Edit](#)
- [Delete](#)

### Creating an Access Profile with the configuration utility

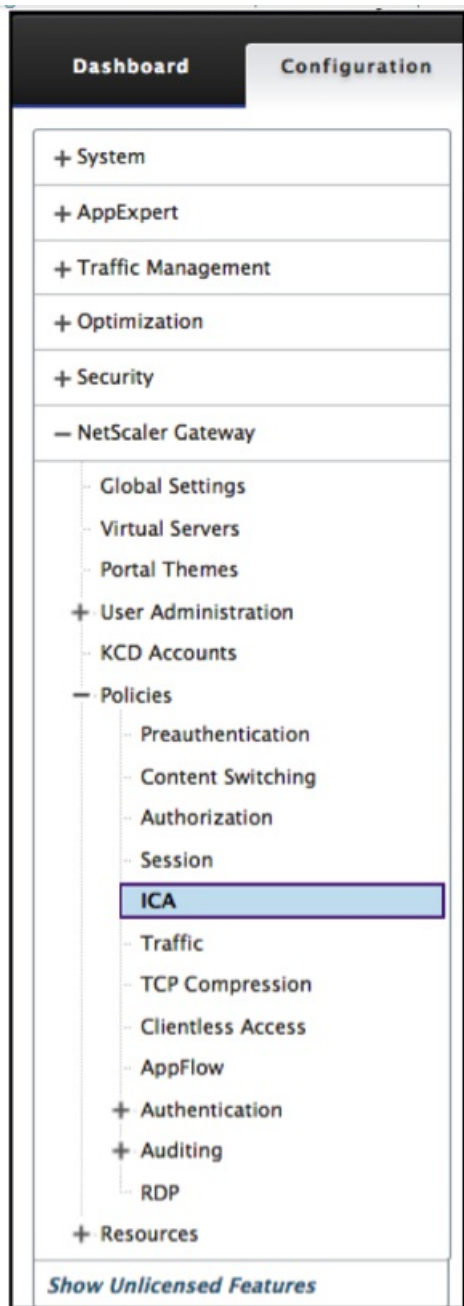
1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.
2. In the details pane, click the Access Profiles tab and then click Add.
3. Configure the settings for the profile, click Create and then click Close. After you create a profile, you can include it in an ICA policy.

### Add an Access Profile to a policy using the configuration utility

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.
2. On the Policies tab, do one of the following:
  - o Click Add to create a new ICA policy.
  - o Select a policy and then click Open.
3. In Action menu, select an Access Profile from the list.
4. Finish configuring the ICA 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.

### Add

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click ICA.



2. In the details pane, on the Access Profiles tab, click **Add**.

NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Access Profiles

| Access Profiles           |                          |                          |                              |
|---------------------------|--------------------------|--------------------------|------------------------------|
| Name                      | Connect Client LPT Ports | Client Audio Redirection | Client Clipboard Redirection |
| default_ica_accessprofile | DISABLED                 | DISABLED                 | DISABLED                     |
| Profile1                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |
| Profile2                  | DEFAULT                  | DEFAULT                  | DISABLED                     |
| Profile7                  | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile_X                 | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile9                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |

3. In Name, type a name for the Access Profile. This is a required field.

Dashboard Configuration Reporting Documentation Downloads

← Back

### Create Access Profile

Name\*

|   |  |
|---|--|
| <p>Connect Client LPT Ports<br/>Default</p> <p>Client Audio Redirection<br/>Default</p> <p>Local - Remote Data Sharing<br/>Default</p> <p>Client Clipboard Redirection<br/>Default</p> <p>Client COM Port Redirection<br/>Default</p> | <p>Client Drive Redirection<br/>Default</p> <p>Client Printer Redirection<br/>Default</p> <p>Multistream<br/>Default</p> <p>Client USB Drive Redirection<br/>Default</p> |
|---|--|

Create Close

4. Select Default or Disable from the pull down menus shown to create the Access Profile.

5. Click **Create**.

Edit



1. Select the Access Profile you want to edit.
2. In the details pane, on the Access Profiles tab, click **Edit**.

NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Access Profiles

Policies Action Access Profiles

Add Edit Delete Search

| Name                      | Connect Client LPT Ports | Client Audio Redirection | Client Clipboard Redirection |
|---------------------------|--------------------------|--------------------------|------------------------------|
| default_ica_accessprofile | DISABLED                 | DISABLED                 | DISABLED                     |
| Profile1                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |
| Profile2                  | DEFAULT                  | DEFAULT                  | DISABLED                     |
| Profile7                  | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile_X                 | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile9                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |

## Configure Access Profile

3. Verify that the **Name** is the one you want to revise.

Configure Access Profile

Name **3**

Profile1 **4**

Connect Client LPT Ports: Default

Client Audio Redirection: Default

Local Remote Data Sharing: Default

Client Clipboard Redirection: Default

Client COM Port Redirection: Default

Client Drive Redirection: Default

Client Printer Redirection: Default

Multistream: Default

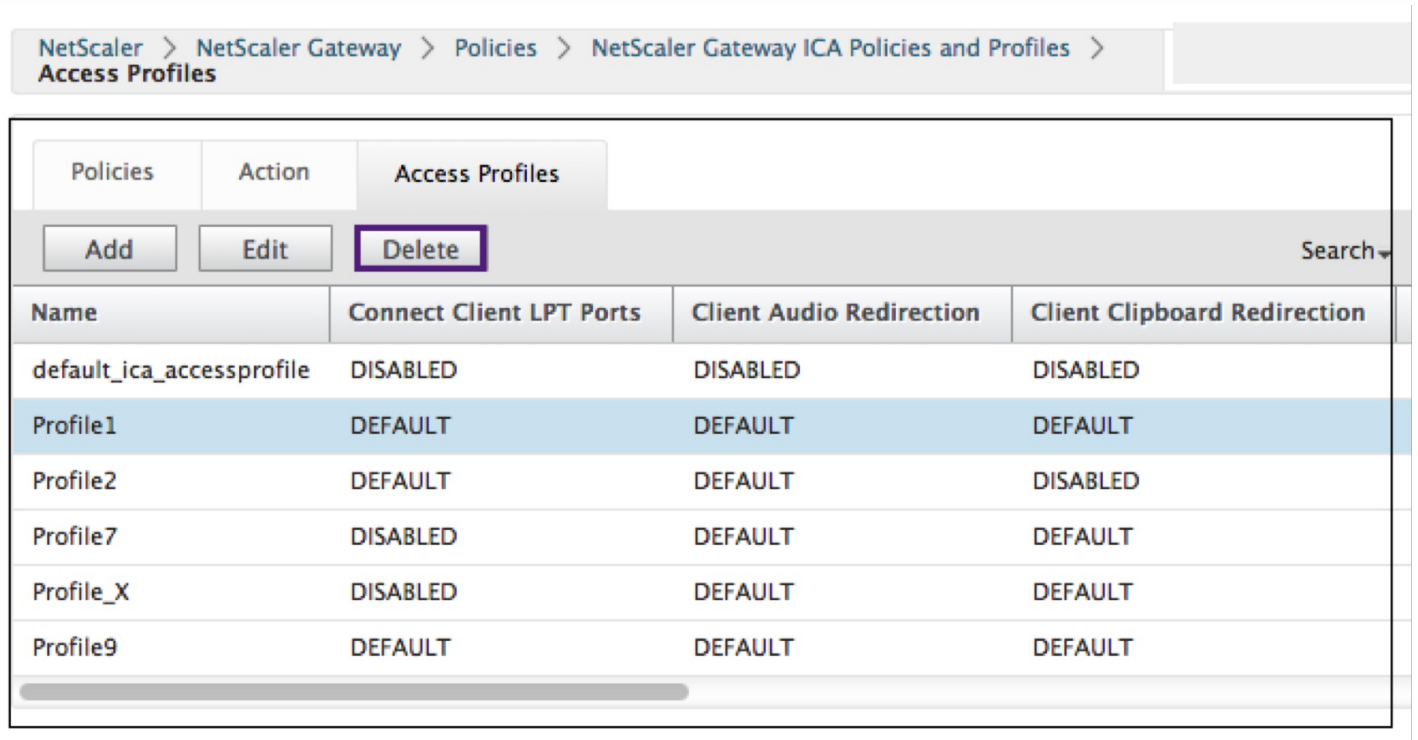
Client USB Drive Redirection: Default

OK Close **5**

4. Select Default or Disable from the pull down menu to configure as required.
5. Click **OK**.

## Delete

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Action and then click ICA.
2. Select the desired ICA Action from the list.
3. In the details pane, on the Action tab, click **Delete**.



NetScaler > NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Access Profiles

Policies Action Access Profiles

Add Edit Delete Search

| Name                      | Connect Client LPT Ports | Client Audio Redirection | Client Clipboard Redirection |
|---------------------------|--------------------------|--------------------------|------------------------------|
| default_ica_accessprofile | DISABLED                 | DISABLED                 | DISABLED                     |
| Profile1                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |
| Profile2                  | DEFAULT                  | DEFAULT                  | DISABLED                     |
| Profile7                  | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile_X                 | DISABLED                 | DEFAULT                  | DEFAULT                      |
| Profile9                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |

4. Confirm the Access Profile you want to delete by clicking **Yes**.

## Common Processes

### Create a new action

1. Type a Name for the Action.
2. Select one of the following to supply the Access Profile:
  - Click the > to select an existing Access Profile. See for details [Select an existing Access Profile](#).
  - Click the + to create a new Access Profile. See for details [Create an Access Profile](#).
  - The **pencil** icon is disabled.

3. Click **Create**.

**Create Action**

Create Action

Name\* 1

Access Profile\* 2

Click to select > + /

**Create** Close 3

Select an action

1. Select an Action by clicking the radio button to the left of it. The associated Access Profile specifies the allowed user functions.
2. Click the **Select** button.

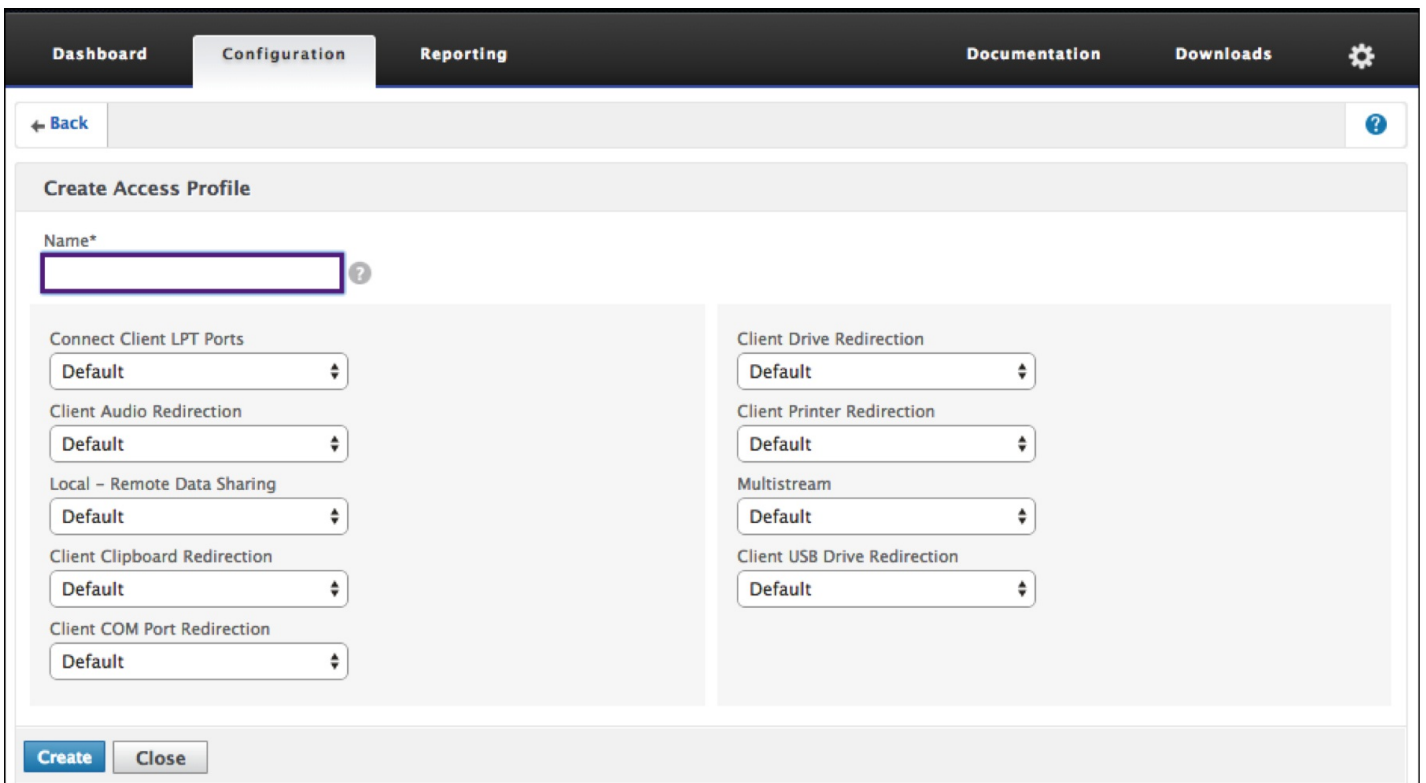
**Action** 1

**Select** Add Edit Delete Action

|   | Name     | Access Profile            |
|---|----------|---------------------------|
| <input type="radio"/>                           | Action_1 | default_ica_accessprofile |
| <input checked="" type="radio"/> <span>2</span> | Action_2 | Profile_2                 |
| <input type="radio"/>                           | Action_3 | Profile_4                 |
| <input type="radio"/>                           | Action_7 | Profile_7                 |
| <input type="radio"/>                           | Action_5 | Profile_5                 |

Create an Access Profile

1. Name the Access Profile.



2. You have the option to configure the Access Profile from this menu.
3. Click **Create**.

Select an existing Access Profile

1. Select an Access Profile by clicking on it.

| Policies                  |                          | Action                   |                              | Access Profiles |  |
|---------------------------|--------------------------|--------------------------|------------------------------|-----------------|--|
| Add                       |                          | Edit                     |                              | Delete          |  |
| Name                      | Connect Client LPT Ports | Client Audio Redirection | Client Clipboard Redirection | Search          |  |
| default_ica_accessprofile | DISABLED                 | DISABLED                 | DISABLED                     |                 |  |
| Profile1                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |                 |  |
| Profile2                  | DEFAULT                  | DEFAULT                  | DISABLED                     |                 |  |
| Profile7                  | DISABLED                 | DEFAULT                  | DEFAULT                      |                 |  |
| Profile_X                 | DISABLED                 | DEFAULT                  | DEFAULT                      |                 |  |
| Profile9                  | DEFAULT                  | DEFAULT                  | DEFAULT                      |                 |  |

2. Click Edit.

3. Configure the Access Profile. For details see [Configure Access Profile](#).

## Expressions

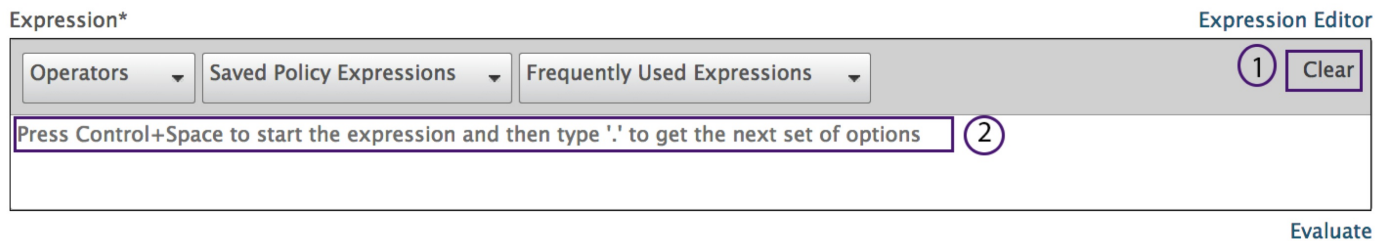
1. To create or revise an existing Expression, select Clear.

These are the typical ICA Expressions. For the HTTP expressions enter the name with the "" and remove the ().

|  |   |
|--|---|
| ICA.SERVER.PORT  | This expression checks that the port specified matches the port number on the XenApp/XenDesktop that the user is attempting to connect. |
| ICA.SERVER.IP  | This expression checks that the IP specified matches the IP address on the XenApp/XenDesktop that the user is attempting to connect.    |
| HTTP.REQ.USER.IS_MEMBER_OF("").NOT   | This expression checks that the current connection is access by a user that is NOT a member of the specified group name.                |
| HTTP.REQ.USER.IS_MEMBER_OF("groupname")  | This expression checks that the user accessing the current connection is a member of the specified group.                               |
| HTTP.REQ.USERNAME.CONTAINS("").NOT   | This expression checks that the user accessing the current connection is NOT a member of the specified group.                           |
| HTTP.REQ.USERNAME.CONTAINS("enter username") Specifies the resources for a username. | This expression checks that the current connection is access by the specified name.   |
| CLIENT.IPDST.EQ(enter ip address here).NOT   | This expression checks that the destination IP of the current traffic is NOT equal to the specified IP address.                         |
| CLIENT.IPDST.EQ(enter ip address here)   | This expression checks that the destination IP of the current traffic is equal to the specified IP address.                             |
| CLIENT.TCPDSTPORT.EQ (enter port number).NOT   | This expression checks that the destination port is NOT equal to the specified port   |

|  |   |
|--|---|
|  | number.   |
| CLIENT.TCPDSTPORT.EQ (enter port number) | This expression checks that the destination port is equal to the specified port number. |

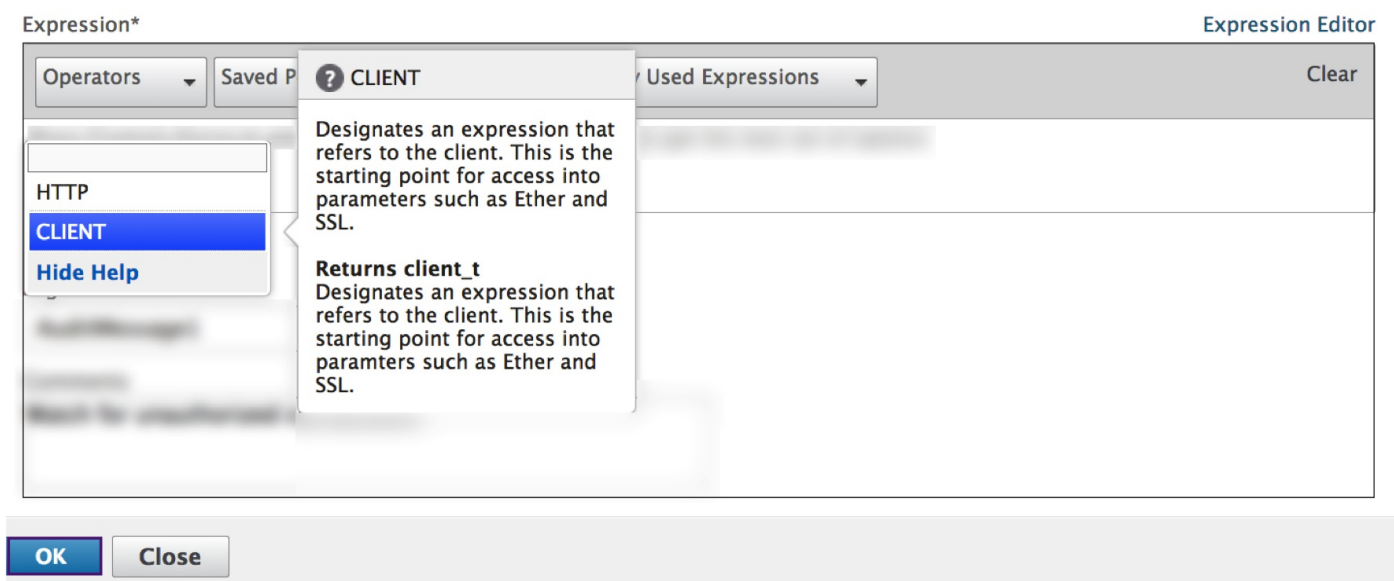
2. Simultaneously, select **Control** and the **Space** bar; then your options are visible.



3. Type the period. Make your selection, and press the **Space** bar.

4. At each period of the expression in the table above, type the period. Make your selection, and press the Space bar.

5. Click **OK**.



## Group Identification

Expression with a groupname variable are defined by the Preauthentic or Session functions.

Preauthentication

1. Select Preauthentication from the configuration pane.



+ System

+ AppExpert

+ Traffic Management

+ Optimization

+ Security

- NetScaler Gateway

Global Settings

Virtual Servers

Portal Themes

+ User Administration

KCD Accounts

- Policies

**Preauthentication**

Content Switching

Authorization

Session

ICA

Traffic

TCP Compression

Clientless Access

AppFlow

+ Authentication

+ Auditing

RDF  
+ Resources



2. Select a name from the Preauthentication Policies.
3. Select **Edit** from the Preauthentication Policies tab.




| Name                 | Expression                                   | Request Action            | Globally Bound? |
|----------------------|--|---------------------------|-----------------|
| SETPREAUTHPARAMS_POL | ns_true                                      | SET_PREAUTHPARAMS_ACT     | ✗               |
| Jedi                 | CLIENT.APPLICATION.AS(FILTER).VERSION == all | Pre-auth_Profile          | ✓               |
| Jedi2                | CLIENT.APPLICATION.AS(FILTER).VERSION == all | Preauthentication_Profile | ✗               |
| Obi                  | CLIENT.APPLICATION.AS(FILTER).VERSION == all | Preauthentication_Profile | ✓               |
| R2D2                 | CLIENT.APPLICATION.AS(AtoZ).VERSION == all   | Sift                      | ✗               |


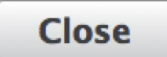
4. Select the **pencil** icon or + next to the Request Action dialoge box.

### Configure Preauthentication Policy

Name  
Jedi

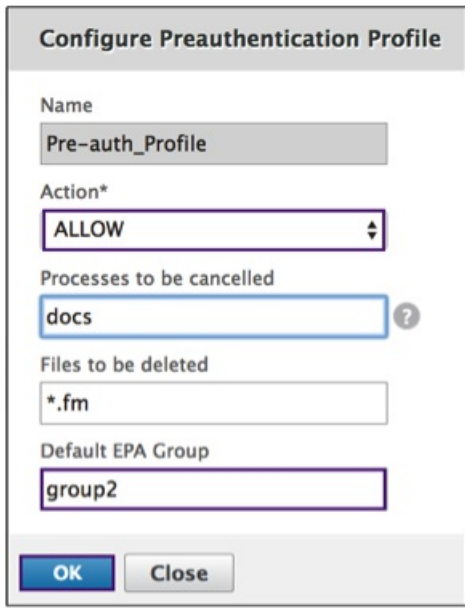
Request Action\*  
Pre-auth\_Profile  

Expression\*  
Operators  Saved Policy Expressions  Frequently Used Expressions   
CLIENT.APPLICATION.AS(FILTER).VERSION == all



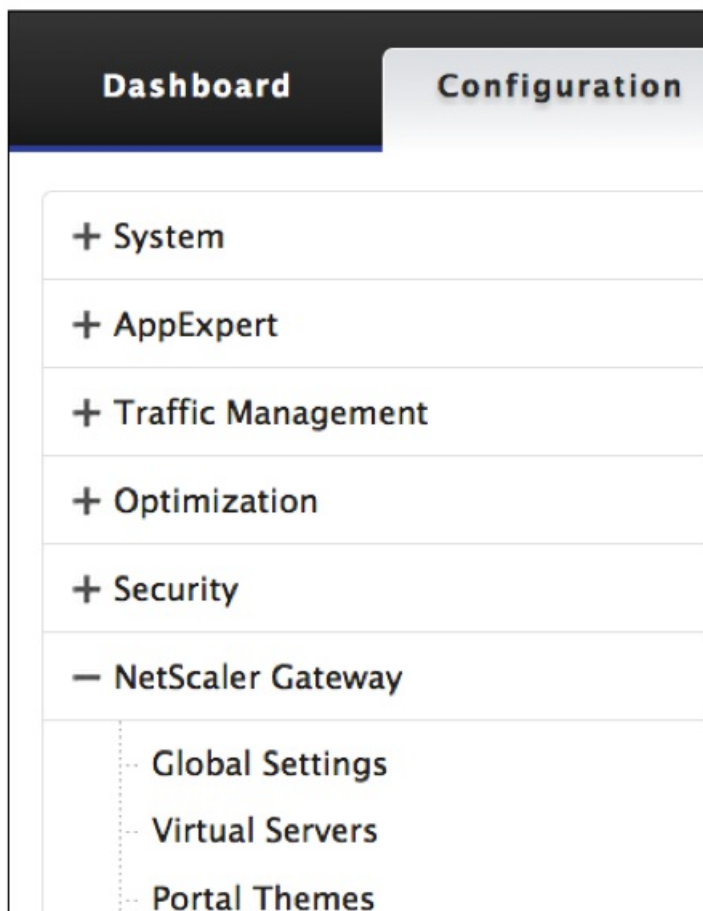
5. Define the (“<groupname>”) in the Default EPA Group dialoge box.

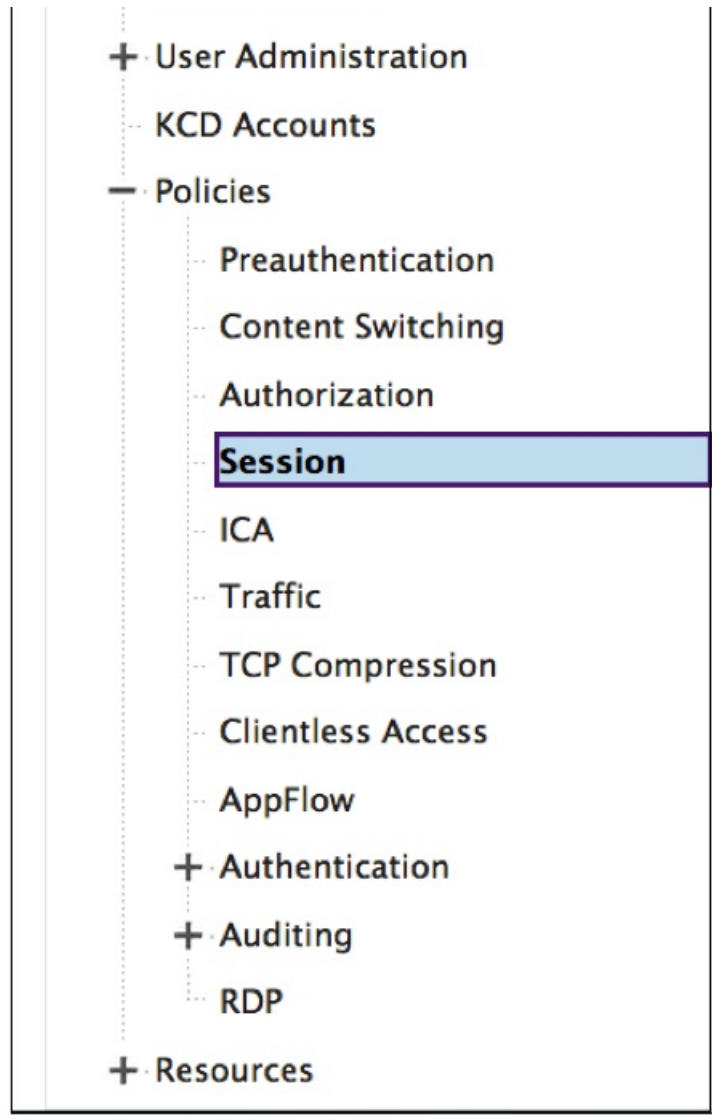


The image shows a dialog box titled "Configure Preauthentication Profile". It contains several input fields and a dropdown menu. The "Name" field is filled with "Pre-auth\_Profile". The "Action\*" dropdown menu is set to "ALLOW". The "Processes to be cancelled" field is filled with "docs" and has a question mark icon to its right. The "Files to be deleted" field is filled with "\*.fm". The "Default EPA Group" field is filled with "group2". At the bottom, there are "OK" and "Close" buttons.

## Session

1. Select Session from the configuration pane.





## Create a Log Action

1. In the Configure Policy screen, next to the Log Action dialog box select the + icon

**Configure Policy**

Name  
policy\_2

Action\*  
Action\_7

Expression\* Expression Editor  
 Operators Saved Policy Expressions Frequently Used Expressions Clear  
 CLIENT.TCP.DSTPORT.EQ(2) Evaluate

Log Action  
AuditMessage1

Comments  
Watch for unauthorized connections!

OK Close

### Create Audit Message Action

2. The Create Audit Message Action screen appears. Name the Audit Message. The Audit message only accepts numbers, letters or an underscore character.
3. From the pull-down menu specify the Audit Log Level.

|               |   |
|---------------|---|
| Emergency     | Events that indicate an immediate crisis on the server. |
| Alert         | Events that might require action.                       |
| Critical      | Events that indicate an imminent server crisis.         |
| Error         | Events that indicate some type of error.                |
| Warning       | Events that require action in the near future.          |
| Notice        | Events that the administrator should know about.        |
| Informational | All but low-level events.                               |
| Debug         | All events, in extreme detail.                          |

4. Enter an Expression. The Expression defines the format and content of the log.
5. The check boxes
  - Check the Log in newslog to send the message to a new ns log.

- Check Bypass Safety Check to bypass the safety check. This allows unsafe expressions.

6. Click **Create**.

**Create Audit Message Action**

Name\*  
Notice 1 (2)

Log Level\*  
NOTICE (3)

Expression\*  
Expression Editor  
Operators Saved Policy Expressions Frequently Used Expressions Clear  
CLIENT.IP.SRC (4)  
Evaluate

Log in newslog (5)  
 Bypass Safety Check

Create Close (6)

## Revise a Log Action

1. In the Configure Policy screen, next to the Log Action dialog box click the icon.

**Configure Policy**

Name  
policy\_2

Action\*  
Action\_7 > + [Pencil]

Expression\*  
Expression Editor  
Operators Saved Policy Expressions Frequently Used Expressions Clear  
CLIENT.TCP.DSTPORT.EQ(2) (1)  
Evaluate

Log Action  
AuditMessage1 + [Pencil] (?)

Comments  
Watch for unauthorized connections! (2)

OK Close

## Configure Audit Message Action

The following are editable fields:

2. From the pull-down menu specify the Audit Log Level.
3. Enter an Expression. The Expression defines the format and content of the log.
4. The check boxes:
  - Check the Log in newslog to send the message to a new ns log.
  - Check Bypass Safety Check to bypass the safety check. This allows unsafe expressions.
5. Click **OK**.

**Configure Audit Message Action**

Name  
AuditMessage1

Log Level\*  
ALERT

Expression\*  
Expression Editor  
Operators Saved Policy Expressions Frequently Used Expressions Clear  
CLIENT.IP.SRC  
Evaluate

Log in newslog  
 Bypass Safety Check

OK Close

## Select an existing policy

1. Click the > icon to select an existing policy.

**Policy Binding**

**Policy Binding**

Select Policy\*  
Click to select > +

**Binding Details**

Priority\*  
150

Goto Expression\*  
END

Bind Close

2. Select the radio button of the desired policy.

| Name                                      | Action       | Expression                                |
|---|--------------|---|
| <input type="radio"/> ica_pol1            | ica_deux     | HTTP.REQ.USER.NAME.CONTAINS("Jon")        |
| <input checked="" type="radio"/> ica_pol4 | ica_act4     | client.TCP.DSTPORT.EQ(7)                  |
| <input type="radio"/> ica_pol5            | ica_act5     | HTTP.REQ.USER.IS_MEMBER_OF("group1")      |
| <input type="radio"/> ica_pol6            | ica_trois_B  | client.IP.DST.BETWEEN(1.1.1.1, 1.2.1.2)   |
| <input type="radio"/> ica_pol2            | ica_action20 | client.IP.DST.EQ(15)                      |
| <input type="radio"/> ica_pol3            | ica_act5     | HTTP.REQ.USER.IS_MEMBER_OF("engineering") |
| <input type="radio"/> ica_pol7            | ica_act2     | client.IP.DST.EQ(15).NOT                  |
| <input type="radio"/> ica_pol8            | ica_act2     | HTTP.REQ.USER.IS_MEMBER_OF("pubs").NOT    |
| <input type="radio"/> ica_pol10           | ica_act10    | client.TCP.DSTPORT.EQ(15)                 |
| <input type="radio"/> ica_pol11           | ica_trois_B  | client.IP.DST.EQ(21)                      |
| <input type="radio"/> ica_pol12           | ica_trois    | client.IP.DST.EQ(21)                      |
| <input type="radio"/> ica_pol13           | ica_trois    | client.IP.DST.EQ(35)                      |

### Create a new policy

1. In Name, type a name for the policy. This is a required field.
2. Click the + to create a new policy.

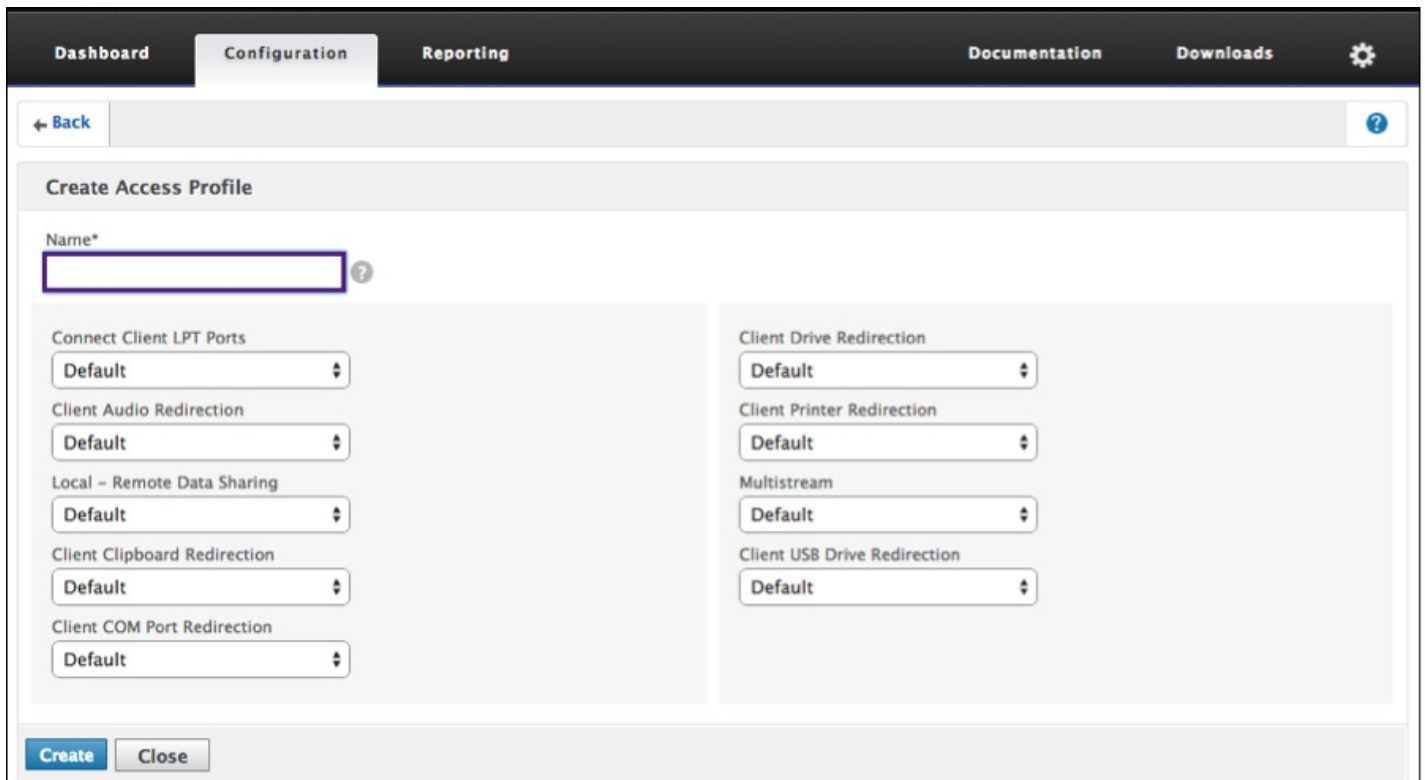
**Create Policy**

Name\*

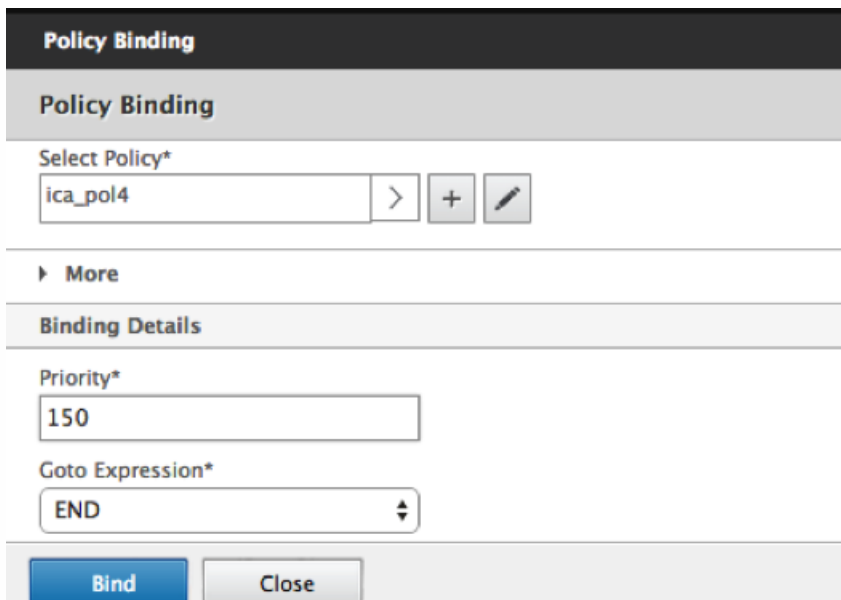
Action\*  
Click to select > + ✎

Expression\*  
Operators Saved Policy Expressions Frequently Used Expressions  
Press Control+Space to start the expression and then type '.' to get the next set of options

3. Create an Action. For details see **Create a new action**.
4. Name the Access Profile.



5. Configure the Access Profile from this menu.
6. Click **Create**.
7. Click **Bind**.



## Configuring pre-authentication and post-authentication end point analysis

This section describes how to configure post-authentication and pre-authentication end point analysis (EPA).

To configure post-authentication EPA with Smartcontrol use the Smartgroup parameter from the VPN session action. The EPA expression is configured on the VPN session policy.

You can specify a groupname for the smartgroup parameter. This groupname can be any string. The groupname does not need to be an existing group on the active directory.

Configure the ICA policy with the expression, HTTP.REQ.IS\_MEMBER\_OF ("groupname"). Use the groupname that was previously specified for the Smartgroup.

To configure pre-authentication EPA with Smartcontrol use the Default EPA group parameter from the pre-authentication profile. The EPA expression is configured on the pre-authentication policy.

You can specify a groupname for the Default EPA group parameter. This groupname can be any string. The groupname does not need to be an existing group on the active directory.

Configure the ICA policy with the expression, HTTP.REQ.IS\_MEMBER\_OF ("groupname"), use the groupname that was previously specified for the Default EPA Group.

## Post- authentication configuration

Use the following procedure to set up smart groups for Post-authentication configuration.

1. Go to NetScaler Gateway>Policies> **Session**.

2. Go to Session Profiles> **Add**.

## Create NetScaler Gateway Session Profile

3. Select the **Security** tab.
4. Enter a **Name** for your NetScaler Gateway Profile (action).
5. Select the box to the right of the pull down menu and select the desired **Default Authorization Action**.

Specify the network resources that users have access to when they log on to the internal network. 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. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security.

6. Select the box to the right of the pull down menu and select the desired **Secure Browse**.

Allow users to connect through NetScaler Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.



7. Select the box to the right of the pull down menu and enter the **Smartgroup** name.

This is the group in which the user is placed when the sessionpolicy associated with this session action succeeds. The vpn session policy will do the post auth EPA check and if the check succeeds the user is placed in the group specified with Smartgroup. The is\_member\_of (http.req.user.is\_member\_of) expression can then be used with policies to check if EPA has passed on the user belonging to this smartgroup.

8. Click **Create**.

1. Go to NetScaler Gateway> Policies >**Session**.

2. Go to Session Policies> **Add**.

1. Enter the **Name** in this field.

This the Name for the new session policy that is applied after the user logs on to NetScaler Gateway.

2. Select the **Profile** action using the drop down menu.

This the Action applied by the new session policy if the rule criterion is met.

**Note:** If the desired profile needs to be created select the +. For more details see [Create NetScaler Gateway Session Profile](#).

3. Enter **Expression** in this field.

This field defines the named expression that specifies the traffic that matches the policy. The expression can be written in either default or classic syntax. The maximum length of a literal string for the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "" + ""

Note: The following requirements apply only to the NetScaler CLI:

\* If the expression includes one or more spaces, enclose the entire expression in double quotation marks.\* If the expression itself includes double quotation marks, escape the quotations by using the character. \* Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

4. Click **Create**.

1. Go to **Session Policies**.
2. Select the **Name** of the Session Policy.
3. Select **Global Bindings** from the Action drop down menu.

4. Select **Add Binding**.

5. Select the > to choose an existing policy.

**Note:** Select the + to create a new policy. For more details see [Create NetScaler Gateway Session Profile](#).

6. Choose a name from the list and press the **Select** button.

7. Enter the **Priority** and click **Bind**.

8. Click **Done**

9. The check shows that your selection is Globally Bound.

## Pre-authentication configuration

Use the following procedure to set up Pre-authentication configuration.

1. Go to NetScaler Gateway>Policies> **Preauthentication**.

2. Select the **Preauthentication Profiles** tab and select **Add**.

1. Enter the **Name**

This is the Name for the preauthentication action. The name must begin with a letter, number, or the underscore character ( ), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after preauthentication action is created.

**Note:** 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.

2. Select a **Request Action** from the drop down menu. This is the action that the policy is to invoke when a connection matches the policy.

**Note:** If you want to or create a Preauthentication Profile, select the +. For more information see [Create Preauthentication Profile](#)

3. Enter an **Expression**

This is the name of the NetScaler named rule, or default syntax expression that defines the connections that match the policy.

4. Click **Create**.

5. Go to the Preauthentication Policies tab and select the desired policy.

6. Select **Global Binding** form the Action Drop down menu.

7. Select **Add Bindings**.

8. Select the > to select an existing policy.

Note: Select the + to create a new policy. For more details see [Create NetScaler Gateway Session Profile](#).

9. **Select** Policy.

10. Enter the **Priority** and click **Bind**.

11. Click **Done**.

12. The check shows that the **Preauthentication Policy** is **Globally Bound**.

## Create Preauthentication Profile

1. Enter the **Name**

This is the **Name** for the preauthentication action. The name must begin with a letter, number, or the underscore character ( ), and must consist only of letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after preauthentication action is created.

**Note:** 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.

2. Enter the **Action** from the drop down menu.

This option will Allow or Deny logon after endpoint analysis (EPA) results.

3. **Processes to be Cancelled**

This option identifies a string of processes to be terminated by the endpoint analysis (EPA) tool.

4. **Files to be deleted**

This option identifies a string specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA)

tool.

5. **Default EPA Group**

This is the default group that is chosen when the EPA check succeeds.

6. Click **Create**.

# Configuring Single Sign-On to the Web Interface

Mar 26, 2014

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 NetScaler Gateway Plug-in from a bookmark configured in the Access Interface or a web address that users type in the web browser.

If you are redirecting the Access Interface to a SharePoint site or the 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 and logged on automatically. 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 rejects 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.

You can also configure single sign-on to the Web Interface by using a smart card. For details, see [Configuring Single Sign-On to the Web Interface by Using a Smart Card](#).

NetScaler Gateway works with the following versions of the Web Interface:

- Web Interface 4.5
- Web Interface 5.0
- Web Interface 5.1
- Web Interface 5.2
- Web Interface 5.3
- Web Interface 5.4

Before you configure single sign-on, make sure the Web Interface is already configured and working with NetScaler Gateway.

# To configure single sign-on to Web applications globally

Nov 11, 2014

Applying single sign-on globally will allow a Web service to authenticate all Web application sessions rather than authenticating those sessions on the 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 Single Sign-on to Web Applications and then click OK.

# To configure single sign-on to Web applications by using a session policy

Feb 20, 2014

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 policy and then click Add.
3. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
4. In the Configure Session Profile dialog box, 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

May 16, 2013

Single sign-on is attempted only for network traffic where the destination port is considered to be 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. You configure the ports 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. In HTTP Ports, type the port number, click Add and then click OK.

Note: If web applications in the internal network use different port numbers, type the port number and then click Add. You must define the HTTP port number to allow single sign-on to web applications, including the Web Interface.

# Additional Configuration Guidelines

May 14, 2013

When you configure the Web Interface for single sign-on, use the following guidelines:

- The Authentication Service URL must begin with https.
- The server running the Web Interface must trust the NetScaler Gateway certificate and be able to resolve the certificate fully qualified domain name (FQDN) to the virtual server IP address.
- The Web Interface must be able to open a connection to the NetScaler Gateway virtual server. Any NetScaler Gateway virtual server can be used for this purpose; it does not have to be the virtual server to which users log on.
- If there is a firewall between the Web Interface and NetScaler Gateway, firewall rules could prevent user access, which disables single sign-on to the Web Interface. To work around this issue, either relax your firewall rules or create another virtual server on NetScaler Gateway to which the Web Interface can connect. The virtual server must have an IP address that is in the internal network. When connecting to the Web Interface, use the secure port 443 as the destination port.
- If you are using a certificate from a private Certificate Authority (CA) for the virtual server, in the Microsoft Management Console (MMC), use the certificates snap-in to install the CA root certificate in the local computer certificate store on the server running the Web Interface.
- When users log on and receive an access denied error message, check the Web Interface event viewer for more information.
- For successful user connections to published applications or desktops, the Secure Ticket Authority (STA) that you configured on NetScaler Gateway must match the STA that you configured on the Web Interface.

# To test the single sign-on connection to the Web Interface

Feb 20, 2014

After you configure single sign-on for the Web Interface, from a client device, open a web browser, and test for a successful connection.

1. In a web browser, type `https://NetScalerGatewayFQDN`, where `NetScalerGatewayFQDN` is the fully qualified domain name (FQDN) in the certificate bound to the virtual server.
2. Log on to a domain user account in Active Directory. At logon, you are redirected to the Web Interface.

Applications appear automatically with no additional authentication. When users start a published application, Citrix Receiver directs traffic through the NetScaler Gateway appliance to servers in the farm.

# Configuring Single Sign-On to the Web Interface by Using a Smart Card

Mar 26, 2014

If you use smart cards for user logon, you can configure single sign-on to the Web Interface. You configure settings on NetScaler Gateway, and then you configure the Web Interface to accept single sign-on with a smartcard. Single sign-on is also called pass-through authentication.

Web Interface Versions 5.3 and 5.4 support single sign-on to the Web Interface using a smart card. If you enable the Web Interface on NetScaler feature available in NetScaler version 10, you can also use single sign-on with a smartcard. For more information about configuring this feature, see [Using Smart Card Authentication for Web Interface through NetScaler Gateway](#).

Users can be in multiple CN groups in Active Directory for single sign-on to work, as long as the user name extraction in the certificate action is SubjectAltName:PrincipalName. If you use the parameter Subject:CN, users cannot be part of multiple CN groups.

To configure NetScaler Gateway for single sign-on to the Web Interface by using a smart card, you need to do the following:

- Install a signed server certificate from a Certificate Authority (CA). For more information, see [Installing the Signed Certificate on NetScaler Gateway](#).
- Install a root certificate on NetScaler Gateway and the user device.
- Create a virtual server as the logon point for the Web Interface. When you configure the virtual server, you must set the client certificate SSL parameter to Optional. For more information about configuring a virtual server, see [Creating Virtual Servers](#).
- Create a secondary virtual server in which client authentication is disabled in the SSL parameters. This configuration prevents users receiving a secondary request for their personal identification number (PIN).
- Create a client certificate authentication policy. In the User Name Field, use the parameter SubjectAltName:PrincipalName to extract users from multiple groups. Leave the Group Name Field blank.
- Create a session policy and profile on NetScaler Gateway. Within the session profile, you enable ICA proxy and specify the Web Interface and domain that you use for single sign-on.

You can use the following procedure to create a session profile for single sign-on with a smart card.

To create a session profile for single sign-on by using a smart card

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. On the Client Experience tab, next to Home Page, click Override Global and then clear Display Home Page.
4. Next to Single sign-on to Web Applications, click Override Global and then click Single sign-on to Web Applications.
5. Click the Published Applications tab.
6. Next to ICA Proxy, click Override Global and then select ON.
7. In Web Interface Address, click Override Global and then type the fully qualified domain name (FQDN) or the Web Interface.
8. In Single Sign-on Domain, click Override Global and then type the domain name.

Note: You must use the format domain and not the format domain.com.

9. Click Create and then click Close.

After you have completed the session profile, configure the session policy and use the profile as part of the policy. You can then bind the session policy to the virtual server.

# To configure the client certificate for single sign-on by using a smart card

Feb 20, 2014

If you configure single sign-on to the Web Interface using a smart card, you must select Client Authentication on the Certificates in the virtual server dialog box and then configure the client certificate as Optional. If you select Mandatory, single sign-on to the Web Interface fails.

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, on the Certificates tab, click SSL Parameter.
4. In the Configure SSL Params dialog box, under Others, click Client Authentication.
5. In Client Certificate, select Optional and then click OK twice.

# To configure single sign-on for XenApp and file shares

Feb 20, 2014

If users are connecting to servers running Citrix XenApp and using SmartAccess, you can configure single sign-on for users connecting to the server farm. When you configure access to published applications by 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.

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.

# Allowing File Type Association

Jan 22, 2014

File type association allows users to open documents in applications published through Citrix XenApp or Citrix XenDesktop 7. You can use this permission to allow users to open and edit documents on servers in the trusted environment and avoid sending the document to the user device. You can use file type association only for document types that are associated with a published application and only if you correctly configure the virtual server properties on NetScaler Gateway.

Providing file type association as the only means for editing resource documents can help to heighten security because it requires that editing occur on the server and not on the user device. For example, you might choose to grant file type association for a file share in which employees post reports of ongoing project meetings, without providing the ability to download or upload.

Providing file type association requires that:

- Users run Citrix Receiver on the user device.
- Users connect through a virtual server that has a traffic policy bound to it and that you configure the policy for XenApp.
- Users are assigned to the desired applications in XenApp or XenDesktop 7.
- Administrators configure XenApp to work with NetScaler Gateway.

The steps for creating file type association include:

- Creating a Web Interface site.
- Configuring file type association using a traffic policy on NetScaler Gateway.
- Defining file extensions in XenApp or XenDesktop 7.



# Creating a Web Interface Site

Apr 29, 2013

To configure the Web Interface to work with file type association, you first create the Web Interface site. The Web Interface site can be in Direct or Advanced Access Control. Copy the following directories to your Web Interface site:

- app\_data
- auth
- site

When you copy these directories to the Web Interface site, the existing directories are overwritten.

If you are using Web Interface 4.6 or 5.0, open the web.config file in the Web Interface site directory and add the following code. You can download this code from the Citrix Support site at <http://support.citrix.com/article/ctx116253>.

```
<location path="site/contentLaunch.ica" >
<system.web>
<httpHandlers>
<add verb="*" path="*.ica" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
<location path="site/contentLaunch.rad" >
<system.web>
<httpHandlers>
<add verb="*" path="*.rad" type="System.Web.UI.PageHandlerFactory"/>
</httpHandlers>
</system.web>
</location>
```

This code must be added after the following section in the web.config file:

```
<location path="site/launch.rad" >
  <system.web>
    <httpHandlers>
      <add verb="*" path="*.rad" type="System.Web.UI.PageHandlerFactory"/>
    </httpHandlers>
  </system.web>
</location>
```

# Configuring NetScaler Gateway for File Type Association

Mar 25, 2014

Before you configure file type association on NetScaler Gateway, configure a Web Interface site to work with file type association. After you create and configure the Web Interface, you need to create settings on NetScaler Gateway. The steps include:

- Creating a new virtual server or using an existing one. For more information about creating a virtual server, see [Creating Virtual Servers](#).
- Creating a new session policy and profile that has the Web Interface configured.
- Binding the session policy to the virtual server.
- Creating a traffic policy.

After you create the session policy and bind it to the virtual server, create the traffic policy and also bind it to the virtual server.

When you configure a traffic policy for file type association, you create an expression to define the file extensions. For example, you want to enable file type association for Microsoft Word and Microsoft Excel. An example expression is:

```
REQ.HTTP.URL == /*.doc || REQ.HTTP.URL == /*.xls
```

To create a session policy and profile for file type association

1. In the configuration utility, click the Configuration tab and then 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 Published Applications tab, configure the following settings:
  1. Next to Web Interface Address, click Override Global and then type the Web address of the Web Interface.
  2. Next to Web Interface Portal Mode, click Override Global and then select either Normal or Compact.
  3. Next to Single Sign-on Domain, click Override Global, type the name of the domain in which the user accounts reside and then click Create.
7. In the Create Session Policy dialog box, next to Named Expression, select True value, click Add Expression, click Create and then click Close.

To create a traffic profile for file type association

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 Profiles tab and then click Add.
3. In Name, type a name for the profile.
4. In File Type Association, select ON, click Create and then click Close.

To configure file type association in a traffic policy

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, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. In Request Profile, select a profile.
5. In the Create Traffic Policy dialog box, under Expressions, select Advanced Free-Form and then click Add.
6. In the Add Expression dialog box, do the following:
  1. In Expression Type, click General.
  2. In Flow Type, select REQ.
  3. In Protocol, select HTTP.
  4. In Qualifier, select URL.
  5. In Operator, select = =.
  6. In Value, type /\*.  
— *FileExtensionType*  
, where .  
— *FileExtensionType*  
is the file type, such as .doc or .xls and then click OK.
7. In the Create Traffic Policy dialog box, under Expressions, next to Advanced Free-Form, click OR.
8. Repeat Steps 4, 5 and 6 for each file extension you want to include, click Create and then click Close.

# Integrating with App Controller or StoreFront

Feb 27, 2014

This section contains information about configuring connections from remote users through NetScaler Gateway to your App Controller and StoreFront deployment.

You can configure NetScaler Gateway to work with App Controller and StoreFront. When you configure NetScaler Gateway to work with App Controller or StoreFront, Citrix recommends using the Quick Configuration wizard to configure your settings. The Quick Configuration wizard configures a virtual server and the settings for session, clientless access, and authentication policies. You can also configure DNS servers for connections to StoreFront and App Controller.

## Integrating NetScaler Gateway and App Controller

If you deploy App Controller in your network, you can allow user connections from remote users by integrating NetScaler Gateway and App Controller. This deployment allows users to connect to App Controller to obtain their web, Software as a Service (SaaS), Android and iOS mobile apps, along with documents from ShareFile. Users connect by using Worx Home, Citrix Receiver, or the NetScaler Gateway Plug-in.

In this App Controller deployment, NetScaler Gateway resides in the DMZ and App Controller resides in the internal network.

To allow connections from remote users to App Controller, Citrix recommends using the Quick Configuration wizard in NetScaler Gateway to configure the web address for App Controller, StoreFront or the Web Interface. The wizard configures all of the policies required for users to connect to App Controller, which include authentication, session, and clientless access policies. For more information about the wizard, see [Configuring Settings with the Quick Configuration Wizard](#).

You can also configure connections to App Controller by creating policies with the configuration utility, such as:

- One session policy manages Receiver and Worx Home connections to StoreFront. This session policy supports Receiver for Windows, Receiver for Mac, Receiver for Android, and Receiver for iOS. If users connect with Worx Home, WorxMail, or WorxWeb on an iOS device, you must enable clientless access and Secure Browse to allow connections through NetScaler Gateway. You need to configure Secure Browse for iOS devices only. Both iOS and Android devices use Micro VPN that establishes the VPN tunnel to the internal network.
- One session policy manages browser connections to Receiver for Web. Users connect by using clientless access.
- One virtual server with SmartAccess mode enabled which also enables clientless access. This deployment requires the Universal license.
- Custom clientless access policies. These policies define rewriting policies for XML and HTML traffic, along with how cookies are handled by NetScaler Gateway.

## Integrating NetScaler Gateway and StoreFront

Users can connect in one of the following ways through StoreFront:

- Clientless access and Receiver for Web
- NetScaler Gateway Plug-in
- Receiver for Android
- Receiver for iOS
- Receiver for Mac

- Receiver for Windows
- Worx Home

Important: The fully qualified domain name (FQDN) for StoreFront must be unique and different from the NetScaler Gateway virtual server FQDN. You cannot use the same FQDN for StoreFront and the NetScaler Gateway virtual server. Citrix Receiver requires that the StoreFront FQDN is a unique address that resolves only from user devices connected to the internal network. If this is not the case, Receiver for Windows users cannot use email-based account discovery. When users connect, a list of available applications, desktops, and documents appear in the Receiver window. Users can also subscribe to applications from the store. The store enumerates and aggregates desktops and applications from XenDesktop sites, XenApp farms, and App Controller, making these resources available to users.

Note: To allow users access to MDX mobile apps, you must deploy App Controller in front of StoreFront. If you are not providing access to MDX mobile apps, StoreFront resides in front of App Controller.

When you configure NetScaler Gateway to connect to StoreFront, you configure the following:

- One session policy to manage Worx Home and Receiver connections to StoreFront. This session policy supports Receiver for Windows, Receiver for Mac, Receiver for Android, and Receiver for iOS. If users connect with Receiver for Android or Receiver for iOS, you must enable clientless access and Secure Browse to allow connections through NetScaler Gateway.
- One session policy to manage browser connections to Receiver for Web. Users connect by using clientless access.
- One session policy to manage PNA Services connections made through Receiver for Android, Receiver for iOS, and other mobile devices if you do not enable Secure Browse. If you configure the session policy for PNA Services, Receiver for Windows is not supported.
- One virtual server with SmartAccess mode enabled which also enables clientless access. This deployment requires the Universal license.
- Custom clientless access policies. These policies define rewriting policies for XML and HTML traffic, along with how cookies are handled by NetScaler Gateway.

### Configuring Policies for App Controller and StoreFront

If you deploy App Controller and StoreFront and you do not use the Quick Configuration wizard to configure settings, you need to configure the following policies. You can configure these policies for NetScaler Gateway and App Controller only, NetScaler Gateway and StoreFront only, or a deployment that contains NetScaler Gateway, App Controller, and StoreFront.

- One session policy to manage Receiver connections to App Controller or StoreFront. This session policy supports Receiver for Windows, Receiver for Mac, Receiver for Android, and Receiver for iOS. If users connect with Receiver for Android or Receiver for iOS, you must enable clientless access. For connections from Receiver for iOS, you must enable Secure Browse to allow connections through NetScaler Gateway.
- One session policy to manage browser connections to Receiver for Web. Users connect by using clientless access.
- One virtual server with SmartAccess mode enabled which also enables clientless access. This deployment requires the Universal license.
- Custom clientless access policies. These policies define rewriting policies for XML and HTML traffic, along with how cookies are handled by NetScaler Gateway.

If you deploy StoreFront and users connect with legacy versions of Receiver, create one session policy to manage PNA Services connections made through Receiver for Android, Receiver for iOS, and other mobile devices if you do not enable Secure Browse. If you configure the session policy for PNA Services, Receiver for Windows is not supported.

Note: When you configure the StoreFront URL in NetScaler Gateway, such as <https://<SFLite-FQDN>/Citrix/StoreWeb>,

the text StoreWeb is case sensitive.

# How NetScaler Gateway and App Controller Integrate

Feb 23, 2014

You can configure NetScaler Gateway to work with App Controller. In this deployment, NetScaler Gateway resides in the DMZ. App Controller and StoreFront reside in the secure network. NetScaler Gateway must have access to the same forest that App Controller and StoreFront reside in.

When you configure user connections through NetScaler Gateway to App Controller or StoreFront, users can connect in the following ways:

- By using Receiver.
- By using Worx Home, WorxMail, or WorxWeb for iOS and Android devices. To enable this connection, you configure Secure Browse for iOS devices and clientless access in NetScaler Gateway. For more information, see [Allowing Access from Mobile Devices with Worx Apps](#).
- By using NetScaler Gateway through a web browser and Receiver for Web.
- By using Receiver for Android or Receiver for iOS.

Users can connect by using the following versions of Receiver and the following operating systems:

| Receiver   | Operating system  |
|--|---|
| Receiver for Windows 4.1 and 4.2                       | Window 7 Home (32-bit and 64-bit versions)<br><br>Windows 7 Enterprise (32-bit and 64-bit versions)   |
| Receiver for Mac 11.5 and 11.6, 11.7, 11.8, and 11.8.2 | <ul style="list-style-type: none"><li>• Mac OS X Mavericks (version 10.9)</li><li>• Mac OS X 10.8</li><li>• Mac OS X 10.7</li><li>• Mac OS X 10.6</li></ul> <p>For more information, see the system requirements for your version of Receiver for Mac in the<br/><i>— Receivers and Plug-ins</i><br/>node in Citrix eDocs</p> |
| Receiver for iOS 5.7 and 5.8                           | iOS 5.1, 6.1.x, and 7<br><br>For more information, see the system requirements for your version of Receiver for iOS in the<br><i>— Receivers and Plug-ins</i><br>node in Citrix eDocs   |
| Receiver for Android 3.3 and 3.4                       | Android 3.2   |

Users can connect through NetScaler Gateway to App Controller by using the following methods:

- Connect to Receiver for Web by using the NetScaler Gateway web address in a web browser. When users connect with clientless access and Receiver for Web, they can start their applications from within the web browser. When you configure NetScaler Gateway to support Receiver for Web, other clientless access policies that are bound to the virtual server, such as for Outlook Web App 2010 or SharePoint, are not supported. When users connect with Receiver for Web, subscriptions to web or SaaS applications are supported as long as users connect with clientless access through NetScaler Gateway 10.
- Connect to App Controller by using Receiver for Windows by using native protocols. When users connect with clientless access to App Controller or StoreFront, users download a provisioning file from the Receiver for Web site and install the file on the device. Receiver uses settings within the provisioning file to determine if the user device is inside or outside the secure network. Users connect with the NetScaler Gateway web address, such as <https://<AccessGatewayFQDN>>. When logon is successful, users can start or subscribe to their web, SaaS, or mobile apps. Users can also access documents located in ShareFile.  
Note: You can also email the provisioning file to users.
- Connect to App Controller by using Worx Home. When users connect with Worx Home from an iOS or Android mobile device, they have access to mobile, web, and SaaS apps.
- Connect to App Controller by using the NetScaler Gateway Plug-in. You can use the NetScaler Gateway Plug-in for Windows or NetScaler Gateway Plug-in for Mac to connect to web applications hosted by App Controller.

Users can connect to StoreFront only by using the following connection methods:

- Connect to StoreFront by using email-based discovery. NetScaler Gateway supports Accounts Services that allows users to connect by using an email address or the NetScaler Gateway FQDN. When users log on, Receiver instructs users about how to configure access.
- Connect to StoreFront by using PNA Services. If users connect with legacy versions Receiver for Mac, Receiver for Android, or Receiver for iOS, users must manually configure a store within Receiver by using the NetScaler Gateway web address. When users successfully log on, they can start their published applications and virtual desktops. Users cannot connect with Receiver for Windows if you use PNA Services.  
Remote access to web or SaaS applications hosted in App Controller through PNA Services is not supported for Receiver for Android or Receiver for iOS.

To allow users to connect with the NetScaler Gateway Plug-in and access web applications from App Controller, when you configure the application connector in App Controller, you select a check box that identifies that the web application is hosted in the internal network. This adds the VPN keyword to the application and allows the connection request through NetScaler Gateway. For more information, see [Configuring Connections to Enterprise Web Applications Through NetScaler Gateway](#).



# Creating Policies with the Quick Configuration Wizard

Mar 18, 2014

You can configure settings in NetScaler Gateway to enable communication with App Controller, StoreFront, or the Web Interface by using the Quick Configuration wizard. When you complete the configuration, the wizard creates the correct policies for communication between NetScaler Gateway, App Controller, 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 that the wizard creates.

When you complete the Quick Configuration wizard, NetScaler Gateway can communicate with App Controller 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 App Controller.

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)
- App Controller, StoreFront, or Web Interface

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.

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 can only configure one LDAP authentication policy by using the Quick Configuration wizard. The wizard does not allow you to configure multiple LDAP authentication policies. If you run the wizard more than one time and want to use a different LDAP policy, you must configure the additional policies manually. 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 configuration utility to create the authentication policies. For more information about configuring NetScaler Gateway to authenticate user access with one or more LDAP servers, see [Configuring LDAP Authentication](#).

When you create a virtual server by using the Quick Configuration wizard, if you want to remove the virtual server at a later time, Citrix recommends removing it by using the Home tab. When you use this method to remove the virtual server, the policies and profiles configured through the wizard are removed. If you remove the virtual server by using the Configuration tab, the policies and profiles are not removed. The wizard does not remove the following items:

- Certificate key pair created during the wizard are not removed, even if the certificate is not bound to a virtual server
- LDAP authentication policy and profile remains if the policy is bound to another virtual server. NetScaler Gateway removes the LDAP policy only if the policy is not bound to a virtual server.

The following tables describe the policies and profiles that the Quick Configuration wizard creates. As described in the tables, the policies and profiles that are configured depend on how users connect - with either the NetScaler Gateway Plug-in, Citrix Receiver, or Worx Home. The policies that are enforced depend on the XenMobile Universal or Platform license that is used when users connect. When you purchased NetScaler Gateway, you also purchased a set number of Universal licenses; for example, 100. If users connect with the NetScaler Gateway Plug-in, the session uses one Universal license. If users connect with Receiver to access Windows-based applications or XenDesktop, the session uses the Platform license. If users connect from a mobile device by using micro VPN, and connect with Worx Home, or start apps, such as WorxMail or WorxWeb, the session uses a Universal license.

## Session Policies, Rules, and Profiles for the Universal License

The Quick Configuration wizard creates the following session policies and rules that are enforced when the session uses the Universal license.

| Policy type                     | Rule  |
|---------------------------------|---|
| Session - Worx Home or Receiver | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS |
| Session - Receiver for Web      | REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS       |
| Session - NetScaler Gateway     | REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer NOTEXISTS    |

The following table shows the session profile settings that the Quick Configuration wizard creates for each session policy type in the preceding table. The first column describes where to find the profile setting or the tab in the session profile in the configuration utility.

The StoreFront URL you enter depends on how users connect. If users connect by using Receiver for Web or by using a web browser, you use the URL form <https://SF-FQDN/Citrix/StoreWeb>. If users connect by using Receiver on Windows, Mac, or mobile devices, you use the URL form <https://SF-FQDN/Citrix/Store>.

| Profile location                  | Profile setting          | Receiver | Receiver for Web | NetScaler Gateway |
|-----------------------------------|--------------------------|----------|------------------|-------------------|
| Resources > Intranet Applications | Transparent interception | N/A      | Off              | On                |

| Profile location   | Profile setting                    | Receiver                    | Receiver for Web            | NetScaler Gateway           |
|--|------------------------------------|-----------------------------|-----------------------------|-----------------------------|
| Session >Client Experience tab   | Clientless access                  | On                          | On                          | Off                         |
| Session >Published Applications tab  | ICA Proxy                          | Off                         | Off                         | Off                         |
| Session >Client Experience tab   | Single sign-on to Web applications | On                          | On                          | On                          |
| Session >Published Applications tab  | Single sign-on domain              | App Controller StoreWeb URL | App Controller StoreWeb URL | App Controller StoreWeb URL |
| Session >Published Applications tab  | Web Interface Address              | App Controller StoreWeb URL | App Controller StoreWeb URL | App Controller StoreWeb URL |
| Session >Published Applications tab  | Account Services Address           | StoreFront URL              | N/A                         | StoreFront URL              |
| Session >Client Experiences tab  | Split Tunnel                       | Off                         | N/A                         | Off                         |
| Session >Client Experiences tab  | Clientless Access URL Encoding     | Clear                       | N/A                         | Clear                       |
| Session >Client Experiences tab  | Home Page                          | N/A                         | App Controller StoreWeb URL | App Controller StoreWeb URL |
| Session >Client Experiences tab and then click the Advanced Settings > General tab | Client Choices                     | Off                         | Off                         | Off                         |
| Session >Security tab  | Default Authorization Action       | Allow                       | Allow                       | Allow                       |
| Session >Client Experiences tab  | Session Time-out (mins)            | 24 hours                    | N/A                         | N/A                         |
| Session >Client Experiences tab  | Client Idle Time-out (mins)        | (0) disabled                | N/A                         | N/A                         |
| Session >Network Configuration tab and then click Advanced Settings                | Forced Time-out (mins)             | 24 hours                    | N/A                         | N/A                         |

#### Clientless Access Profile Settings for the Universal License

The Quick Configuration wizard creates the following clientless access profile settings for the Universal license:

- Configure Domains for Clientless Access to allow access. Configures the pattern set ns\_cvpn\_default\_inet\_domains <—App Controller FQDN >. For example, ns\_cvpn\_default\_inet\_domainsAppController\_domain\_com
- App Controller URL. Configures the pattern set ns\_cvpn\_default\_inet\_domains <—App Controller FQDN >. For example, ns\_cvpn\_default\_inet\_domainsAppController\_domain\_com
- ShareFile. Allows for up to five bindings. Configure the pattern set ns\_cvpn\_default\_inet\_domains <—App Controller FQDN >. For example, ns\_cvpn\_default\_inet\_domainsAppController\_domain\_com

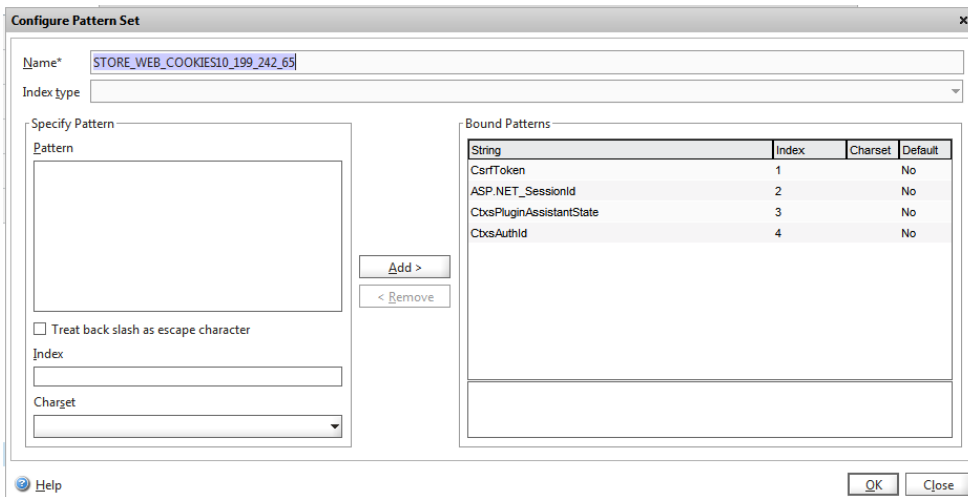
#### Clientless Access Settings and Rules for the Universal License

The following table lists the clientless access policy settings that are enforced when the session uses the Universal license.

| Policy name                    | Rule               | Profile      | URL rewrite label              | Javascript rewrite label | Pattern set            | Comments           |
|--------------------------------|--------------------|--------------|--------------------------------|--------------------------|------------------------|--------------------|
| CLT_LESS_VIP                   | Receiver_NoRewrite | NO_RW_VIP    | Default                        | Default                  | Default                | Receiver_NoRewrite |
| CLT_LESS_RF_VIPCLT_LESS_RF_VIP | True               | ST_WB_RW_VIP | ns_cvpn_default_inet_url_label | Default                  | STORE_WEB_COOKIES<VIP> | RfWeb_Rewrite      |

The pattern set STORE\_WEB\_COOKIES for Receiver for Web appends the NetScaler Gateway virtual IP address to the name, as shown in the next figure:

Figure 1. Pattern Set for Receiver for Web



### Session Policies, Rules, and Profiles for the Platform License

The Platform license with NetScaler Gateway allows for an unlimited number of ICA connections to Windows-based applications and desktops hosted by XenApp and XenDesktop. The following tables show the session rules and session policy settings for users who connect with Citrix Receiver.

| Policy type                                      | Rule  |
|--|---|
| Session - Operating System and NetScaler Gateway | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver    REQ.HTTP.HEADER Referer NOTEXISTS |
| Session - Receiver for Web                       | ns_true   |

| Profile location  | Profile setting                    | Operating system/NetScaler Gateway                          | Web            |
|---|------------------------------------|---|----------------|
| Resources > Intranet Applications   | Transparent interception           | N/A   | Off            |
| Session > Client Experience tab   | Clientless Access                  | Off   | Off            |
| Session > Published Applications tab  | ICA Proxy                          | On  | On             |
| Session > Client Experience tab   | Single Sign-on to Web Applications | On  | On             |
| Session > Published Applications tab  | Single Sign-on Domain              | Set   | Set            |
| Session > Published Applications tab  | Web Interface Address              | config.xml if Web Interface<br>StoreFront URL with StoreWeb | StoreFront URL |
| Session > Published Applications tab  | Account Services Address           | StoreFront URL with StoreWeb                                | N/A            |
| Session > Client Experiences tab  | Split Tunnel                       | Off   | N/A            |
| Session > Client Experiences tab  | Clientless Access URL Encoding     | N/A   | N/A            |
| Session > Client Experiences tab  | Home Page                          | N/A   | N/A            |
| Session > Client Experiences tab and then click the Advanced Settings > General tab | Client Choices                     | Off   | Off            |
| Session > Security tab  | Default Authorization Action       | Allow   | Allow          |
| Session > Client Experiences tab  | Session Time-out (mins)            | N/A   | N/A            |
| Session > Client Experiences tab  | Client Idle Time-out (mins)        | N/A   | N/A            |
| Session > Network Configuration tab and then click Advanced Settings                | Forced Time-out (mins)             | N/A   | N/A            |

# Examples of Session Policies Created by the Quick Configuration Wizard

Feb 06, 2014

The following figures show examples of session policies for integrating App Controller, StoreFront, or the Web Interface with NetScaler Gateway. If you run the Quick Configuration wizard, NetScaler Gateway creates these policies automatically. You can also use these examples to configure the policies manually by using the configuration utility.

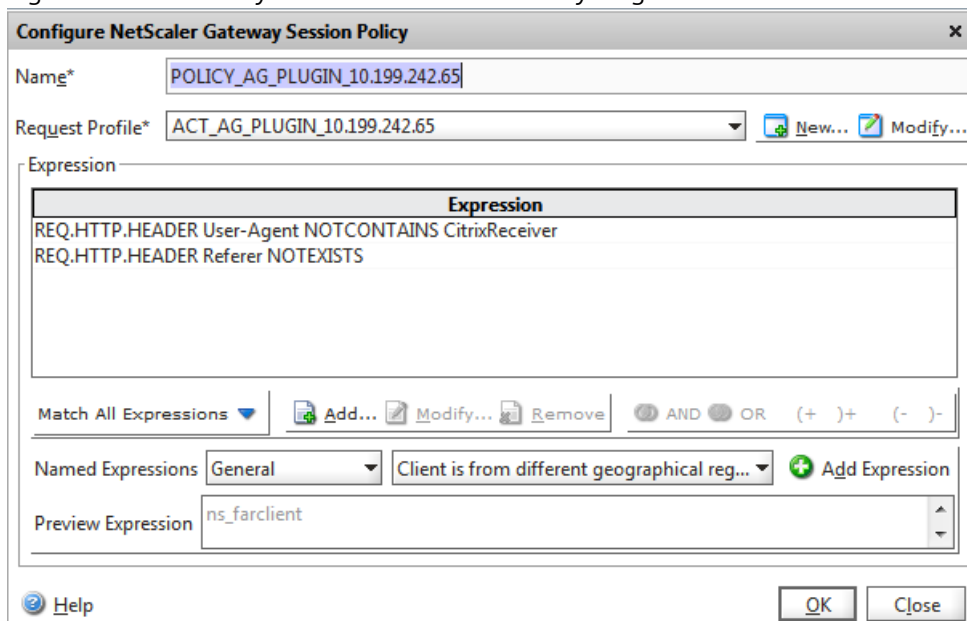
The Quick Configuration wizard configures the following four session policies automatically. These include:

- NetScaler Gateway Plug-in
- Citrix Receiver
- Receiver for Web
- Program Neighborhood Agent

The following figures show the configured expressions for each of these policies. The Quick Configuration wizard appends the virtual server IP address to the policy and profile name.

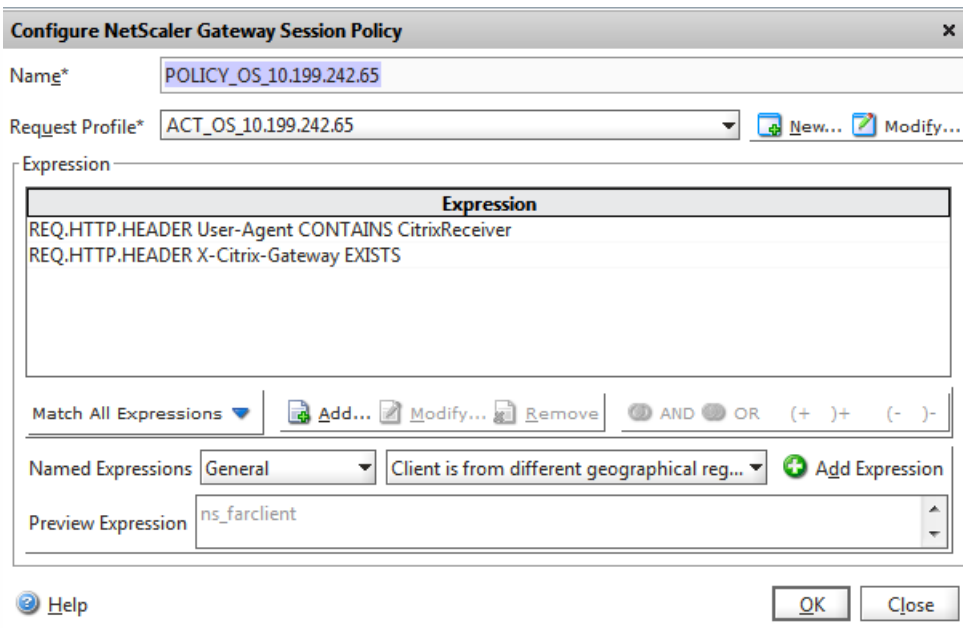
This policy is for users who connect with the NetScaler Gateway Plug-in for Windows or the NetScaler Gateway Plug-in for Mac.

Figure 1. Session Policy for the NetScaler Gateway Plug-in



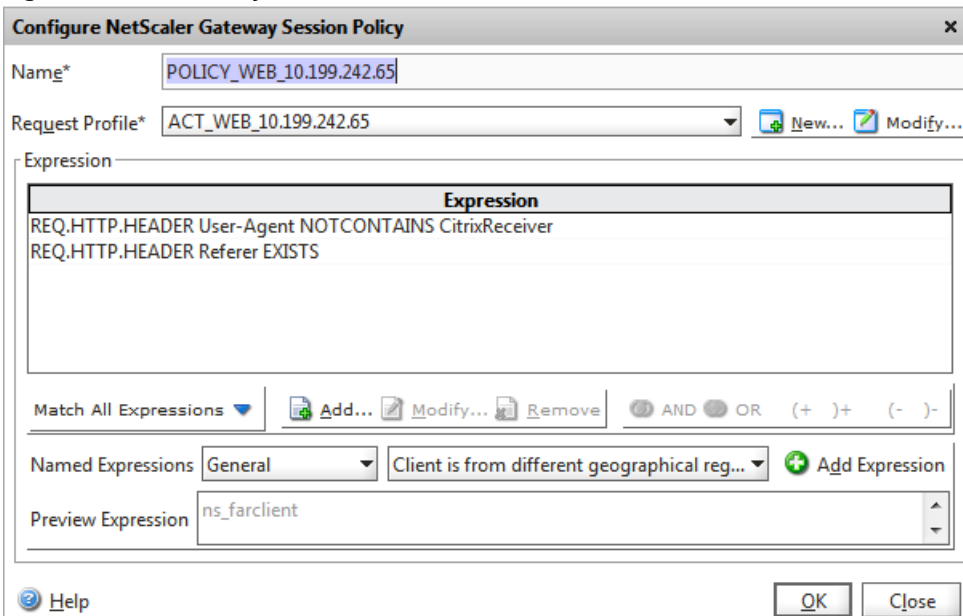
This policy checks to see if users connect with Receiver and if the connection goes through NetScaler Gateway.

Figure 2. Session Policy for Citrix Receiver



This policy is for users who connect with Receiver for Web.

Figure 3. Session Policy for Receiver for Web



This policy is for users who connect with Program Neighborhood Agent.

Figure 4. Session Policy for Program Neighborhood Agent

**Configure NetScaler Gateway Session Policy** x

Name\*

Request Profile\*  [New...](#) [Modify...](#)

Expression

| Expression   |
|--|
| REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver |
| REQ.HTTP.HEADER X-Citrix-Gateway NOTEXISTS         |

Match All Expressions  [Add...](#) [Modify...](#) [Remove](#)  AND  OR  (+) +  (-) -

Named Expressions   [Add Expression](#)

Preview Expression

[Help](#)

# Examples of the Session Profile Settings Created by the Quick Configuration Wizard

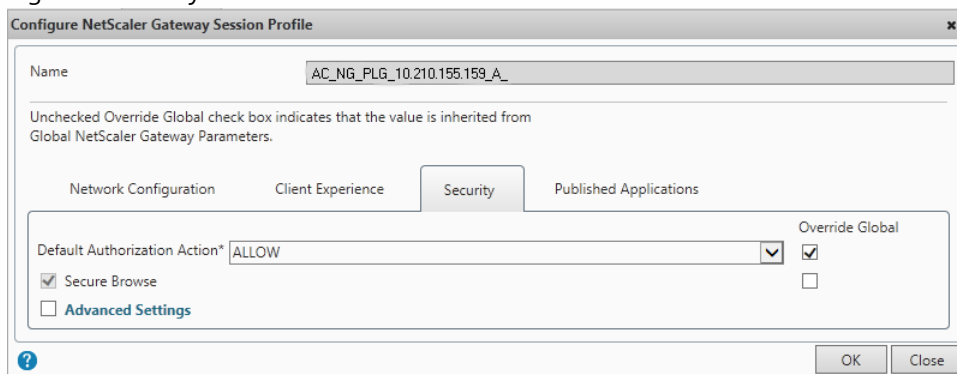
Feb 26, 2014

The following figures show examples of session profiles created by the Quick Configuration wizard. If you run the Quick Configuration wizard, NetScaler Gateway creates these profile settings automatically. You can also use these examples to configure the policies manually by using the configuration utility.

Note: When you configure the StoreFront URL in NetScaler Gateway, such as <https://<SFLite-FQDN>/Citrix/StoreWeb>, the text StoreWeb is case sensitive.

Each profile contains the same setting on the Security tab, as shown in the following figure:

Figure 1. Security Tab in the Session Profile



## Examples of Profile Settings for the NetScaler Gateway Plug-in

The following examples show the session profile settings on the Client Experience and Published Applications tab for the NetScaler Gateway Plug-in.

Figure 2. Session Profile Settings on the Client Experience Tab

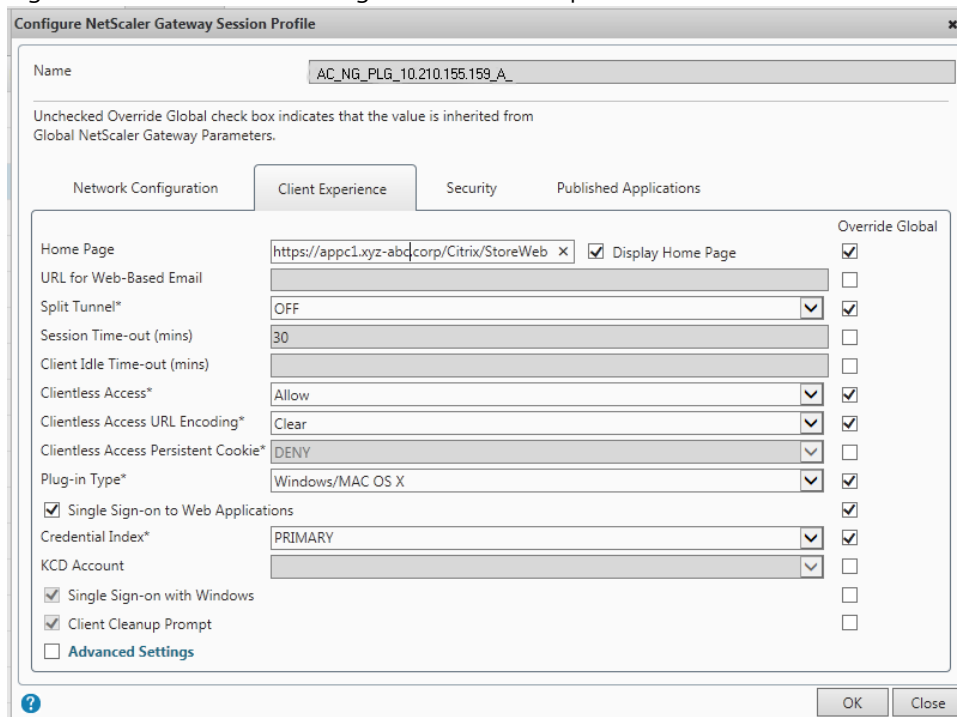
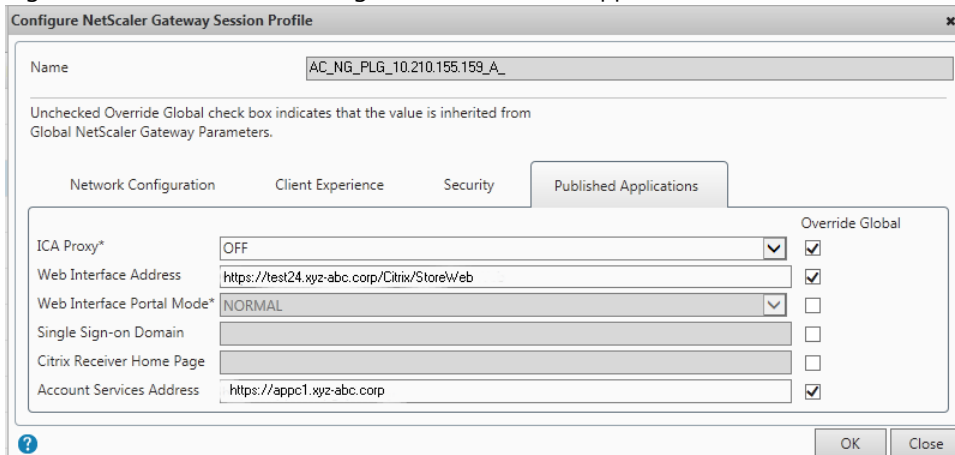


Figure 3. Session Profile Settings on the Published Applications Tab



### Examples of Profile Settings for Receiver or Worx Home

The following examples show the session profile settings on the Client Experience and Published Applications tab for Receiver or Worx Home.

Figure 4. Session Profile Settings on the Client Experience Tab

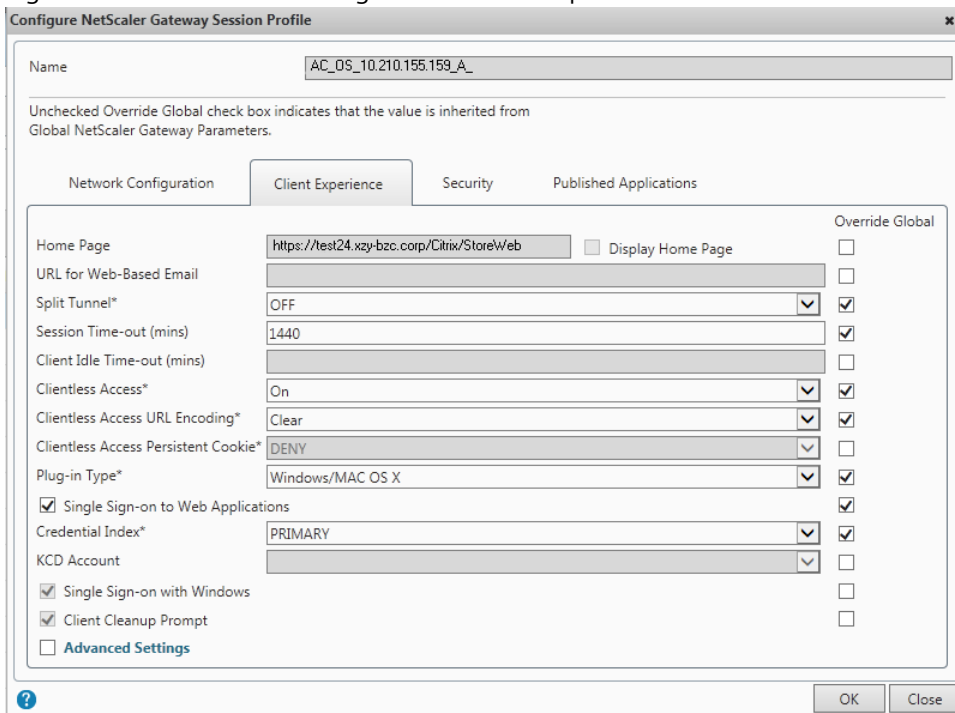
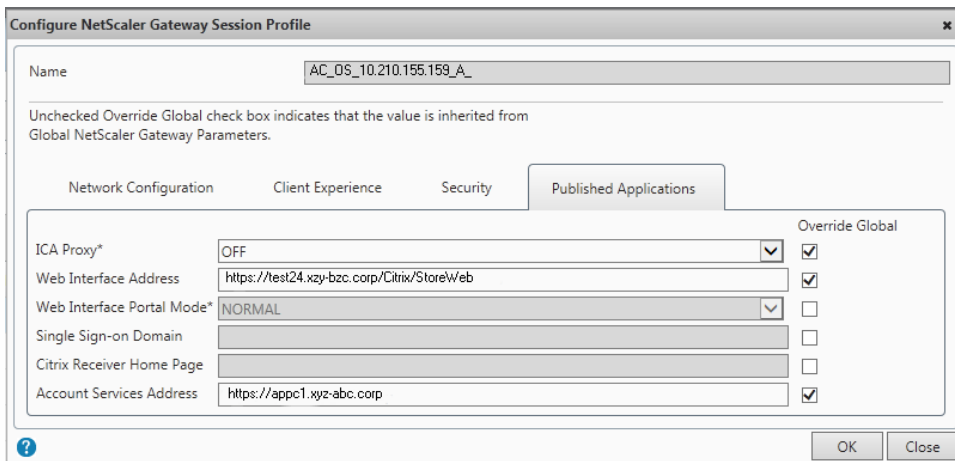


Figure 5. Session Profile Settings on the Published Applications Tab





## Examples of Profile Settings for Receiver for Web

The following examples show the session profile settings on the Client Experience and Published Applications tab for Receiver for Web.

Figure 6. Session Profile Settings on the Client Experience Tab

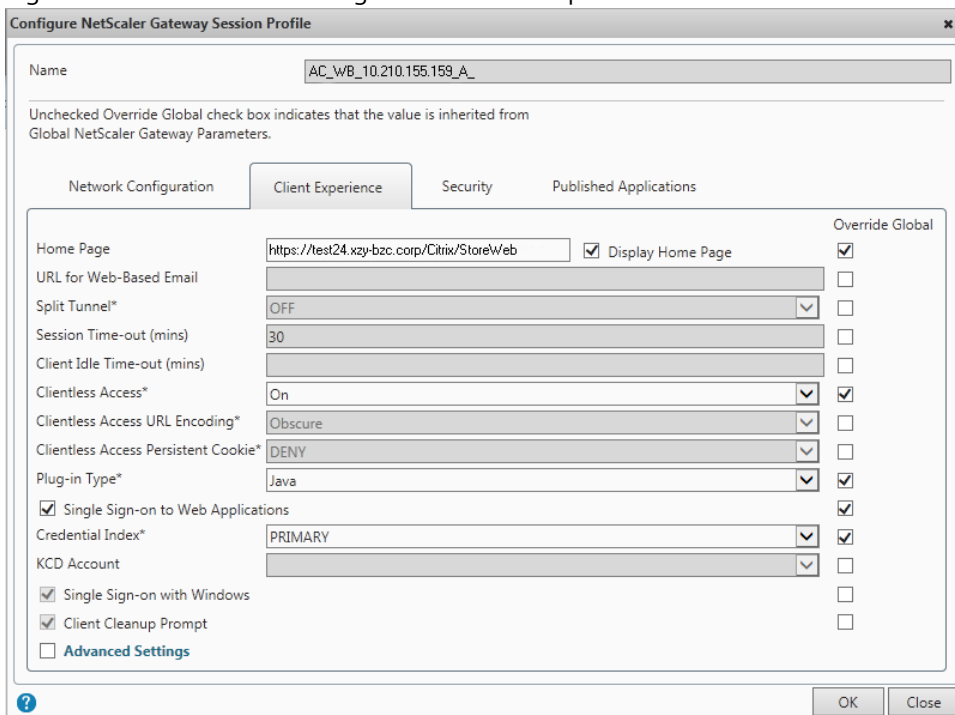


Figure 7. Session Profile Settings on the Published Applications Tab

**Configure NetScaler Gateway Session Profile** [x]

Name: AC\_WB\_10.210.155.159\_A

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration   Client Experience   Security   **Published Applications**

|                            |   | Override Global                     |
|----------------------------|---|-------------------------------------|
| ICA Proxy*                 | OFF   | <input checked="" type="checkbox"/> |
| Web Interface Address      | https://test24.xzy-bzc.corp/Citrix/StoreWeb | <input checked="" type="checkbox"/> |
| Web Interface Portal Mode* | NORMAL                                      | <input type="checkbox"/>            |
| Single Sign-on Domain      |   | <input type="checkbox"/>            |
| Citrix Receiver Home Page  |   | <input type="checkbox"/>            |
| Account Services Address   |   | <input type="checkbox"/>            |

[?]   [OK]   [Close]

# Examples of Clientless Access Policies Created by the Quick Configuration Wizard

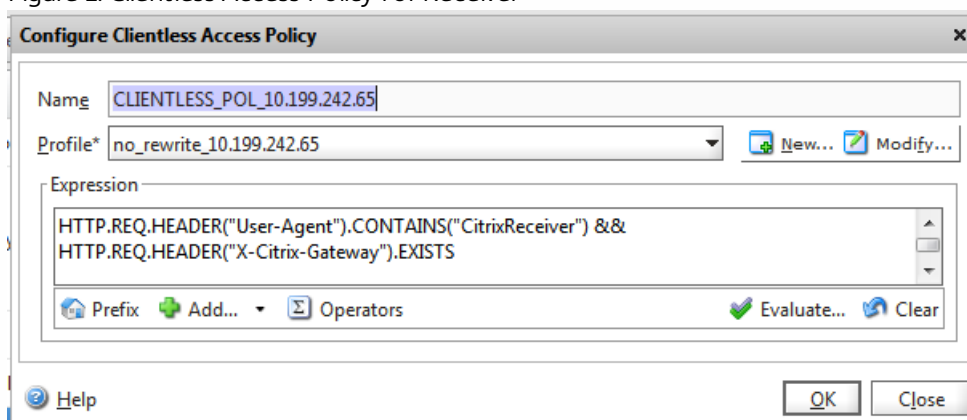
Aug 02, 2013

The following figures show examples of the clientless access policies and profile settings for Citrix Receiver and Receiver for Web that you can create with the Quick Configuration wizard.

## Clientless Access Policy for Receiver

The clientless access policy expression, as shown in the following figure, contains two parts that, in one part, identifies the User-Agent and Receiver and in another part, if NetScaler Gateway is present. There are no other profile settings created for this policy.

Figure 1. Clientless Access Policy for Receiver

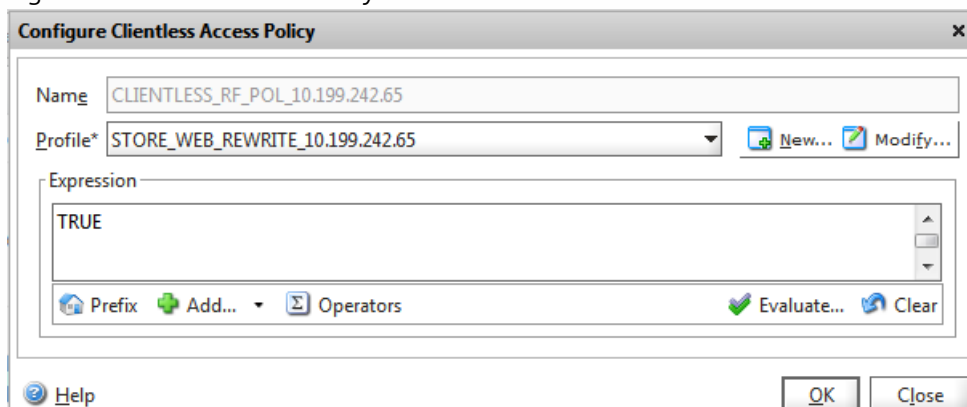


## Clientless Access Policies for Receiver for Web

When the Quick Configuration wizard creates the policy for Receiver for Web, the wizard also creates profiles for URL rewriting and for client cookies, including the pattern set. The following figures show these settings as they appear in the configuration utility.

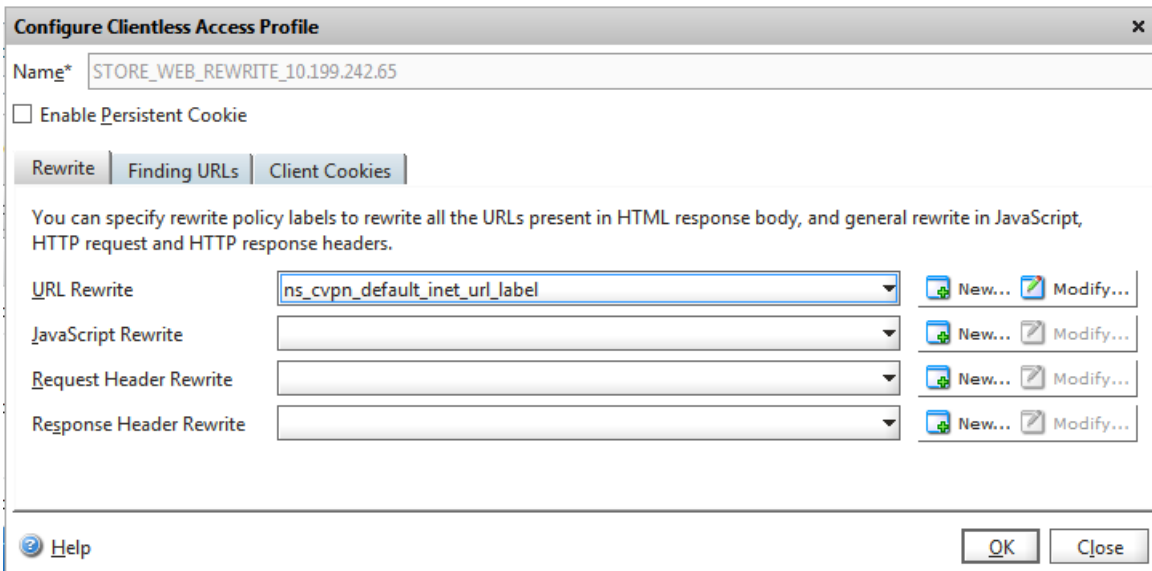
This figure shows the clientless access policy with the expression set to TRUE for Receiver for Web.

Figure 2. Clientless Access Policy



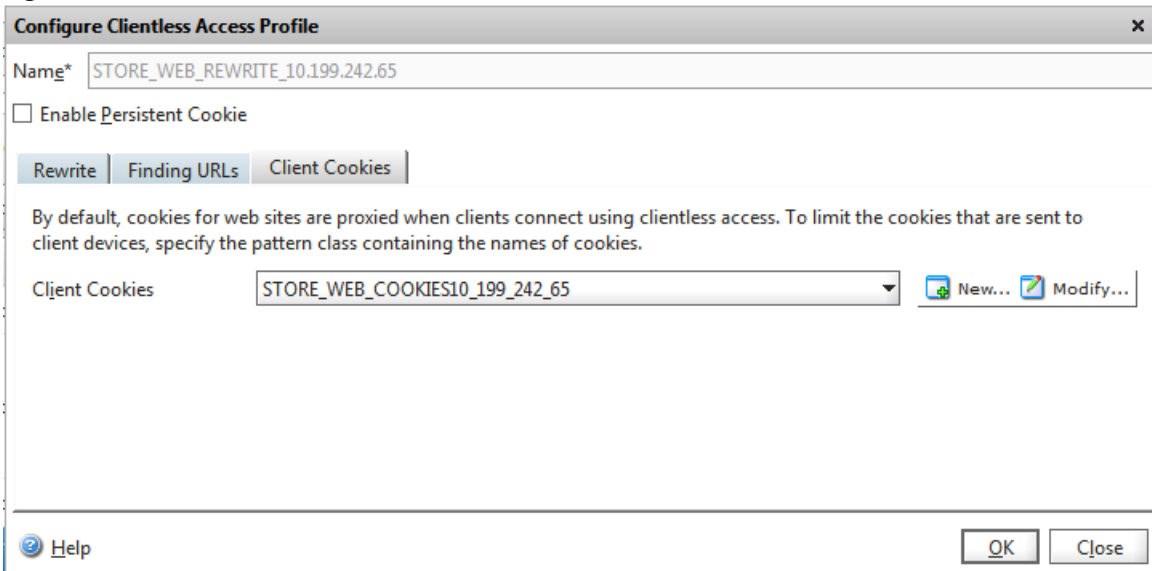
This policy contains the URL rewrite label ns\_cvpn\_default\_inet\_url\_label.

Figure 3. Clientless Access Profile URL Rewrite Label



The Receiver for Web profile also contains the cookie for StoreFront.

Figure 4. Client Cookies for Receiver for Web



The Quick Configuration wizard configures this pattern set for the StoreFront cookie.

Figure 5. Pattern Set for Client Cookies for Receiver for Web

Configure Pattern Set

Name\* STORE\_WEB\_COOKIES10\_199\_242\_65

Index type

Specify Pattern

Pattern

Treat back slash as escape character

Index

Charset

Add >

< Remove

Bound Patterns

| String                   | Index | Charset | Default |
|--------------------------|-------|---------|---------|
| CsrfToken                | 1     |         | No      |
| ASP.NET_SessionId        | 2     |         | No      |
| CtxsPluginAssistantState | 3     |         | No      |
| CtxsAuthId               | 4     |         | No      |

Help

OK

Close

# Configuring NetScaler Gateway and App Controller

Mar 25, 2014

To enable communication from user devices to the secure network, you need to configure settings in NetScaler Gateway and in App Controller. Citrix recommends running the Quick Configuration wizard to configure these settings, which include settings for App Controller and StoreFront.

When you run the wizard, NetScaler Gateway creates the virtual server and policies that are needed for user connections to App Controller. For more information about running the Quick Configuration wizard, see [Configuring Settings with the Quick Configuration Wizard](#). The Quick Configuration wizard configures the following policies automatically:

- Virtual server. When you configure a virtual server, you enable SmartAccess mode. When you enable SmartAccess mode (the default setting), this setting also enables clientless access. If users connect by using Receiver for Web, you must install a Universal license on NetScaler Gateway. If you do not install the Universal license, users cannot access Windows-based, web, SaaS, or mobile applications from Receiver for Web or Worx Home.
- Session policies bound to the virtual server. You create session policies in NetScaler Gateway. You can create the following four session policies:
  - Two session policies manage Receiver and Worx Home connections and web browser connections with Receiver for Web. When you configure the session policy for Receiver, and you want to allow users to connect with Worx Home for iOS, you can enable Secure Browse on the Security tab in the session profile
  - Optionally, if you deploy StoreFront, you can configure a third session policy that manages legacy PNA Services connections from Receiver for Android and Receiver for iOS. If you enable a session policy for PNA Services, users cannot use this connection method from Receiver for Windows.
  - A fourth session policy manages connections to applications and virtual desktops by using the NetScaler Gateway Plug-in. You can also configure Account Services that allows email-based discovery of the StoreFront or NetScaler Gateway web address.
- Authentication policies bound to the virtual server. You can configure LDAP and RADIUS authentication policies in NetScaler Gateway. If you use two-factor authentication, Citrix recommends using LDAP as the primary authentication policy and RADIUS as the secondary policy.
- Expressions. In each session policy, you configure expressions, or rules, that use the User-Agent header.
- Custom clientless access policy. You create a custom clientless access policy to control the rewriting of URLs and how cookies are proxied through NetScaler Gateway.
- Intranet Applications for Android Worx apps. If you enable split tunneling on NetScaler Gateway, when you configure the IP address routes for Android Worx apps, include the IP addresses of App Controller, the Exchange server (if you are using WorxMail), and all of the IP addresses of internal application web sites that users access from WorxWeb. Bind these settings to the virtual server on NetScaler Gateway.

## Configuring App Controller Settings

There are two steps for allowing connections to App Controller applications in the secure network through NetScaler Gateway. In App Controller, you:

- Configure NetScaler Gateway trust settings.
- Specify the application to accept connections from remote users.

To route user connections through NetScaler Gateway, you provide the following information:

- Name for the appliance. This can be any name you choose.

- Fully qualified domain name (FQDN) to which users connect, such as `https://NetScalerGatewayFQDN`.
- FQDN for the callback URL that verifies that the request came from NetScaler Gateway. You use the same FQDN to which users connect. App Controller appends the FQDN automatically with the authentication service URL. For example, the URL appears as `https://NetScalerGatewayFQDN/CitrixAuthService/AuthService.asmx`.

You can select the web applications that require remote user connections through NetScaler Gateway. When you configure an application in App Controller, you select a check box that identifies that the web application is hosted in the internal network. This adds the VPN keyword to the application and allows the connection request through NetScaler Gateway.

For more information about configuring App Controller, see [Configuring Connections to Applications Through NetScaler Gateway](#).

## Configuring StoreFront Settings

To support all access methods for users, you need to configure the following settings in StoreFront:

1. Authentication methods, which include the following settings:
  - User name and password
  - Domain pass-through
  - Pass-through from NetScaler Gateway
2. The Enable legacy support setting.
3. NetScaler Gateway settings, including:
  - NetScaler Gateway web address
  - Deployment mode
  - NetScaler Gateway mapped or subnet IP address
  - Logon type as Domain
  - Silent authentication by using the URL `https://<NetScalerGatewayFQDN>/CitrixAuthService/AuthService.asmx`, where NetScalerGatewayFQDN is the FQDN that is in the certificate bound to the virtual server.

If you configure two-factor authentication on NetScaler Gateway, when you configure the settings in StoreFront and you configure the Logon type, select Domain and security token.

# Configuring Session Policies and Profiles for App Controller and StoreFront

Feb 24, 2014

To allow connections through NetScaler Gateway from the different versions of Receiver and by using Worx Home, you need to create session policies and profiles for App Controller and StoreFront with specific rules to enable the connections to work. You can create separate session policies and profiles for the following:

- NetScaler Gateway Plug-in
- Receiver for Android
- Receiver for BlackBerry 10 1.0
- Receiver for BlackBerry 2.2
- Receiver for Chromebook
- Receiver for HTML5
- Receiver for iOS
- Receiver for Linux
- Receiver for Mac
- Receiver for Playbook 1.0
- Receiver for Windows 8/RT
- Receiver for Web
- Worx Home

When you configure the expression for Worx Home, Receiver for Windows, Receiver for Mac, or Receiver for Web, the User-Agent header always starts with CitrixReceiver. More recent versions of Receiver that recognize the native protocols in App Controller also include a header called X-Citrix-Gateway.

When you create a rule, you can use AND (&&) or OR (| |) to specify the condition for two configured expressions.

Important: Citrix recommends running the Quick Configuration wizard to configure all of the required policies for connections to App Controller and StoreFront from NetScaler Gateway. The following sections provide information about configuring the policies manually.

## Configuring Virtual Servers

If App Controller is part of your deployment, you need to create two virtual servers:

- The first virtual server is for users who connect by using Worx Home. After user authentication occurs, this virtual server communicates directly with App Controller.
- The second virtual server is users who connect by using Receiver for Web, Citrix Receiver for Windows, or Citrix Receiver for Mac. Receiver communicates directly with StoreFront, instead of the App Controller, after NetScaler Gateway authenticates users.

On each NetScaler Gateway virtual server, you must install a server certificate that has a unique fully qualified domain name.

## Configuring Session Policies

You configure session policies for App Controller and StoreFront deployments. You can use the same policy expressions for both deployments, however the session profile settings are slightly different. The session policy expressions you configure depend on the version of Receiver and the NetScaler Gateway Plug-in you are using.



Some versions of Receiver do not fully support the StoreFront services protocols that allow direct connections through NetScaler Gateway to stores in StoreFront. The earlier Receiver versions that do not support these protocols include:

- Receiver for Windows 3.0 and earlier versions
- Receiver for Mac 11.4 and earlier versions
- Receiver for Android 3.0 and earlier versions
- Receiver for iOS 5.5 and earlier version

The following table shows the policy expression to configure based on the version of Receiver and the NetScaler Gateway Plug-in you are using :

|  |  |
|--|--|
| Receiver version does not support StoreFront services protocols                | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver &&<br>REQ.HTTP.HEADER X-Citrix-Gateway NOTEXISTS    |
| Worx Home or Receiver version supports StoreFront services protocols           | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver &&<br>REQ.HTTP.HEADER X-Citrix-Gateway EXISTS       |
| NetScaler Gateway Plug-in for Windows<br><br>NetScaler Gateway Plug-in for Mac | REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver &&<br>REQ.HTTP.HEADER Referer NOTEXISTS          |
| Receiver for Web   | REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver &&<br>REQ.HTTP.HEADER Referer EXISTS             |
| Receiver for Windows 8/RT  | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver &&<br>REQ.HTTP.HEADER User-Agent CONTAINS WindowsRT |

When you configure the policy expression for Receiver versions, you can distinguish between the Receiver type in the policy expression.

|                             |   |
|-----------------------------|---|
| Receiver for Android        | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Android/    |
| Receiver for BlackBerry 2.2 | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Blackberry/ |
| Receiver for Chromebook     | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Chromebook/ |
| Receiver for HTML5          | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS HTML5/      |

|                                |  |
|--------------------------------|--|
| Receiver for iOS               | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS iOS/         |
| Receiver for Linux             | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Linux/       |
| Receiver for Mac               | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS MacOSX/      |
| Receiver for Playbook 1.0      | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Playbook/    |
| Receiver for Windows 8/RT. 1.3 | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Win8/        |
| Receiver for Windows           | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Windows/     |
| Receiver for Windows Phone 8   | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS WindowsPhone |
| Worx Home                      | REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER User-Agent CONTAINS Windows/     |

If you configure a session policy that supports StoreFront services protocols and Receiver for iOS, the expression might look like the following:

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS && REQ.HTTP.HEADER User-Agent CONTAINS iOS/

#### To configure expressions in session policies

When you configure the expression for a session policy, use the following guidelines. You can use this procedure for App Controller and StoreFront deployments.

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.  
Note: To modify a session policy, in the details pane, select the policy and then click Open.
3. In the Create NetScaler Gateway Session Policy dialog box, select Advanced Free-Form and then click Add.
4. In the Add Expression dialog box, use the following parameters as a guideline for the expression:
  1. In Expression Type, select General.
  2. In Flow Type, select REQ.
  3. In Protocol, select HTTP.
  4. In Qualifier, select Header.

5. In Operator, select CONTAINS, NOTCONTAINS, EXISTS, or NOTEXISTS depending on the expression.
  6. In Value, type the parameter, such as CitrixReceiver.
  7. In Header Name, type User-Agent and then click OK.
5. After you save the first expression, click And in the Create NetScaler Gateway Session Policy dialog box to add && to the expression and then click Add.
  6. Repeat Step 2 to configure the second rule.
  7. When you finish adding the rules, click Create and then click Close.

## Configuring Session Profiles

When you configure session profiles for use with a session policy, you need to configure parameters that are specific for the type of connection the profile supports.

If the StoreFront IP address is a public IP address and if you disable split tunneling in the session profile, SSO functionality is internally disabled on NetScaler Gateway. Users receive an access denied error message when they attempt to log on to StoreFront. You must enable split tunneling to allow SSO from a public IP address.

When you finish configuring the policy and profile, you then bind the session policy to the virtual server. You also need to assign a priority number for each session policy.

The session profiles you configure have different settings for App Controller and StoreFront. For more information, see the topics for App Controller and StoreFront later in this section.

# Configuring Access to App Controller Through NetScaler Gateway

May 29, 2013

You can configure session policies to allow users to connect to App Controller. Users can access applications hosted on App Controller and documents stored in ShareFile.

You can configure the following session profiles that allow user access to App Controller through NetScaler Gateway:

- Citrix Receiver
- Receiver for Web
- PNA Services
- NetScaler Gateway Plug-in

When you configure the session profile for App Controller, configure the virtual server for SmartAccess to allow user connections with the NetScaler Gateway Plug-in.

Note: Citrix recommends using the Quick Configuration wizard to configure these settings. When you run the wizard, NetScaler Gateway configures the session policies for App Controller automatically.

# Creating the Session Profile for Receiver for App Controller

Feb 07, 2014

When you configure session policies and profiles for Receiver or Worx apps to connect to App Controller, you configure expressions within the session policies. The User-Agent header must always start with "CitrixReceiver." Receiver versions that recognize StoreFront services protocols must also include a header called X-Citrix-Gateway when accessing the native StoreFront service interfaces.

Note: Citrix recommends using the Quick Configuration wizard to configure these settings. For more information, see [Configuring Settings with the Quick Configuration Wizard](#).

If your deployment contains App Controller and NetScaler Gateway only or the deployment contains StoreFront, App Controller, and NetScaler Gateway, you need to configure the App Controller web address as the home page on the Client Experience tab and in the Web Interface address on the Published Applications tab.

To configure the session profile for Receiver or Worx apps

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. Click the Client Experience tab and then do the following:
  1. Next to Split Tunnel, select Override Global and then click ON.  
Configure this option to allow Worx Home, WorxMail, and WorxWeb for Android and iOS to use Micro VPN to connect through NetScaler Gateway. You also need to do the following:
    - Configure transparent interception. For details, see [Configuring Intranet Applications for the NetScaler Gateway Plug-in](#).
    - Configure split DNS settings to support DNS queries. For details, see [Supporting DNS Queries by Using DNS Suffixes for Android Devices](#).
  2. Next to Clientless Access, select Override Global and then click On.
  3. Next to Clientless Access URL Encoding, select Override Global and then click Clear.
  4. Next to Single Sign-on to Web Applications, select Override Global and then select the check box Single Sign-on to Web Applications.
7. Click the Published Applications tab and then configure the following settings:
  1. Next to Single Sign-on Domain, select Override Global and then enter the domain name. . For example, enter mydomain
  2. Next to Account Services Address, select Override Global and then enter the StoreFront URL.  
For example, enter https://<StoreFrontFQDN>.
8. Click Create.

After you create and close the session profile, create the expression for the session policy in the Create NetScaler Gateway Session Policy dialog box.

# Creating the Session Profile for Receiver for Web for App Controller

Feb 07, 2014

Users connect to Receiver for Web by using clientless access. When users connect by using a web browser and successfully log on, they can access or subscribe to their published applications.

If users connect to StoreFront by using clientless access, they need to download a provisioning file from the Receiver for Web page. Users can also import the provisioning file you provide by email or a USB flash drive. Settings within the provisioning file detect if users log on from within the internal network or from a remote location. If users connect from a remote location, the connection routes through NetScaler Gateway.

If your deployment contains App Controller and NetScaler Gateway only, or contains App Controller, StoreFront, and NetScaler Gateway, you need to configure the App Controller web address as the home page on the Client Experience tab and the Web Interface address on the Published Applications tab.

## To create the session profile for Receiver for Web

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 Name, type a name for the policy.
  4. Next to Request Profile, click New.
  5. In Name, type a name for the profile.
  6. Click the Client Experience tab and then do the following:
    1. In Home Page, click Override Global, and then type the web address for App Controller or Storefront.  
For example, enter `https://<StoreFrontFQDN>/Citrix/<StoreWebName>/where`  
— *StoreFrontFQDN*  
— *StoreWebName*  
is the fully qualified domain name (FQDN) of Storefront and  
is the name of the store.

Note: The web address is case sensitive. For example, use `https://<App ControllerFQDN>/Citrix/StoreWeb`.
  2. In Clientless Access, click Override Global and then select On.
  3. In Clientless Access URL Encoding, click Override Global and then select Clear. You can also select Obscure or Encrypt as the URL encoding for Receiver for Web. If users connect by using Receiver for Web from an iOS device, you must select Clear.
  4. Next to Single Sign-on to Web Applications, click Override Global and then select the check box for Single Sign-on to Web Applications.
7. On the Published Applications tab, do the following:
    1. Next to ICA Proxy, click Override Global, and then select OFF.
    2. Next to Web Interface Address, click Override Global and then enter the web address for App Controller or StoreFront.

3. In Single Sign-on Domain, type the domain name.  
For example, type mydomain.

8. Click Create.

# Creating the Session Profile for PNA Services for App Controller

Feb 07, 2014

If users connect with Receiver versions that do not support the StoreFront services protocol, you can configure a session policy for PNA Services. You can configure this session policy for the following Receiver versions:

- Receiver for Mac 11.4 and earlier versions
- Receiver for Android 3.0 and earlier versions
- Receiver for iOS 5.5 and earlier version

Important: User connections with any version of Receiver for Windows is not supported with PNA Services.

When you configure the session profile for PNA Services, you must enable single sign-on (SSO) in order to use ICA proxy.

PNA services do not support SSO, so you need to use the complete URL for the PNA site as the Web Interface home page.

When you enable PNA legacy support in StoreFront, make sure to specify the server URL on the StoreFront server when entering the Web Interface address in the session profile. You can also enter the Web Interface XenApp Services site of an existing XenApp or XenDesktop farm.

## To create the session profile for PNA Services

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 Name, type a name for the profile.
4. Click the Client Experience tab, and next to Single Sign-on to Web Applications, click Override Global and then select the check box for Single Sign-on to Web Applications.
5. Click the Published Applications tab and then do the following:
  1. Next to ICA Proxy, click Override Global, and then select ON.
  2. In Web Interface Address, click Override Global, and then type the web address for StoreFront.

For example, enter `https://<`

`— StoreFrontFQDN`

`>/Citrix/<`

`— StoreName`

`/PNAgent` where

`— StoreFrontFQDN`

is the fully qualified domain name (FQDN) of StoreFront and

`— StoreName`

is the name of the store.

6. Click Create.

After you close the session profile, you then create the rule for the policy.



# Creating a Session Policy and Profile for the NetScaler Gateway Plug-in

Feb 07, 2014

You can configure NetScaler Gateway to provide users access to published applications and virtual desktops with the NetScaler Gateway Plug-in instead of with Receiver. Then, in the session policy, you add an HTTP header rule for the NetScaler Gateway Plug-in.

To create the session policy rule for the NetScaler Gateway Plug-in

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 the Create NetScaler Gateway Session Policy dialog box, next to Match Any Expression, click the down arrow, select Advanced Free-Form and then click Add.
4. In the Add Expression dialog box, do the following:
  1. In Expression Type, click General.
  2. In Flow Type, select REQ.
  3. In Protocol, select HTTP.
  4. In Qualifier, select Header.
  5. In Operator, select NOTEXISTS.
  6. In Header Name, type Referer and then click OK.
5. Click Create and then click Close.

If users install the following versions of Receiver, you need to configure the following session profile for the NetScaler Gateway Plug-in:

- Receiver for Windows 3.4
- Receiver for Windows 8/RT 1.3
- Receiver for Mac 11.7
- Receiver for iOS 5.7
- Receiver for Android 3.3

To configure the session profile for the NetScaler Gateway Plug-in

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 Name, type a name for the profile.
4. Click the Client Experience tab and then do the following:
  1. Next to Single Sign-on to Web Applications, click Override Global and then select the check box. This setting is required to allow single sign-on for desktop versions of Receiver and uses an NetScaler Gateway Plug-in cookie.
  2. Next to Clientless Access URL Encoding, click Override Global and then select Clear.  
Important: Set Clientless Access to Off.
5. Click the Published Applications tab and then configure the following settings:
  1. Next to Single Sign-on Domain, click Override Global, enter the domain name and then click Create. For example, enter mydomain.

2. Next to Account Services Address, click Override Global and then enter the StoreFront URL.  
For example, enter `https://<StoreFrontFQDN>`.

This setting is needed for adding accounts if both Receiver and the NetScaler Gateway Plug-in are already installed on the user device.

# Access to StoreFront Through NetScaler Gateway

Feb 26, 2014

You can configure session policies to allow users to connect to StoreFront. Users can access published applications from XenApp and virtual desktops from XenDesktop through Citrix StoreFront.

You can configure the following session profiles that allow user access to StoreFront through NetScaler Gateway:

- Citrix Receiver
- Receiver for Web
- PNA Services

When you configure the session profile for StoreFront, configure the virtual server for Basic mode. This allows users to access StoreFront through connections from one of the software types in the preceding list. When users connect, they use an ICA connection instead of the full VPN tunnel with the NetScaler Gateway Plugin.

When you configure the session profile, you select the NetScaler Gateway Plug-in for Java instead of the NetScaler Gateway Plug-in for Windows or Mac OS X. When you select the Java plug-in, it restricts the connection to using the ICA protocol.

Note: Citrix recommends using the Quick Configuration wizard to configure these settings. When you run the wizard, NetScaler Gateway configures the session policies for StoreFront automatically with the correct settings.

# Creating the Session Profile for Receiver or Worx Home for StoreFront

Feb 27, 2014

When you configure session policies and profiles for Receiver or Worx Home to connect to StoreFront, you configure expressions within the session policies. The User-Agent header must always start with CitrixReceiver. Receiver versions that recognize StoreFront services protocols must also include a header called X-Citrix-Gateway when accessing StoreFront service interfaces. In this scenario, App Controller is not part of the deployment. When you configure the settings, you select the NetScaler Gateway Plug-in for Java, instead of the plug-in for Windows or Mac. This allows user connections by default to Receiver.

Note: Citrix recommends configuring these settings by using the Quick Configuration wizard. For more information, see [Configuring Settings with the Quick Configuration Wizard](#).

You need to configure the StoreFront web address as the home page on the Client Experience tab and as the Web Interface address on the Published Applications tab.

To configure the session profile for Receiver

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 Name, type a name for the profile.
4. Click the Security tab and in Default Authorization Action, click Override Global, and then select ALLOW.
5. Click the Client Experience tab and then do the following:
  1. Next to Plug-in Type, click Override Global and then select Java.
  2. Next to Single Sign-on to Web Applications, click Override Global and then select the check box Single Sign-on to Web Applications.
  3. Next to Clientless Access, click Override Global and then select Off.
6. Click the Published Applications tab and then configure the following settings:
  1. Next to ICA Proxy, click Override Global, and then select ON.
  2. Next to Single Sign-on Domain, click Override Global, enter the domain name and then click Create. For example, enter mydomain.
  3. In Web Interface Address, click Override Global, and then type the web address for StoreFront. For example, enter *— https://storefront.t.com/Citrix/StoreWeb*

Note: When you configure the StoreFront URL in NetScaler Gateway, such as https://<SFLite-FQDN>/Citrix/StoreWeb, the text StoreWeb is case sensitive.

7. Click Create.

After you create and close the session profile, add the profile and create the expression for the session policy in the Create NetScaler Gateway Session Policy dialog box.

# Creating the Session Profile for Receiver for Web for StoreFront

Feb 07, 2014

Users connect to Receiver for Web by using clientless access. When users connect by using a web browser and successfully log on, they can access or subscribe to their published applications.

If users connect to StoreFront by using clientless access, they need to download a provisioning file from the Receiver for Web page. Users can also import the provisioning file that you give them in email or with a USB flash drive. Settings within the provisioning file detect if users log on from within the internal network or from a remote location. When remote users log on by using Receiver for Web, the connection routes through NetScaler Gateway, however users cannot use the NetScaler Gateway Plug-in to establish the connection. When you configure the virtual server, configure Basic mode.

To create the session profile for Receiver for Web

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 Name, type a name for the profile.
  4. Click the Client Experience tab and then do the following:
    1. In Clientless Access, click Override Global and then select Allow.
    2. In Single Sign-on to Web Applications, click Override Global and then select the check box.
  5. On the Published Applications tab, do the following:
    1. Next to ICA Proxy, click Override Global, and then select ON.
    2. Next to Web Interface Address, click Override Global and then enter the web address (URL) for StoreFront.  
Note: The StoreFront URL is case sensitive, such as `https://<StoreFrontFQDN>/Citrix/<StoreWebName>/`. If the case is incorrect, when users log on, they receive the following error:  
Http/1.1 Gateway Timeout  
  
Unable to find the requested server or DNS Error.
  3. In Single Sign-on Domain, type the domain name.  
For example, type mydomain.
6. Click Create.

# Creating the Session Policy for PNA Services for StoreFront

Feb 07, 2014

If users connect with Receiver versions that do not support the StoreFront services protocol, you can configure a session policy for PNA Services. You can configure this session policy for the following Receiver versions:

- Receiver for Mac 11.4 and earlier versions
- Receiver for Android 3.0 and earlier versions
- Receiver for iOS 5.5 and earlier version

Important: User connections with any version of Receiver for Windows are not supported with PNA Services. When you configure the session profile for PNA Services, you must enable single sign-on (SSO) in order to use ICA proxy. PNA services do not support SSO, so you need to use the complete URL for the PNA site as the Web Interface home page. When you enable PNA legacy support in StoreFront, make sure to specify the server URL on the StoreFront server when entering the Web Interface address in the session profile. You can also enter the Web Interface XenApp Services site of an existing XenApp or XenDesktop farm.

Note: Citrix recommends running the Quick Configuration wizard to configure the policies for StoreFront. To create the session profile for PNA Services

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 Name, type a name for the profile.
4. Click the Client Experience tab, and next to Single Sign-on to Web Applications, click Override Global and then select the check box for Single Sign-on to Web Applications.
5. Click the Published Applications tab and then do the following:
  1. Next to ICA Proxy, click Override Global, and then select ON.
  2. In Web Interface Address, click Override Global, and then type the Web address for StoreFront.  
For example, enter `https://<StoreFrontFQDN>/Citrix/<StoreName>/PNAgent` where `<StoreFrontFQDN>` is the fully qualified domain name (FQDN) of StoreFront.
6. Click Create.

After you close the session profile, you then create the rule for the policy.

# Connecting to StoreFront by Using Email-Based Discovery

Feb 07, 2014

You can configure NetScaler Gateway to accept user connections by using an email address to discover the StoreFront or NetScaler Gateway URL. The process for user connections is:

- When users connect from inside your network or a remote location and install Receiver for the first time, they enter their email address or the StoreFront URL.
- Receiver then queries the appropriate DNS server, which responds with the StoreFront or NetScaler Gateway URL. The URL depends on whether users connect from the internal network or they connect from a remote location.
- Users then log on to Receiver with their user name, password, and domain.
- If users connect from a remote location, NetScaler Gateway provides the StoreFront URL to Receiver.
- Receiver gets the account information from StoreFront. If users connect through NetScaler Gateway, the appliance performs SSO to StoreFront. If more than one account is available, users receive a list of accounts from which to choose.
- When users log on to an account, a list of applications appear in Receiver. Users can then select an app to open.

To allow users to connect to their apps by using an email address, you need to do the following:

1. Add a service record (SRV) to your DNS server to support email-based discovery. For more information, see [Configuring Email-Based Account Discovery](#) in the StoreFront documentation.
2. Add the StoreFront URL to NetScaler Gateway.

In NetScaler Gateway, you can configure StoreFront URL from the following locations:

- Quick Configuration wizard
- Global settings
- Session policy

Note: Citrix recommends running the Quick Configuration wizard to configure the session policies and profiles for email-based discovery. The wizard configures the correct policy and profile settings that enables this feature.

You configure the StoreFront URL on the Published Applications tab in the session profile or in global settings. In the Quick Configuration wizard, you configure the StoreFront URL on the XenApp / XenDesktop tab. For more information about configuring NetScaler Gateway with the Quick Configuration wizard, see [Configuring Settings with the Quick Configuration Wizard](#).

To configure email-based discovery globally

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. On the Published Applications tab, in Account Services Address, enter the StoreFront URL and then click OK.

To configure email-based discovery in a session profile

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, click the Profiles tab and then do one of the following:
  1. Select an existing session profile and then click Open.
  2. Click Add to create a new profile.
3. On the Published Applications tab, in Account Services Address, click Override Global and then enter the StoreFront URL.

4. Do one of the following:

1. Click OK if you modified a session profile.
2. Click Create if you are adding a new session profile.



# Binding Session Policies and Setting the Priority

Feb 07, 2014

After you configure session policies for StoreFront or App Controller integration, you can bind the policies to a user, group, virtual server, or globally. Session policies are applied as a hierarchy in the following order:

- Users
- Groups
- Virtual servers
- Globally

If you configure two or more session policies for Receiver for Windows and Receiver for Mac, Receiver for Web, and the NetScaler Gateway Plug-in, you bind the policies and then you need to set the priority number for each policy.

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.

The Program Neighborhood Agent session policy receives the lowest priority number and the NetScaler Gateway Plug-in session policy receives the highest priority number. Citrix recommends setting the session policies in the following order to ensure that any change to the User-Agent header does not affect user connections:

- Program Neighborhood Agent session policy
- Receiver for Web
- Receiver for Windows and Receiver for Mac
- NetScaler Gateway Plug-in

For more information about binding session policies, see [Binding Session Policies](#).

To set the priority of a session policy

1. In the configuration utility, on the Home tab, click Create New NetScaler Gateway.
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 Session.
4. Next to the session policy, under Priority, enter the priority number and then click OK.

# Configuring Custom Clientless Access Policies for Receiver

Aug 12, 2014

You can configure a custom clientless access policy for the following versions of Citrix Receiver, which support StoreFront services protocols:

- Receiver for Android
- Receiver for Chromebook
- Receiver for iOS
- Receiver for Linux
- Receiver for Mac
- Receiver for Windows

If you create clientless access policies for Receiver and Receiver for Web, you must bind the Receiver policy to the virtual server before you bind the Receiver for Web policy. When you bind the Receiver policy, set a lower priority number to make sure that this policy takes precedence over the Receiver for Web policy.

## To configure a clientless access policy for Receiver

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies and then click Clientless Access.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Under Expression, type `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver") && HTTP.REQ.HEADER("X-Citrix-Gateway").EXISTS .`
5. Next to Profile, click New.
6. In Name, type a name for the profile.  
Important: Do not change any settings in the profile.
7. Click Create two times and then click Close.

# Configuring Custom Clientless Access Policies for Receiver for Web

Feb 07, 2014

You can configure custom clientless access policies on NetScaler Gateway for user connections with Receiver for Web by adhering to the following guidelines:

- Receiver requires that StoreFront XML traffic cannot be rewritten, which would occur when users connect to NetScaler Gateway with clientless access.
- App Controller requires the rewriting of HTML traffic.
- Receiver for Web requires that certain cookies are not proxied through NetScaler Gateway.

If you create clientless access policies for Receiver and Receiver for Web, bind the Receiver policy to the virtual server before you bind the Receiver for Web policy. When you bind the Receiver policy, set a lower priority number to make sure that this policy takes precedence over the Receiver for Web policy.

## To configure a clientless access policy for Receiver for Web

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies and then click Clientless Access.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Under Expression, type true.
5. Next to Profile, click New.
6. In Name, type a name for the profile.
7. On the Rewrite tab, in URL Rewrite, select ns\_cvpn\_default\_inet\_url\_label.
8. On the Client Cookies tab, next to Client Cookies, click New.
9. In the Configure Pattern Set dialog box, under Specify Pattern, in Pattern, add the following cookies in this order:
  1. Enter the value Csrftoken and then click Add.
  2. Enter the value ASP.NET\_SessionId and then click Add.
  3. Enter the value CtxsPluginAssistantState and then click Add.
  4. Enter the value CtxsAuthId and then click Add.
10. Click Create three times and then click Close.

## To bind a clientless access policy to a virtual server

After you create the custom clientless access policy, bind the policy 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. Next to a policy, under Priority, type the number and then click OK.

# Using WebFront to Integrate with StoreFront

Jul 28, 2015

## Overview

WebFront is a Web Application hosted on a Tomcat Container that runs on NetScaler. WebFront provides optimization and improved performance for users accessing StoreFront through Gateway using Client Browsers and Citrix Native Receivers. WebFront coexists with the Web Interface on NetScaler.

WebFront provides the following functionalities:

- Receiver for Web Proxy
- Transparent SSO

## Receiver for Web Proxy

Receiver for Web Proxy (RfWeb) provides a way for web browsers to communicate with a store in StoreFront. Functionally, it is the same as RfWeb in StoreFront with a few optimizations like caching and packet flow optimization.

### Features

For users accessing through browsers (ReceiverforWeb Proxy):

- StoreFront's RfWeb feature on NetScaler
- Caches Static content and StoreFront served icons
- Optimized packet flow for Apps/Desktop enumeration.
- Supports HTML5 Receiver

## Transparent Single Sign On (SSO)

Native Citrix Receivers currently require a minimum of 12 HTTP transactions with StoreFront to perform resource enumeration. Along with this, an authentication token size of 4K is carried along with each HTTP request. WebFront optimizes this by reducing the number of transactions from 12 to 2 and prevents the sending of the token by proxy.

### Features

For users accessing through Citrix Native Receivers (Transparent SSO):

- Caches StoreFront served icons
- Optimized packet flow for Apps/Desktop enumeration (Data transferred over WAN reduced b1%)
- Entire Authentication to SF is delegated to WebFront

### Note

The native ICA traffic does not flow via WebFront.

# Functionality

## Receiver for Web Proxy

The RfWeb Proxy used with the Tomcat Web Server serves static content (HTML, CSS, JS, Static Icons, etc.) to web browsers and provides the following services:

- Lists all applications in the store. The information returned is in JSON format.
- Gets information for an application specified by the application ID. The information returned is in JSON format.
- Gets an application icon specified by the icon ID. Icons are returned in PNG format.
- Gets the launch information for a given HDX application specified by the application ID. The response is in the form of an ICA file.
- Supports launching web/SaaS apps.
- Powers off desktops.
- Assigns desktops.
- Subscribes to a given application specified by the application ID and the position in the subscribed application list.
- Unsubscribes a given application specified by the application ID.
- Updates subscription position for a given application specified by the application ID.

In the Workspace Control the following actions are performed:

- Lists available sessions (includes active sessions)
  - Launches sessions
  - Disconnects user sessions
  - Logs off user sessions
1. Performs Single Sign On (SSO) with StoreFront using credentials from Gateway, and stores the token in the Tomcat Session cache for reuse for subsequent requests.
  2. Supports the ICA apps launch through the HTML5 Receiver client.

## Icon and Static content caching

Icon and static content caching: This is done using Integrated Caching feature of NetScaler. This does not require an IC license; only a VPN license is sufficient.

## Transparent SSO

Transparent SSO (single sign on) is applicable only for native Citrix Receivers.

WebFront is designed as a Java Webapp, which runs on the Tomcat v6, hosted on NetScaler. WebFront is developed using Spring MVC v3.1.2. WebFront is designed to work via Gateway with SSO on ONLY.

# Installing and Configuration WebFront Using the WebFront Wizard

## Install WebFront

1. Go to System>WebFront. Select Install WebFront from the Getting Started heading.

2. Get the JRE TAR files for installation. Select the Download JRE link at the bottom of the page for the JRE TAR file.
3. For the WebFront tar ball, go to <https://www.citrix.com/downloads/netscaler-gateway/components/components-for-netscaler-gateway-110.html>

### Install WebFront

WebFront TAR File Path\*

**3**

JRE Tar File Path\*

Download JRE **2**

4. Select WebFront on NetScaler Gateway 11.0 Download button.

Home / Downloads / NetScaler Gateway / Components / Components for NetScaler Gateway 11.0

## Components for NetScaler Gateway 11.0

Release Date: Jun 30, 2015

Find Downloads

NetScaler Gateway

or

Search Downloads

Support Resources

- eDocs
- Knowledge Center
- Support Forums
- More...

WebFront

**WebFront on NetScaler Gateway 11.0**

Jun 30, 2015  
105 MB - (.TAR) [Download](#)

Web Interface

Insight Center

5. Read the Download Agreement and check the box stating your compliance. Then, click the **Accept** button.

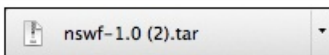
### Download Agreement

Export Controls. You are advised that this software is subject to U.S. Export Administration Regulations. You shall not export, re-export, import or transfer this Software contrary to U.S. or other applicable laws, whether directly or indirectly, and you shall not assist or facilitate others in doing any of the foregoing. You represent and warrant that (a) neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked, or denied your export privileges, and (b) you are not located , a resident of, or a citizen of, Cuba, Iran, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods. You agree not to use or transfer the Software for end use relating to any nuclear, chemical, biological weapons or missile technology unless authorized by the U.S. Government by regulation or specific license. You acknowledge it is your responsibility to comply with any and all export and import laws and that Citrix Corp has no further responsibility after the initial distribution to you within the original country of distribution.

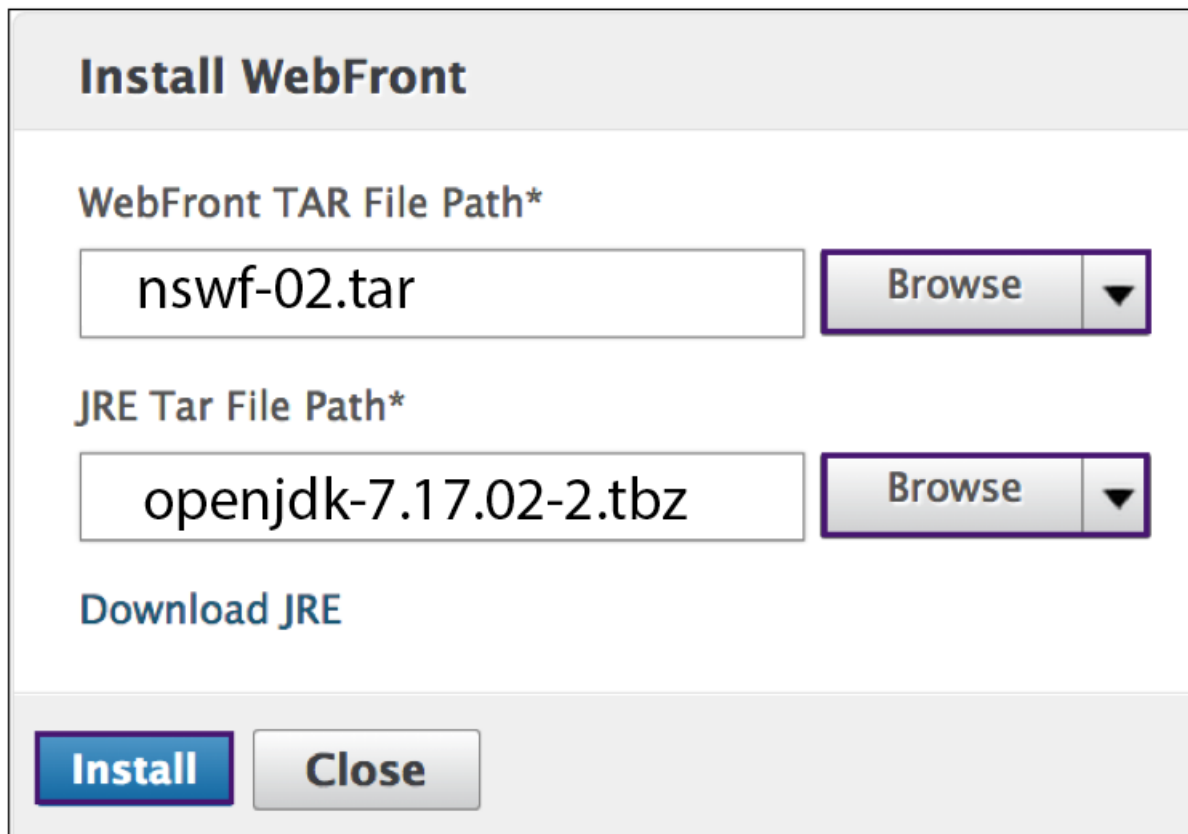
I have read and certify that I comply with the above Export Control Laws.

[Accept](#)

6. See the WebFront TAR file in the left hand corner.



7. From the WebFront Browse button, select **Local**. Then, select the WebFront TAR file. From the JRE **Browse** button, select **Local**. Then, select the JRE TAR file. Click **Install**.

A screenshot of the 'Install WebFront' dialog box. The title bar says 'Install WebFront'. There are two sections: 'WebFront TAR File Path\*' with a text box containing 'nswf-02.tar' and a 'Browse' button with a dropdown arrow; and 'JRE Tar File Path\*' with a text box containing 'openjdk-7.17.02-2.tbz' and another 'Browse' button with a dropdown arrow. Below these is a link 'Download JRE'. At the bottom are two buttons: 'Install' and 'Close'.

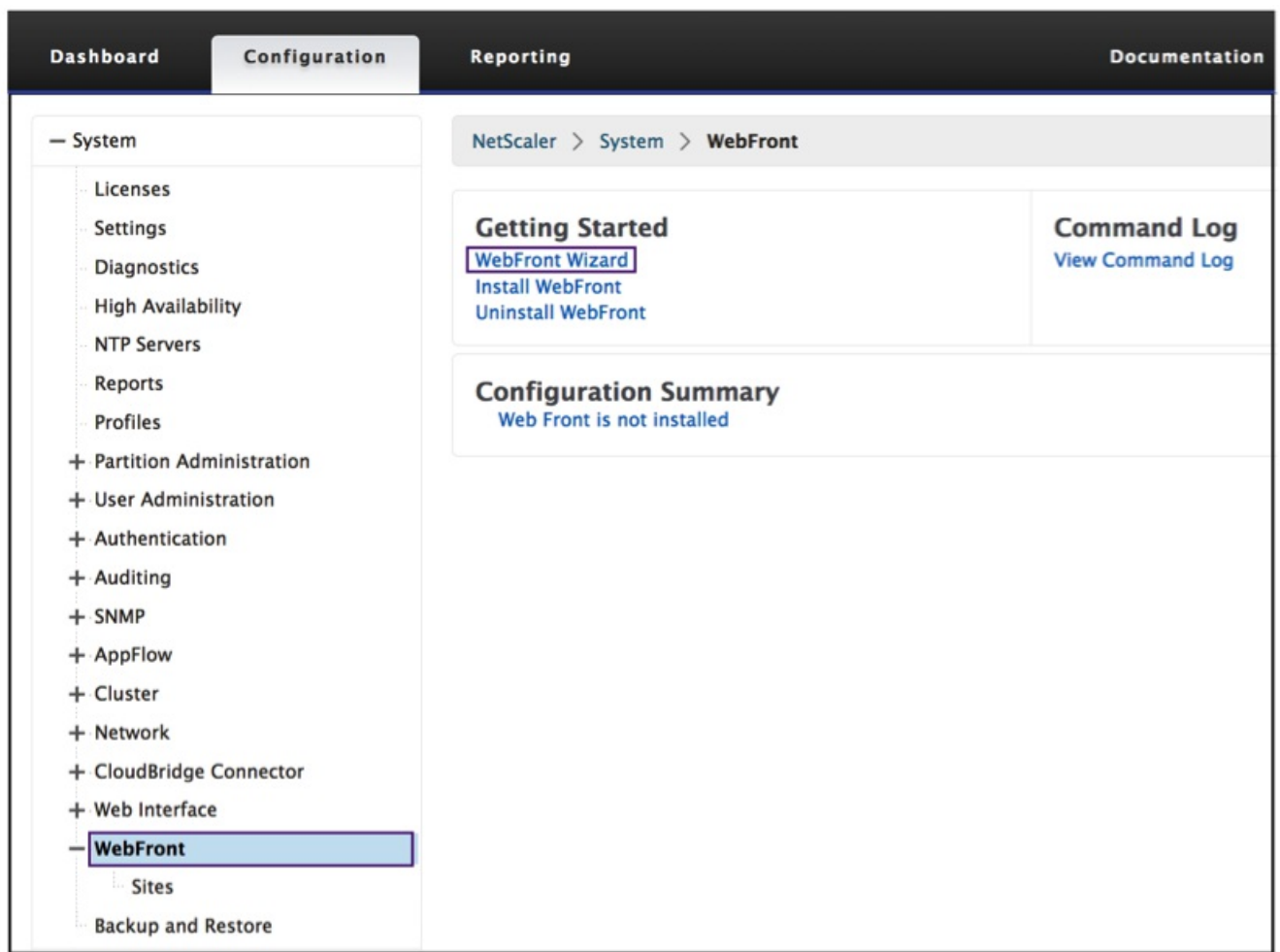
The following screen confirms that the installation was completed successfully.



## WebFront Wizard

1. Go to System>WebFront. Select **WebFront Wizard** from the Getting Started heading.





2. The following screen appears. The fields with asterisks are mandatory. Enter mandatory information and Click Continue.

- See [NetScaler Gateway Virtual Server information](#) for details.
- See [Trust SSL Certificate](#) for details.

3. Complete all mandatory fields. Verify and click **Continue**.

4. Verify data and click **Done**.

# NetScaler Gateway Virtual Server

This section describes the options to select a NetScaler Gateway Virtual Server.

1. Select a virtual server that is already configured for your device. See [Select a Configured Virtual Server](#) for more information.
2. Configure a new virtual server. See [Configured Virtual Server](#) for more information.

## Select a Configured Virtual Server

1. Select a configured virtual server from the pull-down menu.

## Configure a Virtual Server

1. Specify the NetScaler Gateway IP Address.
2. Specify the port.
3. Assign the virtual server a name.
4. Check this box to enables NetScaler Gateway to redirect HTTP connections to an HTTPS secure connection.
5. Click the **Continue** button.

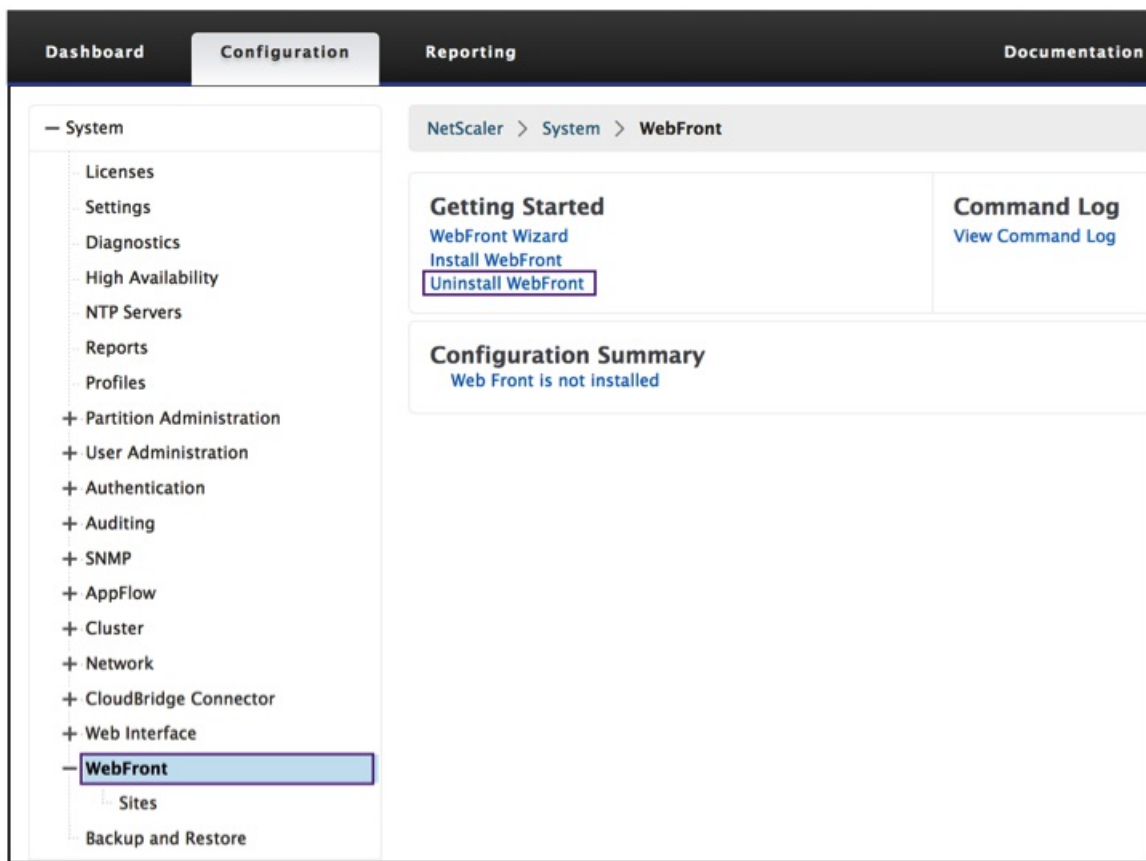
## Trust SSL Certificate

By selecting the **Browse** button, you can select a certificate from the appliance or from your local directory.

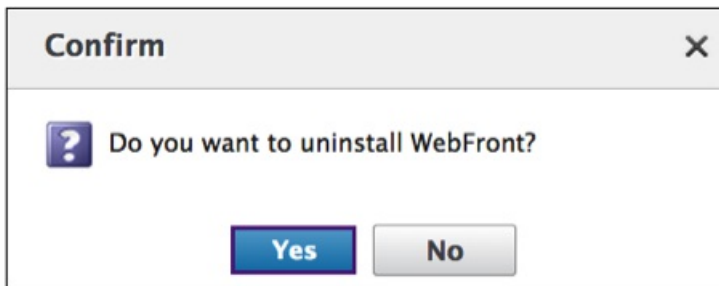
1. From the appliance, select a certificate from the list and click **Open**.

# Uninstall WebFront

1. Go to System>WebFront. Select **Uninstall WebFront** from the Getting Started heading.

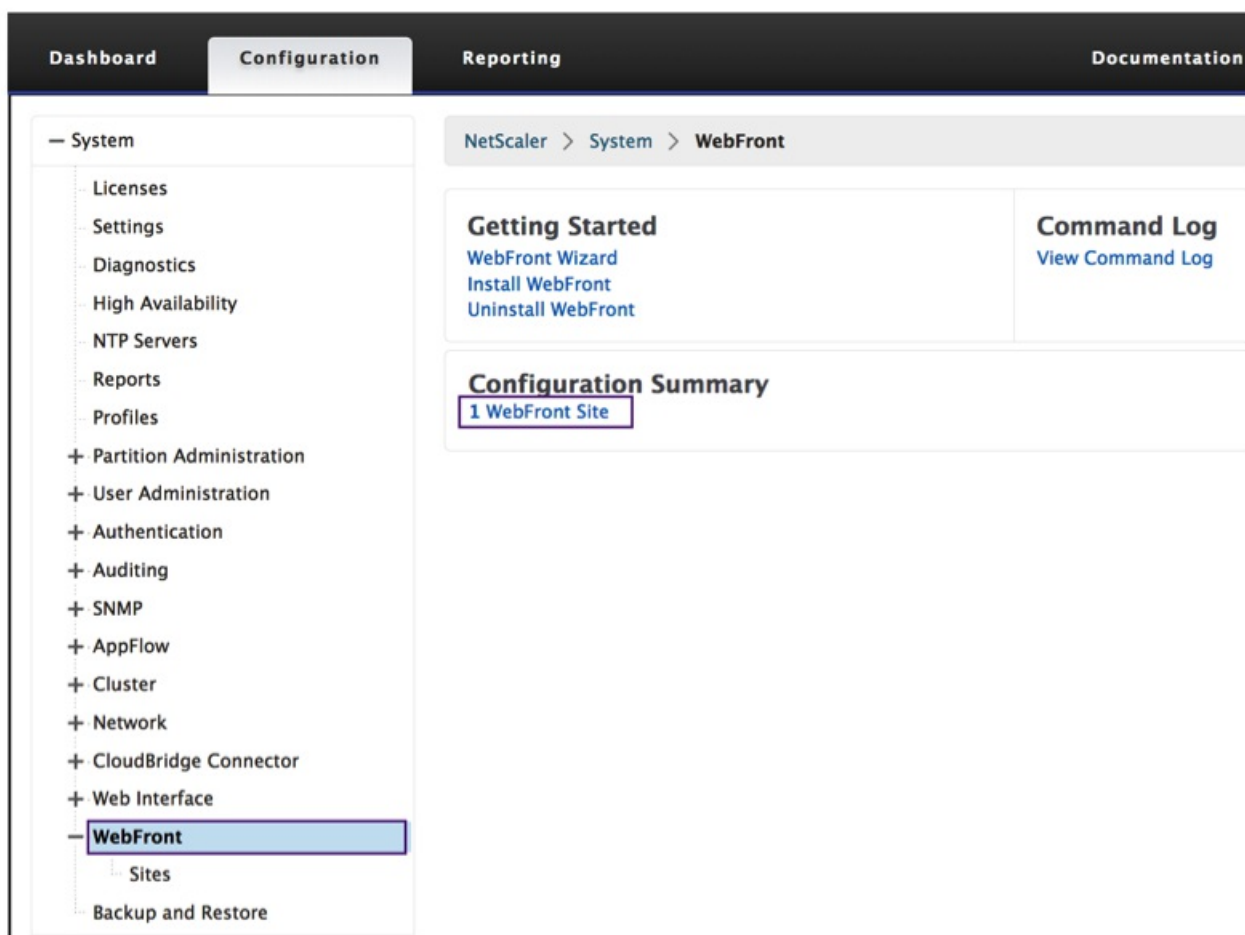


2. Click **Yes**.



Configure WebFront Sites

1. Go to System>WebFront. Select **WebFront Sites** from the Configuration Summary.



2. The WebFront Sites allows the following the site operations:

- Add – For detailed information see [Add WebFront Sites](#).
- Edit – For detailed information see [Edit WebFront Sites](#).
- Delete – For detailed information see [Delete WebFront Sites](#).

## Add WebFront Sites

1. Click the **Add** button to insert a new site.

| NetScaler > System > WebFront > WebFront Sites   |                                      |            |
|--|--------------------------------------|------------|
| <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |                                      |            |
| Site Name  | StoreFront URL                       | Store Name |
| myHome   | https://go.citrix.com/vpn/index.html | server     |
| HomeAway   | https://go.citrix.com/vpn/index.html | server7    |
| DarkStar   | https://go.citrix.com/vpn/index.html | server9    |

2. The following screen appears. The mandatory fields indicated by an asterisk.

Click **Continue**.

3. Create the VPN Session Action. The mandatory fields indicated by an asterisk. Add a name for the action, and verify the information. Click **Continue**.

4. Shown is a summary of the complete configuration. Verify and click **Done**.

## Edit WebFront Sites

1. Select a Web Front site, and then click the **Edit** button to revise the configuration.

2. Click on the **pencil**.

3. Revise the configuration. Click **Continue**.

4. The following screen appears. An asterisk indicates the mandatory fields. Click **Continue**.

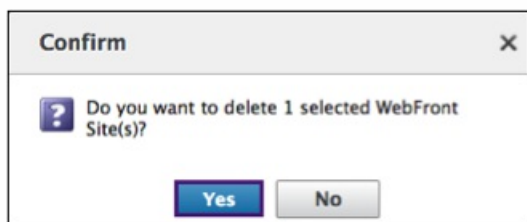
5. Shown is a summary of the complete configuration. Verify and click **Done**.

## Delete WebFront Sites

1. Select the site you want to delete. Click the **Delete** button to remove the site.

| Site Name | StoreFront URL                       | Store Name |
|-----------|--------------------------------------|------------|
| myHome    | https://go.citrix.com/vpn/index.html | server     |
| HomeAway  | https://go.citrix.com/vpn/index.html | server7    |
| DarkStar  | https://go.citrix.com/vpn/index.html | server9    |
| B_B       | https://go.citrix.com/vpn/index.html | server21   |

2 Click **Yes**.



## Installing and Configuration WebFront Using the CLI Commands

### Install WebFront Package

The following CLI command installs WebFront.

```
command
install wf package -jre <JDK location> -wf <WebFront location>
```

This command installs WebFront on the system. On the shell it creates a /var/wi folder if not present, and installs WebFront in the ROOT directory present in the /var/wi/tomcat/webapps folder. WebFront can coexist with Web Interface. For example, if WI is already installed, WebFront extracts itself only in the ROOT directory; all the wi sites and configuration will remain untouched. After the extraction, WebFront re-starts Tomcat if already running.

As part of the install command, WF allocates 198MB of RAM on a VPX and 576MB of RAM on an MPX, in addition to memory allocated by WI.

In order for RfWebProxy to work with CVPN, bind a ClientlessAccessPolicy, ns\_cvpn\_wf\_policy, to VPN global during install time.

### Uninstall WebFront Package

This command uninstalls WebFront from the system.

command

COPY

```
uninstall wf package -jre <JDK location> -wf <WebFront location>
```

If WI is present in the system, it will not remove the complete /var/wi directory structure - only WebFront part. If WI is not present, it will remove the whole /var/wi folder.

Uninstall unbinds policy ns\_cvprn\_wf\_policy from VPN global.

### Show WebFront Package

This command shows the WebFront files and installation location.

command

COPY

```
sh wf package
```

This command is helpful if there is a WebFront version number change. The user sees the installed WebFront and where WebFront is installed.

### Add WebFront Package

This command adds a WF site.

command

COPY

```
add wf site <siteName> -storefront url <string> -storeName <string>
```

```
[-html5Receiver <html5Receiver>] [-workspaceControl ( ON | OFF )]
```

```
[-displayRoamingAccounts ( ON | OFF )]
```

```
[-xframeOptions ( ALLOW | DENY )]
```

In PPE, a WebFront site will be created with storefront FQDN and store Name. Both the arguments are compulsory. User can change these by using the set command.

1. It does not create a separate folder for wf site in /var/wi/tomcat/webapps directory instead it creates a soft link from /var/wi/tomcat/ROOT/<siteName> to ROOT/WEB-INF/views. This modification was done to avoid the duplication of

static HTML display part. Since ever WF site is going to use the same Front End.

2. It also appends an entry <siteName>=<storeFront URL>#<storeName>#<html5>#<workspace Control>#<session timeout>#<roamingaccounts>#<xframe> in the file /var/wi/tomcat/ROOT/WEB-INF/classes/wfsite.properties. This is needed for when tomcat is restarted.
3. Also the CLI sends HTTP POST <http://127.0.0.1:8080/addsite/<SiteName>> with Post body “<storeFront URL>#<storeName>#<html5>#<workspace Control>#<session timeout>#<roamingaccounts>#<xframe>”. This instructs WF to fetch Store Service and Authentication URLs (Discovery &Endpoints) from the StoreFront.

| Property Name          | Description   | Default Value |
|------------------------|---|---------------|
| HTML5Receiver          | <p>Specifies whether or not to use HTML5 receiver for launching apps for all WF sites.</p> <p><u>Possible values:</u></p> <p>Always – Always use only HTML5 receiver for launching apps</p> <p>Fallback – Use HTML5 receiver as fallback, if launch through native receiver is not possible</p> <p>Off – Never use HTML5 receiver, always use native receiver</p> | Fallback      |
| WorkspaceControl       | <p>Specifies whether to use or not workspace control for all WF sites.</p> <p><u>Possible values:</u></p> <p>On – Workspace control is enabled</p> <p>Off – Workspace control is disabled</p>   | On            |
| DisplayRoamingAccounts | <p>Specifies whether or not to display the accounts selection screen during First Time Use of Receiver.</p> <p><u>Possible Values:</u></p> <p>On – Display account selection</p>  | Off           |



|               |  |      |
|---------------|--|------|
|               | screen<br><br>Off – Do not display account selection screen.   |      |
| XFrameOptions | The value to be sent in the X-Frame-Options header<br><br><u>Possible values:</u><br><br>Allow - Allow displaying in a Frame<br><br>Deny - Disallow display in a Frame | Deny |

### rm wf site

This command removes the site (if present) from WebFront. More importantly it undoes what add wf site has done. It removes the entry from wfsite.properties and it removes the symbolic link from ROOT directory also sends http post request “POST <http://127.0.0.1:8080/rmsite/<siteName>>”. As always site would be removed from PPE.

```

command COPY

set wf site <siteName> -storeFronturl <> -storeName <>

[-html5Receiver <html5Receiver>] [-workspaceControl ( ON | OFF )]

[-displayRoamingAccounts ( ON | OFF )]

[-xframeOptions ( ALLOW | DENY )]
```

If user wants to edit the entry in already present WF site he/she can use set command. User can edit either StoreFrontFQDN or StoreName or both. It also sends http post request “POST <http://127.0.0.1:8080/modsite/<SiteName>>” with post body ““<storeFront URL>#<storeName>#<html5>#<workspace Control>#<session timeout>#<roamingaccounts>#<xframe>”. This change would be reflected in wfsite.properties and PPE.

### sh wf site

It will display the details of the WF site. Including the state of the WF site. The state of the site will be UP or (DOWN and reason for being DOWN, suggested remedy).

The state is got by sending a POST request to <http://127.0.0.1:8080/shsite/<SiteName>>. The response body will have the

message to be displayed in the “Status” field.

| Error Message    | Cause for Failure   | Suggested Remedy  |
|------------------|---|---|
| INITIALIZING     | WF site is still initializing   | Check status of site after a few seconds                                    |
| DOWN-HostUnknown | Hostname of StoreFront cannot be resolved to an IP address                  | Make sure the hostname is resolvable or add a dns addrec on NS              |
| DOWN-ReqTimeout  | StoreFront server cannot be reached. Request timed out while contacting SF. | Make sure SF is reachable through NSIP                                      |
| DOWN-Wrong Store | StoreName specified does not exist in SF                                    | Change the storeName to the correct storeName using the set wf site command |
| DOWN-SSL Error   | CA used to sign SF's server cert is not present in java's trusted CA store  | Add the CA cert using exportcert.sh command                                 |
| DOWN-SF Error    | Internal Error in SF  | Check error in SF through Windows Event Viewer and rectify error            |
| DOWN-ConnReset   | Connection was reset while communicating with SF                            | Make sure SF is reachable through NSIP                                      |
| DOWN             | Unknown Error occurred  | Collect files described in section 13.1 and contact Tech support            |

#### Co-existence of WebFront and WebInterface(both are installed)

1. We are disallowing the same site Name for both WF and WI. CLI will throw the error that site is already present if site by that name is already present in webapps folder and attempt is to create in its counterpart.

#### Steps to install and Use WF through CLI:

1. Install WebFront on NS:  
install wf package -jre "file:///var/openjdk7.tbz" -wf "file:///var/nswf-1.0.tar"
2. Import StoreFront's CA cert to NS (Required only if SF is configured for https):  
shell /netscaler/wi/export\_cert.sh /var/CA.cer
3. Add a WF site: add wf site site1 -StoreFrontURL http://storefront.lab.com -storeName store 1
4. Check status of newly added WF site and debug if state is DOWN: sh wf site site1
5. If Site is UP, set up VPN vServer with WF: add vpn sessionaction WF\_ACT -sso ON -ntDomain lab.com -wihome <http://127.0.0.1:8080/site1> add vpn sessionpolicy WF\_POL NS\_TRUE WF\_ACT
6. Bind vpn vs VPN1 -policy WF\_POL -priority 10

How to configure WF to work in the 1st pane of the 3-pane window VPN Homepage:

command

COPY

```
Set wf site <siteName> -XFrameOptions ALLOW
```

This setting sets the X-Frame-Options HTTP header to Allow, making it display in an iframe (1<sup>st</sup> pane of 3-pane window).

# Configuring Settings for Your XenMobile Environment

Mar 07, 2014

You can use the integrated XenMobile configuration wizard to configure settings that enable NetScaler load balancing virtual servers for your XenMobile environment.

You can use the XenMobile links to configure the following NetScaler deployment scenarios:

- Load balance Device Manager servers. In this scenario, the NetScaler appliance resides in the DMZ between the user device and the Device Manager servers to load balance encrypted data from mobile devices to the Device Manager servers.
- Load balance Microsoft Exchange servers with email filtering. In this scenario, the NetScaler appliance sits between the user device and the XenMobile NetScaler Connector (XNC) 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. Based 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. This scenario prompts you for basic information about your StorageZones Controller environment and then generates a configuration that does the following:
  - Load balances traffic across StorageZones 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 StorageZones Controller](#).

In addition to the preceding configurations for XenMobile, you need to install licenses to enable the following NetScaler features:

- XenMobile MDM load balancing requires a NetScaler standard license.
- ShareFile load balancing with StorageZones requires a NetScaler standard license.
- Exchange load balancing requires a NetScaler Platinum license or a NetScaler Enterprise license with an Integrated Caching license added on.

# To configure load balancing servers for XenMobile MDM Edition

Feb 27, 2014

1. After you log on to the configuration utility, on the Home tab, in MDM Server LB, click Configure.
2. Under LB Virtual Server for Device Management, in Name, type a name for the server.
3. In IP Address, type the IP address for the virtual server and then click Continue.
4. On the Load Balance XenMobile MDM Servers page, repeat Steps 2 and 3 and then click Create.
5. Verify that the settings are correct and then click Done.

# To configure load balancing servers for Microsoft Exchange with Email Security Filtering

Feb 28, 2014

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, do one of the following:
  1. Click Choose Certificate and then in Certificate, select the certificate.
  2. Click Install Certificate and then in Choose Certificate, click Browse and then select one of the following:
    - Select Local to navigate to the certificate on your computer.
    - Select Appliance to navigate to the certificate on the NetScaler appliance.In Choose Key, repeat the preceding instructions to navigate to the private key for the certificate.
  3. Click Use Test Certificate and then in Certificate FQDN, type the fully qualified domain name (FQDN) that is in the certificate.
7. Click Continue.
8. Under Exchange CAS Service Instances, do the following:
  1. In Name, type a name for the server.
  2. In IP Address, type the IP address for the virtual server.
  3. In Port, type the port number.
9. Click Create and then click Done.

When you click Done, the fields for configuring the XenMobile NetScaler Connector (XNC) ActiveSync Filtering appears.

# To configure XenMobile NetScaler Connector (XNC) ActiveSync Filtering

Feb 27, 2014

The XenMobile 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. Authorization is controlled by a combination of policies defined within XenMobile Device Manager and by rules defined locally by the XNC.

1. In Callout Protocol, select http or https.
2. In XNC IP Address, type the IP address of the XNC.
3. In Port, type 9080 for HTTP network traffic or 9443 for HTTPS network traffic, click Continue and then click Done.

# To configure ShareFile settings

Feb 27, 2014

1. On the Home tab, in ShareFile LB, click Configure.
2. On the Setup Load Balancing for ShareFile page, do the following:
  1. Under ShareFile Configuration, in Name, type a name for the load balancing server.
  2. In IP Address, type the IP address of the ShareFile server or the StorageZones Connector.
  3. Enable Sharefile Data and StorageZone Connector for Network File Shares/SharePoint and then click Continue.
3. Under Certificates, do one of the following:
  1. Click Choose Certificate and then in Certificate, select the certificate.
  2. Click Install Certificate and then in Choose Certificate, click Browse. Select Local to navigate to the certificate on your computer. Select Appliance to navigate to the certificate on the NetScaler appliance. In Choose Key, repeat the preceding instructions to navigate to the private key for the certificate.
  3. Click Use Test Certificate and then in Certificate FQDN, type the fully qualified domain name (FQDN) that is in the certificate.
4. In ShareFile StorageZone Controller Configuration, under Add New StorageZone Controller, do the following:
  1. In StorageZone Controller IP Address, enter the IP address of the StorageZone Controller. You can add multiple IP addresses by clicking the plus (+) sign and entering the IP address for each server.
  2. In Port, type the port number.
  3. In Protocol, select http or https
5. Click Create and then click Done.
6. In LDAP Authentication Settings, do one of the following:
  1. Click Choose LDAP and then select a server from the list.
  2. Click Configure New and then configure LDAP server settings.

Important: If you have an existing LDAP server configured on the appliance, you cannot create a new LDAP server by using integrated XenMobile configuration. You can create additional LDAP authentication policies by using the configuration utility.
7. Click Continue and then click Done.



# Allowing Access from Mobile Devices with Worx Apps

May 07, 2015

When users connect from a mobile device with Worx Apps, NetScaler Gateway needs to discover the platform of the device, Android or iOS. You can allow users to connect from Android or iOS devices through NetScaler Gateway to mobile apps and resources in the internal network. Users connect by using Worx Home.

Android and iOS devices connect by using Worx Home that establishes a Micro VPN tunnel. When users connect, a VPN tunnel opens to NetScaler Gateway and then is passed to App Controller in the internal network. Users can then access their web, mobile, and SaaS apps from App Controller.

If users connect from an Android device, you must configure DNS settings on NetScaler Gateway. For details, see [Supporting DNS Queries by Using DNS Suffixes for Android Devices](#).

Secure Browse allows users of iOS devices to connect through NetScaler Gateway to network resources from Worx Home or Receiver for iOS, Version 5.6.x. Users do not need to establish a full VPN tunnel to access resources in the secure network. Secure Browse is enabled by default.

When you run the Quick Configuration wizard, the settings for connections from Android and iOS mobile devices are configured by the wizard. Citrix recommends using the Quick Configuration wizard to configure settings for mobile devices. For more information about running the Quick Configuration wizard, see [Configuring Settings with the Quick Configuration Wizard](#).

## How Licensing Works for Mobile Devices

Users who connect with Micro VPN consume a Universal license installed on NetScaler Gateway. The Quick Configuration wizard sets the virtual server for SmartAccess that allows for Micro VPN connections. 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](#). Users who connect with Receiver from mobile devices use the Platform license.

If a user connects by using Worx Home, a Universal license is used. Users can also connect with Receiver for Android or Receiver for iOS. When users connect by using either of these methods, the Platform license is used.

## Configuring Secure Browse by Using the Configuration Utility

You enable 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 the Clientless Access URL Encoding to Clear.

## How Secure Browse Connections Work

When users log on from an iOS device, the request from the mobile device contains a session cookie. When NetScaler Gateway and Receiver respond, the response body contains prefixes that indicate that Secure Browse and clientless access are enabled.

When you enable Secure Browse, URL rewriting occurs on the mobile device. Receiver uses the prefix to rewrite the URL when accessing internal resources. For example, if the internal resource being accessed is `http://mywebapp.net` and the fully qualified domain name (FQDN) of NetScaler Gateway is `https://my.agee.com`, the rewritten request looks like

<https://my.agee.com/SecureBrowse/http/mywebapp.net>.

If you enable Client Choices and Secure Browse as part of the session profile, when users log on from an iOS device, Secure Browse disables the client choices page. When users log on, they do not receive a choice to select the NetScaler Gateway Plug-in, clientless access, or an ICA connection as they would if logging on from a Windows-based or Mac OS X computer.

# How User Connections Work with Worx Apps

Jan 31, 2014

NetScaler Gateway supports Worx Home, WorxMail, and WorxWeb. Users can connect through NetScaler Gateway from Android and iOS mobile devices. The tunnel type is called Micro VPN.

To allow connections from an iOS-based device, you must enable Secure Browse in a session profile to allow connections through NetScaler Gateway. When users log on through Worx Home to NetScaler Gateway, the connection works the same as if users log on with the NetScaler Gateway Plug-in only.

Users can also establish a Micro VPN tunnel from Android devices with WorxHome. When users connect, the Android app uses the Micro VPN to tunnel the connection through NetScaler Gateway. You do not need to configure Micro VPN settings on NetScaler Gateway for Android devices. When users log on, their mobile applications including WorxMail and WorxWeb, appear in the Worx Home window.

# Configuring Secure Browse in NetScaler Gateway

Mar 25, 2014

You can configure Secure Browse globally or as part of a session policy. When you enable Secure Browse, you need to enable clientless access and set the URL encoding to clear. For more information, see the following:

- [Enabling Clientless Access](#)
- [Encoding the Web Address](#)

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 new 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.

# Configuring Application and MDX Token Time-Outs

Feb 03, 2014

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 web page.

Token time-outs are global settings. When you configure the setting, it applies to all users who log on to NetScaler Gateway.

## To configure application and MDX token time-outs

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.

# Disabling Endpoint Analysis for Mobile Devices

May 29, 2013

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 || CLIENT.APPLICATION.PROCESS (virus.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 Policies](#).

# Supporting DNS Queries by Using DNS Suffixes for Android Devices

Feb 03, 2014

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 either Remote or Both, the Android device sends the DNS request based on the DNS suffixes. The setting Both is the default setting. If the DNS request ends with one of the configured DNS suffixes, the request is sent to NetScaler Gateway for resolution; otherwise, the request is sent to the local DNS server. For this reason, you must configure the DNS suffix when you set split DNS to Remote or Both.
- If a DNS A record query matches the NetScaler Gateway fully qualified domain name (FQDN) to which users connect with a VPN connection, the user device replies with a cached local DNS server response. For example, if users establish a VPN connection to mycompany.ng.com and if the user device makes a DNS request for mycompany.ng.com, the DNS response comes from the cached DNS response. This is true even if the NetScaler Gateway FQDN matches the configured DNS suffix.

If the DNS query does not contain a domain name, DNS requests are sent to NetScaler Gateway for resolution. For example, a user is connecting to an internal web site, such as mycompany and the DNS query is sent to NetScaler Gateway for resolution. If you configure split DNS to either Both or Remote, if users enter the full FQDN, mycompany.nginternal.com, the DNS resolution occurs based on the DNS suffix.

- If the DNS query is not a DNS A record, the DNS query strictly follows the NetScaler Gateway split DNS setting.

For more information about configure DNS suffixes, see [Configuring a DNS Suffix](#).

## 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 value, click Add Expression, click Create and then click Close.



# Configuring TCP Compression Policy Expressions for Mobile Devices

May 14, 2013

Some versions of Citrix Receiver do not support compressed responses from NetScaler Gateway, even if you configure a TCP compression policy in NetScaler Gateway. You can configure a TCP compression policy to skip the compression for Android or iOS mobile devices. You can use expressions within a TCP compression policy so that responses from NetScaler Gateway through a mobile device are not compressed.

For Android devices, you can use either of the following expressions:

- In the TCP compression profile, select NoCompress and then create this policy expression in the policy:  
REQ.HTTP.HEADER User-Agent CONTAINS Android
- In the TCP compression profile, select Deflate and then create this policy expression in the policy: REQ.HTTP.HEADER User-Agent NOTCONTAINS Android

For iOS devices, you can use one of the following expressions:

- REQ.HTTP.HEADER User-Agent NOTCONTAINS iPad
- REQ.HTTP.HEADER User-Agent NOTCONTAINS iPhone
- REQ.HTTP.HEADER User-Agent NOTCONTAINS iOS

For more information about configuring TCP compression policies, see [How TCP Compression Policies Work](#).

# Enabling Support for Device Polling for Mobile Devices

Jan 31, 2014

App Controller includes a policy setting for mobile devices that use Citrix Receiver called Active poll period. Polling determines the status of the current application (enabled or disabled) and device (lock or erase). When a device has network connectivity, polling allows the running application to detect and respond to changes in the app state. To allow polling to work with App Controller from NetScaler Gateway, you need to provide an IP address, such as

— *https://ipaddress*

or

— *https://AppControllerIPaddress*

, or the fully qualified domain name (FQDN) of AppController, such as

— *http://AppC-FQDN*

or

— *https://AppCFQDN*

, in the NetScaler Gateway configuration utility to enable support for the Active poll period policy. The device status appears in the App Controller management console on the Devices tab.

To use this feature, you need one of the following NetScaler Gateway versions:

- NetScaler Gateway 10.1
- Access Gateway 10, Build 71.6104.e
- Access Gateway 10, Build 73.5002.e

Note: If your appliance is licensed as a NetScaler VPX running on the SDX platform and you configure link aggregation, Citrix recommends installing Access Gateway 10, Build 73.5002.e after you install Build 71.6104.e. This allows user connections through Access Gateway to AppController 2.5.

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 AppController URL.
3. In the Configure AppController dialog box, in AppController URL, enter the IP address for AppController, such as <https://192.10.10.122> or <https://appcontroller.domain.net> and then click OK.

If you restart NetScaler Gateway, you must enter the IP address again.

# To configure NetScaler Gateway settings

Feb 26, 2014

NetScaler Gateway supports user access to web, SaaS, and mobile apps and ShareFile only through App Controller. 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:

- App Controller only
  - StoreFront only
  - App Controller and StoreFront together
  - Web Interface only
1. On the Home tab, in NetScaler Gateway, click Configure.
  2. On the NetScaler Gateway Settings page, do the following:
    1. In Name, type the name of the NetScaler Gateway to which users connect.
    2. In IP Address, enter the IP address of the appliance to which users connect.
    3. In Port, type the port number through which users connect. The default port number is 443.
    4. Click Redirect requests from port 80 to secure port to route user connections from an unsecure port (80) to a secure port (443).
  3. Click Continue.
  4. Under Certificates, do one of the following:
    1. Click Choose Certificate and then in Certificate, select the Certificate.
    2. Click Install Certificate and then in Choose Certificate, click Browse. Select Local to navigate to the certificate on your computer. Select Appliance to navigate to the certificate on the NetScaler appliance. In Choose Key, repeat the preceding instructions to navigate to the private key for the certificate.
    3. Click Use Test Certificate and then in Certificate FQDN, type the fully qualified domain name (FQDN) that is in the certificate.
  5. In LDAP Authentication Settings, do one of the following:
    1. Click Choose LDAP and then select a server from the list.
    2. Click Configure New and then configure LDAP server settings.

Important: If you have an existing LDAP server configured on the appliance, you cannot create a new LDAP server by using integrated XenMobile configuration. You can create additional LDAP authentication policies by using the configuration utility.

After you configure network settings, certificates, and authentication policies, you then configure the settings for the Enterprise Store. The following are procedures for StoreFront, App Controller, and the Web Interface.

## To configure settings for StoreFront only

1. Click XenApp / XenDesktop.
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 XenApp or virtual desktops from XenDesktop.

8. Click Done.

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

To configure settings for App Controller only

1. Click XenMobile.
2. In App Controller FQDN, enter the FQDN for App Controller.
3. Click Done.

To configure Web Interface settings

1. In the Quick Configuration wizard, click XenApp / XenDesktop.
2. In Deployment Type, select Web Interface and then configure the following:
  1. In XenApp Site URL, type the complete IP address or FQDN of the Web Interface.
  2. In XenApp Services Site URL, type the complete IP address or FQDN of the Web Interface with the PNAgent Path.  
You can enter the default path or enter your own path.
  3. In Single Sign-on Domain, enter the domain to use.
  4. In STA URL, type the complete IP address or FQDN of the server running the STA.
3. Click Done.

# Optimizing Network Traffic with CloudBridge

Feb 05, 2014

When users log on with the NetScaler Gateway Plug-in, the connection can be optimized by using the CloudBridge Plug-in, which installs on the user device from CloudBridge. When the connection is optimized through the use of the CloudBridge Plug-in, network traffic is compressed and accelerated through NetScaler Gateway. When CloudBridge is enabled for a connection, TCP compression policies on the NetScaler Gateway are disabled.

The CloudBridge Plug-in is deployed and works with the NetScaler Gateway Plug-in.

NetScaler Gateway supports Versions 5.5 and 6.1 of the Repeater Plug-in and Versions 6.2 and 7.0 of the CloudBridge Plug-in.

CloudBridge optimization and flow control take precedence over NetScaler Gateway optimization features that require dynamic content modification. If CloudBridge optimization is enabled for HTTP traffic, the following NetScaler Gateway features are not available:

- Single sign-on to Web applications
- File type association
- HTTP authorization

To allow single sign-on to Web applications, you can disable acceleration on HTTP. To do so, you use the command line. Log on to the NetScaler Gateway serial console and then at a command prompt, type:

```
add vpn trafficAction ssoact http -SSO ON
```

Network traffic destined for a configured HTTP port on NetScaler Gateway is excluded automatically from CloudBridge optimization. This is the default setting. If you configure a traffic policy for CloudBridge optimization on an HTTP port, the traffic policy is honored and the network traffic is optimized by CloudBridge. However, the NetScaler Gateway optimization features are disabled for all traffic affected by that policy. CloudBridge can accelerate network traffic destined for non-HTTP ports without affecting other NetScaler Gateway features.

You use a traffic policy to configure user connections to use the CloudBridge Plug-in. You can then bind the policy to users, groups, virtual servers, or globally. The policy is prioritized based on where you bind the policy or by the priority number you give the policy.

## To create a traffic policy

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 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. In Branch Repeater, select ON and then click Create.
7. In the Create Traffic Policy dialog box, next to Add Expression, select or enter an expression that represents the traffic types to enable CloudBridge acceleration click Add Expression, click Create and then click Close.

When adding an expression, choose a network expression to use the same IP addresses and port ranges for which the

CloudBridge is configured to accelerate. For CloudBridge acceleration to occur, the traffic types configured on NetScaler Gateway must match the Service Class Policies configured on CloudBridge.

All TCP traffic benefits from CloudBridge acceleration. If you are planning to use single sign-on, do not accelerate HTTP traffic because the acceleration disables single sign-on.

# Stateless RDP Proxy

May 04, 2017

## Overview

The Stateless RDP Proxy accesses a 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.

The flow and new knobs created for this functionality are described here.

### Requirements

This solution should meet the following conditions:

- User is authenticated on NetScaler Gateway Authenticator.
- The initial /rdpproxy URL and RDP Client are connected to a different RDPListener NetScaler Gateway.
- The RDPListener Gateway information is securely passed by the Authenticator Gateway using a STA Server.

### Configuration

Add a new *rdpServer* Profile. The server profile is configured on the RDPListener Gateway.

```
command COPY  
  
add rdpServer Profile <profilename> -rdpIP <IPV4 address of the RDP listener> -rdpPort <port for terminating RDP client con
```

For stateless RDP proxy, the STA Server validates the STA ticket, which is sent by the RDP client, to obtain the RDP Target/RDPUser information.

The rdpServer Profile is configured on the 'vpn vserver'.

```
command COPY  
  
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -rdpServerProfile <rdpServer Profile>
```

### Warning

Once the rdpServerProfile is configured on the vpn vserver, it cannot be modified. Also, the same serverProfile cannot be reused on

another vpn vserver.

The **rdp profile** command was renamed as **rdpClient profile** and has new parameters. The **multiMonitorSupport** command was added. Also, an option to configure custom params, which are not supported as part of the RDP client profile, has been added. The **clientSSL** param was removed, since the connection is always secured. The client profile is configured on the Authenticator Gateway.

```
command COPY  
  
add rdpClient profile <name> -rdpHost <optional FQDN that will be put in the RDP file as 'fulladdress'> [-rdpUrlOverride ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-v  
[-rdpCookieValidity <positive_integer>] [-multiMonitorSupport ( ENABLE | DISABLE )] [-rdpCustomParams <string>]
```

The `-rdpHost` configuration is used in a single Gateway deployment.

- Associate the RDP Profile with the vpn vserver.

This can be done either by configuring a `sessionAction+sessionPolicy` or by setting the global vpn parameter.

Example:

```
command COPY  
  
add vpn sessionaction <act name> -rdpClient profile <rdpprofilename>  
  
add vpn sessionpolicy <polname> NS_TRUE <act name>  
  
bind vpn vserver <vservername> -policy <polname> -priority <prioritynumber>  
  
OR  
  
set vpn parameter -rdpClient profile <name>
```

### Connection Counter

A new connection counter `ns_rdp_tot_curr_active_conn` was added, which keeps the record of number of active

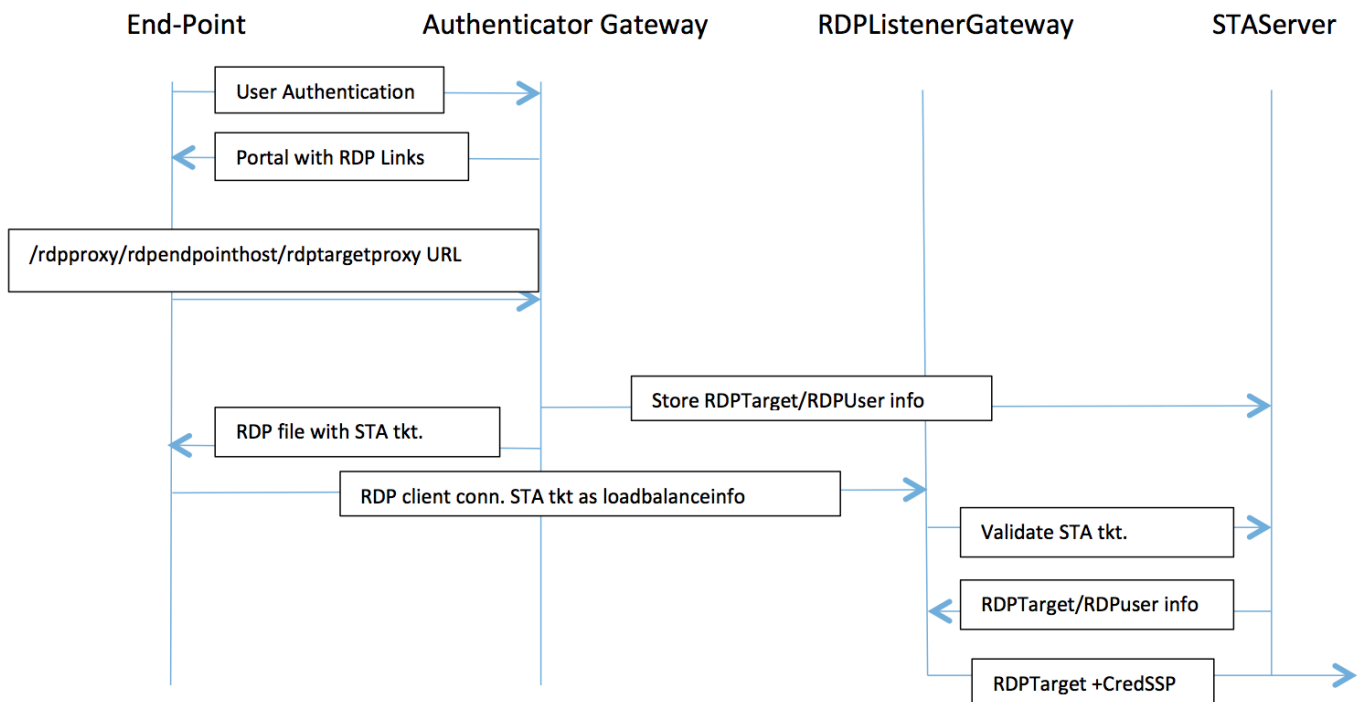


connections in use. It can be viewed as a part of nsconnmsg command on NetScaler shell. Later, we will be providing a new CLI command to view this counters.

## 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 (configures using rdpIP and rdpPort) on the NetScaler Gateway, and subsequent proxying of the RDP client to server packets securely.



- User connects to the Authenticator Gateway VIP and provides his/her credentials.
- After successful login to the Gateway, user is redirected to the homepage/external portal which enumerates the remote desktop resources that the user can access.
- Once the user selects a 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.
- The `/rdpproxy/` request is processed by the Authenticator Gateway. Since 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 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 will use one of the STA servers that is configured on the Gateway Vserver.

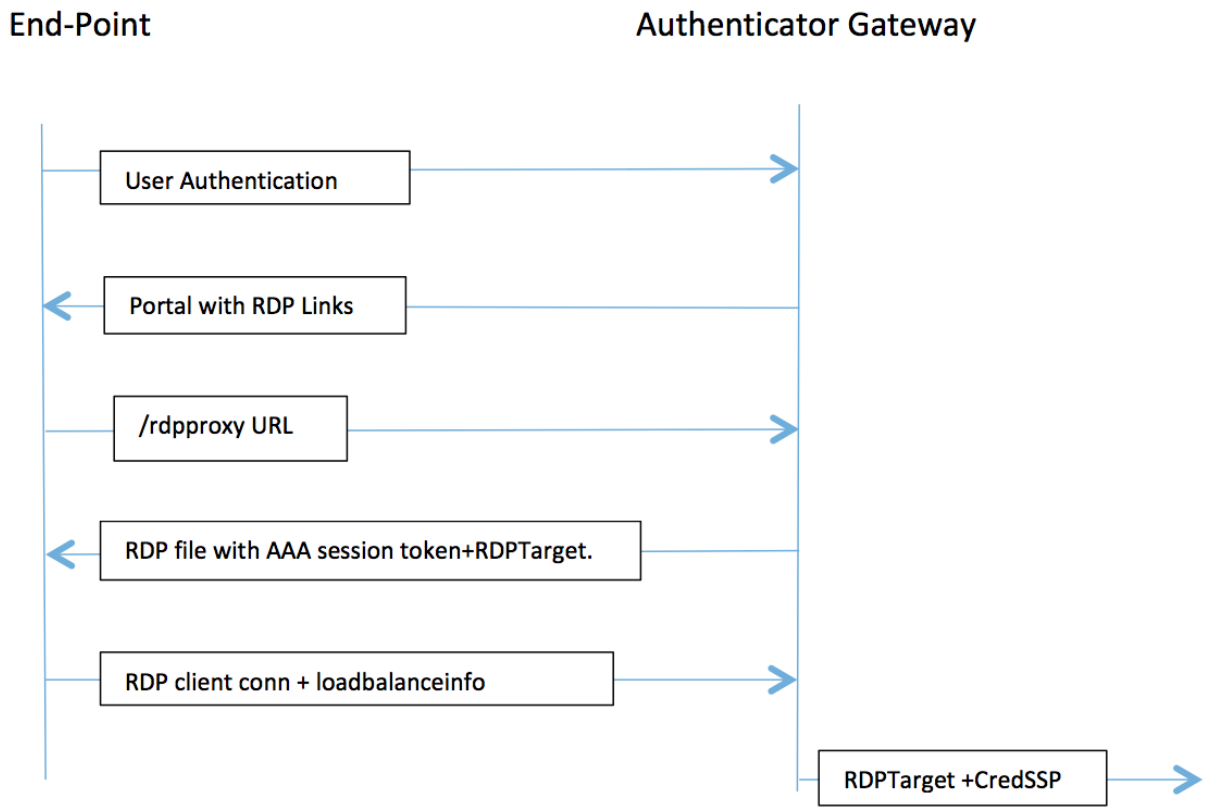
- The XML blob will be in this format

```
<Value name="IPAddress">ipaddr</Value>\n<Value name="Port">port</Value>\n
<Value name="Username">username</Value>\n<Value name="Password">pwd</Value>
```

- 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.
- 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 x.224 packet.
- 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.
- A Gateway session is created for storing authorization/auditing policies. If a session already exists for the user, it is re-used.
- The RDPListener Gateway connects to the RDPTarget and single signs on using CREDSSP.

### Single Gateway Compatibility

If the RDP file is generated using the /rdpproxy/rdptarget/rdptargetproxy URL, we will generate a STA ticket, otherwise the current method of the 'loadbalanceinfo' referring to the session directly will be used.



In case of a single gateway deployment, the /rdpproxy URL comes to the Authenticator Gateway itself. A STA server is not required. The authenticator gateway encodes the RDPTarget and the AAA session cookie securely and sends this as the 'loadbalanceinfo' in the .rdp file. When the RDP Client sends this token in the x.224 packet, the authenticator gateway decodes the RDPTarget information, looks up the session and connects to the RDPTarget.

## Upgrade Notes

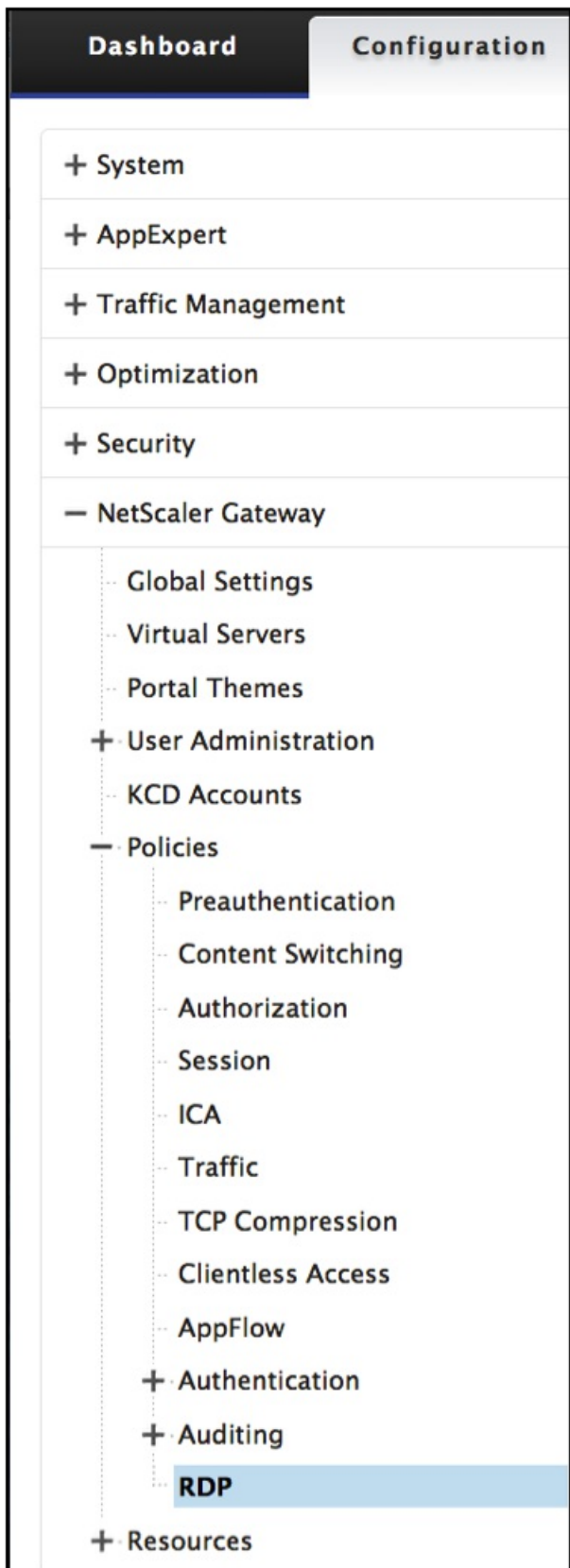
Earlier configuration doesn't work with this new release, since the parameters rdpIP and rdpPort, which were earlier configured on vpn vserver has been updated to be part of the rdpServerProfile and 'rdp Profile' has been renamed as 'rdp ClientProfile' and the old parameter clientSSL has been removed.

## Limitations

In this build the data between the Gateway and STA server is not encrypted using the preshared key, and is sent unencrypted. This will be addressed in the GA.

# Create RDP Server Profile

1. Go to NetScaler Gateway > Policies > RDP.



2. Go to Server Profiles tab and click **Add**.

| Server Profiles |  |  | Client Profiles |  |  | Connections |  |  |          |  |  |
|-----------------|--|--|-----------------|--|--|-------------|--|--|----------|--|--|
| Add             |  |  | Edit            |  |  | Delete      |  |  | Search ▾ |  |  |
| Name            |  |  | RDP IP          |  |  | RDP Port    |  |  |          |  |  |
| test_rdp        |  |  | 10.207.27.28    |  |  | 3389        |  |  |          |  |  |
| Mars            |  |  | 10.10.10.9      |  |  | 3389        |  |  |          |  |  |
| Saturn          |  |  | 11.10.12.8      |  |  | 3389        |  |  |          |  |  |

3. Enter the following information to create the RDP Server Profile.

### Create RDP Server Profile

Name\*  
 ?

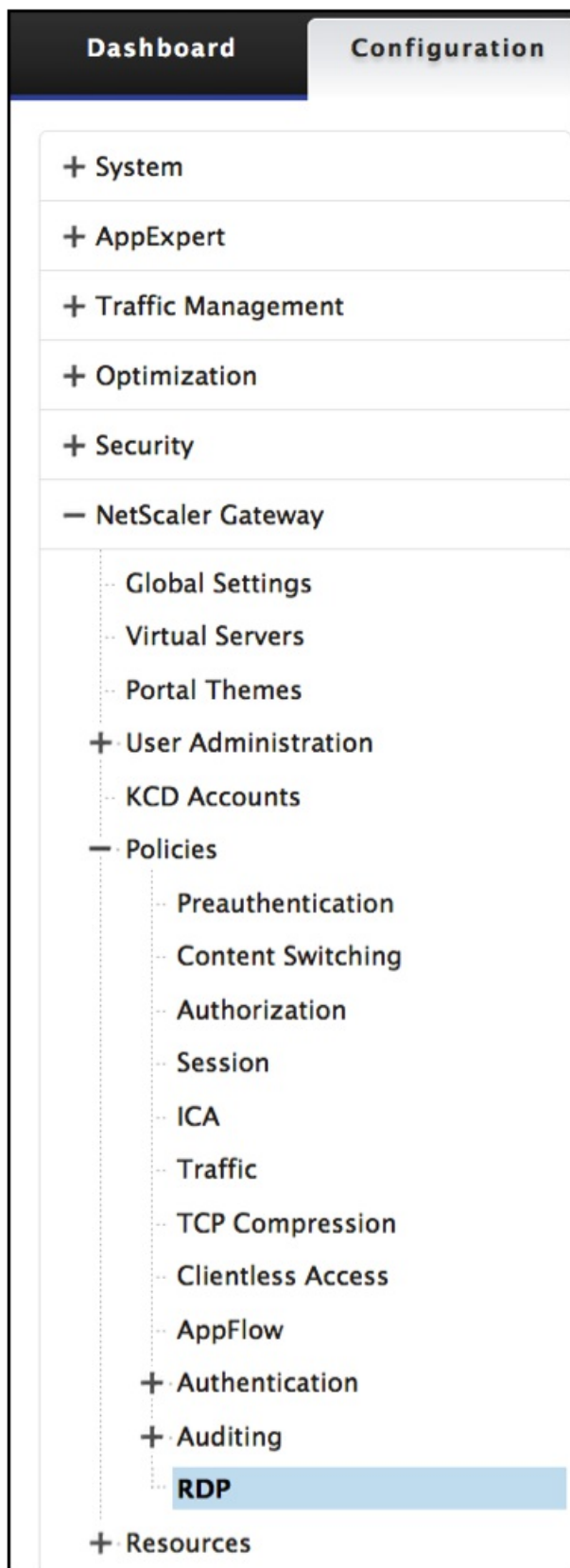
RDP IP\*

RDP Port

Pre Shared Key\*

## Configure RDP Client Profile

1. Go to NetScaler Gateway > Policies > RDP



2. Go to Client Profiles tab and click **Add**.

NetScaler > NetScaler Gateway > Policies > RDP Profiles and Connections > Client Profiles

Server Profiles | **Client Profiles** | Connections

Add | Edit | Delete | Search ▾

| Name    | URL Override | Redirect Clipboard | Redirect Drives | Redirect Printers |
|---------|--------------|--------------------|-----------------|-------------------|
| ▶ Tight | ENABLE       | ENABLE             | ENABLE          | ENABLE            |
| ▶ Jack  | ENABLE       | ENABLE             | ENABLE          | ENABLE            |

3. Enter the following information to configure the RDP Server Profile.

### Create RDP Client Profile

Name\*

URL Override\*

Redirect Clipboard\*

Redirect Drives\*

Redirect Printers\*

Keyboard Hook\*

Audio Capture Mode\*

Video Playback Mode\*

RDP Cookie Validity (seconds)

Add Username In RDP File\*

RDP File Name

RDP Host

Multiple Monitor Support\*

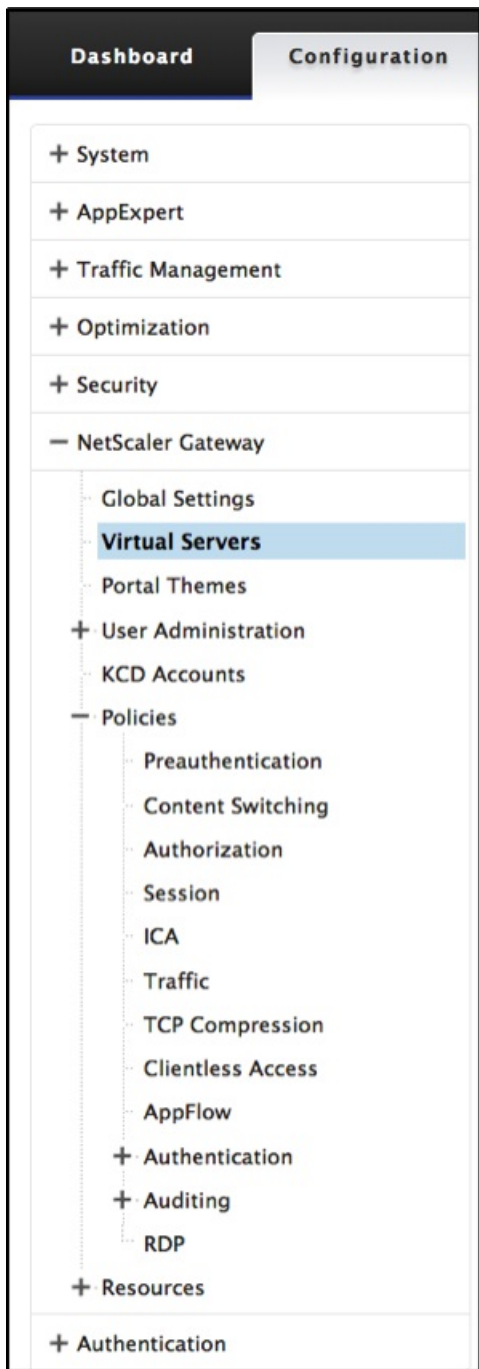
Custom Parameters

Pre Shared Key

## Setup a Virtual Server

1. Go to NetScaler Gateway > Virtual Server.





2. Click **Add** to create a new RDP Server.

| <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Statistics"/> <input type="button" value="Visualizer"/> <input type="button" value="Action"/> |   |              |      |          |               |               | Search ▾ |
|--|---|--------------|------|----------|---------------|---------------|----------|
| Name   | State                                   | IP Address   | Port | Protocol | Maximum Users | Current Users |          |
| RDP  | <span style="color: red;">●</span> Down | 10.0.0.1     | 3389 | SSL      | 0             | 0             |          |
| Twilight   | <span style="color: green;">●</span> Up | 10.127.27.80 | 443  | SSL      | 0             | 0             |          |
| Dolphin  | <span style="color: green;">●</span> Up | 10.208.28.24 | 443  | SSL      | 25            | 0             |          |
| Quicksilver  | <span style="color: green;">●</span> Up | 20.20.15.9   | 443  | SSL      | 0             | 0             |          |
| Quicksilver2   | <span style="color: green;">●</span> Up | 20.20.15.8   | 443  | SSL      | 0             | 0             |          |
| Minerva  | <span style="color: green;">●</span> Up | 20.20.20.3   | 443  | SSL      | 0             | 0             |          |
| Pluto  | <span style="color: green;">●</span> Up | 15.15.9.7    | 443  | SSL      | 0             | 0             |          |
| Penquin  | <span style="color: red;">●</span> Down | 2.3.4.3      | 443  | SSL      | 0             | 0             |          |
| UG_VPN_UG-Virtual-Server-1   | <span style="color: green;">●</span> Up | 0.0.0.0      | 0    | SSL      | 0             | 0             |          |
| PrimaryGateway   | <span style="color: green;">●</span> Up | 10.207.27.24 | 443  | SSL      | 0             | 0             |          |
| UG_VPN_UnifiedGW   | <span style="color: red;">●</span> Down | 0.0.0.0      | 0    | SSL      | 0             | 0             |          |
| UG_VPN_Dandelion   | <span style="color: green;">●</span> Up | 0.0.0.0      | 0    | SSL      | 0             | 0             |          |
| Twilight Sky   | <span style="color: green;">●</span> Up | 10.12.7.8    | 443  | SSL      | 90            | 0             |          |
| Leonis   | <span style="color: red;">●</span> Down | 0.0.0.0      | 0    | SSL      | 25            | 0             |          |

3. Complete the data on this Basic Settings page and click **OK**.

## VPN Virtual Server

### Basic Settings

Name  
RD Server

IP Address Type  
IP Address

IP Address\*  
10 . 101 . 101 . 10  IPv6

Port  
3389

RDP Server Profile  
Saturn

Maximum Users  
0

Max Login Attempts  
10

Failed Login Timeout  
1

Windows EPA Plugin Upgrade  
Always

Linux EPA Plugin Upgrade  
Always

Mac EPA Plugin Upgrade  
Essential

Login Once  
 ICA Only  
 Double Hop  
 DTLS  
 ICA Proxy Session Migration  
 Enable Device Certificate

Enable Authentication  
 Down State Flush  
 AppFlow Logging  
 State

Comments

Less

OK Cancel

### Help

Advanced Settings

- + Content Switching Policies
- + SSL Profile
- + SSL Ciphers
- + SSL Policies
- + Intranet IP Addresses
- + Intranet Applications
- + Published Applications
- + Portal Themes
- + EULA

4. Click the **pencil** to edit the page.

VPN Virtual Server

| Basic Settings                  |                                  |                             |           | Help  |
|---------------------------------|----------------------------------|-----------------------------|-----------|---|
| Name                            | RDP                              | Maximum Users               | 0         | <b>Advanced Settings</b><br>+ SSL Profile<br>+ SSL Ciphers<br>+ SSL Policies<br>+ Intranet IP Addresses<br>+ Published Applications<br>+ EULA |
| IPAddress                       | 10.0.0.1                         | Max Login Attempts          | -         |   |
| Port                            | -                                | Failed Login Timeout        | -         |   |
| State                           |                                  | ICA Only                    | false     |   |
| RDP Server Profile              | Saturn                           | Enable Authentication       | true      |   |
| Login Once                      | false                            | Windows EPA Plugin Upgrade  | Always    |   |
| Double Hop                      | false                            | Linux EPA Plugin Upgrade    | Always    |   |
| Down State Flush                | false                            | Mac EPA Plugin Upgrade      | Essential |   |
| DTLS                            | false                            | ICA Proxy Session Migration | false     |   |
| AppFlow Logging                 | false                            | Enable Device Certificate   | false     |   |
| Certificates                    |                                  |                             |           |   |
| No Server Certificate >         |                                  |                             |           |   |
| No CA Certificate >             |                                  |                             |           |   |
| <b>Continue</b>                 |                                  |                             |           |   |
| SSL Parameters                  |                                  |                             |           |   |
| Enable DH Param                 | DISABLED                         | Clear Text Port             | 0         |   |
| Enable DH Key Expire Size Limit | DISABLED                         | Enable Cipher Redirect      | DISABLED  |   |
| Enable Ephemeral RSA            | ENABLED                          | Client Authentication       | DISABLED  |   |
| Refresh Count                   | 0                                | Send Close-Notify           | YES       |   |
| Enable Session Reuse            | ENABLED                          | PUSH Encryption Trigger     | Always    |   |
| Time-out                        | 120                              | SNI Enable                  | DISABLED  |   |
| SSL Redirect                    | DISABLED                         | TLSv1                       | ENABLED   |   |
| SSLv2 Redirect                  | DISABLED                         | TLSv11                      | ENABLED   |   |
| SSLv2                           | DISABLED                         | TLSv12                      | ENABLED   |   |
| SSLv3                           | ENABLED                          |                             |           |   |
| Profiles                        |                                  |                             |           |   |
| Net Profile                     | Bang                             |                             |           |   |
| TCP Profile                     | nstcp_default_tcp_ifp            |                             |           |   |
| HTTP Profile                    | nshttp_default_strict_validation |                             |           |   |