



# Access Gateway 10

2015-05-03 05:22:56 UTC

© 2015 Citrix Systems, Inc. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

---

---

# Contents

- Access Gateway 10** ..... 13
  - Access Gateway 10..... 15
    - About This Release ..... 16
      - Introduction ..... 17
      - Key Features ..... 18
        - Access Gateway Architecture ..... 19
        - How Access Gateway Works with the Access Gateway Plug-in ..... 21
        - Access Gateway 10 Compatibility with Citrix Products ..... 23
      - What's New ..... 24
      - Known Issues ..... 27
    - System Requirements ..... 30
      - Access Gateway Plug-in System Requirements ..... 31
      - Endpoint Analysis Requirements ..... 36
  - Plan ..... 37
    - Identifying Access Gateway Prerequisites ..... 38
    - Access Gateway 10 Pre-Installation Checklist ..... 39
    - Planning for Security with Access Gateway ..... 47
  - Deploy ..... 49
    - Deploying Access Gateway Appliances in the DMZ ..... 50
    - Deploying Access Gateway Appliances in the Secure Network ..... 51
    - Deploying Access Gateway with CloudGateway ..... 52
    - Deploying Access Gateway with the Web Interface..... 53
      - Deployment Options for the Web Interface ..... 55
        - Deploying the Web Interface in the Secure Network ..... 56
        - Deploying the Web Interface Parallel to the Access Gateway in the DMZ ..... 57
        - Deploying the Web Interface Behind the Access Gateway in the DMZ ..... 58
    - Deploying Plug-ins for User Access ..... 59
    - Deploying Access Gateway in a Double-Hop DMZ ..... 61

---

Install and Setup .....	62
Configuring Settings Using the Configuration Utility.....	63
Configuring Settings with the Access Gateway Policy Manager .....	64
Configuring the Access Gateway Using Wizards .....	65
Configuring Access Gateway Settings with the Remote Access Wizard	67
Configuring Settings Using the Access Gateway Wizard .....	70
Configuring the Host Name .....	71
Configuring IP Addresses on the Access Gateway .....	72
Changing Mapped IP Addresses .....	73
Configuring Subnet IP Addresses .....	74
Configuring IPv6 for Client Connections.....	75
Configuring Routing on the Access Gateway .....	76
Testing Your Access Gateway Configuration .....	78
Configuring Name Service Providers.....	80
Configuring Auto Negotiation.....	82
Upgrading the Access Gateway .....	83
Licensing .....	85
Access Gateway License Types.....	86
Obtaining Your Platform or Universal License Files.....	88
To install a license on the Access Gateway using the configuration utility .....	91
Verifying Installation of the Universal License .....	92
Installing Licenses on Appliances in a High Availability Pair .....	93
Manage .....	94
Creating Additional Virtual Servers.....	95
To create additional virtual servers .....	96
Configuring Connection Types on the Virtual Server .....	97
Configuring A Listen Policy for Wildcard Virtual Servers .....	98
Configuring High Availability on Access Gateway Enterprise Edition.....	100
How High Availability Works .....	101
Configuring Access Gateway Enterprise Edition for High Availability	103
Adding an RPC Node .....	104
Configuring the Primary and Secondary Appliances for High Availability .....	105
Disabling Access Gateway Network Interfaces.....	106
Customizing Your High Availability Deployment .....	107
Synchronizing Access Gateway Appliances.....	108
Disabling High Availability Propagation .....	110

---

Troubleshooting Command Propagation .....	111
Forcing the Primary Access Gateway to Stay Primary .....	112
Forcing the Secondary Appliance to Stay Secondary .....	113
Configuring Fail-Safe Mode .....	114
Configuring the Virtual MAC Address .....	115
Configuring High Availability Pairs over Routed Networks .....	117
Configuring an Independent Network Computing High Availability Pair .....	119
Configuring Route Monitors .....	120
Configuring Link Redundancy .....	121
Installing and Managing Certificates .....	123
Creating a Private Key .....	124
Creating a Certificate Signing Request .....	126
Installing the Signed Certificate on the Access Gateway .....	128
Configuring Intermediate Certificates .....	130
Importing and Installing an Existing Certificate to Access Gateway .....	133
Certificate Revocation Lists .....	135
Monitoring Certificate Status with OCSP .....	136
Configuring OSCP Certificate Status .....	137
Configuring Policies and Profiles on the Access Gateway .....	139
How Policies Work .....	140
Setting the Priorities of Policies .....	141
Configuring Conditional Policies .....	142
Configuring System Expressions .....	143
Creating Simple and Compound Expressions .....	144
Adding Custom Expressions .....	145
Creating Policies on the Access Gateway .....	146
How Session Policies Work .....	147
Creating a Session Profile .....	149
Binding Session Policies .....	152
How a Traffic Policy Works .....	153
Creating a Traffic Policy .....	154
Configuring Form-Based Single Sign-On .....	156
Binding a Traffic Policy .....	157
Removing Traffic Policies .....	158
Allowing File Type Association .....	159
Creating a Web Interface Site .....	160
Configuring the Access Gateway for File Type Association .....	161

---

Configuring Citrix XenApp for File Type Association .....	164
How TCP Compression Policies Work .....	165
Creating or Modifying a TCP Compression Policy .....	166
Binding, Unbinding, and Removing TCP Compression Policies .....	168
Monitoring TCP Compression on User Connections .....	171
Configuring Authentication and Authorization.....	172
Configuring Authentication on Access Gateway.....	173
Authentication Types Supported on the Access Gateway .....	174
Configuring Default Global Authentication Types .....	175
Configuring Authentication without Authorization.....	176
Configuring Local Users .....	177
Configuring Groups .....	179
Adding Users to Groups.....	180
Configuring Policies with Groups.....	181
How Authentication Policies Work .....	183
Configuring Authentication Profiles .....	184
Binding Authentication Policies .....	186
Setting Priorities for Authentication Policies .....	188
Configuring LDAP Authentication.....	189
To configure LDAP authentication .....	191
Determining Attributes in your LDAP Directory.....	194
Configuring RADIUS Authentication .....	195
Choosing RADIUS Authentication Protocols.....	197
Configuring IP Address Extraction .....	198
Configuring the Access Gateway to Use One-Time Passwords .....	199
Configuring RSA SecurID Authentication .....	200
Configuring Password Return with RADIUS .....	201
Configuring SafeWord Authentication.....	202
Configuring Gemalto Protiva Authentication.....	203
Configuring TACACS+ Authentication .....	204
Configuring Client Certificate Authentication.....	205
Configuring and Binding a Client Certificate Authentication Policy .....	206
Configuring Two-Factor Client Certificate Authentication .....	208
Configuring Smart Card Authentication.....	209
Configuring a Common Access Card .....	212
Configuring Multifactor Authentication .....	213
Configuring Multifactor Authentication .....	214

---

Configuring Double-Source Authentication .....	216
Selecting the Authentication Type for Single Sign-On	217
Using Certificates and LDAP Authentication .....	218
Disabling Authentication.....	222
Configuring the Number of User Sessions .....	223
Configuring Authentication for Specific Times .....	224
Configuring Authorization .....	225
Setting Default Global Authorization.....	226
Configuring Authorization Policies.....	227
Binding Authorization Policies .....	228
Setting the Priority for Authorization Policies	229
Configuring LDAP Group Extraction.....	230
Group Memberships from Group Objects Working Evaluations	231
Group Memberships from Group Objects Non-Working Evaluations.....	232
LDAP Authorization Group Attribute Fields .....	233
Configuring LDAP Authorization .....	234
Configuring LDAP Nested Group Extraction .....	235
Configuring LDAP Group Extraction for Multiple Domains	237
Creating Session Policies for Group Extraction	238
Creating LDAP Authentication Policies for Multiple Domains	240
Creating Groups and Binding Policies for LDAP Group Extraction for Multiple Domains.....	242
Configuring RADIUS Group Extraction .....	243
To configure RADIUS authorization.....	245
Configuring Endpoint Polices .....	246
How Endpoint Policies Work .....	247
Evaluating Client Logon Options.....	249
Configuring Preauthentication Policies and Profiles .....	250
Configuring Endpoint Analysis Expressions .....	254
Configuring Custom Expressions.....	256
Configuring Multiple Expressions.....	258
Binding Preauthentication Policies .....	259
Setting the Priority of Preauthentication Policies .....	260
Unbinding and Removing Preauthentication Polices.....	261
Configuring Post-Authentication Policies .....	262
Configuring a Post-Authentication Policy.....	263
Configuring the Frequency to Run a Post- Authentication Policy	264

---

Configuring Quarantine and Authorization Groups .....	265
Configuring Quarantine Groups .....	266
Configuring Authorization Groups .....	268
Configuring Security Preauthentication Expressions for User Devices	270
Configuring Antivirus, Firewall, Internet Security or Antispam Expressions .....	271
Configuring Service Policies .....	273
Configuring Process Policies .....	274
Configuring Operating System Policies .....	275
Configuring File Policies .....	277
Configuring Registry Policies .....	278
Configuring Compound Client Security Expressions .....	280
Connect Users .....	282
How User Connections Work with the Access Gateway Plug-in .....	283
How User Connections Work with Receiver .....	284
Tunneling Private Network Traffic over Secure Connections .....	285
Operation through Firewalls and Proxies .....	286
Terminating the Secure Tunnel and Returning Packets to the User Device .....	287
Supporting the Access Gateway Plug-in .....	288
Choosing the User Access Method .....	289
How Users Connect to Applications, Desktops, and ShareFile .....	290
Integrating the Access Gateway Plug-in with Receiver .....	291
Adding the Access Gateway Plug-in to Receiver .....	293
Configuring the Receiver Home Page on Access Gateway .....	296
Applying the Receiver Theme to the Logon Page .....	297
Creating a Custom Theme for the Logon Page .....	298
Allowing Access from Mobile Devices .....	300
Configuring Secure Browse in Access Gateway .....	301
Configuring Endpoint Analysis for Mobile Devices .....	303
Configuring TCP Compression Policy Expressions for Mobile Devices	304
Enabling Support for Device Polling for Mobile Devices .....	305
Selecting the Plug-in Type .....	306
Configuring the Access Gateway Plug-in for Windows or Mac OS X .....	308
Installing the Access Gateway Plug-in .....	309
Deploying the Access Gateway Plug-in from Active Directory .....	311
Upgrading and Removing the Access Gateway Plug-in for Active Directory .....	313

---

Troubleshooting the Access Gateway Plug-in Installation Using Active Directory .....	314
Monitoring and Ending User Sessions.....	315
Configuring Access to Applications and Virtual Desktops in the Web Interface .....	316
Connecting Using the Access Gateway Plug-in for Java .....	319
How Clientless Access Works .....	322
Enabling Clientless Access.....	323
Encoding the Web Address .....	325
How Clientless Access Policies Work.....	327
Creating New Clientless Access Policies .....	328
Configuring Domain Access for Users .....	330
Configuring Clientless Access for SharePoint 2003 and SharePoint 2007	332
Setting a SharePoint Site as the Home Page .....	333
Enabling Name Resolution for SharePoint 2007 Servers	334
Enabling Clientless Access Persistent Cookies.....	335
Configuring Persistent Cookies for Clientless Access for SharePoint.....	336
Saving User Settings for Clientless Access Through Web Interface	337
Configuring the Client Choices Page .....	339
Showing the Client Choices Page at Logon.....	340
Configuring Client Choices Options .....	342
Configuring Access Scenario Fallback .....	345
Creating Policies for Access Scenario Fallback.....	346
Using the Repeater Plug-in .....	349
Managing User Sessions.....	351
Configuring Connections for the Access Gateway Plug-in.....	353
Connecting to Internal Network Resources .....	354
Enabling Proxy Support for User Connections .....	355
Configuring Time-Out Settings.....	357
Configuring Forced Time-Outs.....	358
Configuring Session or Idle Time-Outs .....	360
Configuring Single Sign-On .....	362
Configuring Single Sign-On with Windows .....	363
Configuring Single Sign-on to Web Applications .....	365
Configuring Single Sign-On to Web Applications Using LDAP	367
Configuring Single Sign-On to a Domain .....	368
Configuring Client Interception.....	369
Configuring Intranet Applications for the Access Gateway Plug-in	370



---

Configuring Intranet Applications for the Access Gateway Plug-in for Java .....	372
Configuring Address Pools .....	373
Configuring IP Pooling Using the Configuration Utility .....	375
Defining Address Pool Options.....	376
Configuring Split Tunneling .....	378
Configuring Name Service Resolution.....	380
Supporting VoIP Phones .....	381
Configuring Application Access for the Access Gateway Plug-in for Java .....	382
Configuring the Access Interface .....	384
Replacing the Access Interface with a Custom Home Page .....	385
Changing the Access Interface .....	386
Creating and Applying Web and File Share Links .....	387
Configuring User Name Tokens in Bookmarks .....	389
Configuring Distributed File System Links.....	390
Integrate .....	392
Integrating Access Gateway with CloudGateway.....	393
How Access Gateway and CloudGateway Integrate .....	396
Configuring Access Gateway and CloudGateway.....	398
Configuring Session Policies and Profiles for CloudGateway .....	401
Configuring Session Profiles for CloudGateway Express .....	405
Creating the Session Profile for Receiver for CloudGateway Express .....	406
Creating the Session Profile for Receiver for Web for CloudGateway Express .....	408
Creating the Session Policy for PNA Services for CloudGateway Express .....	410
Connecting to StoreFront by Using Email-Based Discovery .....	412
Configuring Session Profiles for CloudGateway Enterprise .....	414
Creating the Session Profile for Receiver for CloudGateway Enterprise .....	415
Creating the Session Profile for Receiver for Web for CloudGateway Enterprise.....	417
Creating the Session Policy and Profile for PNA Services for CloudGateway Enterprise.....	419
Creating a Session Policy and Profile for the Access Gateway Plug-in .....	421
Binding Session Policies and Setting the Priority .....	423
Configuring Custom Clientless Access Policies for Receiver .....	425
Configuring Custom Clientless Access Policies for Receiver for Web .....	427
Configuring Domains for Clientless Access for Access Gateway and StoreFront.....	430

---

---

Providing Access to Published Applications .....	431
Integrating Access Gateway with XenApp or XenDesktop .....	432
Establishing a Secure Connection to the Server Farm .....	433
Setting Up a Web Interface Site to Work with the Access Gateway	436
Web Interface Features .....	437
Setting Up a Web Interface Site .....	438
Creating a Web Interface Site in XenApp 5.0 or XenDesktop 2.1	439
Configuring Access Gateway Settings for the Web Interface on XenApp 5.0 or XenDesktop 2.1 .....	441
Creating a Web Interface 5.3 Site .....	442
Configuring Access Gateway Settings in Web Interface 5.3	444
Adding XenApp and XenDesktop to a Single Site .....	445
Routing Client Connections Through the Access Gateway	447
Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface .....	448
Configuring Policies for Published Applications and Desktops	449
To run the Published Applications Wizard .....	451
Configuring the Secure Ticket Authority on the Access Gateway	452
Configuring Additional Web Interface Settings on Access Gateway Enterprise Edition.....	454
Configuring Web Interface Failover .....	455
Configuring Smart Card Access with the Web Interface	456
Configuring SmartAccess on Access Gateway Enterprise Edition	457
How SmartAccess Works for XenApp and XenDesktop	458
Configuring XenApp Policies and Filters .....	459
To configure a session policy for SmartAccess	460
Configuring Client Device Mapping on XenApp.....	461
To configure a restrictive policy on XenApp 5.0	462
To configure a non-restrictive policy on XenApp 5.0	463
To configure a restrictive policy on XenApp 6	464
To configure a non-restrictive policy on XenApp 6	465
Enabling XenApp as a Quarantine Access Method .....	466
Creating a Session Policy and Endpoint Analysis Scan for a Quarantine Group.....	467
Configuring XenDesktop 4.0 for SmartAccess .....	469
To configure a session policy for SmartAccess	470
To configure policies and filters in XenDesktop 4.0	471
To configure policies and filters in XenDesktop 5	472
To add the Desktop Delivery Controller as the STA	473

Configuring Single Sign-on to the Web Interface on Access Gateway Enterprise Edition.....	474
Configuring Single Sign-On to the Web Interface.....	475
To configure single sign-on to Web applications globally	476
To configure single sign-on to Web applications by using a session policy .....	477
To define the HTTP port for single sign-on to Web applications.....	478
Additional Configuration Guidelines .....	479
To test the single sign-on connection to the Web Interface	480
To configure single sign-on for XenApp and file shares	481
Configuring Single Sign-On to the Web Interface using a Smart Card .....	482
To configure the client certificate for single sign-on using a smart card .....	484
Customize .....	485
Deploying Access Gateway in a Double-Hop DMZ .....	486
How a Double-Hop Deployment Works .....	487
Communication Flow in a Double-Hop DMZ Deployment .....	488
Authenticating Users.....	489
Creating a Session Ticket .....	490
Starting Citrix Receiver.....	491
Completing the Connection.....	492
Preparing for a Double-Hop DMZ Deployment.....	494
Installing the Access Gateway in a Double-Hop DMZ .....	495
Step 1: Installing an Access Gateway in the First DMZ	496
Step 2: Configuring the First Access Gateway .....	497
Step 3: Installing an Access Gateway in the Second DMZ	498
Step 4: Configuring a Virtual Server on the Access Gateway Proxy	499
Step 5: Configuring the Access Gateway to Communicate with the Access Gateway Proxy .....	500
Step 6: Binding Access Gateway in the Second DMZ Globally or to a Virtual Server .....	501
Step 7: Configuring Access Gateway to Handle the STA and ICA Traffic.....	502
Step 8: Opening the Appropriate Ports on the Firewalls	503
Step 9: Managing SSL Certificates in a Double-Hop DMZ Deployment .....	505
Configuring DNS Virtual Servers.....	508
Resolving DNS Servers Located in the Secure Network.....	509
Using Operators and Operands in Policy Expressions .....	511
Configuring Server-Initiated Connections .....	518

---

Monitor .....	520
Configuring Delegated Administrators .....	521
Configuring Command Policies for Delegated Administrators .....	522
Configuring Custom Command Policies for Delegated Administrators .....	524
Viewing Access Gateway Configuration Settings .....	526
Saving the Access Gateway Configuration .....	527
Clearing the Access Gateway Configuration .....	529
Configuring Auditing on the Access Gateway .....	530
Configuring Logs on Access Gateway .....	531
Configuring ACL and TCP Logging .....	533
Enabling Access Gateway Plug-in Logging .....	535
To monitor ICA connections .....	537

---

# Access Gateway 10

Citrix Access Gateway is a secure desktop and application access solution. The appliance gives administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere by using HDX SmartAccess. Access Gateway gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, the solution empowers users with a single point of access—optimized for roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today’s mobile workforce.

## In This Section

This section of eDocs contains information about installing, setting up, and configuring Access Gateway 10.

<a href="#">About This Release</a>	Contains information about this release, including Access Gateway features, components, what's new, and known issues.
<a href="#">System Requirements</a>	Provides system requirements for the appliance, the Access Gateway Plug-in, and the Endpoint Analysis Plug-in.
<a href="#">Plan</a>	Provides information for evaluating and planning your installation of Access Gateway. Includes the Access Gateway Pre-Installation Checklist.
<a href="#">Deploy</a>	Provides information about deploying the Access 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 the Access Gateway with Citrix XenApp, Citrix XenDesktop and the Web Interface.
<a href="#">Install and Setup</a>	Provides information about using the configuration utility and wizards to configure settings such as the host name, IP addresses, configure routing, configure name service providers, upgrade the Access Gateway software and test the Access Gateway configuration.
<a href="#">Licensing</a>	Discusses how to license Access Gateway 10.

<p><a href="#">Manage</a></p>	<p>Provides information about configuring detailed settings that enable users to connect to resources in the secure network, such as adding virtual servers, configuring high availability, installing and managing certificates, configuring policies and profiles, configuring authentication and authorization, understanding various user connection methods, configuring connections for the Access Gateway Plug-in, configuring the Access Interface, and configuring endpoint policies.</p>
<p><a href="#">Connect Users</a></p>	<p>Provides information about deploying the Access Gateway Plug-in and the ways users connect.</p>
<p><a href="#">Integrate</a></p>	<p>Explains how to configure the Access Gateway appliance to work with Citrix CloudGateway, XenApp, XenDesktop, and the Web Interface. CloudGateway includes the components AppController and StoreFront.</p>
<p><a href="#">Customize</a></p>	<p>Provides information about deploying Access Gateway in a double-hop DMZ, configuring DNS virtual servers, using operators and operands in policy expressions, configuring server-initiated connections, and enabling Access Gateway Plug-in logging.</p>
<p><a href="#">Monitor</a></p>	<p>Describes ways to manage your Access Gateway environment.</p>

---

# About This Release

Citrix Access Gateway 10 offers support for the following:

- Clientless access for Receiver for Web
- 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

Access Gateway 10 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, data through SmartAccess, and published desktops with Citrix XenDesktop
- Integration and control of remotely delivered Web and SaaS applications, mobile apps for iOS, and ShareFile data from Citrix CloudGateway
- 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 Access Gateway universal license (included in XenApp Platinum Edition, XenDesktop Platinum Edition, and Citrix NetScaler Platinum Edition)

---

# About This Release

Citrix Access Gateway 10 offers support for the following:

- Clientless access for Receiver for Web
- 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

Access Gateway 10 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, data through SmartAccess, and published desktops with Citrix XenDesktop
- Integration and control of remotely delivered Web and SaaS applications, mobile apps for iOS, and ShareFile data from Citrix CloudGateway
- 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 Access Gateway universal license (included in XenApp Platinum Edition, XenDesktop Platinum Edition, and Citrix NetScaler Platinum Edition)



---

# Introduction

Before you install and configure Access 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 Access Gateway in any network infrastructure without requiring changes to the existing hardware or software running in the secure network. Access 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 Access Gateway Pre-Installation Checklist to have on hand before you configure Access Gateway.

<a href="#">Access Gateway Appliances</a>	Provides information about Access Gateway appliances and the appliance installation instructions.
<a href="#">Access Gateway 10 Pre-Installation Checklist</a>	Provides planning information to review and a list of tasks to complete before you install Access Gateway in your network.
<a href="#">Deploying Access Gateway</a>	Provides information about deploying the Access 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 Access Gateway with Citrix XenApp and Citrix XenDesktop.
<a href="#">Installing Licenses on Access Gateway</a>	Provides information about installing licenses on the appliance. Also provides information about installing licenses on multiple Access Gateway appliances.

---

# Key Features

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

The first time you start Access 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 5500 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 Access Gateway operation, such as the options for authentication, authorization, network resources, virtual servers, session policies, and endpoint policies.

The key features of Access 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

---

# Access Gateway Architecture

The core components of Access Gateway are:

- Virtual servers. The Access 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 Access 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 Access Gateway with credentials that either Access 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 Access Gateway activity, including user logon events, resource access instances, and operational errors. This information is stored on Access Gateway or on an external server. For more information about accounting, see [Configuring Auditing on the Access Gateway](#).
- User connections. Users can log on to Access Gateway by using the following access methods:
  - The Access Gateway Plug-in for Windows is software that is installed on the user device. 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 Access 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 Access Gateway Plug-in from Receiver. When Receiver and the Access Gateway Plug-in are installed on the user device, Receiver adds the Access Gateway Plug-in automatically.
  - The Access 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 Access Gateway Plug-in for Windows.
  - The Access 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. Users can also connect to Web and SaaS applications, iOS mobile apps, and ShareFile data hosted in AppController.
  - Clientless access that provides users with the access they need without installing software on the user device.

When configuring Access 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 Access Gateway, such as file servers, applications, and Web sites.
- Virtual adapter. The Access Gateway virtual adapter provides support for applications that require IP spoofing. The virtual adapter is installed on the user device when the Access Gateway Plug-in is installed. When users connect to the internal network, the outbound connection between Access Gateway and internal servers use the intranet IP address as the source IP address. The Access Gateway Plug-in receives this IP address from the server as part of the configuration.

If you enable split tunneling on Access 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 Access Gateway Works with the Access Gateway Plug-in

Access Gateway allows user access to resources in the internal network through the following steps:

1. A user connects to Access Gateway for the first time by typing the Web address in the browser. The logon page appears and the user is prompted to enter a user name and password. If external authentication servers are configured, Access Gateway contacts the server and the authentication servers verify the user's credentials. If local authentication is configured, Access Gateway performs the user authentication.
2. If you configure a *preauthentication policy* and a user logs on from a Windows-based computer, when the user types the Access Gateway Web address, Access 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, Access 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.
3. When the user is successfully authenticated, the Access Gateway tunnel is initiated. Access Gateway now prompts the user to download and install the Access Gateway Plug-in for Windows or Access Gateway Plug-in for Mac OS X. If you are using the Access 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, Access 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 an Access Gateway home page where the user can select resources to access. The home page that is included with Access Gateway is called the *Access Interface*. If the user logs on by using the Access 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, Access 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 Access 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.

**Note:** If you deploy CloudGateway Enterprise with AppController in your internal network, a user who connects from outside the internal network must connect to Access Gateway first. When the user establishes the connection, he or she can access Web and SaaS applications, native iOS mobile apps, and ShareFile data hosted on AppController. A user can connect with the Access Gateway Plug-in, through clientless access, or by using Citrix Receiver. For more information about AppController, see [AppController](#).

---

# Access Gateway 10 Compatibility with Citrix Products

The following table provides the Citrix product names and versions that Access Gateway Enterprise Edition is compatible with.

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

Citrix product	Release version
Branch Repeater	4.3.27, 5.0, 5.5, and 5.7
CloudGateway	Express - 1.0, 1.1 and 1.2 (StoreFront) Enterprise - 1.1 and 2.0 (AppController)
Receiver for Android	3.0
Receiver for iOS	5.5.x
Receiver for Mac	11.4 and 11.5
Receiver For Windows	1.2, 2.0, 2.1, 3.0, 3.1, and 3.2
VDI-in-a-Box	5.1 and 5.0.3
Web Interface	4.5, 5.0.1, 5.1, 5.2, 5.3, and 5.4
XenApp	4.5 (Windows Server 2003) 5.0 (Windows Server 2003 and 2008) XenApp 5 Feature Pack 2 for Windows Server 2003 6.0 (Windows Server 2008) 6.5 for Windows Server 2008 R2
XenDesktop	2.1, 3.0, 4.0, 5.0, 5.5, and 5.6

**Note:** Compatibility with VDI-in-a-Box, Version 5.0.3 supports the SOCKet Secure (SOCKS) protocol only.

---

# What's New

Access Gateway 10 has the following new features:

- **Apply the original Access Gateway theme, the Citrix Receiver theme, or a custom theme to the logon page.** You can use the configuration utility or command line to change the original Access Gateway logon, logoff, and endpoint analysis pages to use either the Citrix Receiver theme or your own custom theme. For more information, see [Applying the Receiver Theme to the Logon Page](#) and [Creating a Custom Theme for the Logon Page](#).

**Note:** To use this feature, you must install Access Gateway 10, Build 71.6014.e. In addition, if your appliance is licensed as a NetScaler VPX running on the SDX platform and you configure link aggregation, Citrix recommends installing Access Gateway 10, Build 73.5002.e after you install Build 71.6014.e. This allows user connections through Access Gateway to CloudGateway 2.5.

- **Configure an IP address to support device polling.** If you deploy AppController in your internal network, to support the Active poll period policy in AppController 2.5 for mobile devices using Citrix Receiver, you provide an IP address, such as `https://AppControllerIPaddress` or a fully qualified domain name (FQDN) such as `https://AppControllerFQDN`. Polling determines the current application (enabled or disabled) and device (lock or erase) status. The status appears on the Devices tab in the AppController management console. When a device has network connectivity, polling allows the running application to detect and respond to changes in the app state. For more information, see [Enabling Support for Device Polling for Mobile Devices](#).

**Note:** To use this feature, you must install Access Gateway 10, Build 71.6014.e. In addition, if your appliance is licensed as a NetScaler VPX running on the SDX platform and you configure link aggregation, Citrix recommends installing Access Gateway 10, Build 73.5002.e after you install Build 71.6014.e. This allows user connections through Access Gateway to CloudGateway 2.5.

- **Configure cache, responder, and rewrite policies.** Access Gateway supports cache, responder, and rewrite policies that you bind to the Access Gateway virtual server. Cache redirection policies allow repeated requests for content to be delivered from the cache server. Responder policies enable the Access Gateway virtual server to deliver different responses to similar HTTP requests. Access Gateway can base the response on who sends the request, where it is sent from, and other criteria with security and system management implications. The rewrite feature allows you to rewrite URL information in requests and responses to and from the Access Gateway virtual server. For example, you can rewrite all HTTP links to HTTPS in the response body. For more information about configuring these policies, see the NetScaler documentation in eDocs. On Access Gateway, you can configure and bind these policies by using the Access Gateway Policy Manager.
- **Configure clientless access for Receiver for Web and Receiver.** You can configure session and clientless access policies and profiles in the configuration utility to configure clientless access for Receiver for Web and Receiver. Users can gain access to Windows, Web, and SaaS applications by using Receiver for Web and Receiver through Access Gateway.



- **Configure connections from Receiver for iOS.** Secure Browse allows users to connect through Access Gateway to network resources from iOS mobile devices with Receiver.  
  
**Note:** Android devices use Micro VPN to connect to network resources through Access Gateway.
- **Configure connections with the Remote Access Wizard.** Access Gateway includes a new wizard that allows you to configure the following settings for user access:
  - Access Gateway-specific settings including the IP address, port, and mapped IP address
  - LDAP and RADIUS authentication
  - DNS server IP address
  - Certificates
  - CloudGateway settings for AppController 2.0
  - CloudGateway settings for StoreFront
  - Web Interface settings
  - Account Services address for email-based discovery
- **Configure email-based discovery.** You can configure Access Gateway to allow email-based discovery of the StoreFront server. When users log on to Receiver for the first time, they enter their email address or the StoreFront URL if they do not have email-based discovery configured. You configure email-based discovery as part of global settings or in a session policy. You must also configure an authoritative DNS server in StoreFront to respond to the SRV request from Receiver. For more information about configuring DNS settings in StoreFront, see [Configuring Email-Based Account Discovery](#). To configure email-based discovery in Access Gateway, see [Connecting to StoreFront by Using Email-Based Discovery](#).
- **Configure smart card support for Web Interface on NetScaler.** You can configure settings to allow users to log on with a smart card to the Web Interface on NetScaler.
- **Enable Access Interface bookmarks.** Access Gateway supports the following four services to enable bookmarks to appear in the Access Interface when users log on with Receiver: Enumeration, Check Protection, Ticketing, and Access.
- **Enable multistream ICA support.** Access Gateway supports the delivery of ICA over multiple streams: four TCP/IP streams. This gives full flexibility for Quality of Service (QoS) routing over the network and provides superior audio quality when packet loss or congestion occurs. This feature enhances the end user experience and improves the performance of XenApp and XenDesktop sessions significantly for remote users.
- **Enable static caching.** When you configure authentication globally, you can select the Enable static caching check box. This option enables Access Gateway to deliver logon pages from the Access Gateway in-memory cache rather than from the HTTP server running on Access Gateway. If you choose to deliver the logon page from the in-memory cache, Access Gateway delivery of the logon page is significantly faster than from the HTTP server. Choosing to deliver the logon page in this manner reduces the wait time when a large number of users log on at the same time.

- **Enable Web socket protocol support for HTML5 Receiver.** Access Gateway supports bi-directional communication between clients and servers over HTTP.
- **Integrate Access Gateway with CloudGateway Enterprise.** You can configure the appliance to allow users to connect directly to AppController, the unified policy controller of CloudGateway Enterprise. When users connect, they can access their Web, SaaS, mobile iOS applications, along with ShareFile data.
- **Integrate Access Gateway with CloudGateway Express.** You can configure the appliance to work with StoreFront, a component of CloudGateway, to allow access to Windows-based applications and virtual desktops hosted in XenApp and XenDesktop. You enable users to connect by using Receiver for Web or Receiver.
- **Support for Outlook Web App for Exchange Server 2010.** Preconfigured clientless access policies support Outlook Web App for Exchange Server 2010 as well as the earlier version, referred to as Outlook Web Access
- **View new visual theme.** The configuration utility has a new look and feel. The organization will be almost identical to earlier versions of Access Gateway Enterprise Edition, but the theme is updated to look similar to other Citrix products. Logon pages for users and the choices page also have a new look and feel.

---

# Known Issues

Version: 1.0

## Finding Documentation

To access complete and up-to-date product information, in the Citrix eDocs library, expand the topics for [Access Gateway 10](#).

### Licensing Documentation

To access licensing documentation for Access Gateway Enterprise Edition, see [Installing Licenses on the Access Gateway](#).

For the current list of known and fixed issues, see the [NetScaler Access Gateway 10 Maintenance Build](#) readme in the Citrix Knowledge Center.

## New Features

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

## Known Issues in This Release

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

1. When you enable ICA proxy on Access Gateway, when users connect to XenDesktop, if users attempt to open a published application, the Secure Ticket Authority (STA) issues a session ticket with an invalid format and the connection fails. [#251110]
2. After you configure Access Gateway to provide user connections through Citrix Receiver, when users right-click the Receiver icon in the notification area, the Log on option does not appear. Users must connect by using the Web browser or they must right-click the Receiver icon, click Preferences, and then click Plug-in status. You can also enable the log on option to appear when users right-click the Receiver icon by adding the following settings in the registry:
  - a. Add the Receiver key (if the key doesn't already exist) under the following registry locations:
    - HKEY\_CURRENT\_USER\Software\Citrix\
    - HKEY\_LOCAL\_MACHINE\Software\Citrix\
  - b. Add the Inventory key in the following registry locations:

- HKEY\_CURRENT\_USER\Software\Citrix\Receiver
  - HKEY\_CURRENT\_USER\Software\Citrix\Receiver
- c. In the Inventory key, configure the following REG\_SZ values:
- VPNAddress. Provide the value as the Web address for the Access Gateway appliance; for example, `https://<AccessGatewayFQDN>/`.
  - VPNPrompt1. Provide the value as "UserName".
  - VPNPrompt3. Provide the value as "\*Password".
- [#251596]
3. When you enable Access Gateway as a reverse proxy and you enable basic preauthentication and post-authentication scans, as well as encryption and client choices, when users log on with the Access Gateway Plug-in, the preauthentication scan passes, but the post-authentication scan fails. [#261547]
  4. If you configure Access Gateway to assign an intranet IP address to user devices that connect to Access Gateway, when users log on with the Access Gateway Plug-in, the secure DNS dynamic update does not occur and the intranet IP address is not registered with the DNS Server. [#285995]
  5. After you configure a virtual server to use the Access Gateway Plug-in for Java, when users log on with the Access Gateway Plug-in by using a browser that has a 64-bit Java Runtime Environment (JRE) installed, the plug-in fails to establish a connection. [#288469]
  6. When you configure a post authentication policy on Access Gateway and configure the policy to redirect the connection to the Web Interface if the endpoint analysis fails, when users log on with the Access Gateway Plug-in, if the user device fails the endpoint analysis scan, users receive the Access Gateway logon page instead of the Web Interface. [#290976]
  7. If you create a Web Interface 5.4 site and enable authentication through Access Gateway, and you enable single sign-on with a smart card to the Web Interface that enables smart card pass-through, when users log on with the Access Gateway Plug-in, the users' desktops are not listed on the Web Interface. [#291264]
  8. If you create a Web Interface 5.4 site and enable authentication with a smart card through Access Gateway, and you configure the Single Sign-on Domain on the Published Applications tab using the format domainname.com instead of domainname, when users start a published application or desktop, authentication fails. [#291821]
  9. If you create a Web Interface 5.4 site and enable single sign-on with a smart card to the Web Interface that prompts user for a personal identification number (PIN), and if you do not configure the Single Sign-on Domain on the Published Applications tab, when users log on with the Access Gateway Plug-in and start a published application or desktop, authentication (directly or through single sign-on) fails. You must configure the Single Sign-on Domain. [#291822]
  10. When users connect with clientless access and try to download a file larger than 1 gigabyte (GB) from the file share on the home page, as the file is downloading, if an upload is attempted, the download process fails but the upload continues. [#292005]

11. When users log on with the Access Gateway Plug-in for Java and the Web Interface opens in Internet Explorer 9, if users do not turn on Compatibility View in Internet Explorer, when they click a published application, the following error appears: Resource shortcuts are not available. [#298971]
12. If you configure an intranet IP address on Access Gateway, when users connect with the Access Gateway Plug-in on a computer running Windows XP Service Pack 3 and try to access a CIFS share hosted on a computer in the secure network, users receive an error that the share is inaccessible. [#299515]
13. When users log on using clientless access and click a bookmark from the home page to open a Distributed File Share (DFS), if the target folder resides on a different computer than the computer where the domain DFS server resides, the share does not open. [#300511]
14. When you configure address pools, enable intranet IP addresses, and disable spillover, when users log on with the Access Gateway Plug-in and then try to log on from a second user device, the Transfer Login page appears. However, the message appears incorrectly as text only on a blank page. When users click Cancel, the button is disabled, rather than redirecting users to the logon page again. [#301060]
15. If a user password is longer than 31 characters, when users try to log on through the Access Gateway Plug-in logon dialog box rather than through a Web browser, logon fails. A message appears stating that the user name and password are invalid. [#301338]
16. If Access Gateway license is bound to any host name other than "ns" or "ANY", the license is considered to be inapplicable on Access Gateway. [#306678]
17. When you configure a preauthentication and post-authentication policy with an expression to scan a user device for a file, Access Gateway does not check for expression syntax. As a result, Access Gateway accepts inappropriate syntax configuration and the scan fails. [#309017]

---

# System Requirements

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.

# Access Gateway Plug-in System Requirements

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

The Access 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 and 10.8)	x	x	Safari Google Chrome
Windows 7 Home Basic Edition	x	x	Google Chrome 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	Google Chrome Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox, Version 9 Mozilla Firefox, Version 10

## Access Gateway Plug-in System Requirements

Windows 7 Professional Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox Version 9</p> <p>Mozilla Firefox Version 10</p>
Windows 7 Enterprise Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>
Windows 7 Ultimate Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 7</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>



## Access Gateway Plug-in System Requirements

Windows Vista Home Basic Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 7</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>
Windows Vista Home Premium Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>
Windows Vista Enterprise Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 7</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>

## Access Gateway Plug-in System Requirements

Windows Vista Business Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 7</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>
Windows Vista Ultimate Edition	x	x	<p>Google Chrome</p> <p>Internet Explorer, Version 7</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>
Windows XP Home Edition	x		<p>Google Chrome</p> <p>Internet Explorer, Version 8</p> <p>Internet Explorer, Version 9</p> <p>Mozilla Firefox, Version 9</p> <p>Mozilla Firefox, Version 10</p>

## Access Gateway Plug-in System Requirements

---

Windows XP Professional Edition	x		Google Chrome Internet Explorer, Version 7 Internet Explorer, Version 8 Internet Explorer, Version 9 Mozilla Firefox, Version 9 Mozilla Firefox, Version 10
---------------------------------	---	--	--

---

# Endpoint Analysis Requirements

When Access 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 Access Gateway. The requirements include information, such as 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, Access Gateway installs the Endpoint Analysis Plug-in without requiring user intervention. When users log on subsequently, Access Gateway checks the version of the plug-in. If the versions do not match, Access 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, or Windows 7 with all service packs and critical updates installed.
- Internet Explorer with cookies enabled. The minimum required version is 7.0.
- Firefox 3.0 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 Access 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 Access 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.

---

# Planning Your Access Strategy

Before you install Citrix Access Gateway 10, 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.

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 or published applications, 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. 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 Access 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 topics to help you plan your access strategy.

---

# Identifying Access Gateway Prerequisites

Before you start to configure settings on Access Gateway, review the following prerequisites:

- Access Gateway is physically installed in your network and has access to the network. Access Gateway is deployed in the demilitarized zone (DMZ) or internal network behind a firewall. You can also configure Access Gateway in a double-hop DMZ and for connections to a server farm.
- You configured Access Gateway with a default gateway or with static routes to the internal network so users can access resources in the network. Access 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 Access Gateway user functionality.
- You downloaded the Universal licenses for user connections with the Access Gateway Plug-in from My Citrix and the licenses are ready to be installed on Access Gateway.
- Access Gateway has a certificate that is signed by a trusted Certificate Authority (CA). For more information, see [Installing and Managing Certificates](#).

---

# Access Gateway 10 Pre-Installation Checklist

The checklist consists of a list of tasks and planning information you should complete before you install Access Gateway 10.

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 Access Gateway.

For instructions about installing and configuring Access Gateway, see [Installing the Access Gateway Appliance](#) in the Access Gateway appliances node and [Installing Access Gateway 10](#) in eDocs.

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

## User Devices

1	Ensure that user devices meet the installation prerequisites described in <a href="#">Access Gateway Enterprise Edition Client Connection Methods</a> .	
---	---	--

## Access Gateway Basic Network Connectivity

2	<p>Identify and write down the Access Gateway host name.</p> <p><b>Note:</b> 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.</p>	
3	Obtain universal licenses from My Citrix.	
4	Generate a Certificate Signing Request (CSR) and send to a Certificate Authority (CA) (date completed).	
5	Write down the system IP address and subnet mask.	
6	Write down the mapped IP address and subnet mask.	
7	Write down the subnet IP address and subnet mask (optional).	
8	<p>Write down the administrator password.</p> <p>The default password that comes with Access Gateway is <i>nsroot</i>.</p>	
9	<p>Write down the port number.</p> <p>This is the port on which Access Gateway listens for secure user connections. The default is TCP port 443. This port must be open on the firewall between the unsecured network and the DMZ.</p>	
10	Write down the default gateway IP address.	
11	Write down the DNS server IP address.	
12	Write down the first virtual server IP address and host name.	
13	Write down the second virtual server IP address and host name (if applicable).	
14	Write down the WINS server IP address (if applicable).	



## Internal Networks Accessible Through Access Gateway

15	<p>Write down the internal networks that users can access through Access 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 Access Gateway by using the Access Gateway Plug-in.</p>	
----	--	--

## High Availability

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

16	<p>Write down the Access Gateway software version number.</p> <p>The version number must be the same on both Access Gateway appliances.</p>	
17	<p>Write down the administrator password (nsroot).</p> <p>The password must be the same on both appliances.</p>	
18	<p>Write down the primary Access Gateway IP address and ID.</p> <p>The maximum ID number is 64.</p>	
19	<p>Write down the secondary Access Gateway IP address and ID.</p>	
20	<p>Obtain and install the Universal license on both appliances.</p> <p>You must install the same Universal license on both appliances.</p>	
21	<p>Write down the RPC node password.</p>	

## Authentication and Authorization

Access 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.

22	<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>	
23	<p>Write down the security type.</p> <p>You can configure security with or without encryption.</p>	
24	<p>Write down the administrator bind DN.</p> <p>If your LDAP server requires authentication, enter the administrator DN that Access Gateway should use to authenticate when making queries to the LDAP directory. An example is “cn=administrator, cn=Users, dc=ace, dc=com.”</p>	
25	<p>Write down the administrator password.</p> <p>This is the password associated with the administrator bind DN.</p>	
26	<p>Write down the Base DN.</p> <p>DN (or directory level) under which users are located; for example, “ou=users, dc=ace, dc=com.”</p>	
27	<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>	

28	<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 Access Gateway to identify the directory groups to which a user belongs.</p>	
29	Write down the subattribute name.	

## RADIUS Authentication and Authorization

If your environment includes a RADIUS server, you can use RADIUS for authentication.

RADIUS authentication includes RSA SecurID, SafeWord, and Gemalto Protiva products.

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

## Opening Ports Through the Firewalls (Single-Hop DMZ)

If your organization protects the internal network with a single DMZ and you deploy the Access Gateway in the DMZ, open the following ports through the firewalls. If you are installing two Access Gateway appliances in a double-hop DMZ deployment, see Double-Hop DMZ Deployment with Citrix XenApp.

On the Firewall Between the Unsecured Network and the DMZ

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

On the Firewall Between the Secured Network

36	<p>Open one or more appropriate ports on the firewall between the DMZ and the secured network. Access Gateway connects to one or more authentication servers or to computers running XenApp or Citrix XenDesktop in the secured network on these ports.</p>	
37	<p>Write down the authentication ports.</p> <p>Open only the port appropriate for your Access Gateway configuration.</p> <ul style="list-style-type: none"> <li>· For LDAP connections, the default is TCP port 389.</li> <li>· For a RADIUS connection, the default is UDP port 1812.</li> </ul>	
	<p>Write down the XenApp or XenDesktop ports.</p> <p>If you are using Access Gateway with XenApp or XenDesktop, open TCP port 1494. If you enable session reliability, open TCP port 2598 instead of 1494.</p> <p>Citrix recommends keeping both of these ports open.</p>	

## XenDesktop, XenApp, the Web Interface, or CloudGateway Express

Complete the following tasks if you are deploying Access Gateway to provide access to XenApp or XenDesktop through the Web Interface or StoreFront. The Access Gateway Plug-in is not required for this deployment. Users access published applications and desktops through Access Gateway by using only Web browsers and Citrix Receiver.

38	<p>Write down the FQDN or IP address of the server running the Web Interface or StoreFront.</p>	
39	<p>Write down the FQDN or IP address of the server running the Secure Ticket Authority (STA) (for Web Interface only).</p>	

## CloudGateway Enterprise

Complete the following tasks if you deploy AppController in your internal network. If users connect to AppController from an external network, such as the Internet, users must connect to Access Gateway before accessing Web and SaaS apps.

40	Write down the FQDN or IP address of AppController.	
41	Identify Web, SaaS, and mobile iOS applications users can access.	

## Double-Hop DMZ Deployment with XenApp

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

### Access 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 Access Gateway in the first DMZ through the firewall separating the Internet from the DMZ. Collect this information before installing Access Gateway in the first DMZ.

42	<p>Complete the items in the Access Gateway Basic Network Connectivity section of this checklist for this Access Gateway.</p> <p>When completing those items, note that Interface 0 connects this Access Gateway to the Internet and Interface 1 connects this Access Gateway to Access Gateway in the second DMZ.</p>	
43	<p>Configure the second DMZ appliance information on the primary appliance.</p> <p>To configure Access Gateway as the first hop in the double-hop DMZ, you must specify the host name or IP address of Access Gateway in the second DMZ on the appliance in the first DMZ. After specifying when the Access Gateway proxy is configured on the appliance in the first hop, bind it to Access Gateway globally or to a virtual server.</p>	
44	<p>Write down the connection protocol and port between appliances.</p> <p>To configure Access Gateway as the first hop in the double DMZ, you must specify the connection protocol and port on which Access 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>	

### Access Gateway in the Second DMZ

## Access Gateway 10 Pre-Installation Checklist

---

The second DMZ is the DMZ closest to your internal, secure network. Access 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.

45	<p>Complete the tasks in the Access Gateway Basic Network Connectivity section of this checklist for this Access Gateway.</p> <p>When completing those items, note that Interface 0 connects this Access Gateway to Access Gateway in the first DMZ. Interface 1 connects this Access Gateway to the secured network.</p>	
----	---	--

---

# Planning for Security with Access Gateway

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

## Configuring Secure Certificate Management

By default, Access 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 Access 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 Access Gateway.

If you deploy Access Gateway in any environment where Access 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 Access Gateway. For example, if you deploy Access Gateway with Citrix XenApp and the Web Interface, you can encrypt connections from Access Gateway to the Web Interface with SSL. In this configuration, you must install a trusted root certificate on Access Gateway.

## Authentication Support

You can configure Access 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 Access 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 Access Gateway. You can then configure Access Gateway to authenticate users against this local list. With this configuration, you do not need to maintain user accounts in a separate,

external directory.



---

# Deploying the Access Gateway

You can deploy the Access 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 residing in the internal network. All remote users must connect to the Access Gateway before they can access any resources on the internal network.

You can also deploy the Access Gateway with Citrix XenApp or Citrix XenDesktop. If your deployment includes XenApp, you can deploy the Access Gateway in a single-hop or double-hop DMZ configuration. A double-hop deployment is not supported with XenDesktop.

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

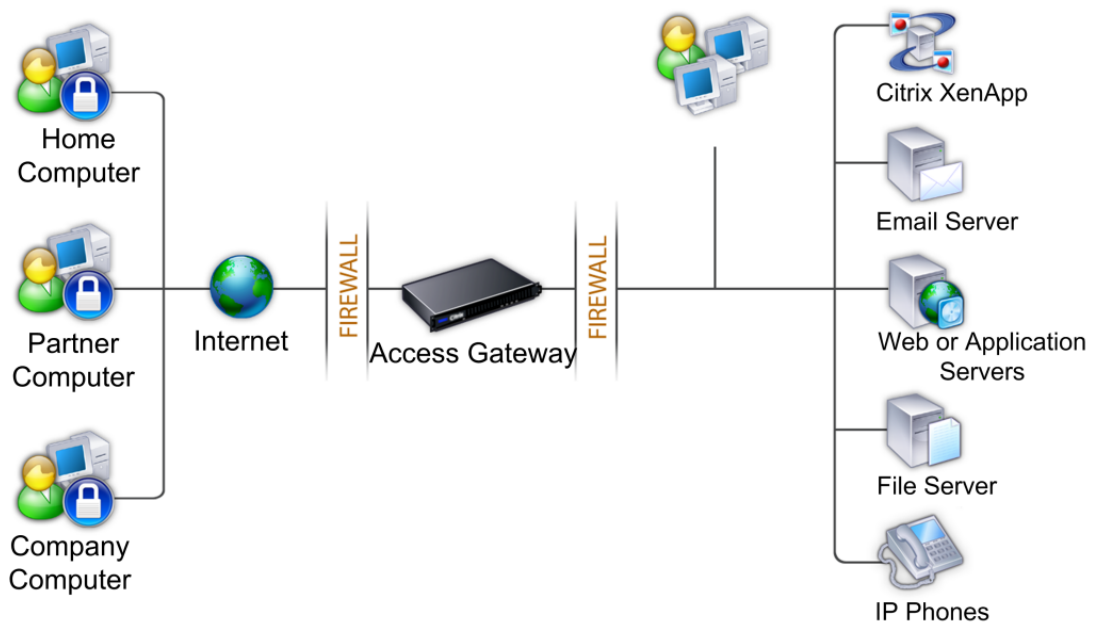
- In the network demilitarized zone (DMZ)
- In a secure network that does not have a DMZ
- With additional Access Gateway appliances to support load balancing and failover

---

# Deploying Access Gateway Appliances in the DMZ

Many organizations protect their internal network with a DMZ. A DMZ is a subnet that lies between an organization's secure internal network and the Internet (or any external network). When the Access Gateway is deployed in the DMZ, users access it using Citrix Access Gateway Plug-in or Citrix XenApp online plug-ins (the new name for Citrix Presentation Server Clients).

Figure 1. Access Gateway deployed in the DMZ



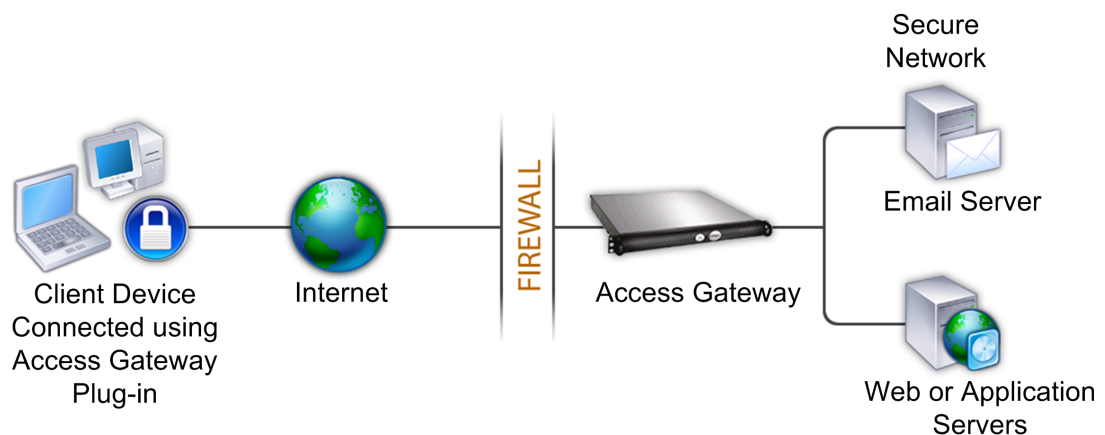
In this configuration, you install the Access Gateway in the DMZ and configure it to connect to both the Internet and the internal network.

---

# Deploying Access Gateway Appliances in the Secure Network

You can install the Access Gateway in the secure network. In this scenario, there is typically one firewall between the Internet and the secure network. The Access Gateway resides inside the firewall to control access to the network resources.

Figure 1. Access Gateway deployed in the secure network



When the Access Gateway is deployed in the secure network, connect one interface on the Access Gateway to the Internet and the other interface to servers running in the secure network. Putting the Access Gateway in the secure network provides access for local and remote users; however, it is a less secure method for users connecting from a remote location because there is only one firewall. While the Access Gateway intercepts traffic from the Internet, this traffic is let into the secure network before authenticating users. When the Access Gateway is deployed in a DMZ, users are authenticated before network traffic reaches the secure network.

When an Access Gateway is deployed in the secure network, Access Gateway Plug-in connections must traverse the firewall to connect to the Access Gateway. By default, client connections use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall.

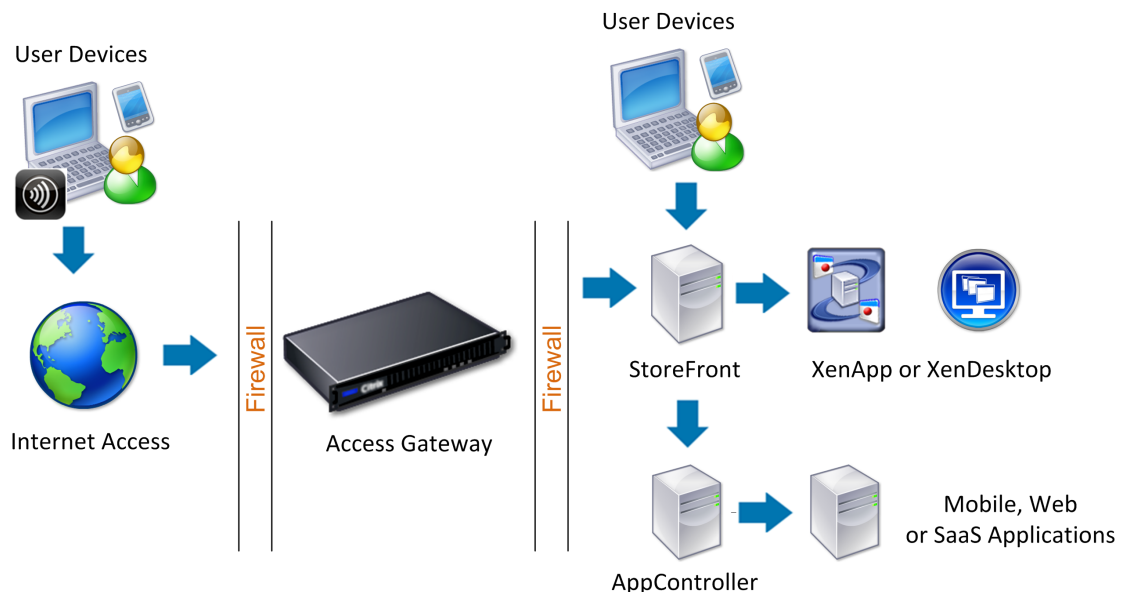
# Deploying Access Gateway with CloudGateway

You can have users connect to Windows, Web, and SaaS applications and virtual desktops hosted in your network. You can provide access to your applications and desktops for remote and internal users by using Access Gateway and CloudGateway. Access Gateway authenticates users and then allows them to access their applications by using Citrix Receiver.

CloudGateway Express contains Receiver and StoreFront which allows user access to Windows-based applications published in XenApp and virtual desktops published in XenDesktop.

CloudGateway Enterprise contains AppController, which allows users to connect to Web, SaaS and mobile applications. AppController allows you to manage Web, SaaS, and mobile applications for single sign-on, along with ShareFile documents. You install AppController in the internal network. Remote users connect directly to AppController through Access Gateway to access their applications and ShareFile data. Remote users can connect with either the Access Gateway Plug-in or Receiver to access applications and ShareFile. Users who are in the internal network can connect directly to AppController by using Receiver. The following figure shows Access Gateway deployed with CloudGateway components.

Figure 1. Access Gateway and CloudGateway Deployment



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

---

# Deploying Access Gateway with the Web Interface

When you deploy Access Gateway to provide secure remote access to XenApp or XenDesktop, Access 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.

This section covers the basic aspects of deploying Access Gateway with a server farm.

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

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

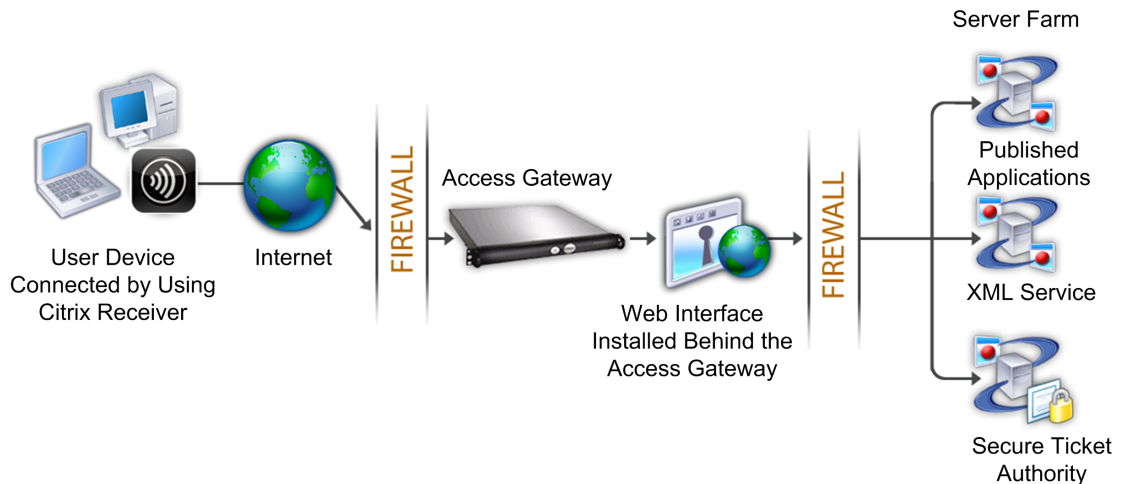
**Note:** You can also configure a double-hop DMZ with the second Access Gateway appliance in the secure network.

## Deploying Access Gateway in the DMZ with a Server Farm

Deploying Access Gateway in the DMZ is the most common configuration when Access Gateway operates with a server farm.

In this configuration, Access Gateway provides a secure single point-of-access for the Web browsers and Citrix online plug-ins that access the published resources through the Web Interface.

Figure 1. Access Gateway and Web Interface deployed in the DMZ



When you deploy Access 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 Access Gateway in the DMZ. In this configuration, both Access Gateway and the Web Interface are deployed in the DMZ. The initial user connection goes to Access Gateway and is then redirected to the Web Interface.
- Deploy Access Gateway parallel to the Web Interface in the DMZ. In this configuration, both Access Gateway and the Web Interface are deployed in the DMZ, but the initial user connection goes to the Web Interface instead of Access Gateway.
- Deploy Access Gateway in the DMZ and deploy the Web Interface in the internal network. In this configuration, Access Gateway authenticates user requests before relaying them 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 Access Gateway to the server farm.

---

# Deployment Options for the Web Interface

When deploying Access Gateway with the Web Interface, you can install the Web Interface in the demilitarized zone (DMZ) or in the secure network. The location in which you deploy the Web Interface depends on a number of factors, including:

- Authentication. When users log on, either Access 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 Access Gateway Plug-in or Citrix online plug-ins. You can limit the resources users can access by using online plug-ins only, or give users greater network access with the Access 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.

The Web Interface deployment options are:

- Web Interface in the secure network
- Web Interface parallel to Access Gateway in the DMZ
- Web Interface behind Access Gateway in the DMZ

The topics in this section discuss these options.

---

# Deploying the Web Interface in the Secure Network

In this deployment, the Web Interface resides in the trusted network. The Access Gateway is in the DMZ. User requests are authenticated by the Access Gateway before being sent to the Web Interface.

When the Web Interface is deployed in the secure network, authentication must be configured on the Access Gateway. Users connect to the Access Gateway, type their credentials, and then are connected to the Web Interface.

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

**Important:** When the Web Interface is in the secure network, authentication should be enabled on the Access Gateway. When authentication is disabled, unauthenticated HTTP requests are sent directly to the server running the Web Interface. Disabling authentication on the Access Gateway is recommended only when the Web Interface is in the DMZ and users are connecting directly to the Web Interface.



---

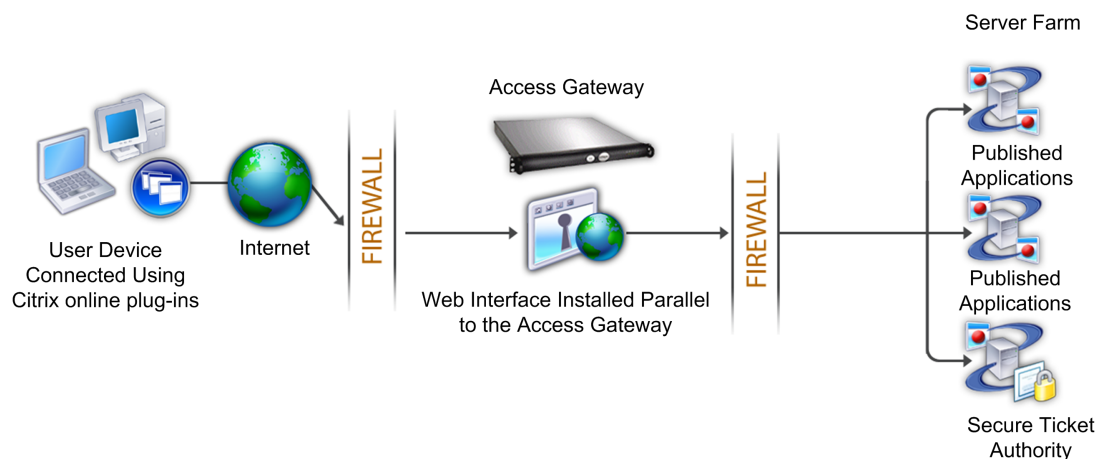
# Deploying the Web Interface Parallel to the Access Gateway in the DMZ

In this deployment, the Web Interface and Access Gateway both reside in the DMZ. Users connect directly to the Web Interface using a Web browser. After users log on to the Web Interface, they can access published applications or desktops in the server farm. When users start an application or desktop, the Web Interface sends an ICA file containing instructions for routing ICA traffic through the Access Gateway as if it were a server running the Secure Gateway. The ICA file delivered by the Web Interface includes a session ticket produced by the Secure Ticket Authority.

When XenApp Plug-ins connect to the Access Gateway, the ticket is presented. The Access Gateway contacts the STA to validate the session ticket. If the ticket is still valid, the user's ICA traffic is relayed to the server in the server farm.

When the Web Interface runs parallel to the Access Gateway in the DMZ, authentication on the Access Gateway does not need to be configured.

Figure 1. The Web Interface installed parallel to the Access Gateway



Client connections are first sent to the Web Interface for authentication. After authentication, the connections are routed through the Access Gateway.

---

# Deploying the Web Interface Behind the Access Gateway in the DMZ

To route all HTTPS and ICA traffic through a single external port and require the use of a single SSL certificate, the Access Gateway can act as a reverse Web proxy for the Web Interface.

When the Web Interface is deployed behind the Access Gateway in the DMZ, authentication on the appliance can be configured but is not required.

---

# Deploying Plug-ins for User Access

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

## Deploying the Access Gateway Plug-in with Citrix Receiver Updater

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

## Deploying the Access Gateway Plug-in by Using the MSI Installer Package

You can deploy the Access Gateway Plug-in by using a Microsoft Active Directory infrastructure or a standard third-party MSI deployment tool, such as Windows Server Update Services. If you use a tool that supports Windows Installer packages, you can deploy the packages with any tool that supports MSI files. Then, use your deployment tool to deploy and install the software on the appropriate user devices.

Advantages of using a centralized deployment tool include:

- Ability to adhere to security requirements. For example, you can install user software without enabling software installation privileges for non-administrative users.
- Control over software versions. You can deploy an updated version of the software to all users simultaneously.
- Scalability. A centralized deployment strategy easily scales to support additional users.
- Positive user experience. You can deploy, test, and troubleshoot installation-related issues without involving users in this process.

Citrix recommends this option when administrative control over the installation of user software is preferred and access to user devices is readily available.

For more information, see [Deploying the Access Gateway Plug-in from Active Directory](#).

## Determining Which Software Plug-in to Deploy

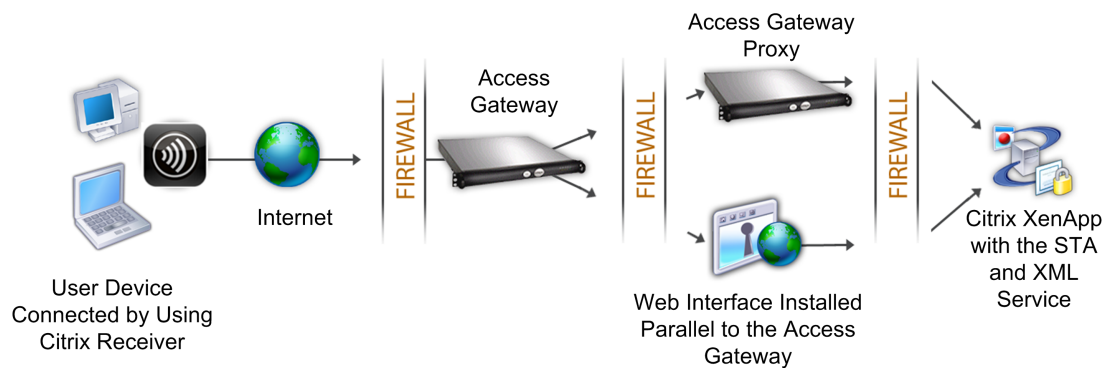
If your Access Gateway deployment does not require any software plug-in on user devices, your deployment is considered to provide clientless access. In this scenario, users need only a Web browser to access network resources. However, certain features require the plug-in software on the user's device.

---

# Deploying Access Gateway in a Double-Hop DMZ

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. Access Gateway appliances deployed in a double-hop DMZ



**Note:** For illustration purposes, the preceding example describes a double-hop configuration using three firewalls, 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.

---

# Installing Access Gateway 10

When you receive your Citrix Access Gateway appliance, you unpack the appliance and prepare the site and rack. After you determine that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you install the hardware. After you mount the appliance, you connect it to the network, to a power source, and to the console terminal that you use for initial configuration. After you turn on the appliance, you perform the initial configuration, and assign management and network IP addresses. Be sure to observe the cautions and warnings listed with the installation instructions.

Citrix recommends using the [Access Gateway 10 Pre-Installation Checklist](#) so you can make a note of your settings before installing the Access Gateway appliance. The checklist also contains information about installing Access Gateway. For more installation instructions, see [Installing the Access Gateway Appliance](#).

---

# Configuring Settings Using the Configuration Utility

The configuration utility allows you to configure most of the Access Gateway settings. You log on to the configuration utility using a Web browser.

## Related Information

## To log on to the configuration utility

1. In a Web browser, type the system IP address of the Access Gateway, such as `http://192.168.100.1`.

**Note:** The Access Gateway is preconfigured with a default IP address of `192.168.100.1` and subnet mask of `255.255.0.0`.

2. In User Name and Password, type `nsroot`.
3. In Start in, select Configuration, and then click Login.

When you start the configuration utility, you are given the option of starting it one of two ways. The Applet Client is a Java-based client that allows you to start the configuration utility in a Web browser. The Web Start Client allows you to download Java components and start future connections to the configuration utility without typing the system IP address. Both clients require Java Runtime Environment (JRE) Version 1.4.x or later.

The configuration utility has navigation and detail panes that you can use to configure the Access Gateway. The left pane, called the *navigation pane*, contains the nodes that are used to configure settings on the Access Gateway. Depending on the node that you select in the navigation pane, the details pane displays the information for the node. After you log on, you can run the Setup Wizard to configure the initial settings on the Access Gateway.

## Related Information

[Configuring Initial Settings Using the Setup Wizard](#)

[Configuring Settings Using the Access Gateway Wizard](#)

---

# Configuring Settings with the Access Gateway Policy Manager

The Access Gateway Policy Manager allows you to configure all of your policies in one place.

The Access Gateway Policy Manager has two columns. The left pane shows the levels to which policies are bound. The details pane shows the policies that can be configured. To bind a policy, you can simply drag and drop the policy from Available Policies / Resources to the level to which you want it bound under Configured Policies / Resources.

The exception to this are servers running the Secure Ticket Authority. These are configured at the Access Gateway Global or virtual server level in the left pane under Configured Policies / Resources.

To create or modify a policy, such as a session policy, click on the node under Available Policies / Resources and then under Related Tasks, select the action you want to perform. In Related Tasks, you can create, modify, show bindings or remove policies.

You can start the Access Gateway Policy Manager in the configuration utility.

## To start the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.



---

# Configuring the Access Gateway Using Wizards

The Access Gateway has three wizards to configure settings on the appliance. These include:

- The Setup Wizard
- The Access Gateway wizard
- The Published Applications Wizard

## How the Setup Wizard Works

The Setup Wizard is used to configure the initial settings on the appliance. The Setup Wizard configures the following settings:

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

**Note:** Before running the Setup Wizard, download your licenses from the Citrix Web site. For more information, see [Installing Licenses on the Access Gateway](#).

## How the Access Gateway Wizard Works

The Access Gateway wizard is used to configure the following settings on the appliance:

- Virtual servers
- Certificates
- Name service providers
- Authentication
- Authorization
- Port redirection

- Clientless access
- Clientless access for SharePoint

## How the Published Applications Wizard Works

The Published Applications Wizard allows you to configure the Access Gateway to connect to servers running Citrix XenApp or Citrix XenDesktop in the internal network. With the Published Applications Wizard, you can:

- Select a virtual server for connections to the server farm
- Configure the settings for client connections for the Web Interface, single sign-on, and the Secure Ticket Authority
- Create or select session policies for SmartAccess

Within the wizard, you can also create session policy expressions for user connections. For more information about configuring the Access Gateway to connect to a server farm, see [Integrating Access Gateway Enterprise Edition with Citrix XenApp and Citrix XenDesktop](#).

---

# Configuring Access Gateway Settings with the Remote Access Wizard

After you install Access Gateway in your network and configure the initial settings, you can configure settings to allow communication with Citrix CloudGateway. When you complete the Remote Access wizard, Access Gateway can communicate with AppController or StoreFront and users can access their Windows-based applications and virtual desktops. If you deploy AppController 1.1, user connections must route through StoreFront. If you deploy AppController Version 2.0 or 2.5, users can connect directly to AppController.

When you run the Remote Access wizard, you configure a virtual server to allow connections through Access Gateway to AppController or StoreFront.

When you run the Remote Access wizard, you can configure the following settings:

- Virtual server name, IP address, and port
- Mapped IP address and subnet mask
- Redirection from an unsecure to a secure port
- LDAP server
- RADIUS server
- Certificates
- DNS server
- CloudGateway and Web Interface

When you configure CloudGateway or Web Interface, the wizard creates the correct policies for communication between Access Gateway, AppController, StoreFront, or the Web Interface. This includes, authentication, session, and clientless access policies. When the wizard completes, you can bind the policies to the virtual server.

You can run the Remote Access wizard before configuring any other settings or running any other wizards, including virtual servers, by using the configuration utility. You can also use the Remote Access wizard to create additional virtual servers and settings.

The Remote Access wizard uses LDAP authentication as the primary authentication type. If you use double-source authentication, you can configure RADIUS as the secondary authentication type.

**Note:** If you used the Setup Wizard or the configuration utility to configure a mapped IP address, you cannot configure the mapped IP address in the Remote Access wizard. The option does not appear.

You can install a signed server certificate and private key by using the Remote Access wizard. You must upload the certificate and private key. You can also use a test certificate

that is already installed on the appliance. If you use a test certificate, you must add the fully qualified domain name (FQDN) that is in the certificate.

There are two ways that you can open the Remote Access wizard:

- The Home tab, if the appliance is licensed for Access Gateway only. If you install a license that enables NetScaler features, the Home tab does not appear.
- The link Create/Monitor Access Gateway in the Access Gateway details pane.

## To configure settings with the Remote Access wizard

1. In the configuration utility, click Access Gateway.
2. In the details pane, under Getting Started, click Create/Monitor Access Gateway.
3. In the dashboard, click Create New Access Gateway.
4. Under Server Info, configure the following:
  - a. In Name, type a name for the virtual server.
  - b. In IP address, type the IP address for the virtual server.
  - c. In Port, type the port number.
  - d. Select Redirect requests from port 80 to secure port to allow users connections on port 443.
  - e. In Mapped IP address, enter the mapped IP address of Access Gateway.
  - f. In Netmask, enter the subnet mask.
5. Under LDAP, configure the settings for your LDAP server.

For more information, see [Configuring LDAP Authentication](#).

6. Select RADIUS (secondary) and then configure the settings for your RADIUS server.

Only select this check box if you use double-source authentication in your deployment. For more information about RADIUS, see [Configuring RADIUS Authentication](#).

7. If you have a signed certificate, under Certificate, do one of the following: .
  - a. To install a signed server certificate, click Install certificate, click Browse and then browse to the certificate on your computer. In Choose key, click Browse and then navigate to the private key.
  - b. To use a test certificate, click Use Test Certificate. In Certificate File Name type the name of the certificate and then in FQDN, type the FQDN from the certificate.
8. Click DNS, in IP address, type the IP address of the DNS server.

To use an IPv6 address, click IPv6 and then enter the IP address.

When you finish configuring the network settings, you can then configure CloudGateway or Web Interface settings.

### To configure CloudGateway settings

You can configure remote access to StoreFront and AppController by using the Remote Access wizard. Access Gateway supports user access to Web, SaaS, and mobile apps and ShareFile only through AppController. If you also deploy StoreFront, users have additional access to Windows-based apps and virtual desktops.

1. In the Remote Access wizard, click CloudGateway/Web Interface.
2. Click the CloudGateway tab and configure the following:
  - a. In StoreFront FQDN, enter FQDN of the StoreFront server. For secure connections, click Use HTTPS.
  - b. In AppController FQDN, enter the FQDN of the AppController virtual machine.
  - c. In Receiver for Web Path, leave the default path or enter your own path.
  - d. In PNAgent Path, leave the default path or enter your own path.
  - e. In Single Sign-on Domain, enter the domain for AppController and StoreFront.
  - f. In Secure Ticket Authority, enter the IP address or FQDN of the server running the Secure Ticket Authority (STA) if you deploy StoreFront and provide access to published applications from XenApp or virtual desktops from XenDesktop.
  - g. In Account Services Address, enter the StoreFront URL. For example, enter `https://storefront.t.com/Citrix/StoreWeb`. This setting allows users to enter their email address rather than a server URL during initial Receiver installation and configuration. Receiver determines the Access Gateway or StoreFront server associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications, desktops, and data. For more about configuring email-based discovery, see [Connecting to StoreFront by Using Email-Based Discovery](#).
3. Click Done.

### To configure Web Interface settings

1. In the Remote Access wizard, click CloudGateway/Web Interface.
2. Click Web Interface and then configure the following:
  - a. In Web Interface Address, type the IP address or FQDN of the Web Interface.
  - b. In Single Sign-on Domain, enter the domain of the Web Interface.
  - c. In Secure Ticket Authority, enter the IP address or FQDN of the server running the STA.
3. Click Done.

---

# Configuring Settings Using the Access Gateway Wizard

After running the Setup Wizard, run the Access Gateway wizard to configure additional settings on the Access Gateway. The Access Gateway wizard is run from the configuration utility.

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

The Access Gateway comes with a test certificate. If you do not have a signed certificate from a Certificate Authority, you can use the test certificate when using the Access Gateway wizard. When you receive the signed certificate, you can remove the test certificate and install the signed certificate. Citrix recommends obtaining the signed certificate before making the Access Gateway publicly available for users.

**Note:** You can create a Certificate Signing Request (CSR) from within the Access Gateway wizard. If you create the CSR using the Access Gateway wizard, you must exit from the wizard and then start it again when the signed certificate is received from the Certificate Authority (CA). For more information about certificates, see [Installing and Managing Certificates](#).

You can configure client connections for Internet Protocol version 6 (IPv6) in the Access Gateway wizard when you configure a virtual server. For more information about using IPv6 for client connections, see [Configuring IPv6 for Client Connections](#).

---

# Configuring the Host Name

The host name is the name of the Access Gateway that is associated with the license file. The host name is unique to the Access Gateway and is used when you download the universal license. The host name is defined when you run the Setup Wizard to configure the Access Gateway for the first time.

## Defining the Fully-Qualified Domain Name

The fully-qualified domain name (FQDN) is included in the signed certificate that is bound to a virtual server. This address can be the same as the appliance host name. One appliance can have a unique FQDN assigned to each virtual server that is configured on the Access Gateway. The FQDN is not configured on the Access Gateway.

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

### To view the FQDN of a certificate

1. In the configuration utility, in the navigation pane, expand SSL and click Certificates.
2. In the details pane, select a certificate and click Details.
3. In the Certificate Details dialog box, click Subject. The FQDN of the certificate appears in the lower pane.

---

# Configuring IP Addresses on the Access Gateway

You can configure IP addresses to log on to the configuration utility and for user connections.

The Access Gateway is configured with a default IP address of 192.168.100.1 and subnet mask of 255.255.0.0 for management access. The default IP address is used whenever a user-configured value for the system's IP address is absent.

- **System IP address.** The management IP address for the Access Gateway that is used for all management-related access to the appliance.
- **Mapped IP address.** Used by the Access Gateway to represent the user device when communicating with servers in the secure network.
- **Default gateway.** The router that forwards traffic from outside the secure network to the Access Gateway.
- **Subnet IP address.** Represents the user device by communicating with a server on a secondary network. This is similar to the mapped IP address.

The system IP address, the mapped IP address, and default gateway are configured using the Setup Wizard.

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

## How the Access Gateway Uses IP Addresses

The Access Gateway sources traffic from IP addresses based on the function that is occurring. As a general guideline, the Access Gateway sources from the following:

- Authentication uses the system IP address
- File transfers from the home page use the system IP address
- DNS and WINS queries use either the mapped IP address or subnet IP address
- Network traffic to resources in the secure network use the mapped IP address, the subnet IP address, or IP pooling that depends on the configuration on the Access Gateway
- ICA proxy setting uses the mapped IP address or subnet IP address



---

# Changing Mapped IP Addresses

A mapped IP address cannot be changed. If one mapped IP address is configured on the appliance, it cannot be changed or deleted. If a second mapped IP address is configured, the first mapped IP address can be deleted.

Additional mapped IP addresses can be configured using either the Setup Wizard or the Network node in the configuration utility.

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

---

# Configuring Subnet IP Addresses

This IP address allows the user to access an Access Gateway from an external host that resides on another subnet. When a subnet IP address is added, 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 the Access Gateway.

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

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

---

# Configuring IPv6 for Client Connections

You can configure the Access Gateway to listen for client connections using IPv6. When you configure one of the following, you can select the IPv6 check box and then enter the IPv6 address in the dialog box.

- Global Authentication - Radius
- Global Authentication - LDAP
- Global Authentication - TACACS
- Global Authentication - NT4
- Access Gateway Virtual Servers
- Create Authentication Server - Radius
- Create Authentication Server - LDAP
- Create Authentication Server - TACACS
- Create Authentication Server- NT4
- Create Auditing Server
- High Availability Setup
- Bind / Unbind Route Monitors for High Availability
- Virtual server (Load Balancing)

When the Access Gateway virtual server is configured to listen on an IPv6 address, users can connect using Citrix online plug-ins.

**Important:** User connections using the Access Gateway Plug-in are not supported with IPv6.

When you configure IPv6 for user connections and if there is a mapped IP address using IPv6, XenApp and Web Interface servers can also use IPv6. The Web Interface must be installed behind the Access Gateway. When users connect through the Access Gateway, the IPv6 address is translated to IPv4. When the connection returns the IPv4 address is translated to IPv6.

You can configure IPv6 for a virtual server when you run the Access Gateway wizard. In the Access Gateway wizard on the Virtual Servers page, click IPv6 and enter the IP address. An IPv6 address for a virtual server can only be configured using the Access Gateway wizard.

To configure IPv6 for authentication, auditing, and high availability, select the IPv6 check box in the dialog box and then type the IP address.

---

# Configuring Routing on the Access Gateway

To provide access to internal network resources, the Access Gateway must be capable of routing data to the internal networks. By default, the Access Gateway uses a static route.

The networks to which the Access Gateway can route data are determined by the configuration of the Access Gateway routing table and the Default Gateway specified for the Access Gateway.

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

The Access 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, a static route might need to be added from the Access Gateway to the new destination if you do not use dynamic routing.

### To configure a static route

1. In the configuration utility, in the navigation pane, expand Network and click Routes.
2. In the details pane, on the Basic tab, click Add.
3. Configure the settings for the route and 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 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, repeat the procedure to add a static route.

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

---

# Testing Your Access Gateway Configuration

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

To test your Access Gateway, create a local user account. Then, using either the virtual server IP address or 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`.

## To create a local user account

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Users.
4. Under Related Tasks, click Create new user.
5. In User Name, type the user name.
6. If using local authentication, clear the External Authentication check box.
7. In Password and Confirm Password, type the password for the user, click Create, and then click Close.

If you receive a certificate warning, either a test certificate or an invalid certificate is installed on the Access Gateway. If a certificate signed by a CA is installed on the appliance, make sure 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 using the signed CSR, and that the distinguished name data entered in the CSR is accurate. The problem may also be a host name to IP address mismatch with 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 all steps were performed correctly and that all parameters were entered accurately.

At the logon screen, enter the user name and password of the user account you created earlier. You are prompted to install the Access Gateway Plug-in.

## Testing Your Access Gateway Configuration

---

When the Access Gateway Plug-in is installed and connected, the Access Interface, which is the default home page, appears.

---

# Configuring Name Service Providers

Name service providers are used to convert Web addresses to IP addresses. You can configure a domain name server (DNS) or a Windows Internet Naming Service (WINS) server on the Access Gateway.

When you run the Access Gateway wizard, you can configure either a DNS server or a WINS server. If you need to configure additional DNS or WINS servers, you can do so using the configuration utility.

## To add a DNS name server to the Access Gateway

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

## To add a WINS name server to the Access Gateway

You can also add additional WINS name servers to the Access Gateway.

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

Next, specify the DNS virtual server name and IP address. Like the Access 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 all internal addresses are resolved properly by clients. The DNS port must also be specified. For more information, see [Configuring DNS Virtual Servers](#)

If you configure a DNS server and WINS server for name resolution, you can select which server performs name resolution first using the Access Gateway wizard.



## To specify name lookup priority

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

---

# Configuring Auto Negotiation

By default, the appliance is configured to use auto negotiation, which sets the direction for transmitted data. This is either half-duplex or full-duplex. For first time installation, configure the Access Gateway to use auto negotiation for those ports connected to the appliance. After initial logon and configuration, auto negotiation can be disabled. Auto negotiation cannot be configured globally. It must be enabled or disabled for each interface.

## To enable or disable auto negotiation

1. In the configuration utility, in the navigation pane, expand Network and click Interfaces.
2. In the details pane, select the interface and click Open.
3. Do one of the following:

To enable auto negotiation, click Yes and click OK. When this is enabled, the Access Gateway uses full duplex.

To disable auto negotiation, click No and click OK. When this setting is disabled, the Access Gateway uses half-duplex.

---

# Upgrading the Access Gateway

The software that resides on the Access Gateway can be upgraded when new releases are made available. You can check for updates on the Citrix Web site at My Citrix. You can upgrade to a new release only if your Access Gateway licenses are under the Subscription Advantage program when the update is released. Subscription Advantage can be renewed at any time. For more information, see the Citrix Support Web site at <http://support.citrix.com>.

## To check for software updates

1. Go to the Citrix Web site at <http://www.citrix.com>, click My Citrix, and log on.
2. At the top of the Web page, click Downloads and in Search Downloads by Product, select Citrix Access Gateway.
3. In Select Product Version, select the Access Gateway version to start the download.
4. Follow the instructions on the screen.

When the software is downloaded to your computer, you can install the software using the Upgrade Wizard in the configuration utility or a command prompt.

## To upgrade the Access Gateway using the Upgrade Wizard

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

## To upgrade the Access Gateway using a command prompt

1. To upload the software to the Access 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 an SSH client, such as PuTTY, to open an SSH connection to the appliance.
4. Log on to the Access 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 the Access Gateway.

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

---

# Installing Licenses on the Access Gateway

Before an Access Gateway appliance can be deployed to support user connections, the appliance must be properly licensed.

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

Before installing licenses on the Access Gateway, set the host name of the appliance and then restart the Access Gateway. The host name is configured using the Setup Wizard. When you generate the universal license for the Access Gateway, the host name is used in the license.

For more information about Access Gateway license types, see [Access Gateway License Types](#).

---

# Access Gateway License Types

The Access Gateway has two types of licenses, the Platform and Universal License. The platform license is supported on the following Access Gateway versions:

- Access Gateway 4.6, Standard Edition running on the Model 2010
- Access Gateway VPX running Access Gateway 4.6.2, Standard Edition
- Access Gateway 9.2, Enterprise Edition

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

## What the Platform License is

The platform license allows user connections to XenApp hosted applications or XenDesktop hosted desktops and do not use an Access Gateway Universal license for each connection. If you only want users to connect with online plug-ins or Desktop Receiver to XenApp or XenDesktop, the platform license is all that is required.

The Platform license is delivered electronically with all new Access 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 using the Product Upgrades/Fulfillment toolbox on My Citrix.

## What the Universal License Is

The Access Gateway universal license limits the number of concurrent user sessions to the number of licenses purchased.

The universal license supports the following features:

- Full VPN tunnel
- 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 the Access Gateway from more than one computer occupies a license for each session.

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

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

- Receive the License Authorization Code (LAC) in email.
- Configure the Access Gateway with the host name using the Setup Wizard,
- Allocate the Access Gateway licenses from My Citrix. Use the host name to bind the licenses to the appliance during the allocation process.
- Install the license file on the Access Gateway.

---

# Obtaining Your Platform or Universal License Files

After you install the Access Gateway, you are ready to obtain your license files from Citrix. You connect to My Citrix to access your available licenses and to generate a license file. When the license file is generated, download it to a computer. When the license file is on the computer, you can then upload it to the Access Gateway.

Before going to the Citrix Web site, you need the following information:

- The license code. You can find the code in an email you receive from Citrix or from My Citrix. If you are upgrading from an older version of the Access Gateway, you can continue to use the existing license, if the license was obtained from the Subscription Advantage Management-Renewal-Information system (SAMRI) and the Subscription Advantage date is not expired.
- Your user ID and password for My Citrix. You can register for this password on My Citrix.

**Note:** If you cannot locate either of these items, contact Citrix Customer Service at 1-800-4-CITRIX.

- The host name of the Access Gateway. The entry field for this name on My Citrix is case-sensitive, so make sure that you copy the host name exactly as it is configured on the Access Gateway appliance.
- How many licenses you want to include in the license file. You do not have to download all of the licenses to which you are entitled at once. For example, if your company purchases 100 licenses, you can choose to download 50. At a later date, you can allocate the rest in another license file. Multiple license files can be installed on the Access Gateway.

Before obtaining your licenses, make sure you configure the host name of the appliance using the Setup Wizard and then restart the appliance. When you are ready to install the universal license on the Access Gateway, go to My Citrix to get your license.



## To obtain your platform or universal license file

1. From a Web browser, go to <http://www.citrix.com/> and click on My Citrix.
2. Enter your user name and password. If this is your first time logging on to the site, you are asked for additional background information.

**Note:** If you are an existing customer, proceed with Steps 3 through 11. If you are a new customer, go to Steps 9 through 11 to obtain your licenses.

3. In Choose a Toolbox, click Product Upgrades/Fulfillment.
4. On the Product Upgrades/Fulfillment page, next to Current Tool, select Upgrade Eligible Products.
5. Under Product Fulfillment Selection, in Select the product you have, select Access Gateway/Secure Access Manager.
6. Under Select the product you would like to receive, select one of the following:

- Access Gateway Platform License

**Note:** If you selected the platform license, a screen appears that explains the platform license, eligibility, and appliance software requirements.

- Access Gateway Universal License

**Note:** This option is available only if you have a valid Subscription Advantage or purchased the universal license as a standalone license.

7. Click Submit.

A second Web browser window opens with the selection for the platform or universal license.

8. Under the Access Gateway appliance description, click on one of the serial numbers and click Continue.

The Confirmation page appears. This screen displays an agreement between you and Citrix. Click Accept.

The Fulfillment Request Confirmation page appears showing that your request is registered. When this is complete, you will receive an email containing download links for media, license code and sever (if needed) from the GTL License Administrator.

9. When you receive the license email from Citrix, click the link to allocate the license.

The Citrix Activation System page appears. You need the host name or host ID reference to activate your license.

The host name or host ID is based on the MAC address of Access Gateway VPX or the host ID of the Access Gateway appliance on which you install the license.

10. Click Continue.

The platform or universal license name, license code and quantity appears.

11. In Host name of your citrix license server, enter the MAC address of Access Gateway VPX or the host ID of the appliance, click Allocate and then click Confirm.

When you click Confirm, a screen appears with your licensing information. To download and save the license file, click Download License File and save the file to your computer. You can then install the license on the Access Gateway.

To install the license on Access Gateway Enterprise Edition, see [To install a license on the Access Gateway using the configuration utility](#).

---

# To install a license on the Access Gateway using the configuration utility

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

If you used the Setup Wizard to configure the initial settings on the Access Gateway, the license file is installed when you run the wizard. If you allocated part of your licenses and then at a later date 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 and then click Add.
3. Navigate to the license file, select it, click Select, and then click OK to restart the Access Gateway.

After the Access Gateway restarts, set the number of users that are allowed to connect and verify that the license is correctly installed.

## 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. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In Maximum Number of Users, type the total amount of users and 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 that can log on is equal to or less than 500. Users who attempt to log on over the 500 limit are denied access.

---

# Verifying Installation of the Universal License

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

## To verify installation of the universal license using the configuration utility

1. In a Web browser, type the IP address for the appliance, such as `http://192.168.100.1`.
2. In User Name and Password, type the administrator credentials.
3. 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 Access Gateway. The Maximum Access Gateway Users Allowed field displays the number of concurrent user sessions licensed on the appliance.

## To verify installation of the universal license using the command line

1. Open an SSH connection to the appliance 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 licences.

---

# Installing Licenses on Appliances in a High Availability Pair

Licenses can also be used when your deployment includes a high availability pair. If you are deploying the appliance as part of a high availability pair, both appliances must have the same host name. Only one appliance in the pair can be active. When the host name is configured, install the same license on both Access Gateway appliances. This ensures that if the primary appliance fails, the secondary appliance is fully licensed.

**Note:** The same license can be installed on multiple Access Gateway appliances. In addition, the same license file can be shared by Access Gateway appliances in different locations to facilitate disaster recovery deployments.

---

# Configuration and Management of the Access Gateway

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

- [Configuring High Availability on Access Gateway Enterprise Edition](#)
- [Installing and Managing Certificates](#)
- [Configuring Policies and Profiles on the Access Gateway](#)
- [Configuring Authentication and Authorization](#)
- [Access Gateway Enterprise Edition Client Connection Methods](#)
- [Configuring Connections for the Access Gateway Plug-in](#)
- [Configuring the Access Interface](#)
- [Configuring Endpoint Policies](#)
- [Maintaining the Access Gateway](#)

---

# Creating Additional Virtual Servers

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 can be configured to use certificates, authentication, policies, bookmarks, IP pooling, configuring the Access Gateway in a double-hop DMZ deployment, and configuring the Secure Ticket Authority. Virtual servers contain the connection settings for when users log on to the appliance.

If you ran the Access Gateway wizard, a virtual server is configured during the wizard. You can configure additional virtual servers using either the Access Gateway Policy Manager or the virtual servers node in the navigation pane of the configuration utility. If you use the Access Gateway Policy Manager, you can create a virtual server and then bind a certificate to the virtual server. When the virtual server is created in the configuration utility, you can also bind the following to the virtual server:

- Pre-authentication policies
- Authentication policies
- Auditing policies
- Session policies
- Traffic policies
- Clientless access policies
- Bookmarks
- Intranet applications
- Access Gateway proxy (double-hop configuration)
- IP pooling (also known as *intranet IPs*)

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

You can also configure how users log on to the Access 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

You can add, modify, enable or disable, and remove virtual servers using the Access Gateway Policy Manager or the virtual server node in the navigation pane of the configuration utility.

## To create a virtual server using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. Under Configured Policies / Resources, click Virtual Servers.
4. Under Related Tasks, click Create new virtual server.
5. Configure the settings you want, click Create, and click Close.

## To create a virtual server using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click Add.
3. Configure the settings you want, click Create, and click Close.



---

# Configuring Connection Types on the Virtual Server

You can configure a virtual server that allows ICA connections only to XenDesktop without SmartAccess, endpoint analysis, or network layer tunneling features. When you create and configure a virtual server, you can select if users receive only the ability to establish an ICA connection or if they can log on with the Access Gateway Plug-in and SmartAccess.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click Add.
3. In Name, type a name for the virtual server.
4. In IP Address and Port, type the IP address and port number for the virtual server.
5. Do one of the following:
  - a. To allow ICA connections only, click Basic Mode.
  - b. To allow user logon with the Access Gateway Plug-in and SmartAccess, click SmartAccess Mode.
6. Configure the other settings for the virtual server, and click Create.

---

# Configuring A Listen Policy for Wildcard Virtual Servers

You can configure Access 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 creating 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	This is the IP address of the virtual server. For a wildcard virtual server bound to the VLAN, this is always *.
Type	This is 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 client connections. The port number must be between 0 and 65535. For the wildcard virtual server bound to a VLAN, this 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:  <code>CLIENT.VLAN.ID.EQ (&lt;integer&gt;)</code>  For <integer>, substitute the ID number assigned to the VLAN.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click Add.
3. In Name, type a name for the virtual server.
4. In Protocol, select the protocol.
5. In IP Address, type the IP address for the virtual server.
6. In Port, type the port for the virtual server.

7. On the Advanced tab, in Listen Priority, type the priority for the listen policy.
8. Next to Listen Policy Rule, and click Configure.
9. In the Create Expression dialog box, click Add, configure the expression, click OK, click Create and then click Close.

---

# Configuring High Availability on Access Gateway Enterprise Edition

If you have two Access Gateway appliances, you can deploy them in a configuration where one Access Gateway accepts and manages connections, while a second Access Gateway monitors the first appliance. If the first Access Gateway stops accepting connections for any reason, the second Access Gateway takes over and begins actively accepting connections. This prevents downtime and ensures that the services provided by the Access Gateway remain available, even if one Access Gateway is not working.

You can configure the Access Gateway in a high availability pair to support failover.

---

# How High Availability Works

When the Access Gateway is configured in a high availability pair, the secondary Access Gateway monitors the first appliance by sending periodic messages, also called a *health check*, to determine if the first appliance is accepting connections. If a health check fails, the secondary Access Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. When the determination is made, the secondary Access Gateway takes over for the primary Access Gateway. This is called *failover*.

The following ports are used to exchange high availability-related information between Access 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

## Gathering Information for High Availability

To record your settings for a high availability deployment, see the [Access Gateway Enterprise Edition Pre-Installation Checklist](#). Before configuring a high availability pair, you need the following information:

- Each Access Gateway appliance must be running the same version of the Access Gateway software. You can find the version number in the configuration utility by clicking System in the navigation pane.
- The Access Gateway does not automatically synchronize passwords between two appliances. You can choose to configure each Access 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 Access Gateway must match, with the following exceptions:
  - The primary and secondary Access 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 Access Gateway.
  - In a high availability pair, the Access Gateway ID and associated IP address must point to the other Access Gateway.

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

**Note:** Each Access Gateway appliance always refers to itself 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 the Access Gateway](#).
- Any configuration file that you create or copy onto either Access Gateway using a method other than direct commands (such as SSL certificates or changes to startup scripts) must be created on or copied to both the primary and secondary Access Gateway.

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 exactly the same. If necessary, you can change the mapped IP address at any time by running the Setup Wizard. For more information, see [Configuring Initial Settings Using the Setup Wizard](#).

---

# Configuring Access Gateway Enterprise Edition for High Availability

When configuring two Access Gateway appliances in a high availability pair, first configure the primary appliance and then the secondary appliance.

## Adding a High Availability Node

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

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, click Add.
3. In the High Availability Setup dialog box, in Remote Node IP Address, type the IP address of the second Access Gateway appliance.
4. Leave the default settings.
5. 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.
6. In User Name, type the user name of the remote appliance.
7. In Password, type the password of the remote appliance, click OK and then click Close.

## To configure settings for high availability

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. 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 click OK. IP Address specifies the IP address of the other appliance.

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

---

# Adding an RPC Node

You must configure RPC node passwords on both Access Gateway appliances in a high availability pair. Initially, each Access Gateway is configured with the same RPC node password. To enhance security, change these default RPC node passwords.

**Note:** The Access Gateway administrator password and the RPC node password must be the same. To change the RPC node, use the procedure below.

RPC nodes are internal system entities used for system-to-system communication of configuration and session information. One RPC node exists on each Access Gateway. This node stores the password, which is checked against the one provided by the contacting Access Gateway.

To communicate with other Access Gateway appliances, each appliance requires knowledge of the other appliances, including how to authenticate on the Access Gateway. RPC nodes maintain this information, which includes the IP addresses of the other Access Gateway appliances and the passwords used to authenticate on each.

RPC nodes are configured and changed using the configuration utility.

**Important:** Secure the network connection between the appliances. You can configure security when you configure the RPC node password.

## To create or change an RPC node password and enable a secure connection

1. In the configuration utility, in the navigation pane, expand Network and 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 Access Gateway appliance.
5. Click Secure and click OK.



---

# Configuring the Primary and Secondary Appliances for High Availability

After changing the RPC node password and enabling secure communication, configure the primary and secondary Access Gateway using the configuration utility.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under High Availability Status, click Enabled and then click OK.

---

# Disabling Access Gateway Network Interfaces

When the Access Gateway appliances are deployed in a high availability setup, you must disable all network interfaces except the one connected to the network switch or hub. When a network interface is enabled, and is not connected, the Access Gateway interprets this as a failure and activates a failover event. On the Access Gateway that is going to be the secondary appliance, disable all network interfaces that are not connected or used for network traffic.

After the network interfaces are disabled, you can configure the primary and secondary Access Gateway appliances.

1. In the configuration utility, in the navigation pane, expand Network and click Interfaces.
2. In the details pane, select a network interface and click Disable.
3. Repeat Step 2 for each network interface you want to disable.

When the network interface is disabled, No appears in the Enabled column.

---

# Customizing Your High Availability Deployment

When you configure the Access Gateway as a high availability pair, you can configure the secondary Access Gateway to listen at specific intervals. This is known as *hello intervals* and *dead intervals*.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open. Select the node whose status must be changed.
3. Under Intervals, do one or both of the following:
  - In Hello Interval (msecs), type the value and click OK.
  - In Dead Interval (msecs), type the value and click OK.

---

# Synchronizing Access Gateway Appliances

You can configure the Access Gateway appliances in a high availability pair to synchronize automatically with one another. Automatic synchronization allows you to make changes to one appliance and have those changes propagate automatically to the second appliance.

You can enable and disable synchronization on each Access Gateway appliance in a high availability pair.

## To configure automatic synchronization on the primary appliance

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under HA Synchronization, click Secondary node will fetch the configuration from Primary and click OK.

## To disable a node from synchronizing automatically

You can prevent the secondary Access Gateway from synchronizing its configuration with the primary Access Gateway whenever there is a change on the primary.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under HA Synchronization, click to clear Secondary node will fetch the configuration from Primary and click OK.

## Forcing Synchronization between Appliances

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

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

- The command is executed on a standalone Access Gateway
  - The command is executed on an Access Gateway where high availability is disabled
  - The command is executed on an Access Gateway that has high availability synchronization disabled
1. In the configuration utility, in the navigation pane, expand System and click High Availability.
  2. On the Nodes tab, click Force Synchronization.

---

# Disabling High Availability Propagation

When propagation is disabled on the primary Access Gateway after synchronization is successful, changes to settings on the primary appliance are not propagated to the secondary Access Gateway. However, if synchronization occurs during this period, the configuration changes that were made when propagation was disabled are synchronized with the secondary Access Gateway. This is also true for cases where propagation is disabled when synchronization is in progress.

When you disable propagation on both appliances, it is effective only on the primary Access Gateway. When propagation is enabled again, force the synchronization between the appliances.

When you disable propagation on a primary node after synchronization is successfully completed, commands executed on the primary node are not propagated to the secondary node. However, if synchronization occurs during this period, the configuration-related changes that you made when propagation was disabled are synchronized with the secondary node. This is also true for cases where propagation is disabled while synchronization is in progress.

**Note:** If command propagation is disabled and then enabled, force synchronization between the appliances to make sure the commands are properly synchronized.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under HA propagation, click to clear Primary node will propagate configuration to the Secondary and click OK.

## To verify command propagation in your high availability pair

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Verify that the settings are the same as for the other node in the high availability pair and click OK.

---

# Troubleshooting Command Propagation

The following are reasons for command propagation failure and their solutions.

- Network connectivity is not active. If a command propagation fails, check the network connection between the primary and secondary Access Gateway appliances.
- Missing resources on secondary Access Gateway. If a command execution succeeds on the primary Access Gateway but fails to propagate to the secondary Access Gateway, run the command directly on the secondary Access Gateway to see the error message. The error may have occurred because the resources required by the command are present on the primary Access Gateway and are not available on the secondary Access Gateway. Also, verify that the license files on each appliance match.

For example, verify that all of your SSL certificates are present on each Access Gateway. Verify that any initialization script customization exists on both Access Gateway appliances.

- Authentication failure. If you receive an authentication failure error message, verify the RPC node settings on both appliances.

---

# Forcing the Primary Access Gateway to Stay Primary

In a high availability setup, the primary Access Gateway can be forced to stay primary even after failover.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select a node and click Open.
3. Under High Availability Status, click Stay Primary and click OK.

This setting can be configured only on Access Gateway appliances that are a standalone and the Access Gateway that is the primary in a high availability pair.

On a standalone Access Gateway appliance, this setting must be configured before adding a second Access Gateway to create a high availability pair. When you add the new appliance, the existing Access Gateway stops processing traffic and becomes the secondary Access Gateway in the high availability pair. The new Access Gateway becomes the primary appliance.

This configuration can be cleared only by using the following command:

```
clear configuration full
```

The following commands do not change the Access Gateway configuration:

```
clear configuration basic
```

```
clear configuration extended
```

Setting the Access Gateway as primary is not propagated or synchronized and affects only the Access Gateway on which the setting is configured.



---

# Forcing the Secondary Appliance to Stay Secondary

In a high availability setup, the secondary Access Gateway can be forced to stay secondary, independent of the state of the primary Access Gateway.

For example, in an existing high availability setup, suppose that the primary Access Gateway has to be upgraded and that this process takes a specified amount of time. During the upgrade, the primary Access Gateway could become unavailable, but you do not want the secondary Access Gateway to take over. You want it to remain the secondary Access Gateway, even if it detects a failure in the primary Access Gateway.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
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 click OK.

When the Access Gateway is configured to stay secondary, it remains secondary even if the primary Access Gateway fails. If the status of an Access 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 Access Gateway in the configuration utility on the Nodes tab.

This setting works on both a standalone and a secondary Access Gateway.

When you set the high availability node, it is not propagated or synchronized and affects only the Access Gateway on which the setting is configured.

## To return the Access Gateway to service as an active high availability appliance

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, select the appliance that is going to stay the primary node and click Open.
3. Under High Availability Status, click Enabled and click OK.

# Configuring Fail-Safe Mode

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

High availability fail-safe mode is configured independently on each node.

The following table shows some of the fail-safe cases.

Table 1. Fail-Safe Mode Cases

Node A (Primary) Health State	Node B (Secondary) Health State	Default HA Behavior	Fail-Safe Enabled HA 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 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 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. In the configuration utility, in the navigation pane, expand System and click High Availability.
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 click OK.

---

# Configuring the Virtual MAC Address

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

In a high availability setup, the primary Access 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 Access Gateway MAC address. When a failover occurs, the secondary Access Gateway takes over as the new primary Access 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 the Access Gateway. As a result, some of the external devices retain the old IP to MAC mapping advertised by the old primary Access Gateway. This can cause a site to become unavailable.

To resolve the problem, configure a virtual MAC address on both Access Gateway appliances of a high availability pair. This implies that both the Access Gateway appliances have identical MAC addresses. As a result, when failover occurs, the MAC address of the secondary Access Gateway remains unchanged and ARP tables on the external devices do not need to be updated.

The virtual MAC address is a user-defined address that is shared by the primary and secondary appliances. To create a virtual MAC address, create a virtual router identifier and bind it to an interface. In a high availability setup, the user needs to bind it to the interfaces on both the appliances. When the virtual router identifier is bound to an interface, the system generates a virtual MAC address with the virtual router identifier 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 identifier 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 identifier. You can create 255 virtual router identifiers ranging from 1 to 254.

1. In the configuration utility, in the navigation pane, expand Network and click VMAC.
2. In the details pane, click Add.
3. In Virtual Router ID, type the value.
4. Under Associated Interfaces, in Available Interfaces, select a network interface, click Add, click Create, and click Close.

When the virtual MAC address is created, it appears in the configuration utility. If you selected a network interface, the virtual router identifier is bound to that interface.

## Deleting a Virtual MAC Address

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

1. In the configuration utility, in the navigation pane, expand Network and click VMAC.
2. In the details pane, select an item and click Remove.

## Binding and Unbinding a Virtual MAC Address

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

1. In the configuration utility, in the navigation pane, expand Network and click VMAC.
2. In the details pane, select an item and click Open.
3. Under Configured Interfaces, select a network interface, click Remove, click OK, and then click Close.

---

# Configuring High Availability Pairs over Routed Networks

A typical deployment of high availability is where both the appliances that comprise a high availability pair reside on the same subnet. A high availability deployment can also consist of two Access Gateway appliances with each appliance located in a different network. This information describes a high availability configuration with the Access Gateway appliances on different networks. It also provides some sample configurations, and a list of differences between the high availability configurations within one network and across networks.

You can also configure link redundancy and route monitors, Access Gateway functions that can be helpful in a cross-network high availability configuration, and covers the health check process used by each Access Gateway to ensure that its partner appliance is active.

## How Independent Network Configuration Works

The Access Gateway appliances are connected to different routers, called R3 and R4, on two different networks. The appliances exchange heartbeat packets through these routers. You can expand this configuration to accommodate deployments involving any number of interfaces.

**Note:** To make sure that heartbeat packets are sent and received successfully if static routing is configured, you must add the static routes from each Access Gateway to the other appliance.

When the appliances in a high availability pair reside on two different networks, the secondary Access Gateway must have an independent network configuration. This means that Access Gateway appliances on different networks cannot share mapped IP addresses, virtual LANs, or network routes. This type of configuration, where the Access 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 they must be set on each Access Gateway:

Configurable Parameters	Behavior
IP addresses	Access Gateway specific. Active only on that appliance.
Virtual IP address	Floating.
Virtual LAN	Access Gateway specific. Active only on that appliance.
Routes.	Access Gateway specific. Active only on that appliance. LLB route is floating.
Access Control Lists (ACLs)	Floating (Common). Active on both appliances.

## Configuring High Availability Pairs over Routed Networks

---

Dynamic routing	Access Gateway specific. Active only on that appliance. The secondary Access 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	Access Gateway specific. Reverse network address translation with virtual IP address as network address translation IP address is floating.

---

# Configuring an Independent Network Computing High Availability Pair

When two Access Gateway appliances of a high availability pair reside on different subnets, each Access Gateway must have a different network configuration. For this reason, to configure two independent Access Gateway appliances to function as a high availability pair, you must specify independent network computing mode during the configuration process.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. In the details pane, on the Nodes tab, click Add.
3. In the High Availability Setup dialog box, in the Remote Node IP Address, type the IP address.
4. Click Turn on INC (Independent Network Configuration) mode on self node, click OK and then click Close.

---

# Configuring Route Monitors

When the appliances of a high availability pair reside on different networks, the high availability state of an Access Gateway depends on if it can be reached or not. In a cross-network high availability configuration, a route monitor on each Access Gateway watches the internal routing table to make sure that an entry for the other Access Gateway is always present.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. On the Route Monitors tab, click Configure.
3. Under Specify Route Monitor, in Network, type the IP address of the network of the other Access Gateway appliance.
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 the Access Gateway.

**Note:** When a route monitor is not bound to an Access Gateway, the high availability state of either appliance is determined by the state of the interfaces.

## To remove a route monitor

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. On the Route Monitors tab, click Configure.
3. Under Configured Route Monitors, select the monitor, click Remove, and click OK.



---

# Configuring Link Redundancy

Link redundancy group network interfaces together to prevent failover due to a failure on one network interface of an Access Gateway that has other functioning interfaces. The failure of the first interface on the primary Access Gateway triggers failover, although it can still serve client requests using its second link. When link redundancy is configured, you can group the two interfaces into a failover interface set, preventing the failure of a single link from causing failover to the secondary Access Gateway unless all interfaces on the primary Access Gateway are nonfunctional.

Each interface in a failover interface set maintains independent bridge entries. The enabled and the high availability monitor interfaces on an Access Gateway that are not bound to a failed interface set are known as critical interfaces, because if any of them fails, failover is triggered.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. On the Failover Interface Set tab, click Add.
3. In Name, type a name for the set.
4. Under Available Interfaces, select an interface and click Add.
5. Repeat Step 4 for the second interface, click Create, and then click Close.

You can add as many interfaces as you need for failover between the interfaces. After you configure a failover interface set, you can remove interfaces.

## To remove an interface from the failover interface set

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. On the Failover Interface Set tab, select a set and click Open.
3. In the Configure FIS dialog box, under Configured Interfaces, select the interface(s) you want to remove, click Remove, and then click OK.

## To remove a failover interface set

If the failover interface set is no longer needed, you can remove it from the Access Gateway.

1. In the configuration utility, in the navigation pane, expand System and click High Availability.
2. On the Failover Interface Set tab, select a set and click Remove.



---

# Installing and Managing Certificates

On Access 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. Access 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 a user device, the server sends its certificate to the client.

When receiving a server certificate, the Web browser (for example, Internet Explorer) on the user device 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 this site).

Access 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. Access 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 Access Gateway.

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

---

# Creating a Private Key

Private keys that are generated with the Certificate Signing Request are stored in an encrypted and password-protected format on the Access Gateway. When creating the Certificate Signing Request, you are asked to provide a password for the private key. The password is used to protect the private key from tampering, and it is also required when restoring a saved configuration to the Access Gateway. Passwords are used whether the private key is encrypted or unencrypted.

The private key is required to install a valid certificate issued by the CA. The certificate that you receive from the CA is valid only with the private key used to create the Certificate Signing Request (CSR).

You can also import a password-protected certificate and private key in the PKCS#12 format. This allows encrypted and password-protected private keys and certificates created on the Access Gateway to be imported.

Two types of private keys can be created on the Access Gateway: RSA and DSA.

An RSA private key is the most commonly used private key. It provides strong encryption and security for the Access Gateway. Citrix recommends using an RSA private key on the Access Gateway.

A DSA private key is an older type of private key. It also provides encryption and is paired with the server certificate.

Creating a private key is the starting point for creating secure certificates. You specify the name of the private key and the key bit length. The supported lengths are 512, 1024, and 2048 bits.

For added security, encrypt your private key with Data Encryption Standard (DES) or triple DES (3DES). The DES and 3DES options are valid only for keys stored in PEM format, not for keys stored in DER format.

To create the CSR, you need either an RSA or a DSA private key. When you create a CSR using the Access Gateway wizard, a private key is generated with the CSR. You can also create a private key separately and then pair it with the certificate.

**Note:** Citrix recommends using a password to protect the private key and to use the private key generated by the CSR.

## To create an RSA private key

1. In the configuration utility, in the navigation pane, click SSL.
2. In the details pane, under SSL Keys, click Create RSA Key.
3. In Key Filename, type the name of the private key or click Browse to navigate to an existing file.
4. In Key Size (Bits), type the size of the private key.
5. In Key Format, select PEM or DER. Citrix recommends PEM format for the certificate.
6. In PEM Encoding Algorithm, select DES or DES3.
7. 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 the encoding algorithm must be selected.

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.

---

# Creating a Certificate Signing Request

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

**Important:** When you use the Access 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 Access Gateway wizard again to create the settings and install the certificate. For more information about the Access Gateway wizard, see [Configuring Settings Using the Access Gateway Wizard](#).

## To create a CSR by using the Access Gateway wizard

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Getting Started, click Access Gateway wizard.
3. Follow the directions in the wizard until you come to the Specify a server certificate page.
4. Click Create a Certificate Signing Request and complete the fields.

**Note:** The fully qualified domain name (FQDN) does not need to be the same as the Access Gateway host name. The FQDN is used for user logon.

5. Click Create to save the certificate on your computer and then click Close.
6. Exit the Access 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 Access Gateway wizard.

1. In the configuration utility, in the navigation pane, click SSL.
2. In the details pane, under SSL Certificates, click Create CSR (Certificate Signing Request).
3. Complete the settings for the certificate and then click Create.

## Creating a Certificate Signing Request

---

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

---

# Installing the Signed Certificate on the Access Gateway

When you receive the signed certificate from the CA, pair it with the private key and then install the certificate on the Access Gateway.

1. Copy the certificate to the Access Gateway to the folder `nsconfig/ssl` using an SSH program such as WinSCP.
2. In the configuration utility, in the navigation pane, expand `SSL` and click `Certificates`.
3. In the details pane, click `Add`.
4. In `Certificate-Key Pair Name`, type the name of the certificate.
5. Under `Details`, in `Certificate File Name`, select the drop-down box in `Browse (Appliance)` and select `Appliance`.
6. Navigate to the certificate, click `Select`, and click `Install`.
7. In `Private Key File Name`, select the drop-down box in `Browse (Appliance)` and select `Appliance`. The name of the private key is the same name as the `Certificate Signing Request`. The private key is located on the Access Gateway in the directory `\nsconfig\ssl`.
8. Choose the private key and click `Select`.
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, in `Notifies When Expires`, click `Enable`. In `Notification Period`, type the number of days, click `Install`, and click `Close`.

## Binding the Certificate and Private Key to a Virtual Server

When a certificate and private key pair are created and linked, bind it to a virtual server.

1. In the configuration utility, in the navigation pane, expand `Access Gateway` and click `Virtual Servers`.
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`.



## Unbinding Test Certificates from the Virtual Server

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

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

# Configuring Intermediate Certificates

An *intermediate certificate* is one that goes between the Access 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 that of applying different issuing policies to different sections of the organization.

Responsibility for issuing certificates can be delegated by setting up subordinate CAs. The X.509 standard includes a model for setting up a hierarchy of CAs. In this model, the root CA is at the top of the hierarchy and has a self-signed certificate. 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.

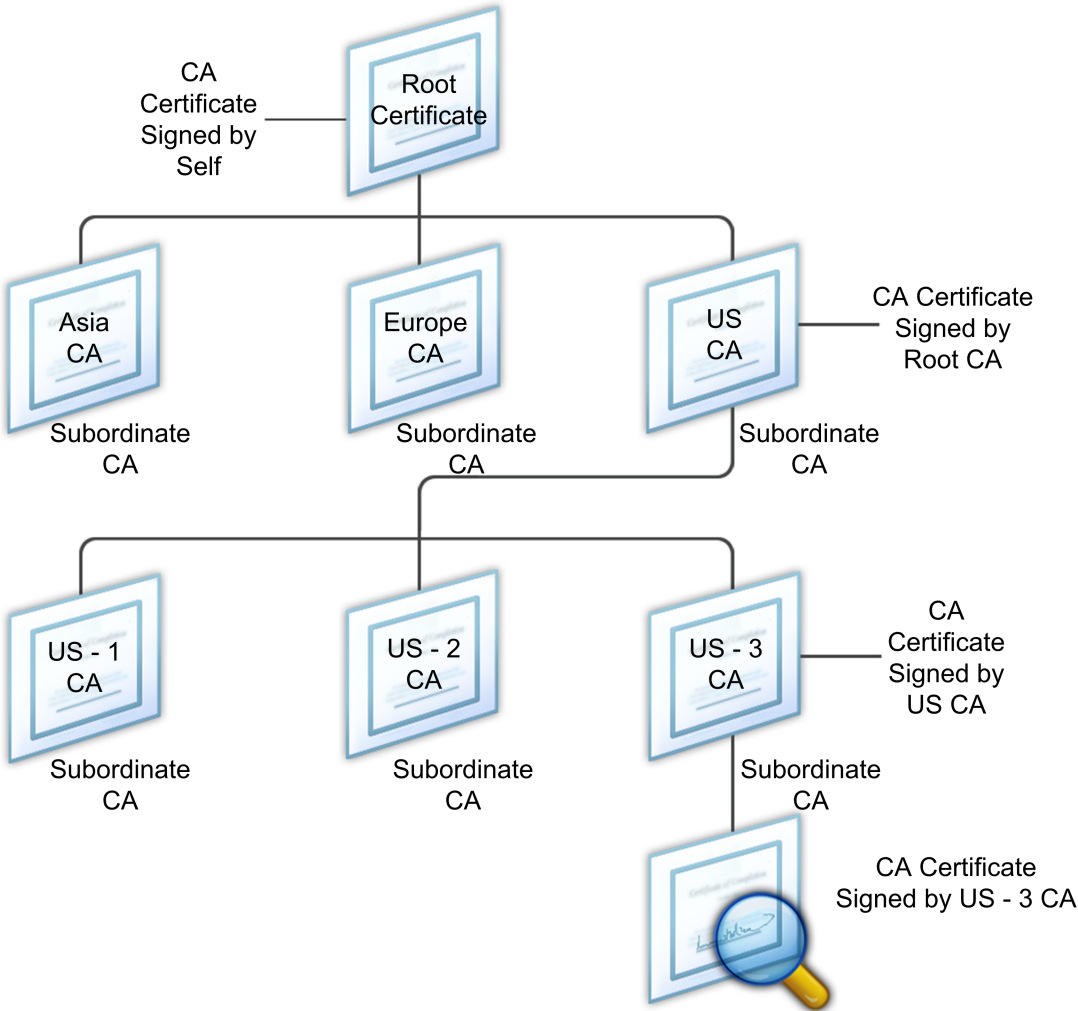


Figure 1. The X.509 model showing the hierarchical structure of a typical digital certificate chain

CAs can sign their own certificates (that is, they are self-signed) or they can be signed by another CA. If the certificate is self-signed, it is called a root CA. If they are not self-signed, they are called *subordinate* or *intermediate* CAs.

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

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



Figure 2. A typical digital certificate chain

## To install an intermediate certificate

1. In the configuration utility, in the navigation pane, expand SSL and click Certificates.
2. In the details pane, click Add.
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 with Local or Appliance.
5. Navigate to the certificate on your computer or on the Access Gateway.
6. In Certificate Format, select PEM.
7. Click Install and click Close.

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

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

## To link an intermediate certificate to a server certificate

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

---

# Importing and Installing an Existing Certificate to Access Gateway

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 Access Gateway. If this occurs, use the Certificate Signing Request (CSR) to create a new certificate. For more information, 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 Access Gateway as a PKCS#12 certificate.

If you are replacing the Secure Gateway with Access 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 Access 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 Access Gateway, and then test the configuration. The Secure Gateway and Access 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 Access 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 Access Gateway.

## To install the certificate and private key on Access Gateway

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

This is the password you used when converting the certificate to PEM format.

7. Click Next to finish the Access Gateway wizard without changing any other settings.

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

---

# Certificate Revocation Lists

From time to time, Certificate Authorities 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.

Access Gateway Enterprise Edition supports two CRL types:

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

When you bind a certificate to a virtual server, you can select which certificate revocation type you want to use.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click a virtual server and click Open.
3. On the Certificates tab, under **Configured**, select a certificate.
4. Under Check, select CRL Mandatory or OSCP Mandatory, and then click OK.

---

# Monitoring Certificate Status with OCSP

Online Certificate Status Protocol (OCSP) is an Internet protocol that is used to determine the status of a client SSL certificate. The Access 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. The Access Gateway implementation of OCSP includes request batching and response caching.

## Access Gateway Implementation of OCSP

OCSP validation on an Access Gateway appliance begins when the appliance receives a client certificate during an SSL handshake. To validate the certificate, the Access Gateway creates an OCSP request and forwards it to the OCSP responder. To do so, the Access 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 the Access Gateway evaluates the response from the server and determines whether to allow the transaction or reject it. If the response from the server is delayed beyond the configured time and no other responders are configured, the Access Gateway allows the transaction or displays an error, depending on whether the OCSP check was set to optional or mandatory. The Access 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 the Access Gateway receives a client certificate, it sends a request to the OCSP responder. To help avoid overloading the OCSP responder, the Access Gateway can query the status of more than one client certificate in the same request. For this to work efficiently, 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 clients and reduces the load on the OCSP responder. Upon receiving the revocation status of a client certificate from the OCSP responder, the Access Gateway caches the response locally for a predefined length of time. When a client certificate is received during an SSL handshake, the Access 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), it is evaluated and the client certificate is accepted or rejected. If a certificate is not found, the Access 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

Configuring 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 an SSL virtual server. If you need to bind a different certificate and private key to an OCSP responder that has already been configured, you need to first unbind the responder and then bind the responder to a different certificate.

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

This field is mandatory. The URL cannot exceed 32 characters.

5. To cache the OSCP responses, click Cache and in Time-out, type the number of minutes the Access Gateway holds the response.
6. In Batching Depth, type the maximum number of client certificates to combine into one OCSP request.

The minimum value is 1 and the maximum value is 255.

7. In Batching Delay, specify the time, in milliseconds, allowed for batching a group of OCSP requests.

The values can be between 0 and 10000. The default is 1.

8. Select Trust Responses if you want to disable signature checks by the OCSP responder.

If you enable Trust Responses, skip Step 9.

9. In Certificate, select the certificate that is used to sign the OCSP responses.

If a certificate is not selected, the Certificate Authority (CA) that the OCSP responder is bound to is used to verify responses.

10. In Produced in Time Skew, type the amount of time the Access Gateway can use to decide when it needs to consider or accept the response.

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 between 0 and 120000. The default is 2000.

12. In Signing Certificate, select the certificate and private key used to sign OCSP requests. If a certificate and private key are not specified, the requests are not signed.

13. Select Nonce if you want to enable the number used once (nonce) extension.
14. Click Create and then click Close.

---

# Configuring Policies and Profiles on the Access Gateway

Policies 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 authentication and authorization policies, see [Configuring Authentication and Authorization](#). For more information about configuring clientless access, see [How Clientless Access Works](#). For more information about configuring endpoint policies, see [Configuring Endpoint Policies](#).

---

# How Policies Work

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

A profile is a collection of settings, using specific parameters. The profile can have any name and it can be reused in more than one policy. There can be multiple settings within the profile, but there is one profile per policy.

Policies, with the configured conditions and profiles, can be bound 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 the Access Gateway with Citrix XenApp, Access Gateway policy names are sent to XenApp as filters. When configuring the Access Gateway to work with XenApp and SmartAccess, the administrator uses the settings in XenApp for Access Gateway Advanced Edition, substituting the following to create the policy:

- The name of the virtual server that is configured on the appliance is sent to XenApp as the Access Gateway farm name
- The names of the pre-authentication or session policies are sent as filter names

For more information about configuring the Access Gateway to work with Citrix XenApp, see [Providing Access to Published Applications](#).

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

---

# Setting the Priorities of Policies

Policies are prioritized and evaluated in the order to which the policy is bound. Policies are evaluated and then run based on this order:

- User (highest priority)
- Group
- Virtual server
- Global (lowest priority)

The priority of policies is determined by two methods:

- The level to which the policy is bound: globally, virtual server, group, or user.
- The numerical priority takes precedence regardless of where 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. The lower the priority number, the higher the precedence is for the policy.

---

# Configuring Conditional Policies

When configuring policies, you can use any Boolean expression to express the condition for when the policy applies. You can use any of the available system expressions, such as client security strings, network information, HTTP headers and cookies, time of day, or client certificate values.

Policies can be created to apply only when the user device meets specific criteria, such as a session policy for SmartAccess.

Policy conditions based on endpoint analysis results cannot be used if the policy rule is configured as part of security settings in a session profile.

Another example of configuring a conditional policy is varying the authentication policy for users. For example, users who are connecting using the Access Gateway Plug-in from outside the internal network, such as from their home computer, can be authenticated using LDAP. Users who are connecting through a wide area network (WAN) can be authenticated using RADIUS.

---

# Configuring System Expressions

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

Expressions on the Access Gateway include:

- General expressions that limit the objects users can use when establishing a connection to the Access Gateway
- Client security expression that defines the software, files, processes, or registry values that must be installed and running on the client device
- Network-based that restricts access based on network settings

Access Gateway Enterprise Edition 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 Access Gateway. Client security expressions are used on the Access 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:

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

---

# Creating Simple and Compound Expressions

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. Compound expressions are created by connecting to one or more expression names using the logical operators && and ||, grouped for order of evaluation using the symbols.

Compound expressions can be categorized as:

- Named expressions
- Inline expressions

Named expressions are independent entities. A named expression can be reused by other policies and are included within the policy. Named expressions are configured at the system level in the configuration utility.

You can use a predefined named expression in the policy or create one of your own.

## To create a named expression

1. In the configuration utility, in the navigation pane, expand AppExpert > Expressions and click Classic 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. In Client Security Message, type the message that users see in the connection log if the user device fails to meet the policy criteria.
5. To create an expression, click Add.
6. Configure the parameters of the expression, click OK, click Create and then click Close.



---

# Adding Custom Expressions

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 using the Access Gateway Plug-in, set a time limit for the session, and allow single sign-on with Windows. After creating 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 the Access Gateway

You can create policies using either the configuration utility or the Access Gateway Policy Manager. After a policy is created, you bind the policy to the appropriate level: user, group, virtual server, or global. When a policy is bound 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.

The Access Gateway Policy Manager provides an easy way to configure multiple policies and then binding the policies quickly to the appropriate level. Using the expandable nodes in the left and right panes, you can configure the policy in the right pane and then simply drag-and-drop the policy to the node in the left pane.

---

# How Session Policies Work

A *session policy* is a collection of expressions and settings that are applied to users, groups, virtual servers, and globally.

A session policy is used for configuring the settings for client connections. You can define settings to configure the software users log on with, such as the Access Gateway Plug-in for Windows or the Access Gateway Plug-in for Java. 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 those 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 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.

## To create a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Complete the settings for the session profile and click Create.
9. 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

A session profile contains the settings for client connections. Profiles are used with session policies. You can create profiles separately from the policy using the configuration utility and then use the profile for multiple policies. Only one profile can be used with a policy.

You can also create a profile using the Access Gateway Policy Manager when configuring a session policy.

Within the session profile, you can configure:

- The DNS servers
- The settings for client connections, which includes the plug-in with which users connect, time-out settings, split tunneling, and single sign-on

Session profiles specify the actions that are applied to a user session if the policy expression conditions are met. You can use session profiles to configure the following network settings:

- DNS server
- WINS server IP address
- Using the mapped IP address as the client IP address
- Intranet IP address (also called *IP pooling*)
- Intranet IP DNS suffix
- HTTP ports
- Forced time-out settings

The following settings are used for when users log on to the appliance:

- Access Interface or customized home page
- Web address for Web-based email, such as Outlook Web Access
- Plug-in type (Access Gateway Plug-in for Windows, Access Gateway Plug-in for Mac OS X, or Access Gateway Plug-in for Java)
- Split tunneling
- Session and idle time-out settings
- Clientless access
- Clientless access URL encoding
- Single sign-on to Web Applications

- Credential index for authentication
- Single sign-on with Windows
- Logon scripts
- Client debug settings
- Split DNS
- Access to private network IP addresses and local LAN access
- Client choices
- Client cleanup behavior
- Proxy settings

For more information about configuring settings for client connections, see [Configuring Connections for the Access Gateway Plug-in](#).

The following are security settings that can be configured using a session profile:

- Default authorization action (allow or deny)
- Quarantine groups
- Authorization groups

For more information about configuring authorization on the Access Gateway, see [Configuring Authorization](#).

The following are settings for connections to servers running Citrix XenApp or XenDesktop:

- ICA proxy, which are client connections using Citrix online plug-ins
- Web Interface address
- Web Interface portal mode
- Single sign-on to the server farm domain

For more information about configuring settings for connecting to published applications in a server farm, see [Providing Access to Published Applications](#).

## To create a session profile

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

When a profile is created, you can include it in a session policy.

### To add a profile to 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 click Open
3. In Request Profile, select a profile from the list.
4. Finish configuring the session policy and exit the dialog box.

---

# Binding Session Policies

After creating the 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, in the navigation pane, click Access Gateway.
  2. In the details pane, under Policy Manager, click Change group settings and user permissions.
  3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Session Policies and click a policy.
  4. Drag the session policy to the user, group, virtual server, or Access Gateway Global session policy under Configured Policies / Resources.



---

# How a Traffic Policy Works

Traffic policies allow you to configure the following for client connections:

- Enforcing shorter time-outs for sensitive applications that are accessed from untrusted networks.
- Switching network traffic to use TCP for some applications. If TCP is selected, you need to enable or disable single sign-on for certain applications.
- Identifying situations where you want to use other HTTP features for Access Gateway Plug-in traffic.
- Defining the file extensions that are used with file type association.

---

# Creating a Traffic Policy

To configure a traffic policy, you create a profile and configure the following parameters:

- Protocol (HTTP or TCP)
- Application time-out
- Single sign-on to Web applications
- Form single sign-on
- File type association
- Repeater Plug-in

When the traffic policy is created, 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 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 creating the policy, use the HTTP parameter for the action. In the expression, create the destination address for the server running the application.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Traffic Policies.
4. Under Related Tasks, click Create new traffic policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. In Protocol, select either HTTP or TCP.

**Note:** If you select TCP as the protocol, single sign-on cannot be configured and is disabled in the profile dialog box.

9. To limit the time users can stay logged on to the Web application, in AppTimeout (minutes), type the number of minutes.

10. 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 the traffic profile. For more information, see [Configuring Form-Based Single Sign-On](#).

11. To specify a file type association, in File Type Association, select ON.

12. To use the Repeater Plug-in to optimize network traffic, in Branch Repeater, select ON.

13. In the Create Traffic Policy dialog box, create or add an expression, click Create and click Close.

---

# Configuring Form-Based Single Sign-On

Form-based single sign-on allows users to log on once to all protected applications in your network, rather than requiring them to log on separately to access each one. Form-based single sign-on allows users to access Web applications that require an HTML form-based logon without having to type their password again.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Traffic.
2. In the details pane, click the Form SSO Profiles tab and 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 using the Prefix, Add, and Boolean 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.

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](#)

---

# Binding a Traffic Policy

Traffic policies can be bound to virtual servers, groups, users, and Access Gateway Global. You can bind a traffic policy using either the Access Gateway Policy Manager or the configuration utility.

## To bind a traffic policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. Under Available Policies / Resources, expand Traffic Policies and click a traffic policy.
4. Drag the policy to Traffic Policies under Configured Policies / Resources for the level to which you want the policy bound.

## To bind a traffic policy globally using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Traffic.
2. In the details pane, select a policy and 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

You can remove traffic policies from the Access Gateway using either the configuration utility or the Access Gateway Policy Manager. If you are using 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 using the Access Gateway Policy Manager.

## To unbind a traffic policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. Under Configured Policies / Resources, expand the node that has the traffic policy bound to it, click Traffic Policies, and then click the traffic policy.
4. Under Related Tasks, click Unbind traffic policy.

After the traffic policy is unbound, you can remove the policy.

## To remove a traffic policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. Under Available Policies / Resources, expand Traffic Policies and select the traffic policy.
4. Under Related Tasks, click Remove traffic policy.

---

# Allowing File Type Association

File type association allows users to open documents in applications published through Citrix XenApp. 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 the virtual server properties on the Access Gateway are correctly configured.

Providing file type association as the only means for editing resource documents can heighten security because it requires that editing occur on the server and not on the client device.

For example, you might choose to grant file type association for a file share where employees post reports of ongoing project meetings, without providing the ability to download or upload.

Providing file type association requires that:

- Users run Citrix online plug-ins on the user device
- Users connect through a virtual server that has a traffic policy bound to it and is configured for XenApp
- Users are assigned to the desired applications in XenApp
- Administrators configure XenApp to work with Access Gateway Enterprise Edition

The steps for creating file type association include:

- Creating a Web Interface site
- Configuring file type association using a traffic policy on the Access Gateway
- Defining file extensions in XenApp

---

# Creating a Web Interface Site

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 the Access Gateway for File Type Association

After creating and configuring the Web Interface, you need to create settings on the Access 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.

## To create a session policy and profile for file type association

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Published Applications tab, configure the following settings:
  - a. Next to Web Interface Address, click Override Global and type the Web address of the Web Interface.
  - b. Next to Web Interface Portal Mode, click Override Global and select either Normal or Compact.
  - c. Next to Single Sign-on Domain, click Override Global and type the name of the domain in which the user accounts reside and click Create.
9. In the Create Session Policy dialog box, next to Named Expression, select True value, click Add Expression, click Create, and click Close.

After creating the session policy and binding 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, create an expression to define the file extensions to be used. 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
```

First, create the traffic profile for file type association. Then, create a traffic policy using the profile and creating the expression. Create both the policy and the profile using the configuration utility.

## To create a traffic profile for file type association

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

After you create the profile, create the policy and add the profile.

## To configure file type association using a traffic policy

1. On the Policies tab, click Add.
2. In Name, type a name for the policy.
3. In Request Profile, select a profile.
4. In the Create Traffic Policy dialog box, under Expressions, select Advanced Free-Form and click Add.
5. In the Add Expression dialog box, do the following:
  - a. In Expression Type, click General.
  - b. In Flow Type, select REQ.
  - c. In Protocol, select HTTP.
  - d. In Qualifier, select URL.
  - e. In Operator, select = =.
  - f. In Value, type `/*.FileExtensionType`, where *.FileExtensionType* is the file type, such as .doc or .xls, and click OK.
6. In the Create Traffic Policy dialog box, under Expressions, next to Advanced Free-Form, click OR.
7. Repeat Steps 4 and 5 for each file extension you want to include, click Create, and click Close.

After creating the policy, bind it to the virtual server.

---

# Configuring Citrix XenApp for File Type Association

For each published application, examine the properties you want to use with file type association. Enable each file extension using the published application's content redirection properties. In the following illustration, Microsoft Word is a published application and all of its file extensions are enabled.

After file extensions are enabled in XenApp, file type association is enabled and functional with Access Gateway. For more information about defining file extensions in XenApp 6, see [To update file type associations](#). For more information about defining file extensions in XenApp 5, see [Configuring Content Redirection](#).

---

# How TCP Compression Policies Work

You can compress TCP data that goes through the Access Gateway using a TCP compression policy. You can enable compression of network traffic that is destined for one port or to a range of ports.

A TCP compression policy is used with the Access Gateway Plug-in. TCP data on the user device is intercepted and the configured policy is applied before the data is sent through the secure tunnel. Network traffic from the internal network, that is sent to the user device, is also compressed.

When network data is compressed, it can increase the performance of TCP-based applications with compressible content.

When a TCP compression policy is configured and bound, it can help with:

- Wide area network (WAN) latency reduction. The number of round trips of the network traffic is reduced due to the reduced number of packets after compression.
- Reduce bandwidth costs. The bandwidth requirements of the site are reduced, resulting in lower expenses.
- Faster transmission. Transmission of compressed data is between the Access Gateway and the user device. The server in the internal network is free from transmitting the data.

The Access Gateway combines compression with the SSL acceleration feature to ensure continuous delivery of secure content without compromising performance. The Access Gateway supports the following compression methods:

- GNU zip (GZIP)
- Deflate
- Compress
- No compression

**Note:** When a TCP compression profile is configured and saved, the parameters cannot be changed. If you want to change the profile for a TCP compression policy, create a new profile and then select it in the policy.

# Creating or Modifying a TCP Compression Policy

You can create a TCP compression policy using either the Access Gateway Policy Manager or the configuration utility. To configure a policy, you create a compression profile that selects the type of compression and then an expression for the policy. For example, you can create a policy using GZIP compression to a destination port, as shown in the following illustration:

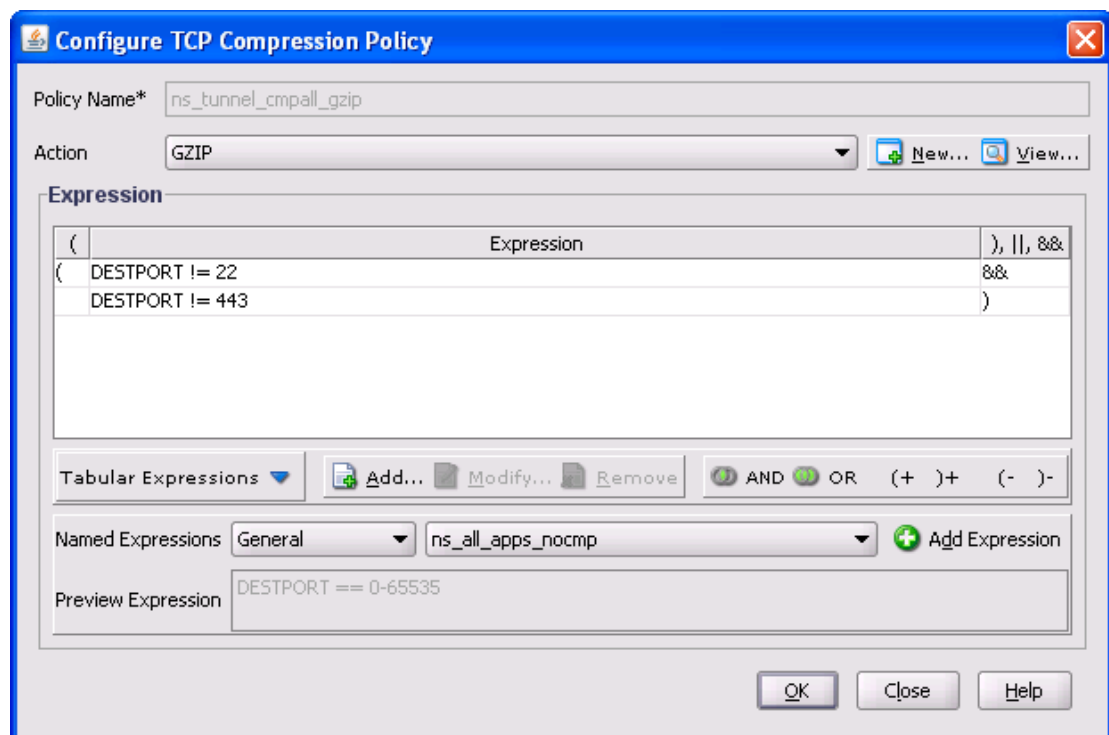


Figure 1. A configured TCP compression policy with the profile configured to use GZIP and the destination ports for the expression

In this illustration, traffic from the user device to all destination ports other than 22 and 443 are compressed using GZIP.

TCP compression policies are bound to the Access Gateway globally.

## To create a TCP compression policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click TCP Compression Policies.
4. Under Related Tasks, click Create new TCP compression policy.
5. In Name, type a name for the policy.
6. Next to Action, click New to create the profile.
7. In Name, type a name for the profile.
8. Under Compression Type, select the compression type and click Create.
9. Configure the expression, click Create, and then click Close.

## To modify a TCP compression policy using the Access Gateway Policy Manager

After you create a TCP compression policy, you can modify the policy expression at a later time using the Access Gateway Policy Manager.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click TCP Compression Policies and then select a policy.
4. Under Related Tasks, click Modify TCP compression policy.
5. Make the changes to the policy expression and click OK.

---

# Binding, Unbinding, and Removing TCP Compression Policies

TCP compression policies are bound only at the Access Gateway Global level. You can bind TCP compression policies using either the Access Gateway Policy Manager or the configuration utility.

## To bind a TCP compression policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configure Policies / Resources, expand Access Gateway Global.
4. Under Available Policies / Resources, expand TCP Compression Policies and then click a policy.
5. Drag the policy to TCP Compression Policies under Access Gateway Global.

## To bind a TCP compression policy using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click TCP Compression.
2. In the details pane, select a policy and click Global Bindings.
3. In the Bind/Unbind TCP Compression Policies to Global dialog box, under Details, click Insert Policy.
4. Under Policy Name, select the policy and click OK.
5. In Priority, type a number and click OK.



## To unbind a TCP compression policy using the Access Gateway Policy Manager

You can remove TCP compression policies from the Access Gateway. If the policy is bound, the binding must be removed before the policy can be removed from the appliance.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand the node for Access Gateway Global.
4. Expand the node for TCP Compression Policies and select a policy.
5. Under Related Tasks, click Unbind TCP compression policy and click Yes.

## To unbind a TCP compression policy using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click TCP Compression.
2. In the details pane, select a policy and click Global Bindings.
3. In the Bind/Unbind TCP Compression Policies to Global dialog box, select a policy and click Unbind Policy.

## To remove a TCP compression policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand the node for TCP Compression Policies.
4. Select a policy and under Related Tasks, click Remove TCP compression policy and click Yes.

## To remove a TCP compression policy using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click TCP Compression.
2. In the details pane, select a policy and click Remove.

---

# Monitoring TCP Compression on User Connections

You can monitor the compression rate of client connections from the Access Gateway Plug-in. In the plug-in Configuration dialog box, you can monitor the following items:

- The port the traffic is sent through
  - The size of uncompressed data
  - The size of compressed data
  - The bandwidth savings
  - The compression ratio
1. On the user device, in the notification area, right-click the Access Gateway icon and click Configure Access Gateway.
  2. In the Configuration dialog box, click the Compression tab.

**Note:** Users must be logged on to open the Configuration dialog box.

---

# Configuring Authentication and Authorization

Authentication allows users to log on to the Access Gateway and connect to resources in the internal network. Authentication provides security for your internal network and is configured using policies. After authentication is configured, you can add the policy globally or to virtual servers.

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

---

# Configuring Authentication on Access Gateway

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 the Access Gateway

The Access Gateway supports the following authentication types:

- Local
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- TACACS+
- Client certificate authentication

The Access Gateway also supports RSA SecurID, SafeWord products, and Gemalto Protiva. Authentication using these products is configured using a RADIUS server. You can also configure smart card authentication using client certificates.

Citrix recommends that you do not configure NTLM authentication on Access Gateway.

---

# Configuring Default Global Authentication Types

When you installed the Access Gateway and used the Access Gateway wizard, you configured authentication during the wizard. This authentication policy is bound automatically to the Access Gateway global level. The authentication type you configure during the Access Gateway wizard becomes the default authentication type. You can change the default authorization type by running the Access Gateway wizard again or using the global authentication settings in the configuration utility.

If you need to add additional authentication types, you can configure authentication globally on the Access Gateway. When authentication is configured 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 override the authentication type configured in the Access Gateway wizard.

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 Access Gateway subnet, mapped or virtual IP addresses. This is an optional setting.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In Maximum Number of Users, type the number of users who can be authenticated using this authentication type.
4. In NAT IP address, type the unique IP address for authentication.
5. In Default Authentication Type, select the authentication type.
6. Configure the settings for your authentication type and click OK.

---

# Configuring Authentication without Authorization

Authorization defines the resources users are allowed to connect to through the Access Gateway. Authorization policies are configured using an expression and then setting the policy to be allowed or denied. You can configure the Access Gateway to use authentication only, without authorization.

When authentication is configured without authorization, the Access Gateway does not perform a group authorization check. The policies configured for the user or group are assigned to the user.

For more information about configuring authorization, see [Configuring Authorization](#).



---

# Configuring Local Users

You can create user accounts locally on Access 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 Access Gateway. After configuring users and groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP address of file shares and servers to which users have access.

## To create local users

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Users.
4. Under Related Tasks, click Create new user.
5. In User Name, type the user name.
6. 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 Access Gateway authenticate against the local user database.

7. In Password and Confirm Password, type the password for the user, click Create and then click Close.

## To change a user password

After creating a local user, you can change the user's password or configure the user account to be authenticated against an external authentication server.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Users and click the user name.

4. Under Related Tasks, click Modify user.
5. In Password and Confirm Password, type the new password for the user and then click OK.

## To change a user's authentication method

If you have users who are configured for local authentication, you can change the authentication to an external authentication server. To do this, enable external authentication.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Users and click the user name.
4. Under Related Tasks, click Modify user.
5. Select External Authentication and then click OK.

## To remove a user

You can also remove a user from Access Gateway.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Users and click the user name.
4. Under Related Tasks, click Remove user and then click Yes.

When the user is removed from Access Gateway, all associated policies are also removed from the user profile.

---

# Configuring Groups

You can have groups on the Access Gateway that are local groups and can authenticate users with local authentication. If you are using external servers for authentication, groups on the Access 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 the Access Gateway. After configuring 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 the Access 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 the Access Gateway must be the same as the Active Directory group.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Groups.
4. Under Related Tasks, click Create new group.
5. 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 the Access Gateway.

1. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Groups and select a user group.
2. Under Related Tasks, click Remove group.

---

# Adding Users to Groups

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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Groups and select a user group.
4. Under Related Tasks, click Modify group.
5. On the Users tab, under Available Users, select the users, click Add and click OK.

---

# Configuring Policies with Groups

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 Access 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
- Bookmarks
- Session policies
- Traffic policies
- Auditing policies
- 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

When users log on to the Access Gateway, they are authenticated by a policy. The policy defines the authentication type. A single authentication policy can be used for simple authentication needs. Multiple policies can also be configured and bound to create a detailed authentication procedure. An authentication policy is comprised of an expression and an action.

Once created, an authentication policy can be bound either at the global level or to virtual servers. When at least one authentication policy is bound to a virtual server, any authentication policies bound to the global level are not used when users log on to the virtual server.

When a user logs on to the Access 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, global authentication policies are checked
- If an authentication policy is not bound to a virtual server or globally, the user is authenticated using the default authorization type, which is local authentication

---

# Configuring Authentication Profiles

You can create an authentication profile using the Access Gateway wizard, the configuration utility, or the Access Gateway Policy Manager. The profile contains all of the settings for the authentication policy. You configure the profile when you create the authentication policy.

With the Access Gateway wizard, you can configure authentication using the chosen authentication type. If you want to configure additional authentication policies after running the wizard, you can use the Access Gateway Policy Manager. For more information about the Access Gateway wizard, see [Configuring Settings Using the Access Gateway Wizard](#).

## To create an authentication policy using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select the authentication type.
7. If you are using an external authentication type, next to Server, click New.
8. Configure the settings for your authentication type and click Create.
9. 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 an authentication type is selected and the authentication profile is saved, the authentication type cannot be changed.

## To modify an authentication policy

You can modify configured authentication policies and profiles, such as changing the IP address of the authentication server or modifying the expression.

1. In the configuration utility, in the navigation pane, click Access Gateway.



2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Authentication Policies, and select the authentication policy.
4. Under Related Tasks, click Modify authentication policy.
5. In the Configure Authentication Policy dialog box, make the changes and click Close.

## To remove an authentication policy

If you changed or removed an authentication server from your network, remove the corresponding authentication policy from the Access Gateway.

1. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Authentication Policies, and select the authentication policy.
2. Under Related Tasks, click Remove authentication policy and click Yes.

---

# Binding Authentication Policies

After you configure the authentication policies, you bind the policy either globally or to a virtual server. You can use either the configuration utility or the Access Gateway Policy Manager to bind an authentication policy.

## To bind an authentication policy by using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Authentication Policies and then select a policy.
4. Under Configured Policies / Resources, do one of the following:
  - Expand System Global.
  - Expand Access Gateway Global.
  - Expand Virtual Servers and then expand a virtual server node.
5. If you selected System Global in Step 4, drag-and-drop the policy to Authentication Policies.
6. If you selected either Access Gateway Global or Virtual Servers in Step 4, drag-and-drop the policy to Authentication Policies (Primary) or Authentication Policies (Secondary).

## To bind an authentication policy globally by using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. In the navigation pane, select an authentication type.
3. On the Policies, tab, select a server and then click Global Bindings.
4. Under Details, click Insert Policy.
5. Under Policy Name, select the policy and then click OK.

If you configure multiple authentication policies on Access Gateway and the policies are bound at different levels, use the Access Gateway Policy Manager to find where

authentication policies are bound. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand the System Global, Access Gateway Global, or Virtual Servers node to see the bound authentication policies.

You can also use the Access Gateway Policy Manager or the configuration utility to remove bound authentication policies.

## To remove a bound authentication policy by using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand the node for the authentication policy and then select a policy.
4. Under Related Tasks, click Unbind authentication policy and then click Yes.

## To unbind a global authentication policy by using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. On the Policies tab, click Global Bindings.
3. In the Bind/Unbind Authentication Policies dialog box, in Policy Name, select the policy, click Unbind Policy and then click OK.

---

# Setting Priorities for Authentication Policies

Authentication policies are validated against those bound to the virtual server first and then globally. If you have an authentication policy bound globally and want it to take precedence over an authentication policy bound 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. If a priority number is not assigned, the virtual server authentication policy is applied first and then the global policy.

## To set or the priority for global authentication policies

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. On the Policies tab, click Global Bindings.
3. In the Bind/Unbind Authentication Global Policies dialog box, under Priority, type the number and 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers, expand a virtual server node, expand Authentication Policies (Primary) or Authentication Policies (Secondary), and select a policy.
4. Under Related Tasks, click Modify priority.
5. In Priority, type the number of the priority and click OK.

---

# Configuring LDAP Authentication

You can configure the Access 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 the Access Gateway. The characters and case must also be the same.

By default, LDAP authentication is secure using SSL/TLS. There are two types of secure LDAP connections. With one type, the LDAP server accepts the SSL/TLS connection on a port separate from the port used to accept clear LDAP connections. After users establish the SSL/TLS connection, LDAP traffic can be sent over the connection. The second type allows both unsecured and secure LDAP connections and is handled by a single port on the server. In this scenario, to create a secure connection, the client first establishes a clear LDAP connection. Then, the LDAP command StartTLS is sent to the server over the connection. If the LDAP server supports StartTLS, the connection is converted to a secure LDAP connection using TLS.

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

LDAP connections that use the StartTLS command use port number 389. If port numbers 389 or 3268 are configured on the Access Gateway, it tries to use StartTLS to make the connection. If any other port number is used, connection attempts are made using SSL/TLS. If StartTLS or SSL/TLS cannot be used, the connection fails.

When configuring the LDAP server, the letter case must match on the server and on the Access Gateway. If the root directory of the LDAP server is specified, all of the subdirectories are also searched to find the user attribute. In large directories, this 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	cn	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:

## Configuring LDAP Authentication

---

LDAP Server	Base DN
Microsoft Active Directory Server	DC=citrix, DC=local
Novell eDirectory	dc=citrix,dc=net
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, dc=citrix, dc=net
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 further information regarding LDAP sever settings, see [Determining Attributes in your LDAP Directory](#)

---

# To configure LDAP authentication

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select LDAP.
7. Next to Server, click New.
8. In Name, type the name of the server.
9. Under Server, in IP Address and Port, type the IP address and port number of the LDAP server.
10. Under Connection Settings, complete the following:

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

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
```

- 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 is defined in the Access Gateway must be identical to the group name that is defined on the LDAP server.

For other LDAP directories, the group name either is not required or, if required, is specified as `ou=groupname`.

The Access Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, the Access Gateway unbinds the administrator credentials and rebinds with the user credentials.

- In Administrator Password and Confirm Administrator Password, type the administrator password for the LDAP server.

11. 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.

12. Under Other Settings, in Server Logon Name Attribute, type the attribute under which the Access Gateway should look for user logon names for the LDAP server that you are configuring. The default is `samAccountName`.

13. In Group Attribute, leave the default `memberOf` for Active Directory or change it to that of the LDAP server type you are using. This attribute enables the Access Gateway to obtain the groups associated with a user during authorization.

14. In Security Type, select the security type and click Create.

15. To allow users to change their LDAP password, select Allow Password Change.

**Note:** If you select PLAINTEXT as the security type, allowing users to change their passwords is not supported.

16. Create an expression, click Create and click Close.

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



The screenshot shows a configuration window titled "Create Authentication Server". The window is divided into several sections:

- Name\*:** ldapauthserver
- Authentication Type:** LDAP
- Server:**
  - IP Address: 10 . 3 . 3 . 3
  - IPv6:
  - Port: 389
  - Time-out (seconds): 3
- Connection Settings:**
  - Base DN (location of users): DC=domainname, DC=com
  - Administrator Bind DN: LDAPaccount@domainname.com
  - Administrator Password: [masked]
  - Confirm Administrator Password: [masked]
  - Retrieve Attributes: [button]
- Other Settings:**
  - Server Logon Name Attribute: samAccountName
  - Search Filter: [empty]
  - Group Attribute: memberOf
  - Sub Attribute Name: CN
  - SSO Name Attribute: [empty]
  - Security Type:  PLAINTEXT,  TLS,  SSL
  - Authentication:
  - User Required:
  - Allow Password Change:
  - Nested Group Extraction: [expandable]

At the bottom of the window, there are "Help" and "Quick Link" icons on the left, and "Create" and "Close" buttons on the right.

Figure 1. A completed LDAP authentication configuration on the Access Gateway

---

# Determining Attributes in your LDAP Directory

If you need help determining your LDAP directory attributes, 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 at <http://www.ldapbrowser.com>. After the browser is installed, 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 can be left blank.

The information provided by the LDAP browser can help you determine the base DN needed for the Authentication tab.

- 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

You can configure the Access 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 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 your Access 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 the NAS IP is enabled, the appliance ignores any NAS ID that is configured using the NAS IP to communicate with the RADIUS server.
1. In the configuration utility, in the navigation pane, click Access Gateway.
  2. In the details pane, under Policy Manager, click Change group settings and user permissions.
  3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
  4. Under Related Tasks, click Create new authentication policy.
  5. In Name, type a name for the policy.
  6. In Authentication Type, select RADIUS.
  7. Next to Server, click New.
  8. In Name, type a name for the server.
  9. Under Server, in IP Address, type the IP address of the RADIUS server.
  10. In Port, type the port. The default is 1812.
  11. Under Details, in Secret Key and Confirm Secret Key, type the RADIUS server secret.
  12. In NAS ID, type the identifier number and click Create.
  13. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

After the RADIUS server settings are configured on the Access Gateway, bind the policy to make it active. This can be done either globally or to a virtual server. For more information about binding authentication policies, see [Binding Authentication Policies](#).

---

# Choosing RADIUS Authentication Protocols

The Access 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 Access 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 Access 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 Access Gateway policy that uses RADIUS authentication.

Shared secrets are configured on the Access Gateway when a RADIUS policy is created.

---

# Configuring IP Address Extraction

You can configure the Access Gateway to extract the IP address from a RADIUS server. When a user authenticates with the RADIUS server, the server returns a framed IP address that is assigned to the user. The 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 the Access Gateway
- Allows configuration for any RADIUS attribute using the type *ipaddress*, including those that are vendor encoded

When configuring the RADIUS server for IP address extraction, you configure the vendor identifier and the attribute type.

The vendor identifier 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 and attributes are used to make the association between the RADIUS client and 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 one and the maximum value is 255.

A common configuration is to extract the RADIUS attribute *framed IP address*. The vendor ID is set to zero or is not specified. The attribute type is set to eight.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, select a RADIUS authentication policy.
4. Under Related Tasks, click Modify authentication policy.
5. In the Configure Authentication Policy dialog box, next to Server, click Modify.
6. Under Details, in Group Vendor Identifier, type the value.
7. In Group Attribute Type, type the value, and click OK twice.

---

# Configuring the Access Gateway to Use One-Time Passwords

You can configure the Access Gateway to use one-time passwords, such as a token personal identification number (PIN) or passcode. After the passcode or PIN is used, it is immediately invalidated by the authentication server and cannot be used again.

Products that include using a one-time password include:

- RSA SecurID
- Imprivata's OneSign
- SafeWord
- Gemalto Protiva

To use each of these products, configure the authentication server in the internal network to use RADIUS. For more information, see [Configuring RADIUS Authentication](#).

---

# Configuring RSA SecurID Authentication

When configuring the RSA/ACE server, you need to complete the following on the RSA/ACE server:

Configure the RADIUS client with the following information:

- Provide the name of the Access Gateway appliance
- Provide a description (not mandatory)
- Provide the system IP address
- Provide the shared secret between Access 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 the Access Gateway (as it appears on the certificate bound to the virtual server). After providing the FQDN, click the tab button and the Network Address window populates itself.

When the FQDN is entered, the network address automatically appears. If it does not, enter the system IP address.

- Provide the Agent Type using Communication Server.
- Configure to import all users or a set of users that are allowed to authenticate through the Access 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.

When the FQDN is entered, 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

You can replace domain passwords with a one-time password generated by a hardware token from a RADIUS server. When users log on to the Access Gateway, they use a personal identification number (PIN) and the passcode from the token. When their credentials are validated, the RADIUS server returns the user's Windows password to the Access Gateway. The Access Gateway accepts the response from the server and then uses the returned password for single sign-on instead of using the passcode that users type during logon. This allows you to configure single sign-on without requiring users to know their Windows password.

To enable single sign-on using returned passwords, you configure a RADIUS authentication policy on the Access Gateway using the Password Vendor Identifier and Password Attribute Type parameters. These two parameters return the user's Windows password to the Access Gateway.

The Access Gateway supports Imprivata OneSign Version 4.0 with service pack 3 or later.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select RADIUS.
7. Next to Server, click New.
8. In Name, type the name of the server.
9. Configure the settings for the RADIUS server.
10. In Password Vendor Identifier, type the vendor identifier that is returned by the RADIUS server. This must have a minimum value of 1. The default password vendor identifier for Imprivata OneSign is 398.
11. 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 to 255. The default password attribute type code for Imprivata OneSign is 5.
12. 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

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.

Configure a SafeWord policy to authenticate users. The Access Gateway acts as a SafeWord agent authenticating on behalf of users logged on using the Access Gateway Plug-in.

To configure SafeWord authentication on the Access Gateway, follow the steps for configuring a RADIUS server. For more information, see [Configuring RADIUS Authentication](#).

---

# Configuring Gemalto Protiva Authentication

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 Access 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.
- Configure a policy on the Access Gateway to use RADIUS authentication and enter the settings of the Protiva server. For more information, see [Configuring RADIUS Authentication](#).

If authentication on the Access Gateway is configured to use a one-time password with RADIUS, such as provided by an RSA SecurID token, the Access Gateway attempts to reauthenticate users using the cached password. This occurs when changes are made to the Access Gateway or if the connection between the Access Gateway Plug-in and the Access Gateway is interrupted and then restored.

This can also occur when connections are configured to use Citrix online plug-ins and connect to the Web Interface using RADIUS or LDAP. When a user starts an application and uses it, then returns to the Web Interface to start another application, the Access Gateway uses cached information to authenticate the user.

For more information about installing the Protiva server, see the manufacturer's documentation.

---

# Configuring TACACS+ Authentication

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 the Access Gateway to use a TACACS+ server, provide the server IP address and the TACACS+ secret. The port needs to be specified only when the server port number in use is something other than the default port number of 49.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select TACACS.
7. Next to Server, click New.
8. In Name, type a name for the server.
9. Under Server, type the IP address and port number of the TACACS+ server.
10. Under TACACS server information, in TACACS Key and Confirm TACACS key, type the key.
11. In Authorization, select ON and click Create.
12. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

After the TACACS+ server settings are configured on the Access Gateway, bind the policy to make it active. This can be done on either the global or virtual server level. For more information about binding authentication policies, see [Binding Authentication Policies](#).

---

# Configuring Client Certificate Authentication

Users logging on to an Access Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. This can also be used with another authentication type, such as LDAP or RADIUS, to provide double-source 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. A root certificate must be bound to the virtual server on the Access Gateway.

When users log on to the Access 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 SSL handshake or if the user name extraction fails, the 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. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In Maximum Number of Users, type the number of users who can be authenticated using the client certificate.
4. In Default Authentication Type, select Cert.
5. In User Name Field, select the type of certificate field that holds the user names.
6. In Group Name Field, select the type of the certificate field that holds the group name and click OK.

---

# Configuring and Binding a Client Certificate Authentication Policy

You can also create a client certificate authentication policy and bind it to a virtual server. This policy takes precedence over the global policy and can be used to restrict access to specific groups or users.

## To configure a client certificate authentication policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select Cert.
7. Next to Server, click New.
8. In Name, type a name for the profile.
9. Next to Two Factor, select OFF.
10. In User Name Field and Group Name Field, select the values and click Create.

**Note:** If you previously configured client certificates as the default authentication type, use the same names as 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.

11. 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

When the client certificate authentication policy is configured, you can bind it to a virtual server.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.

2. In the details pane, click a virtual server and click Open.
3. In the Configure Access Gateway Virtual Server dialog box, click the Authentication tab.
4. Under Details, click Insert Policy.
5. In Policy Name, select the policy and click OK.

## To configure a virtual server to request the client certificate

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

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click a virtual server and click Open.
3. On the Certificates tab, click SSL Parameters.
4. Under Others, click Client Authentication.
5. In Client Certificate, select Optional or Mandatory and 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

You can configure a client certificate to authenticate users first and then require users to log on using a secondary authentication type, such as LDAP or RADIUS. In this scenario, users are authenticated with the client certificate first and then they are presented with a logon page where they can enter their user name and password. When the SSL handshake is complete, the logon sequence can take either of the following paths.

- Neither the user name nor the group is extracted from the certificate. The user is presented with the logon page and is requested to provide valid logon credentials. The credentials provided are authenticated as in the case of normal password authentication and the required information is obtained.
- The user name and group name are extracted from the client certificate. If only the user name is extracted, the user is presented with a logon page where the logon name is present and cannot be modified. Only the password field is left blank.

Group information that is extracted during the second round of authentication is appended to the group information extracted from the certificate (if any).



# Configuring Smart Card Authentication

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

To configure a smart card to work with the Access 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 the Access Gateway. For more information, see [To install a root certificate on the Access 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.

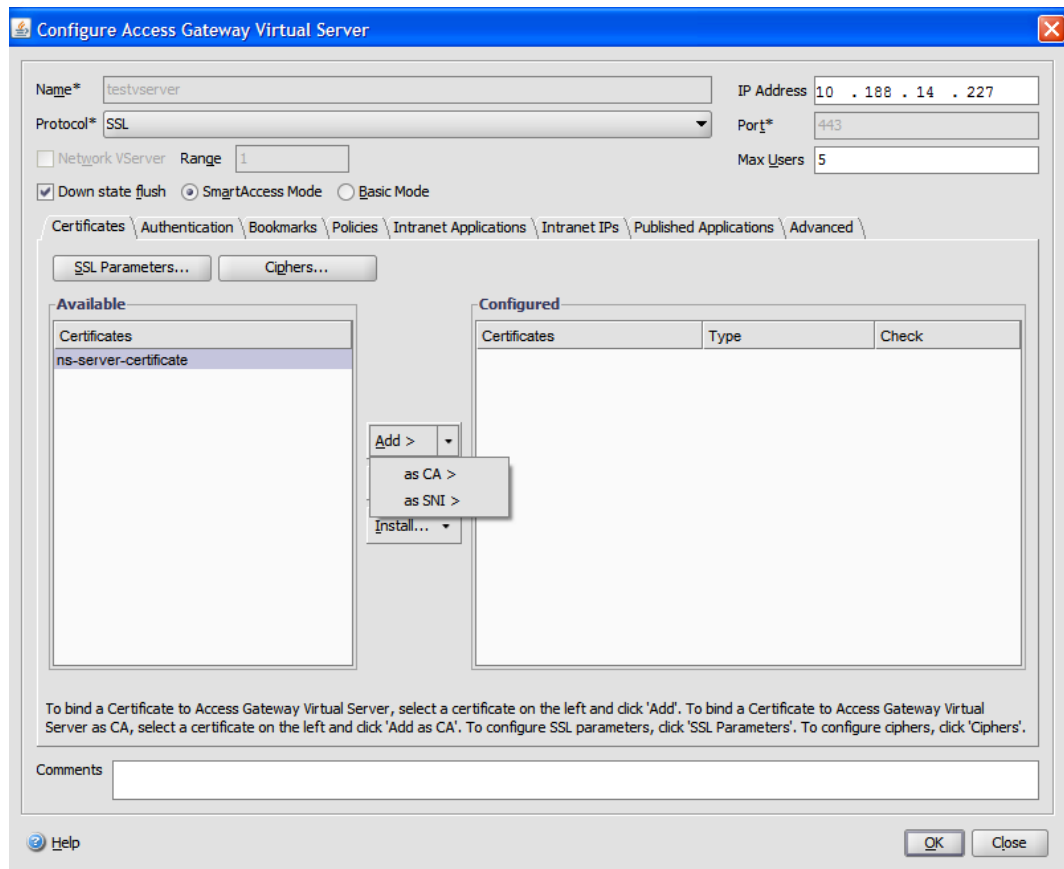


Figure 1. Adding a root certificate for smart card authentication

- Bind the root certificate to the virtual server. For more information, see [To add a root certificate to a virtual server](#).
- Configure the Access Gateway for client certificate authentication.

When the client certificate is created, you can flash the certificate onto the smart card. When that is completed, test the smart card.

To configure a client certificate on the Access Gateway, see [Configuring and Binding a Client Certificate Authentication Policy](#).

# Configuring Smart Card Authentication with Secure ICA Connections

If users log on using a smart card with single sign-on configured on the Access Gateway and establish a secure ICA connection, users might receive two prompts for their personal identification number (PIN): when logging on and when trying to start a published resource. This occurs if the Web browser and the online plug-ins are using the same virtual server that is configured to use client certificates. The online plug-ins do not share a process or an SSL connection with the Web browser, so when the ICA connection completes the SSL handshake with the Access Gateway, the client certificate is required a second time.

To prevent clients 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.

Users log on to the first virtual server and the second virtual server is used for the ICA connection. The Web Interface needs to be configured to use the Gateway Direct method. On the Access Gateway, configure the Secure Ticket Authority (STA) and bind it to the virtual server.

For more information about configuring the Web Interface, see one of the following topics:

- [Configuring Access Gateway Settings for the Web Interface on XenApp 5.0 or XenDesktop 2.1](#)
- [Configuring Access Gateway Settings in Web Interface 5.3](#)

## To create a second virtual server for ICA connections

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Virtual Servers.
4. Under Related Topics, click Create new virtual server.
5. In Name, type a name for the virtual server.
6. In IP Address, type the IP address for the virtual server.
7. In Max Users, type the number of users allowed to log on to the virtual server.
8. On the Certificates tab, click SSL Parameters.
9. In the Configure SSL Params dialog box, under Others, clear Client Authentication and click OK.
10. 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 the Access Gateway](#).

## To test smart card authentication

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

---

# Configuring a Common Access Card

Common access cards are used by the United States Department of Defense for identification and authentication.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. On the Servers tab, click Add.
3. In Name, type a name.
4. In Authentication Type, select Cert.
5. In User Name Field, type `SubjectAltName:PrincipalName` and 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

There are two types of multifactor authentication:

- Cascading authentication that sets the authentication priority level
- Double-source authentication that requires users to log on using two types of authentication

If you have multiple authentication servers, you can set the priority of your authentication policies that determines the order in which the authentication servers validates user's 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 and then using a personal identification number (PIN) and the code from the RSA token.

---

# Configuring Multifactor Authentication

There are two types of multifactor authentication:

- Cascading authentication that sets the authentication priority level
- Double-source authentication that requires users to log on using two types of authentication

## Setting Priorities for Authentication Policies

Authentication allows you to create a cascade of multiple authentication servers using policy prioritization. When a cascade is configured, the system traverses each authentication server defined by the cascaded policies to validate a client's credentials. Prioritized authentication policies are cascaded in ascending order and can have priority values from 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 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 multiple policies are bound to a virtual server or globally, define unique priorities for all authentication policies.

## To set the priority for global authentication policies

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. Select the policy that is bound globally and click Global Bindings.
3. In the Bind/Unbind Authentication Global Polices dialog box, under Priority, type the number and 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers, expand a virtual server node, expand Authentication Policies, and select a policy.
4. Under Related Tasks, click Modify priority.
5. In Priority, type the number and click OK.

---

# Configuring Double-Source Authentication

The Access Gateway supports double-source authentication. Normally, when authenticating users, the Access Gateway stops the authentication process as soon as it successfully authenticates a user employing 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 key authentication and user groups are stored on that server, you may need to authenticate users to that server so you can extract the groups.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. On the Policies tab, click Global Bindings.
3. In the Bind/Unbind Authentication Policies to Global dialog box, click Primary.
4. Click Insert Policy.
5. Under Policy Name, select the authentication policy.
6. Click Secondary, repeat Steps 4 and 5, and then click OK.



---

# Selecting the Authentication Type for Single Sign-On

If you have single sign-on and double-source authentication configured on the Access 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.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
2. In the details pane, click the Profiles tab and 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. Click Create if this is a new profile or OK if modifying an existing profile.

---

# Using Certificates and LDAP Authentication

You can use a secure client certificate with LDAP authentication and authorization. For example, you are using smart card authentication with LDAP. The user logs on and then the user name is extracted from the client certificate. LDAP is the primary form of authentication and the client certificate is the secondary form.

To use a client certificate, you must have an enterprise Certificate Authority, such as Certificate Services in Windows Server 2003, running on the same computer that is running Active Directory. You can create a client certificate using the Certificate Authority.

To use a client certificate with LDAP authentication and authorization, it must be a secure certificate using SSL. To use secure client certificates for LDAP, the client certificate is installed on the user device and a corresponding root certificate on the Access 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 a secure client certificate for LDAP

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select Cert.
7. Next to Server, click New.
8. In Name, type a name for the server.
9. In the Configure Authentication Server dialog box, in Name, type the name of the server.
10. Next to Two Factor, select ON.
11. In the User Name Field, select `Subject:CN` and click Create.
12. In the Create Authentication Policy dialog box, next to Named Expressions, select True value, click Add Expression, click Create, and click Close.

When the certificate authentication policy is created, bind the policy to the virtual server. After binding the certificate authentication policy, bind the LDAP authentication policy to the virtual server.

**Important:** The certificate authentication policy must be bound to the virtual server before the LDAP authentication policy.

## To install a root certificate on the Access Gateway

After creating the policy, download and install a root certificate from your Certificate Authority in Base 64 format and save it on your computer. You can then upload the root certificate to the Access Gateway.

1. In the configuration utility, in the navigation pane, expand SSL and click Certificates.
2. In the details pane, click Add.
3. In Certificate - Key Pair Name, type a name for the certificate.
4. Under Details, in Certificate Filename, 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 the Access Gateway, add it 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.

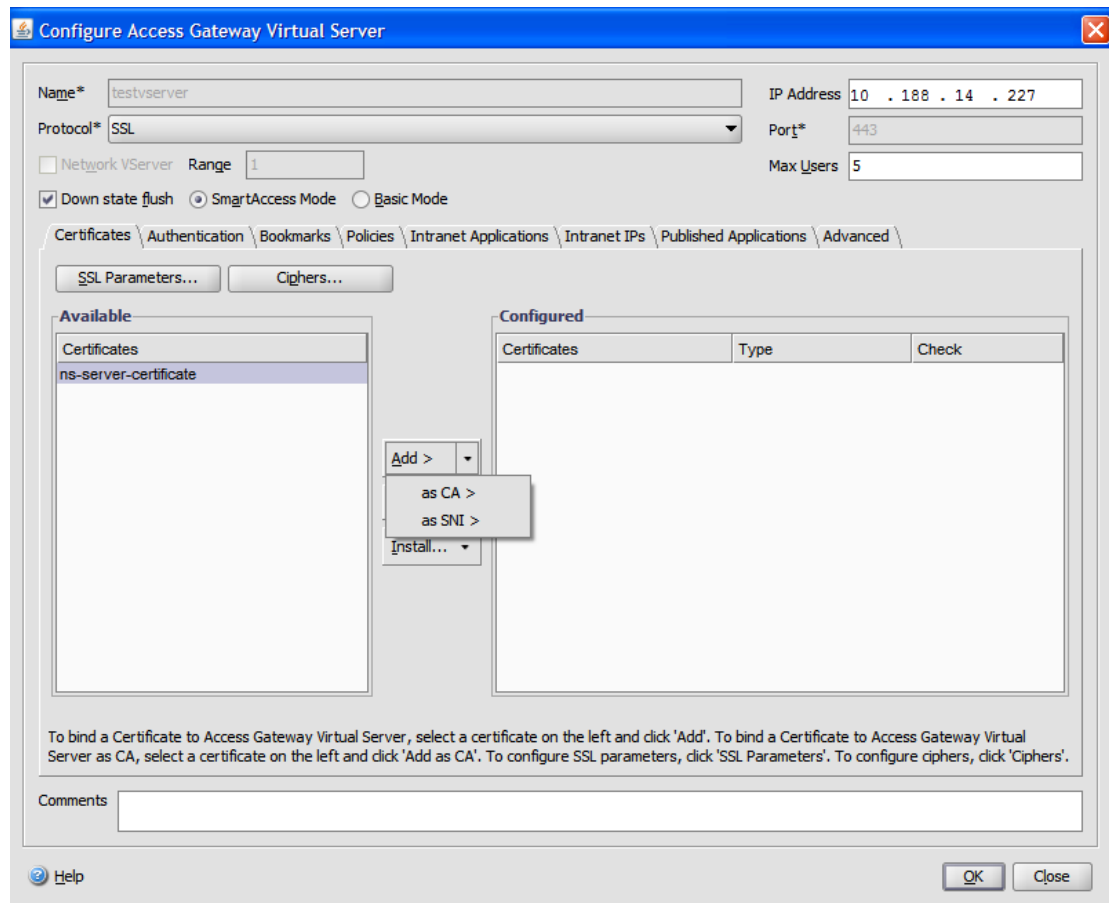


Figure 1. Adding a root certificate for smart card authentication

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers and select the virtual server.
4. Under Related Tasks, click Modify virtual server.
5. On the Certificates tab, under Available, select the certificate, next to Add, in the drop down box click as CA, and click OK.
6. Repeat Step 4.
7. On the Certificates tab, click SSL Parameters.

8. Under Others, select Client Authentication.
9. Under Others, next to Client Certificate, select Optional and click OK twice.

After configuring the client certificate, test the authentication by logging on to the Access Gateway using the Access Gateway Plug-in. If you have more than one certificate installed, you receive a prompt asking you to select the correct certificate. After selecting the certificate, the logon screen appears with the user name populated with the information obtained from the certificate. Type the password and 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 Active Directory. The groups that are defined on the Access Gateway must be the same as those in Active 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, this could cause incorrect reading of the client certificate.

If users and groups are not at the domain root level, the Access 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 the Access Gateway, leave User Name Field and Group Name Field blank.

---

# Disabling Authentication

If your deployment does not require authentication, you can disable it. This should be done for each virtual server that does not require authentication.

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

**Important:** Disabling authentication stops the use of authentication, authorization, and accounting features that control and monitor connections to the Access Gateway. When users type a Web address to connect to the Access Gateway, the logon page does not appear.

---

# Configuring the Number of User Sessions

The maximum number of users who are allowed to connect to the Access Gateway at a particular point in time can be configured at either the global level or on a per virtual server level. Sessions are not created on the Access Gateway if the number of users connecting to the appliance exceeds the value that is configured. If the number of users exceeds the number allowed, users receive an error message.

## Configuring the Global User Limit

When the user limit is configured globally, the restriction applies to all users who establish sessions to different virtual servers on the system. When the configured limit is reached, no new sessions can be established on any virtual server present on the Access Gateway.

Setting the maximum number of users at the global level is done when setting the default authentication type for the Access Gateway.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In the Global Authentication Settings dialog box, in Maximum Number of Users, type the number of users and click OK.

## Configuring the User Limit Per Virtual Server

The user limit can also be applied to each virtual server on the system. When the user limit is configured per virtual server, the restriction applies only to those users who establish sessions with the particular virtual server. Users who establish sessions with other virtual servers are not affected by this limit.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click a virtual server and click Open.
3. In Max Users, type the number of users and click OK.

---

# Configuring Authentication for Specific Times

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 the Access Gateway, create an expression within the authentication policy and then bind it to a virtual server or globally.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Authentication Policies, and select the authentication policy.
4. Under Related Tasks, click Modify authentication policy.
5. Under Expression, next to Match Any Expression, click Add.
6. In the Add Expression dialog box, in Expression Type, select Date/Time.
7. 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
8. In Operator, select the value.
9. In Value, click the calendar next to the text box and select the day, date, or time.
10. Click OK twice, click Close, and click OK.



---

# Configuring Authorization

Authorization specifies the network resources users have access to when they log on to the Access 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.

Authorization on the Access Gateway is configured using an authorization policy and expressions. When an authorization policy is created, you can bind it to users or groups configured on the appliance.

---

# Setting Default Global Authorization

To define the resources users have access to on the internal network, you can configure default global authorization. Global authorization is configured by allowing or denying access to network resources on the internal network.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Security tab, next to Default Authorization Action, select Allow or Deny and click OK.

If you set the default authorization policy to deny, you must to explicitly authorize access to any network resource, which improves security.

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 before network resources are accessible to those users or groups.

---

# Configuring Authorization Policies

When configuring 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, the Access Gateway performs a group authorization check by obtaining the user's group information from either an LDAP server, a RADIUS server, or a TACACS+ server. If group information is available for the user, the Access Gateway checks the network resources allowed for the group.

To control which resources clients have access to, you must create authorization policies. If you do not need to create authorization policies, you can configure default global authorization. For more information, see [Setting Default Global Authorization](#).

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authorization Policies.
4. Under Related Tasks, click Create new authorization policy.
5. In Name, type a name for the policy.
6. In Action, select Allow or Deny.
7. Next to Match Any Expression, click Add.
8. Configure the expression, click OK, click Create, and click Close.

---

# Binding Authorization Policies

When the authorization policy is configured, bind it to a user or group. You can bind the policy using either the Access Gateway Policy Manager or the configuration utility.

## To bind an authorization policy to a user or group using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Groups or Users and then expand the node for the user or group to which you want to add the authorization policy.
4. Under Available Policies / Resources, select the authorization policy and drag it to Authorization Policies for the user or group.

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

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Users.
2. In the details pane, select a user and click Open.
3. On the Authorization tab, click Insert Policy.
4. Under Policy Name, double-click the policy and click OK.

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

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Groups.
2. In the details pane, select a group and click Open.
3. On the Authorization tab, click Insert Policy.
4. Under Policy Name, double-click the policy and click OK.

---

# Setting the Priority for Authorization Policies

Authorization policies are applied first to users and then to groups. When a user logs on, the Access Gateway checks to see if an authorization policy is bound to the user. If an authorization policy is not bound to the user, the Access Gateway checks for group authorization policies. If none are found at the group level, the default global authorization is applied.

You can set the priority of an authorization policy. For example, you configured an authorization policy for a group and for a user. You set the priority so that the Access Gateway checks the group policy before checking the user policy. A numeric value is assigned to the priority. For example, you can set the group priority to zero and the user priority to one for the Access Gateway to check the group authorization policy first.

1. In the configuration utility, in the navigation pane, do one of the following:
  - Expand Access Gateway and then click Groups
  - Expand Access Gateway and then click Users
2. In the details pane, select a user or group and click Open.
3. On the Authorization tab, next to the policy, under Priority, type the priority number and click OK.

---

# Configuring LDAP Group Extraction

If you are using double-source 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 the Access 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, the Access Gateway extracts user information from all the groups to which users belong. If a user is a member of two groups on the Access 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 Access Gateway authorization, see the following:

- [Group Memberships from Group Objects Working Evaluations](#)
- [Group Memberships from Group Objects Non-Working Evaluations](#)

---

# Group Memberships from Group Objects Working Evaluations

LDAP servers that evaluate group memberships from group objects indirectly work with Access Gateway authorization.

Some LDAP servers enable user objects to contain information about groups to which they belong, such as Active Directory or eDirectory. A user's group membership can be computable attributes from the user object, such as IBM Directory Server or Sun ONE directory server. In some LDAP servers, this attribute can be used to include a user's dynamic group membership, nesting group membership, and static group membership to locate all group memberships from a single attribute.

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

---

# Group Memberships from Group Objects

## Non-Working Evaluations

LDAP servers that evaluate group memberships from group objects indirectly will not work with Access Gateway authorization.

Some LDAP servers enable only group objects such as the Lotus Domino LDAP server to contain information about users. The LDAP server does not enable the user object to contain information about groups. For this type of LDAP server, group membership searches are performed by locating the user on the member list of groups.



---

# LDAP Authorization Group Attribute Fields

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

---

# Configuring LDAP Authorization

LDAP authorization is configured in the authentication policy by setting the group attribute name and the subattribute.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select LDAP.
7. Next to Server, click New.
8. In Name, type the name of the server.
9. Under Server, type the IP address and port of the LDAP server.
10. In Group Attribute, type `memberOf`.
11. In Sub attribute Name, type `CN` and click Create.
12. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

---

# Configuring LDAP Nested Group Extraction

The Access Gateway can query LDAP groups and extract group and user information from ancestor groups configured on the authentication server. For example, you created group1 and within that group, created group2 and group3. If the user belongs to group3, the Access Gateway extracts information from all the ancestor groups (group2, group1) up to the specified level.

You can configure LDAP nested group extraction using an authentication policy. When the query is run, the Access Gateway searches the groups until the maximum nesting level is reached or until there are no further groups to search.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select LDAP.
7. Next to Server, click New.
8. In Name, type the name of the server.
9. Configure the settings for the LDAP server.
10. Expand Nested Group Extraction and click Enable.
11. In Maximum Nesting Level, type the number of levels the Access Gateway checks.
12. In Group Name Identifier, type the LDAP attribute name that uniquely identifies a group name on the LDAP server, such as `sAMAccountName`.
13. 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`.
14. 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`.
15. In Group Search Filter, type the query string. For example, the filter could be `(&(samaccountname=test)(objectClass=*))`.

16. Click Create.
17. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create, and click Close.

---

# Configuring LDAP Group Extraction for Multiple Domains

If you have multiple domains for authentication and are using the Web Interface, you can configure the Access 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 the group is created, add users that belong to the group and specified domain. After the groups are configured in Active Directory, configure the Access Gateway.

To configure the Access Gateway for group extraction for multiple domains, you need to create the same number of session and authentication policies as there are domains. 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 the Access Gateway, binding the session policies to the group. Then, bind the authentication policies to a virtual server.

---

# Creating Session Policies for Group Extraction

The first step is to create two session profiles and set the following parameters:

- Enable ICA proxy
- Add the Web Interface Web address
- Add the Windows domain
- Add the profile to a session policy and set the expression to true

## To create the session profiles for group extraction

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
2. In the details pane, click the Profiles tab and click Add.
3. In Name, type a name for the profile. For example, type `Sampa`.
4. On the Published Applications tab, do the following:
  - a. Next to ICA Proxy, click Override Global and select ON.
  - b. Next to Web Interface Address, click Override Global and type the URL of the Web Interface.
  - c. Next to Single Sign-On Domain, click Override Global, type the name of the domain, and 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 domain and type the name of the second domain, click Create, and then click Close.

When the session profiles are created, create two session policies. Each session policy uses one of the profiles.

## To create a session policy

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. In Request Profile, select the profile for the first domain.
5. Next to Named Expressions, click General, select True value, click Add Expression, and 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 click Close.

---

# Creating LDAP Authentication Policies for Multiple Domains

After the session policies are created, create LDAP authentication policies that are almost identical. When configuring the authentication policy, the important field is the Search Filter. You must type the name of the group you created in Active Directory in this field.

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

## To create authentication profiles for multiple domain group extraction

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. In the details pane, click the Servers tab and click Add.
3. In Name, type the name of the first domain, such as *Sampa*.
4. Next to Authentication Type, select LDAP and click Create.
5. Configure the settings for the LDAP server.
6. Repeat Steps 3, 4, and 5 to configure the authentication profile of the second domain. Click Close.

When the profiles are created and saved, create the authentication policies.



## To create authentication policies for multiple domain group extraction

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Authentication.
2. In the details pane, click the Policies tab and 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 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 click Close.

---

# Creating Groups and Binding Policies for LDAP Group Extraction for Multiple Domains

After creating the authentication policies, create groups on the Access Gateway. After creating the groups, bind the authentication policy to a virtual server.

**Important:** When creating groups on the Access Gateway for group extraction from multiple domains, group names must be the same as those defined in Active Directory. Group names are also case-sensitive and must match those in Active Directory.

## To create groups on the Access Gateway

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Groups.
2. In the details pane, click Add.
3. In Group Name, type the name of the first Active Directory group.
4. On the Policies tab, click Session and click Insert Policy.
5. Under Policy Name, double-click the policy and click Create.

## To bind the authentication policies to a virtual server

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click a virtual server and click Open.
3. On the Authentication tab, click Primary, under Policy Name, double-click Insert Policy and select the first authentication policy.
4. Under Policy Name, click Insert Policy, double-click the second authentication policy and click OK.

---

# Configuring RADIUS Group Extraction

You can configure RADIUS authorization using a method called *group extraction*. This allows you to administer users on your RADIUS server instead of adding them to the Access Gateway.

RADIUS authorization is configured using an authentication policy and configuring the group vendor identifier (ID), the group attribute type, the group prefix, and a group separator. When the policy is configured, add an expression, and then bind the policy either globally or to a virtual server.

If you are using Microsoft's Internet Authentication Service (IAS) for RADIUS authorization, during configuration of the Access Gateway, the following information needs to be provided:

- Vendor ID is the vendor-specific code number that was entered in IAS.
- Type is the vendor-assigned attribute number.
- Attribute name is the type of attribute name that is 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 Access Gateway needs the Vendor-Specific Attribute to match the users defined in the group on the server with those on the Access Gateway. This is done by sending the Vendor-Specific Attributes to the Access Gateway. Make sure you select *RADIUS=Standard*.

- The RADIUS default is 0. Use this number for the vendor code.

- The vendor-assigned attribute number is 0.

This is the assigned number for the User Group attribute. The attribute is in string format.

- Select String for the Attribute format.

The Attribute value requires the attribute name and the groups.

For the Access Gateway, the attribute value is `CTXSUserGroups=groupname`. If two groups are defined, such as sales and finance, the attribute value is `CTXSUserGroups=sales;finance`. Separate each group with a semicolon.

- Remove all other entries in the Edit Dial-in Profile dialog box, leaving the one that says Vendor-Specific.

When you are finished configuring the Remote Access Policy in IAS, go to the Access Gateway and configure the RADIUS authentication and authorization.

When configuring RADIUS authentication, use the settings that are configured on the IAS server.

---

# To configure RADIUS authorization

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Authentication Policies.
4. Under Related Tasks, click Create new authentication policy.
5. In Name, type a name for the policy.
6. In Authentication Type, select RADIUS.
7. Next to Server, click New.
8. In Name, type the name of the RADIUS server.
9. Under Server, type the IP address and port of the RADIUS server.
10. Under Details, enter the values for Group Vendor Identifier and Group Attribute Type.
11. In Password Encoding, select the authentication protocol and then click Create.
12. 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

*Endpoint analysis* is a process that scans a client device and detects information such as the presence and version level of operating system, antivirus, firewall, or Web browser software. You can use endpoint analysis to verify that the client 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 client device during the user session to ensure that the device continues to meet requirements.

---

# How Endpoint Policies Work

You can configure the Access 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 the Access Gateway to check for antivirus, firewall, antispam, processes, files, registry entries, Internet security, or operating systems. If the user device fails the preauthentication scan, users are not allowed to log on. This information can be included as a filter within an access policy or a connection policy.

If you need to configure additional security requirements that are not used in a preauthentication policy, configure a session policy and bind it to a user or group. This is called a *post-authentication policy*. When this is configured, the Access Gateway sends a file to Internet Explorer that downloads the endpoint analysis plug-in and runs the post-authentication scan. If users are not using Internet Explorer, the Access Gateway Plug-in runs the post-authentication scan.

Endpoint policies are configured using three types of policies:

- Preauthentication policies that use a yes or no parameter.
- Session policy that is conditional and can be used for SmartAccess
- Client security expression within a session policy

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 using client devices that are current with antivirus and firewall software requirements. For users connecting from untrusted computers, you can provide a more restricted level of access that allows editing the documents on remote servers without downloading them.

Endpoint analysis performs these basic steps:

- Examines an initial set of information about the user device to determine which scans to apply
- Runs all applicable scans
- 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

When a user tries to connect, endpoint analysis checks the scans that are filtered for the endpoint policy. These scans return results (called scan outputs) of detected information or true or false results of required property values.

Endpoint analysis completes before the user session uses a license.

A preauthentication scan is the yes or no parameter to determine if the user device meets the specified requirements. If the scan fails, credentials cannot be entered on the logon

page.

A session policy is conditional and typically used for SmartAccess. Within the session policy, there is a client security expression. 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 have additional checks.

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 that are contained within a session profile and policy.

## System Requirements for Endpoint Analysis

When the Endpoint Analysis Plug-in is installed on the user device, it allows the Web browser to scan the user device for the endpoint security requirements configured on the Access Gateway.

When users connect, the Access Gateway detects the correct version of the Endpoint Analysis Plug-in. If it is the correct version, the plug-in scans the user device. Otherwise, users receive a download button to install or upgrade the plug-in.

The Endpoint Analysis Plug-in requires the following:

- Internet Explorer 6.0 or later with ActiveX control enabled
- Firefox 3.0 or later with the Access Gateway Plug-in enabled



---

# Evaluating Client Logon Options

When users log on, they can choose to skip the endpoint analysis scan. If users skip the scan, the Access Gateway processes this as a failed endpoint analysis.

For example, you want to provide client access with network-layer access using the Access Gateway Plug-in. To log on to the Access Gateway, users must be running an antivirus application, such as Norton Antivirus. If the client device is not running the application, users can log on only to the Web Interface and use published applications.

To configure the Access Gateway, assign a restrictive session policy as the default and then upgrade users to a privileged session policy when the client device passes the endpoint analysis scan.

To configure the Access Gateway to enforce the restrictive session policy first, perform the following steps:

- Configure the global settings with ICA proxy enabled and all other settings needed if the specified application is not running on the client device
- Create a session policy and profile that enables the Access 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, the settings in the session policy are ignored and users have restricted access using the Web Interface or clientless access. If endpoint analysis passes, the session policy is applied and users have full access.

If users skip the endpoint analysis scan, the expression in the session policy is considered false.

---

# Configuring Preauthentication Policies and Profiles

You can configure Access Gateway to check for client-side security before users are authenticated. This method ensures that the user device establishing a session with Access 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 Access 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.

## To configure a preauthentication profile globally by using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the Global Settings pane, under Settings, click Change pre-authentication settings.
3. In the Global Pre-authentication settings dialog box, configure the following settings:
  - Action. Denies or allows logon after endpoint analysis.
  - Processes to be killed. Specifies the processes to be stopped by the Endpoint Analysis Plug-in.
  - Files to be deleted. Specifies the files to be deleted by the Endpoint Analysis Plug-in.
  - Expression. Includes the following settings to help you to create expressions:
    - Expression. Displays all 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 using the OR (||) or AND (&&) operators.
    - Advanced Free-Form. Creates custom compound expressions 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 Access 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 Access Gateway when you select a named expression.
  - Create. Creates the compression policy.

## To configure a preauthentication profile by using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Pre-Authentication.
2. In the details pane, click Profiles and then 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 killed, 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.

You can also use the Access Gateway Policy Manager to create a policy and profile together.

## To create a preauthentication policy and profile by using the Access Gateway Policy Manager

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Pre-Authentication Policies.
4. Under Related Tasks, click Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type the name of the application to be checked.
8. In Action, select ALLOW or DENY.
9. In Process to be killed, type the name of the process to be stopped.
10. In Files to be deleted, type the name of the file to be deleted, such as *c:\clientext.txt* and then click Create.
11. Next to Named Expressions, select General, select True Value, click Add Expression, click Create and then click Close.

---

# Configuring Endpoint Analysis Expressions

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 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

The Access Gateway comes with pre-configured expressions, called *named expressions*. When you are configuring 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.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Pre-Authentication Policies.
4. Under Related Tasks, click Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.

8. In Action, select Allow or Deny and click Create.
9. Next to Named Expressions, select Anti-Virus, select Symantic AntiVirus 10 (with Updated Definition Files), click Add Expression, click Create, and then click Close.

---

# Configuring Custom Expressions

A custom expression is one that you create within the policy. When you create an expression, 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.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Pre-Authentication Policies.
4. Under Related Tasks, click Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile and in Action, select Allow.
8. In the Create Pre-Authentication Policy dialog box, next to Match Any Expression, click Add.
9. In Expression Type, select Client Security.
10. Configure the following:
  - a. In Component, select Anti-Virus
  - b. In Name, type a name for the application
  - c. In Qualifier, select Version
  - d. In Operator, select ==
  - e. In Value, type the value
  - f. In Freshness, type 3 and click OK.
11. In the Create Pre-Authentication Policy dialog box, click Create, and then click Close.

When a custom expression is configured, it is added to the Expression box in the policy dialog box.





---

# Configuring Multiple Expressions

The preauthentication policy can have one profile and multiple expressions. If multiple expressions are configured, you use operators to specify the conditions of the expression. For example, the user device must run one of the following antivirus applications:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

You can configure the expression with the “or” operator to check for these three applications. If the correct version of any of these applications is found on the client device, users are allowed to log on. The expression in the policy dialog box appear as follows:

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

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

---

# Binding Preauthentication Policies

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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, under Pre-authentication Policies, click a pre-authentication policy.
4. Drag the policy to one of the following under Configured Policies / Resources:
  - Under AAA Global > Pre-authentication Policies
  - Under Virtual Servers, expand a node, and drop the policy to Pre-authentication Policies

---

# Setting the Priority of Preauthentication Policies

You can have multiple preauthentication policies that are bound to different levels. For example, you have a policy that checks for a specific antivirus application bound 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 and then the policy bound at AAA Global. You can change the order that the preauthentication scans occur. To make the Access Gateway apply the global policy first, change the priority number of the policy bound to the virtual server so it is a higher 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, the global policy is applied first and then the virtual server policy.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand either AAA Global or Virtual Servers.
4. If you selected Virtual Servers, expand a virtual server node.
5. Expand the Pre-authentication Policies node and then click a policy.
6. Under Related Tasks, click Modify priority.
7. In the Modify Priority dialog box, in Priority, type a number and click OK.

---

# Unbinding and Removing Preauthentication Policies

If a preauthentication policy is no longer needed on the Access Gateway, you can remove it. Before removing a preauthentication policy, unbind it from the virtual server or globally.

## To unbind a preauthentication policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click the AAA Global or Virtual Server node to which the policy is bound.
4. Select the policy and under Related Tasks, click Unbind pre-authentication policy.

When the preauthentication policy is unbound, the policy can be removed from the Access Gateway.

## To remove a preauthentication policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Pre-Authentication Policies and then select the policy.
4. Under Related Policies, click Remove pre-authentication policy.

---

# Configuring Post-Authentication Policies

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 the Access Gateway is closed. You can configure any setting for client connections that can be made conditional in the post-authentication policy.

**Note:** This functionality works only with the Access Gateway Plug-in. If users log on with Citrix online plug-ins, the endpoint analysis scan runs at logon only.

Post-authentication policies are configured using session policies. First, create the users to which the policy applies. Then, add the users to a group and bind session, traffic policies, and intranet applications to the group.

You can 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.

A post-authentication policy can also be configured to put users in a quarantine group if the user device does not meet the requirements of the policy.

Post-authentication policies are also used with SmartAccess. For more information about SmartAccess, see [How SmartAccess Works for XenApp and XenDesktop](#).

If users fail a post-authentication policy, they can be put into a quarantine group. When users are in the quarantine group, logon to the Access Gateway is permitted, however users receive limited access to network resources.

---

# Configuring a Post-Authentication Policy

The post-authentication policy is configured using a session policy. A simple policy includes a client security expression and a client security message.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Security tab, click Advanced.
9. Under Client Security, click Override Global and click New.
10. Configure the client security expression and click Create.
11. Under Client Security, in Quarantine Group, select a group.
12. In Error Message, type the message you want users to receive if the post-authentication scan fails.
13. Under Authorization Groups, click Override Global, select a group, click Add, click OK, and then click Create.
14. 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.

---

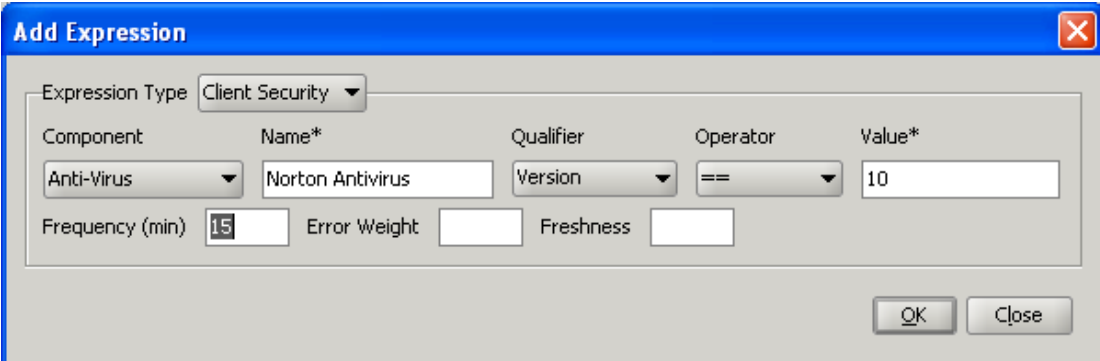
# Configuring the Frequency to Run a Post-Authentication Policy

You can configure the Access 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 do this by creating a custom expression within the policy.

**Note:** The frequency check functionality works only with the Access Gateway Plug-in. If users log on with Citrix online plug-ins, the endpoint analysis scan runs at logon only.

When you configure the client security policy using the procedure [Configuring a Post-Authentication Policy](#) you can set the frequency at that time.

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



The screenshot shows a dialog box titled "Add Expression" with a blue header and a close button in the top right corner. The dialog is used for configuring expressions for Client Security. It features a table with columns for Component, Name\*, Qualifier, Operator, and Value\*. Below the table, there are input fields for Frequency (min), Error Weight, and Freshness. The "OK" and "Close" buttons are located at the bottom right.

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

Frequency (min)  Error Weight  Freshness

OK Close



---

# Configuring Quarantine and Authorization Groups

When users log on to the Access Gateway, users can be assigned to a group that is configured either on the Access Gateway or on an authentication server in the secure network. If a user fails a post-authentication scan, the user can be placed in 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 defined on the Access Gateway, users can be added to groups dynamically.

Quarantine and authorization groups are configured using either global settings or session policies 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, the session policy is applied based on group membership.

---

# Configuring Quarantine Groups

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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Security tab, click Advanced.
9. Under Client Security, click Override Global and click New.
10. In the Client Expression dialog box, configure the client security expression and click Create.
11. In Quarantine Group, select the group.
12. In Error Message, type a message that describes the problem for users and click Create.
13. 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 the session policy is created, 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 has an equal or lower priority number than the policies bound to the quarantine group.

## To configure a global quarantine group

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Security tab, click Advanced.
4. Under Client Security, click New.
5. In the Client Expression dialog box, configure the client security expression and click Create.
6. In Quarantine Group, select the group.
7. In Error Message, type a message that describes the problem for users and click OK twice.

---

# Configuring Authorization Groups

When users pass the endpoint analysis scan, you can add them to an authorization group. If users are not part of a group configured locally on the Access Gateway and an authorization group is configured, users are assigned to the authorization group. This allows you to bind authorization policies to the authorization group instead of binding the policies globally.

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 members of another group configured on the Access Gateway.

## To configure an authorization group using a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Security tab, click Advanced.
9. Under Authorization Groups, click Override Global, select a group from the drop-down list, click Add, click OK and click Create.
10. 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 the session policy is created, you can bind it to a user, group, or virtual server.

## To configure a global authorization group

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Security tab, click Advanced.
4. Under Authorization Groups, select a group from the drop-down list, click Add, and 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 click Remove.

---

# Configuring Security Preauthentication Expressions for User Devices

Access 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 an Access Gateway session.

The following are the types of security checks on user devices that you can configure on Access Gateway:

- Antivirus
- Personal firewall
- Internet security
- Antispam
- Service policies
- Process policies
- Operating system
- File policies
- Registry 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 Access Gateway.

You can use the Access Gateway Policy Manager 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

The settings for antivirus, firewall, Internet security, and antispam policies are configured within the Add Expression dialog box. The settings for each are the same: the differences are the values that you select. For example, you want to check the client device for Norton AntiVirus Version 10 and ZoneAlarm Pro. You create two expressions with the name and version number of each application.

When you select client security as the expression type, you can configure the following:

- Component that 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 component for which the expression checks.
- Operator checks is the value exists or is equal to the value.
- Value is the application version for antivirus, firewall, Internet security, or antispam software on the client device.
- Frequency is how often a post-authentication 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, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:

- a. In Component, select the item for which to scan.
- b. In Name, type the name of the application.
- c. In Qualifier, select Version.
- d. In Operator, select the value.
- e. In Value, type the client security string, click OK, and then click Close.



---

# Configuring Service Policies

A service is a program that runs silently on the user device. When you create a session or preauthentication policy, you can create an expression that ensures that user devices are running a particular service when the session is established.

## To configure a service policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:
  - a. In Component, select Service.
  - b. In Name, type the name of the service.
  - c. In Qualifier, leave blank or select Version.
  - d. Depending on your selection in Qualifier, do one of the following:
    - If left blank, in Operator, select == or !=
    - If you selected Version, in Operator, in Value, type the value, click OK and then click Close.

You can check a list of all available services and the status for each on a Windows-based computer at the following location:

Control Panel > Administrative Tools > Services

**Note:** The service name for each service varies from its listed name. Check for the name of the service by looking at the Properties dialog box.

---

# Configuring Process Policies

When creating a session or preauthentication policy, you can define a rule that requires all user devices to have a particular process running when users log on. The process can be any application and can include customized applications.

**Note:** The list of all processes running on a Windows-based computer appears on the Processes tab of Windows Task Manager.

## To configure a process policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:
  - a. In Component, select Process.
  - b. In Name, type the name of the application.
  - c. In Operator, select EXISTS or NOTEXISTS, click OK and then click Close.

When you configure an endpoint analysis policy (pre-authentication or post-authentication) to check for a process, you can configure an MD5 checksum.

When you create the expression for the policy, you can add the MD5 checksum to the process you are checking for. For example, if you are checking to see if notepad.exe is running on the user device, the expression is:

```
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS
```

---

# Configuring Operating System Policies

You can configure client security strings to determine whether or not the client is logging on from a particular operating system. 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 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, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:
  - a. In Component, select Operating System.
  - b. In Name, type the name of the operating system.
  - c. In Qualifier, do one of the following:
    - Leave blank
    - Select Service Pack
    - Select Hotfix

d. Depending on your selection in Step C, in Operator, do one of the following:

- If Qualifier is blank, in Operator, select EXISTS or NOTEXISTS
- If you selected Service Pack or Hotfix, select the operator and in Value, type the value

9. Click OK and click Close.

if you are configuring a service pack, such as `client.os (winxp).sp`, if a number is not in the Value field, the Access Gateway returns an error message because this is an invalid check.

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 Service Pack 4's presence automatically indicates that previous service packs are present.

---

# Configuring File Policies

You can define a rule within a session or preauthentication policy that checks if a file exists or does not exist on the user device to establish the session. You can also specify the time stamp to define the age of the file. If the file on the user device does not match the expression in the policy, the endpoint analysis scan fails.

## To configure a session or preauthentication policy to check for a file on the user device

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:
  - a. In Component, select File.
  - b. In Name, type the name of the application.
  - c. In Qualifier, leave blank or select Time Stamp. If Time Stamp is selected, in Value, type the value.
  - d. In Operator, select the value, click OK and then click Close.

**Note:** If you use the command line to configure a file check, use four backslash (\) characters instead of one. For example, the configuration shows `c:\\\\file.txt` and not `c:\file.txt`. You can also use a forward slash to configure a file check, such as `c:/file.txt`.

---

# Configuring Registry Policies

When you create a session or preauthentication policy, you can check for the existence and value of registry entries on the user device. The session is established only if the particular entry exists or has the configured or higher value.

When configuring a registry expression, use the following guidelines:

- Four backslashes are used to separate keys and subkeys, such as

```
HKEY_LOCAL_MACHINE\\\\"SOFTWARE
```

- Underscores are used to separate the subkey and the associated value name, such as

```
HKEY_LOCAL_MACHINE\\\\"SOFTWARE\\\\"VirusSoftware_Version
```

- A backslash (\) is used to denote a space, such as in the following two examples:

```
HKEY_LOCAL_MACHINE\\\\"SOFTWARE\\Citrix\\\\"Secure\ Access\  
Client_ProductVersion
```

```
CLIENT.REG(HKEY_LOCAL_MACHINE\\\\"Software\\\\"Symantec\\Norton\  
AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5
```

The following is a registry expression that looks for the Access Gateway Plug-in registry key when users log on:

```
CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\"SOFTWARE\\\\"CIT  
RIX\\\\"Secure\Access\Client_ProductVersion
```

**Note:** If you are scanning for registry keys and values and you select Advanced Free-Form in the Expression dialog box, the expression must start with `CLIENT.REG`

Registry checks are supported under the following most common five types:

- HKEY\_CLASSES\_ROOT
- HKEY\_CURRENT\_USER
- HKEY\_LOCAL\_MACHINE
- HKEY\_USERS
- HKEY\_CURRENT\_CONFIG

Registry values to be checked use the following types:

- String  
For the string value type, case-sensitivity is checked.
- DWORD

For DWORD type, the value is compared and must be equal.

- Expanded String

Other types such as Binary and Multi-String, are not supported.

- Only the '==' comparison operator is supported.
- Other comparison operators such as <, > and case-sensitive comparisons are not supported.
- The total registry string length should be less than 256 bytes.

You can add a value to the expression. The value can be a software version, service pack version, or any other value that appears in the registry. If the data value in the registry does not match the value you are testing against, users are denied logon.

**Note:** You cannot scan for a value within a subkey. The scan must match the named value and the associated data value.

## To configure a registry policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies or Pre-authentication Policies.
4. Under Related Tasks, click Create new session policy or Create new pre-authentication policy.
5. In Name, type a name for the policy.
6. Next to Match Any Expression, click Add.
7. In the Add Expression dialog box, in Expression Type, select Client Security.
8. Configure the settings for the following:
  - a. In Component, select Registry.
  - b. In Name, type the name of the registry key.
  - c. In Qualifier, leave blank or select Value.
  - d. In Operator, do one of the following:
    - If Qualifier is left blank, select EXISTS or NOTEXISTS
    - If you selected Value in Qualifier, select either == or !=
  - e. In Value, type the value as it appears in the registry editor, click OK and then click Close.

---

# Configuring Compound Client Security Expressions

The client security strings mentioned above can be combined to form different compound client security expressions.

The Boolean operators that are supported in the Access Gateway are:

- And (&&)
- Or (||)
- Not (!)

The strings can be grouped together using parentheses for greater precision.

**Note:** If you are using the command line to configure expressions, use parentheses to group security expressions together when you form a compound expression. It improves understanding and debugging of the client expression.

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

The AND operator works by combining two client security strings so that the compound check passes only when both checks are true. The expression is evaluated from left to right and if the first check fails, the second check is not carried out.

The AND operator can be configured using the keyword 'AND' or the symbols '&&'.

Example:

The following is a client security check that determines if the client device has Version 7.0 of Sophos AntiVirus installed and running. It also checks if the netlogon service is running on the same computer.

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS
```

This string can also be configured as

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS
```



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

The OR operator works by combining two security strings such that 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.

The OR operator can be configured using the keyword 'OR' or the symbols '||'.

Example:

The following is a client security check that determines if the client computer has either the file c:\file.txt on it or the putty.exe process running on it.

```
client.file(c:\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS
```

This string can also be configured as

```
client.file(c:\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS
```

## Configuring Policies Using the NOT ( ! ) Operator

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

Example:

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

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

---

# Access Gateway Enterprise Edition Client Connection Methods

Users can connect to your organization's network resources using several different methods. These include:

- Citrix online plug-ins that establish an ICA session to a server farm
- Access Gateway Plug-in for Windows that is software installed on the user device
- Access Gateway Plug-in for Mac OS X (supported on Versions 10.5 and 10.6)
- Access Gateway Plug-in for Java that is software that allows connections using a Macintosh, Linux, UNIX, or Windows computer
- Clientless access that provides users with the access they need without installing client software
- Interoperability with Citrix Repeater Plug-in

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 Access Gateway Enterprise Edition](#).

---

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

Access Gateway operates as follows:

- When users attempt to access network resources across the VPN tunnel, the Access Gateway Plug-in encrypts all network traffic destined for the organization's internal network and forwards the packets to Access Gateway.
- Access Gateway terminates the SSL tunnel, accepts any incoming traffic destined for the private network, and forwards the traffic to the private network. Access Gateway sends traffic back to the remote computer over a secure tunnel.

When users type the Web address, they receive a logon page where users enter their credentials and log on. If the credentials are correct, Access 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 Access Gateway Plug-in is installed on the user device. After the first connection, if users log on using a Windows-based computer, they can use the icon in the notification area to establish the connection.

---

# How User Connections Work with Receiver

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

- Windows-based applications and virtual desktops published in CloudGateway Express
- Web, SaaS, and native mobile iOS applications configured in CloudGateway Enterprise
- ShareFile data accessed through CloudGateway

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 Access Gateway and the connection to internal resources is established. Users can then access their Windows, Web, and SaaS applications that are available from CloudGateway. Users can also connect to their virtual desktops from XenDesktop.

Users can establish a connection from an iOS device through Access Gateway. If users connect from an iOS-based device, you must enable Secure Browse to allow connections to Access Gateway without requiring the full VPN tunnel. When users log on through Receiver to Access Gateway, the connection works the same as if users log on with the Access Gateway Plug-in only.

Users can also establish a full VPN tunnel from Android devices by using Receiver. When users log on, their Web applications appear in the Receiver window.

---

# Tunneling Private Network Traffic over Secure Connections

When the Access Gateway Plug-in is started and the user is authenticated, all network traffic destined for specified private networks is captured and redirected over the secure tunnel to the Access Gateway.

The Access Gateway intercepts all network connections made by the client device and multiplexes/tunnels them over SSL to the Access Gateway, where the traffic is demultiplexed and the connections are forwarded to the correct host and port combination.

The connections are subject to administrative security policies that apply to a single application, a subset of applications, or an entire intranet. You specify the resources (ranges of IP address/subnet pairs) that remote users can access through the VPN connection.

The Access Gateway Plug-in intercepts and tunnels the following protocols for the defined intranet applications:

- TCP (all ports)
- UDP (all ports)
- ICMP (types 8 and 0 - echo request/reply)

Connections from local applications on the client device are securely tunneled to the Access Gateway, which reestablishes the connections to the target server. Target servers view connections as originating from the local Access Gateway on the private network, thus hiding the client device. This is also called *reverse Network Address Translation (NAT)*. Hiding IP addresses adds security to source locations.

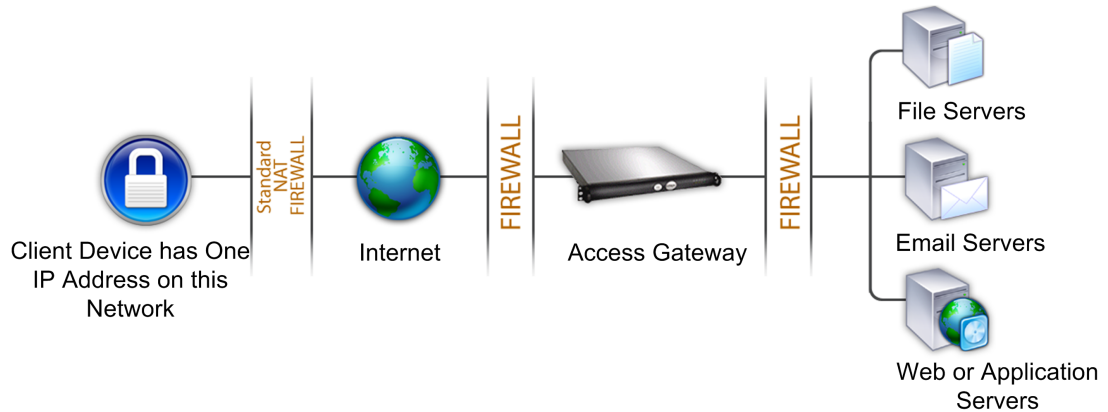
Locally, on the client device, all connection-related traffic (such as SYN-ACK, PUSH, ACK, and FIN packets) is recreated by the Access Gateway Plug-in to appear from the private server.

---

# Operation through Firewalls and Proxies

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

Figure 1. Client connection through two internal firewalls



NAT firewalls maintain a table that allows them to route secure packets from the Access Gateway back to the client device. For circuit-oriented connections, the Access Gateway maintains a port-mapped, reverse NAT translation table. The reverse NAT translation table enables the Access Gateway to match connections and send packets back over the tunnel to the client device with the correct port numbers so that the packets return to the correct application.

---

# Terminating the Secure Tunnel and Returning Packets to the User Device

Access Gateway terminates the SSL tunnel and accepts any incoming packets destined for the private network. If the packets meet the authorization and access control criteria, Access Gateway regenerates the packet IP headers so that they appear to originate from the Access Gateway's private network IP address range or the client-assigned private IP address. Access Gateway then transmits the packets to the network. This also occurs of users log on to Access Gateway with Citrix Receiver.

The Access Gateway Plug-in maintains two tunnels:

- An SSL tunnel over which data is sent to Access Gateway
- A tunnel between the user device and local applications

The encrypted data that arrives over the SSL tunnel is then decrypted before being sent to the local application over the second tunnel.

If you run a packet sniffer such as Ethereal on the user device where the Access Gateway Plug-in is running, you will see unencrypted traffic that appears to be traveling between the user device and Access Gateway. That unencrypted traffic, however, is not over the tunnel between the user device and Access Gateway, but rather the tunnel to the local applications.

When an application client connects to its application server, certain protocols may require the application server to in turn attempt to create a new connection with the client. In this case, the client sends its known local IP address to the server by means of a custom client-server protocol. For these applications, the Access Gateway Plug-in provides the local client application with a private IP address representation, which Access Gateway uses on the internal network. Many real-time voice applications and FTP use this feature.

Users can access resources in the secure network by connecting through Access Gateway from their own computer or from a public computer.

---

# Supporting the Access Gateway Plug-in

To enable users to connect to and use the Access Gateway, you need to provide them with the following information:

- Access Gateway Web address, such as <https://AccessGatewayFQDN/>.
- Path to any network drives that the users can access, which is done by mapping a network drive on the client device.
- Any system requirements for running the Access Gateway Plug-in if you configured endpoint resources and policies.
- If a user runs a firewall on the client device, the user might need to change the firewall settings so that it does not block traffic to or from the IP addresses corresponding to the resources for which you granted access. The Access Gateway Plug-in automatically handles Internet Connection Firewall in Windows XP and Windows Firewall in Windows XP Service Pack 2, Windows Vista and Windows 7.

Because users work with files and applications just as if they were local to the organization's network, no retraining of users or configuration of applications is needed.



---

# Choosing the User Access Method

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

- User connections by using Citrix Receiver. Receiver is software installed on the user device and contains the plug-ins, including the Access Gateway Plug-in for user connections. Access Gateway also supports connections from Receiver for Android and Receiver for iOS. Users can connect to their virtual desktops and Windows-based, Web, and SaaS applications through CloudGateway.
- User connections by using the Access Gateway Plug-in as a standalone application. The Access Gateway Plug-in is software that is downloaded and installed on a user device. When users log on with the plug-in, users can access resources in the secure network as if they were in the office. Resources include email servers, file shares, and intranet Web sites.
- User connections by using the Web Interface or StoreFront. Receiver works with the Web Interface or StoreFront to provide users with access to published applications or virtual desktops in a server farm. Receiver is software that uses the ICA network protocol to establish user connections.
- User connections by using clientless access. Clientless access provides users with the access they need without requiring them to install software, such as the Access Gateway Plug-in or Receiver. Clientless access allows connections to a limited set of Web resources, such as Outlook Web Access or SharePoint, applications published on Citrix XenApp, virtual desktops from Citrix XenDesktop, and file shares in the secure network through the Access Interface without installing software on the user device.
- User connections if a preauthentication or post-authentication scan fails. This scenario is called *access scenario fallback*. Access scenario fallback allows a user device to fall back from the Access Gateway Plug-in to the Web Interface (using Receiver) if the user device does not pass the initial endpoint analysis check.

If users log on to Access Gateway through Receiver, the preauthentication scan does not work. Post-authentication scans do work when Access Gateway establishes the VPN tunnel.

---

# How Users Connect to Applications, Desktops, and ShareFile

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

- Access Gateway Plug-in that establishes a full VPN tunnel to resources in the internal network. You create a session profile to select the Access Gateway Plug-in for Windows or the Access Gateway Plug-in for Mac. When users log on by using the Access Gateway Plug-in for Windows, endpoint analysis scans can run on the user device.
- Citrix Receiver to connect to Web, SaaS, and native iOS mobile applications and documents from ShareFile through CloudGateway. When users log on with Receiver, Access Gateway routes the connection to AppController. When Receiver established the connection, users' applications and documents appear in Receiver. If users connect to AppController, you must enable clientless access in Access Gateway. This deployment does not require StoreFront.
- Receiver to connect to published applications and virtual desktops through StoreFront. When users log on with Receiver, Access Gateway routes the connection to StoreFront. When Receiver establishes the connection, user applications and desktops appear in Receiver.

In any of the preceding scenarios, if users want to connect through Access Gateway, they can log on by using the Access Gateway Plug-in or Receiver. To log on for the first time, the user opens a Web browser and types the fully qualified domain name (FQDN) of Access Gateway or Receiver. On the logon page, the user logs on and is authenticated. After authentication, the user session is redirected to StoreFront or AppController. If you deploy both StoreFront and AppController, Access Gateway contacts StoreFront which then contacts AppController. All of the users' desktops, documents, and Web, SaaS, and Windows-based applications appear in Receiver.

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

**Important:** Citrix recommends configuring authentication on the Access Gateway virtual server. When you disable authentication in Access Gateway, unauthenticated HTTP requests are sent directly to the servers running StoreFront or CloudGateway in the internal network.

---

# Integrating the Access Gateway Plug-in with Receiver

Access Gateway supports Receiver. The orchestrated system consists of the following CloudGateway components:

- Receiver for Windows 3.0, 3.1, and 3.2
- Receiver for Mac
- Receiver for Android
- Receiver for iOS
- StoreFront 1.0, 1.1, and 1.2
- AppController 1.1 and 2.0
- Citrix online plug-ins
- Self-service plug-in
- Merchandising Server that is installed on a virtual machine (VM) in your data center
- Citrix Update Service that is hosted on the [Citrix Web site](#)

You can configure Access Gateway so that when users log on to the appliance, the Access Gateway Plug-in opens a Web browser that allows single sign-on to the Receiver home page. Users can download Receiver from the home page. Citrix recommends using the Merchandising Server to deploy and update plug-ins to a user device.

When users log on with Receiver, the connection can route directly to AppController, directly to StoreFront, or to StoreFront and then AppController if you deploy both products in your network.

**Note:** Connections that are routed directly to AppController are supported in AppController 2.0 and AppController 2.5 only. If you have AppController 1.1 deployed in your network, user connections must route through StoreFront.

## Configuring Receiver and Merchandising Server

Receiver and CloudGateway streamline the installation and management of application delivery to user desktops. When you include Merchandising Server, you select the plug-ins to install on the user device. When users log on for the first time, the plug-ins download and install on the users' device.

Receiver and Merchandising Server together provide the following two important features:

- The Merchandising Server allows you to configure, deliver, and upgrade plug-ins on your user's devices.
- Receiver manages all the operations for Citrix plug-ins on user devices; the self-service plug-in provides the ability to create an application and services store for users.

When users install Receiver, all plug-ins installed on the user device, including the Access Gateway Plug-in, become part of Receiver automatically. To easily enable subsequent updates, users can install Citrix Receiver Updater for Windows 3.0 or Receiver Updater for Mac, which is an optional software client for use with Receiver for Windows and earlier versions of Citrix online plug-ins. Citrix Receiver Updater, a separate component, works with Merchandising Server to deploy and automatically update Receiver and associated plug-ins to user devices or on virtual desktops through XenDesktop.

The self-service plug-in is fully integrated with Receiver. You can load the Receiver plug-in for the self-service plug-in into Merchandising Server, schedule it for delivery, and then silently push the plug-in to user devices that have Receiver installed. When users start the self-service plug-in, the store is fully stocked with all the applications users are authorized to access.

The Merchandising Server Administrator Console is the interface on the Merchandising Server that you use to configure Citrix applications (and application plug-ins) and schedule their delivery to user devices. The Merchandising Server broadcasts the plug-ins and their installation instructions to users on the scheduled date. Users simply install Receiver on their user devices. Once installed, Receiver gets the delivery information from the Merchandising Server and installs the plug-ins. After installation is complete, Receiver starts its plug-ins in the correct order, ensuring that connectivity services are available for plug-ins that require it.

If users install the Repeater Plug-in or the offline plug-in on the user device, users might be prompted to restart the device.

---

# Adding the Access Gateway Plug-in to Receiver

When Citrix Receiver is installed on the user device, users can log on with the Access Gateway Plug-in through Receiver. You upload the Access Gateway Plug-in to Merchandising Server, which then downloads and installs the plug-in to Receiver on the user device. If users have the Access Gateway Plug-in installed when they install Receiver for the first time, the plug-in is automatically added to Receiver.

## Delivering Plug-ins to User Devices

To deliver plug-ins to user devices, you must upload and configure the Access Gateway Plug-in on the Merchandising Server. When users make a selection, the plug-in downloads and installs from the Merchandising Server.

If users install the Access Gateway Plug-in and then later install Receiver, when the Receiver installation is complete, the Access Gateway Plug-in appears in the Receiver menu.

If users have Citrix Receiver for Windows 3.0, 3.1 or 3.2, users can install Receiver Updater for Windows. This is an optional component that updates the plug-ins and communicates with Merchandising Server. Receiver includes all of the plug-ins available for delivery, including the Access Gateway Plug-in. For more information about Receiver Updater for Windows, see the Receivers and Plug-ins section in the Citrix eDocs library

## Connecting to Access Gateway with Receiver

If users connect with Receiver for Windows 3.0 or 3.1, they can right-click the Receiver icon in the notification area and then click Preferences. If users log on with Receiver for 3.2, they can right-click the Receiver icon and then click About. If the Access Gateway Plug-in is installed on the user device, users right-click the Access Gateway Plug-in and then click Logon. When authentication succeeds, the Access Gateway Plug-in establishes the connection to Access Gateway and establishes a full VPN tunnel.

The Access Gateway Web address is part of the metadata configured on Merchandising Server and users cannot change the address. The Access Gateway Plug-in initiates the logon to Access Gateway. If the version of Access Gateway Plug-in for Windows that is installed on the user device is different than the version on the Access Gateway appliance, the plug-in downgrades or upgrades automatically when users log on. The Access Gateway Plug-in for Mac OS X does not downgrade automatically. To install an earlier version of the plug-in on a Mac computer, users must first uninstall the Access Gateway Plug-in and then download the earlier version from Access Gateway.

## Upgrading or Downgrading the Access Gateway Plug-in

During an upgrade or downgrade of the Access Gateway Plug-in, the existing version is removed and the version downloaded from Access Gateway is installed. Users can confirm the new installation by checking the plug-in entry on the Preferences > Plug-in status panel in Receiver 3.0 or 3.1. The newly installed version of the Access Gateway Plug-in might be a different version than what is configured on Merchandising Server.

## Adding the Access Gateway Plug-in to Merchandising Server

You can also configure Access Gateway Plug-in delivery on Merchandising Server, which provides a Web configuration interface that allows you to upload the Access Gateway Plug-in MSI installation package. On Merchandising Server, you can:

- Specify the version and metadata for the Access Gateway Plug-in.
- Configure one or more Web addresses for the Access Gateway appliance.
- Associate specific rules based on operating system or other parameters for delivery.

**Note:** Users cannot add or remove servers from the list of servers configured on Merchandising Server, although they can select a different server from the configured list in the Network Settings panel.

If you are using Access Scenario Fallback or load balancing, you can configure a fixed set of Access Gateway Web addresses and designate Merchandising Server as the default address. Users connect to the default server when they select Log On from the Receiver menu. Users can select a different address from the provided list by using the Receiver's Preferences > Network Settings panel in Receiver 3.0 or 3.1. Users can select a different address in Receiver 3.2 from the About panel.

Users can continue to use a Web browser to log on to any Access Gateway.

The following are general steps for adding the Access Gateway Plug-in to Merchandising Server. For specific configuration steps, see Merchandising Server under Receiver and Plug-ins in the Citrix eDocs library.

- Configure the settings on the General tab in the Merchandising Server Administrator Console.
- Add the Access Gateway Plug-in to Merchandising Server.

Select the appropriate plug-in version for the target platform. The Access Gateway Plug-in must be added to the main page of Merchandising Server for the plug-in to appear in the Add Plug-ins to Delivery page.

- Configure delivery for the Access Gateway Plug-in.

Use a friendly name for the location that identifies the Access Gateway Web address. This name appears in Receiver. You can also add additional Access Gateway appliances.

- Specify authentication type and customize specific labels that appear in the Receiver logon dialog box, such as the user name, password, or personal identification number (PIN).

- Add rules for the delivery.

You must create rules if you want rules to appear in the Add Rule to Delivery page.

- Schedule the delivery.

## Uninstalling Receiver

If users uninstall Receiver without uninstalling individual plug-ins from the user device, all plug-ins registered with Receiver, including the Access Gateway Plug-in, are removed from the user device. If users want to log on with the Access Gateway Plug-in, users need to install the plug-in as a standalone application.

---

# Configuring the Receiver Home Page on Access Gateway

You can configure the Receiver home page either globally or as part of a session profile. If you want to configure Receiver for Web and earlier Receiver versions that do not recognize StoreFront through Access Gateway, you need to create two separate session profiles. The field Citrix Receiver Home Page needs to have the correct Web address for each profile so users can log on successfully.

For Receivers that recognize StoreFront through Access Gateway, you can have Receiver for Web and Receiver share a profile. However, Citrix recommends that you configure a session profile for Receiver for Web and a separate session profile for all other Receivers.

## To configure the Receiver home page globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Access Gateway .
2. In the Global Settings pane, under Settings, click Change global settings.
3. In the Global Access Gateway Settings dialog box, click the Published Applications tab.
4. In Citrix Receiver Home Page, type the Web address for the Receiver or Receiver for Web home page and then click OK.

## To configure the Receiver home page in a session profile

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and then click Session.
2. In the details pane, on the Profiles tab, click Add.
3. In the Create Access Gateway Session Profile dialog box, on the Published Applications tab, next to Citrix Receiver Home Page, click Override Global.
4. In Citrix Receiver Home Page, type the Web address for the Receiver or Receiver for Web home page and then click OK.



---

# Applying the Receiver Theme to the Logon Page

You can use the configuration utility to apply the Receiver theme to the logon page for Access Gateway. You can switch between the Receiver theme, the default theme, or a custom theme that you create.

**Note:** To use this feature, you must install Access Gateway 10, Build 71.6014.e. In addition, if your appliance is licensed as a NetScaler VPX running on the SDX platform and you configure link aggregation, Citrix recommends installing Access Gateway 10, Build 73.5002.e after you install Build 71.6104.e. This allows user connections through Access Gateway to CloudGateway 2.5.

1. In the configuration utility, click Access Gateway.
2. In the Details pane, click Global Settings.
3. In Global Access Gateway Settings, click the Client Experience tab.
4. Next to UI Theme, click GREENBUBBLE and then click OK. This command overwrites the original logon page with the Receiver theme.

**Note:** After you apply a different theme, advise users to clear the browser cache to prevent cached pages from appearing.

---

# Creating a Custom Theme for the Logon Page

You can use the configuration utility to create a custom theme for the logon page for Access Gateway. You can also leave the default theme or use the Citrix Receiver theme. When you choose to apply a custom theme to the logon page, you use the Access Gateway command line to create and deploy the theme. You then use the configuration utility to set the custom theme page.

**Note:** To use this feature, you must install Access Gateway 10, Build 71.6104.e. To use this feature with AppController 2.5, you must install Access Gateway 10, Build 73.5002.e after you install Build 71.6104.e.

## To create and deploy the custom theme by using the command line

1. Log on to the Access Gateway command line.
2. At a command prompt, change the directory to `/netscaler/ns_gui/`. The folder contains files related to the default theme.
3. Create a copy of the folders within the `/netscaler/ns_gui/` directory to use as a template for customization. The `ns_gui/vpn` and `ns_gui/epa` folders in particular contain pages related to log on, log off, and endpoint analysis. Citrix recommends that you do not customize the `ns_gui/admin_ui` files.
4. After you customize the pages, archive the `ns_gui` folder and then zip the folder into a `customtheme.tar.gz`. Give the archive a name that, when unzipped, will extract into the original `ns_gui` folder.
5. Copy `customtheme.tar.gz` into the `/var/ns_gui_custom/` folder. You may need to create the folder.
6. If you have a high availability configuration, repeat Step 5 for all appliances.

## To apply the custom theme by using the configuration utility

1. In the configuration utility, click Access Gateway.
2. In the details pane, click Global Settings.
3. In Global Access Gateway Settings, click the Client Experience tab.
4. Next to UI theme, click CUSTOM and then click OK.

**Note:** If you upgrade Access Gateway, Citrix recommends that you set the theme back to the default theme page. Then, follow the preceding steps after you install the new version.

---

# Allowing Access from Mobile Devices

Access Gateway provides access to internal resources by using the Access Gateway Plug-in, clientless access, and connections to XenApp and XenDesktop from a Windows-based or Mac OS X computer. *Secure Browse* allows users to connect through Access Gateway to network resources from Receiver for iOS, Version 5.6.x. Users do not need to establish a full VPN tunnel to access resources in the secure network.

## Configuring Secure Browse

You enable Secure Browse as part of global settings or as part of a session policy. You can bind the session policy to users, groups, or virtual servers. When you configure Secure Browse, you must also enable clientless access. However, clientless access does not require you to enable Secure Browse. When you configure clientless access, set the Clientless Access URL Encoding to Clear.

## How Secure Browse Connections Work

When users log on from an iOS device, the request from the mobile device contains a session cookie. When Access Gateway and Receiver respond, the response body contains prefixes that indicate that Secure Browse and clientless access are enabled.

When you enable Secure Browse, URL rewriting occurs on the mobile device. Receiver uses the prefix to rewrite the URL when accessing internal resources. For example, if the internal resource being accessed is `http://mywebapp.net` and the fully qualified domain name (FQDN) of Access Gateway is `https://my.agee.com`, the rewritten request looks like `https://my.agee.com/SecureBrowse/http/mywebapp.net`.

If you enable Client Choices and Secure Browse as part of the session profile, when users log on from an iOS device, Secure Browse disables the client choices page. When users log on, they do not receive a choice to select the Access Gateway Plug-in, clientless access, or an ICA connection as they would if logging on from a Windows-based or Mac OS X computer.

## Integrating Access Gateway and Receiver for Mobile Devices

When users connect, Access Gateway needs to discover the platform of the device, Android or iOS. Access Gateway also needs to recognize if the Receiver version supports Access Gateway. To establish this support, the Access Gateway Plug-in is packaged with Receiver.

---

# Configuring Secure Browse in Access Gateway

You can configure Secure Browse globally or as part of a session policy. When you enable Secure Browse, you need to enable clientless access and set the URL encoding to clear. For more information, see the following:

- [Enabling Clientless Access](#)
- [Encoding the Web Address](#)

## To configure Secure Browse globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the right pane, under Settings, click Change global settings.
3. In the Global Access Gateway Settings dialog box, on the Security tab, click Secure Browse and then click OK.

## To configure Secure Browse in a session profile

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Do one of the following:
  - If you are creating a new session policy, under Related Tasks, click Create new session policy.
  - If you are changing an existing policy, select a policy and then under Related Tasks, click Modify session policy.
5. Create a new profile or modify an existing profile. To do so, do one of the following:
  - Next to Request Profile, click New.
  - Next to Request Profile, click Modify.
6. On the Security tab, next to Secure Browse, click Override Global and then select Secure Browse.
7. Do one of the following:
  - If you are creating a new profile, click Create, set the expression in the policy dialog box, click Create and then click Close.
  - If you are modifying an existing profile, after making the selection, click OK twice.

---

# Configuring Endpoint Analysis for Mobile Devices

If you configure endpoint analysis, you need to configure the policy expressions so that the endpoint analysis scans do not run on Android or iOS mobile devices. Endpoint analysis scans are not supported on mobile devices.

If you bind an endpoint analysis policy to a virtual server, you must create a secondary virtual server for mobile devices. Do not bind preauthentication or post-authentication policies to the mobile device virtual server.

When you configure the policy expression in a preauthentication policy, you add the User-Agent string to exclude Android or iOS. When users log on from one of these devices and you exclude the device type, endpoint analysis does not run.

For example, you create the following policy expression to check if the User-Agent contains Android, if the application virus.exe does not exist, and to end the process keylogger.exe if it is running by using the preauthentication profile. The policy expression might look like this:

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

After you create the preauthentication policy and profile, bind the policy to the virtual server. When users log on from an Android or iOS device, the scan does not run. If users log on from a Windows-based device, the scan does run.

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

---

# Configuring TCP Compression Policy Expressions for Mobile Devices

Some versions of Citrix Receiver do not support compressed responses from Access Gateway, even if you configure a TCP compression policy in Access Gateway. You can configure a TCP compression policy to skip the compression for Android or iOS mobile devices. You can use expressions within a TCP compression policy so that responses from Access Gateway through a mobile device are not compressed.

For Android devices, you can use either of the following expressions:

- In the TCP compression profile, select NoCompress and then create this policy expression in the policy: REQ.HTTP.HEADER User-Agent CONTAINS Android
- In the TCP compression profile, select Deflate and then create this policy expression in the policy: REQ.HTTP.HEADER User-Agent NOTCONTAINS Android

For iOS devices, you can use one of the following expressions:

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

For more information about configuring TCP compression policies, see [How TCP Compression Policies Work](#).



---

# Enabling Support for Device Polling for Mobile Devices

Citrix AppController includes a policy setting for mobile devices that use Citrix Receiver called *Active poll period*. Polling determines the status of the current application (enabled or disabled) and device (lock or erase). When a device has network connectivity, polling allows the running application to detect and respond to changes in the app state. To allow polling to work with AppController from Access Gateway, you need to provide an IP address, such as `https://ipaddress` or `https://AppControllerIPaddress`, or the fully qualified domain name of AppController, such as `http://AppC-FQDN` or `https://AppCFQDN`, in the Access Gateway configuration utility to enable support for the Active poll period policy. The device status appears in the AppController management console on the Devices tab.

**Note:** To use this feature, you must install Access Gateway 10, Build 71.6104.e. In addition, if your appliance is licensed as a NetScaler VPX running on the SDX platform and you configure link aggregation, Citrix recommends installing Access Gateway 10, Build 73.5002.e after you install Build 71.6104.e. This allows user connections through Access Gateway to CloudGateway 2.5.

1. In the configuration utility, click Access Gateway.
2. In the Details pane, click Global Settings.
3. In Global Access Gateway Settings, click Bind/Unbind AppController URL.
4. In Configure AppController, next to AppController URL, enter the IP address for AppController, such as `https://192.10.10.122` or `https://appcontroller.domain.net` and then click OK.
5. In the upper-right corner of the configuration utility, click Refresh or Save.

If you restart Access Gateway, you must enter the IP address again.

---

# Selecting the Plug-in Type

When you are configuring the Access Gateway, you can choose how clients log on: using Access Gateway Plug-in for Windows, Access Gateway Plug-in for Mac OS X, or Access Gateway Plug-in for Java.

Configuration is completed using a session policy and then bound to users, groups, virtual servers, or globally.

## To configure a session policy for client connections

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Do one of the following:
  - If you are creating a new session policy, under Related Tasks, click Create new session policy.
  - If you are changing an existing policy, select a policy and under Related Tasks, click Modify session policy.
5. Create a new profile or modify an existing profile. To do so, do one of the following:
  - Next to Request Profile, click New.
  - Next to Request Profile, click Modify.
6. On the Client Experience tab, next to Plug-in Type, click Override Global and select Windows/Mac OS X.
7. Do one of the following:
  - If you are creating a new profile, click Create, set the expression in the policy dialog box, click Create, and then click Close.
  - If you are modifying an existing profile, after making the selection, click OK twice

## To set the interception mode for the Access Gateway Plug-in for Windows

If you are configuring the Access Gateway Plug-in, you also need to configure the interception mode and set it to transparent.

1. In the configuration utility, in the navigation pane, click Access Gateway.

## Selecting the Plug-in Type

---

2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Intranet Applications.
4. Under Related Tasks, click Create new intranet application.
5. In Name, type a name for the policy.
6. Under Options, next to Interception Mode, select Transparent.
7. In Protocol, select ANY.
8. Under Destination, click Specify an IP Address and in IP address type the IP address.
9. In Netmask, type the subnet mask, click Create, and then click Close.

---

# Configuring the Access Gateway Plug-in for Windows or Mac OS X

You can configure the Access Gateway Plug-in either globally or using a session policy on the Access Gateway. If you create a session policy, you can bind it to a user, group, virtual server, or globally.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. Next to Plug-in Type, select Windows/Mac OS X and click OK.

To configure a session policy, see [To configure a session policy for client connections](#).

---

# Installing the Access Gateway Plug-in

When users log on to the Access Gateway, the Access Gateway Plug-in is downloaded and installed on the user device.

To install the plug-in, users must be a local administrator or a member of the Administrators group to install programs on their device. This restriction applies for first-time installation only, not for upgrades.

To enable users to connect to and use the Access Gateway, you need to provide them with the following information:

- Access Gateway Web address, such as *https://AccessGatewayFQDN/*
- Path to any network drives that the users can access, which is done by mapping a network drive on the user device
- Any system requirements for running the Access Gateway Plug-in if you configured endpoint resources and policies

Depending on the configuration of a user device, you might also need to provide additional information:

- If a user runs a firewall on their computer, the user might need to change the firewall settings so that it does not block traffic to or from the IP addresses corresponding to the resources for which you granted access. The Access Gateway Plug-in automatically handles Internet Connection Firewall in Windows XP and Windows Firewall in Windows XP Service Pack 2, Windows Vista or Window 7.
- Users who want to send traffic to FTP over the Access Gateway connection must set their FTP application to perform passive transfers. A passive transfer means that the remote computer establishes the data connection to your FTP server, rather than your FTP server establishing the data connection to the remote computer.
- Users who want to run X client applications across the connection must run an X server, such as XManager, on their computers.

Because users work with files and applications just as if they were local to the organization's network, no retraining of users or configuration of applications is needed.

To establish a secure connection for the first time, log on to the Access Gateway using the Web logon page. The typical format of a Web address is *https://companyname.com*. When users log on, they can install the Access Gateway Plug-in on their computer.

## To install the Access Gateway Plug-in

1. In a Web browser, type the Web address of the Access Gateway.
2. Type the user name and password and click Logon.
3. Select Network Access and then click Download.
4. Follow the instructions to install the plug-in.

When the download is complete, the Access Gateway Plug-in connects and displays a message in the notification area.

If you want users to connect using the Access Gateway Plug-in without using a Web browser, you can configure the plug-in to display the logon dialog box when you click the icon on your desktop. Users can also right-click the Access Gateway icon in the notification area on a Windows computer.

## To configure logon using the Access Gateway Plug-in

Users must be logged on to complete this procedure.

1. On a Windows computer, in the notification area, right-click the Access Gateway icon and click Configure Access Gateway.
2. Click the Profile tab and then click Change Profile.
3. On the Options tab, click Use the Access Gateway Plug-in for logon.

Users can log on by double-clicking the Access Gateway icon on the desktop or by right-clicking the Access Gateway icon in the notification area.

---

# Deploying the Access Gateway Plug-in from Active Directory

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

When you deploy the Access Gateway Plug-in using this method, you can extract the installation program and then deploy it using a group policy. The general steps for this type of deployment are:

- Extracting the MSI package
- Distributing the plug-in using a group policy
- Creating a distribution point
- Assigning the Access Gateway Plug-in package using a Group Policy Object

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

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

## To download the Access Gateway Plug-in MSI package from the configuration utility

1. In the configuration utility, click Downloads.
2. Under Citrix Access Gateway Plugin, click Download Access Gateway Plugin for Windows and save the file `nsvpnc_setup.exe` to your Windows server.

**Note:** If the File Download dialog box does not appear, press the CTRL key when you click the link Download Access Gateway Plugin for Windows.

3. At a command prompt navigate to the folder that you saved `nsvpnc_setup.exe` to and type:

```
nsvpnc_setup /c
```

This extracts the file `agee.msi`.

4. Save the extracted file to a folder on the Windows server.

After the file is extracted, you want to distribute the file using a group policy on Windows Server 2003.

Before starting the distribution, install the Group Policy Management Console on Windows Server 2003. For more information, see the Windows online help.

**Note:** When you are publishing the Access Gateway Plug-in using a group policy, Citrix recommends assigning the package to the user device. The MSI package is designed to be installed on a per-device basis.

Before you can distribute the software, create a distribution point on a network share on a publishing server, such as Microsoft Internet Security and Acceleration (ISA) Server.

## To create a distribution point

1. Log on to the publishing server as an administrator.
2. Create a folder and share it on the network with read permission for all accounts that need access to the distribution package.
3. At a command prompt, navigate to the folder where the extracted file is and type:  
`msiexec -a agee.msi`
4. On the Network Location screen, click Change and navigate to the shared folder where you want to create the administrative installation of the Access Gateway Plug-in. Click OK and click Install.

After you have put the extracted package on the network share, assign the package to a Group Policy Object in Windows.

When the Access Gateway Plug-in is successfully configured as a managed software package, it is installed automatically the next time the user device starts.

**Note:** When the installation package is assigned to a computer, restarting the computer is required.

When the installation starts, users receive a message that the Access Gateway Plug-in is installing.



---

# Upgrading and Removing the Access Gateway Plug-in for Active Directory

Each release of the Access Gateway Plug-in is packaged as a full product installation, instead of as a patch. When a new version of the Access Gateway is detected, the Access Gateway Plug-in upgrades automatically. The automatic upgrade occurs only when users log on to the Access Gateway. You can deploy the Access Gateway Plug-in to upgrade using Active Directory. For more information, see [Deploying the Access Gateway Plug-in from Active Directory](#).

To do so, create a new distribution point of the Access 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. When this link is created, the Access Gateway Plug-in is updated.

## Removing the Access Gateway Plug-in from Client Devices

To remove the Access Gateway Plug-in from client 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 client is uninstalling.

---

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

If the assigned package fails to install when the user device starts, you might see the following warning in the application event log:

```
Failed to apply changes to software installation settings. Software installation policy application has been delayed until the next logon because an administrator has enabled logon optimization for group policy. The error was: The group policy framework 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.

---

# Monitoring and Ending User Sessions

You can use the configuration utility to monitor user sessions. You can determine the user device IP address and port, the virtual server to which users are logged on, and the destination port.

You can also use the configuration utility to end user sessions. When you end a session, the user cannot connect to resources in the secure network.

## To end a user session

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Click Active Users.
4. Under Sessions, select a user, click Terminate and then click Close.

## To terminate user session based on IP addresses

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Click Intranet IP.
4. In Intranet IP, type the IP address and in Netmask, type the subnet mask.
5. Click Terminate and then click Close.

---

# Configuring Access to Applications and Virtual Desktops in the Web Interface

You can configure Access Gateway to provide users access to published applications and virtual desktops with the Access Gateway Plug-in instead of with Receiver. To configure access to applications and desktops, you change the configuration on Access Gateway from using Receiver only to connect to Access Gateway, to a configuration that enables connections by using the Access Gateway Plug-in with single sign-on to the Web Interface. For example, you configure Access Gateway so that all users connect with the Access 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 Access Gateway.
- Configure policies and filters on Citrix XenApp and XenDesktop.
- Configure Access Gateway so users log on by using the Access 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 Policies](#)
- [Configuring XenApp Policies and Filters](#)
- [To configure policies and filters in XenDesktop 5](#)
- [Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface](#)

When configuring user logon to XenApp and XenDesktop, you first create a session profile to select the Access 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 Access Gateway Plug-in for access to applications and desktops

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Published Applications tab, next to ICA Proxy, select OFF.
4. In Web Interface Address, type the URL of the Web Interface site. This becomes the home page for users.
5. In Single Sign-On Domain, type the Active Directory domain name.
6. On the Client Experience tab, next to Plug-in Type, select Windows/Mac OS X and then click OK.

## To configure the intranet application

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. in the details pane, under Resources, click Intranet Applications.
3. In the right pane, click Add.
4. In Name, type a name for the application.
5. Under Options, next to Interception Mode, select Transparent.
6. In Protocol, select the TCP, UDP, or Any.
7. In Destination Type, click Specify an IP Address and Netmask, type the IP address and subnet mask that represents your internal network, click Create and then click Close. 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.

## To bind an intranet application globally

1. Click Access Gateway > Global Settings.
2. In the details pane, under Intranet Applications, click Create mappings to TCP applications in the secure network for the Access Gateway Plug-in for Java.
3. In the Bind Intranet Applications dialog box, under Available Intranet Applications, select the intranet application, click Add and then click OK.

## To bind an intranet application to a virtual server

1. Click Access Gateway > Virtual Servers.
2. In the details pane, select a virtual server and then click Open.
3. In the Configure Access Gateway Virtual Server dialog box, click the Intranet Applications tab.
4. Under Available Application Name, select the intranet applications, click Add and then clickOK.

When users log on with the Access Gateway Plug-in, the VPN tunnel is established and the Web Interface is used as the home page.

---

# Connecting Using the Access Gateway Plug-in for Java

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

**Note:** Java Runtime Environment (JRE) 1.4.2 and above is required for the following operating systems and Web browsers.

- Mac OS X
- Linux
- Windows XP (all versions), Windows Vista, and Windows 7
- Internet Explorer
- Firefox
- Safari 1.2 or later

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

Users do not require administrative privileges on the user device to use the Access 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 the Access Gateway to install the Access 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 Windows 7 computer, the proxy server information is not set automatically in Internet Explorer. Users must manually configure the proxy server on Windows 7.

## To configure the Access Gateway Plug-in for Java

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Select a policy and then under Related Tasks, click Modify session policy.
5. Next to Request Profile, click Modify.
6. Next to Plug-in Type, click Override Global, select Java, and click OK twice.

## To set the interception mode

After creating the session policy, create an intranet application to define the interception mode for users logging on using the Access Gateway Plug-in for Java.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Intranet Applications.
4. Under Related Tasks, click Create new intranet application.
5. In Name, type a name.
6. Under Options, next to Interception Mode, select Proxy.
7. Under Destination, in IP Address, type the IP address.
8. In Port, type the port number, click Create, and click Close.

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

## Updating the HOSTS File in Windows Vista and Windows 7

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

1. Click Start > All Programs.



2. Click Accessories, right-click Notepad and then click Run as administrator. If you are prompted for an administrator password or for a confirmation, type the password or click Allow.
3. Open the HOSTS file and add the mapping entries for the intranet application for the Access Gateway Plug-in for Java and save the file.

---

# How Clientless Access Works

Clientless access allows users the access they need without installing client software, such as the Access Gateway Plug-in. Users can use their Web browser to connect to Web applications such as Outlook Web Access

Clientless access is configured using the following steps:

- Enabling clientless access either globally or 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 enable it using a session policy.

If you use the Access 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 Access Gateway wizard, you can configure the following client connection methods:

- Access Gateway Plug-in. Users are allowed to log on using the Access Gateway Plug-in only.
- Use the Access Gateway Plug-in and allow access scenario fallback. Users log on to the Access Gateway using the Access 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 using clientless access and they receive limited access to network resources.

---

# Enabling Clientless Access

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

In 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 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 the Web Interface, users log on with the Access 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 Access Gateway wizard, you can enable it globally by using the configuration utility. You can also configure clientless access in a session by using the Access Gateway Policy Manager.

## To enable clientless access globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access, select ON and then click OK.

## To enable clientless access by using a session policy

If you want only a select group of users, groups, or virtual servers to use clientless access, disable or 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.

3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Client Experience tab, next to Clientless Access, click Override Global, select On 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.
10. 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

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 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. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access URL Encoding, select the encoding level and then click OK.

## To configure Web address encoding by creating a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Client Experience tab, next to Clientless Access URL Encoding, click Override Global, select the encoding level and then click OK.
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.

---

# How Clientless Access Policies Work

Clientless access to Web applications is configured using policies. You can configure the settings for a clientless access policy in the Access Gateway Policy Manager or from the configuration utility. A clientless access policy is composed of a rule and a profile.

Three default clientless access policies are included with the Access Gateway. The first policy is a preconfigured policy for Outlook Web Access. The second is the default policy for all other Web applications. The third is a policy for SharePoint 2007. These policies are configured automatically and cannot be changed. In addition, each policy is bound at the global level and is not enforced unless clientless access is enabled either globally or using a session policy.

The global bindings for the default clientless access policies cannot be removed or modified, even if clientless access is not enabled. The default policies are bound only at the global level. If you want to bind clientless access policies to a virtual server, create a new policy and then bind it. Custom clientless access policies can be bound either globally or to a virtual server.

To enforce different policies for clientless access at either the virtual server or global levels, change the priority number of the custom policy so it has a lower number than the default policies. If no other clientless access policies are bound to the virtual server, the default global policies take precedence.

**Note:** The priority numbers of the default clientless access policies cannot be changed.

---

# Creating New Clientless Access Policies

If you want to use the same settings as the default clientless access policies but bind the policy to a virtual server, you can copy the default policies, providing a new name for the policy. Citrix recommends copying the default policies using the Access Gateway Policy Manager.

When the new policy is bound 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Clientless Access Policies and click a default policy.
4. Under Related Tasks, click Create new clientless access policy.
5. 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

When the new policy is created, bind it to the virtual server.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Virtual Servers and expand the node for a virtual server.
4. Under Available Policies / Resources, expand Clientless Access Policies, click the new policy, and drag it to Clientless Access Policies in the virtual server node.
5. In the Modify Priority dialog box, in Priority, type a priority number and 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Clientless Access Policies.
4. Under Related Tasks, click Create new clientless access policy.
5. In Name, type a name for the policy.
6. Next to Profile, click New.
7. In Name, type a name for the profile.
8. Configure the rewrite settings and click Create.
9. In the Create Clientless Access Policy dialog box, under Expression, click Add.
10. In the Add Expression dialog box, create the expression and click OK.
11. In the Create Clientless Access Policy dialog box, click Evaluate, and if the expression tests as correct, click Create.

---

# Configuring Domain Access for Users

If users connect using clientless access, you can restrict the network resources, domains, and Web sites they are permitted to access. You can use the Access 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.

If you configure clientless access policies for CloudGateway and users connect with Receiver for Web, you need to allow the domains that Receiver for Web can access. This is required so Access Gateway can rewrite network traffic for StoreFront and AppController.

## To configure domain access by using the Access Gateway wizard

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Getting Started, click Access 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 using the Access Gateway wizard.

## To configure domain settings by using the configuration utility

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

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

---

# Configuring Clientless Access for SharePoint 2003 and SharePoint 2007

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

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

In the Access 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 Access Gateway wizard, you use the configuration utility.

## To configure clientless access for SharePoint by using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Clientless Access, click Configure Clientless Access for SharePoint.
3. Under Clientless Access for SharePoint, in Host name of 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

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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Client Experience tab, next to Home Page click Override Global and then type the name of the SharePoint site.
9. Next to Clientless Access, click Override Global, select On and then click Create.
10. 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

SharePoint 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), the Access Gateway is not able to 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 the Access Gateway so that the SharePoint host name is converted to an FQDN before name resolution
- Configure a local DNS entry on the Access Gateway for every SharePoint server name
- Change all the SharePoint server names to use the FQDN, such as *SharePoint.intranetdomain* instead of just SharePoint

## To configure a DNS suffix

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

## To configure a local DNS record for every SharePoint server name on the Access Gateway

1. In the configuration utility, in the navigation pane, expand DNS > Records and 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. Under IP Address, in Enter a valid IP Address and click on Add 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

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. Access 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 Access 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.

For more information about configuring persistent cookies globally, see [To configure persistent cookies globally](#). For more information about configuring persistent cookies as part of a session policy, see [To configure persistent cookies as part of a session policy](#).

---

# Configuring Persistent Cookies for Clientless Access for SharePoint

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

## To configure persistent cookies globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access Persistent Cookies, select an option and then click OK.

## To configure persistent cookies as part of a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Client Experience tab, next to Clientless Access Persistent Cookies, click Override Global, select an option and then click Create.
9. 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

When users log on and log off from the Web Interface by using clientless access, Access 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, expand Access Gateway > Policies and then click Clientless Access.
2. In the right pane, 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 Access Gateway command line by using a Secure Shell (SSH) connection.
2. At a 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

You can configure the Access Gateway to provide users with multiple logon options. With client choices, users have the option of logging on using the Access Gateway Plug-in for Windows, Access Gateway Plug-in for Java, the Web Interface, or clientless access from one location.

Users log on to the Access Gateway using the Web address of the Access Gateway or virtual server. Using a session policy and profile, you can determine the logon choices users receive. Depending on how the Access Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Access Gateway Plug-in for Windows, Web Interface, and clientless access.

If users select the Access Gateway Plug-in to log on, a Web page appears and installation of the plug-in starts. After the plug-in is installed, users can log on using the icon located in the notification area or on the desktop.

If users select the Web Interface to log on, the Web Interface page appears. Users can then access their published applications.

If users select clientless access to log on, the Access Interface or your customized home page appears. On the Access Interface, users can navigate to file shares, Web sites, and use Outlook Web Access.

If users select the Access Gateway Plug-in for Java, the plug-in starts and users are logged on.

For more information about configuring client choices, see [Choosing the User Access Method](#).

---

# Showing the Client Choices Page at Logon

With the client choices option, users can log on using the Access Gateway Plug-in, the Web Interface, or clientless access from one Web page after successful authentication to the Access Gateway. Users are presented with icons and can choose which method they want to use to establish a connection. You can also configure the Access Gateway Plug-in for Java to appear on the choices page.

Client choices can be used without using endpoint analysis or implementing access scenario fallback. If a client security expression is not defined, users receive connection options for the settings that are configured on the Access 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 log on using clientless access.

Client choices are configured either globally or 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. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced.
4. On the General tab, click Client Choices and click OK twice.

## 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.

4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Client Experience tab, click Advanced.
9. On the General tab, next to Client Choices, click Override Global, click Client Choices, click OK, and then click Create.
10. 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

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 Access Gateway Plug-in, 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. In the configuration utility, in the navigation pane, expand Access Gateway and click Groups.
2. In the details pane, click Add.
3. In Group Name, type the name of the group.
4. On the Users tab, select the users, click Add for each one, click Create and then click Close.

The following procedure is an example session profile for client choices with the Access Gateway Plug-in, Web Interface, and clientless access.

## To create a session profile for client choices

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
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:
  - a. Next to Home Page, click Override Global and then clear Display Home Page. This disables the Access Interface.
  - b. Next to Clientless Access, click Override Global and then select OFF.
  - c. Next to Plug-in Type, click Override Global and then select Windows/Mac OS X.
  - d. Click Advanced and next to Client Choices, click Override Global, click Client Choices and then click OK.
5. On the Security tab, next to Default Authorization Action, click Override Global and then select ALLOW.
6. On the Security tab, click Advanced.
7. Under Authorization Groups, click Override Global, select the group, click Add and then click OK.
8. On the Published Applications tab, do the following:
  - a. Next to ICA Proxy, click Override Global and then select OFF.
  - b. Next to Web Interface Address, click Override Global and then type the Web address of the Web Interface, such as `http://ipAddress/Citrix/`.
  - c. Next to Web Interface Portal Mode, click Override Global and then select COMPACT.
  - d. Next to Single Sign-On Domain, click Override Global and then type the name of the domain.
9. Click Create and then click Close.

If you want to use the Access 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. For more information about the interception mode, see [To set the interception mode](#).

After creating the session profile, create a session policy. Within the policy, select the profile, and set the expression to True value.

To use the Web Interface as a client choice, you must also configure the Secure Ticket Authority (STA) on the Access Gateway. The STA is bound to the virtual server.

**Note:** If the server running the Web Interface is not available, the Citrix XenApp choice does not appear on the choices page.

## To configure and bind the STA to a virtual server

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers and then expand a virtual server node.
4. Click STA Servers.
5. Under Related Tasks, click Bind new STA server.
6. In URL, type the IP address or URL of the server running the STA and then click Create.

**Note:** The IP address or URL must match what is configured in the Web Interface.



---

# Configuring Access Scenario Fallback

SmartAccess allows the Access 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 Access Gateway Plug-in to the Web Interface (using Citrix online plug-ins) if the user device does not pass the initial endpoint analysis scan.

To enable access scenario fallback, you configure a post-authentication policy that decides whether or not users receive an alternative method of access when logging on to the Access Gateway. This post-authentication policy is defined as a client security expression that is configured either globally or as part of a session profile. If you are configuring a session profile, it is associated to a session policy that is then bound to users, groups, virtual servers, or global. When this is enabled, the Access 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 using the Web Interface only
- If clientless access and client choices are disabled, users can be quarantined into a group that provides access only to the Web Interface
- If clientless access and the Web Interface are enabled on the Access Gateway and ICA proxy is disabled, users fall back to clientless access
- If the Web Interface 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 and published applications

---

# Creating Policies for Access Scenario Fallback

To configure Access 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 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.
- 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 Access Gateway Plug-in or the Web Interface.

**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. When you configure both home pages, the Access Interface home page takes precedence for the Access Gateway Plug-in and the Web Interface home page takes precedence for Web Interface users.

## To create a quarantine group

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Groups.
2. In the details pane, click Add.
3. In Group Name, type a name for the group, click Create, and then click Close.

**Important:** The name of the quarantine group must not match the name of any domain group to which users might belong. If the quarantine group matches an Active Directory group name, users are quarantined even if the user device passes the endpoint analysis security scan.

After creating the group, configure Access Gateway to fall back to the Web Interface if the user device fails the endpoint analysis scan.

## To configure the Web Interface for quarantined user connections

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. In the Global Access 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 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.

## To create a session policy for Access Scenario Fallback

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
2. In the details pane, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. On the Published Applications tab, next to ICA Proxy, click Override Global, select On and then click Create.
6. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.

After creating the session policy, bind the policy to a quarantine group.

## To bind the session policy to the quarantine group

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Groups.
2. In the details pane, select a group and click Open.
3. On the Policies tab, click Insert Policy.
4. Under Policy Name, select the policy and then click OK.

After creating the session policy and profile enabling the Web Interface on Access Gateway, create a global client security policy.

## To create a global client security policy

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Security tab, click Advanced.
4. Under Client Security, click New.
5. In the Create Expression dialog box, next to Match Any Expression, click Add, configure the client security expression and then click Create.
6. In Quarantine Group, select the group you configured in the group procedure and then click OK twice.

---

# Using the Repeater Plug-in

When users log on using the Access Gateway Plug-in, the connection can be optimized using the Repeater Plug-in. When the connection is optimized, network traffic is compressed and accelerated through the Access Gateway. When Branch Repeater is enabled for a connection, TCP compression policies on the Access Gateway are disabled.

The Repeater Plug-in is deployed and works with the Access Gateway Plug-in.

The Access Gateway supports Version 4.3.26 or later of the Repeater Plug-in.

Branch Repeater optimization and flow control take precedence over Access Gateway optimization features that require dynamic content modification. If Branch Repeater optimization is enabled for HTTP traffic, these Access Gateway features are not available:

- Single sign-on to Web applications
- File type association
- HTTP authorization

Network traffic destined for a configured HTTP port on the Access Gateway is excluded automatically from Branch Repeater optimization. This is the default setting. If you configure a traffic policy for Branch Repeater optimization on an HTTP port, the traffic policy is honored and the network traffic is optimized by Branch Repeater. However, the Access Gateway optimization features are disabled for all traffic affected by that policy. Network traffic destined for non-HTTP ports can be accelerated by Branch Repeater without affecting other Access Gateway features.

Configuring client connections to use the Repeater Plug-in is accomplished using a traffic policy and can be bound to users, groups, virtual servers, or globally. The policy is prioritized based on where it is bound or by the priority number.

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Traffic.
2. In the details pane, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. In Branch Repeater, select ON and click Create.
7. In the Create Traffic Policy dialog box, next to Add Expression, select or enter an expression that represents the traffic types for which Branch Repeater acceleration should be enabled, 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 Branch Repeater is configured to accelerate. For Branch Repeater acceleration to occur, the traffic types configured on the Access Gateway must match the Service Class Policies configured on Branch Repeater.

All TCP traffic benefits from Branch Repeater acceleration. If you are planning to use single sign-on, do not accelerate HTTP traffic since the acceleration disables single sign-on.

After creating the policy, bind it to a user, group, virtual server, or globally.

---

# Managing User Sessions

You can manage user sessions in the configuration utility with the Active Access Gateway Users and Connections dialog box. This dialog box displays a list of active user sessions on the Access Gateway.

You can end user or group sessions in this dialog box 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 client device
- Port number of the client device
- IP address of the virtual server
- Port number of the virtual server
- Intranet IP address assigned to the user

## To view user sessions

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. View the list of sessions under Active connections between the client and Appliance.

## To refresh the session list

You can retrieve updated information about sessions to the Access Gateway.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Click Refresh.

## To end user or group sessions

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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Under To end session(s), select a user or group from the list and click on the [Terminate] button, do one of the following:
  - To terminate a user session, click Active Users, select a user, and click Terminate User
  - To terminate a group session, click Active Groups, select a group, and click Terminate Group

## To end a session using an intranet IP address

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Monitor Connections, click Active user sessions.
3. Under To end session(s), enter Intranet IP and/or netmask and click on [Terminate] button, next to Intranet IP, type the IP address.
4. In Netmask, type the subnet mask and click Terminate.



---

# Configuring Connections for the Access Gateway Plug-in

Client connections are configured by defining the resources users can access in the internal network. Configuring client connections includes:

- Defining the domains to which users are allowed access
- Configuring IP addresses for users, including IP pooling
- Configuring time-out settings
- Configuring single sign-on
- Configuring client interception
- Configuring split tunneling
- Configuring connections through a proxy server
- Configuring client software to connect through the Access Gateway

Most client connections are configured using a profile that is part of a session policy. You can also define client connection settings using intranet applications, preauthentication and traffic policies.

---

# Connecting to Internal Network Resources

The Access Gateway can be configured for users to access resources in the internal network. If split tunneling is disabled, all client traffic is sent to the Access Gateway and authorization policies determine whether the traffic is allowed to pass through to internal network resources. When split tunneling is enabled, only traffic destined for the internal network is intercepted by the client and sent to the Access Gateway. You configure which IP addresses are intercepted using intranet applications. If you are using the Access Gateway Plug-in for Windows, set the interception mode to transparent. If you are using the Access Gateway Plug-in for Java, set the interception mode to proxy.

When the interception mode is set 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, in the navigation pane, expand Access Gateway > Resources and click Intranet Applications.
2. In the details pane, click Add.
3. Complete the parameters for allowing network access, click Create and then click Close.

For more information about configuring specific settings for the Access Gateway Plug-in for Windows or Access Gateway Plug-in for Java, see [Configuring Client Interception](#).

---

# Enabling Proxy Support for User Connections

The user device can connect through a proxy server for access to internal networks. Access Gateway supports the HTTP, SSL, FTP, and SOCKS protocols. To enable proxy support for user connections, you specify the settings on Access Gateway. You can specify the IP address and port used by the proxy server on Access Gateway. The proxy server is used as a forward proxy for all further connections to the internal network.

## To configure proxy support for user connections

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced.
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 twice.

**Note:** If you select Appliance, you can configure only proxy servers that support secure and unsecure HTTP connections.

After you enable proxy support on Access Gateway, you specify configuration details on the user device for the proxy server that corresponds to the protocol.

After you enable proxy support, Access 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 Access Gateway, the user device can communicate with the proxy server directly for connection to the user's network.

## To configure one proxy server to use all protocols for Access Gateway

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

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced.

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 twice.

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.

Access Gateway makes connections to the proxy server on behalf of the user device. The proxy settings are not propagated to the user's browser, so no direct communication between the user device and the proxy server is possible.

## To configure the Access Gateway to be a proxy server

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

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced.
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 twice.

---

# Configuring Time-Out Settings

You can configure the Access Gateway Plug-in to force a disconnection with Access Gateway 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, the Access Gateway Plug-in disconnects 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. The default setting is 30 minutes. If you set this value to zero, the setting is disabled.
- **Session time-out.** The duration after which Access Gateway terminates an idle session. The default setting is 30 minutes. If you set this value to zero, the setting is disabled.
- **Idle session time-out.** If you enable this setting, the user session times out if there is no mouse or keyboard activity on the user device for the specified interval. The default time-out 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 using a session profile. When you add the profile to a session policy, the policy is then bound to a user, group, virtual server, or globally. If you want to configure user time-out settings globally, use the configuration utility. When you configure the time-out settings globally, the settings are applied to all user sessions.

---

# Configuring Forced Time-Outs

A forced time-out disconnects the Access 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.

## To configure a global forced time-out

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, click Advanced.
4. Under Timeouts, 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 twice.

## To configure a forced time-out within a session policy

If you want to have further control over who receives the forced time-out, create a session policy and then apply the policy to a user or group.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. On the Network Configuration tab, click Advanced.
9. Under Timeouts, click Override Global and in Forced Time-out (mins) type the number of minutes users can stay connected.
10. 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 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 Session or Idle Time-Outs

You can also configure session and client time-out settings globally using the configuration utility. To apply these values to a user, group, or virtual server use the Access Gateway Policy Manager and create a session policy and profile, setting the expression to true.

## To configure a session or client idle time-out globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. Do one or both of the following:
  - On the Client Experience tab, in Session Time-out (mins), type the number of minutes
  - In Client Idle Time-out (mins), type the number of minutes and click OK



## To configure session or client idle time-out settings using a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Do one or both of the following:
  - On the Client Experience tab, next to Session Time-out (mins), click Override Global and then type the number of minutes
  - Next to Client Idle Time-out (mins), click Override Global, type the number of minutes, and 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.

---

# Configuring Single Sign-On

You can configure Access 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 are users access through the file transfer utility in the Access Interface or from the Access 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

Users open a connection by starting the Access Gateway Plug-in from the desktop. You can specify that the Access 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 Access Gateway for authentication. Enabling single sign-on for the Access Gateway Plug-in facilitates operations on the user device, such as installation scripts and automatic drive mapping.

Enable single sign-on only if user devices are logging on to your organization's domain. If single sign-on is enabled and a user connects from a device that is not on your domain, the user is prompted to log on.

You configure single sign-on with Windows either globally or by using a session profile that is attached to a session policy.

## To configure single sign-on with Windows globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Single Sign-on with Windows and then click OK.

## To configure single sign-on with Windows by using a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. 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.
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 Single Sign-on to Web Applications

You can configure Access 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 Access 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 Access Gateway or an external authentication server, users are redirected to the specified home page. User credentials are passed transparently to the Web server. If the Web server accepts the credentials, users are logged on automatically. If the Web server denies the credentials, users receive an authentication prompt asking for their user name and password.

You can configure single sign-on to Web applications globally or by using a session policy.

## To configure single sign-on to Web applications globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Single Sign-on to Web Applications and then click OK.

## To configure single sign-on to Web applications by using a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies and then select a session policy.
4. Under Related Tasks, click Modify session policy.
5. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
6. On the Client Experience tab, next to Single Sign-On to Web Applications, click Global Override, click Single Sign-On to Web Applications and then click OK.

## To define the HTTP port for single sign-on to Web applications

Single sign-on is attempted only for network traffic where the destination port is considered an HTTP port. To allow single sign-on to applications that use a port other than port 80 for HTTP traffic, add one or more port numbers on Access Gateway. You can enable multiple ports. The ports are configured globally.

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, click Advanced.
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 Access 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 Using LDAP

When single sign-on is configured and users log on using the user principal name (UPN) with a format of *username@domain.com*, by default single sign-on fails and users must authenticate twice. If you need to use this format for user logon, modify the LDAP authentication policy to accept this form of user name.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Authentication Policies, and select the authentication policy.
4. Under Related Tasks, click Modify authentication policy.
5. In the Configure Authentication Policy dialog box, next to Server, click Modify.
6. Under LDAP Server Information, in Base DN (location of users), type `DC=domainname, DC=com`.
7. In Administrator Bind DN, type `LDAPaccount@domainname.com`, where *domainname.com* is the name of your domain.
8. In Administrator Password and Confirm Administrator Password, type the password.
9. In Server Logon Name Attribute, type `UserPrincipalName`.
10. In Group Attribute, type `memberOf`.
11. In Sub Attribute Name, type `CN`.
12. In SSO Name Attribute, type the format of how users logon and click OK twice. This value is either `SamAccountName` or `UserPrincipleName`.

---

# Configuring Single Sign-On to a Domain

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.

## To configure single sign-on to a domain

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Session Policies and then select the policy for your published applications.
4. Under Related Tasks, click Modify session policy.
5. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
6. 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 Access Gateway with XenApp, see [Providing Access to Published Applications](#).



---

# Configuring Client Interception

You configure interception rules for user connections on Access 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 either the configuration utility or the Access Gateway Policy Manager. You can bind intranet applications to users, groups, or virtual servers.

If you enable split tunneling and users connect by using @WorkWeb™ or @WorkMail™, when you configure client interception you must add the IP addresses for AppController and your Exchange server. If you do not enable split tunneling, you do not need to configure the AppController and Exchange IP addresses in Intranet Applications.

---

# Configuring Intranet Applications for the Access Gateway Plug-in

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 Access Gateway, the Access Gateway Plug-in for Windows intercepts user traffic that is destined to the resource and sends the traffic through Access 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 Access Gateway with the Access Gateway Plug-in for Windows
  - Split tunneling is disabled
- If users connect to Access Gateway using the Access Gateway Plug-in for Java, you must define intranet applications. The Access 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 Access Gateway Plug-in for Windows and Access Gateway Plug-in for Java, configure two intranet application policies and bind the policies to the user, group, virtual server, or Access Gateway global.

## To create an intranet application for one IP address

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Intranet Applications.
4. Under Related Tasks, click Create new intranet application.
5. In Name, type a name for the profile.
6. Under Options, next to Interception Mode, select Transparent.
7. In Protocol, select the protocol that applies to the network resource.
8. Under Destination, click Specify an IP Address and Netmask.
9. In IP Address, type the IP address and in Netmask, type the subnet mask, click Create and then click Close.

## To configure an IP address range

If you have multiple servers in your network, such as Web, email, and file shares, you can configure a network resource that includes the IP range for network resources. This setting allows users access to the network resources contained in the IP address range.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Intranet Applications.
4. Under Related Tasks, click Create new intranet application.
5. In Name, type a name for the profile.
6. Under Options, next to Interception Mode, select Transparent.
7. In Protocol, select the protocol that applies to the network resource.
8. Under Destination, click Specify an IP Address Range.
9. 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 Access Gateway Plug-in for Java

If clients are using the Access Gateway Plug-in for Java to connect, an intranet application must be configured and set to proxy interception. The client software intercepts traffic by using the client device loopback IP address and port number specified in the profile.

If users are connecting from a Windows-based device, the Access 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, applications must be configured manually using the source IP address and port values specified in the intranet application profile.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Intranet Applications.
4. Under Related Tasks, click Create new intranet application.
5. In Name, type a name for the profile.
6. Under Options, next to Interception Mode, select Proxy.
7. Under Destination, in IP Address and Port, type the destination IP address and port.
8. Under Source, in IP Address and Port, type the source IP address and port.

**Note:** The source IP address should be set to the loopback IP address of 127.0.0.1. If an IP address is not specified, the loopback IP address is used. If a port value is not entered, the destination port value is used.

---

# Configuring Address Pools

In some situations, users who connect with the Access Gateway Plug-in need a unique IP address for Access 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, Access 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 Access Gateway to assign an internal IP address to users that connect to Access 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.

Access 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 Access 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.

- Access 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, Access Gateway reclaims the IP address from the user who is logged off from Access Gateway the longest.

If an address cannot be reclaimed and all addresses are actively in use, Access Gateway does not allow the user to log on. You can prevent this situation by allowing Access Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are unavailable.

---

# Configuring IP Pooling Using the Configuration Utility

IP pooling is configured using the configuration utility at the level to which you want to bind the policy. For example, if you want to create an IP address pool for a virtual server, configure the intranet IP addresses on that node. When the IP pool is configured, it is bound to the entity where it is configured.

## To configure IP pooling for a user, group or virtual server using the configuration utility

1. In the configuration utility, in the navigation pane, expand Access Gateway, and then click Users, Groups or Virtual Servers.
2. In the details pane, click a user, group, or virtual server and click Open.
3. On the Intranet IPs tab, in IP Address and Netmask, type the IP address and subnet mask; click Add.
4. Repeat Step 3 for each IP address you want to add to the pool and then click OK.

## To configure IP pooling globally using the configuration utility

You can also create an IP address pool and bind it globally on the Access Gateway using the configuration utility.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Intranet IPs, click To assign a unique, static IP Address or pool of IP Addresses for use by all client Access Gateway sessions, configure Intranet IPs.
3. In IP Address and Netmask, type the IP address and subnet mask and click Add.
4. Repeat Step 3 for each IP address you want to add to the pool and then click OK.

---

# Defining Address Pool Options

You can use a session policy or the global Access 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 Access Gateway, while disabling the use of intranet IP addresses for a particular group of users.

You can configure address pools by using a session policy in one of the following three ways:

- **Nospillover.** When you configure address pools and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- **Spillover.** When you configure address pools and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- **Off.** Address pools are not configured.

## To configure address pools

1. In the configuration utility, in the navigation pane, click **Access Gateway**.
2. In the details pane, under **Policy Manager**, click **Change group settings and user permissions**.
3. In the **Access Gateway Policy Manager**, under **Available Policies / Resources**, click **Session Policies**.
4. Under **Related Tasks**, click **Create new session policy**.
5. In **Name**, type a name for the policy.
6. Next to **Request Profile**, click **New**.
7. In **Name**, type a name for the profile.
8. On the **Network Configuration** tab, click **Advanced**.
9. Next to **Intranet IP**, click **Override Global** and then select an option.
10. 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**.
11. In the **Create Session Policy** dialog box, create an expression, click **Create** and then click **Close**.



## Using the Transfer Login Page

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

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

## Configuring a DNS Suffix

When a user logs on to Access Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the Access 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 Access Gateway, the record is removed from the DNS cache.

## To configure a DNS suffix

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies and select a session policy.
4. Under Related Tasks, click Modify session policy.
5. Next to Request Profile, click Modify.
6. On the Network Configuration tab, click Advanced.
7. Next to Intranet IP DNS Suffix, click Override Global, type the DNS suffix and then click OK three times.

---

# Configuring Split Tunneling

You can enable *split tunneling* to prevent the Access Gateway Plug-in from sending unnecessary network traffic to the Access Gateway.

When split tunneling is not enabled, the Access Gateway Plug-in captures all network traffic originating from a client device and sends the traffic through the VPN tunnel to the Access Gateway.

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

When the Access Gateway Plug-in starts, it obtains the list of intranet applications from the Access Gateway. The Access Gateway Plug-in examines all packets transmitted on the network from the client 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 Access Gateway Plug-in sends the packet through the VPN tunnel to the Access Gateway. If the destination address is not in a defined intranet application, the packet is not encrypted and the client routes the packet appropriately. When split tunneling is enabled, intranet applications define the network traffic that is intercepted.

**Note:** If users are going to connect to published applications in a server farm using Citrix online plug-ins, split tunneling does not need to be configured.

The Access Gateway also supports reverse split tunneling, which defines the network traffic that is not intercepted by the Access Gateway. If split tunneling is set to reverse, intranet applications define the network traffic that is not intercepted. When this is enabled, all network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through the Access 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 using the Access Gateway Plug-in, network traffic destined to a printer or another device within the wireless network is not intercepted.

For more information about intranet applications, see [Configuring Client Interception](#).

Split tunneling is configured as part of the session policy.

1. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies and select a session policy.
2. Under Related Tasks, click Modify session policy.
3. Next to Request Profile, click Modify.
4. On the Client Experience tab, next to Split Tunnel, select Global Override, select the option from the drop-down list and click OK twice.

## Configuring Split Tunneling and Authorization

When planning your Access 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. Split tunneling is set to on and intranet applications are not configured to send network traffic through the Access Gateway. When this type of configuration is on the Access Gateway, access to the resource is allowed, but the resources cannot be accessed.

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

---

# Configuring Name Service Resolution

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

## To add a DNS or WINS server within a session profile

1. In the configuration utility, in the navigation pane, expand Access Gateway, expand Policies and then click Session.
2. In the details pane, on the Profiles tab, select a profile and then click Open.
3. On the Network Configuration tab, do one of the following:
  - To configure a DNS server, next to DNS Virtual Server, click Override Global, select the server and then click OK twice.
  - To configure a WINS server, next to WINS Server IP, click Override Global, type the IP address and then click OK twice.

---

# Supporting VoIP Phones

When you install Access Gateway as a standalone appliance and users connect with the Access Gateway Plug-in, Access 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.

Access 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 Access 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 Access Gateway Plug-in for Java

You can configure the access level and the applications users are allowed to access in the secure network. If users are logged on using the Access 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 using the Access Gateway Plug-in for Java, there are two methods for accessing user applications:

- HOSTS File Modification Method
- SourceIP and SourcePort Method

## Accessing Applications using the HOSTS File Modification Method

When this method is used, the Access Gateway Plug-in for Java adds an entry that corresponds to the applications configured by the administrator 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 on the client device. If you are not logged on with administrator privileges, manually edit the HOSTS file adding the appropriate entries.

**Note:** On a Windows 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, such as from home. The IP address should be the localhost IP address, 127.0.0.1. In the HOSTS file, 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, test your connection. You can test your connection by opening a command prompt and connecting using Telnet. If users are employing a user device that is not within the secure network, log on to the Access 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 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 client device, configure the HOSTS file 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. 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

The Access Gateway includes a home page that is a Web page that appears after users log on. The default home page is called the *Access Interface*. The home page can be the Access Interface, the Web Interface, or a customized home page.

The Access Interface is used to provide links to Web sites, both internal and external, and links to file shares in the internal network. The Access Interface can be customized with the following:

- Changing the Access Interface
- Creating Access Interface links

Users can customize the Access Interface, adding their own links to Web sites and file shares. Users can also transfer files from the internal network to their device using the home page.

**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 Access 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

You use 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 a custom home page

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. 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.
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.

---

# Changing the Access Interface

You might want to direct users to a customized home page, rather than relying on the Access Interface. To do this, install the home page on Access Gateway and then configure the session policy to use the new home page. For more information about creating a session policy, see [Replacing the Access Interface with a Custom Home Page](#).

## To install a customized home page

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Customize Access Interface, click Upload the Access Interface.
3. To install the home page from a file on a computer in your network, in Local File, click Browse, navigate to the file and then click Select.
4. To use a home page that is installed on Access 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

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 and then 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 appear under Personal Web Sites and Personal File Shares.

## To create an Access Interface link

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Resources / Policies, click Bookmarks.
4. Under Related Tasks, click Create new bookmark.
5. In Name, type a name for the bookmark.
6. In Text to display, type the description of the link. The description appears in the Access Interface.
7. In Bookmark, type the Web address, click Create, and then click Close.

If clientless access is enabled, you can make sure that requests to Web sites go through the Access Gateway. For example, you added a bookmark for *http://www.agexternal.com*. In the Add Bookmark dialog box, you can click Use Access Gateway as a reverse proxy. When this check box is enabled, Web site requests go from the user device to the Access Gateway and then to the Web site. When this check box is disabled, requests go from the user device to the Web site. In addition, this check box works only if clientless access is enabled.

## To bind an Access Interface link

In the Access Gateway Policy Manager, under Available Policies / Resources, click a bookmark and drag-and-drop it to one, some, or all of the following locations:

- To bind a bookmark globally, under Configured Policies / Resources, expand Access Gateway Global and drop the book mark in Bookmarks.
- To bind the bookmark to a virtual server, under Configured Policies / Resources, expand Virtual Servers and then expand a virtual server node. Drop the bookmark in

### Bookmarks.

- To bind the bookmark to a group, under Configured Policies / Resources, expand Group and then expand a group node. Drop the bookmark in Bookmarks.
- To bind the bookmark to a user, under Configured Policies / Resources, expand Users and then expand a user node. Drop the bookmark in Bookmarks.

When the configuration is saved, 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 – Web site links or file share links.

---

# Configuring User Name Tokens in Bookmarks

You can configure bookmark and file share URLs using a special token, *%username%*. When users log on, the token is replaced with each users' logon name. For example, you create a bookmark for a folder as `\\EmployeeServer\%username%`. When Jack logs on, the file share URL is mapped to `\\EmployeeServer\Jack\`.

If you are using one authentication type, the user name replaces the token *%username%*.

If you are using double source 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.

---

# Configuring Distributed File System Links

A Distributed File System (DFS) link provides access to shared folders in a wide area network (WAN) and access to shared folders that are in different geographic locations.

A DFS namespace allows you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. This structure increases availability and connects users automatically to shared folders in the same Active Directory domain, instead of routing the folders over WAN connections.

DFS Replication keeps folders synchronized between servers. It replaces the File Replication Service (FRS) as the replication engine for DFS namespaces in a Windows Server 2008 domain.

Each DFS referral request is sent to the server. The DFS referral cache is not supported.

The DFS namespace has a root and many links and targets. The namespace starts with a root that maps to one or more root targets. Below the root are links that map to their own targets. The DFS root namespace can have one of the following formats:

- `\\ServerName\Root Name`. This is a standalone DFS namespace for which the configuration information is stored locally in the registry of the root server. This type of root is not fault tolerant: when the root is unavailable, the entire DFS namespace is inaccessible. You can make standalone DFS namespaces fault tolerant by creating the namespace on server clusters.
- `\\DomainName\Root Name`. The DFS namespace is stored in Active Directory. The path to access the root or a link starts with the host domain name. A domain-based DFS root can have multiple root targets, which offers fault tolerance and load sharing.

Access Gateway acts as a DFS client for the server. When users click a link in the Access Interface, Access Gateway contacts the server and the shared folders appear as bookmarks in the Access Interface.

## To create a DFS share bookmark in the Access Interface

1. In the configuration utility, in the navigation pane, expand Access Gateway > Resources and then click Bookmarks.
2. In the details pane, click Add.
3. In Name, type a name for the DFS share.
4. In Text to Display, type a descriptive title for the DFS share.
5. In Bookmark, type the server or domain name path to the shared folder, click Create and then click Close.

After you create the bookmark, you can then bind it to Access Gateway global, virtual servers, groups, or users. For more information, see [To bind an Access Interface link](#).

---

# Integrating Access Gateway Enterprise Edition with Citrix XenApp and Citrix XenDesktop

If you are a system administrator responsible for installing and configuring the Access Gateway, you can configure the appliance to work with Citrix XenApp and Citrix XenDesktop. It is assumed that the Access Gateway is connected to an existing network and that you have experience configuring that network.

To allow user connections to a server farm through the Access Gateway, you configure settings in the Web Interface and on the Access Gateway appliance.

The configuration steps assume that the Access Gateway is deployed as a standalone appliance and that users connect directly to the Access Gateway.



---

# Integrating Access Gateway with CloudGateway

You can configure Access Gateway to work with CloudGateway components. When you configure Access Gateway to work with AppController, you might need a specific Access Gateway build to configure features, as follows:

- Access Gateway 10, Build 54.7 works with AppController 1.1 and StoreFront 1.1.
- 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 71.6014.e works with AppController Versions 2.5 and 2.6
- Access Gateway 10, Build 73.5002.e works with AppController Versions 2.5 and 2.6

When you configure Access Gateway to work with AppController or StoreFront, you can use the Remote Access wizard to configure your settings. The Remote Access 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 AppController.

This section contains information about configuring connections from remote users through Access Gateway to your CloudGateway deployment.

## Integrating Access Gateway and AppController

If you deploy CloudGateway Enterprise in your network, you can allow user connections from remote users to AppController by integrating Access Gateway and AppController. This deployment allows users to connect to AppController to obtain their web, Software as a Service (SaaS) and iOS apps, along with documents from ShareFile. Users connect by using either Citrix Receiver or the Access Gateway Plug-in.

In this CloudGateway deployment, Access Gateway resides in the DMZ and AppController resides in the internal network.

To allow connections from remote users to AppController, you can use the Remote Access wizard in Access Gateway to configure the web address for AppController. The wizard configures the policies required for users to connect to AppController, which include authentication, session, and clientless access policies. For more information about the wizard, see [Configuring Access Gateway Settings with the Remote Access Wizard](#).

You can also configure connections to AppController by creating policies with the configuration utility, such as:

- One session policy to manage 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 Access 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 Access Gateway.

## Integrating Access Gateway and StoreFront

You can configure Access Gateway to work with StoreFront 1.1 and 1.2. Users can connect in one of the following ways:

- Clientless access and Receiver for Web
- Receiver for Windows
- Receiver for Mac
- Receiver for Android
- Receiver for iOS
- Access Gateway Plug-in

**Important:** The fully qualified domain name (FQDN) for StoreFront must be unique and different from the Access Gateway virtual server FQDN. You cannot use the same FQDN for StoreFront and the Access 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 AppController, making these resources available to users.

When you configure Access Gateway to connect to StoreFront, you configure the following:

- One session policy to manage 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 Access 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 Access Gateway.

## Configuring Policies for AppController and StoreFront

If you deploy AppController and StoreFront and you do not use the Remote Access wizard to configure settings, you need to configure the following policies. You can configure these policies for Access Gateway and AppController only, Access Gateway and StoreFront only, or a deployment that contains Access Gateway, AppController, and StoreFront.

- One session policy to manage Receiver connections to AppController 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 and Secure Browse to allow connections through Access 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 Access 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.

---

# How Access Gateway and CloudGateway Integrate

You can configure Access Gateway to work with CloudGateway. In this deployment, Access Gateway resides in the DMZ. AppController and StoreFront reside in the secure network. Access Gateway must have access to the same forest that AppController and StoreFront reside in.

When you configure user connections through Access Gateway to AppController or StoreFront, users can connect in the following ways:

- By using Receiver
- By using Access Gateway through a web browser and Receiver for Web
- By using Receiver for Android or Receiver for iOS. To enable this connection, you configure Secure Browse and clientless access in Access Gateway. For more information, see [Allowing Access from Mobile Devices](#).

Users can connect by using the following versions of Receiver and the following operating systems:

Receiver	Operating system
Receiver for Windows 3.2 and 3.3	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	Mac OS X Version 10.7 (Lion)
Receiver for iOS 5.5.1 and 5.6	iOS 5.1
Receiver for Android 3.0.67 and 3.1	Android 3.2

Users can connect through Access Gateway to CloudGateway by using the following methods:

- Connect to Receiver for Web by using the Access 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 Access 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 Access Gateway 10.

- Connect to CloudGateway by using Receiver for Windows by using native protocols. When users connect with clientless access to AppController 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 Access 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 AppController by using the Access Gateway Plug-in. You can use the Access Gateway Plug-in for Windows or Access Gateway Plug-in for Mac to connect to web applications hosted by CloudGateway.

Users can connect to StoreFront only by using the following connection methods:

- Connect to StoreFront by using email-based discovery. Access Gateway supports Accounts Services that allows users to connect by using an email address or the Access 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 Access 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 AppController through PNA Services is not supported for Receiver for Android or Receiver for iOS.

To allow users to connect with the Access Gateway Plug-in and access web applications from AppController 2.0, 2.5, 2.6 or App Controller 2.8 when you configure the application connector in AppController, 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 Access Gateway. For more information, see [Configuring Connections to Enterprise Web Applications Through Access Gateway](#).

To allow users to connect with the Access Gateway Plug-in and access web applications from AppController 1.1, you must also configure the VPN keyword for web applications in AppController. For more information, see *Configuring Parameters to Enable Connections Through Access Gateway* in AppController 1.1 documentation located in the Archive node. In this deployment, users must connect through StoreFront to access their applications in AppController.

---

# Configuring Access Gateway and CloudGateway

To enable communication from user devices to the secure network, you need to configure settings in Access Gateway and in CloudGateway. Citrix recommends running the Remote Access wizard to configure these settings, which include settings for AppController and StoreFront.

When you run the wizard, Access Gateway creates the virtual server and policies that are needed for user connections to CloudGateway. For more information about running the Remote Access wizard, see [Configuring Access Gateway Settings with the Remote Access Wizard](#). The Remote Access wizard configures the following policies automatically:

- Virtual server. When you configure a virtual server, you enable SmartAccess mode in the virtual server dialog box. 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 Access Gateway. If you do not install the Universal license, users cannot access Windows-based, web, SaaS, or mobile applications from Receiver for Web.
- Session policies bound to the virtual server. You create session policies in Access Gateway. You can create the following four session policies:
  - Two session policies manage Receiver 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 Receiver for Android or Receiver 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 Access Gateway Plug-in. You can also configure Account Services that allows email-based discovery of the StoreFront or Access Gateway web address.
- Authentication policies bound to the virtual server. You can configure LDAP and RADIUS authentication policies in Access Gateway. If you use double-source 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 Access Gateway.
- Intranet Applications for Android @Work apps. If you enable split tunneling on Access Gateway, when you configure the IP address routes for Android @Work apps, include the IP addresses of AppController, the Exchange server (if you are using @WorkMail™),

and all of the IP addresses of internal application web sites that users access from @WorkWeb™. Bind these settings to the virtual server on Access Gateway.

You can also configure connections to CloudGateway by using the configuration utility and you can configure virtual servers and policies individually.

## Configuring AppController Settings

There are two steps for allowing connections to AppController applications in the secure network through Access Gateway. In AppController, you:

- Configure Access Gateway trust settings.
- Specify the application to accept connections from remote users.

To route user connections through Access 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://AccessGatewayFQDN`.
- FQDN for the callback URL that verifies that the request came from Access Gateway. You use the same FQDN to which users connect. AppController appends the FQDN automatically with the authentication service URL. For example, the URL appears as `https://AccessGatewayFQDN/CitrixAuthService/AuthService.asmx`.

You can select the web applications that require remote user connections through Access Gateway. When you configure an application in AppController, 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 Access Gateway.

For more information about configuring AppController, see [Configuring Connections to Enterprise Web Applications Through Access 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 Access Gateway
2. The Enable legacy support setting.
3. Access Gateway settings, including:
  - Access Gateway web address

- Deployment mode
- Access Gateway mapped or subnet IP address
- Logon type as Domain
- Silent authentication by using the URL  
`https://<AccessGatewayFQDN>/CitrixAuthService/AuthService.asmx`, where  
*AccessGatewayFQDN* is the FQDN that is in the certificate bound to the virtual  
server.

If you configure double-source authentication on Access 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 CloudGateway

To allow connections through Access Gateway from the different versions of Receiver, you need to create session policies and profiles for CloudGateway with specific rules to enable the connections to work. You can create separate session policies and profiles for the following:

- Receiver for Android
- 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
- Access Gateway Plug-in

When you configure the expression for 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 CloudGateway 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.

## Configuring Session Policies

You configure session policies for CloudGateway Express and CloudGateway Enterprise 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 Access Gateway Plug-in you are using.

Some versions of Receiver do not fully support the StoreFront services protocols that allow direct connections through Access 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 Access 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
Receiver version supports StoreFront services protocols	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS
Access Gateway Plug-in for Windows Access 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	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

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 CloudGateway Express and CloudGateway Enterprise deployments.

1. In the Create Access Gateway Session Policy dialog box, select Advanced Free-Form and then click Add.
2. In the Add Expression dialog box, use the following parameters as a guideline for the expression:
  - a. In Expression Type, select General.
  - b. In Flow Type, select REQ.
  - c. In Protocol, select HTTP.

- d. In Qualifier, select Header.
  - e. In Operator, select CONTAINS, NOTCONTAINS, EXISTS, or NOTEXISTS depending on the expression.
  - f. In Value, type the parameter, such as CitrixReceiver.
  - g. In Header Name, type User-Agent and then click OK.
3. After you save the first expression, click And in the Create Access Gateway Session Policy dialog box to add && to the expression and then click Add.
  4. Repeat Step 2 to configure the second rule.
  5. 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 Access 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 CloudGateway Enterprise and CloudGateway Express. For more information, see the topics for CloudGateway Enterprise and CloudGateway Express later in this section.

---

# Configuring Session Profiles for CloudGateway Express

You can configure session policies to allow users to connect to CloudGateway Express. 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 Access Gateway:

- Citrix Receiver
- Receiver for Web
- PNA Services

When you configure the session profile for CloudGateway Express, configure the virtual server for Basic access. This allows users to access CloudGateway Express through connections from one of the software types in the preceding list. When you configure session profiles for StoreFront, users do not connect with the Access Gateway Plug-in.

---

# Creating the Session Profile for Receiver for CloudGateway Express

When you configure session policies and profiles for Receiver 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.

You can also configure these settings by using the Remote Access wizard. For more information, see [Configuring Access Gateway Settings with the Remote Access Wizard](#).

If your deployment contains StoreFront and Access Gateway only, you need to configure the StoreFront web address as the home page on the Client Experience tab and the Web Interface address on the Published Applications tab.

## To configure the session profile for Receiver

1. In the configuration utility, in the navigation pane, click Access Gateway.
  2. In the details pane, under Policy Manager, click Change group settings and user permissions.
  3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
  4. Under Related Tasks, click Create new session policy.
  5. In Name, type a name for the policy.
  6. Next to Request Profile, click New.
  7. In Name, type a name for the profile.
  8. Click the Security tab and in Default Authorization Action, click Override Global, and then select ALLOW.
  9. Click the Client Experience tab and then do the following:
    - a. Next to Plug-in Type, click Override Global and then select Java.
    - b. Next to Single Sign-on to Web Applications, click Override Global and then select the check box Single Sign-on to Web Applications.
    - c. Next to Clientless Access, click Override Global and then select Off.
  10. Click the Published Applications tab and then configure the following settings:
    - a. Next to ICA Proxy, click Override Global, and then select ON.
    - b. Next to Single Sign-on Domain, click Override Global, enter the domain name and then click Create. For example, enter *mydomain*.
    - c. In Web Interface Address, click Override Global, and then type the web address for StoreFront. For example, enter *https://storefront.t.com/Citrix/StoreWeb*.
- After you create and close the session profile, create the expression for the session policy in the Create Access Gateway Session Policy dialog box.

---

# Creating the Session Profile for Receiver for Web for CloudGateway Express

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 Access Gateway, however users cannot use the Access Gateway Plug-in to establish the connection. When you configure the virtual server, configure Basic mode.



## To create the session profile for Receiver for Web

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Click the Client Experience tab and then do the following:
  - a. In Clientless Access, click Override Global and then select Allow.
  - b. Next to Single Sign-on to Web Applications, click Override Global and then select the check box for Single Sign-on to Web Applications.
9. On the Published Applications tab, do the following:
  - a. Next to ICA Proxy, click Override Global, and then select ON.
  - b. Next to Web Interface Address, click Override Global and then enter the web address (URL) for StoreFront.
  - c. In Single Sign-on Domain, type the domain name.  
For example, type `mydomain`.
10. Click Create.

---

# Creating the Session Policy for PNA Services for CloudGateway Express

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.

## To create the session profile for PNA Services

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. 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.
9. Click the Published Applications tab and then do the following:
  - a. Next to ICA Proxy, click Override Global, and then select ON.
  - b. 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.
10. Click Create.

After you close the session profile, you then create the rule for the policy.

---

# Connecting to StoreFront by Using Email-Based Discovery

You can configure Access Gateway to accept user connections by using an email address to discover the StoreFront or Access 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 Access 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, Access Gateway provides the StoreFront URL to Receiver.
- Receiver gets the account information from StoreFront. If users connect through Access 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](#).
2. Add the StoreFront URL to Access Gateway.

In Access Gateway, you can configure StoreFront URL from the following locations:

- Remote Access wizard
- Global settings
- Session policy

You configure the StoreFront URL on the Published Applications tab in the session profile or in global settings. In the Remote Access wizard, you configure the StoreFront URL on the CloudGateway tab. For more information about configuring Access Gateway with the Remote Access wizard, see [Configuring Access Gateway Settings with the Remote Access Wizard](#).

## To configure email-based discovery globally

1. In the configuration utility, in the navigation pane, expand Access 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 Access Gateway > Policies and then click Session.
2. In the details pane, click the Profiles tab and then do one of the following:
  - a. Select an existing session profile and then click Open.
  - b. 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:
  - a. Click OK if you modified a session profile.
  - b. Click Create if you are adding a new session profile.

---

# Configuring Session Profiles for CloudGateway Enterprise

You can configure session policies to allow users to connect to CloudGateway Enterprise. Users can access applications hosted on AppController and documents stored in ShareFile.

You can configure the following session profiles that allow user access to AppController through Access Gateway:

- Citrix Receiver
- Receiver for Web
- PNA Services
- Access Gateway Plug-in

When you configure the session profile for CloudGateway Enterprise, configure the virtual server for SmartAccess to allow user connections with the Access Gateway Plug-in.

---

# Creating the Session Profile for Receiver for CloudGateway Enterprise

When you configure session policies and profiles for Receiver to connect to CloudGateway Enterprise, 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.

You can also configure these settings by using the Remote Access wizard. For more information, see [Configuring Access Gateway Settings with the Remote Access Wizard](#).

If your deployment contains AppController and Access Gateway only or the deployment contains StoreFront, AppController, and Access Gateway, you need to configure the AppController Web address as the home page on the Client Experience tab and the Web Interface address on the Published Applications tab.

## To configure the session profile for Receiver

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Click the Client Experience tab and then do the following:

- a. Next to Split Tunnel, select Override Global and then click ON.

Configure this option to allow Receiver for Android to use micro VPN to connect through Access Gateway. You also need to configure transparent interception. For more information, see [Configuring Intranet Applications for the Access Gateway Plug-in](#).

- b. Next to Clientless Access, select Override Global and then select On.
  - c. Next to Clientless Access URL Encoding, select Override Global and then select Clear.
  - d. Next to Single Sign-on to Web Applications, select Override Global and then select the check box Single Sign-on to Web Applications.
9. Click the Published Applications tab and then configure the following settings:
    - a. Next to Single Sign-on Domain, select Override Global and then enter the domain name. For example, enter *mydomain*.
    - b. Next to Account Services Address, select Override Global and then enter the StoreFront URL.

For example, enter `https://<StoreFrontFQDN>`.

10. Click Create.

After you create and close the session profile, create the expression for the session policy in the Create Access Gateway Session Policy dialog box.



---

# Creating the Session Profile for Receiver for Web for CloudGateway Enterprise

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 Access Gateway.

If your deployment contains AppController and Access Gateway only, or contains AppController, StoreFront, and Access Gateway, you need to configure the AppController Web address as the home page on the Client Experience tab and the Web Interface address on the Published Applications tab.

## To create the session profile for Receiver for Web

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Click the Client Experience tab and then do the following:

- a. In Home Page, click Override Global, and then type the Web address for AppController 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://<AppControllerFQDN>/Citrix/StoreWeb`.

- b. In Clientless Access, click Override Global and then select On.
  - c. 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.
  - d. Next to Single Sign-on to Web Applications, click Override Global and then select the check box for Single Sign-on to Web Applications.
9. On the Published Applications tab, do the following:
    - a. Next to ICA Proxy, click Override Global, and then select OFF.
    - b. Next to Web Interface Address, click Override Global and then enter the Web address for AppController or StoreFront.
    - c. In Single Sign-on Domain, type the domain name.

For example, type `mydomain`.

10. Click Create.

---

# Creating the Session Policy and Profile for PNA Services for CloudGateway Enterprise

If users connect with Receiver versions that do not support the StoreFront services protocol, you can configure a session policy for PNA Services. You can configure this session policy for the following Receiver versions:

- Receiver for Mac 11.4 and earlier versions
- Receiver for Android 3.0 and earlier versions
- Receiver for iOS 5.5 and earlier version

**Important:** User connections with any version of Receiver for Windows is not supported with PNA Services.

When you configure the session profile for PNA Services, you must enable single sign-on (SSO) in order to use ICA proxy. PNA services do not support SSO, so you need to use the complete URL for the PNA site as the Web Interface home page. When you enable PNA legacy support in StoreFront, make sure to specify the server URL on the StoreFront server when entering the Web Interface address in the session profile. You can also enter the Web Interface XenApp Services site of an existing XenApp or XenDesktop farm.

## To create the session profile for PNA Services

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. 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.
9. Click the Published Applications tab and then do the following:
  - a. Next to ICA Proxy, click Override Global, and then select ON.
  - b. 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.
10. Click Create.

After you close the session profile, you then create the rule for the policy.

---

# Creating a Session Policy and Profile for the Access Gateway Plug-in

You can configure Access Gateway to provide users access to published applications and virtual desktops with the Access Gateway Plug-in instead of with Receiver or StoreFront. You configure a session profile by using the instructions in [Configuring Access to Applications and Virtual Desktops in the Web Interface](#). Then, in the session policy, you add an HTTP header rule for the Access Gateway Plug-in.

## To create the session policy rule for the Access Gateway Plug-in

1. In the Create Access Gateway Session Policy dialog box, next to Match Any Expression, click the down arrow, select Advanced Free-Form and then click Add.
2. In the Add Expression dialog box, do the following:
  - a. In Expression Type, click General.
  - b. In Flow Type, select REQ.
  - c. In Protocol, select HTTP.
  - d. In Qualifier, select Header.
  - e. In Operator, select NOTEXISTS.
  - f. In Header Name, type `Referer` and then click OK.
3. Click Create and then click Close.

If users install the following versions of Receiver, you need to configure the following session profile for the Access Gateway Plug-in:

- Receiver for Windows 3.4
- Receiver for Windows 8/RT 1.2 (Preview)
- Receiver for Mac 11.7
- Receiver for iOS 5.7
- Receiver for Android 3.3

## To configure the session profile for the Access Gateway Plug-in

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In Name, type a name for the profile.
8. Click the Client Experience tab and then do the following:
  - a. Next to Single Sign-on to Web Applications, click Override Global and then select the check box Single Sign-on to Web Applications. This setting is required to allow single sign-on for desktop versions of Receiver and uses an Access Gateway Plug-in cookie.
  - b. Next to Clientless Access URL Encoding, click Override Global and then select Clear.
9. Click the Published Applications tab and then configure the following settings:
  - a. Next to Single Sign-on Domain, click Override Global, enter the domain name and then click Create. For example, enter *mydomain*.
  - b. Next to Account Services Address, click Override Global and then enter the StoreFront URL.

**Important:** Set Clientless Access to Off.

For example, enter `https://<StoreFrontFQDN>`.

This setting is needed for adding accounts if both Receiver and the Access Gateway Plug-in are already installed on the user device.

---

# Binding Session Policies and Setting the Priority

After you configure session policies for StoreFront 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 Access 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 Access 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
- Access Gateway Plug-in

For more information about binding session policies, see [Binding Session Policies](#).

## To set the priority of a session policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand the node to which the session policy is bound, expand Session Policies and then click the policy.
4. Under Related Tasks, click Modify priority.
5. In the Modify priority dialog box, in Priority, type the number and then click OK.



---

# Configuring Custom Clientless Access Policies for Receiver

You can configure a 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Clientless Access Policies.
4. Under Related Tasks, click Create new clientless access policy.
5. In Name, type a name for the policy.
6. Under Expression, type  
`HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver") &&  
HTTP.REQ.HEADER("X-Citrix-Gateway").EXISTS .`
7. Next to Profile, click New.
8. In Name, type a name for the profile.

**Important:** Do not change any settings in the profile.

9. Click Create two times and then click Close.



---

# Configuring Custom Clientless Access Policies for Receiver for Web

You can configure custom clientless access policies on Access 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 Access Gateway with clientless access.
- AppController requires the rewriting of HTML traffic.
- Receiver for Web requires that certain cookies are not proxied through Access 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, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Clientless Access Policies.
4. Under Related Tasks, click Create new clientless access policy.
5. In Name, type a name for the policy.
6. Under Expression, type `true`.
7. Next to Profile, click New.
8. In Name, type a name for the profile.
9. On the Rewrite tab, in URL Rewrite, select `ns_cvpn_default_inet_url_label`.
10. On the Client Cookies tab, next to Client Cookies, click New.
11. In the Configure Pattern Set dialog box, under Specify Pattern, in Pattern, add the following cookies in this order:
  - a. Enter the value `CsrfToken` and then click Add.
  - b. Enter the value `ASP.NET_SessionId` and then click Add.
  - c. Enter the value `CtxsPluginAssistantState` and then click Add.
  - d. Enter the value `CtxsAuthId` and then click Add.
12. Click Create three times and then click Close.

## To bind a clientless access policy to a virtual server

After you create the custom clientless access policy, bind the policy to the virtual server.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, click Virtual Servers and then expand the node for a virtual server.
4. Under Available Policies / Resources, expand Clientless Access Policies, click the new policy and then drag it to Clientless Access Policies in the virtual server node.

5. In the Modify Priority dialog box, in Priority, type a priority number and then click OK.

---

# Configuring Domains for Clientless Access for Access Gateway and StoreFront

When you configure Access Gateway and StoreFront, the configuration should not allow HTML rewriting rules in the StoreFront session profile to rewrite all network traffic. If all traffic is rewritten, Internet SaaS applications started through AppController would also proxy through Access Gateway.

You must configure StoreFront and AppController as the only domains for which clientless access is permitted. In this way, you allow external URLs to go directly through the web browser instead of going through Access Gateway. For more information about configuring domains for clientless access, see [Configuring Domain Access for Users](#).

When you add domains, you use the fully qualified domain name (FQDN) of AppController and StoreFront.

---

# Providing Access to Published Applications

One or more computers running Citrix XenApp or Citrix XenDesktop creates a server farm. If your enterprise network contains a server farm, you can deploy the Access Gateway to provide secure Internet access to published applications or published desktops.

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

This functionality is achieved by integrating Access Gateway components with the Web Interface, XenApp, or XenDesktop. This 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 Citrix eDocs at <http://edocs.citrix.com>.

Remote connectivity to a server farm does not require the Access Gateway Plug-in. To access published applications, users connect using Citrix XenApp online plug-ins. To access published desktops, users connect using Citrix Desktop Receiver.

**Important:** Installation of either the Desktop Receiver or the Desktop Receiver Embedded Edition on the same computer as Citrix online plug-ins (client-side software for Citrix XenApp) is not supported. If you want your users to be able to access both virtual desktops and virtual applications from the same computer, Citrix recommends installing Citrix online plug-ins on the virtual desktops that you create with XenDesktop. This allows your virtual desktops to receive virtual applications.

---

# Integrating Access Gateway with XenApp or XenDesktop

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

The tasks for integrating these three products include:

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

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

The Access Gateway and Web Interface use the Secure Ticket Authority and Citrix XML Service to establish client connections. The Secure Ticket Authority and XML Service runs on the XenApp or XenDesktop server.



---

# Establishing a Secure Connection to the Server Farm

The following example shows how an Access 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:

- Client devices from the Internet connect to the Access Gateway using XenApp online plug-ins or Citrix Desktop Receiver.
- The Web Interface resides behind the Access Gateway in the secure network. The user device makes the initial connection to the Access 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 the Access 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 this connection to succeed.
2. The Access Gateway receives the connection request and users are asked for their credentials. The credentials are passed back through the Access 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 client.
6. The user clicks a published application or desktop link. An HTTP request is sent to the Web Interface indicating the published resource that was selected.
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 client Web browser.

The ICA file generated by the Web Interface contains the Fully Qualified Domain Name (FQDN) or the Domain Name Server (DNS) name of the Access 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 the XenApp online plug-ins or Citrix Desktop Receiver. The client connects to the Access Gateway using the Access Gateway FQDN or DNS name in the ICA file. Initial SSL/TLS handshaking occurs to establish the identity of the Access Gateway.
11. The user device sends the session ticket to the Access Gateway and the Access Gateway contacts the STA for ticket validation.
12. The STA returns the IP address of the server on which the requested application resides to the Access Gateway.
13. The Access Gateway establishes a TCP connection to the server.
14. The Access 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 simply proxied through the Access Gateway.

The traffic between the user device and Access Gateway is encrypted. The traffic between the Access Gateway and the server can be encrypted independently but is not encrypted by default.

---

# Setting Up a Web Interface Site to Work with the Access Gateway

The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their published applications through a standard Web browser or through the Citrix XenApp online plug-ins (the new name for the Program Neighborhood Agent). Users access published desktops using Citrix Desktop Receiver.

You can configure Web Interface sites created on Windows platforms using the Access Management Console. The Access Management Console can be installed on Windows platforms only.

To configure the Web Interface to work with the Access Gateway, create the Web Interface site, configure the settings in the Web Interface, and then configure the Access Gateway.

---

# Web Interface Features

Before you configure the Web Interface to work with Access 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 (the new name for access platform 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 (the new name for Program Neighborhood Agent 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

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

**Important:** Install and configure the Web Interface before you configure Access 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 either a Web browser, the Access Gateway Plug-in, or Citrix Receiver. For more information, see [Web Interface Features](#).
- Identify where users authenticate from: Access Gateway or the Web Interface.

**Note:** When the Web Interface is in the secure network, you enable authentication on the virtual server on the Access Gateway. When you disable authentication, unauthenticated HTTP requests are sent directly to the server running the Web Interface. Disabling authentication on Access 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 Access Gateway. For more information about working with certificates, see [Installing and Managing Certificates](#).

**Important:** For the Web Interface to work properly with Access Gateway 10, the server running the Web Interface must trust the Access Gateway certificate and be able to resolve the virtual server fully qualified domain name (FQDN) to the correct IP address.

---

# Creating a Web Interface Site in XenApp 5.0 or XenDesktop 2.1

When you create a Web Interface site in XenApp 5.0 or XenDesktop 2.1, you can configure user logon using either a Web browser, Citrix XenApp online plug-ins, or Citrix Desktop Receiver. You can use the following procedure to create multiple Web Interface sites using the Access Management Console.

To create the Web Interface site on a XenDesktop server, you must install the Web Interface Access Management Console on the XenDesktop server.

1. Click Start > All Programs > Citrix > Management Console > Access Management Console. If prompted, configure and run discovery.
2. Under Citrix Resources > Configuration Tools, click Web Interface, and under Common Tasks, click Create site.
3. Select one of the following and click Next:

- XenApp Web. Users log on to the Web Interface using a Web browser.

If you are creating a Web Interface site on XenDesktop, select this option. Users log on using Citrix Desktop Receiver.

- XenApp Services. Users log on using Citrix XenApp Plug-ins. The Desktop Receiver is not supported if this option is selected.

If you are configuring the Web Interface for use with Access Gateway Standard Edition and this option is selected, logon page authentication must be disabled on the Access Gateway. In addition, the Web Interface must be deployed in the DMZ.

**Note:** If you select this option, do not perform Steps 5 and 6.

4. Keep the default Internet Information Services (IIS) site and path.

If you selected XenApp Web in Step 3, the site path is /Citrix/XenApp and continue with Step 5.

If you selected XenApp Services, the site path is /Citrix/PNAgent and click Next to complete the configuration.

**Note:** If there are any pre-existing XenApp Web sites or XenApp Services 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 the Access Gateway in the DMZ.

- At Access Gateway to have users authenticate using the Access Gateway appliance.

If you select this option, the Access 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 Access Gateway Enterprise Edition, this setting enables SmartAccess in XenApp or XenDesktop.

6. If you selected At Access Gateway in Step 5, in Authentication service URL, type the Web address to the Access Gateway authentication service URL, such as `https://access.company.com/CitrixAuthService/AuthService.asmx`, and click Next.

**Note:** If you select At Web Interface in Step 5, you do not need to perform Step 6.

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 Access Gateway Settings for the Web Interface on XenApp 5.0 or XenDesktop 2.1

After you create the Web Interface site, you can use the Access Management Console to configure settings for the Access Gateway.

1. Click Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. In the left pane of the Access Management Console, click Citrix Resources, click Configuration Tools, click Web Interface and then click the Web Interface site.
3. Under Common Tasks, click Manage secure client access and click Edit secure client access settings.
4. In Specify Access Methods, select the Default entry and click Edit.
5. In Access Method, select Gateway direct, click OK and click Next.
6. In Address (FQDN), type the Access Gateway FQDN. This must be the same FQDN that is used on the Access Gateway certificate.
7. In Port, type the port number. The default is 443.
8. To enable session reliability, click Enable session reliability and 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 or the Desktop Delivery Controller, click OK and click Finish. For example, type `http://xenappsrv01/Scripts/CtxSta.dll`.

After you configure the settings in the Web Interface, configure the Access Gateway.

---

# Creating a Web Interface 5.3 Site

When you create a Web Interface 5.3 site, you can configure user logon using either a Web browser, Citrix online plug-ins, or Citrix Desktop Receiver. You can use the following procedure to create multiple Web Interface sites using the Citrix Web Interface Management console.

Single sign-on to the Web Interface using a smart card is available only 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 click Next.

The default site path is /Citrix/Xenapp or you can type one of your own choosing.

**Note:** If there are any pre-existing 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 the Access Gateway in the DMZ.

- At Access Gateway to have users authenticate using the Access Gateway appliance.

If you select this option, the Access 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 Access Gateway Enterprise Edition, 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 Access Gateway authentication service URL, such as `https://access.company.com/CitrixAuthService/AuthService.asmx`, and click Next.
8. Under Authentication Options, select how users log on:
  - Explicit - users log on using a Web browser.
  - Smart Card - users log on 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 Access Gateway Settings in Web Interface 5.3

After you create the Web Interface site, you can use Citrix Web Interface Management to configure settings for the Access 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 IP address and subnet mask and in Access Method, select Gateway direct, click OK and then click Next.
6. In Address (FQDN), type the Access Gateway FQDN. This must be the same FQDN that is used on the Access Gateway certificate.
7. In Port, type the port number. The default is 443.
8. To enable session reliability, click Enable session reliability and 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 click Finish. For example, type `http://xenappsrv01/Scripts/CtxSta.dll`.

After you configure the settings in the Web Interface, configure the Access Gateway.

---

# Adding XenApp and XenDesktop to a Single Site

If you are running XenApp and XenDesktop, you can add both to a single Web Interface site. This allows you to use the same Secure Ticket Authority server from either XenApp or Desktop Delivery Controller.

**Note:** XenDesktop supports Web Interface 5.0 and later.

If you are using Web Interface 5.0 or 5.1, you combine the XenApp and XenDesktop sites using the Access Management Console.

If you are using Web Interface 5.2 or 5.3, you combine the XenApp and XenDesktop sites using the Web Interface Management console.

**Note:** If the server farms are in different domains, you must establish two-way trust between the domains.

## To add XenApp or XenDesktop to a single site using Web Interface 5.0 or 5.1

1. Click Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Expand Citrix Resources > Configuration Tools > Web Interface.
3. Click a Web Interface site and under Common Tasks, click Manage server farms.
4. In the Manage Server Farms dialog box, click Add.
5. Complete the settings for the server farm and click OK twice.

## To add XenApp or XenDesktop to a single site using Web Interface 5.2 or 5.3

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 click Server Farms.
4. In the Manage Server Farms dialog box, click Add.
5. Complete the settings for the server farm and click OK twice.

For the best experience using XenDesktop, change the setting `UserInterfaceBranding` to `Desktops` in the `WebInterface.conf` configuration file.

---

# Routing Client Connections Through the Access Gateway

In XenApp and XenDesktop, you can configure the servers to only accept connections that are routed through the Access Gateway. You use the Access Management Console to modify the server properties for XenApp and Desktop Delivery Controller.

1. Click Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Do one of the following:
  - In the Desktop Deliver Controller, expand Citrix Resources > Desktop Delivery Controller and click a server farm.
  - In XenApp 5.0, expand Citrix Resources > XenApp and click on a server farm.
3. Under Common Tasks, click Modify farm properties and click Modify all properties.
4. In the Farm Properties dialog box, under Properties > Farm-wide, click Connection Access Controls.
5. Click Citrix Access Gateway connections only and click OK.

---

# Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface

You can configure Access Gateway to communicate with the Web Interface running on Citrix XenApp and Citrix XenDesktop. To do so, configure a virtual server on Access Gateway. Next, bind a signed server certificate and authentication, session, preauthentication, and post-authentication policies to the virtual server. Access Gateway uses the virtual server IP address to route user connections to the Web Interface.

The Published Applications Wizard allows you to configure Access Gateway to route user connections to the Web Interface. Access Gateway uses the Secure Ticket Authority (STA) for user connections.



---

# Configuring Policies for Published Applications and Desktops

To establish communication with XenApp and XenDesktop servers, you need to configure the Access Gateway to recognize the servers. You can configure the settings globally or using policies that are bound to users, groups, or virtual servers.

## To configure the Web Interface globally on the Access Gateway

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. In the Global Access Gateway Settings dialog box, on the Published Applications tab, next to ICA Proxy, select ON.
4. Next to Web Interface Address, type the Web address of the Web Interface and click OK.

## To configure a session policy for the Web Interface

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

**Note:** Citrix recommends using the Access Gateway Policy Manager to create a session policy for the Web Interface and then bind it to a virtual server.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In the Create Session Policy dialog box, in Name, type a name for the policy.
6. Next to Request Profile, click New.
7. In the Create Session Profile dialog box, in Name, type a name for the profile.

8. On the Published Applications tab, next to ICA Proxy, click Override Global and select ON.
9. Next to Web Interface Address, click Override Global, type the Web address of the Web Interface and click Create.
10. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and click Close.

When the session policy is created, bind the policy to a virtual server.

## To bind a session policy to a virtual server

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers and then expand the virtual server node.
4. Under Available Policies / Resources, click Session Policies, select the policy and drag it to Session Policies in the virtual server node.

---

# To run the Published Applications Wizard

To configure the Access Gateway with the Web Interface, you need the following information:

- IP addresses of servers running Citrix XenApp or Citrix XenDesktop
  - Fully qualified domain name of the server running the Web Interface
  - Virtual server configured on the Access Gateway
  - Session policy configured for SmartAccess
  - IP addresses of additional servers running the Web Interface if you are configuring Web Interface failover
1. In the configuration utility, in the navigation pane, click Access Gateway.
  2. In the details pane, under Getting Started, click Published applications wizard.
  3. Click Next and follow the instructions in the wizard.

The Published Applications Wizard also allows you to configure and activate the Secure Ticket Authority (STA) from within the wizard. When you complete the Published Applications Wizard, the settings are bound globally.

---

# Configuring the Secure Ticket Authority on the Access Gateway

The Secure Ticket Authority 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.

The STA is configured on the Access Gateway using one of three methods:

- Global settings in the configuration utility
- Published Applications Wizard
- Access Gateway Policy Manager

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 Access Gateway and the STA, make sure a server certificate is installed on the server running the STA.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand either Access Gateway Global or Virtual Servers. If you select Virtual Servers, expand a node and select a server.
4. Click STA Servers.
5. Under Related Tasks, click Bind new STA server.
6. In the STA Server dialog box, in URL, type the IP address or FQDN of the server running the STA and 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 those that are configured on the Access Gateway. If you are configuring multiple STAs, do not use load balancing between the Access Gateway and the servers running the STA.

You can remove a STA by unbinding the STA either globally or from a virtual server.

## To remove a Secure Ticket Authority server

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand either Access Gateway Global or Virtual Servers and expand a virtual server node.
4. Under STA Servers, click a STA and under Related Tasks, click Unbind STA server.

---

# Configuring Additional Web Interface Settings on Access Gateway Enterprise Edition

If you are deploying Access Gateway Enterprise Edition with a server farm, there are additional tasks you can complete. These tasks include:

- [Configuring Web Interface Failover](#)
- [Configuring SmartAccess on Access Gateway Enterprise Edition](#)

---

# Configuring Web Interface Failover

You can configure the Access Gateway to failover to a secondary server running the Web Interface using the Published Applications Wizard.

Web Interface failover allows user connections to stay active in the event 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 Web Interface failover is configured on the Access 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 IP address and 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. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Getting Started, click Published applications wizard.
3. Click Next, select a virtual server, and click Next.
4. On the Configure Client Connections page, click Configure Web Interface Failover.
5. Under Primary Web Interface, in Virtual Server IP, type the new IP address for failover.
6. 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.
7. In Web Interface Server Port, type the port number of the Web Interface and click OK. Click Next and follow the instructions in the wizard.

---

# Configuring Smart Card Access with the Web Interface

If users are logging on directly to the Web Interface using Citrix XenApp online plug-ins and smart card authentication, the Web Interface must be parallel to the Access Gateway in the DMZ. The server running the Web Interface must also be a domain member.

If users are logging on using the Access Gateway Plug-in, initial authentication is done by the Access Gateway. When the VPN tunnel is established, the user can log on to the Web Interface using the smart card. In this scenario, the Web Interface can be installed behind the Access Gateway or in the secure network.

If the Web Interface is configured to use smart card authentication and is installed parallel to the Access Gateway, the Access Gateway and the Web Interface each perform SSL termination.

The Web Interface terminates secure HTTP traffic including user authentication, display of published applications, and starting published applications. The Access Gateway terminates SSL for incoming ICA connections.

**Note:** Access Gateway Enterprise Edition can also use the smart card for authentication using a client certificate.



---

# Configuring SmartAccess on Access Gateway Enterprise Edition

You can use SmartAccess with XenApp and XenDesktop to intelligently deliver published applications and desktops to users.

SmartAccess allows you to control access to published applications and desktops on a server through the use of Access Gateway session policies. This permits the use of preauthentication and post-authentication checks as a condition for access to published resources, along with other factors. These include anything you can control with a XenApp or XenDesktop policy, such as printer bandwidth limits, client drive mapping, client clipboard, client audio, and client printer mapping. Any XenApp or XenDesktop policy can be applied based on whether or not users pass an Access Gateway check.

Access Gateway can deliver XenDesktop using the same options that are available with Web Interface, ICA proxy access, clientless access, and Access Gateway access.

This functionality is achieved by integrating Access Gateway Enterprise Edition components with the Web Interface and XenApp or XenDesktop. This provides advanced authentication and an access control option to the Web Interface. For more information, see the Web Interface documentation in the Technologies node in Citrix eDocs at <http://edocs.citrix.com>.

Remote connectivity to a server farm does not require the Access Gateway Plug-in. Users connect using Citrix online plug-ins. For connections to published desktops, users can use Citrix Desktop Receiver. Users can use the Access Gateway Plug-in to log on and receive their published applications and desktops using the Access Interface, which is the default home page for the Access Gateway.

**Important:** Installation of either the Desktop Receiver or the Desktop Receiver Embedded Edition on the same computer as Citrix online plug-ins (client-side software for Citrix XenApp) is not supported. If you want your users to be able to access both virtual desktops and virtual applications from the same computer, Citrix recommends installing Citrix online plug-ins on the virtual desktops that you create with XenDesktop. This allows your virtual desktops to receive virtual applications.

---

# How SmartAccess Works for XenApp and XenDesktop

To configure SmartAccess, you need to configure Access Gateway settings on the Web Interface and configure session policies on the Access Gateway. When you run the Published Applications Wizard, you can select the session policies you created for SmartAccess.

When a user types the Web address of a virtual server in a Web browser, any preauthentication policies that are configured are downloaded to the user device. The Access 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 set. 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.

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.

SmartAccess endpoint analysis can be configured on the Access Gateway. To configure endpoint analysis, create a session policy that enables the ICA proxy setting and then configure a client security string. When the session policy is configured, you can bind the policy globally and to users, groups, and virtual servers.

When the user logs on, the endpoint analysis policy runs a security check of the client device with the client security strings configured on the Access 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 the policy is configured, bind it to a user, group, virtual server, or globally. When users log on, the SmartAccess policy check starts and verifies whether or not the client device has Version 10.0.2 or higher 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 are creating a session policy for SmartAccess, the session profile does not have any settings configured, creating a null profile. The Access Gateway uses the Web Interface URL configured globally for SmartAccess.

---

# Configuring XenApp Policies and Filters

After you create the session policy on Access Gateway, configure policies and filters on the computer running XenApp that are applied to users according to the endpoint analysis configuration.

## To configure XenApp 5.0 policies and filters

1. On the server running XenApp, click Start > All Programs > Citrix > Management Consoles > Access Management Console. If prompted, configure and run discovery.
2. In the left pane, click Citrix Resources > XenApp > Server Farm > Applications.
3. Right-click an application, point to Modify application properties, and then click Modify All Properties.
4. Under Properties, click Advanced > Access Control.
5. In the right pane, click Any connection that meets the following filters and then click Add.
6. In Access Gateway farm, type the name of the Access Gateway virtual server.
7. In Access Gateway filter, type the name of the endpoint session policy and then click OK.
8. In the Application Properties dialog box, clear Allow all other connections and then click OK.

---

# To configure a session policy for SmartAccess

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Resource / Policies, click Session Policies.
4. Under Related Tasks, click Create new session policy.
5. In the Create Session Policy dialog box, in Name, type a name for the policy, such as `ValidEndpoint`.
6. In Request Profile, click New and in Name, type a name for the profile, such as `Null` and then click Create.
7. 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 Client Device Mapping on XenApp

You can also use Access Gateway filters that are applied to policies on a computer running XenApp. This allows users access to XenApp capabilities such as client drive mapping, printer mapping, or clipboard mapping based on the results of the endpoint analysis.

The Citrix online plug-ins support mapping devices on user devices so users can access external devices within client sessions. User device mapping provides:

- Access to local drives and ports
- Cut-and-paste data transfer between a client session and the local clipboard
- Audio (system sounds and .wav files) playback from the client session

During logon, the client informs the server of the available user drives and COM ports. In XenApp 5.0, user drives are mapped to server drive letters so they appear to be directly connected to the server. In XenApp 6.0, user drives are mapped to the server and use the client device drive letter. These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

After enabling the XML Service, configure policies for client device mapping.

To enforce user device mapping policies based on SmartAccess filters, create two policies on the server:

- A restrictive ICA policy that disables user device mapping and applies to all Access 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, it overrides the policy that disables user device mapping.

Restrictive and non-restrictive policies on XenApp 5.0 are configured using Citrix XenApp Advanced Configuration.

Restrictive and non-restrictive policies on XenApp 6.0 are configured using the Delivery Services Console.

---

# To configure a restrictive policy on XenApp 5.0

1. Click Start > Citrix > Administrative Tools > XenApp Advanced Configuration.
2. In Advanced Configuration, in the left pane, right-click Policies and then click Create Policy.
3. In Policy Name, type a name for the policy, such as `Restrictive ICA` and then click OK.
4. In the right pane, right-click the restrictive ICA policy and then click Properties.
5. Click Client Devices > Resources > Drives > Connection.
6. In the right pane, under Connection, click Enabled and then click Do Not Connect Client Drives at Logon.
7. Configure any other settings you want to enforce on invalid user connections and then click OK.
8. Right-click the restrictive ICA policy and then select Apply this policy to.
9. In the left pane, click Access Control.
10. In the right pane, click Filter based on Access Control, click Apply to connections made through Access Gateway, click Any connection and then click OK.

After you create the restrictive ICA policy, create a non-restrictive ICA policy.

---

# To configure a non-restrictive policy on XenApp 5.0

1. Click Start > Citrix > Administrative Tools > XenApp Advanced Configuration.
2. In Advanced Configuration, in the left pane, right-click Policies and click Create Policy.
3. In Policy Name, type a name for the policy, such as Full ICA, and click OK.
4. In the right pane, right-click the non-restrictive ICA policy and click Properties.
5. Click Client Devices > Resources > Drives > Connection.
6. In the right pane, under Connection, click Enabled and click Connect Client Drives at Logon.
7. Configure any other settings you want to enforce on invalid client connections and click OK.
8. Right-click the non-restrictive ICA policy and select Apply this policy to.
9. In the left pane, click Access Control.
10. In the right pane, click Filter based on Access Control, click Apply to connections made through Access Gateway, click Any connection that meets any of the following filters, and click Add.
11. In Access Gateway Farm, type or select the virtual server name.
12. In Access Gateway filter, type or select a session policy name that is configured on the Access Gateway and click OK twice.
13. Right-click the non-restrictive policy and click Priority > Make highest priority.

---

# To configure a restrictive policy on XenApp 6

1. Click Start > All Programs > Management Consoles > Citrix Delivery Console.
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, click Auto connect client drives and then click Add.
7. Click Disabled, click OK and then click Next.
8. Under Categories, click All Filters.
9. Under Filters, click Access Control and then 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 Access Gateway Farm, type the virtual server name.
14. In Access Condition, type or select the session policy name that is configured on Access Gateway, click OK twice and then complete the wizard.



---

# To configure a non-restrictive policy on XenApp 6

1. Click Start > All Programs > Management Consoles > Citrix Delivery Console.
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, click Auto connect client drives and then click Add.
7. Click Enabled, click OK and then click Next.
8. Under Categories, click All Filters.
9. Under Filters, click Access Control and then 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 Access Gateway Farm, type the virtual server name.
14. In Access Condition, type or select the session policy name that is configured on Access Gateway, click OK twice and then complete the wizard.

---

# Enabling XenApp as a Quarantine Access Method

If you have endpoint analysis configured on the Access Gateway, users who pass an endpoint scan can access all the resources that are configured on the Access Gateway. You can put users who fail an endpoint scan in a quarantine group. When this occurs, users can access published resources only.

For example, you created an endpoint analysis scan to check whether or not Notepad is running on the client device when users log on. If Notepad is running, users can log on using the Access 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 the Access 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

To enable XenApp as a quarantine access method, create a group on Access 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 Access 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 Policies](#).

## To create an endpoint analysis scan and add a quarantine group

1. In the Access Gateway Policy Manager, under Available Policies / Resources, click Session Policies.
2. Under Related Tasks, click Create new session policy.
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 OK and then click Create twice.
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 4.0 for SmartAccess

The Access Gateway enables XenDesktop to deliver secure desktops to remote users. XenDesktop can intelligently deliver desktops using the SmartAccess capabilities of the Access Gateway. When you create desktop groups using the Delivery Services Console in XenDesktop, you then configure policies and filters for access control.

To configure the Access Gateway to deliver published desktops, you use the same options that are available with the Web Interface, ICA proxy access, clientless access, and Access Gateway access.

When you create a session policy using the Published Applications tab, use the Web address for the XenDesktop Web Interface site. After creating the policy, bind it to a virtual server. Then create a null session profile where settings are not configured. The Web Interface configuration is inherited from global settings.

---

# To configure a session policy for SmartAccess

You configure SmartAccess on the Access Gateway to access XenDesktop using a session policy bound to a virtual server.

1. In the Access Gateway Policy Manager, under Available Resource / Policies, click Session Policies.
2. Under Related Tasks, click Create new session policy.
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 and in the Create Session Profile dialog box in Name, type a name for the profile, such as `XenDesktopProfile`.
5. On the Published Applications tab, next to ICA Proxy, click Override Global and select ON.
6. In Web Interface Address, click Override Global and type the URL to the XenDesktop Web Interface site.
7. In Single Sign-on Domain, click Override Global, type the domain name and click Create.
8. In the Create Session Policy dialog box, next to Named Expressions, select True Value, click Add Expression, click Create and 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 save the policy.

When both session policies are created, bind both policies to the virtual server.

---

# To configure policies and filters in XenDesktop 4.0

You can use SmartAccess policies to show and hide desktop groups. When you configure settings on XenDesktop, you configure the settings to use the Access Gateway virtual server name and the session policy name. Then you configure access control to allow connections to meet defined filters. You can also use SmartAccess policies.

1. In the Delivery Services Console, click Citrix Resources > Desktop Delivery Controller > Desktop Groups.
2. Right-click the desktop group and click Properties.
3. Under Properties > Advanced, click Access Control.
4. Click Allow connections made through Access Gateway Advanced Edition (version 4.0 or later).
5. Click Any connection that meets any of the following filters and click Add.
6. In Access Gateway Farm, type the name of the virtual server on the Access Gateway.
7. In Access Gateway Filter, type the name of the session policy on the Access Gateway and click OK twice.

---

# To configure policies and filters in XenDesktop 5

You can configure settings in XenDesktop 5 by using either the Desktop Studio or the Group Policy Editor. When you configure Access Gateway settings in XenDesktop, use the Access 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 Access Gateway without considering Access 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 Access Gateway based on existing Access Gateway policies, do the following:
  - a. In AG farm name, type the virtual server name.
  - b. In Access condition, type the name of the endpoint analysis policy or session policy.

**Important:** XenDesktop does not validate Access 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

To establish ICA connections with XenDesktop, you add the IP address of the Desktop Delivery Controller to the virtual server as the Secure Ticket Authority (STA).

1. In the Access Gateway Policy Manager, under Configured Policies / Resources, expand Virtual Servers and then expand a virtual server node.
2. Click STA Servers.
3. Under Related Tasks, click Bind new STA server.
4. In the Configure STA Server dialog box, in URL, type the IP address or URL of the server running the STA and then click Create.

---

# Configuring Single Sign-on to the Web Interface on Access Gateway Enterprise Edition

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

---

# Configuring Single Sign-On to the Web Interface

The Access Gateway can be configured 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 Access Gateway Plug-in from a bookmark configured in the Access Interface or a Web address 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 the Access 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 credentials are accepted by the Web server, users are logged on automatically. If the credentials are rejected by the Web server, users receive an authentication prompt asking for their user name and password.

You can configure single sign-on to Web applications globally or using a session policy.

You can also configure single sign-on to the Web Interface using a smart card. For more information, see [Configuring Single Sign-On to the Web Interface using a Smart Card](#).

---

# To configure single sign-on to Web applications globally

1. In the configuration utility, in the navigation pane, expand Access Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. In the Global Access 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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Session Policies and then select a policy.
4. Under Related Tasks, click Modify session policy.
5. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
6. 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

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 Access Gateway. You can enable multiple ports. You configure the ports globally.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, click Advanced.
4. In the Network Configuration - Advanced dialog box, under HTTP Ports, type the port number, click Add and then click OK twice.

**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

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 Access 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 Access Gateway virtual server. Any Access 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 Access 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 Access 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 Access Gateway must match the STA that you configured on the Web Interface.

---

# To test the single sign-on connection to the Web Interface

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://AccessGatewayFQDN`, where *AccessGatewayFQDN* is the fully qualified domain name (FQDN) of Access Gateway.
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 starting a published application, Citrix XenApp Plug-ins direct traffic through the Access Gateway appliance to servers in the farm.



---

# To configure single sign-on for XenApp and file shares

If users are connecting to servers running Citrix XenApp and using SmartAccess, you can configure single sign-on for users connecting to the server farm. When you configure access to published applications by using a session policy and profile, use the domain name for the server farm.

You can also configure single sign-on to file shares in your network.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies / Resources, expand Session Policies and then select the policy for your published applications.
4. Under Related Tasks, click Modify session policy.
5. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
6. 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 using a Smart Card

If you use smart cards for user logon, you can configure single sign-on to the Web Interface. You configure settings on the Access Gateway and then configure the Web Interface to accept single sign-on with a smartcard. Single sign-on is also called *pass-through authentication*.

Single sign-on to the Web Interface using a smart card is supported only in Web Interface 5.3.

Users can be in multiple CN groups in Active Directory for single sign-on to work provided that the user name extracted in the certificate action is *SubjectAltName:PrincipalName*. If you are using the parameter *Subject:CN*, users cannot be part of multiple CN groups.

To configure the Access Gateway for single sign-on to the Web Interface 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 the Access Gateway](#).
- Install a root certificate on the Access Gateway and 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 the SSL parameter, see [To configure the client certificate for single sign-on using a smart card](#). For more information about configuring a virtual server, see [Creating Additional Virtual Servers](#).
- Create a secondary virtual server where client authentication is disabled in the SSL parameters. This prevents users receiving a secondary request for their personal identification number (PIN). For more information, see [To create a second virtual server for ICA connections](#).
- 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 the Access Gateway.

## To create a session profile for single sign-on using a smart card

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Session.
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 click Single sign-on to Web Applications.
5. Click the Published Applications tab.
6. Next to ICA Proxy, click Override Global, and select ON.
7. In Web Interface Address, click Override Global, and type the fully qualified domain name (FQDN) or the Web Interface.
8. In Single Sign-on Domain, click Override Global, and type the domain name.

**Note:** You must use the format *domain* and not the format *domain.com*. For more information about configuring this setting, see [To configure single sign-on to Web applications by using a session policy](#).

9. Click Create, and then click Close.

When 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 using a smart card

If you are configuring single sign-on to the Web Interface using a smart card, the client certificate setting on the Access Gateway must be set to optional. If it is set to mandatory, single sign-on to the Web Interface fails.

1. In the configuration utility, in the navigation pane, expand Access Gateway and click Virtual Servers.
2. In the details pane, click a virtual server and click Open.
3. In the Configure Access Gateway Virtual Server dialog box, on the Certificates tab, click SSL Parameters.
4. In the Configure SSL Params dialog box, under Others, click Client Authentication.
5. In Client Certificate, select Optional, and click OK twice.

---

# Access Gateway Advanced Concepts

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

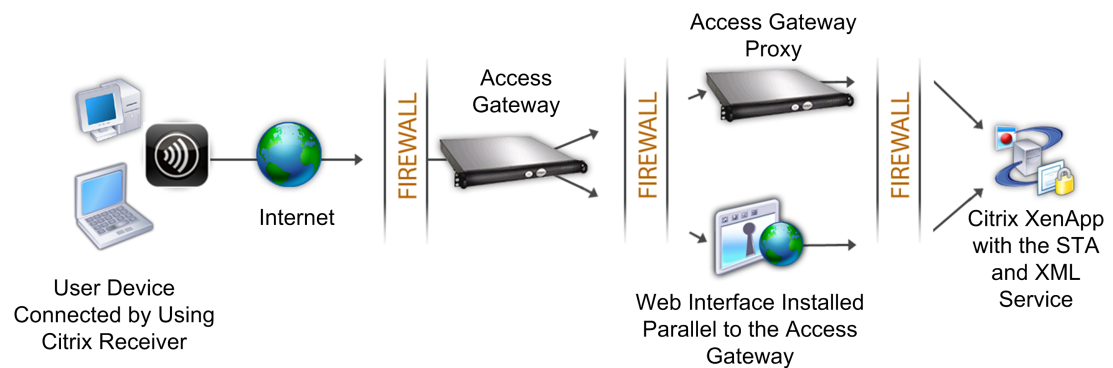
- Deploying Access Gateway in a double-hop DMZ. You can deploy two Access Gateway appliances in a double-hop DMZ in two stages to provide an extra layer of security for the internal network.
- Configuring DNS virtual servers. You can configure a DNS server as a virtual server and then bind the server 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 Access 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 Access Gateway Plug-in logging. You can configure the Access Gateway Plug-in to log all errors to a text file.

---

# Deploying Access Gateway in a Double-Hop DMZ

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. Access Gateway appliances deployed in a double-hop DMZ



**Note:** For illustration purposes, the preceding example describes a double-hop configuration using three firewalls, 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.

---

# How a Double-Hop Deployment Works

You can deploy Access Gateway appliances in a double-hop DMZ to control access to servers running Citrix XenApp, as shown in the previous figure.

In a double-hop DMZ deployment, users connect to the Access Gateway in the first DMZ with a Web browser and Citrix XenApp online plug-ins.

A user begins by connecting to the Access Gateway with a Web browser and selecting a published application from the Web Interface. After selecting a published application, XenApp online plug-ins are started programmatically on the client device. The client connects to the Access Gateway to access the published application running in the server farm in the secure network.

**Note:** The Access Gateway Plug-in is not supported in a double-hop DMZ deployment. Only Citrix online plug-ins are used for client connections.

The Access Gateway in the first DMZ handles client connections and performs the security functions of an SSL VPN. This Access Gateway encrypts the client connections, determines how clients are authenticated, and controls access to the servers in the internal network.

The Access Gateway in the second DMZ serves as a proxy device. This Access Gateway enables the ICA traffic to traverse the second DMZ to complete client connections to the server farm. Communications between the Access Gateway in the first DMZ and the Secure Ticket Authority (STA) in the internal network are also proxied through the Access Gateway in the second DMZ.

**Note:** The term *Access Gateway proxy* refers to an Access Gateway appliance deployed in the second DMZ.

Review the following topics about deploying the Access Gateway in a double-hop DMZ configuration:

- [Communication Flow in a Double-Hop DMZ Deployment](#). For reference purposes, this provides a summary and links to a detailed, step-by-step description of the client connection process and the interactions that occur among the various components involved in a double-hop DMZ deployment.
- [Preparing for a Double-Hop DMZ Deployment](#). This discusses the configuration issues you should be aware of before deploying Access Gateway appliances in a double-hop DMZ.
- [Installing the Access Gateway in a Double-Hop DMZ](#). This describes the procedures you must perform to deploy Access Gateway appliances in a double-hop DMZ configuration.

# Communication Flow in a Double-Hop DMZ Deployment

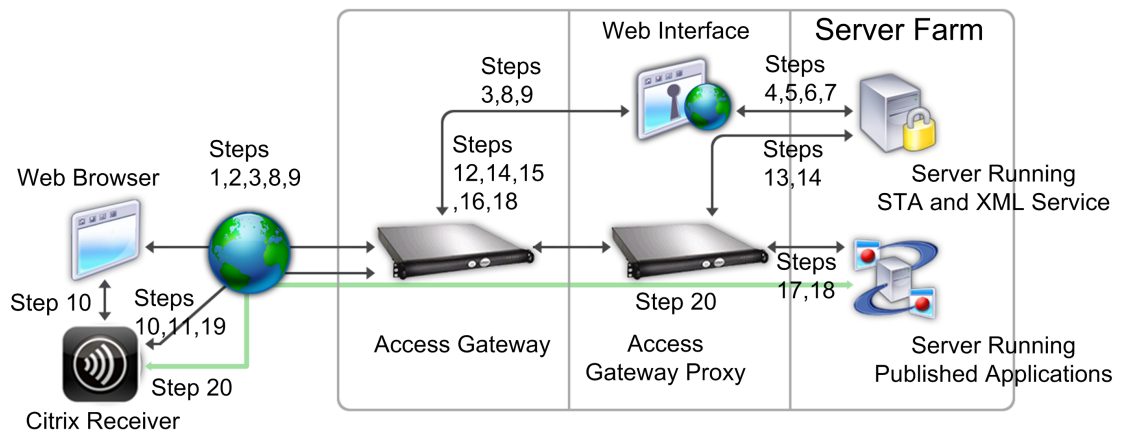
To understand the configuration issues involved in a double-hop DMZ deployment, you should have a basic understanding of how the various Access Gateway and XenApp components in a double-hop DMZ deployment communicate to support a user connection.

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. 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

User authentication is the first stage of the user connection process in a double-hop DMZ deployment.

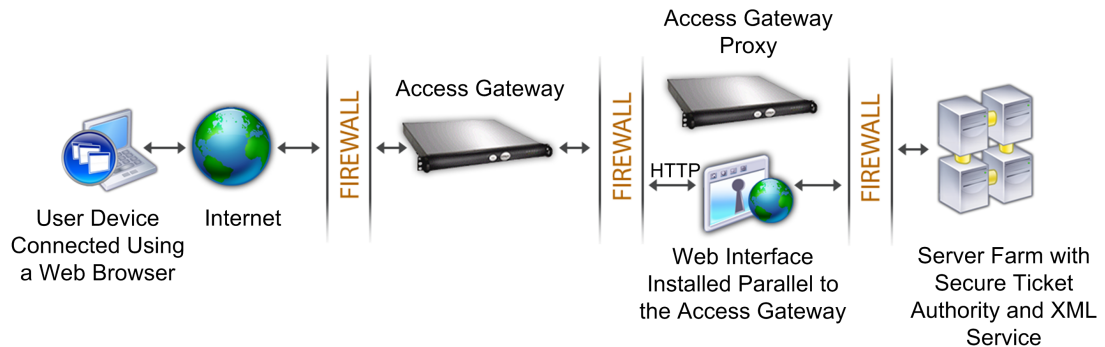


Figure 1. Basic communication flow for user authentication in a double-hop DMZ

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

1. A user types the address of Access Gateway, such as `https://www.ag.wxyco.com` in a Web browser to connect to Access Gateway in the first DMZ. If you enabled logon page authentication on Access Gateway, Access Gateway authenticates the user.
2. Access Gateway in the first DMZ receives the request.
3. Access 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 Access Gateway, the appliance sends the Access Gateway logon page to the user. The user enters authentication credentials on the logon page and the appliance authenticates the user. Access Gateway then returns the user credentials to the Web Interface.

If you do not enable authentication, Access 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 Access Gateway passes the user credentials back to the Web Interface.

---

# Creating a Session Ticket

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

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 XenApp online plug-ins.

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

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

---

# Completing the Connection

Completing the connection is the fourth and last stage of the user connection process in a double-hop DMZ deployment. The following figure shows user connections to and from a server farm in a double-hop DMZ.

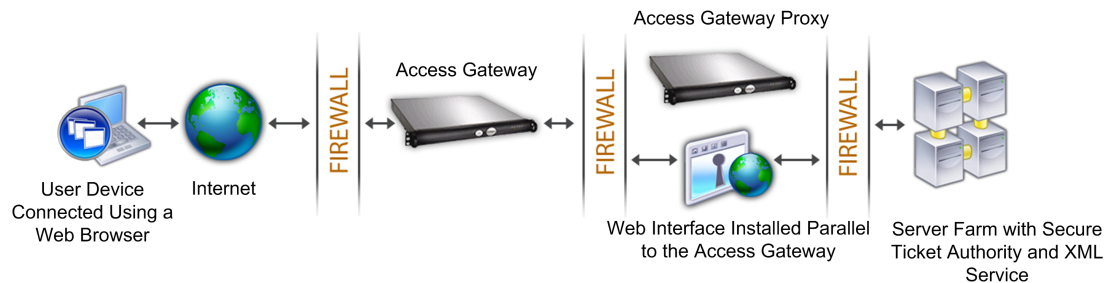


Figure 1. Basic communication flow for connection completion in a double-hop DMZ

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 launches Citrix Receiver.  
**Note:** The ICA file contains code that instructs the Web browser to launch Receiver.
- Receiver initiates an ICA connection to Access Gateway in the first DMZ.
- Access 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. This communication is proxied through the second DMZ by the Access Gateway proxy.
- Access Gateway in the first DMZ completes the ICA connection to the online plug-ins.
- Receiver can now communicate through both Access 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 Access Gateway in the first DMZ.
2. Access Gateway in the first DMZ contacts the STA in the internal network for ticket validation. To contact the STA, Access Gateway establishes a SOCKS or SOCKS with SSL connection to the Access Gateway proxy in the second DMZ.
3. The Access 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 Access Gateway proxy in the second DMZ, which is passed to Access 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. Access Gateway in the first DMZ incorporates the address of the XenApp server into the user connection packet and sends this packet to the Access Gateway proxy in the second DMZ.
6. The Access Gateway proxy in the second DMZ makes a connection request to the server specified in the connection packet.
7. The server responds to the Access Gateway proxy in the second DMZ. The Access Gateway proxy in the second DMZ passes this response to Access Gateway in the first DMZ to complete the connection between the server and Access Gateway in the first DMZ.
8. Access 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 Access Gateway in the first DMZ and the Access Gateway proxy in the second DMZ.

---

# Preparing for a Double-Hop DMZ Deployment

To prepare appropriately for a double-hop DMZ deployment, you must answer the following questions before you begin the deployment. Answering these questions before you begin the deployment will help you avoid unnecessary problems when performing the deployment procedures.

- 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 remaining topics in this section contain information to help you answer these questions appropriately for your environment.

## Components Required to begin the Deployment

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

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

Additional certificates are needed if you want to encrypt connections occurring among the other components in a double-hop DMZ deployment.

---

# Installing the Access Gateway in a Double-Hop DMZ

There are several steps required to deploy the Access Gateway in a double-hop DMZ. This includes installation of the appliances in both DMZs and configuring the appliances for client connections.

The tasks to deploy Access Gateway appliances in a double-hop DMZ include:

- [Step 1: Installing an Access Gateway in the First DMZ](#)
- [Step 2: Configuring the First Access Gateway](#)
- [Step 3: Installing an Access Gateway in the Second DMZ](#)
- [Step 4: Configuring a Virtual Server on the Access Gateway Proxy](#)
- [Step 5: Configuring the Access Gateway to Communicate with the Access Gateway Proxy](#)
- [Step 6: Binding the Access Gateway in the Second DMZ Globally or to a Virtual Server](#)
- [Step 7: Configuring the Access Gateway to Handle the STA and ICA Traffic](#)
- [Step 8: Opening the Appropriate Ports on the Firewalls](#)
- [Step 9: Managing SSL Certificates in a Double-Hop DMZ Deployment](#)

---

# Step 1: Installing an Access Gateway in the First DMZ

To install the Access Gateway in the first DMZ, follow the instructions in [Access Gateway Appliances](#).

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



---

## Step 2: Configuring the First Access Gateway

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

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

---

## Step 3: Installing an Access Gateway in the Second DMZ

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

Follow the instructions in [Access Gateway Appliances](#) to install each Access Gateway appliance in the second DMZ.

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

---

## Step 4: Configuring a Virtual Server on the Access Gateway Proxy

Create a virtual server on the Access Gateway proxy. On Access Gateway in the first DMZ, configure the virtual server to communicate with Access Gateway in the second DMZ. You do not need to configure authentication or policies on the Access Gateway proxy. Citrix recommends disabling authentication on the virtual server.

### To disable authentication on the virtual server

1. In the configuration utility, in the navigation pane, click Access Gateway > Virtual Servers.
2. In the details pane, click a virtual server and then click Open.
3. On the Authentication tab, under User Authentication, clear Enable Authentication and then click OK.

---

# Step 5: Configuring the Access Gateway to Communicate with the Access Gateway Proxy

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

If you deployed multiple appliances in the second DMZ, you must configure each Access Gateway in the first DMZ to communicate with every Access Gateway appliance in the second DMZ.

You can use this procedure to enable an Access Gateway in the first DMZ to communicate with one or more Access Gateway appliances in the second DMZ.

1. In the Access Gateway Policy Manager, under Available Policies / Resources, click Next Hop Servers.
2. Under Related Tasks, click Create a new next hop server.
3. In Name, type a name for the first Access Gateway.
4. In IP address, type the virtual server IP address of the Access Gateway proxy in the second DMZ.
5. In Port, type the port number, click Create, and click Close. If you are using a secure port, such as 443, select Secure. This check box is enabled by default.

Each Access Gateway installed in the first DMZ must be configured to communicate with all Access Gateway proxy appliances installed in the second DMZ.

---

# Step 6: Binding Access Gateway in the Second DMZ Globally or to a Virtual Server

After you configure Access Gateway in the second hop, you can bind it to either the Access Gateway global level or to virtual servers configured on Access Gateway in the first DMZ.

Perform this procedure on each appliance installed in the second DMZ.

## To bind Access Gateway globally or to a virtual server

1. In the Access Gateway Policy Manager, do one of the following
  - Under Configured Resources / Policies, expand the node for Access Gateway Global
  - Under Configure Resources / Policies, expand the node for Virtual Server and then expand the node for a virtual server in the list
2. Under Available Resources / Policies, under Next Hop Servers, click and drag a configured server to Next Hop Server under Access Gateway Global or Virtual Servers.

---

# Step 7: Configuring Access Gateway to Handle the STA and ICA Traffic

When you deploy Access Gateway in a double-hop DMZ, you must configure Access 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.

Configure Access Gateway in the first DMZ to communicate with the STA running in the internal network. After you configure the STA, you can bind the STA either globally or to a virtual server.

## To bind the STA globally or to a virtual server

1. In the Access Gateway Policy Manager, do one of the following
  - Under Configured Resources / Policies, expand the node for Access Gateway Global
  - Under Configure Resources / Policies, expand the node for Virtual Server and then expand the node for a virtual server in the list
2. Click STA Servers and under Related Tasks, click Bind new STA server.
3. In URL, type the path to the server running the STA, such as `http://mycompany.com` or `http://ipAddress` and then click Create.

# Step 8: Opening the Appropriate Ports on the Firewalls

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 a detailed discussion of 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.

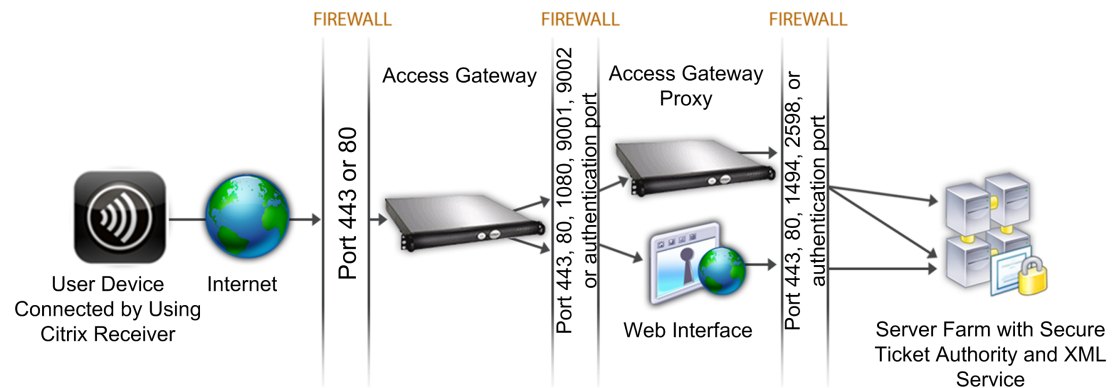


Figure 1. Ports in a double-hop DMZ deployment

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

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

Connections through the second firewall	Ports used

## Step 8: Opening the Appropriate Ports on the Firewalls

Access Gateway in the first DMZ connects to the Web Interface in the second DMZ.	Open either TCP port 80 for an unsecure connection or TCP port 443 for a secure connection through the second firewall.
Access Gateway in the first DMZ connects to Access Gateway in the second DMZ.	Open TCP port 443 for a secure SOCKS connection through the second firewall.
If you enabled authentication on Access 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
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.
The Web Interface in the second DMZ connects to the Secure Ticket Authority (STA) hosted on a server in the internal network.	
Access Gateway in the second DMZ connects to the STA residing in the secure network.	
Access Gateway in the second DMZ makes an ICA connection to a published application 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 Access 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.



---

# Step 9: Managing SSL Certificates in a Double-Hop DMZ Deployment

You must install the SSL certificates necessary to secure (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 table below 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 the Access Gateway in the first DMZ.	The Access 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 CA as the server certificate on the Access Gateway.
XenApp Plug-ins from the Internet connects to the Access Gateway in the first DMZ.	The certificate management for this connection is the same as the Web browser to Access Gateway connection described above. If you installed the certificates to encrypt the Web browser connection, this connection is also encrypted using those certificates.

The table below 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
The Access Gateway in the first DMZ connects to the Web Interface in the second DMZ.	The Web Interface must have an SSL server certificate installed.  The Access 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.

Step 9: Managing SSL Certificates in a Double-Hop DMZ Deployment

<p>The Access Gateway in the first DMZ connects to the Access Gateway in the second DMZ.</p>	<p>The Access Gateway in the second DMZ must have an SSL server certificate installed.</p> <p>The Access Gateway in the first DMZ must have a root certificate installed that is signed by the same CA as the server certificate on the Access Gateway in the second DMZ.</p>
--	---

The 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
<p>The Web Interface in the second DMZ connects to the XML Service hosted on a server in the internal network.</p>	<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>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>
<p>The Web Interface in the second DMZ connects to the STA hosted on a server in the internal network.</p>	<p>The certificate management for this connection is the same as the Web Interface to XML Service connection described immediately above. 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.)</p>
<p>The Access Gateway in the second DMZ connects to the STA hosted on a server in the internal network.</p>	<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>The Access 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>

## Step 9: Managing SSL Certificates in a Double-Hop DMZ Deployment

---

The Access Gateway in the second DMZ makes an ICA connection to a published application on a server in the internal network.

An SSL server certificate must be installed within the SSL Relay on the server hosting the published application.

The Access 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.

---

# Configuring DNS Virtual Servers

To configure a DNS virtual server, you specify a name and IP address. Like the Access 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.

## To configure a DNS virtual server

1. In the configuration utility, 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 Access Gateway through one of the following two methods, depending on the needs of your deployment:

- Bind the server globally to Access 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

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 Access 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 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, 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 [Configuring DNS Virtual Servers](#) 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

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

For each user logged on to Access 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 VNC client can access the user device for diagnosing a problem application. It is also possible for two Access Gateway users with internal network IP addresses who are remotely logged on to communicate with each other through Access 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 Access 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 Access Gateway. The internal network IP address that is assigned to each user device logged on to Access Gateway is used for these connections. The different types of server-initiated connections that Access 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. Access 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 Access 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. Access Gateway supports connections between plug-ins through the use of the internal network IP addresses.

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

If a user logged on to Access Gateway does not execute a clean logoff (the logoff request did not reach the appliance), the user can log on again using any device and replace the previous session with a new session. This feature might be beneficial in deployments where one IP address is appended per user.

When an inactive user logs on to Access 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 Access 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.

---

# Maintaining the Access Gateway

After the Access Gateway is configured, you can maintain and monitor the Access Gateway. This includes:

- [Upgrading the Access Gateway](#)
- [Configuring Delegated Administrators](#)
- [Viewing Access Gateway Configuration Settings](#)
- [Clearing the Access Gateway Configuration](#)
- [Managing User Sessions](#)
- [Configuring Auditing on the Access Gateway](#)



---

# Configuring Delegated Administrators

The Access 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 change the administrator password.

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

A delegated administrator is configured using command policies and system users and groups. Command policies are rules that control what individual users can access and do on the Access Gateway. Command policies allow you to define what parts of the Access Gateway configuration a user or group is allowed to access and modify. You can also regulate which commands, command groups, virtual servers, and other elements administrators and groups are permitted to configure.

The Access Gateway has a default deny system command policy. Command policies cannot be bound globally. The policies must be bound 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 the Access Gateway.

All administrators inherit the policies of the groups to which they belong. When configuring delegated administration, assign priorities to the administrator or group so the Access Gateway can determine which policy takes precedence.

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

- Add a system user
- Add a system group
- Create a command policy
- Bind the command policy to the user or group by setting the priority

---

# Configuring Command Policies for Delegated Administrators

Access 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 Access Gateway

1. In the configuration utility, in the navigation pane, expand System and then click 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. Under Member of, in Available Groups, select a group and then click Add.
6. Under Command Policies, select a policy, in Priority type a number, click OK and then click Close.

## Creating Administrative Groups

When you are configuring an administrative user on the appliance, you can add the user to a group. You can create a new group from within the Create User dialog box or by using the configuration utility.

## **To create an administrative group from within the Create User dialog box**

1. In the configuration utility, in the navigation pane, expand System and then click Users.
2. In the Create User dialog box, under Member of, click New.
3. In Group Name, type a name for the group, select a user and then click Create.

## **To configure an administrative group by using the configuration utility**

1. In the configuration utility, in the navigation pane, expand System and then click 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, under Members > Available Users, select a user and then click Add.
5. Under Command Policies, select a policy or policies, click Create and then click Close.

## **To configure an administrative user from within the Create Group dialog box**

When creating a new administrative group, you can also create a new user.

1. In the Configure Group dialog box, under Members, click New.
2. In User Name type a user name.
3. In Password and Confirm Password, type the password
4. Under Command Policies, select a policy and then click Create.

The new user appears under Configured Users in the Configure Group dialog box.

---

# Configuring Custom Command Policies for Delegated Administrators

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 Access 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, in the navigation pane, expand System 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, expand System 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, in the navigation pane, expand System and then click Users or click 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 Access Gateway Configuration Settings

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

- Saved configuration, which is where you have saved your settings on the Access Gateway
- Running configuration, which is where you configured settings, such as a virtual server or authentication policy, and have not saved the configuration to the Access Gateway
- Running versus saved configuration where you can compare side-by-side the running and saved configuration on the Access Gateway

In addition to viewing configuration settings, you can configure settings using a batch file. The batch file contains a list of configuration commands that you can use to configure the Access Gateway. The batch file can reside on the Access Gateway or a computer in your network. You can type the commands in the Batch Configuration dialog box.

You can also clear configuration settings on the Access Gateway.

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

---

# Saving the Access Gateway Configuration

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

## To save the configuration on Access Gateway

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

## To view the saved configuration on Access Gateway

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

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

## To save the Access Gateway configuration to a file on your computer

When you configure settings on Access Gateway, you can save the settings to a file on your computer. If you need to reinstall the Access 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 Access Gateway and restart the appliance by using the command-line interface or a program, such as WinSCP, to copy the file to Access Gateway.

1. In the configuration utility, in the navigation pane, expand System and 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 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 Access Gateway that occur without an effort to save them is called the *running configuration*. These settings are active on Access 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, in the navigation pane, expand System and click Diagnostics.
2. In the details pane, under View Configuration > Configuration Difference, 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, in the navigation pane, expand System and click Diagnostics.
2. In the details pane, under View Configuration, click Saved v/s running configuration.



---

# Clearing the Access Gateway Configuration

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

**Important:** Citrix recommends saving your configuration before you clear the Access 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.
- **All.** Restores the configuration to the original factory settings including the system IP 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 Access 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 Access Gateway. After you restore the file to the appliance and restart Access 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 Access 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 Access Gateway configuration settings

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

The Access Gateway allows logging of all the states and status information collected, so you can see the event history in chronological order. The messages contain information about the event that generated the message, a time stamp, the message type, and predefined log levels and message information. The Access Gateway also provides control over the information that is logged and the location where these messages are stored.

The Access 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 Access Gateway logs to provide any of the following information:

Level	Description
EMERGENCY	Only major errors in the Access Gateway are logged. Entries in the log indicate that the Access Gateway is experiencing a critical problem that is causing it to be unusable.
ALERT	Logs problems that might cause the Access Gateway to function incorrectly, but are not critical to its operation. Corrective action should be taken as soon as possible to prevent the Access Gateway from experiencing a critical problem.
CRITICAL	Logs critical conditions that do not restrict the Access Gateway's operation, but that might escalate to a larger problem.
ERROR	Displays messages that result from some failed operation on the Access Gateway.
WARNING	Displays potential issues that could result in an error or a critical error.
NOTICE	Displays more in-depth issues than the information level log, but serves the same purpose as notification.

Compression statistics for the Access Gateway are also stored in the Access Gateway audit log if the TCP compression feature is configured. The compression ratio achieved for different data is stored in the log file for each user session on the Access Gateway in the log file.

With the release of Version 9.1, the log signature *Context* is replaced with a *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 client 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 Access Gateway

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

## To create an auditing policy

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies/Resources, click Auditing Policies.
4. Under Related Tasks, click Create new auditing policy.
5. In Name, type a name for the policy.
6. In Auditing Type, select one of the following:
  - Syslog if you want to send the logs to a Syslog server.
  - Nslog to store the logs on Access Gateway.
7. Next to Server, click New.
8. Type the following information for the server information where the logs are stored:
  - a. In Name, type the name of the server.
  - b. Under Server, type the IP Address and Port.
  - c. Under Log Levels, select the level of logging.
  - d. Next to Select date format, select how you want the date on the log to appear, click Create and then click Close.

## To bind an auditing policy

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

- System global
- Access Gateway global
- Virtual servers

- Groups
- Users
- In the Access Gateway Policy Manager, under Available Policies / Resources, click an auditing policy and then drag it to the Auditing Policies node for the entities you chose from the preceding list.

## To modify an auditing policy

You can modify an existing auditing policy to alter the logging options.

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies/Resources, click Auditing Policies.
4. Click the audit policy.
5. Under Related Tasks, click Modify auditing policy.
6. In the Configure Auditing Policy dialog box, click Modify.
7. Select the changes and then click OK twice.

## To remove an auditing policy

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

1. In the configuration utility, in the navigation pane, click Access Gateway.
2. In the details pane, under Policy Manager, click Change group settings and user permissions.
3. In the Access Gateway Policy Manager, under Available Policies/Resources, click Auditing Policies.
4. Click the policy, under Related Tasks, click Remove auditing policy and then click Yes.

---

# Configuring ACL and TCP Logging

You can configure the Access 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 is enabled.

Logging can be enabled 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. For information on how to enable logging globally, see [Configuring Auditing on the Access Gateway](#).

To optimize logging, when multiple packets from the same flow match an ACL, only the first packet's details are logged, and 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

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 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 Network and click ACLs.
2. In the details pane, click the Extended ACLs tab, and then select the ACL for which you want to configure logging and click Open.
3. In the Modify ACL dialog box, select the Log State check box.
4. In the Log Rate Limit text box, type the rate limit that you want to specify for the rule and click OK.

After you configure ACL logging, you can enable it on the Access Gateway. Create an auditing policy and then bind it to a user, group, virtual server, or globally. To create an auditing policy, see [Configuring Logs on Access Gateway](#).

## To enable ACL or TCP logging on the Access Gateway

1. In the configuration utility, in the navigation pane, expand Access Gateway > Policies and click Auditing.
2. In the details pane, click Add.
3. In Name, type a name for the policy.
4. In Auditing Type, select either syslog or nslog.
5. Next to Server, click New.
6. In the Create Auditing Server dialog box, in Name, type a name for the server and configure the settings
7. Click ACL Logging or TCP Logging and then click Create twice.

---

# Enabling Access Gateway Plug-in Logging

You can configure the Access Gateway Plug-in to log all errors to text files that are stored on the user device. Users can configure the Access 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 Access 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`

You can use these log files to troubleshoot the Access 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 Access Gateway Plug-in. The logging levels are:

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

## To enable logging

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

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



---

# To monitor ICA connections

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 Access Gateway.
  2. In the details pane, under Monitor Connections, click ICA connections.