

NetScaler Gateway 10.1

Jun 28, 2013

About This Release

[Key Features](#)

[What's New](#)

[Known Issues](#)

System Requirements

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

[Endpoint Analysis Requirements](#)

Plan

[NetScaler Gateway Prerequisites](#)

[NetScaler Gateway Pre-Installation Checklist](#)

[Planning for Security with NetScaler Gateway](#)

Deploy

[Deploying NetScaler Gateway in the DMZ](#)

[Deploying NetScaler Gateway in the Secure Network](#)

[Deploying NetScaler Gateway with XenMobile App Edition, XenApp, and XenDesktop](#)

[Deploying NetScaler Gateway with the Web Interface](#)

[Deploying NetScaler Gateway Plug-ins for User Access](#)

[Deploying NetScaler Gateway in a Double-Hop DMZ](#)

Install

[Configuring Settings by Using the Configuration Utility](#)

[Configuring the NetScaler Gateway by Using Wizards](#)

[Configuring IP Addresses on NetScaler Gateway](#)

[Configuring Routing on NetScaler Gateway](#)

[Testing Your NetScaler Gateway Configuration](#)

[Configuring Name Service Providers](#)

[Configuring Auto Negotiation](#)

[Upgrading NetScaler Gateway](#)

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](#)

Configure

[Creating Additional Virtual Servers](#)

[Configuring High Availability on NetScaler Gateway](#)

[Installing and Managing Certificates](#)

[Configuring Policies and Profiles on NetScaler Gateway](#)

[Configuring Authentication and Authorization](#)

[Configuring Endpoint Polices](#)

[Creating Advanced Endpoint Analysis Scans](#)

Connect Users

[How User Connections Work with the NetScaler Gateway Plug-in](#)

[Choosing the User Access Method](#)

[How Users Connect to Applications, Desktops, and ShareFile](#)

[Integrating the NetScaler Gateway Plug-in with Receiver](#)

[Allowing Access from Mobile Devices](#)

[Selecting the NetScaler Gateway Plug-in for Users](#)

[Configuring Clientless Access](#)

[Configuring the Client Choices Page](#)

[Configuring Access Scenario Fallback](#)

[Optimizing Network Traffic with CloudBridge](#)

[Managing User Sessions](#)

[Configuring Connections for the NetScaler Gateway Plug-in](#)

Integrate

[Integrating NetScaler Gateway with App Controller or StoreFront](#)

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

Customize

[Deploying NetScaler Gateway in a Double-Hop DMZ](#)
[Configuring DNS Virtual Servers](#)
[Resolving DNS Servers Located in the Secure Network](#)
[Using Operators and Operands in Policy Expressions](#)
[Configuring Server-Initiated Connections](#)

Maintain and Monitor

[Configuring Delegated Administrators](#)
[Viewing NetScaler Gateway Configuration Settings](#)
[Configuring Auditing on NetScaler Gateway](#)
[Enabling NetScaler Gateway Plug-in Logging](#)
[To monitor ICA connections](#)

About This Release

Jan 14, 2014

Citrix NetScaler Gateway 10.1 offers support for the following:

- Clientless access for Citrix Receiver for Web
- Email-based discovery for Receiver that connects from outside the enterprise and requires a full VPN connection
- Multi-stream ICA that allows you to partition multiple ICA streams in the same session
- Web socket protocol support that allows bi-directional communication between user devices and servers over HTTP
- Connections to Android and iOS mobile devices
- Support for Citrix XenMobile App Edition and Citrix StoreFront
- Single sign-on to XenMobile App Edition
- Support for published applications and virtual desktops

NetScaler Gateway offers the following benefits:

- Remote access for the most demanding and complex environments that require increased scalability and performance
- High availability for uninterrupted access to critical applications and resources
- Tightest level of integration and control of remotely delivered Citrix XenApp applications, MDX applications delivered from App Controller, data through SmartAccess, and published desktops with Citrix XenDesktop
- Micro VPN support for Android and iOS devices that allow users to connect with a VPN tunnel through NetScaler Gateway to internal network resources
- Support for WorxWeb and WorxMail that leverage use of the Secure Ticket Authority (STA) and NetScaler Gateway to create long-lived sessions that can bypass the session created by Receiver on NetScaler Gateway
- Integration and control of remotely delivered web and SaaS applications, mobile apps for iOS, and ShareFile data from XenMobile App Edition
- Support for all versions of Citrix Receiver
- Natural replacement for existing XenApp customers who use the Secure Gateway
- Enterprise-class SSL VPN features, including client-side cache clean-up, detailed auditing, and policy-based access control for web and server applications
- Ability for remote users to work with files on shared network drives, access email and intranet sites, and run applications as if they are working inside of your organization's firewall
- Support for the NetScaler Gateway Universal license (included in XenApp Platinum Edition, XenDesktop Platinum Edition, Citrix NetScaler Platinum Edition, XenMobile Enterprise Edition and XenMobile App Edition)

Key Features

Mar 25, 2014

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 NetScaler Gateway Pre-Installation Checklist to have on hand before you configure NetScaler Gateway.

NetScaler Gateway Appliances	Provides information about NetScaler Gateway appliances and the appliance installation instructions.
NetScaler Gateway 10 Pre-Installation Checklist	Provides planning information to review and a list of tasks to complete before you install NetScaler Gateway in your network.
Deploying NetScaler Gateway	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.

Installing Licenses on NetScaler Gateway	Provides information about installing licenses on the appliance. Also provides information about installing licenses on multiple NetScaler Gateway appliances.
--	--

NetScaler Gateway Architecture

Jan 14, 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. 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 with NetScaler Gateway

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.

NetScaler Gateway 10.1 Compatibility with Citrix Products

Apr 08, 2014

The following table provides the Citrix product names and versions with which NetScaler Gateway 10.1 is compatible.

Note: NetScaler Gateway features are available on NetScaler VPX.

Citrix product	Release version	Notes
Branch Repeater or CloudBridge	5.5, 6.1, 6.2 and 7.0	
NetScaler Platforms	MPX 5550, MPX 7500, MPX 10500, Xen VPX	
NetScaler	9.2, 9.3, and 10.0	
NetScaler VPX	9.1, 9.2 , and 9.3	
Receiver StoreFront	1.2 and 2.1	
VDI-in-a-Box	5.2, 5.3 and 5.4	
Web Interface	4.5, 5.0.1, 5.1, 5.2, 5.3, and 5.4	
XenApp	6.5 for Windows Server 2008 R2	
XenDesktop	7 and 7.1	
XenMobile	8.6, 8.7	<p>Install NetScaler Gateway 10.1, Build 120.1316.e for use with XenMobile 8.6.</p> <p>Install NetScaler Gateway 10.1, Build 124.1308.e for XenMobile 8.7.</p> <p>Note: If you are running XenMobile 8.7 with Build 120.1316.e without experiencing problems, upgrading to Build 124.1308.e is not required.</p>

NetScaler Gateway supports the following versions of client software:

Receiver or Plug-in	Release version	NetScaler Gateway version
NetScaler Gateway Plug-in for Mac OS X		Supports Mac OS X 10.8 (Mountain Lion) starting with enhancement build 10.1, Build 120.1316.e.
NetScaler Gateway Plug-in for Windows		Supports Windows 8.1 starting with enhancement build 10.1, Build 120.1316.e. Supports Windows 8.1 starting with maintenance build 10.1, Build 123.11.
Receiver for Android	3.4.x	Support starts with maintenance build 10.1, Build 69.6.
Receiver for iOS	5.8.x	Support starts with maintenance build 10.1, Build 69.6.
Receiver for Mac	11.8	Support starts with maintenance build 10.1, Build 69.6.
Receiver for Windows	4.0 and 4.1	Support starts with maintenance build 10.1, Build 69.6.
Worx Home for iOS	8.5 and 8.6	Versions 8.5 and 8.6 are supported starting with enhancement build 10.1, Build 120.1316.e
Worx Home for Android	8.5 and 8.6	Versions 8.5 and 8.6 are supported starting with enhancement build 10.1, Build 120.1316.e
WorxMail for iOS	1.3.3-16	Supported starting with enhancement build 10.1, Build 120.1316.e
WorxWeb for iOS	1.3.1-3	Supported starting with enhancement build 10.1, Build 120.1316.e
WorxMail for Android	1.3.13-233936	Supported starting with enhancement build 10.1, Build 120.1316.e
WorxWeb for Android	1.3.3-234245	Supported starting with enhancement build 10.1, Build 120.1316.e

What's New

Mar 31, 2014

NetScaler Gateway 10.1, Build 123.1100.e adds the following new feature:

- SmartAccess Connections. You can configure NetScaler Gateway virtual servers to manage user ICA Proxy sessions between parallel logons. Enabling this feature limits an active user to a single Universal license.

NetScaler Gateway 10.1, Build 120.1316.e has the following new features:

- Advanced endpoint analysis. NetScaler Gateway contains built-in scans for a wide variety of applications and services with the Endpoint Analysis Plug-in Windows-based computers and Mac OS X computers.
- Client certificate authentication for Mac OS X. NetScaler Gateway supports client certificate authentication for Mac OS X computers. When users log on with the NetScaler Gateway Plug-in for Mac, they can choose from a list of client certificates for authentication. If the certificate is accepted, they can then save the certificate to use in future sessions. This way, the next time users log on, NetScaler Gateway uses the same certificate and users do not receive another prompt for the certificate.
- Client certificate authentication for Worx Home. Worx Home can use client certificates to authenticate users when they log on. User devices must enroll in Device Manager. When the device enrolls, Device Manager sends the client certificate to the user device and the certificate is stored in Worx Home. When users log on, NetScaler Gateway requests the client certificate and authenticates the user.
- Device certificates. You can install PKCS#12 certificates on NetScaler Gateway. Device certificates support Windows-based and Mac OS X computers. Device certificates also work with endpoint analysis.
- Kerberos Constrained Delegation (KCD). You can configure KCD support on NetScaler Gateway virtual servers. This feature provides single sign-on to Kerberos-based applications.
- NetScaler Gateway Plug-in support. The NetScaler Gateway Plug-in runs on Windows 8.1 and Mac OS X Version 10.9.
- Proxy support. NetScaler Gateway supports a traffic policy-based proxy configuration that facilitates seamless redirection of secure (HTTPS) and unsecure (HTTP) network traffic from WorxWeb to proxy servers in your network.
- ShareFile Setup Wizard. This wizard allows you to configure secure access to your ShareFile Storage Zone controllers that reside in the internal network.
- XenMobile Deployment Page. NetScaler Gateway supports a consolidated XenMobile deployment page that allows you to configure a XenMobile deployment from a single page.

NetScaler Gateway 10.1 has the following new features:

- First time use configuration. When you install the NetScaler Gateway appliance or NetScaler Gateway VPX for the first time and then log on to the configuration utility, you configure basic network settings for the appliance.
- IPv6 support for ICA Proxy. User connections from Receiver through NetScaler Gateway supports IPv6. You configure IPv6 for ICA proxy by using the command line to enable IPv6 and enter the IP addresses.
- NetScaler Gateway Plug-in for Windows 8. Users can download the plug-in to their Windows 8 computer to connect to resources in the internal network.
- Quick Configuration wizard. You can use an improved Quick Configuration wizard (previously known as the Remote Access wizard) to configure user access to App Controller, StoreFront, and the Web Interface. The Quick Configuration wizard configures the session and clientless access policies with the correct settings that allow users to connect to their Windows, web, SaaS, mobile apps, and virtual desktops.
- Remote access for ShareFile Storage Zones. NetScaler Gateway supports access to ShareFile Storage Zones for remote users. You configure access for the virtual server. When you configure remote access for ShareFile, users do not receive

the NetScaler Gateway Access Interface when they log on. Users receive the ShareFile page that contains the shared file.

- SAML authentication. NetScaler Gateway supports SAML authentication that provides user authentication and single sign-on to NetScaler Gateway. You install an Identity Provider (IdP) certificate on NetScaler Gateway, and provide the issuer name and other parameters. You can also configure SAML authentication for two-factor authentication.
- Support for DNS queries by using DNS suffixes for Android devices. When users establish a Micro VPN connection from an Android device, NetScaler Gateway sends split DNS settings to the user device. NetScaler Gateway supports split DNS queries based on the split DNS settings you configure. NetScaler Gateway can also support split DNS queries based on DNS suffixes you configure on the appliance.

Known Issues

Mar 25, 2014

To access complete and up-to-date product information, in the Citrix eDocs library, expand the topics for [../netscaler-gateway/ng-edocs-con.html](https://docs.citrix.com/en-us/netscaler-gateway/ng-edocs-con.html).

For a current list of known and fixed issues in NetScaler Gateway maintenance builds, see the readmes in the [Citrix Knowledge Center](#).

Licensing Documentation

To access licensing documentation for NetScaler Gateway 10.1, see [Installing Licenses on NetScaler Gateway](#).

NetScaler Gateway contains several new features that support the logon pages, network traffic, policies, and profiles. For more information, see [What's New](#).

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

1. If you configure a load balancing virtual server and the destination port is 21, when users log on with the NetScaler Gateway Plug-in, logon is successful but data connections do not go through. When you configure a load balancing virtual server, do not use port 21. [#244412]
2. Renaming an authorization policy in NetScaler Gateway fails. [#242941]
3. If user names include Unicode characters, when they try to edit their profile from the NetScaler Gateway icon on the taskbar to select the Use the NetScaler Gateway Plug-in for logon check box, the configuration does not save. [#302421]
4. If you configure a preauthentication policy by using the command line and the policy contains an expression greater than 1,434 characters but less than the maximum allowed length of 1,499, an "Invalid rule" error appears. [#332831]
5. When you create an authorization policy in the configuration utility and you bind the policy to a virtual server, when you try to view the bindings on the Policies pane, an Information message for the policy states: This policy is not bound anywhere. If you configure and bind the same policy by using the NetScaler command-line interface, the policies appear on the Policies pane in the configuration utility. [#334382]
6. If you apply the Citrix Receiver theme to the NetScaler Gateway logon page, the layout appears garbled on computers running Windows XP Service Pack 3 with Internet Explorer 7 browsers. [#346729]
7. When you configure an intranet IP address on NetScaler Gateway and bind the address globally, the IP address that appears is slightly different from the address you configured. For example, you bind 55.77.66.0, but the IP address that appears is 55.77.86.0. [#352990]
8. When a large number of users (such as 30,000) log on to NetScaler Gateway at the same time, occasionally further user logons fail. [#357940]
9. When you configure authentication to use a one-time password with RADIUS, when many users log on with the NetScaler Gateway Plug-in simultaneously and they are prompted to enter a one-time password, occasionally authentication fails and some users cannot log on. [#361951]
10. When you configure intranet IP address pools, when users try to use the Windows TFTP utility to send a file to a server that is also connected to NetScaler Gateway, the transfer fails if the file block size is 2048 or greater. [#364532]

11. When you configure NetScaler Gateway with additional appliances in which global server load balancing (GSLB) is enabled in an active-active-data center setup, if one appliance fails, when users log on with the NetScaler Gateway Plug-in and access the Web Interface, occasionally a 302 redirection error occurs in the browser, and users are prompted to log on in a continuous loop. [#365547]
12. If you attempt to create a load balancing virtual server on an appliance that is licensed for NetScaler Gateway only, the load balancing virtual server status appears as DOWN. However, actual redirection from http to https works. [#368163]
13. If you configure an intranet IP address, when users connect to a 4G network and then connect with the NetScaler Gateway Plug-in, if the 4G connection disconnects and a WiFi connection is enabled, the virtual adapter is no longer initialized. [#368257]
14. If users log on with the NetScaler Gateway Plug-in for Windows 8 and if there are multiple server initiated connections, the NetScaler Gateway Plug-in fails to establish a connection. [#370069]
15. If users log on by using the NetScaler Gateway Plug-in and then try to access a subnet IP address, users receive a 401 access denied error. [#373991]
16. When users log on using clientless access, and attempt to open email or a web page, because the Uniform Resource identifier (URI) contains a plus sign (+) within the XML, the page does not open. [#373993, #382858]
17. If you configure the appliance with NetScaler Gateway and Application Firewall, logon attempts by unauthorized users appear in the logs. When an authorized users logs on and then attempts to access a network resource to which users are explicitly denied, the access attempt does not appear in the logs and users receive a 403 error. [#374890]
18. If users log on with Receiver for iOS and connect to web and SaaS applications in App Controller, if there is a high availability failover, the ITMS service fails for the first request and then works from the second request. [#375462]
19. If you configure an intranet IP address, when users log on by using clientless access and then open SharePoint 2007, when they try to open a folder with Windows Explorer, a blank page appears. [#376303]
20. When you configure an authentication policy and a traffic policy to enable single sign-on (SSO), when users log on with the NetScaler Gateway and try to open files larger than 1 gigabyte (GB), NetScaler Gateway occasionally fails. [#378974]
21. If the server hosting XenApp or XenDesktop is also the domain controller in your network and if user connections use SSLRelay through a Domain Name Server (DNS), when NetScaler Gateway starts a second DNS resolution to XenApp or XenDesktop, NetScaler Gateway might fail. Citrix recommends configuring one DNS server for SSLRelay and XenApp or XenDesktop. Also, you need to configure NetScaler Gateway to copy the SSLRelay IP address to the XenApp or XenDesktop address. [#381808]
22. When you create a tertiary authentication policy and bind the policy to a virtual server, you cannot unbind the policy. [#383792]
23. If you configure a SAML authentication policy and use Unicode characters in the Default Authentication Group field, after you save the policy, when you view the group name again, the Unicode characters appear garbled. [#383853]
24. If you configure NetScaler Gateway as a high availability pair and if there is a failover from the primary to the secondary appliance, the ICA connection to published apps that are already open on the user device is reestablished. If users attempt to open more applications from the Web Interface, the applications fail to open and user receive an error message. [#384998]
25. If you have configure a proxy server and you configure NetScaler Gateway to route traffic through the proxy server, when users log off from a clientless access session, a 403 error occurs. [#385318]
26. If you configure a session policy for Outlook Web App, enter the web address for web-based email and enable single sign-on for web applications and add the domain, single sign-on does not work for Russian users. [#385825]
27. If users connect with the NetScaler Gateway Plug-in on a Windows 7 64-bit or Windows 8 64-bit computer and then disconnect the wireless connection when the connection with the plug-in is active, users might receive an error on a blue screen. [#387300]
28. When you configure preauthentication scans, when users log on with clientless access, if you configure Encrypt in URL

- mode encoding, the home page appears distorted. [#388839]
29. When more than 5,000 users log on with the NetScaler Gateway Plug-in and access applications through Citrix Receiver, occasionally, users receive the message, "Error: Not a privileged user." [#389949]
 30. When users log on with the NetScaler Gateway Plug-in, when WiFi roaming occurs, intermittent ICMP requests time out and users cannot access network resources. [#392389]
 31. When you configure a preauthentication endpoint analysis policy, and you configure a custom logon page, when users try to connect with the NetScaler Gateway Plug-in users are redirected to a 403 error page. If users refresh the browser, the endpoint analysis scans run successfully. [#393344]
 32. If a web browser is open on the user device and users start the NetScaler Gateway Plug-in from the menu, the browser opens the virtual IP address and starts the Endpoint Analysis Plug-in. Occasionally, users receive an access denied error message. [#393357]
 33. When users log on by using clientless access and open SharePoint 2007, if they try to open a document with Windows Explorer, an error occurs. [#394800]
 34. If connections interrupt between the user device, NetScaler Gateway, and XenDesktop, session reliability does not reestablish the connection. [#396488]
 35. When the virtual server on NetScaler Gateway replies to the callback request from StoreFront, it uses the translated IPv4 address instead of the IPv6 address. [#397174]
 36. When you configure IPv6 for a virtual server, when users log on with the NetScaler Gateway Plug-in and open XenDesktop, the users' applications do not appear. [#397101]
 37. If you configure the Web Interface Address on the Published Applications tab in a session profile to use a load balancing virtual server that uses IPv6 and then routes users to StoreFront servers running IPv6, when users log on, they receive a 500 internal server error. You can change the Web Interface Address to use the StoreFront URL. When you change the URL, users can successfully log on. [#397150]
 38. If users log in with clientless access, connect to SharePoint 2007 and then open My Site, if users select any view and then cancel without making changes, users receive an "Http/1.1 Service Unavailable" error message. [#397920]
 39. When users log on by using clientless access, open SharePoint 2007 and then try to view an RSS feed, a blank page appears. [#397949]
 40. When users log on to SharePoint 2007 by using clientless access, when users try to add a picture on the My Site page, an Object Not Found error appears. [#398439]
 41. When users install the NetScaler Gateway Plug-in on a computer running Windows, third-party tools like the Wireshark packet analyzer that have drivers that fall into the same filter class do not capture all of the outbound traffic. To resolve the issue, you can use the Microsoft Network Monitor tool, or you can clear the DNE check box for the adapter for which you want to capture a packet. Then, when you need to enable the plug-in again, you need to select the DNE check box again. [#399101]
 42. You cannot use the Quick Configuration wizard to configure an additional NetScaler Gateway virtual server if you use the same IP address as for an existing virtual server, but a different port number. When you try to save the configuration, an error occurs. [#399143]
 43. If there is a high availability failover, occasionally ICA connections to applications or desktops do not reconnect. Users need to start the application or desktop again to reestablish the connection. [#399367]
 44. If users connect with the NetScaler Gateway Plug-in for Java and if the NetScaler Gateway virtual IP address is configured with a port number that is not the default, users cannot connect to internal network resources. [#399405]
 45. If you configure Encrypt or Opaque in Clientless access URL encoding, when users log on by using clientless access and try to upload or download a document to the home page, the upload or download fails. [#399449]
 46. When users log on with the NetScaler Gateway Plug-in and Citrix Receiver, when roaming occurs on the user device from a Sprint 3G network to a LAN connection and the 3G connection disconnects automatically, intermittently the NetScaler Gateway session does not resume. [#399841]

47. You cannot create multiple LDAP authentication policies that use the same LDAP server IP address 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](#). [#399872]
48. When users upgrade the NetScaler Gateway Plug-in from the Access Gateway 10, Build 10.0.75.7, after the plug-in installs successfully and users restart their computer and connect with the plug-in, the NetScaler Gateway icon does not appear in the taskbar. [#400166]
49. When users log on by using clientless access and then try to upload multiple documents to My Doc Library on the home page, the browser may stop responding. [#400049]
50. If you configure a TCP compression policy and bind the policy to the NetScaler Gateway virtual server, the NetScaler Gateway Plug-in for Java does not compress traffic. [#400050]
51. When users open Outlook Web Access 2007 by using clientless access with a Chrome browser, when they try to attach a large file, such as a file larger than 5 megabytes (MB), to an email message, an error occurs. [#400052]
52. When users log on to Outlook Web Access 2007 by using clientless access with a Chrome browser, the browser fails intermittently and the page stops responding. [#400053]
53. When users log on to Outlook Web App by using clientless access on a computer running Windows 8 through a Chrome browser, when users compose a new email message, a browser error occurs, and users cannot send the message. [#400057]
54. NetScaler Gateway 10.1 does not show the success and failure counters for LDAP authentication. [#400147]
55. If you configure the DNS order as AThenAAAAQuery or AAAAThenAQuery and if the FQDN is the Secure Ticket Authority (STA), when user attempt to access applications with Receiver, the secondary NetScaler Gateway in a high availability pair fails occasionally. You can use the IP address for the STA instead of the fully qualified domain name (FQDN). You can also change the DNS resolution order to OnlyAQuery or OnlyAAAAQuery. [#400439]
56. Receiver for Windows 8/RT cannot connect to NetScaler Gateway 10.1 unless NetScaler Gateway is configured for two-factor authentication. [#409263]

System Requirements

Sep 05, 2013

This section describes the system requirements for the Citrix NetScaler Gateway appliance.

Before you install the NetScaler Gateway appliance in your network, review the topics in the section [Access Gateway Appliances](#). The topics discuss the appliance hardware, how to install the appliance in a rack and in your network, and how to configure the appliance for the first time.

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. Installation of the Endpoint Analysis Plug-in is automatic and does not require any user intervention.

NetScaler Gateway Plug-in System Requirements

Jun 25, 2014

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 is supported on the following operating systems and Web browsers.

Operating system	32-bit	64-bit	Browser
Mac OS X (10.7, 10.8, 10.9)	x	x	Safari Google Chrome
Windows 8 and Windows 8.1	x	x	
Windows 8 Pro	x	x	
Windows 8 Enterprise	x	x	
Windows 7 Home Basic Edition	x	x	Microsoft Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows 7 Home Premium Edition	x	x	Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows 7 Professional Edition	x	x	Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9

Operating system	32-bit	64-bit	Mozilla Firefox Version 10 Browser
Windows 7 Enterprise Edition	x	x	Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows 7 Ultimate Edition	x	x	Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows Vista Home Basic Edition	x	x	Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows Vista Home Premium Edition	x	x	Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows Vista Enterprise Edition	x	x	Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows Vista Business Edition	x	x	Internet Explorer, Version 7

Operating system	32-bit	64-bit	Internet Explorer, Version 8 Browser
			Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows Vista Ultimate Edition	x	x	Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows XP Home Edition	x		Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10
Windows XP Professional Edition	x		Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox Version 9 Mozilla Firefox Version 10

Endpoint Analysis Requirements

Jan 14, 2014

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 operating system, antivirus, or web browser versions. The Endpoint Analysis Plug-in is distributed as a Windows 32-bit application.

When users connect, NetScaler Gateway installs the Endpoint Analysis Plug-in without requiring user intervention. When users log on subsequently, NetScaler Gateway checks the version of the plug-in. If the versions do not match, NetScaler Gateway updates the plug-in, which then scans the user device.

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

- Windows XP, Windows Vista, Windows 7, or Windows 8 with all service packs and critical updates installed.
- 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.

You can configure endpoint analysis scans to run on user devices to check for protective measures, such as an operating system with or without service packs and antivirus software, before users access resources in the secure network.

Endpoint analysis scans require the Endpoint Analysis Plug-in for Windows that is installed as a Windows 32-bit application. To download and install the plug-in, Windows users must be members of the Administrators or Power Users group on the user device.

The Endpoint Analysis Plug-in downloads and installs on the user device when users log on to NetScaler Gateway for the first time.

Important: 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. The user can access resources for which a scan is not required by using either clientless access or by using Citrix Receiver.

NetScaler Gateway 10.1, Build 120.1316.e supports Advanced Endpoint Analysis on Windows- and Mac-based computers. When users log on from either of these operating systems, the Endpoint Analysis Plug-in installs on the device and the endpoint analysis runs. For more information about Advanced Endpoint Analysis scans, see [Creating Advanced Endpoint Analysis Scans](#).

Plan

Feb 26, 2014

Before you install Citrix NetScaler Gateway 10.1, 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 App Edition
- XenApp
- XenDesktop
- StoreFront
- Web Interface

For more information about deploying NetScaler Gateway, see [Deploying NetScaler Gateway](#).

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:

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

NetScaler Gateway 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 [Configuring 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.

NetScaler Gateway 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](#) in the NetScaler Gateway appliances node and [Installing NetScaler Gateway 10.5](#) in eDocs.

If you are replacing the Secure Gateway with NetScaler Gateway in your network environment, see [Replacing the Secure Gateway with Access Gateway](#).

Ensure that user devices meet the installation prerequisites described in NetScaler Gateway Plug-in System Requirements .	
Identify the mobile devices with which users connect. 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. Note: This is not the fully qualified domain name (FQDN). The FQDN is contained in the signed server certificate that is bound to the virtual server.	
Obtain Universal licenses from the Citrix web site .	
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).	

<p>Write down the administrator password.</p> <p>The default password that comes with NetScaler Gateway is nsroot.</p>	
<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> <p>The maximum ID number is 64.</p>	
<p>Write down the secondary NetScaler Gateway IP address and ID.</p>	
<p>Obtain and install the Universal license on both appliances.</p> <p>You must install the same Universal license on both appliances.</p>	
<p>Write down the RPC node password.</p>	

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 [Configuring Authentication and Authorization](#).

LDAP Authentication

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

<p>Write down the LDAP server IP address and port.</p> <p>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.</p>	
<p>Write down the security type.</p> <p>You can configure security with or without encryption.</p>	
<p>Write down the administrator bind DN.</p> <p>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>.</p>	
<p>Write down the administrator password.</p> <p>This is the password associated with the administrator bind DN.</p>	
<p>Write down the Base DN.</p> <p>DN (or directory level) under which users are located; for example, <code>ou=users, dc=ace, dc=com</code>.</p>	

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

Write down the user field.	
Write down the signing certificate name.	
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. Open only the port appropriate for your NetScaler Gateway configuration. <ul style="list-style-type: none"> • For LDAP connections, the default is TCP port 389. • For a RADIUS connection, the default is UDP port 1812. 	
Write down the XenApp or XenDesktop ports. 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. 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.

Planning for Security with NetScaler Gateway

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.

Deploy

Jan 15, 2014

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.

You can deploy NetScaler Gateway with XenApp 6.5 for Windows Server 2008 R2, XenDesktop 7, StoreFront, and XenMobile App Edition 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.

You can deploy NetScaler Gateway in the following locations in your network:

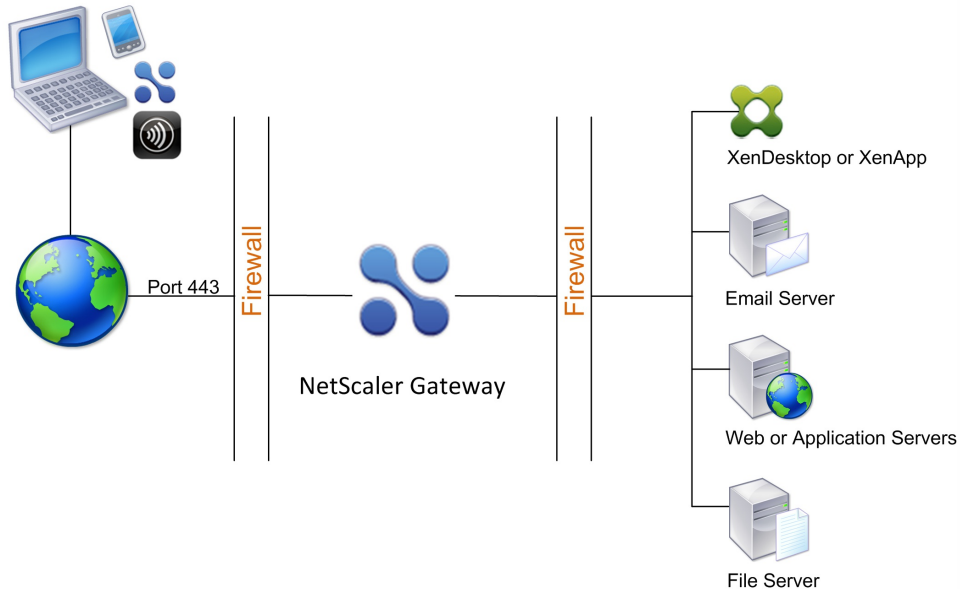
- In the network DMZ
- In a secure network that does not have a DMZ
- With additional NetScaler Gateway appliances to support load balancing and high availability

Deploying NetScaler Gateway 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.

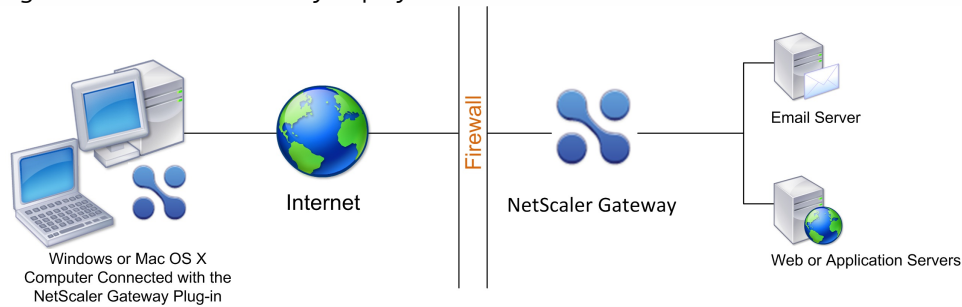
For example, if you authorize external users to access a web server in the internal network, and this server listens for HTTP connections on port 80, you must allow HTTP on port 80 through the second firewall. NetScaler Gateway establishes the connection through the second firewall to the HTTP server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

Deploying NetScaler Gateway 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.

Deploying NetScaler Gateway with XenMobile App Edition, XenApp, and XenDesktop

Mar 25, 2014

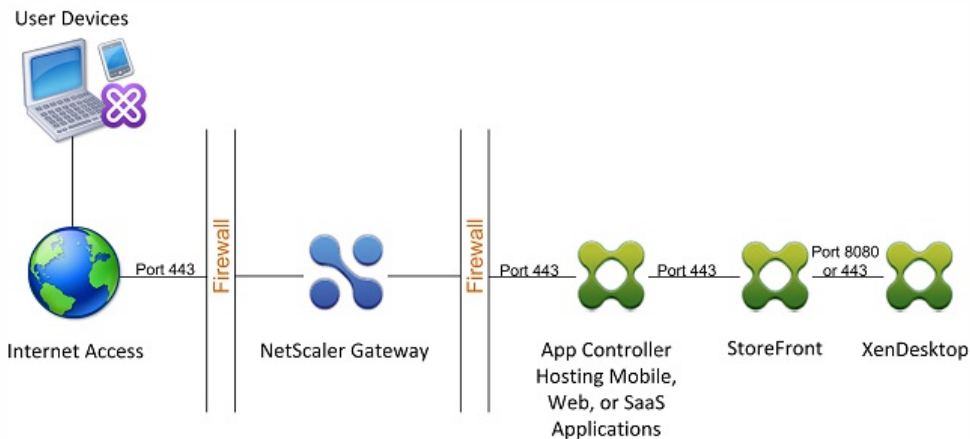
You can have users connect to Windows, web, SaaS, and mobile applications and virtual desktops hosted in your network. You can provide access to your applications and desktops for remote and internal users by using NetScaler Gateway, XenMobile App Edition, and XenApp and XenDesktop. NetScaler Gateway 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.

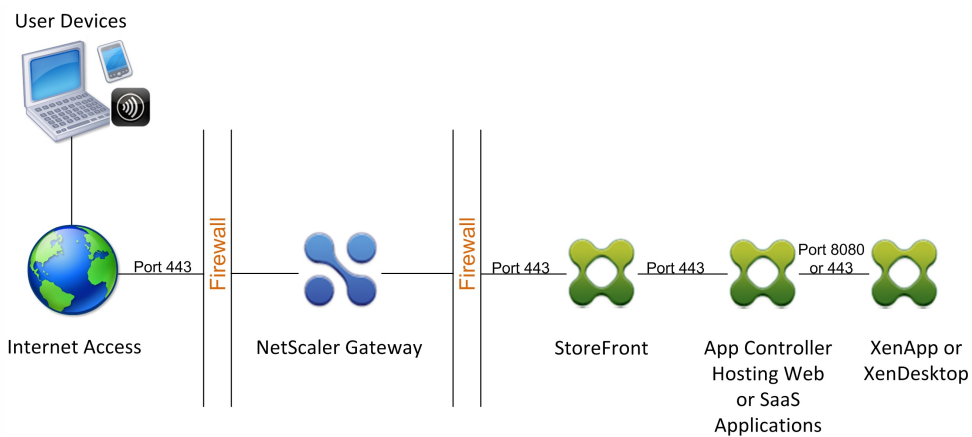
If your deployment provides access to MDX applications from App Controller and access to Windows-based applications from StoreFront, you deploy App Controller in front of StoreFront as shown in the following illustration:

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](#).

Deploying NetScaler Gateway 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:

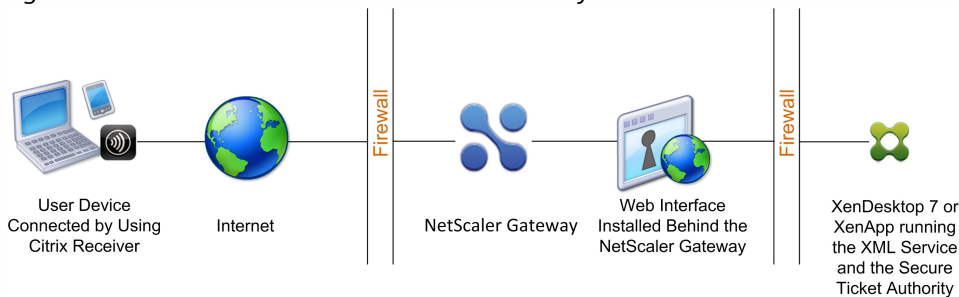
- If your organization protects the internal network with a single DMZ, deploy NetScaler Gateway in the DMZ.
- If your organization protects the internal network with two DMZs, deploy one NetScaler Gateway in each of the two network segments in a double-hop DMZ configuration. For more information, see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

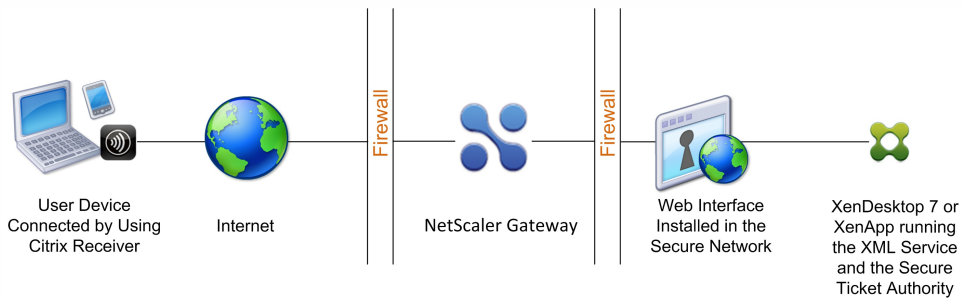


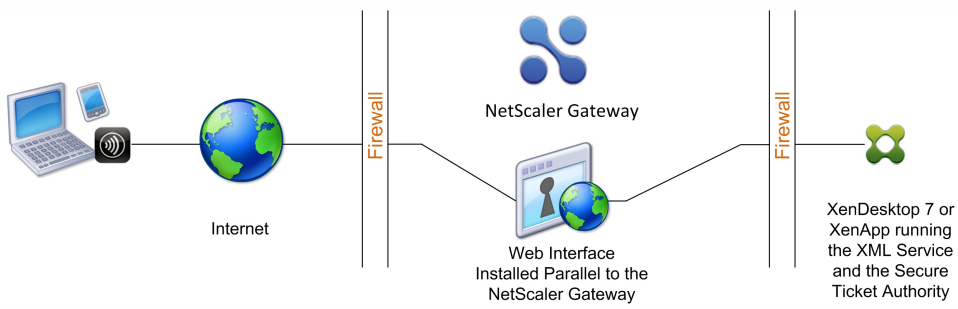
- Deploy NetScaler Gateway parallel to the Web Interface in the DMZ. In this configuration, both NetScaler Gateway and the Web Interface are deployed in the DMZ, but the initial user connection goes to the Web Interface instead of NetScaler Gateway.
- Deploy NetScaler Gateway in the DMZ and deploy the 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.

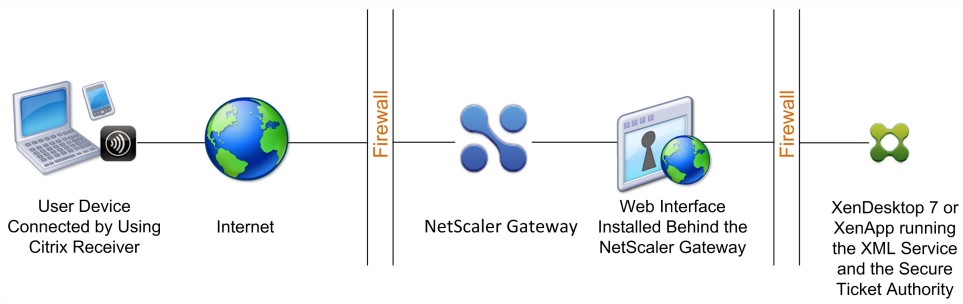
The location in which you deploy the Web Interface depends on a number of factors, including:

- 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.

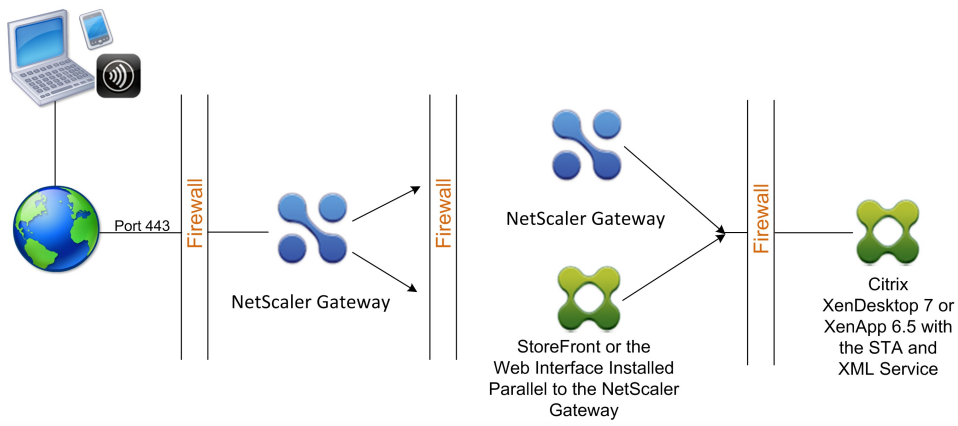






-
-
-

-
-
-
-



-
-
-
-
-
-
-

255.255.0.0

http://192.168.100.1
192.168.100.1

-
-
-

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

-

-

-

-

-
-
-
-
-

-

-

-

-

-

-

-

-

-

-



Login

User Name

Password

Deployment Type

▼ Show Options

To use Secure HTTPS [Click here](#)



Login


User Name

Password

Deployment Type

▼ Show Options

To use Secure HTTPS [Click here](#)

- ☐ Traffic Management
 - **Load Balancing**
 - Content Switching
 - Cache Redirection 
 - DNS
 - GSLB



Getting Started

- Load Balancing wizard
- Load Balancing wizard for Citrix XenApp
- Load Balancing wizard for Citrix XenDesktop



Mobility

[Configure XenMobile, ShareFile and NetScaler Gateway](#)

•
•

-
-
-
-

-
-
-
-
-
-
-

-
-
-

-
-
-

-
-

-
-
-
-

-
-
-

-
-
-
-
-

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.
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.

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.
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 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.

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.
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.

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.
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.
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.
- 2.
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 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.
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.

Upgrading NetScaler Gateway

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 10.1 maintenance release, see article [CTX138708](#) in the Citrix Knowledge Center.

For information about NetScaler Gateway 10.1, Build 120.1316.e, see article [CTX139495](#) in the Citrix Knowledge Center.

To check for software updates

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.

To upgrade the NetScaler Gateway by using the Upgrade Wizard

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

To upgrade the NetScaler Gateway by using a command prompt

1. To upload the software to NetScaler Gateway, use a secure FTP client, such as WinSCP, to connect to the appliance.
2. Copy the software from your computer to the `/var/nsinstall` directory on the appliance.
3. Use a Secure Shell (SSH) client, such as PuTTY, to open an SSH connection to the appliance.
4. Log on to NetScaler Gateway.
5. At a command prompt, type: `shell`
6. To change to the `nsinstall` directory, at a command prompt, type: `cd /var/nsinstall`
7. To view the contents of the directory, type: `ls`
8. To unpack the software, type: `tar -xvzf build_X_XX.tgz`
where `build_X_XX.tgz` is the name of the build to which you want to upgrade.

9. To start the installation, at a command prompt, type: `./installns`
10. When the installation is complete, restart NetScaler Gateway.

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

Licensing

Jul 25, 2013

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

Feb 25, 2014

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 10.1
- Access Gateway 10
- Access Gateway 9.3, Enterprise Edition
- Access Gateway 9.2, Enterprise Edition
- NetScaler VPX

The Platform License

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

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

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

Apr 29, 2013

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, in the navigation pane, expand System and click Licenses.
2. In the details pane, click Manage Licenses.
3. Under Update Licenses, 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 Restart.

To set the maximum number of users

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

- 1.
2. In the details pane, under Settings, click Change authentication 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.

To verify installation of the Universal license by using the configuration utility

1. In the configuration utility, in the navigation pane, expand System and 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.

To verify installation of the Universal license by using the command line

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.

Configure

Mar 18, 2014

After you configure the initial 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.

Creating Additional Virtual Servers

Mar 19, 2014

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.
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.
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: CLIENT.VLAN.ID.EQ (<ipaddressat>) For <ipaddressat>, substitute the ID number assigned to the VLAN.

To create a wildcard virtual server with a listen policy

- 1.
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 High Availability on NetScaler Gateway

May 30, 2013

A high availability deployment of two NetScaler Gateway appliances can provide uninterrupted operation in any transaction. When you configure one appliance as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If, for any reason, the primary node is unable to accept connections, the secondary node takes over.

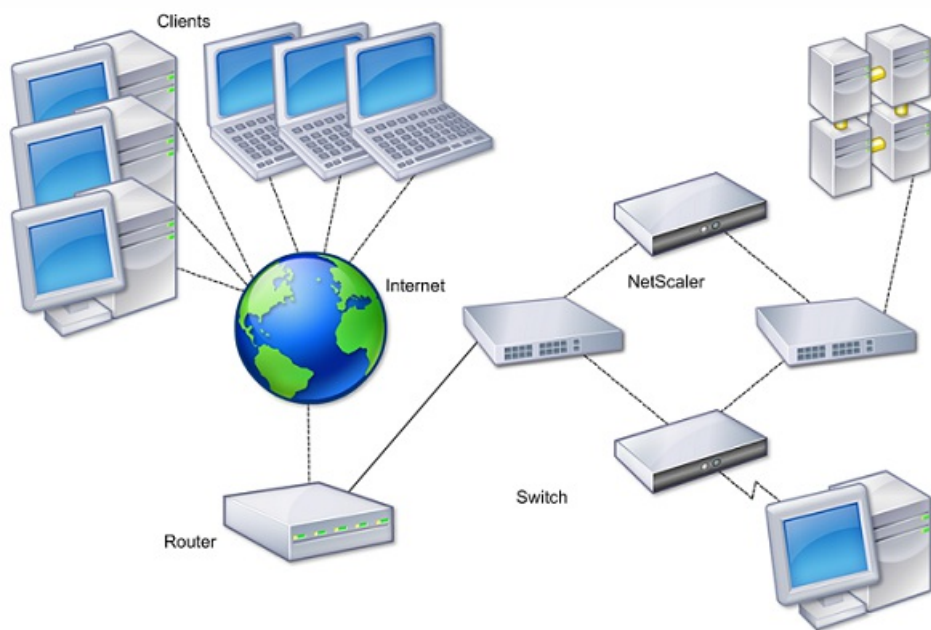
The secondary node monitors the primary by sending periodic messages (often called heartbeat messages or health checks) to determine whether the primary node is accepting connections. If a health check fails, the secondary node retries the connection for a specified period, after which it determines that the primary node is not functioning normally. The secondary node then takes over for the primary (a process called failover).

After a failover, all clients must reestablish their connections to the managed servers, but the session persistence rules are maintained as they were before the failover.

With Web server logging persistence enabled, no log data is lost due to the failover. For logging persistence to be enabled, the log server configuration must carry entries for both systems in the log.conf file.

The following figure shows a network configuration with a high availability pair.

Figure 1. NetScaler Gateway Appliances in a High Availability Configuration



The basic steps to configure high availability are as follows:

1. Create a basic setup, with both nodes in the same subnet.
2. Customize the intervals at which the nodes communicate health-check information.
3. Customize the process by which nodes maintain synchronization.
4. Customize the propagation of commands from the primary to the secondary.
5. Optionally, configure fail-safe mode to prevent a situation in which neither node is primary.
6. Configure virtual MAC addresses if your environment includes devices that do not accept NetScaler Gateway gratuitous ARP messages.

When you are ready for a more complex configuration, you can configure high availability nodes in different subnets.

To improve the reliability of your high availability setup, you can configure route monitors and create redundant links. In some situations, such as when troubleshooting or performing maintenance tasks, you might want to force a node to fail over (assign primary status to the other node), or you might want to force the secondary node to stay secondary or the primary node to stay primary.

How High Availability Works

May 28, 2013

When you configure NetScaler Gateway in a high availability pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway. This is called failover.

The following ports are used to exchange information related to high availability between NetScaler Gateway appliances:

- UDP port 3003 is used to exchange hello packets for communicating the status for intervals.
- TCP port 3010 is used for the high availability configuration synchronization.
- TCP port 3011 is used to synchronize configuration settings.

Guidelines for Configuring High Availability

Before configuring a high availability pair, you should review these guidelines:

- Each NetScaler Gateway appliance must be running the same version of the NetScaler Gateway software. You can find the version number at the top of the page in the configuration utility.
- NetScaler Gateway does not automatically synchronize passwords between two appliances. You can choose to configure each NetScaler Gateway with the user name and password of the other appliance in the pair.
- Entries in the configuration file, `ns.conf`, on both the primary and the secondary NetScaler Gateway must match, with the following exceptions:
 - The primary and secondary NetScaler Gateway appliance must each be configured with its own unique system IP address. Use the Setup Wizard to configure or modify the system IP address on either NetScaler Gateway.
 - In a high availability pair, the NetScaler Gateway ID and associated IP address must point to the other NetScaler Gateway.

For example, if you have two appliances, named AG1 and AG2, you must configure AG1 with the unique NetScaler Gateway ID and IP address of AG2. You must configure AG2 with the unique NetScaler Gateway ID and IP address of AG1.

Note: Each NetScaler Gateway appliance are always identified as Node 0. Configure each appliance with a unique node ID.

- Each appliance in the high availability pair must have the same license. For more information about licensing, see [Installing Licenses on NetScaler Gateway](#).
- If you create a configuration file on either node by using a method that does not go directly through the configuration utility or the command-line interface (for example, importing SSL certificates, or changing to startup scripts), you must copy the configuration file to the other node or create an identical file on that node.
- When you configure a high availability pair, make sure the mapped IP addresses and default gateway address of both the primary and the secondary appliances are identical. If necessary, you can change the mapped IP address at any time by running the Setup Wizard. For more information, see [Configuring Initial Settings by Using the Setup Wizard](#).

You can use the pre-installation checklist to view a list of the specific settings you need to configure in a high availability deployment, For details, see [NetScaler Gateway Pre-Installation Checklist](#).

Configuring Settings for High Availability

Jan 22, 2014

To set up a high availability configuration, you create two nodes, each of which defines the other's NetScaler Gateway IP address as a remote node. You can start by logging on to one of the two NetScaler appliances that you want to configure for high availability and add a node. Specify the other appliance's NetScaler Gateway IP address as the address of the new node. Then, log on to the other appliance and add a node that has the NetScaler Gateway IP address of the first appliance. An algorithm determines which node becomes primary and which becomes secondary.

Before you configure the appliances, add a high availability node. This node represents either the first or second NetScaler Gateway in the high availability pair. To configure high availability, you first create the node and then you configure the high availability settings.

To add a high availability node

- 1.
2. In the details pane, on the Nodes tab, click Add.
3. In the High Availability Setup dialog box, in the HA Setup dialog box, in Remote Node IP Address text box, type the NSIP address of the NetScaler that is to be added as the remote node. If the NetScaler Gateway IP address is an IPv6 address, select the IPv6 check box before entering the address.
4. If you want to add the local node to the remote node automatically, select Configure remote system to participate in High Availability setup. If you do not select this option, you will have to log in to the appliance represented by the remote node and add the node that you are currently configuring.
5. Click to enable Turn off HA monitor on interfaces/channels that are down.
6. If the remote appliance has a different user name and password, in Remote System Logon Credentials, click Login credentials for remote system are different from self node.
7. In User Name, type the user name of the remote appliance.
8. In Password, type the password of the remote appliance.
9. Click OK.

To enable or disable the secondary node

You can disable or enable the secondary node only. When you disable a secondary node, it stops sending heartbeat messages to the primary node, and therefore the primary node can no longer check the status of the secondary node. When you enable a node, the node takes part in the high availability configuration.

- 1.
2. In the details pane, on the Nodes tab, select the local node and then click Open.
3. In the HA Configure Node dialog box, in High Availability Status, select ENABLED (Do not participate in HA).
4. Click OK. A message appears in the status bar, stating that the node has been configured successfully.

To configure settings for high availability

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. In the HA Configure Node dialog box, in ID, type the number of the node identifier. ID specifies the unique node number for the other appliance.
4. In IP Address, type the system IP address and then click OK. The IP Address specifies the IP address of the other

appliance.

Note: The maximum ID for nodes in a high availability pair is 64.

Creating or Changing an RPC Node Password

Jan 21, 2014

To communicate with other NetScaler Gateway appliances, each appliance requires knowledge of the other appliances, including how to authenticate on NetScaler Gateway. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. One RPC node exists on each NetScaler Gateway and stores information, such as the IP addresses of the other NetScaler Gateway appliance and the passwords used for authentication. The NetScaler Gateway that makes contact with another NetScaler Gateway checks the password within the RPC node.

NetScaler Gateway requires RPC node passwords on both appliances in a high availability pair. Initially, each NetScaler Gateway is configured with the same RPC node password. To enhance security, you should change the default RPC node passwords. You use the configuration utility to configure and change RPC nodes.

Note: The NetScaler Gateway administrator password and the RPC node password must be the same. RPC nodes are implicitly created when adding a node or adding a Global Server Load Balancing (GSLB) site. You cannot create or delete RPC nodes manually.

Important: You should also secure the network connection between the appliances. You can configure security when you configure the RPC node password by selecting the Secure check box.

1. In the configuration utility, in the navigation pane, expand System > Network > Advanced and then click RPC.
2. In the details pane, select the node and then click Open.
3. In Password and Confirm Password, type the new password.
4. In Source IP Address, type the system IP address of the other NetScaler Gateway appliance.
To use an IPv6 address, select IPv6 and then enter the IP address.
5. Click Secure and then click OK.

Configuring the Primary and Secondary Appliances for High Availability

Apr 30, 2013

After changing the RPC node password and enabling secure communication, use the configuration utility to configure the primary and secondary NetScaler Gateway.

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under High Availability Status, click Enabled (Actively Participate in HA) and then click OK.

Configuring Communication Intervals

Apr 30, 2013

When you configure NetScaler Gateway as a high availability pair, you can configure the secondary NetScaler Gateway to listen at specific intervals, measured in milliseconds (msec). These intervals are known as hello intervals and dead intervals.

The hello interval is the interval at which the heartbeat messages are sent to the peer node. The dead interval is the time interval after which the peer node is marked DOWN if heartbeat packets are not received. The heartbeat messages are UDP packets sent to port 3003 of the other node in a high availability pair.

When you configure the hello interval, you can use the values 200 to 1000. The default value is 200.

The dead interval values are 3 to 60. The default value is 3.

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under Intervals, do one or both of the following:
 - In Hello Interval (msec), type the value and then click OK. The default is 200 milliseconds.
 - In Dead Interval (secs), type the value and then click OK. The default setting is three seconds.

Synchronizing NetScaler Gateway Appliances

Feb 27, 2014

Automatic synchronization of NetScaler Gateway appliances in a high availability pair is enabled by default. With automatic synchronization, you can make changes to one appliance and enable the changes to propagate automatically to the second appliance. Synchronization uses port 3010.

Synchronization starts when the following occurs:

- The secondary node restarts.
- The primary node becomes secondary after a failover.

You can disable synchronization, which prevents the secondary NetScaler Gateway from synchronizing its configuration with the primary NetScaler Gateway when a change occurs on the primary appliance. You can also force synchronization.

You enable or disable high availability synchronization on the secondary node in the pair.

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. In the Configure Node dialog box, under HA Synchronization, do one of the following:
 - To disable synchronization, clear the Secondary node will fetch the configuration from Primary check box.
 - To enable synchronization, select the Secondary node will fetch the configuration from Primary check box.
4. Click OK. A message appears in the status bar stating that the node configuration is successful.

In addition to automatic synchronization, NetScaler Gateway supports forced synchronization between the two nodes in a high availability pair.

You can force synchronization on both the primary and secondary NetScaler Gateway appliances. However, if synchronization is already in progress, the command fails and NetScaler Gateway displays a warning. Forced synchronization also fails in the following circumstances:

- You force synchronization on a standalone system.
- The secondary node is disabled.
- You disable high availability synchronization on the secondary node.

- 1.
2. On the Nodes tab, click Force Synchronization.

Synchronizing Configuration Files in a High Availability Setup

Jan 22, 2014

In a high availability setup, you can synchronize various configuration files from the primary node to the secondary node.

Mode

The type of synchronization to be performed. The following descriptions include, in parentheses, the command-line argument that specifies the option.

- **Everything except licenses and rc.conf** (all). Synchronizes files related to system configuration, NetScaler Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, and Application Firewall XML objects.
- **Bookmarks** (bookmarks). Synchronizes all NetScaler Gateway bookmarks.
- **SSL certificates and keys** (ssl). Synchronizes all certificates, keys, and CRLs for the SSL feature.
- **Licenses and rc.conf** (misc). Synchronizes all license files and the rc.conf file.
- **Everything including licenses and rc.conf** (all_plus_misc). Synchronizes files related to system configuration, NetScaler Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, Application Firewall XML objects, licenses, and the rc.conf file.

Note: There are more options available if you install a NetScaler license on the appliance.

1. In the navigation pane, expand System and then click Diagnostics.
2. In the details pane, under Utilities, click Start HA files synchronization.
3. In the Start file synchronization dialog box, in the Mode drop-down list, select the appropriate type of synchronization (for example, Everything except licenses and rc.conf) and then click OK.

Configuring Command Propagation

Jan 22, 2014

In a high availability setup, any command issued on the primary node propagates automatically to, and runs on, the secondary node before the command runs on the primary node. If command propagation fails, or if command execution fails on the secondary node, the primary node executes the command and logs an error. Command propagation uses port 3011.

In a high availability pair configuration, command propagation is enabled by default on both the primary and secondary nodes. You can enable or disable command propagation on either node in a high availability pair. If you disable command propagation on the primary node, commands are not propagated to the secondary node. If you disable command propagation on the secondary node, commands propagated from the primary are not executed on the secondary node.

Note: After reenabling propagation, remember to force synchronization.

Note: If synchronization occurs while you are disabling propagation, any configuration-related changes that you make before the disabling of propagation takes effect are synchronized with the secondary node. This is also true for cases in which propagation is disabled while synchronization is in progress.

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under HA propagation, do one of the following:
 - To disable high availability propagation, clear the Primary node will propagate configuration to the Secondary check box.
 - To enable high availability propagation, select the Primary node will propagate configuration to the Secondary check box.
4. Click OK.

Troubleshooting Command Propagation

Apr 27, 2013

The following list describes the reasons command propagation may fail, as well as solutions for restoring the setting:

- Network connectivity is not active. If a command propagation fails, check the network connection between the primary and secondary NetScaler Gateway appliances.
- Missing resources on secondary NetScaler Gateway. If a command execution succeeds on the primary NetScaler Gateway but fails to propagate to the secondary NetScaler Gateway, run the command directly on the secondary NetScaler Gateway to see the error message. The error may have occurred because the resources required by the command are present on the primary NetScaler Gateway and are not available on the secondary NetScaler Gateway. Also, verify that the license files on each appliance match.
For example, verify that all of your Secure Sockets Layer (SSL) certificates are present on each NetScaler Gateway. Verify that any initialization script customization exists on both NetScaler Gateway appliances.
- Authentication failure. If you receive an authentication failure error message, verify the RPC node settings on each appliance.

Configuring Fail-Safe Mode

Apr 30, 2013

In a high availability configuration, fail-safe mode ensures that one node is always primary when both nodes fail the health check. Fail-safe mode ensures that when a node is only partially available, backup methods can activate and can handle traffic.

You configure high availability fail-safe mode independently on each node.

The following table shows some of the fail-safe cases. The NOT_UP state means that the node failed the health check and yet the node is partially available. The UP state means that the node passed the health check.

Table 1. Fail-Safe Mode Cases

Node A (primary) health state	Node B (secondary) health state	Default high availability behavior	Fail-safe enabled high availability behavior	Description
NOT_UP (failed last)	NOT_UP (failed first)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If both nodes fail, one after the other, the node that was the last primary node remains primary.
NOT_UP (failed first)	NOT_UP (failed last)	A (Secondary), B (Secondary)	A (Secondary), B (Primary)	If both nodes fail, one after the other, the node that was the last primary node remains primary.
UP	UP	A (Primary), B (Secondary)	A (Primary), B (Secondary)	If both nodes pass the health check, no change in behavior with fail-safe enabled.
UP	NOT_UP	A (Primary), B (Secondary)	A (Primary), B (Secondary)	If only the secondary node fails, no change in behavior with fail-safe enabled.
NOT_UP	UP	A (Secondary), B (Primary)	A (Secondary), B (Primary)	If only the primary fails, no change in behavior with fail-safe enabled.
NOT_UP	UP (STAYSECONDARY)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If the secondary is configured as STAYSECONDARY, the primary remains primary even if it fails.

1.

2. In the details pane, on the Nodes tab, select a node and click Open.
3. In the Configure Node dialog box, under Fail-Safe Mode, select Maintain one Primary node even when both nodes are unhealthy and then click OK.

Configuring the Virtual MAC Address

Apr 30, 2013

The virtual MAC address is shared by the primary and secondary NetScaler Gateway appliances in a high availability setup.

In a high availability setup, the primary NetScaler Gateway owns all the floating IP addresses, such as the mapped IP address or the virtual IP address. It responds to address resolution protocol (ARP) requests for these IP addresses with its own MAC address. As a result, the ARP table of an external device (such as a router) is updated with the floating IP address and the primary NetScaler Gateway MAC address. When a failover occurs, the secondary NetScaler Gateway takes over as the new primary NetScaler Gateway. It then uses gratuitous address resolution protocol (GARP) to advertise the floating IP addresses that it acquired from the primary appliance. The MAC address, which the new primary appliance advertises, is that of its own interface.

Some devices do not accept GARP messages generated by NetScaler Gateway. As a result, some of the external devices retain the old IP-to-MAC mapping advertised by the old primary NetScaler Gateway. This situation can cause a site to become unavailable. To resolve the problem, you configure a virtual MAC address on both NetScaler Gateway appliances of a high availability pair. This configuration implies that both NetScaler Gateway appliances have identical MAC addresses. As a result, when failover occurs, the MAC address of the secondary NetScaler Gateway remains unchanged and ARP tables on the external devices do not need to be updated.

To create a virtual MAC address, create a virtual router identifier (ID) and bind it to an interface. In a high availability setup, the user needs to bind the ID to the interfaces on both the appliances.

When the virtual router ID is bound to an interface, the system generates a virtual MAC address with the virtual router ID as the last octet. An example of the generic virtual MAC address is 00:00:5e:00:01:<VRID>. For example, if you created a virtual router ID of value 60 and bind it to an interface, the resulting virtual MAC address is 00:00:5e:00:01:3c, where 3c is the hex representation of the virtual router ID. You can create 255 virtual router IDs ranging from 1 through 254.

You can configure virtual MAC addresses for IPv4 and IPv6.

Configuring IPv4 Virtual MAC Addresses

May 29, 2013

When you create a IPv4 virtual MAC address and bind it to a interface, any IPv4 packet sent from the interface uses the virtual MAC address that is bound to the interface. If there is no IPv4 virtual MAC address bound to an interface, the interface's physical MAC address is used.

The generic virtual MAC address is of the form 00:00:5e:00:01:<VRID>. For example, if you create a VRID with a value of 60 and bind it to an interface, the resulting virtual MAC address is 00:00:5e:00:01:3c, where 3c is the hex representation of the VRID. You can create 255 VRIDs with values from 1 to 255.

Creating or Modifying an IPv4 virtual MAC address

Jan 22, 2014

You create an IPv4 virtual MAC address by assigning it a virtual router ID. You can then you bind the virtual MAC address to an interface. You cannot bind multiple virtual router IDs to the same interface. To verify the virtual MAC address configuration, you should display and examine the virtual MAC address and the interfaces bound to the virtual MAC address.

VrID

The virtual router ID that identifies the virtual MAC address. Possible values: 1 to 255.

if num

The interface number (slot/port notation) to be bound to the virtual MAC address.

- 1.
2. In the details pane, on the VMAC tab, click Add.
3. In the Create VMAC dialog box, in Virtual Router ID, type the value.
4. Under Associated Interfaces, in Available Interfaces, select a network interface, click Add, click Create and then click Close.

After you create the virtual MAC address, it appears in the configuration utility. If you selected a network interface, the virtual router ID is bound to that interface.

To delete a virtual MAC address, you need to delete the corresponding virtual router ID.

- 1.
2. In the details pane, select an item and then click Remove.

When you created the virtual router ID, you selected a network interface on NetScaler Gateway and then bound the virtual router ID to the network interface. You can also unbind a virtual MAC address from the network interface, but leave the MAC address configured on NetScaler Gateway.

- 1.
2. In the details pane, select an item and then click Open.
3. Under Configured Interfaces, select a network interface, click Remove, click OK and then click Close.

Configuring IPv6 virtual MAC addresses

Apr 27, 2013

The NetScaler Gateway supports virtual MAC addresses for IPv6 packets. You can bind any interface to a virtual MAC address for IPv6, even if an IPv4 virtual MAC address is bound to the interface. Any IPv6 packet sent from the interface uses the virtual MAC address bound to that interface. If there is no virtual MAC address bound to an interface, an IPv6 packet uses the physical MAC.

Creating or Modifying a Virtual MAC Address for IPv6

Jan 22, 2014

You create an IPv6 virtual MAC address by assigning it an IPv6 virtual router ID. You can then you bind the virtual MAC address to an interface. You cannot bind multiple IPv6 virtual router IDs to an interface. To verify the virtual MAC address configuration, you should display and examine the virtual MAC addresses and the interfaces bound to the virtual MAC address.

Virtual Router ID

The virtual router ID that identifies the virtual MAC address. Possible values: 1 to 255.

if num

The interface number (slot/port notation) to be bound to the virtual MAC address.

- 1.
2. In the details pane, on the VMAC6 tab, do one of the following:
 - To create a new virtual MAC address, click Add.
 - To modify an existing virtual MAC address, click Open.
3. In the Create VMAC6 or Configure VMAC6 dialog box, in Virtual Router ID, enter the value, such as vrID6.
4. In Associate Interfaces, click Add, click Create and then click Close. A message appears in the status bar, stating that the virtual MAC address is configured.

- 1.
2. In the details pane, on the VMAC6 tab, select the virtual router ID that you want to remove and then click Remove. A message appears in the status bar, stating that the virtual MAC address is removed.

Configuring High Availability Pairs in Different Subnets

Jan 21, 2014

A typical high availability deployment is when both appliances in a high availability pair reside on the same subnet. A high availability deployment can also consist of two NetScaler Gateway appliances in which each appliance is located in a different network. This topic describes the latter configuration, and includes sample configurations and a list of differences among the high availability configurations within one network and across networks.

You can also configure link redundancy and route monitors. These NetScaler Gateway functions are helpful in a cross-network high availability configuration. The functions also cover the health check process used by each NetScaler Gateway to ensure that the partner appliance is active.

The NetScaler Gateway appliances are connected to different routers, called R3 and R4, on two different networks. The appliances exchange heartbeat packets through these routers. A heartbeat packet is a signal that occurs at regular intervals that ensures the connection is still active. You can expand this configuration to accommodate deployments involving any number of interfaces.

Note: If you use static routing on your network, you must add static routes between all the systems to ensure that heartbeat packets are sent and received successfully. (If you use dynamic routing on your systems, static routes are unnecessary.)

When the appliances in a high availability pair reside on two different networks, the secondary NetScaler Gateway must have an independent network configuration. This means that NetScaler Gateway appliances on different networks cannot share mapped IP addresses, virtual LANs, or network routes. This type of configuration, in which the NetScaler Gateway appliances in a high availability pair have different configurable parameters, is known as

— *independent network configuration*

or

— *symmetric network configuration*

The following table summarizes the configurable parameters for an independent network configuration, and shows how you must set them on each NetScaler Gateway:

Configurable parameters	Behavior
IP addresses	NetScaler Gateway specific. Active only on that appliance.
Virtual IP address	Floating.
Virtual LAN	NetScaler Gateway specific. Active only on that appliance.
Routes	NetScaler Gateway specific. Active only on that appliance. A link load balancing (LLB) route is floating.
access control lists	Floating (common). Active on both appliances.

(ACLs) Configurable parameters	Behavior
Dynamic routing	NetScaler Gateway specific. Active only on that appliance. The secondary NetScaler Gateway should also run the routing protocols and peer with upstream routers.
L2 mode	Floating (common). Active on both appliances.
L3 mode	Floating (common). Active on both appliances.
Reverse Network Address Translation (NAT)	NetScaler Gateway specific. Reverse NAT with a virtual IP address because the NAT IP address is floating.

Adding a Remote Node

Jan 21, 2014

When two nodes of a high availability pair reside on different subnets, each node must have a different network configuration. Therefore, to configure two independent systems to function as a high availability pair, you must specify independent network computing mode during the configuration process.

When you add a high availability node, you must disable the high availability monitor for each interface that is not connected or being used for traffic.

- 1.
2. In the details pane, click the Nodes tab, and then click Add.
3. In the High Availability Setup dialog box, in the Remote Node IP Address text box, type the NetScaler Gateway IP address of the appliance that is the remote node.
To use an IPv6 address, click the IPv6 check box before entering the IP address.
4. If you want to add the local node to the remote node automatically, select Configure remote system to participate in High Availability setup. If you do not select this option, you need to log on to the appliance represented by the remote node and add the node that you are currently configuring.
5. Click to enable Turn off HA monitor on interfaces/channels that are down.
6. Click to enable Turn on INC (Independent Network Configuration) mode on self mode.
7. Click OK. The Nodes page displays the local and remote nodes in your high availability configuration.

- 1.
2. In the details pane, click the Nodes tab.
3. Select the node that you want to remove, click Remove and then click Yes.

Configuring Route Monitors

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.

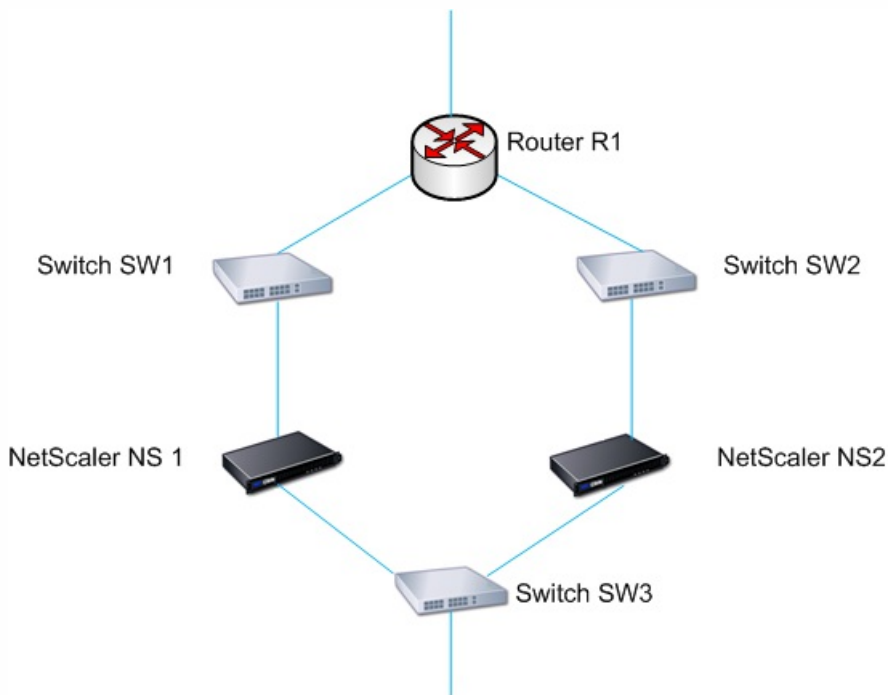
When a NetScaler Gateway appliance has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes for the static routes. The monitored static route removes unreachable static routes from the internal routing table. If you 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">• reboot• failover• set route6 command for v6 routes• set route msr enable/disable command for v4 routes• adding a new route monitor	Not applicable.

Route monitors are useful when you disable Independent Network Configuration mode and you want a gateway from a primary node as unreachable as one of the conditions for high availability failover.

For example, you disable Independent Network Configuration in a high availability setup in a two-arm topology that has NetScaler Gateway appliances NS1 and NS2 in the same subnet, with router R1 and switches SW1, SW2, and SW3, as shown in the following figure. Because R1 is the only router in this setup, you want the high availability setup to 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.
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.
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.
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.
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.
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."

To force failover on the primary or secondary node

- 1.
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.

To force the primary node to stay primary

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
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.

To force the secondary node to stay secondary

- 1.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under High Availability Status, click Stay Secondary (Remain in Listen Mode) and then click OK.

To return NetScaler Gateway to service as an active high availability appliance

- 1.
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.

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. Follow the directions in the wizard until you come to the Specify a server certificate page.
2. 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.
3. Click Create to save the certificate on your computer and then click Close.
4. 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 details pane, under SSL Certificates, click Create CSR (Certificate Signing Request).
2. Complete the settings for the certificate and then click Create.

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

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.
2. In the details pane, click a virtual server and 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.
2. In the details pane, click a virtual server and click Open.
3. On the Certificates tab, under Configured, select the test certificate and then click Remove.

Configuring Intermediate Certificates

Jan 22, 2014

An

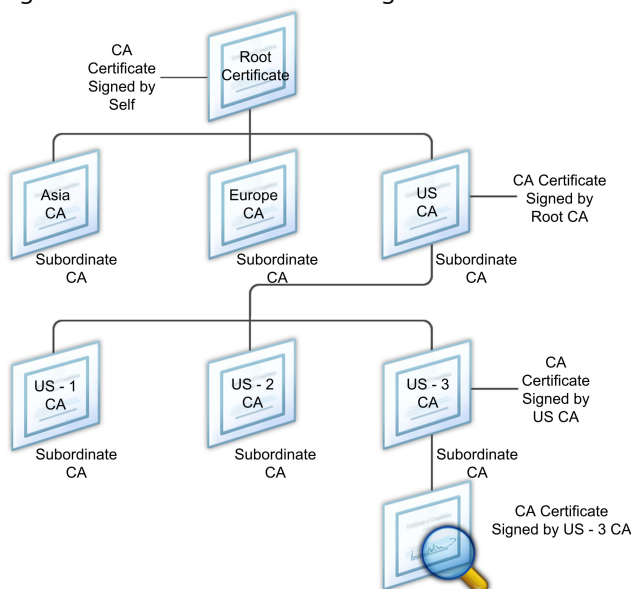
— *intermediate certificate*

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.
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.
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.

Creating Device Certificates for Authentication

Jan 21, 2014

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 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 [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

Oct 09, 2013

After you install device certificates on NetScaler Gateway, you need to enable and then bind the certificates to the virtual server.

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. In the Configure NetScaler Gateway Virtual Server dialog box, click Enable device certificate and then click OK. The device certificates installed on NetScaler Gateway appear automatically in Device certificate CA.

Importing and Installing an Existing Certificate to NetScaler Gateway

Mar 25, 2014

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.
- 2.
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

Jan 21, 2014

- 1.
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 (OCSP), 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.

Configuring Policies and Profiles on NetScaler Gateway

Jan 22, 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, see the following:

- [Configuring Authentication and Authorization](#)
- [Configuring Clientless Access](#)
- [Configuring Endpoint Polices](#)

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 [Integrating NetScaler Gateway 10.1 with XenMobile, StoreFront and the Web Interface](#).

For more information about configuring NetScaler Gateway to work with Citrix XenApp, see [Integrating NetScaler Gateway with XenApp or XenDesktop](#).

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.

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.

Configuring Client Security Expressions

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

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

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.

To create a named expression

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

May 09, 2013

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
```

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 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.

- 1.
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.

- 1.
2. In the details pane, click the Profiles tab and 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.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and 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
-
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.

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.

- 1.
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](#).

- 1.
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.

- 1.
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.

- 1.
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 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.

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.

- 1.
2. In the details pane, on the Policies tab, select the traffic policy and then click Remove.

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 Additional 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
```

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.

- 1.
2. In the details pane, click the Profiles tab and click Add.
3. In Name, type a name for the profile.
4. In File Type Association, select ON, click Create and then click Close.

- 1.

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.

Configuring Authentication and Authorization

May 01, 2013

Authentication allows users to log on to NetScaler Gateway and connect to resources in the internal network.

Authentication provides security for your internal network. You configure authentication through policies. After you configure authentication, you can add the policy globally or to virtual servers.

Authorization defines the resources within the secure network to which users have access. You configure authorization using LDAP and RADIUS.

Configuring Authentication on Access Gateway

Jun 22, 2011

Access Gateway employs a flexible authentication design that permits extensive customization of user authentication for Access Gateway. You can use industry-standard authentication servers and configure Access Gateway to authenticate users with the servers. Access Gateway also supports authentication based on attributes present in a client certificate.

Access 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 Access 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.

Access 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.

Authentication Types Supported on NetScaler Gateway

May 27, 2013

NetScaler Gateway supports 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.

Configuring Default Global Authentication Types

Jan 22, 2014

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.

- 1.
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 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.

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.

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.

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.

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.

To create a new group

1. In the configuration utility, click the Configuration tab and in the navigation pane, expand NetScaler Gateway > User Administration and then click AAA Groups.
2. In the details pane, click Add.
3. In Group Name, type a name for the group, click Create, and then click Close.

To delete a group

You can also delete user groups from NetScaler Gateway.

1. In the configuration utility, click the Configuration tab and in the navigation pane, expand NetScaler Gateway > User Administration and then click AAA Groups.
2. In the details pane, select the group and then click Remove.

Adding Users to Groups

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.

To add users to groups

1. In the configuration utility, click the Configuration tab and in the navigation pane, expand NetScaler Gateway > User Administration and then click AAA 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. Group2 is bound with a session policy configured with home page www.homepage2.com. When these policies are bound to respective groups without a priority number or with same priority number, the home page that appears to users who belong to both the groups depends on which policy is processed first. By setting a lower priority number, which gives higher precedence, for the session policy with home page www.homepage1.com, you can ensure that users who belong to both the groups will always receive the home page www.homepage1.com.

If session policies do not have a priority number assigned or have the same priority number, precedence is evaluated in the following order:

- User
- Group
- Virtual server
- Global

If policies are bound to the same level, without a priority number or if the policies have the same priority number, the order of evaluation is per the policy bind order. Policies that are bound first to a level receive precedence over policies bound later.

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.
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.
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.
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.
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.
- 2.
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.
- 2.
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 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, 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

Mar 30, 2017

1. On the **Configuration** tab, present under the configuration utility, navigate to **NetScaler Gateway > Policies > Authentication/Authorization > 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 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.
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.
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 SAML Authentication on NetScaler Gateway

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.
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 NetScaler Gateway to Use One-Time Passwords

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.

To configure single sign-on by using returned passwords

- 1.
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 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.

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.
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 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 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.

To configure the client certificate as the default authentication type

- 1.
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.

Extracting the User Name from the Client Certificate

If client certificate authentication is enabled on NetScaler Gateway, users are authenticated based on certain attributes of the client certificate. After authentication is 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.

To configure a client certificate authentication policy

- 1.
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 click Close.

To bind a client certificate policy to a virtual server

After you configure the client certificate authentication policy, you can bind it to a virtual server.

- 1.
2. In the details pane, click a virtual server and click Open.
3. In the Configure NetScaler Gateway Virtual Server dialog box, click the Authentication tab.
4. Click Primary or Secondary.
5. Under Details, click Insert Policy.
6. In Policy Name, select the policy and then click OK.

To configure a virtual server to request the client certificate

When you want to use a client certificate for authentication, you must configure the virtual server so that client certificates are requested during the SSL handshake.

- 1.
2. In the details pane, click a virtual server and 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

Feb 27, 2014

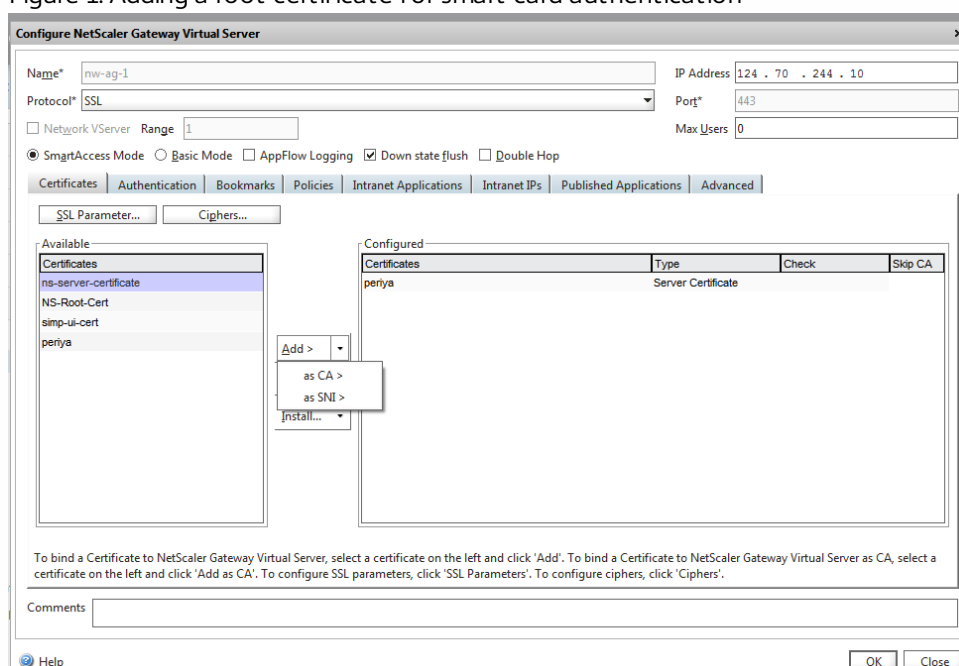
You can configure NetScaler Gateway to use a cryptographic smart card to authenticate users.

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.

Configuring Smart Card Authentication with Secure ICA Connections

If users log on by using a smart card with single sign-on configured on NetScaler Gateway and establish a secure ICA connection, users 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, and so 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, configure a second virtual server that is dedicated to the ICA SSL relay and disable the client certificate authentication requirement. In this way, users log on to the first virtual server and the second virtual server is used for the ICA connection. To enable smart card authentication with secure ICA connections, you need to configure the Web Interface to use the Gateway Direct method. On NetScaler Gateway, you configure the Secure Ticket Authority (STA) and bind it to the virtual server.

For more information about configuring the Web Interface, see [Configuring NetScaler Gateway Settings in Web Interface 5.3](#).

To create a second virtual server for ICA connections

- 1.
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 for the virtual server.
5. In Max Users, type the number of users allowed to log on to the virtual server.
6. On the Certificates tab, click SSL Parameter.
7. In the Configure SSL Params dialog box, under Others, clear Client Authentication and then click OK.
8. Bind the server certificate to the virtual server, click Create and then click Close.

After you configure the new virtual server, bind one or more STA servers to the virtual server. For more information, see [Configuring the Secure Ticket Authority on NetScaler Gateway](#).

To test smart card authentication

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

Configuring 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.
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 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.
2. Select the policy that is bound globally and then in Action, click Global Bindings.
3. In the Bind/Unbind Authentication Global Policies 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.
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.
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.
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.
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.

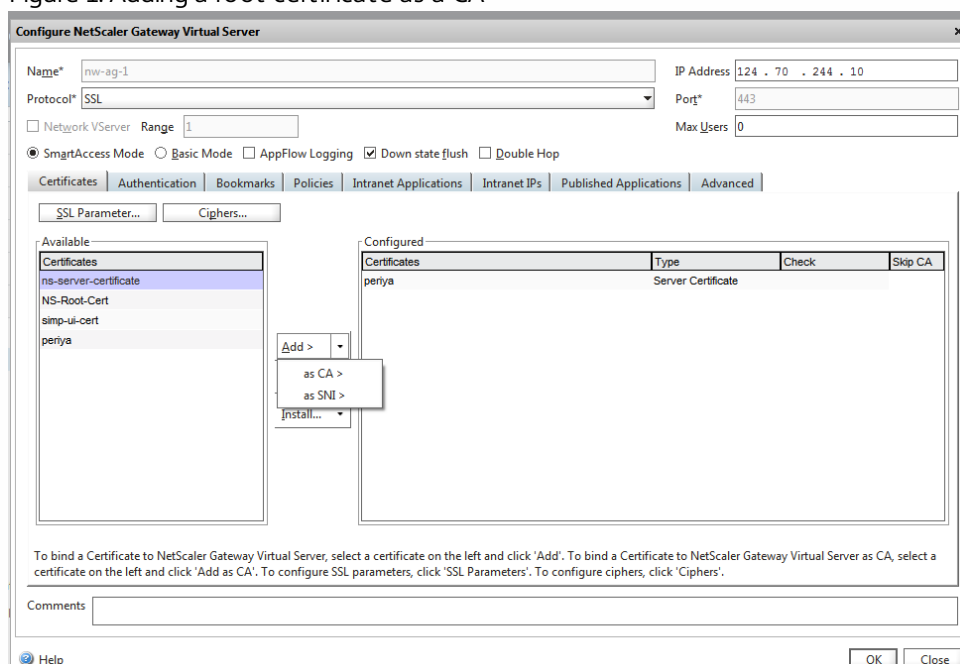
- 1.
2. In the details pane, click Install.
3. In Certificate - Key Pair Name, type a name for the certificate.
4. In Certificate File Name, click Browse and in the drop-down box, select either Appliance or Local.
5. Navigate to the root certificate, click Open and then click Install.

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.
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.

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 click Open.
3. On the Authentication tab, under User Authentication, click to clear Enable Authentication.

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.

To set the global user limit

When you configure the user limit globally, the restriction applies to all users who establish sessions to different virtual servers on the system. When the number of user sessions reaches the value you set, no new sessions can be established on any virtual server present on NetScaler Gateway.

You set the maximum number of users at the global level when you set the default authentication type for NetScaler Gateway.

- 1.
2. In the details pane, under Settings, click Change authentication settings.
3. In the Global Authentication Settings dialog box, in Maximum Number of Users, type the number of users and then click OK.

To set the user limit per virtual server

You can also apply the user limit to each virtual server on the system. When you configure the user limit per virtual server, the restriction applies only to users who establish sessions with the particular virtual server. Users who establish sessions with other virtual servers are not affected by this limit.

- 1.
2. In the details pane, click a virtual server and click Open.
3. In Max Users, type the number of users and then click OK.

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.
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.

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.

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.
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.

Configuring Authorization Policies

Jan 24, 2014

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.

To configure an authorization policy

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication/Authorization.
2. Click Authorization.
3. In the details pane, click Add.
4. In Name, type a name for the policy.
5. In Action, select Allow or Deny.
6. In Expression, click Add.
7. Configure the expression, click OK, click Create and then click Close.

Binding Authorization Policies and Setting the Priority

Jan 24, 2014

When you configure the authorization policy, you then bind it to a user or group. You can use either the the configuration utility to bind the policy.

By default, authentication and authorization polices are validated first against policies that you bind to the virtual server and then against policies bound globally. If you bind an authentication or authorization 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 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.

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.
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.

To configure LDAP nested group extraction

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway > Policies > Authentication/Authorization > Authentication >> Authentication and then click LDAP.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Server, click New.
5. In Name, type the name of the server.
6. Configure the settings for the LDAP server.
7. Expand Nested Group Extraction and then click Enable.
8. In Maximum Nesting Level, type the number of levels that NetScaler Gateway checks.
9. In Group Name Identifier, type the LDAP attribute name that uniquely identifies a group name on the LDAP server, such as `sAMAccountName`.
10. In Group Search Attribute, type the LDAP attribute name that is to be obtained in the search response to determine the parent groups of any group, 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.

To create the session profiles for group extraction

- 1.
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 Child.
6. Next to Single Sign-On Domain, clear the name of the first Windows domain and type the name of the second domain, click Create and then click Close.

After you create the session profiles, you create two session policies. Each session policy uses one of the profiles.

To create a session policy

- 1.
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.

To create authentication profiles for multiple domain group extraction

- 1.
2. In the navigation pane, click LDAP.
3. In the details pane, click the Servers tab and then click Add.
4. In Name, type the name of the first domain, such as Sampa.
5. Configure the settings for the LDAP server and then click Create.
6. Repeat Steps 3, 4, and 5 to configure the authentication profile of the second domain and then click Close.

After you create and save the profiles, create the authentication policies.

To create authentication policies for multiple domain group extraction

- 1.
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.

To create groups on NetScaler Gateway

- 1.
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.

To bind the authentication policies to a virtual server

- 1.
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 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

Jan 24, 2014

- 1.
2. Click RADIUS.
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 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 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.
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.
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.
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.
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.
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.
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.

- 1.
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.

- 1.
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.

- 1.
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.

1. In the details pane, on the Policies tab, click Add.
2. In Name, type a name for the policy.
3. Next to Request Profile, click New.
4. In Name, type a name for the profile.
5. On the Security tab, click Advanced.
6. Under Client Security, click Override Global and then click New.
7. Configure the client security expression and then click Create.
8. Under Client Security, in Quarantine Group, select a group.
9. In Error Message, type the message you want users to receive if the post-authentication scan fails.
10. Under Authorization Groups, click Override Global, select a group, click Add, click OK 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.

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.

- 1.
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.
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.

- 1.
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.

- 1.
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.
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.

- 1.
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.

1. In the configuration utility, in the navigation pane, do one of the following:
 - 1.
 - 2.
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.

1. In the configuration utility, in the navigation pane, do one of the following:
 - 1.
 - 2.
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.

1. In the configuration utility, in the navigation pane, do one of the following:
 - 1.
 - 2.
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

1. In the configuration utility, in the navigation pane, do one of the following:
 - 1.
 - 2.
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.

1. In the configuration utility, in the navigation pane, do one of the following:
 - 1.
 - 2.
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.

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
```

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
```

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

Example:

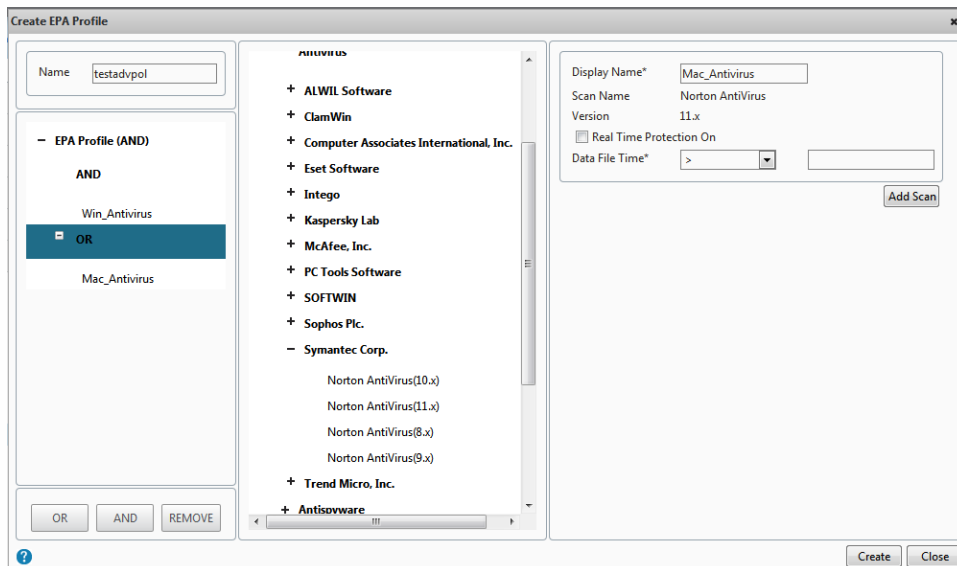
The following client security check passes if the file c:\sophos_virus_defs.dat file is NOT more than two days old:

```
!(client.file(c:\\\\sophos_virus_defs.dat).timestamp==2dy)
```

Creating Advanced Endpoint Analysis Scans

Jan 27, 2014

NetScaler Gateway supports advanced endpoint analysis for users who log on from Windows or Mac OS X computers. NetScaler Gateway contains advanced, built-in endpoint analysis scans. You can use the scans to create advanced endpoint scan packages for a wide variety of software products. When you create a policy in the configuration utility, all available scan types are shown in a tree view in the center pane of the EPA Profile dialog box. In the right pane, you configure the parameters and then you add the scan. The settings for the profile appear in the left pane as shown in the following figure:



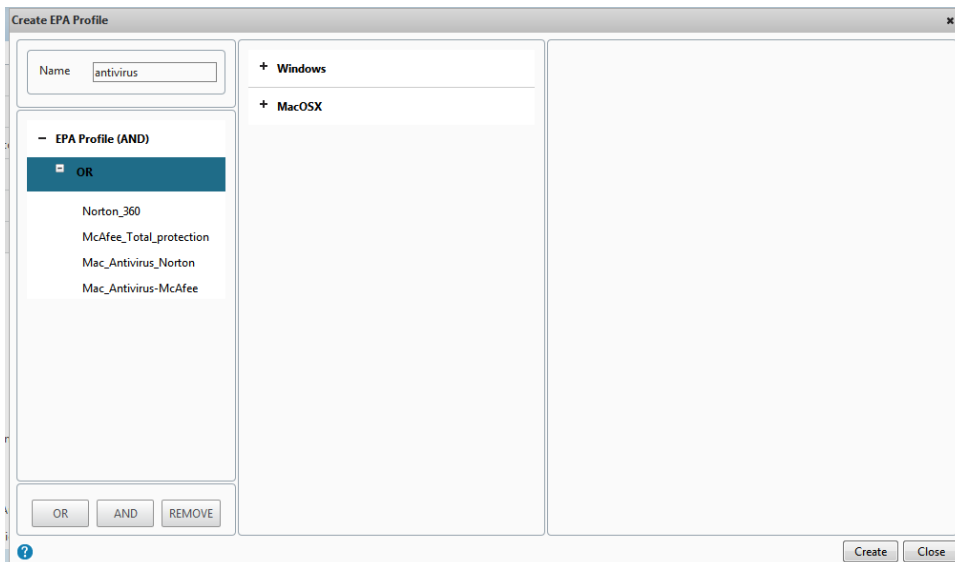
The steps for configuring advanced endpoint analysis scans are as follows:

1. Enable advanced endpoint analysis on the virtual server.
2. Create advanced endpoint analysis policies.
3. Bind the policies to the virtual server.

The categories of product types that you can choose as part of the scan for end user devices include:

- System, including operating system, ports, registry, and other system requirements for Windows and Mac computers
- Antivirus software
- Antispyware software
- Antiphishing software
- Firewall software
- Hard disk encryption software
- Patch management
- Peer-to-peer networking
- Health Agent

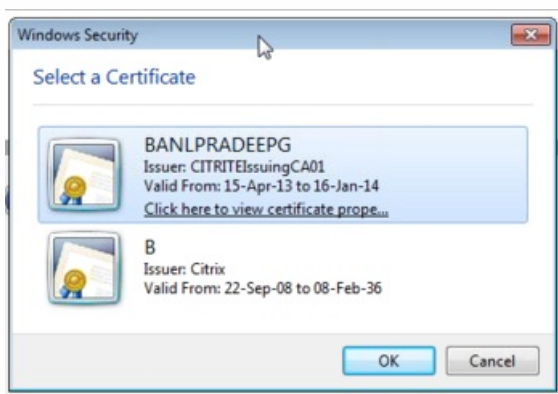
Citrix recommends that you create policies for each endpoint analysis category. For example, you want to check the user device for Symantec or McAfee antivirus software. In the policy, you add the product types for each operating system version, as shown in the following figure:



Peer-to-peer networking does not have any rules. By default, all peer-to-peer networking products are blocked. The only rule you can choose decides which peer-to-peer networking products to allow.

When users log on from a Windows-based or Mac OS X computer, the Endpoint Analysis Plug-in downloads and installs automatically. Then, the plug-in scans the user device to make sure the device meets the requirements. If the device does meet the requirements, users are allowed to log on. If the scan fails, users cannot log on until the computer meets the requirements.

In addition, if you install two or more device certificates on NetScaler Gateway, when the Endpoint Analysis Plug-in runs, a prompt appears directing users to select the device certificates.



After users select the correct certificate, the scan continues to run. For more information about device certificates, see [Creating Device Certificates for Authentication](#).

Configuring Advanced Endpoint Analysis Policies

Jan 28, 2014

You can enable, configure, and bind advanced endpoint analysis policies in NetScaler Gateway. You can use either the configuration utility or the command line to enable advanced endpoint analysis.

Note: You can configure advanced endpoint analysis policies with NetScaler Gateway 10.1, Build 120.1316.e.

1. In the configuration utility, in the navigation pane, do one of the following:
 1. If you log on to the appliance and then select NetScaler ADC as the Deployment Type, expand NetScaler Gateway > Policies and then click EPA Profile.
 2. If you log on to the appliance and then select NetScaler Gateway as the Deployment Type, expand NetScaler Gateway > Policies > Authentication/Authorization and then click EPA Profile.
2. In the details pane, click Add.
3. In the Create EPA Profile dialog box, in Name, type a name for the profile.
4. In the left pane, click OR or AND.
5. Select the operative and then in the center pane, expand either Windows or MacOSX.
6. Expand one of the options and then select the application or system item to include in the policy.
7. In the right pane, configure the parameters for your selection and then click Add Scan.
8. Repeat Steps 3 through 7 to add additional parameters to the scan.
9. When you finish building the scan, click Create and then click Close.

After you create the policy, enable advanced endpoint analysis on the virtual server. Then, you can bind the policy to a virtual server.

Note: You must enable advanced endpoint analysis on the virtual server. If you do not complete this step, you cannot bind the policy to the virtual server.

1. In the configuration utility, 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, select Enable advanced endpoint analysis and then click OK.

1. Log on to the NetScaler Gateway command line by using a Secure Shell (SSH) client, such as PuTTY.
2. At the command prompt, type `set vpn vserver virtualServerName -advancedEpa ON` where `virtualServerName` is the name of the virtual server.

After running this command, log off and then log on again to the configuration utility. When you log on again, you bind the endpoint analysis profile to the virtual server.

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, select a virtual server, click Action and then select Bind EPA profile.
3. In the Bind EPA Profiles dialog box, click Bind EPA profiles.

4. In the EPA Profile dialog box, select the policy and then click OK two times.

Connect Users

Feb 26, 2014

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

- 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 that is software installed on the user device.
- NetScaler Gateway Plug-in for Mac OS X (supported on Versions 10.6, 10.7 and 10.8). To use Version 10.9 (Mavericks), you must install NetScaler Gateway 10.1, Build 120.1316.e.
- NetScaler Gateway Plug-in for Java that is software that allows connections by using a Macintosh, Linux, UNIX, or Windows-based computer.
- 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 XenDesktop 7.1, 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 on NetScaler Gateway](#).

NetScaler Gateway supports Worx Home 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 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, 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.

How User Connections Work with Receiver

Feb 03, 2014

Users can connect to the following applications, desktops, and data from Citrix Receiver:

- Windows-based applications and virtual desktops published in StoreFront and the Web Interface
- ShareFile data accessed through App Controller

Users can log on by using any of the following Receivers:

- Receiver for Web
- Receiver for Windows
- Receiver for Mac
- Receiver for iOS
- Receiver for Android

Users can log on with Receiver for Web by using a web browser or from the Receiver icon on the user device. When users log on with any version of Receiver, applications, ShareFile data, and desktops appear in the browser or Receiver window.

When users start Receiver, they receive a logon page where they enter their credentials and log on. If the credentials are correct, Receiver contacts NetScaler Gateway and establishes the connection to internal resources. Users can then access their Windows, web, mobile, and SaaS applications that are available from App Controller, StoreFront and the Web Interface. Users can also connect to their virtual desktops from XenDesktop.

How User Connections Work with Worx Apps

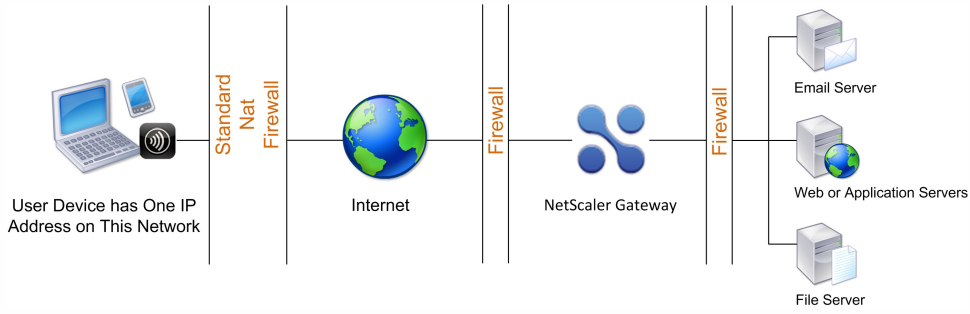
Jan 31, 2014

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.

-
-
-



-

-

-

-

-

-

-

-

-

•

•

•

•

•

•

•

•

•

-
-
-
-
-
-

-
-

-
-
-
-

-
-

-
-
-

-
-

-

-

-

-

-
-
-
-
-

```
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
```


-
-
-

-
-
-

```
shell
mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf
/var/ns_gui_custom/customtheme.tar.gz ns_gui/*
```

-
-

-
-

-
-

-
-

-

-

REQ.HTTP.HEADER User-Agent NOTCONTAINS Android && CLIENT.APPLICATION.PROCESS(keylogger.exe)
contains || CLIENT.APPLICATION.PROCESS (virus.exe) contains

-
-

-

-

- REQ.HTTP.HEADER User-Agent CONTAINS Android
- REQ.HTTP.HEADER User-Agent NOTCONTAINS Android

- REQ.HTTP.HEADER User-Agent NOTCONTAINS iPad
- REQ.HTTP.HEADER User-Agent NOTCONTAINS iPhone
- REQ.HTTP.HEADER User-Agent NOTCONTAINS iOS

-
-
-

-
-
-

-
-

-
-

-

-

-
-
-
-
-
-

-
-
-
-

nsvpnc_setup /c

agee.msi

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.

Removing the NetScaler Gateway Plug-in from User Devices

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.

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.
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.
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.
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.
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.

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.

To configure the NetScaler Gateway Plug-in for Java

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.

To set the interception mode

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.

Updating the HOSTS File on Windows-Based Computers

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.

Configuring Clientless Access

Feb 04, 2014

Clientless access allows users the access they need without requiring them to install user software, such as the NetScaler Gateway Plug-in or Receiver. Users can use their web browser to connect to web applications, such as Outlook Web Access.

You use the following steps to configure clientless access:

- Enabling clientless access either globally or by using a session policy bound to a user, group, or virtual server.
- Selecting the web address encoding method.

To enable clientless access for only a specific virtual server, disable clientless access globally, and then create a session policy to enable it.

If you use the NetScaler Gateway wizard to configure the appliance, you have the choice of configuring clientless access within the wizard. The settings in the wizard are applied globally. Within the NetScaler Gateway wizard, you can configure the following client connection methods:

- NetScaler Gateway Plug-in. Users are allowed to log on by using the NetScaler Gateway Plug-in only.
- Use the NetScaler Gateway Plug-in and allow access scenario fallback. Users log on to NetScaler Gateway with the NetScaler Gateway Plug-in. If the user device fails an endpoint analysis scan, users are permitted to log on using clientless access. When this occurs, users have limited access to network resources.
- Allow users to log on using a Web browser and clientless access. Users can log on only by using clientless access and receive limited access to network resources.

Enabling Clientless Access

Mar 05, 2014

When you enable clientless access on a global level, all users receive the settings for clientless access. You can use the NetScaler Gateway wizard, a global policy, or a session policy to enable clientless access.

In a global setting or a session profile, clientless access has the following settings:

- **On.** Enables clientless access. If you disable client choices and you do not configure or disable StoreFront or the Web Interface, users log on by using clientless access.
- **Allow.** Clientless access is not enabled by default. If you disable client choices, and you do not configure or disable StoreFront or the Web Interface, users log on with the NetScaler Gateway Plug-in. If endpoint analysis fails when users log on, users receive the choices page with clientless access available.
- **Off.** Clientless access is turned off. When you select this setting, users cannot log on by using clientless access and the icon for clientless access does not appear on the choices page.

Note: If you configure clientless access by using the command-line interface, the options are ON, OFF, or Disabled. If you did not enable clientless access by using the NetScaler Gateway wizard, you can enable it globally or in a session policy by using the configuration utility.

To enable clientless access globally

- 1.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access, select ON and then click OK.

To enable clientless access by using a session policy

If you want only a select group of users, groups, or virtual servers to use clientless access, disable or turn off clientless access globally. Then, using a session policy, enable clientless access and bind it to users, groups, or virtual servers.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Clientless Access, click Override Global, select On and then click Create.
7. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.
8. Click Create and then click Close.

After you create the session policy that enables clientless access, you bind it to a user, group, or virtual server.

Encoding the Web Address

Feb 05, 2014

When you enable clientless access, you can choose to encode the addresses of internal web applications or to leave the address as clear text. The settings are:

- **Obscure.** This uses standard encoding mechanisms to obscure the domain and protocol part of the resource.
- **Clear.** The web address is not encoded and is visible to users.
- **Encrypt.** The domain and protocol are encrypted by using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, when users log on and try to connect to the web address again using the bookmark, they cannot connect to the web address.

Note: If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on.

You can configure this setting either globally or as part of a session policy. If you configure encoding as part of session policy, you can bind it to the users, groups, or a virtual server.

To configure web address encoding globally

- 1.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access URL Encoding, select the encoding level and then click OK.

To configure web address encoding by creating a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Clientless Access URL Encoding, click Override Global, select the encoding level and then click OK.
7. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.

How Clientless Access Policies Work

Feb 05, 2014

You configure clientless access to web applications by creating policies. You can configure the settings for a clientless access policy in the configuration utility. A clientless access policy is composed of a rule and a profile. You can use the preconfigured clientless access policies that come with NetScaler Gateway. You can also create your own custom clientless access policies.

NetScaler Gateway provides preconfigured policies for the following:

- Outlook Web Access and Outlook Web App
- SharePoint 2007
- All other Web applications

Keep in mind the following characteristics of the preconfigured clientless access policies:

- They are configured automatically and cannot be changed.
- Each policy is bound at the global level.
- Each policy is not enforced unless you enable clientless access either globally or by creating a session policy.
- You cannot remove or modify global bindings, even if you do not enable clientless access.

Support for other web applications depends on the level of rewrite policies you configure on NetScaler Gateway. Citrix recommends testing any custom policies that you create to ensure that all components of the application rewrite successfully.

If you allow connections from Receiver for Android, Receiver for iOS, or WorxHome, you must enable clientless access. For WorxHome that runs on an iOS device, you must also enable Secure Browse within the session profile. Secure Browse and clientless access work together to allow connections from iOS devices. You do not have to enable Secure Browse if users do not connect with iOS devices.

The Quick Configuration wizard configures the correct clientless access policies and settings for mobile devices. Citrix recommends running the Quick Configuration wizard to configure the correct policies for connections to StoreFront and App Controller.

You can bind custom clientless access policies either globally or to a virtual server. If you want to bind clientless access policies to a virtual server, you need to create a new custom policy and then bind it. To enforce different policies for clientless access either globally or for a virtual server, change the priority number of the custom policy so it has a lower number than the preconfigured policies, thereby giving the custom policy higher priority. If no other clientless access policies are bound to the virtual server, the preconfigured global policies take precedence.

Note: You cannot change the priority numbers of the preconfigured clientless access policies.

Creating New Clientless Access Policies

Feb 05, 2014

If you want to use the same settings as for the default clientless access policies but you want to bind the policy to a virtual server, you can copy the default policies, providing a new name for the policy. You can use the configuration utility to copy the default policies.

After you bind the new policy to the virtual server, you can set the priority of the policy so that it executes first when a user logs on.

To create a new clientless access policy using default settings

1. In the configuration utility, on the navigation pane, expand NetScaler Gateway > Policies and then click Clientless Access.
2. In the details pane, on the Policies tab, click a default policy and then click Add.
3. In Name, type a new name for the policy, click Create and then click Close.

To bind a clientless access policy to a virtual server

After you create the new policy, bind it to the virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, select a virtual server and then click Open.
3. In the Configure NetScaler Gateway Virtual Server dialog box, click the Policies tab and then click Clientless.
4. Click Insert Policy, select a policy from the list and then click OK.

Creating and Evaluating Clientless Access Policy Expressions

When you create a new policy for clientless access, you can create your own expression for the policy. When you are finished creating the expression, you can then evaluate the expression for accuracy.

1. In the configuration utility, on the navigation pane, expand NetScaler Gateway > Policies and then click Clientless Access.
2. In the details pane, on the Policies tab, click a default policy and then click Add.
3. In Name, type a name for the policy.
4. Next to Profile, click New.
5. In Name, type a name for the profile.
6. Configure the rewrite settings and then click Create.
7. In the Create Clientless Access Policy dialog box, under Expression, click Add.
8. In the Add Expression dialog box, create the expression and then click OK.
9. In the Create Clientless Access Policy dialog box, click Evaluate, and if the expression tests as correct, click Create.

Configuring Domain Access for Users

Feb 04, 2014

If users connect by using clientless access, you can restrict the network resources, domains, and web sites users are permitted to access. You can use the NetScaler Gateway wizard or global settings to create lists for including or excluding access to domains.

You can allow access to all network resources, domains, and web sites and then create an exclusion list. The exclusion list cites a specific set of resources that users are not allowed to access. Users cannot access any domains that are in the exclusion list.

You can also deny access to all network resources, domains, and web sites and then create a specific inclusion list. The inclusion list cites the resources that users can access. Users cannot access any domains that do not appear on the list.

Note: If you configure clientless access policies for App Controller or StoreFront and users connect with Receiver for Web, you need to allow the domains that Receiver for Web can access. This is required so NetScaler Gateway can rewrite network traffic for StoreFront and App Controller.

To configure domain access by using the NetScaler Gateway wizard

- 1.
2. In the details pane, under Getting Started, click NetScaler Gateway wizard.
3. Click Next and then follow the directions in the wizard until you reach the Configure clientless access page.
4. Click Configure Domains for Clientless Access and do one of the following:
 - To create a list of excluded domains, click Exclude domains.
 - To create a list of included domains, click Allow domains.
5. Under Domain Names, type the domain name and then click Add.
6. Repeat Step 5 for each domain you want to add to the list and then click OK when finished.
7. Continue configuring the appliance by using the NetScaler Gateway wizard.

To configure domain settings by using the configuration utility

You can also create or modify the domain list by using global settings in the configuration utility.

- 1.
2. In the details pane, under Clientless Access, click Configure Domains for Clientless Access.
3. Do one of the following:
 - To create a list of excluded domains, click Exclude domains.
 - To create a list of included domains, click Allow domains.
4. Under Domain Names, type the domain name and then click Add.
5. Repeat Step 4 for each domain you want to add to the list and then click OK when finished.

Configuring Clientless Access for SharePoint 2003 and SharePoint 2007

Feb 04, 2014

NetScaler Gateway can rewrite content from one or more SharePoint 2003 or SharePoint 2007 sites so that the content is available to users without requiring the NetScaler Gateway Plug-in. For the rewrite process to complete successfully, you must configure NetScaler Gateway with the host name for each SharePoint server in your network.

You can use the NetScaler Gateway wizard or the configuration utility to configure the host name for SharePoint sites.

In the NetScaler Gateway wizard, navigate through the wizard to configure your settings. When you come to the Configure clientless access page, type the web address for the SharePoint site and then click Add.

To add additional Web sites or to configure SharePoint for the first time after running the NetScaler Gateway wizard, you use the configuration utility.

To configure clientless access for SharePoint by using the configuration utility

- 1.
2. In the details pane, under Clientless Access, click Configure Clientless Access for SharePoint.
3. Under Clientless Access for SharePoint, in Host name of SharePoint server, type the host name for the SharePoint site and then click Add.
4. Repeat Step 3 for each SharePoint site you want to add to the list and then click OK when finished.

Setting a SharePoint Site as the Home Page

Feb 05, 2014

If you want to set a SharePoint site as the users' home page, configure a session profile and enter the host name of the SharePoint site.

To configure a SharePoint site as the home page

1. 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 Home Page click Override Global and then type the name of the SharePoint site.
7. Next to Clientless Access, click Override Global, select On and then click Create.
8. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.

After completing the session policy, bind it to users, groups, virtual servers, or globally. When users log on, they see the SharePoint Web site as their home page.

Enabling Name Resolution for SharePoint 2007 Servers

May 14, 2013

SharePoint 2007 servers send the configured server name as the host name within various URLs as part of the response. If a configured SharePoint server name is not the fully qualified domain name (FQDN), NetScaler Gateway cannot resolve the IP address using the SharePoint server name, and some user functions time out with the error message “HTTP:1.1 Gateway Time-out.” These functions can include checking files in and out, viewing the workspace, and uploading multiple files when users are logged on using clientless access.

To resolve this issue, you can try one of the following:

- Configure a DNS suffix on NetScaler Gateway so that the SharePoint host name is converted to an FQDN before name resolution.
- Configure a local DNS entry on NetScaler Gateway for every SharePoint server name.
- Change all the SharePoint server names to use the FQDN, such as

— *SharePoint.intranetdomain*

instead of

— *SharePoint*

,

To configure a DNS suffix

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand DNS and then click DNS Suffix.
2. In the details pane, click Add.
3. In DNS Suffix, type the intranet domain name as the suffix, click Create and then click Close.

You can repeat Step 3 for each domain you want to add.

To configure a local DNS record for every SharePoint server name on NetScaler Gateway

1. In the configuration utility, in the navigation pane, expand DNS > Records and then click Address Records.
2. In the details pane, click Add.
3. In Host Name, type the SharePoint host name for the DNS address record.
4. In IP Address, type the IP address of the SharePoint server, click Add, click Create and then click Close.

The host name for which an A record is added should not have a CNAME record. Also, there cannot be duplicate A records on the appliance.

Enabling Clientless Access Persistent Cookies

May 14, 2013

Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server.

A persistent cookie remains on the user device and is sent with each HTTP request. NetScaler Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends.

In the NetScaler Gateway wizard, administrators can enable persistent cookies globally. You can also create a session policy to enable persistent cookies per user, group, or virtual server.

The following options are available for persistent cookies:

- Allow enables persistent cookies and users can open and edit Microsoft documents stored in SharePoint.
- Deny disables persistent cookies and users cannot open and edit Microsoft documents stored in SharePoint.
- Prompt prompts users to allow or deny persistent cookies during the session.

Persistent cookies are not required for clientless access if users do not connect to SharePoint.

Configuring Persistent Cookies for Clientless Access for SharePoint

Feb 05, 2014

You can configure persistent cookies for clientless access for SharePoint either globally or as part of a session policy.

To configure persistent cookies globally

- 1.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access Persistent Cookies, select an option and then click OK.

To configure persistent cookies as part of a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Clientless Access Persistent Cookies, click Override Global, select an option and then click Create.
7. In the Create authentication policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.

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.

To bind cookies for Web Interface persistence by using the configuration utility

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.

To bind cookies for Web Interface persistence by using the command line

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.

To enable client choices options globally

- 1.
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.

To enable client choices as part of a session policy

You can also configure client choices as part of a session policy and then bind it to users, groups, and virtual servers.

1. In the 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.

To create an authorization group

- 1.
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.

To create a session profile for client choices

- 1.
2. In the details pane, click the Profiles tab and 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. To configure the STA server globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Servers, click Bind/Unbind STA Servers to be used by the Secure Ticket Authority.
3. In the Bind/Unbind STA Servers dialog box, click Add.
4. In the Configure STA Server dialog box, in URL, type the web address of the STA server and then click Create.
5. Repeat Steps 3 and 4 to add more STA servers and then click OK.

To bind the STA to a virtual server

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, click a virtual server and then click Open.
3. On the Published Applications tab, under Secure Ticket Authority, under Active, select the STA servers and then click OK,

You can also add STA servers on the Published Applications tab.

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.
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.
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.
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.
2. In the details pane, select a group and 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.
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.

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.

- 1.
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.

Managing User Sessions

May 14, 2013

You can manage user sessions in the configuration utility in the Active Users Sessions dialog box. This dialog box displays a list of active user sessions on the NetScaler Gateway.

You can end user or group sessions in this dialog box by using the user name, group name, or IP address.

You can also view active sessions within this dialog box. Session information includes:

- User name
- IP address of the user device
- Port number of the user device
- IP address of the virtual server
- Port number of the virtual server
- Intranet IP address assigned to the user

- 1.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. View the list of sessions under Sessions.

You can retrieve updated information about sessions to NetScaler Gateway.

- 1.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Click Refresh.

You can terminate user and group sessions. You can also end a session that has a specific intranet IP address and subnet mask.

- 1.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Under Sessions, select a user or group and then click Terminate.

- 1.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Select Intranet IP
4. In Intranet IP, type the IP address.
5. In Netmask, type the subnet mask and then click Terminate.

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.

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.

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.
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.
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.
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 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.
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.
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.
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.
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.

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.

- 1.
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.

- 1.
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.

- 1.
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.

- 1.
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.

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.
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.

- 1.
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.
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 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 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.
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.

- 1.
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.

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.

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.

- 1.
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.

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.

To configure split tunneling

- 1.
2. In the details pane, on the Profiles tab, select a profile and then click Open.
3. On the Client Experience tab, next to Split Tunnel, select Global Override, select an option and then click OK twice.

Configuring Split Tunneling and Authorization

When planning your NetScaler Gateway deployment, it is important to consider split tunneling and the default authorization action and authorization policies.

For example, you have an authorization policy that allows access to a network resource. You have split tunneling set to ON and you do not configure intranet applications to send network traffic through NetScaler Gateway. When NetScaler Gateway has this type of configuration, access to the resource is allowed, but users cannot access the resource.

If the authorization policy denies access to a network resource, you have split tunneling set to ON, and intranet applications are configured to route network traffic through NetScaler Gateway, the NetScaler Gateway Plug-in sends traffic to NetScaler Gateway, but access to the resource is denied.

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.

To add a DNS or WINS server within a session profile

- 1.
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.

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.
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.
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.
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.
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 Groups.
 - 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.

Integrate

Feb 05, 2014

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.

Integrating NetScaler Gateway with App Controller or StoreFront

Feb 27, 2014

You can configure NetScaler Gateway to work with App Controller and StoreFront. When you configure NetScaler Gateway to work with StoreFront or App Controller, you might need a specific NetScaler Gateway build to configure features, as follows:

- NetScaler Gateway 10.1, Build 120.1316.e works with XenMobile 8.6 (App Controller 2.9) and StoreFront 2.1
- NetScaler Gateway 10.1 works with AppController Versions 2.5, 2.6 and App Controller 2.8
- Access Gateway 10, Build 73.5002.e works with AppController 2.5 and 2.6 (you must install Build 71.6014.e first)
- Access Gateway 10, Build 71.6014.e works with AppController 2.5 and 2.6
- Access Gateway 10, Build 69.6 works with AppController Versions 1.1 and 2.0 and StoreFront Versions 1.1 and 1.2
- Access Gateway 10, Build 54.7 works with AppController 1.1 and StoreFront 1.1.

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.

This section contains information about configuring connections from remote users through NetScaler Gateway to your App Controller and StoreFront deployment.

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

You can configure NetScaler Gateway to work with StoreFront 1.2 and 2.1. Users can connect in one of the following ways:

- 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](#).
- 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) 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">• Mac OS X Mavericks (version 10.9)• Mac OS X 10.8• Mac OS X 10.7• Mac OS X 10.6 <p>For more information, see the system requirements for your version of Receiver for Mac in the — <i>Receivers and Plug-ins</i> node in Citrix eDocs</p>
Receiver for iOS 5.7 and 5.8	iOS 5.1, 6.1.x, and 7 For more information, see the system requirements for your version of Receiver for iOS in the — <i>Receivers and Plug-ins</i> 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

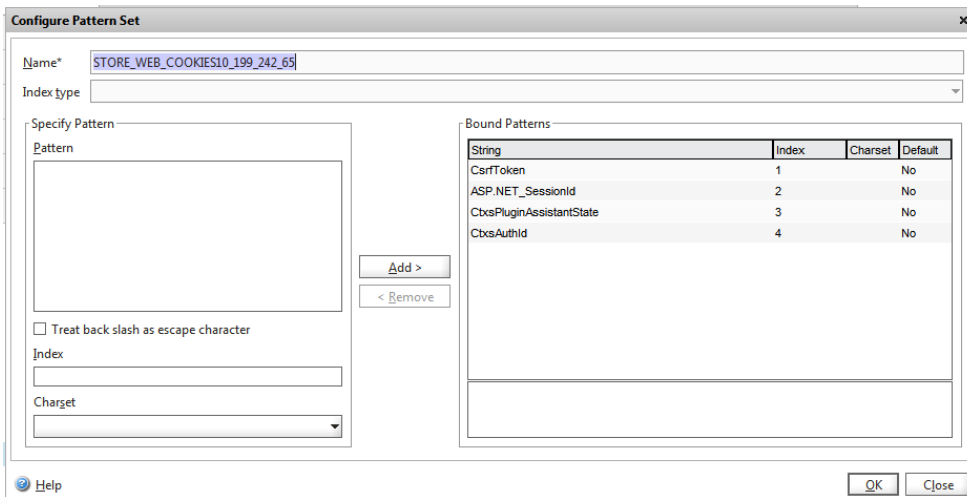
Clientless Access Settings and Rules for the Universal License

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 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.

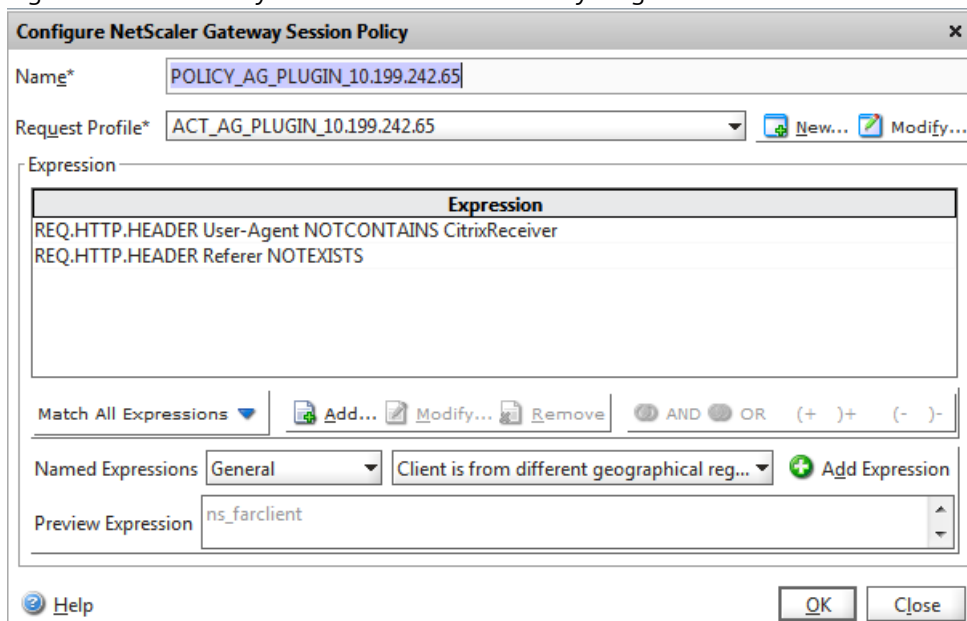
The Quick Configuration wizard configures the following four session policies automatically. These include:

- 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.

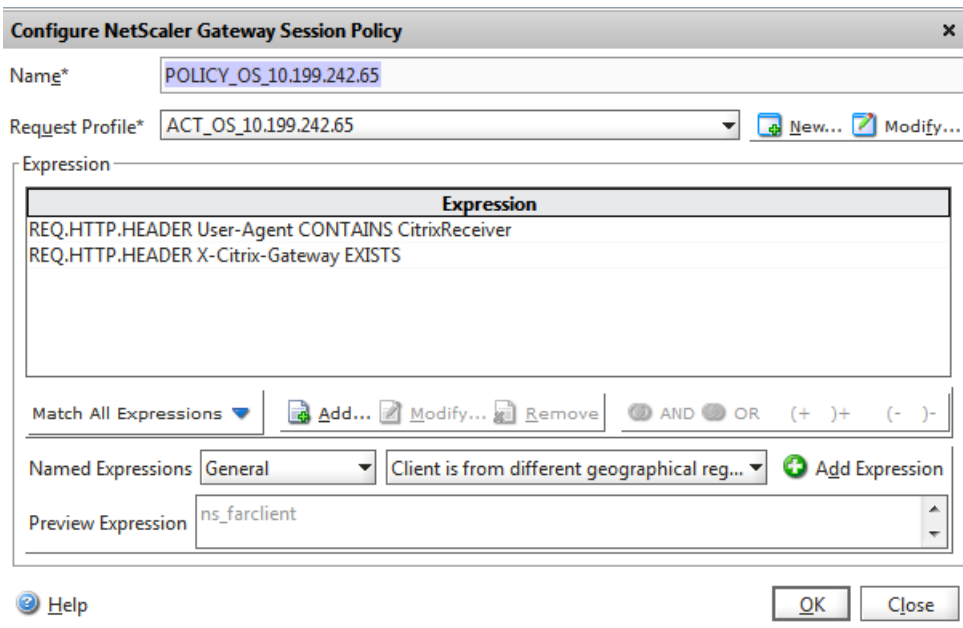
This policy is for users who connect with the NetScaler Gateway Plug-in for Windows or the NetScaler Gateway Plug-in for Mac.

Figure 1. Session Policy for the NetScaler Gateway Plug-in



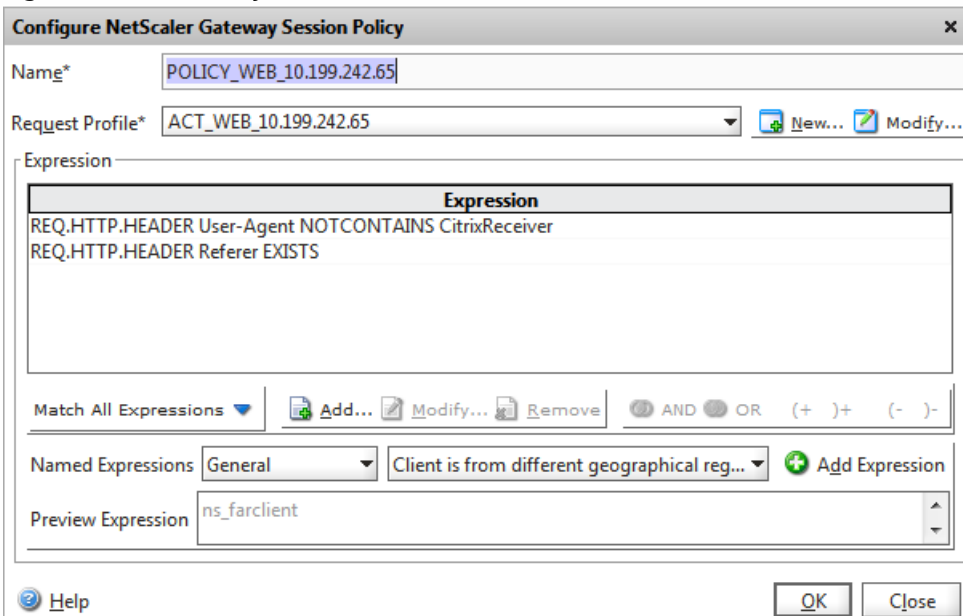
This policy checks to see if users connect with Receiver and if the connection goes through NetScaler Gateway.

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

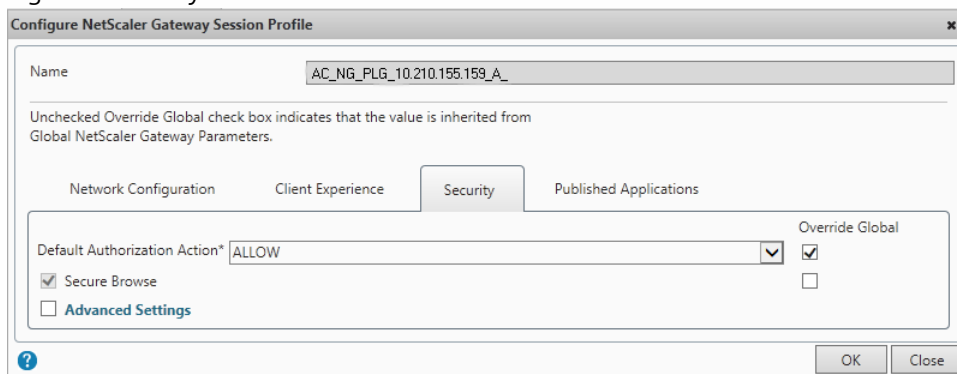
Feb 26, 2014

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

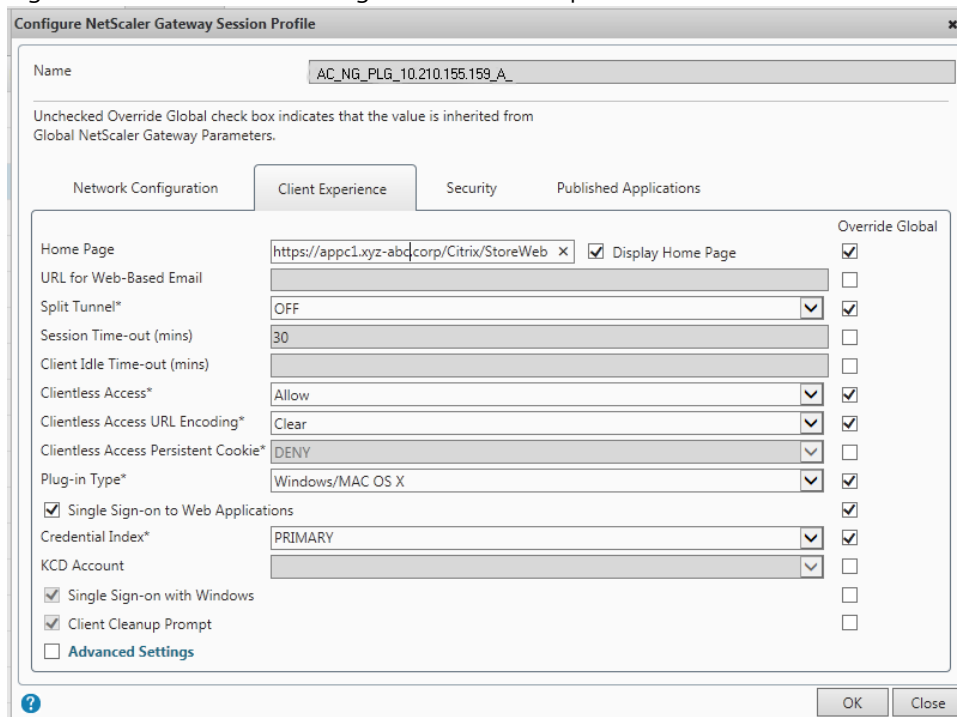
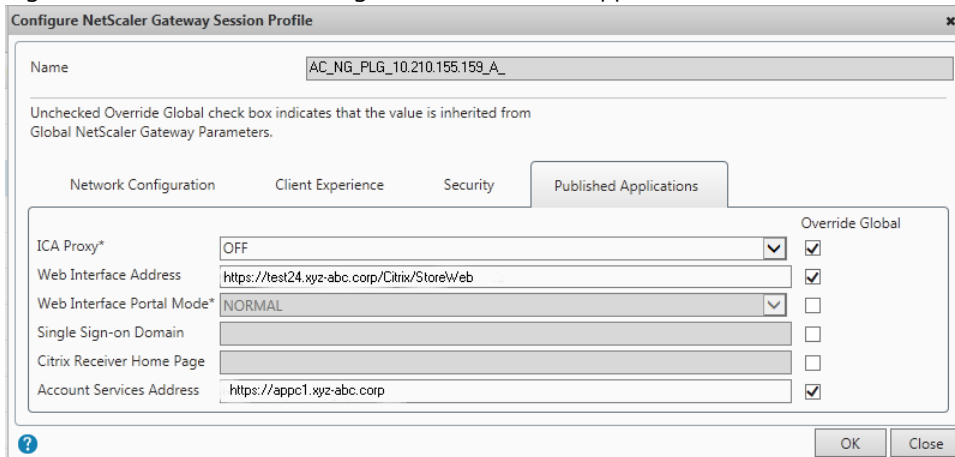


Figure 3. Session Profile Settings on the Published Applications Tab



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

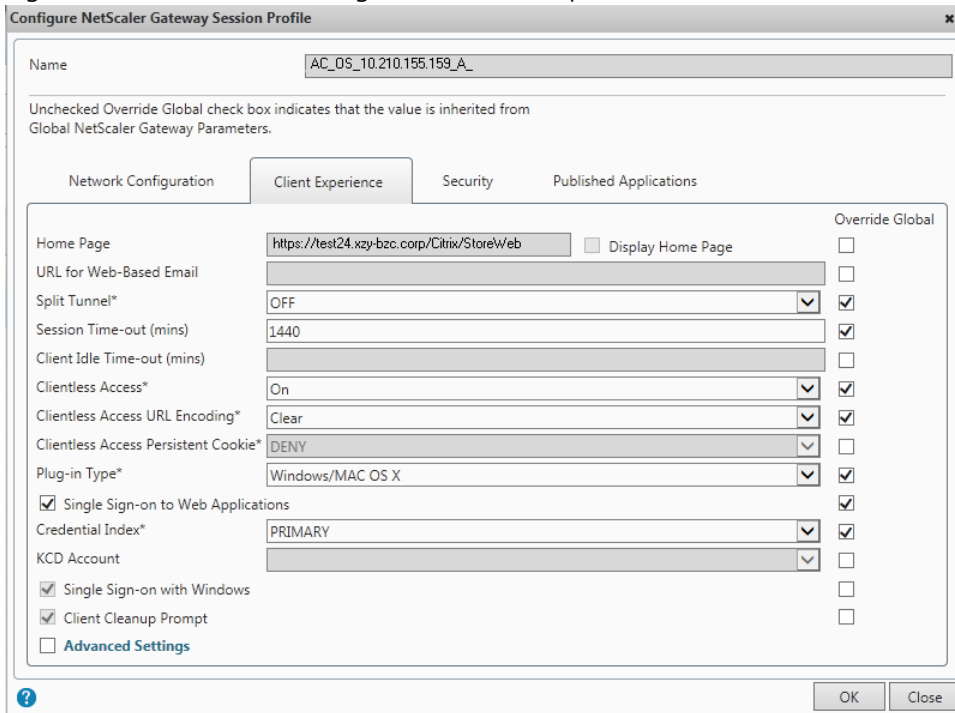
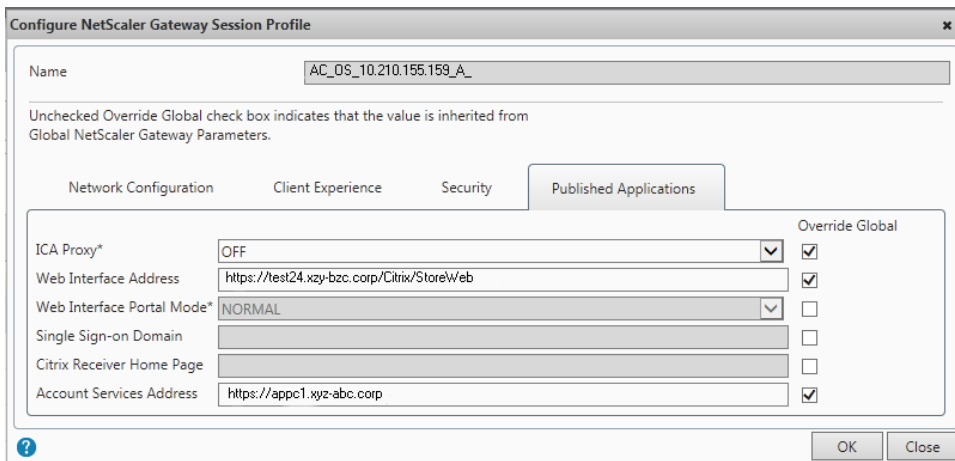


Figure 5. Session Profile Settings on the Published Applications Tab



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

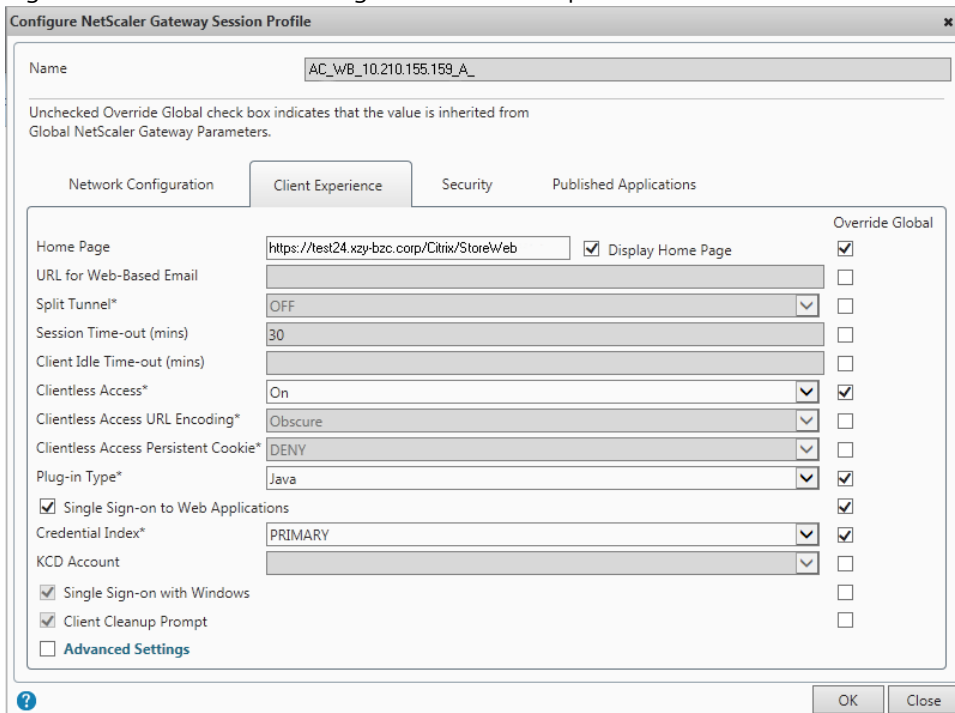


Figure 7. Session Profile Settings on the Published Applications Tab

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

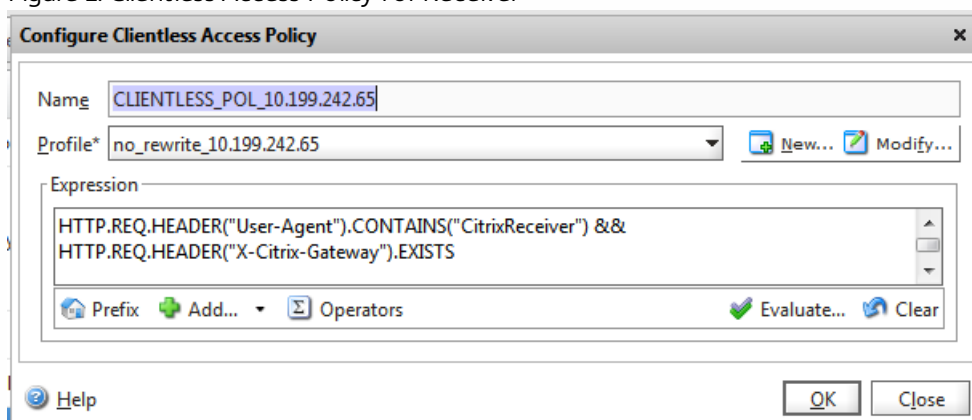
Aug 02, 2013

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

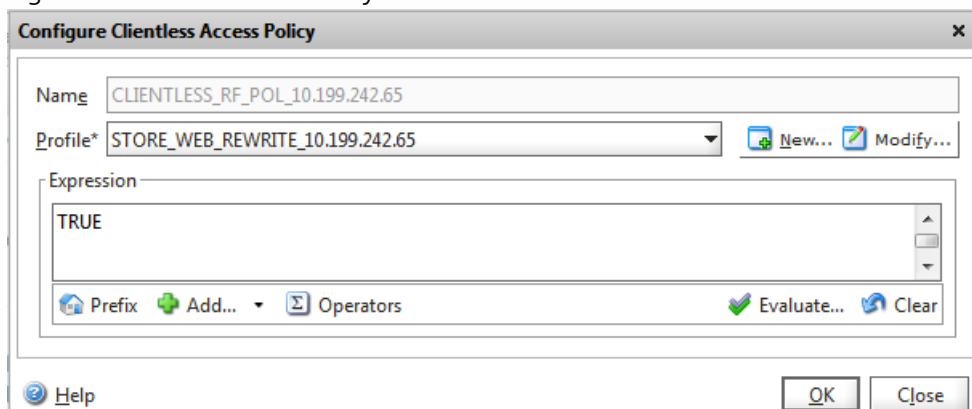


Clientless Access Policies for Receiver for Web

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.

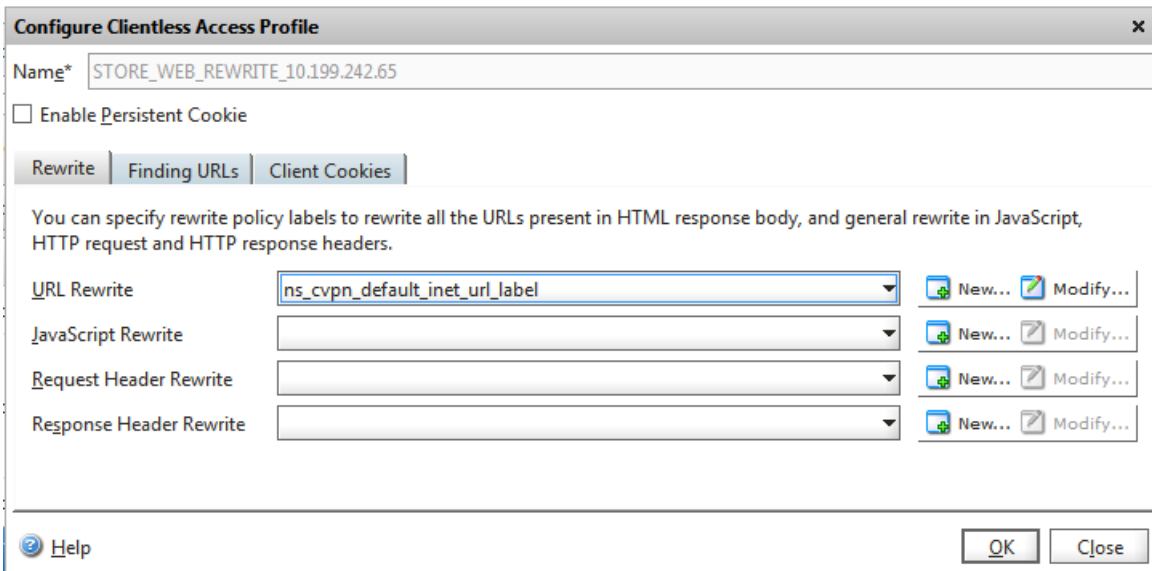
This figure shows the clientless access policy with the expression set to TRUE for Receiver for Web.

Figure 2. Clientless Access Policy



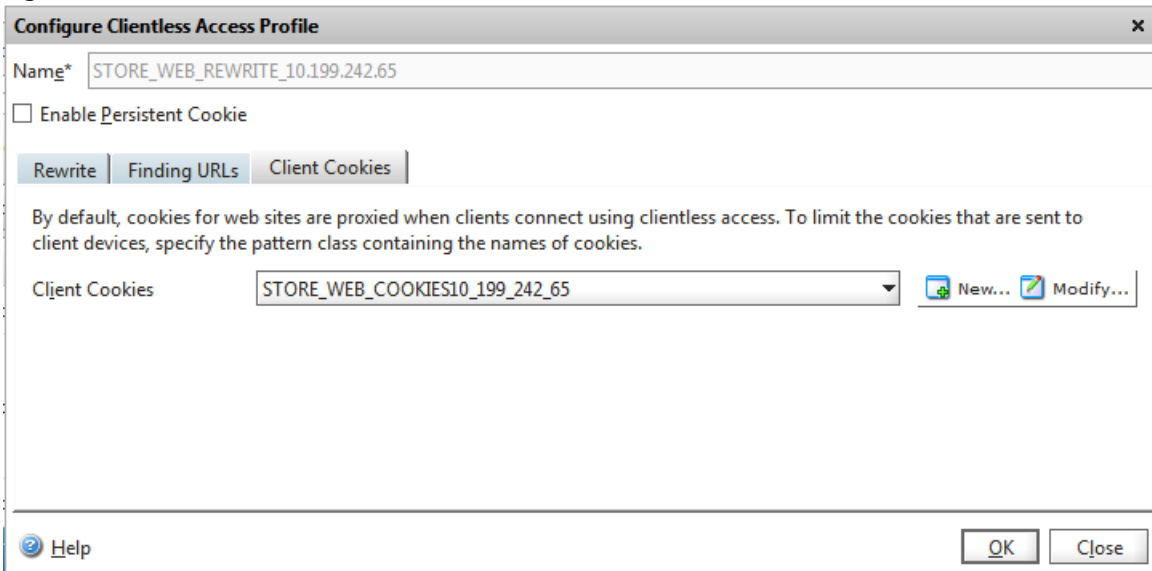
This policy contains the URL rewrite label ns_cvpn_default_inet_url_label.

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 for 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 && REQ.HTTP.HEADER X-Citrix-Gateway NOTEXISTS
Worx Home or Receiver version supports StoreFront services protocols	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS
NetScaler Gateway Plug-in for Windows NetScaler Gateway Plug-in for Mac	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer NOTEXISTS
Receiver for Web	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS
Receiver for Windows 8/RT	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && 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.
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.
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>`
is the fully qualified domain name (FQDN) of Storefront and
`<StoreWebName>`
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.
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.
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 NOT EXISTS.
 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.
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 a 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.
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.
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.
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.
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.
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.

Providing Access to Published Applications and Virtual Desktops Through 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 components 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 eDocs 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.

Process Overview: User Access to Published Resources in the Server Farm

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.

Setting Up a Web Interface Site to Work with NetScaler Gateway

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.

Using Configuration Files

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.

To configure NetScaler Gateway settings in the Web Interface

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 NetScaler Gateway to Communicate 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.

- 1.
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.

You can configure a session policy and bind it to a virtual server to limit access to the Web Interface.

- 1.
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.

- 1.
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

- 1.
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.

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.

- 1.
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 with a server farm, you can complete the following optional tasks:

- [Configuring Web Interface Failover](#) to configure NetScaler Gateway to failover to a secondary server running the Web Interface.
- [Configuring Smart Card Access with the Web Interface](#) that allows users 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.

- 1.
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 SmartAccess on NetScaler Gateway

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.

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.
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](#).

- 1.
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.
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.
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 Single Sign-On to the Web Interface on NetScaler Gateway

May 16, 2013

You can configure NetScaler Gateway to provide single sign-on to the Web Interface. You can configure NetScaler Gateway to work 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.

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](#).

To configure single sign-on to Web applications globally

May 16, 2013

- 1.
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.
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.
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.

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.
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.

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 Additional 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.

- 1.
2. In the details pane, click the Profiles tab and 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.
2. In the details pane, click a virtual server and 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.

Customize

May 15, 2013

This section discusses advanced tasks you can configure on Citrix NetScaler Gateway. These include:

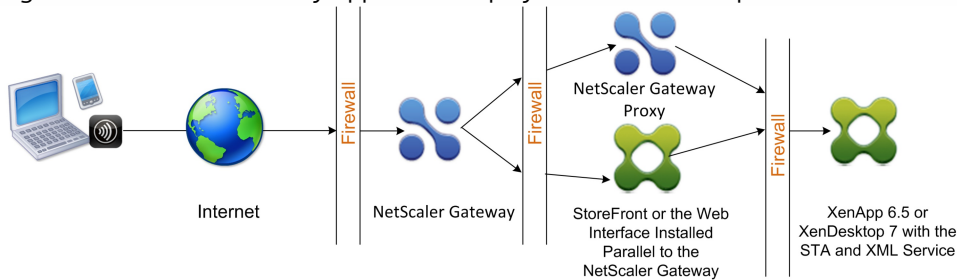
- Deploying NetScaler Gateway in a double-hop DMZ. You can deploy two NetScaler Gateway appliances in a double-hop DMZ in two stages to provide an extra layer of security for the internal network.
- Configuring DNS virtual servers. You can configure a DNS server as a virtual server and then bind the server globally or to another virtual server.
- Resolving DNS name servers located in the secure network. If your DNS server is located in the secure network behind a firewall and the firewall is blocking ICMP traffic, you can use a non-directly addressable DNS virtual server on NetScaler Gateway that resolves to a known fully qualified domain name (FQDN).
- Using operators and operands. You can use operators and operands in policy expressions.
- Configuring server-initiated connections. When an IP address is assigned to a user's session, it is possible to connect to the user device from the internal network, by using Remote Desktop or a virtual network client (VNC).
- Enabling NetScaler Gateway Plug-in logging. You can configure the NetScaler Gateway Plug-in to log all errors to a text file.

Deploying NetScaler Gateway in a Double-Hop DMZ

Feb 20, 2014

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

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



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

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

Note: If you deploy NetScaler Gateway in a double-hop DMZ with StoreFront, email-based auto-discovery for Receiver does not work.

How a Double-Hop Deployment Works

Feb 28, 2014

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

- Users connect to NetScaler Gateway in the first DMZ by using a web browser and by using Citrix Receiver to select a published application.
- Citrix Receiver starts on the user device. The user connects to NetScaler Gateway to access the published application running in the server farm in the secure network.
Note: Work Home and the NetScaler Gateway Plug-in are not supported in a double-hop DMZ deployment. Only Citrix Receiver is used for user connections.
- NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.
- NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm. Communications between NetScaler Gateway in the first DMZ and the Secure Ticket Authority (STA) in the internal network are also proxied through NetScaler Gateway in the second DMZ.

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

Communication Flow in a Double-Hop DMZ Deployment

Feb 27, 2014

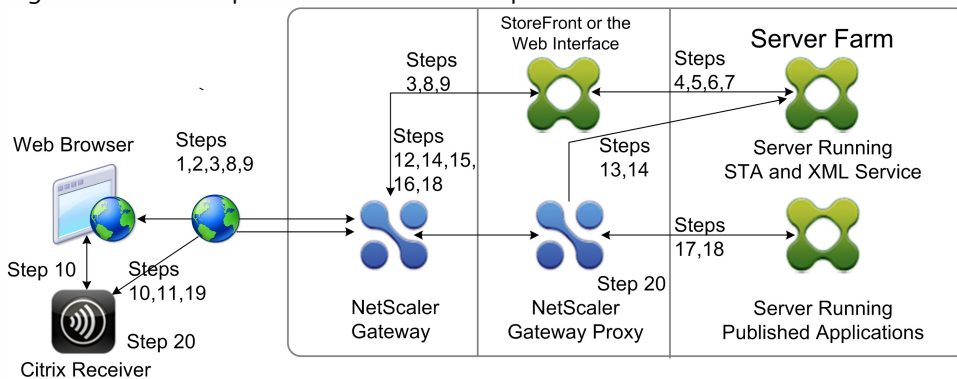
To understand the configuration issues involved in a double-hop DMZ deployment, you should have a basic understanding of how the various NetScaler Gateway and XenApp components in a double-hop DMZ deployment communicate to support a user connection. The connection process for StoreFront and the Web Interface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

Although the user connection process occurs in one continuous flow, the steps are detailed in the four following topics:

- [Authenticating Users](#)
- [Creating a Session Ticket](#)
- [Starting Citrix Receiver](#)
- [Completing the Connection](#)

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

Figure 1. Double-hop DMZ user connection process

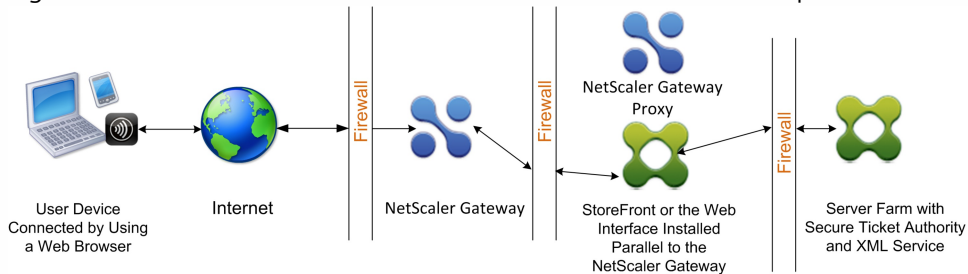


Authenticating Users

Feb 08, 2014

Authenticating users is the first step of the user connection process in a double-hop DMZ deployment. The following figure shows the user connection process in this deployment.

Figure 1. Communication flow for user authentication in a double-hop DMZ



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

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

If you enable authentication on NetScaler Gateway, the appliance sends the NetScaler Gateway logon page to the user. The user enters authentication credentials on the logon page and the appliance authenticates the user. NetScaler Gateway then returns the user credentials to the Web Interface.

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

Creating a Session Ticket

Feb 08, 2014

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

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

1. The Web Interface communicates with both the XML Service and the Secure Ticket Authority (STA) in the internal network to produce session tickets for each of the published applications the user is authorized to access. The session ticket contains an alias address for the computer running Citrix XenApp that hosts a published application.
2. The STA saves the IP addresses of the servers that host the published applications. The STA then sends the requested session tickets to the Web Interface. Each session ticket includes an alias that represents the IP address of the server that hosts the published application, but not the actual IP address.
3. The Web Interface generates an ICA file for each of the published applications. The ICA file contains the ticket issued by the STA. The Web Interface then creates and populates a web page with a list of links to the published applications and sends this web page to the web browser on the user device.

Starting Citrix Receiver

Feb 20, 2014

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

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

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

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

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

Completing the Connection

Feb 20, 2014

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

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

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

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

1. Receiver sends the STA ticket for the published application to NetScaler Gateway in the first DMZ.
2. NetScaler Gateway in the first DMZ contacts the STA in the internal network for ticket validation. To contact the STA, NetScaler Gateway establishes a SOCKS or SOCKS with SSL connection to the NetScaler Gateway proxy in the second DMZ.
3. The NetScaler Gateway proxy in the second DMZ passes the ticket validation request to the STA in the internal network. The STA validates the ticket and maps it to the computer running XenApp that hosts the published application.
4. The STA sends a response to the NetScaler Gateway proxy in the second DMZ, which is passed to NetScaler Gateway in the first DMZ. This response completes the ticket validation and includes the IP address of the computer that hosts the published application.
5. NetScaler Gateway in the first DMZ incorporates the address of the XenApp server into the user connection packet and sends this packet to the NetScaler Gateway proxy in the second DMZ.
6. The NetScaler Gateway proxy in the second DMZ makes a connection request to the server specified in the connection packet.
7. The server responds to the NetScaler Gateway proxy in the second DMZ. The NetScaler Gateway proxy in the second DMZ passes this response to NetScaler Gateway in the first DMZ to complete the connection between the server and NetScaler Gateway in the first DMZ.
8. NetScaler Gateway in the first DMZ completes the SSL/TLS handshake with the user device by passing the final connection packet to the user device. The connection from the user device to the server is established.
9. ICA traffic flows between the user device and the server through NetScaler Gateway in the first DMZ and the NetScaler Gateway proxy in the second DMZ.

Preparing for a Double-Hop DMZ Deployment

Feb 20, 2014

To prepare appropriately and avoid unnecessary problems when configuring a double-hop DMZ deployment, you should answer the following questions:

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

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

Components Required to Begin the Deployment

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

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

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

Installing and Configuring Netscaler Gateway in a Double-Hop DMZ

Feb 21, 2014

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

Installing NetScaler Gateway in the First DMZ

To install NetScaler Gateway in the first DMZ, follow the instructions in [Installing the Model MPX 5500 Appliance](#).

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

Configuring NetScaler Gateway in the First DMZ

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

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

Installing NetScaler Gateway in the Second DMZ

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

Follow the instructions in [Installing the Model MPX 5500 Appliance](#) to install each NetScaler Gateway appliance in the second DMZ.

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

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

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

Configuring Settings on the Virtual Servers on the NetScaler Gateway Proxy

Feb 28, 2014

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

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

To enable double hop on the virtual server on the NetScaler Gateway Proxy

- 1.
2. In the details pane, click a virtual server and then click Open.
3. In the Configure NetScaler Gateway Virtual Server dialog box, click Double Hop and then click OK.

To disable authentication on the virtual server on the NetScaler Gateway proxy

- 1.
2. In the details pane, click a virtual server and then click Open.
3. Click the Authentication tab.
4. Under User Authentication, clear Enable Authentication and then click OK.

Configuring the Appliance to Communicate with the Appliance Proxy

Feb 21, 2014

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

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

Note: If you want to use IPv6, you configure the next hop server by using the configuration utility. To do so, expand NetScaler Gateway > Resources and then click Next Hop Servers. Follow Steps 4 through 7 in the following procedure and then select the IPv6 check box.

To configure NetScaler Gateway to communicate with the NetScaler Gateway Proxy

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

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

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

To bind the NetScaler Gateway next hop server globally

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

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

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

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

Configuring NetScaler Gateway to Handle the STA and ICA Traffic

Feb 21, 2014

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

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

To configure and bind the STA globally

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

To configure and bind the STA to a virtual server

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

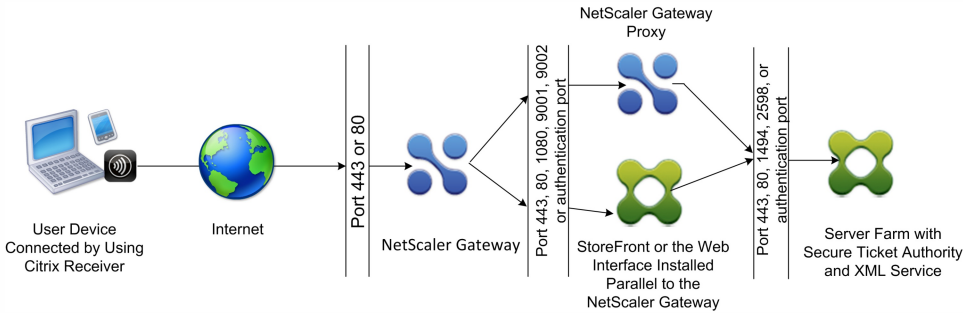
Opening the Appropriate Ports on the Firewalls

Feb 21, 2014

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

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

Figure 1. Ports in a double-hop DMZ deployment



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

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

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

Connections through the second firewall	Ports used
<p>NetScaler Gateway in the first DMZ connects to the Web Interface in the second DMZ.</p>	Open either TCP port 80 for an unsecure connection or TCP port 443 for a secure connection through the second firewall.

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

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

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

Managing SSL Certificates in a Double-Hop DMZ Deployment

Feb 21, 2014

You must install the SSL certificates necessary to encrypt the connections among components in a double-hop DMZ deployment.

In a double-hop DMZ deployment, several different types of connections occur among the various components involved in the deployment. There is no end-to-end SSL encryption of these connections. However, each connection can be encrypted individually.

Encrypting a connection requires you to install the appropriate SSL certificate (either a trusted root or a server certificate) on the components involved in the connection.

The following table shows the connections that occur through the first firewall and the SSL certificates required to encrypt each of these connections. Encrypting the connections through the first firewall is mandatory to secure traffic sent over the Internet.

Connections through the first firewall	Certificates required for encryption
The web browser from the Internet connects to NetScaler Gateway in the first DMZ.	NetScaler Gateway in the first DMZ must have an SSL server certificate installed. The web browser must have a root certificate installed that is signed by the same Certificate Authority (CA) as the server certificate on NetScaler Gateway.
Citrix Receiver from the Internet connects to NetScaler Gateway in the first DMZ.	The certificate management for this connection is the same as the web browser to NetScaler Gateway connection. If you installed the certificates to encrypt the web browser connection, this connection is also encrypted using those certificates.

The following table shows the connections that occur through the second firewall and the SSL certificates required to encrypt each of these connections. Encrypting these connections enhances security but is not mandatory.

Connections through the second firewall	Certificates required for encryption
NetScaler Gateway in the first DMZ connects to the Web Interface in the second DMZ.	StoreFront or the Web Interface must have an SSL server certificate installed. NetScaler Gateway in the first DMZ must have a root certificate installed that is signed by the same CA as the server certificate on the Web Interface.
NetScaler Gateway in the first DMZ connects to NetScaler Gateway in the second DMZ.	NetScaler Gateway in the second DMZ must have an SSL server certificate installed.

Connections through the second firewall	NetScaler Gateway in the first DMZ must have a root certificate installed that is signed by the same CA as the server certificate on NetScaler Gateway in the second DMZ.

The following table below shows the connections that occur through the third firewall and the SSL certificates required to encrypt each of these connections. Encrypting these connections enhances security but is not mandatory.

Connections through the third firewall	Certificates required for encryption
StoreFront or the Web Interface in the second DMZ connects to the XML Service hosted on a server in the internal network.	<p>If the XML Service runs on Microsoft Internet Information Services (IIS) server on the XenApp server, an SSL server certificate must be installed on the IIS server.</p> <p>If the XML Service is a standard Windows service (does not reside in IIS), an SSL server certificate must be installed within the SSL Relay on the server.</p> <p>StoreFront or the Web Interface must have a root certificate installed that is signed by the same CA as the server certificate installed on either the Microsoft IIS server or the SSL Relay.</p>
StoreFront or the Web Interface in the second DMZ connects to the STA hosted on a server in the internal network.	The certificate management for this connection is the same as the Web Interface to XML Service connection. You can use the same certificates to encrypt this connection. (The server certificate must reside on either the Microsoft IIS server or the SSL Relay. A corresponding root certificate must be installed on the Web Interface.)
NetScaler Gateway in the second DMZ connects to the STA hosted on a server in the internal network.	<p>The SSL server certificate management for the STA in this connection is the same as described for the two previous connections discussed in this table. (The server certificate must reside on either the Microsoft IIS server or the SSL Relay.)</p> <p>NetScaler Gateway in the second DMZ must have a root certificate installed that is signed by the same CA as the server certificate used by the STA and XML service.</p>
NetScaler Gateway in the second DMZ makes an ICA connection to a published application on a server in the internal network.	<p>An SSL server certificate must be installed within the SSL Relay on the server hosting the published application.</p> <p>NetScaler Gateway proxy in the second DMZ must have a root certificate installed that is signed by the same CA as the server certificate installed within the SSL Relay.</p>

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.

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.

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.

Operators and Definitions

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).

Qualifiers, Operators, Operands, Actions, and Examples

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'

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.

Maintain and Monitor

May 29, 2013

After you configure 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.

To create an administrative user on NetScaler Gateway

1. In the configuration utility, in the navigation pane, on the Configuration tab, expand System > User Administration and then click System Users.
2. In the details pane, click Add.
3. In User Name, type a user name.
4. In 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.

Creating Administrative Groups

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

To configure an administrative group by using the configuration utility

1. In the configuration utility, in the navigation pane, on the Configuration tab, expand System > User Administration and then click System Groups.
2. In the details pane, click Add.
3. In Group Name, type a name for the group.
4. To add an existing user to the group, in Members, click Add.
5. Under Available, select a user and then click the right arrow.
6. Under Command Policies, in Action, click Insert, select a policy or policies, click OK, click Create and then click Close.

Configuring Custom Command Policies for Delegated Administrators

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.

To create a simple custom command policy

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

To create an advanced custom command policy

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

To bind a custom command policy to a user or group

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

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.

To save the configuration on NetScaler Gateway

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

To view and save the configuration file on NetScaler Gateway

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

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

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

Note: Citrix recommends saving the file using the file name ns.conf.

To view the current running configuration

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

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

To compare the saved and running configuration

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

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

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.

To clear NetScaler Gateway configuration settings

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

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.

To create an auditing policy

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Auditing.
2. In Name, type a name for the policy.
3. Select one of the following:
 - Syslog if you want to send the logs to a Syslog server.
 - Nslog to store the logs on NetScaler Gateway.
Note: If you select this option, logs are stored in the /var/log folder on the appliance.
4. In the details pane, click Add.
5. Type the following information for the server information where the logs are stored:
 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

To bind an auditing policy globally

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

To modify an auditing policy

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

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

To remove an auditing policy

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

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

Configuring ACL Logging

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.

To configure ACL logging by using the configuration utility

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

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

After you configure ACL logging, you can enable it on NetScaler Gateway. Create an auditing policy and then bind it to a

user, group, virtual server, or globally.

To enable ACL or TCP logging on NetScaler Gateway

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway > Policies > Auditing, .
2. Select either syslog or nslog.
3. On the Servers tab, click Add.
4. In the Create Auditing Server dialog box, in Name, type a name for the server and then configure the server settings
5. Click ACL Logging or TCP Logging and then click Create.

Enabling 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

To enable logging

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

May 15, 2013

You can monitor 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.