Web Interface Administrator’s Guide

For other guides in this document set, go to the Document Center

Citrix® Web Interface 4.5

Citrix Access Suite™

Document Code: August 8, 2006 11:12 am (ER)

Contents

Chapter 1 Introduction

Chapter 2 Deploying the Web Interface

Chapter 4 Managing Servers and Farms

Chapter 5 Configuring Authentication for the Web Interface

Chapter 6 Managing Clients

Chapter 7 Customizing the User Experience

Chapter 8 Configuring Web Interface Security

Appendix A Configuring Sites Using the Configuration File

Appendix B Configuring ADFS Support for the Web Interface

Introduction

Overview

Welcome to the Web Interface. This chapter introduces you to the documentation and to the Web Interface. Topics include:

- How to Use this Guide
- Introducing the Web Interface
- What's New in this Release

How to Use this Guide

The *Web Interface Administrator's Guide* is for Citrix administrators and Web masters responsible for installing, configuring, and maintaining Access Platform, Program Neighborhood Agent Services, and Conferencing Manager Guest Attendee sites.

This is a task-based guide to help you set up the Web Interface quickly and easily. This chapter introduces the documentation and the Web Interface, and describes what's new in this version. Subsequent chapters explain how to deploy and configure the Web Interface.

This guide assumes knowledge of Citrix Presentation Server for Windows or Citrix Presentation Server for UNIX.

Getting More Information and Help

This section describes how to get more information about the Web Interface and how to contact Citrix.

Accessing Product Documentation

The documentation for the Web Interface includes online documentation, known issues information, integrated on-screen assistance, and application help as follows:

- Online documentation is provided as Adobe Portable Document Format (PDF) files. Use the Document Center to access the complete set of online guides.
- Be sure to read the Readme.htm file in the \Documentation directory of the product CD before you install the Web Interface or during troubleshooting. This file contains important information that includes last-minute documentation updates and corrections.
- In many places in the user interface, integrated on-screen assistance is available to help you complete tasks. For example, in the Access Management Console, you can position your mouse over a setting to display help text that explains how to use that control.
- Online help is available for some tasks. You can access the online help from the Help menu or Help button.
- For information about terminology related to Presentation Server, see the *Citrix Presentation Server Glossary* that is available from the Document Center.

Important To view, search, and print the PDF documentation, you need to have Adobe Acrobat Reader 5.0.5 with Search or Versions 6 or 7. You can download Acrobat Reader for free from Adobe Systems’ Web site at http://www.adobe.com/.

To provide feedback about the documentation, go to www.citrix.com and click **Support > Knowledge Center > Product Documentation**. To access the feedback form, click the **Submit Documentation Feedback** link.

Accessing the Document Center

The Document Center provides a single point of access to the documentation and enables you to go straight to the section in the documentation that you need. It also includes:

- A list of common tasks and a link to each item of documentation.
- A search function that covers all the PDF guides. This is useful when you need to consult a number of different guides.
- Cross-references between documents. You can move among documents as often as you need using the links to other guides and the links to the Document Center.

You can access the Document Center from your product CD or use Presentation Server Setup to install the Document Center on your servers.

To start the Document Center

1. From your product CD-ROM, navigate to the \Documentation folder.

   —Or—

   From a server on which you installed the Document Center, select **Documentation** from the Citrix program group on the server's Start menu.

2. Open **document_center.pdf**. The Document Center appears.

If you prefer to access the guides without using the Document Center, you can navigate to the component PDF files using Windows Explorer. If you prefer to use printed documentation, you can also print each guide from Acrobat Reader.

Document Conventions

Presentation Server documentation uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

Convention	Meaning
Boldface	Commands, names of interface items such as menu names, text boxes, option and radio buttons, and user input at command lines.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics also are used for new terms, the titles of books, and variables.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name you specify when you install Windows.
`Monospace`	Example text from a text file.

Convention	Meaning
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [**/ping**] means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename*[,…] means you can type additional *devicenames* separated by commas.

UNIX Command-Line Conventions

Presentation Server for UNIX operating systems and some other components that run on UNIX platforms have command line interfaces. If you are not familiar with UNIX command lines, note that:

- All UNIX commands are case-sensitive
- The spacing on the command line is important and must be followed exactly as described in the instruction

Getting Service and Support

Citrix provides technical support primarily through the Citrix Solutions Network (CSN). Our CSN partners are trained and authorized to provide a high level of support to our customers. Contact your supplier for first-line support or check for your nearest CSN partner at http://www.citrix.com/support/.

In addition to the CSN channel program, Citrix offers a variety of self-service, Web-based technical support tools that include the following:

- The Citrix Knowledge Center, an interactive tool containing thousands of technical solutions to support your Citrix environment
- Support Forums, where you can participate in technical discussions and search for previous responses from other forum members
- Software downloads for access to the latest service packs, hotfixes, and utilities
- Downloadable clients available at http://www.citrix.com/download/

Another source of support, Citrix Preferred Support Services, provides a range of options that allows you to customize the level and type of support for your organization’s Citrix products.

Introducing the Web Interface

The Web Interface provides users with access to Presentation Server applications and content through a standard Web browser or through the Program Neighborhood Agent. It also enables guest users to attend Conferencing Manager conferences.

The Web Interface employs Java and .NET technology executed on a Web server to dynamically create an HTML depiction of server farms for Access Platform sites. Users are presented with all the applications published in the server farm(s) you make available. You can create standalone Web sites for application access or Web sites that can be integrated into your corporate portal. Additionally, the Web Interface allows you to configure settings for users accessing applications through the Program Neighborhood Agent and create sites for guest users logging on to Conferencing Manager.

You can configure Web Interface sites created on both Windows and UNIX platforms using the Access Management Console. The Access Management Console can be installed on Windows platforms only. For more information about using this tool, see “Configuring Sites Using the Console” on page 43.

You can also edit the configuration file (WebInterface.conf) to create and manage Access Platform sites. For more information, see “Configuring Sites Using the Configuration File” on page 137.

In addition, you can customize and extend Access Platform sites. The *Customizing the Web Interface Guide* explains how to configure sites using these methods.

The Web Interface Features

This section provides information about the Web Interface’s features. For details about software requirements for particular Web Interface features, see “Additional Software Requirements” on page 27.

Access Platform Sites

The Web Interface provides functionality to create and manage Access Platform sites. Users access remote and streaming applications and content using a Web browser and a client.

Program Neighborhood Agent Services Sites

The Program Neighborhood Agent is a client designed for flexibility and ease of configuration. Using the Program Neighborhood Agent in conjunction with the Web Interface, you can integrate published resources with users' desktops. Users access remote and streamed applications, desktops, and content by clicking icons on their desktop, in the Start menu, in the notification area, or any combination thereof. You can determine what, if any, configuration options your users can access and modify, such as audio, display, and logon settings.

Conferencing Manager Guest Attendee Sites

The Web Interface provides guest attendees with access to Conferencing Manager conferences through a standard Web browser. A guest attendee is a person who is invited to join a conference and either does not have, or does not want to use, a Windows NT domain name. Guest attendees access the conference through the Web Interface and use a locked down version of the published Conferencing Manager application. They have the following restrictions:

- They cannot create or start conferences
- They cannot launch applications within a conference

For more information about Conferencing Manager, see the *Citrix Conferencing Manager Administrator's Guide*.

Management Features

The Access Management Console. You can use the Access Management Console to perform day-to-day administration tasks quickly and easily. For example, you can use the console to specify the settings that users can select and to configure user authentication to the Web Interface. Your configuration takes effect as you make changes using the console.

Centralized configuration support. You can store site configuration in a centralized location on any server running the Configuration Service. Typically, this is also the server running the Citrix XML Service. Using centralized configuration enables you to configure a site from any server within a farm running the Access Management Console.

Management of multiple sites as a group. You can group sites together for ease of administration. A single configuration is stored with the configuration service and applied to all sites within a group.

Multiple server farm support. You can configure multiple server farms and provide users with a display of the applications available to them from all farms. You can configure each server farm individually using the **Manage server farms** task. For more information, see “Configuring Communication with Presentation Server” on page 153.

Integration with popular Web technologies. The Web Interface’s API can be accessed from Microsoft’s ASP.NET and Sun Microsystems’ JavaServer Pages.

Application Access Features

Support for servers on UNIX platforms. Support for Presentation Server for UNIX farms allows the Web Interface to display and launch applications running on UNIX platforms on your users’ client devices.

Backup servers. You can configure backup servers to ensure that users still have access to their applications in the event of a server failure.

Novell Directory Services (NDS) support. The Web Interface provides support for NDS authentication. When you enable this feature, the Web Interface Login page contains a context field. You can also configure the Web Interface to allow users to search for their user name in the tree to determine which context they are in.

Active Directory and User Principal Name (UPN) support. All Web Interface components are compatible with Microsoft Active Directory. Users visiting Access Platform sites can log on to server farms that are part of an Active Directory deployment and seamlessly access published applications. The logon pages are compatible with Active Directory’s use of User Principal Names.

Anonymous users. This feature allows users to log on to Access Platform sites using an anonymous account.

Launching of published content. The Web Interface supports the content publishing features of Presentation Server.

Security Features

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) support. The Web Interface supports SSL to secure communication between the server running the Web Interface and server farms. Implementing SSL on your Web server together with Web browsers that support SSL ensures the security of data as it travels through your network. The Web Interface uses Microsoft's Schannel security protocol on Windows platforms for Access Platform sites. This protocol uses FIPS 140 validated cryptography, a standard required by some organizations. For more information about FIPS 140 validation, see the National Institute of Standards and Technology (NIST) Web site (http://csrc.nist.gov/cryptval/).

Citrix Access Gateway support. The Access Gateway is a universal Secure Socket Layer (SSL) virtual private network (VPN) appliance that, together with the Web Interface, provides a secure single point-of-access to any information resource — both data and voice. The Access Gateway combines the best features of Internet Protocol Security (IPSec) and SSL VPN, without the costly and cumbersome implementation and management, works through any firewall and supports all applications and protocols.

Secure Gateway for Presentation Server support. The Secure Gateway, together with the Web Interface, provides a single, secure, encrypted point of access through the Internet to servers on your internal corporate networks. The Secure Gateway simplifies certificate management, because a server certificate is required only on the Secure Gateway server, rather than on every server in the server farm.

Ticketing. This feature provides enhanced authentication security. The Web Interface obtains tickets that authenticate users to published applications. Tickets have a configurable expiration period and are valid for a single logon. After use, or after expiration, a ticket is invalid and cannot be used to access applications. Use of ticketing eliminates the explicit inclusion of credentials in the ICA files the Web Interface uses to launch applications.

Client Deployment Features

Web-based client installation. You can use the Web Interface to deploy the Clients for Windows to any device that has a Web browser. When a user visits an Access Platform site, the client installation code detects the device and Web browser types and prompts the user to install an appropriate client.

Program Neighborhood Agent support. The Program Neighborhood Agent allows users to access Presentation Server applications directly from the Windows desktop without using a Web browser. The Program Neighborhood Agent user interface can also be "locked down" to prevent user misconfiguration.

Citrix Streaming Client support. The Citrix Streaming Client allows users to stream applications to their desktop and open them locally. You can either install the streaming client with the Program Neighborhood Agent to provide the full set of Citrix application streaming features or install the streaming client alone on the user's desktop so the user can access published applications through a Web browser using an Access Platform site.

What's New in this Release

The Web Interface offers the following new enhancements and features in this release:

Support for access control policies. The Web Interface provides support for access control policies, allowing administrators to control access to available applications on computers running Presentation Server through the use of Advanced Access Control policies and filters. This permits the use of endpoint analysis as a condition of application access, along with other factors. If you want to provide secure access to resources using the Advanced Access Control option you must provide details of the Access Gateway when configuring sites.

Note Access control policy support is available for Access Platform sites and on Windows platforms only.

Password expiration warning notices. You can configure password expiration warning notices to be shown to users for a set period of time before their domain password expires. Users can change their password at any time during this period and continue accessing resources.

Note Support for password expiration warning notices is available for Access Platform sites only.

Account self service support. Integration with Citrix Password Manager allows users to reset their network password and unlock their account, without contacting their administrator, by answering a series of simple security questions.

Note Account self service support is available for Access Platform sites only.

Active Directory Federation Services (ADFS) support. ADFS is a feature of Microsoft Windows Server 2003 R2 Enterprise Edition. ADFS provides single-sign on technology to authenticate a user to multiple Web applications in a single session. ADFS support for the Web Interface enables the resource partner of an ADFS deployment to use Presentation Server. Administrators can create ADFS integrated sites to provide users with access to published applications on the resource partner.

Note ADFS support is available for Access Platform sites and on Windows platforms only.

Published application URL support. This feature allows users to create links to published applications accessed using the Web Interface. These links can be added to the user's Favorites list or desktop.

Note Published application URL support is available for Access Platform sites only.

Support for the Citrix application streaming feature. With the Citrix application streaming feature, you can install and configure an application on one file server and deliver it to any desktop on demand. Upgrading or patching an application is simple, because you are only required to update or patch an application stored in one place: on the file server. Integration with the Web Interface provides users with access to streamed applications using a Web browser or the Program Neighborhood Agent and the Citrix Streaming Client.

Support for upgrades from previous versions of the Web Interface. The feature allows you to upgrade from version 3.0 or later of the Web Interface automatically. Existing locally configured sites are upgraded at installation. Existing centrally configured sites are upgraded using the **Upgrade Configuration** task in the Access Management Console.

Note Support for upgrades from previous versions of the Web Interface is supported on Windows platforms only.

Access Management Console alerts. The Web Interface now supports Access Management Console alerts. If a problem is detected, the Web Interface generates an alert in the Access Management Console. Administrators click on the alert in the console to access associated My Knowledge articles. These articles contain detailed information about a problem and its possible causes and resolutions.

Support for New Presentation Server Features

The Web Interface provides support for the following new Presentation Server features:

Program Neighborhood Agent Backup URLs. You can specify backup URLs for Program Neighborhood Agent. In the event of a failure users are connected to backup sites.

Enhanced proxy detection support. A new option in the **Edit Client-Side Proxy** dialog box is provided to detect a proxy server automatically, so you do not have to configure the proxy server manually. In larger environments, this feature also saves you the time of supporting incorrect or dynamic configurations.

Non-administrator client installation. This feature allows client users who do not have administrator privileges on a remote computer, such as at an Internet cafe or kiosk, can install a modified version of the Web Client. The client is packaged in the Ica32Pkg.msi file with a modified installer program. It can be downloaded and installed locally on all supported Windows platforms to allow users secure access to their applications on the server.

Multilingual User Interface (MUI) client for Windows. The Windows Installer package for the client includes a multi-lingual user interface, meaning it automatically installs the clients in all supported languages. Beginning with version 10.0 of the Windows clients, language-specific installation packages are no longer available.

During the installation of the client, the user selects a language: English, German, French, Spanish, or Japanese. The user interface appears in the selected language.

Web Interface Components

A Web Interface deployment involves the interaction of three network components:

- One or more server farms
- A Web server
- A client device with a browser and a Citrix Presentation Server or Citrix Streaming Server Client

Server Farms

A *server farm* is a group of servers running Presentation Server managed as a single entity. A server farm is composed of a number of servers operating together to serve applications to Citrix Presentation Server Client users.

Important among a server farm’s standard capabilities is *application publishing*. This is an administrative task that lets administrators make available to users specific applications hosted by the server farm. When an administrator publishes an application for a group of users, that application becomes available as an object to which clients can connect and initiate client sessions.

Program Neighborhood automates the client-side configuration process by eliminating the need for administrators or client users to browse the network for published applications. Using Program Neighborhood, users can log on to the server farm and receive a customized list of applications published for their individual user name. This list of applications is called an *application set*.

The server running the Web Interface functions as a Program Neighborhood interface for connecting to one or more server farms. The server running the Web Interface queries server farms for application set information and then formats the results into HTML pages that users can view in a Web browser.

To communicate with server farms, the server running the Web Interface communicates with the Citrix XML Service running on one or more servers. The Citrix XML Service is a Presentation Server component that provides published application information to clients and servers running the Web Interface using TCP/IP and HTTP. This service functions as the contact point between the server farm and the server running the Web Interface. The Citrix XML Service is installed with Presentation Server for Windows, and Presentation Server for UNIX.

Web Server

The Web server hosts the Web Interface. The Web Interface provides the following services:

- Authenticate users to a server farm or farms
- Retrieve application information, including a list of applications a user can access

Client Device

A *client device* is any computing appliance capable of executing a Citrix Presentation Server Client and a Web browser. Client devices include desktop PCs and network computers, among others.

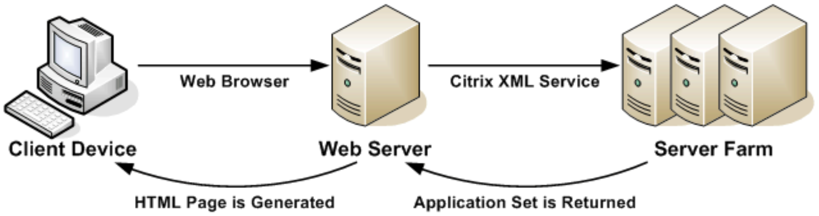
In a client device, the browser and client work together as a viewer and engine. The browser lets users view application sets (created by server-side scripting on the server running the Web Interface) while the client acts as the engine that launches published applications.

The Web Interface provides *Web-based client installation*. Web-based client installation is a method of deploying clients from a Web site. When a user visits a site created with the Web Interface, the Web-based client installation code detects the device and the Web browser prompts the user to install an appropriate client. In the case of Windows devices, Web-based client installation can also detect the presence or absence of an installed client and prompt the user only if necessary. See “Automatically Deploying Clients” on page 102 for more information.

The Web Interface supports many browser/client combinations. For a complete list of supported browser/client combinations, see “Citrix Presentation Server Client Device Requirements” on page 31.

How the Web Interface Works

The following section describes a typical interaction between server farms, a server running the Web Interface, and a client device.



This diagram shows an example of a typical Web Interface interaction. The browser on the client device sends information to the Web server, which communicates with the server farm to allow users to access their applications.

1. Client device users utilize a Web browser to view the **Login** page and enter their user credentials.
2. The Web server reads users' credentials and forwards the information to the Citrix XML Service on servers in the server farms. The designated server acts as a broker between the Web server and servers.
3. The Citrix XML Service on the designated server then retrieves a list of applications from the servers that users can access. These applications comprise the user’s *application set*. The Citrix XML Service retrieves the application set from the Independent Management Architecture (IMA) system.

   In a farm running Presentation Server for UNIX, the Citrix XML Service on the designated server uses information gathered from the ICA browser to determine which applications the user can access.

   The Citrix XML Service then returns the user’s application set information to the Web Interface running on the server.

4. The user initiates the next step by clicking an application icon in the HTML page.
5. The Citrix XML Service is contacted to locate the server in the farm that is the least busy. The XML Service requests a ticket from the least busy server corresponding to the user’s credentials. The XML Service returns the least-busy server’s address and ticket to the Web Interface.
6. The Web Interface generates a customized ICA file and sends it to the Web browser.
7. The Web browser receives the file and passes it to the client device.
8. The client receives the file and initiates a client session with a server according to the file’s connection information.

What to Do Next

For information about system requirements, instructions for installing the Web Interface, and configuring the server running the Web Interface, see “Deploying the Web Interface” on page 25.

Deploying the Web Interface

Overview

This chapter explains how to install the Web Interface on your server and configure the server to run the Web Interface. Topics include:

- System Requirements
- Installing the Web Interface
- Troubleshooting the Web Interface Installation
- Uninstalling the Web Interface

System Requirements

The following section describes server, Web server, and client device requirements for the Web Interface.

Server Requirements

To run the Web Interface, your servers must meet the following requirements.

Supported Citrix Presentation Server Versions

The Web Interface requires one of the following platforms:

- Citrix Presentation Server 4.5 for Windows Server 2003
- Citrix Presentation Server 4.5 for Windows Server 2003 R2
- Citrix Presentation Server 4.5 for Windows Server 2003 x64 Editions
- Citrix Presentation Server 4.0 for Windows Server 2003
- Citrix Presentation Server 4.0 for Windows Server 2003 x64 Editions
- Citrix Presentation Server 4.0 for Windows 2000 Server
- Citrix MetaFrame Presentation Server 3.0 for Windows Server 2003
- Citrix MetaFrame Presentation Server 3.0 for Windows 2000 Server
- Citrix MetaFrame Presentation Server for UNIX Operating Systems
- MetaFrame XP for Windows, Service Pack 2 for Terminal Services Edition
- MetaFrame XP for Windows, Service Pack 3 for Windows 2000 Server
- MetaFrame XP for Windows, Service Pack 3 for Windows Server 2003
- MetaFrame for UNIX Operating Systems Version 1.2

The Web Interface operates with these Presentation Server versions on all of their supported platforms. For a list of supported platforms, see the appropriate Presentation Server documentation. Citrix recommends that you have the latest version of the service pack installed on your system.

Access Management Console

To administer the Web Interface on Windows, you must install the Access Management Console. For information about installing the console, see the *Citrix Presentation Server Administrator's Guide*.

Additional Software Requirements

Without the feature releases, some new features will not be available. For example, to use the Enhanced Content Publishing feature with the Web Interface, you must have MetaFrame XP for Windows, Service Pack 2 and a Feature Release 2 license installed on all servers in the server farm.

The following table summarizes the additional software requirements for key Web Interface features.

Web Interface Feature	**Software Requirements**
Support for streamed applications	Citrix Presentation Server 4.5 Citrix Streaming Client Program Neighborhood Agent 10.0
ADFS support	Citrix Presentation Server 4.5 Client for 32-bit Windows 9.0
Access Control Policy support	Citrix Presentation Server 4.2 Citrix Access Gateway Advanced Access Control Client for 32-bit Windows 9.0
Account Self Service	Citrix Password Manager
Session reliability	Citrix Presentation Server 4.0 Client for 32-bit Windows 9.0
Workspace control	MetaFrame Presentation Server 3.0 or later Client for 32-bit Windows 8.0
Remote Desktop Connection	MetaFrame Presentation Server 3.0 or later
Ticketing	MetaFrame Presentation Server 3.0 or later MetaFrame XP 1.0 MetaFrame for UNIX 1.2 Client for 32-bit Windows 6.0 or later
NDS authentication	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 1 Client for 32-bit Windows 6.20 or later
DNS addressing	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 1 MetaFrame for UNIX 1.2 Client for 32-bit Windows 6.20 or later
Smart card support	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 2 Client for 32-bit Windows 6.30 or later

Web Interface Feature	Software Requirements
Enhanced Content Publishing	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 2 Client for 32-bit Windows 6.20 or later
Server-side firewall support	MetaFrame Presentation Server 3.0 or later MetaFrame XP 1.0 MetaFrame for UNIX 1.2
Client-side firewall support	Client for 32-bit Windows 6.0 or later for SOCKS Client for 32-bit Windows 6.30 or later for Secure Proxy
Load balancing	MetaFrame Presentation Server 3.0 or later MetaFrame XP 1.0 MetaFrame for UNIX 1.2
End-user change password	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 2
Pass-through authentication	MetaFrame Presentation Server 3.0 or later MetaFrame XP Feature Release 2 Full Program Neighborhood Client for Win32/Program Neighborhood Agent 6.20 or later
Secure Gateway support	MetaFrame Presentation Server 3.0 or later MetaFrame XP 1.0 MetaFrame for UNIX 1.2 Client for 32-bit Windows 6.20.986 or later

General Configuration Requirements

Servers must be members of a server farm. The servers in the farm must have applications published. For information about server farm membership and publishing applications in a server farm, see the *Citrix Presentation Server Administrator's Guide.*

Presentation Server for UNIX servers must also have applications published. In addition, these applications must be configured for use with the Web Interface. See the *Citrix Presentation Server for UNIX Administrator's Guide* for information about installing the Citrix XML Service for UNIX and configuring published applications for use with the Web Interface.

Web Server Requirements

A copy of the different Citrix Presentation Server Clients must be present on the server for Web-based installation of the clients. See "Citrix Presentation Server Client Device Requirements" on page 31 for information about supported client versions and "Copying Client Installation Files to the Web Server" on page 95 for information about copying the clients to the server running the Web Interface.

On Windows Platforms

You can use the Web Interface on the following Windows platforms and servers:

Operating System	Web Server	Software
Windows Server 2003	Internet Information Services 6.0	.NET Framework 2.0 Visual J#.NET 2.0 ASP.NET
Windows Server 2003 x64 Editions	Internet Information Services 6.0 in 32 bit mode	.NET Framework 2.0 Visual J#.NET 2.0 ASP.NET
Windows Server 2003 R2	Internet Information Services 6.0	.NET Framework 2.0 Visual J#.NET 2.0
Windows Server 2003 R2 x64 Editions	Internet Information Services 6.0 in 32 bit mode	.NET Framework 2.0 Visual J#.NET 2.0 ASP.NET

On Windows Server 2003 systems, you must configure your server to add the role of Application Server and install IIS and ASP.NET (which is a subcomponent of IIS). If IIS is not installed when you install .NET Framework 2.0, you must install IIS and reinstall the Framework, or install IIS and run the aspnet_regiis.exe -i command in the WINDOWS\Microsoft.NET\Framework\v2.0.50727 directory.

Note The .NET Framework and J# redistributable files are included on the Server CD-ROM in the Support folder.

On UNIX Platforms

You can use the Web Interface with the following UNIX configurations:

Operating System	Server	JDK	Servlet Engine
Red Hat Enterprise Edition	Apache 2.x	Sun 1.5.x	Tomcat 5.5.x
Red Hat Enterprise Edition	WebSphere Application Server 6.0.1.2	WebSphere	WebSphere
Solaris 10	WebLogic Server 9.0	WebLogic	WebLogic

Operating System	Server	JDK	Servlet Engine
Solaris 10	Sun Java System Application Server Platform Edition 8.1	Sun 1.4.x	Sun Java System Application Server

User Requirements

The following browser and operating system combinations are supported for users to log on to the Web Interface:

Browser	Operating System
Internet Explorer 6.x	Windows XP, Windows XP Professional x64 Edition, Windows 2000 with Service Pack 4, Windows 2003 with Service Pack 1, Windows Fundamentals for Legacy PCs
Safari 2.0	Mac OS X
Firefox 1.x	Windows XP, Windows 2000 with Service Pack 4, Windows 2003, Red Hat Enterprise Edition, Mac OS X
Mozilla 1.x	Solaris 10

Requirements for Access to Streamed Applications

The following browser and operating system combinations are supported for users to access streamed applications:

Browser	Operating System
Internet Explorer 6.x	Windows XP, Windows 2000 Professional with Service Pack 4
Firefox 1.x	Windows XP, Windows 2000 Professional with Service Pack 4

Requirements for Personal Digital Assistants

You can run the Web Interface with the following Windows-based Terminals and Personal Digital Assistants (PDAs) configurations:

Device	Operating System	Browser
HP iPAQ hx2410	Windows Mobile 2003 Second Edition	Pocket IE
HP iPAQ rx1950	Windows Mobile 2005	Pocket IE
HP t5510	WincCE.NET 4.2	Internet Explorer 6.0

Device	Operating System	Browser
WYSE 3125se	WincCE.NET 4.2	Internet Explorer 6.0
WYSE V30	WinCE 5.0	Internet Explorer 6.0
WYSE V90	Windows XPe with Service Pack 1	Internet Explorer 6.0

Citrix Presentation Server Client Device Requirements

To operate with the Web Interface, your client devices must have a supported client and Web browser. All clients that ship on the Components CD-ROM are compliant with the Web Interface. The Components CD-ROM is available in the Citrix Presentation Server media or clients are also available for free download from the Citrix Web site.

Citrix recommends that you deploy the latest clients to your users to ensure that they can take advantage of the latest features. The features and capabilities of each client differ—for information about supported client features, see the appropriate Administrator's Guide for the client in question.

Installing the Web Interface

This section explains how to install the Web Interface on your server. An overview of the installation is provided, together with instructions about how to install the Web Interface on different servers.

Installation Overview

You install the Web Interface using the Citrix Presentation Server CD-ROM.

If you install the Web Interface on Windows platforms running in Japanese, simplified Chinese, traditional Chinese, or Korean, do not log on to Windows with a user name containing multibyte characters.

For information about installing the Access Management Console, see the *Citrix Presentation Server Administrator's Guide*.

You can install the Web Interface on the following platforms:

- Microsoft Internet Information Services (IIS)
- Tomcat, Sun ONE, and WebSphere for UNIX

For more information about how to install the Web Interface, see "Installing the Web Interface on Windows Platforms" on page 33 and "Installing the Web Interface on UNIX Platforms" on page 34.

Security Considerations

Citrix recommends that, as with any Windows-based server, you follow Microsoft standard guidelines for configuring your Windows server.

Viewing the Citrix XML Service Port Assignment

During Web Interface site creation (Windows) or .war file generation (UNIX), you are prompted for the port number on which the Citrix XML Service is running. The Citrix XML Service is the communication link between the server farm and the server running the Web Interface. This section explains how to view the port number on which the Citrix XML Service is running.

To view the Citrix XML Service port assignment on Windows platforms

1. On a server in the farm, open the Access Management Console.
2. In the left pane, select the name of the server.
3. On the **Actions** menu, click **Properties**.
4. Select **XML Service** to view the port assignment.

   If during Presentation Server installation, you choose the option to share Internet Information Service's TCP/IP port with the XML Service, the Access Management Console displays **The XML service for this server is using the same port as IIS** as the port in use. In this case, to determine the Citrix XML Service port, you must locate the port used by Internet Information Service's WWW Service. By default, the WWW Service uses port 80.

To view the Citrix XML Service port assignment on UNIX platforms

On Presentation Server for UNIX servers, type **ctxnfusesrv -l** at a command prompt to view port information.

Note If necessary, you can change the port used on the server. For more information, see the appropriate *Citrix Presentation Server Administrator's Guide*.

Installing the Web Interface on Windows Platforms

Before installing the Web Interface, you must configure your server to add the role of Application Server and install IIS and ASP.NET.

If you are upgrading from a previous version of the Web Interface, the installer prompts you to back up your existing sites before upgrading them.

Note On IIS 6.0 running Windows Server 2003, each site is assigned to an Application Pool. The Application Pool configuration contains a setting that determines the maximum number of worker processes. If you change the default value of 1, you may not be able to run the Web Interface.

To install the Web Interface

1. Log on as an administrator.
2. If you are installing the Web Interface from the Citrix Presentation Server CD-ROM, insert the CD-ROM in your Web server's CD-ROM drive.

   If you downloaded the Web Interface from a download site, copy the file WebInterface.exe to your Web server. Double-click the file.
3. Select your language from the list. The language of your operating system is detected and is displayed as the default selection. Click **Next**.
4. On the **Welcome** page, click **Next**.
5. On the **License Agreement** page, select **I accept the license agreement** and click **Next**.
6. On the **Common Components** page, browse to a location for the common Web Interface components (the default is C:\Program Files\Citrix\Web Interface). Click **Next**.
7. On the **Clients** page, select **Install the clients from the Components CD-ROM**. Click **Browse** to search the Components CD-ROM or CD image for the client setup files.

   Setup copies the contents of the CD's Clients directory to the Web Interface Clients directory, typically C:\Program Files\Citrix\Web Interface\4.5\Clients. All Web sites created by the installation process assume that the Web server contains the client files in this directory structure.

   If you do not want to copy the clients to the Web server during Web Interface installation, select **Don't install the clients from the Components CD-ROM** and you can copy the clients to the server later.

8. Click **Next** to continue the installation.
9. When the installation is complete, click **Finish**.
10. Open the Access Management Console to begin creating and configuring your sites.

After installing the Web Interface, you can begin to manage your sites by configuring and running discovery. For more information, see "Configuring and Running Discovery" on page 44.

Installing the Web Interface on UNIX Platforms

This section describes how to install the Web Interface on Tomcat. For other UNIX platforms, refer to the platform's documentation and any accompanying documentation for the platform's administration tool.

Note If you are installing the Web Interface on WebSphere, an Application Security Warnings message appears, indicating a problem with the contents of the was.policy file. This is a policy file created by WebSphere if you select **Enforce Java 2 Security** under **Security**>**Global Security**. Ensure that you edit the was.policy in accordance with the WebSphere Java 2 Security policy, otherwise, the Web Interface may not function properly. This policy file is located in WEBSPHERE_HOME/AppServer/installedApps/*node-name*/*war-file-name*.ear/META-INF.

The Web Interface requires a servlet engine to work on UNIX platforms. The Apache Web server requires an additional servlet engine to support the Web Interface such as Tomcat (note that Tomcat can be used as a standalone Web server or as a servlet engine).

To install the Web Interface on Red Hat (Enterprise or Fedora), ensure that the sharutils package is also installed. This is required for the uudecode utility.

To install the Web Interface on Tomcat

1. Copy the WebInterface.sh.gz file from the Components CD-ROM Web Interface directory to a temporary location.
2. In a UNIX shell, navigate to the directory where the installation file was downloaded. Unzip the file by typing **gunzip WebInterface.sh.gz**.
3. Run the installer by typing **sh WebInterface.sh**.
4. Press **Enter** to read the license agreement.
5. Press **Q** to exit the license agreement.
6. Type **Yes** to accept the license agreement.

7. Select a site type from the list provided.

8. Specify if you want to use local configuration (for example, WebInterface.conf) or centralized configuration (the Configuration Service).

   If you select local file, select the type of applications to make available to users from the list provided and enter the name of the server containing application information. The XML Service must be installed and running on this server. Select an XML Service protocol from the list provided. Specify the port on which the XML Service is listening.

   If you select Configuration Service, enter the server (name or IP address) on which the Configuration Service is running. Enter the XML port number for the Configuration Service.

9. If you are creating a Conferencing Manager Guest Attendee site, enter the External Conference Server location and the port number. Specify if the server is secured with SSL by selecting Yes or No.

   If you are creating an Access Platform or Conferencing Manager Guest Attendee site, the installer offers to copy the client files from the CD-ROM to the .war file.

10. Enter the path and name of the .war file to create.

11. A summary is displayed. Select Yes if the information displayed is correct.

    The .war file is created and the clients are copied from the CD-ROM, if required.

12. Follow the instructions on-screen to complete the installation of the .war file.

Configuring the Security Policy on Sun Java System Application Servers

Before you can create Access Platform sites configured to allow account self service or Conferencing Manager Guest Attendee sites on a Sun Java System Application Server, you must manually configure the server’s security policy.

To configure the security policy on Sun Java System Application Servers

1. Deploy the site’s WAR file on the server.

2. Stop the server.

3. Edit the server.policy file under the deployed domain config directory. For example, if Sun Java System Application Server is installed under *SunJavaApplicationServer root*/AppServer and the site is deployed in

domain1, the file resides in *SunJavaApplicationServer root*/AppServer/domains/domain1/config.

4. Add the following configuration before any generic grant blocks:

   grant codeBase "file:${com.sun.aas.instanceRoot}/applications/j2ee-modules/*WARFileName*/-" {

   permission java.lang.RuntimePermission "getClassLoader";

   permission java.lang.RuntimePermission "createClassLoader";

   permission java.util.PropertyPermission "java.protocol.handler.pkgs", "read, write";

   };

   WARFileName is the first part of the filename of your site's WAR file. For example, CMGuest.

5. Edit the launcher.xml file located in *SunJavaApplicationServer root/* ApplicationServer/lib to add javax.wsdl to the list of values for the sysproperty key="com.sun.enterprise.overrideablejavaxpackages" element.

6. Start the server.

Installation Using the Command Line

You can perform unattended installations and site management through command line scripts.

For more information about how to use the command line with the Web Interface, refer to the Knowledge Center at http://support.citrix.com/.

Using Language Packs

Language packs contain all information required to localize your sites into a specific language (German, English, Spanish, French, and Japanese), including:

- Resource files for sites
- Online help
- Any localized icons and images

After installation, language packs can be added into the Common Files directory on Windows by copying the tree or unpacking the .zip file in that location. To customize a language for a specific site, you can copy the language pack into the site's location and modify it. The site will then use the modified language pack and other sites will continue to use the default.

On UNIX, extra language packs can be installed by moving them into the appropriate directory within the site, and by extracting them if they are supplied in formats such as .zip.

The English language pack is used as the fallback language and must always be present on your server.

Note Language packs for versions 4.2 and earlier of the Web Interface cannot be used with version 4.5 of the Web Interface.

Removing Language Packs

Some clients, such as Windows CE devices, are not capable of displaying specific languages (for example, Japanese). In this case, the language selection drop-down list in the user interface displays block characters for unavailable languages.

To avoid this, you can remove a language for all sites or certain sites.

For ASPX sites, remove *lang-code*.lang (for example, ja.lang) from the common files. This is typically located in C:\Program Files\Citrix\Web Interface\4.5\languages. This removes the language from all sites on the server. If you want to enable this language for a particular site, move the .lang file to the languages folder for that site.

For JSP sites, after creating a WAR file, open the WAR file with an appropriate tool, remove the .lang file, and package it again. This removes the language from sites deployed from that WAR file.

Deploying Languages to Users

When users log on, the language sent by the browser is detected. The screen is displayed in this language or in the site’s default language if the user’s language is not detected or recognized. Users can select a language from those available (if more than one language pack was installed); the **Login** screen reloads itself in the language selected. If the site is set to kiosk mode, the user’s browser language is detected with each new session. If users do not normally view the **Login** screen (for example, during silent authentication), they can select a language from the **Presentation Preferences** screen.

Ensure that users are provided with the correct version of the Citrix Presentation Server Client for their chosen language. When the user launches an application using an embedded client, the Web Interface performs one of the following steps:

- Launches with the user’s preferred language (if available on the client).
- Launches with the site’s default language (if available on the client).
- Displays an error to the user stating that no clients were available on the server. This message is also displayed for Web clients.

Upgrading an Existing Installation

You can upgrade from version 3.0 or later of the Web Interface to the most recent version by installing the Web Interface from either the CD-ROM or Web download files.

You cannot downgrade from Citrix Web Interface 4.5 to a previous version of the Web Interface.

What to Do Next

After you install the Web Interface, you need to make the Web Interface available to your users. To do this, you create and configure sites using the Access Management Console or edit the WebInterface.conf configuration file directly.

Additionally, you may need to configure the Web Interface depending upon other components in your installation, or you may want to customize or extend the Web Interface’s capabilities.

- For information about how to configure the Web Interface for Access Gateway or Secure Gateway using the Access Management Console, see “Configuring Secure Gateway Support” on page 154.
- For information about how to configure the Web Interface using the console or WebInterface.conf file, see “Configuring Sites Using the Console” on page 43 or “Configuring Sites Using the Configuration File” on page 137.
- For information about configuring the Web Interface to use ADFS, see “Configuring ADFS Support for the Web Interface” on page 157.
- For information about security considerations, see “Configuring Web Interface Security” on page 121.
- To extend and customize Web Interface functionality, see the *Customizing the Web Interface* guide.

Troubleshooting the Web Interface Installation

This section explains how to use the **Repair** option on Windows platforms to troubleshoot Web Interface installation, and what to do if the **Repair** option is unavailable or does not fix the problem. It also contains information about disabling error messages.

Using the Repair Option

If you experience problems with the Web Interface installation, try using the **Repair** option to fix the problem. The **Repair** option reinstalls common files; it does not repair or replace existing sites.

To run the Repair option from the .exe file

1. Double-click the WebInterface.exe file.
2. Select **Repair** and click **Next**.
3. Follow the instructions on-screen.

Note If the **Repair** option does not fix the problem, or this option is unavailable (for example, on UNIX platforms), try uninstalling and then reinstalling the Web Interface. For information, see "Uninstalling the Web Interface" on page 39. You must recreate all your sites after reinstalling the Web Interface.

Disabling Error Messages

On Windows platforms, you can disable the error messages provided with the Web Interface and display your own customized error messages. To do this, edit the web.config file located in the site's root directory. Change the following line:

```
<customErrors mode="On" defaultRedirect="html/serverError.html" />
```

to:

```
<customErrors mode="Off" defaultRedirect="html/serverError.html" />
```

Uninstalling the Web Interface

When you uninstall the Web Interface, all Web Interface files are removed, including the Clients directory. Therefore, if you want to keep any Web Interface files, copy these to another location before you uninstall the Web Interface.

Under some circumstances, the Web Interface uninstaller may fail. Possible causes are:

- Insufficient registry access for the uninstaller
- IIS was removed from the system after the Web Interface was installed

Uninstalling the Web Interface on Windows Platforms

To uninstall the Web Interface on Windows Platforms

1. Use the **Add/Remove Programs** option available from **Start** > **Settings** > **Control Panel**.
2. Follow the instructions on-screen.

Uninstalling the Web Interface on UNIX Platforms

To uninstall the Web Interface on Tomcat

1. Navigate to the directory to which you originally copied the WAR file.
2. Stop your Web server.
3. Enter **rm *WAR file name***.
4. You may also need to delete the directories in which the WAR file is expanded. Normally, this is the same directory as the WAR file with the same name. For example, the contents of Citrix.war is expanded into a directory called Citrix.

Files that Remain after Uninstalling

When you uninstall the Web Interface, some files remain on the server. For more details about which files remain, see the *Citrix Presentation Server Readme*.

Getting Started with the Web Interface

Overview

This chapter explains how to configure and customize the Web Interface using the Access Management Console and the Web Interface configuration file. Topics include:

- Deciding Which Configuration Method to Use
- Deciding Where to Store Your Site’s Configuration
- Configuring Sites Using the Console
- Configuring and Running Discovery
- Upgrading Existing Sites
- Creating Sites
- Specifying Initial Configuration Settings for a Site
- Using Site Tasks
- Making the Web Interface Available to Users

Deciding Which Configuration Method to Use

You can configure and customize the Web Interface using either the Access Management Console or the configuration files.

The Access Management Console

The Access Management Console allows you to perform day-to-day administration tasks quickly and easily. For example, you can use the console to specify the settings that users can select and to configure user authentication to the Web Interface. Your configuration takes effect when you commit your changes using the console. You can use the Access Management Console to configure sites created on both Windows and UNIX platforms.

You can install the Access Management Console on computers running:

- Windows Server 2003 with Service Pack 1
- Windows Server 2003 R2
- Windows XP Professional with Service Pack 2
- Windows 2000 Professional with Service Pack 4

Note You must also ensure .NET Framework 2.0 is installed.

For information about how to configure the Web Interface using the console, see “Configuring Sites Using the Console” on page 43 and the Access Management Console online help.

Configuration Files

You can use the following configuration files:

- **The WebInterface.conf file**. The WebInterface.conf file allows you to change many Web Interface properties; it is available on both Windows and UNIX platforms. You can use this file to perform day-to-day administration tasks and customize many more settings. You edit the values in the WebInterface.conf file and save the updated file to apply the changes.

  Note On UNIX platforms you may need to stop and restart the server running the Web Interface for changes to take effect.

For information about configuring the Web Interface using the WebInterface.conf file, see “Configuring Sites Using the Configuration File” on page 137.

- **The Program Neighborhood Agent configuration file**. You can configure the Program Neighborhood Agent using the config.xml file located on the server running the Web Interface.

Deciding Where to Store Your Site’s Configuration

The Web Interface provides support for storing the site configuration in two locations:

- **Local file(s)**. If you are using local file(s), site configuration is stored in a file on the server running the Web Interface. If you are using the Access Management Console for site management you must install the console on the server running the Web Interface.

  Throughout this guide, we refer to sites storing their configuration data in local file(s) as locally configured sites.

  Note On UNIX platforms you manage locally configured sites by editing the WebInterface.conf file.

- **Server(s) running the Configuration Service.** The Configuration Service provides a mechanism for retrieving and persisting site configuration data. If you are using the Configuration Service, site configuration is stored in a centralized location on any server in a farm running Presentation Server. Using centralized configuration enables you to configure a site from any server within a farm running the Access Management Console. It also enables you to group sites together and configure them as a single entity.

  Throughout this document, we refer to sites using this configuration location as sites using centralized configuration.

Configuring Sites Using the Console

The Access Management Console allows you to create and configure Access Platform, Program Neighborhood Agent Services, and Conferencing Manager Guest Attendee sites. The console allows you to manipulate many of the settings quickly and easily.

When using the console, some Web Interface settings may be disabled if their value is not relevant to the current configuration and the corresponding WebInterface.conf settings are reset to their default values. Citrix recommends creating regular backups of the WebInterface.conf and config.xml files for your sites.

Getting Help

You can display online help for the Web Interface by pressing **F1** or by right-clicking any node in the context tree and selecting **Help**.

Getting Started with the Access Management Console

Run the console from **All Programs > Citrix > Management Consoles> Access Management Console**.

For more information about the Access Management Console, see the *Citrix Presentation Server Administrator’s Guide*.

Configuring and Running Discovery

To administer the Web Interface using the Access Management Console, you must run the discovery task in the console. Running *discovery* establishes connections to your server farms.The first time you open the console, you are automatically prompted to start the discovery process: you are guided through selecting the components you want, configuring the discovery process, and finding the items to manage.

Using the **Configure and run discovery** wizard, you can do the following:

- Specify in which component products you want discovery to search for new items
- Indicate whether or not to retrieve centralized configuration for sites installed on your computer
- Edit details of servers running the Configuration Service
- Specify details of farms running Presentation Server

Subsequently, you run the discovery process only if you want to discover a new component product or if items were added to or removed from your deployment.

To configure and run discovery

1. On the **Start** menu, click **All Programs > Citrix > Management Consoles> Access Management Console**.
2. On the **Configure and run discovery** page, click **Yes**. If this page is not displayed automatically, click the **Configure and run discovery** task.
3. Click **Next**.
4. On the **Configuration Servers** page, choose one of the following:
   - If you want to create sites whose configuration is stored in local files or if the servers running the Configuration Service are behind a firewall, click **Do not contact any configuration servers**.

     Note Only local site tasks will be available.

   - If you want to create sites whose configuration is stored in a centralized location on servers running the Configuration Service, click **Contact the following configuration servers**, and then click **Add** to enter the name of a server.
5. Click **Next**.
6. Click **Finish**.

After running discovery to connect to a server farm, you can use the Access Management Console to create sites.

Note You can create sites using only the instance of the Access Management Console installed on the server running the Web Interface.

When discovery is complete, existing sites are displayed under the Web Interface in the console tree and you are ready to create new sites and administer existing sites.

Upgrading Existing Sites

If you are upgrading your installation from a previous version, the Web Interface now provides support for upgrading existing sites, as follows:

- **Locally configured sites**. During installation the Web Interface installer automatically upgrades all locally configured sites to the latest version. After you run discovery, these sites are available immediately.
- **Centrally configured sites**. Upgrading centrally configured sites is a two step process:
  - During installation the Web Interface installer upgrades the files for each centrally configured site
  - After running discovery, you upgrade the configuration information for centrally configured sites using the **Upgrade configuration** task in the console

Important Centrally configured sites are inoperative until you complete the upgrade using the **Upgrade configuration** task because configuration information for those sites is not available when requested by the Web Interface.

Upgrading Centrally Configured Sites

During installation, the Web Interface replaces the files of existing centrally configured sites with the most up to date versions and contacts the central configuration server to re-register each site at the latest version. At the end of the installation process the configuration service contains two versions of centrally configured sites; an existing version 4.x site with a valid configuration and a new version 4.5 site that does not have any configuration.

To complete the upgrade of centrally configured sites, run the **Upgrade configuration** task. You can upgrade all sites, groups of sites, or individual sites.

To upgrade all centrally configured sites

1. In the left pane of the console, select **Web Interface**.
2. Click the **Upgrade configuration** task.
3. Select the sites or groups of sites you want to upgrade and then click **Upgrade**.
4. Click **Yes** to confirm you want to upgrade the selected sites or groups.

To upgrade individual sites or groups of sites

1. In the left pane of the console, select the site or group.
2. Click the **Upgrade configuration** task.
3. Click **Upgrade**.
4. Click **Yes** to confirm you want to upgrade the selected sites or groups.

Upgrading Groups of Sites

For sites grouped in the Access Management Console, a single configuration is stored with the configuration service and applied to all sites within the group. You can only upgrade a group's configuration after files for all sites are upgraded by the Web Interface installer. Sites in a group may exist on different servers and after installation you may find either of the following occurs:

- All sites in a group have their files upgraded
- Some sites in a group have their files upgraded

All sites in a group have their files upgraded

If files for all sites in a group are upgraded during installation, you can upgrade the group's configuration after running discovery. An Upgraded site/group alert appears in the console and the **Upgrade configuration** task is available for the group node.

Some sites in a group have their files upgraded

If files for some sites in a group are upgraded during installation, a Misconfigured site/group alert appears in the console. Sites whose files are upgraded are inoperative until you complete the upgrade, because configuration information is not available when requested by the Web Interface. Sites whose files are not upgraded during installation work normally. You can complete the upgrade process in the following ways:

- By running the Web Interface installer and upgrading files for the remaining sites
- By removing sites that have not had their files upgraded from the group

Deleting Misconfigured Sites

If more than two registered versions exist for a centrally configured site a Misconfigured site/group alert appears in the console. Run the **Clean up configuration** task to delete the site versions you do not want to keep. A site is classed as misconfigured if:

- It is registered at a higher version than that known to the Access Management Console.
- It is upgraded to one version and then upgraded again to a later version without completing the first upgrade by running the Access Management Console. This results in three versions of the site registered with the centralized configuration server.
- It is registered with multiple farms as a result of its configuration files being edited by hand.

To delete misconfigured sites

1. Click the **Clean up configuration** task.
2. Select **Misconfigured sites** from the **Display** list.
3. Select the site versions you want to delete and then click **Delete**.
4. Click **Yes** to confirm you want to delete the selected sites or groups.

Creating Sites

After running discovery you can create sites to provide users with access to published applications using a Web browser or Program Neighborhood Agent and to enable guest users to attend Conferencing Manager conferences.

Creating Sites on Windows Web Servers

Use the **Create site** task in the Access Management Console to create one of the following sites:

- Access Platform—For users accessing applications using the Web Interface.
- Program Neighborhood Agent Services—For users accessing applications using the Program Neighborhood Agent.
- Conferencing Manager Guest Attendee—For users logging on to Guest Attendee conferences.

You use this task to specify the IIS site, the URL to apply changes, the configuration source, and authentication settings for the site. You can update these options later using **Local site tasks**. You must be a local administrator on the system running the Access Management Console to create sites.

Note If sites use centralized configuration, you cannot specify configuration servers from multiple farms. Site configuration can be obtained only from servers in the same farm. Different sites can, however, use servers in different farms.

To create a site

1. Click **Web Interface** in the console tree.
2. Click the **Create site** task.
3. Select the type of site you want to create.
4. Follow the instructions on screen to create the site.
5. Click **Finish**.

Creating Sites on UNIX Web Servers

On UNIX, a pre-install script is run before creating each site. This script creates a customized WAR file for the site, which is then installed (usually by placing the WAR file in the correct location for the servlet engine). This script requires uudecode and Java.

Sites are modified by editing the contents of the unpacked WAR file, and can be removed by deleting the WAR file.

Specifying the Configuration Source for a Site

You can store site configuration in local files or in a centralized configuration location on a server running the configuration service. Typically this is also the server running the XML Service.

You can edit a site to change its configuration source. If you change to local configuration, the existing configuration is obtained from the centralized configuration location and populates the new local file accordingly.

For more information about specifying site configuration sources in the Access Management Console, see “Using Local Site Tasks” on page 57.

You can also import existing configuration files to use with a selected site and export configuration files for use with other sites.

For more information, see “Importing and Exporting Configuration Files” on page 50.

On UNIX, the pre-install script cannot create sites using local configuration files based on existing site configurations.

On Windows, if centralized configuration is selected when installing a site, the site is automatically registered with the configuration service after installation. On UNIX, the site is registered on first page load after it is deployed into a servlet engine.

Importing and Exporting Configuration Files

You can import existing configuration files to use with a selected site and export configuration files for use with other sites. To do this, use the **Import configuration** and **Export configuration** tasks.

Specifying Authentication Settings

When creating an Access Platform site you can specify whether users access that site using built-in authentication or Advanced Access Control, or ADFS. Selecting ADFS enables the resource partner of an ADFS deployment to use Presentation Server. This enables administrators to provide users with access to published applications on the resource partner.

If you are planning on creating ADFS integrated sites, you must be aware of the following:

- ADFS support is not available on UNIX platforms
- ADFS integrated sites support authentication using ADFS only. Other methods of authentication are not supported.
- After an ADFS integrated site is created, you cannot configure that site to use built-in authentication or Advanced Access Control instead of ADFS.

For more information, see “Configuring ADFS Support for the Web Interface” on page 157.

Specifying Initial Configuration Settings for a Site

After creating a site you can specify initial configuration settings by selecting the **Configure this site now** check box on the final page of the **Create site** wizard. Use this wizard to configure communication with one or more server farms, specify the types of applications available to users, and configure how users access a site. If you are creating a Conferencing Manager Guest Attendee site, use this task to specify the External Conference Service URL.

Note You can also run the **Specify Initial Configuration** task from the console at any time for centrally configured sites.

For more information about configuring communication with server farms, see Chapter 4, “Managing Servers and Farms.”

Specifying the Types of Application Available to Users

The Web Interface provides users with access to applications and content through a standard Web browser or through the Program Neighborhood Agent. Integration with the Citrix application streaming feature allows users to stream applications to their desktops and launch them locally. You can grant users access to applications, as follows:

- **remote**—users access published applications installed on a remote server.
- **streaming**—users stream applications to their desktops and launch them locally.
- **dual mode streaming**—users stream applications to their desktop and launch them locally, otherwise virtualize them from Presentation Server. If streamed applications are not available, remote versions are launched.

You can update these settings at any time using the **Manage application types** task.

Configuring How Users Access a Site

Users can gain access to an Access Platform site directly, using the Web Interface URL, or using Advanced Access Control.

Accessing a Site Directly

If users access a site directly, you can enable Published Application URL support. This allows users to create persistent links to published applications accessed using the Web Interface. These links can be added to the user's Favorites list or desktop. You enable Published Application URL support by selecting the **Allow users to launch applications using browser bookmarks** check box.

Accessing a Site with Advanced Access Control

Using Advanced Access Control as your access method controls user access to resources through the use of access control policies and filters. This permits the use of endpoint analysis as a condition for application access, along with other factors.

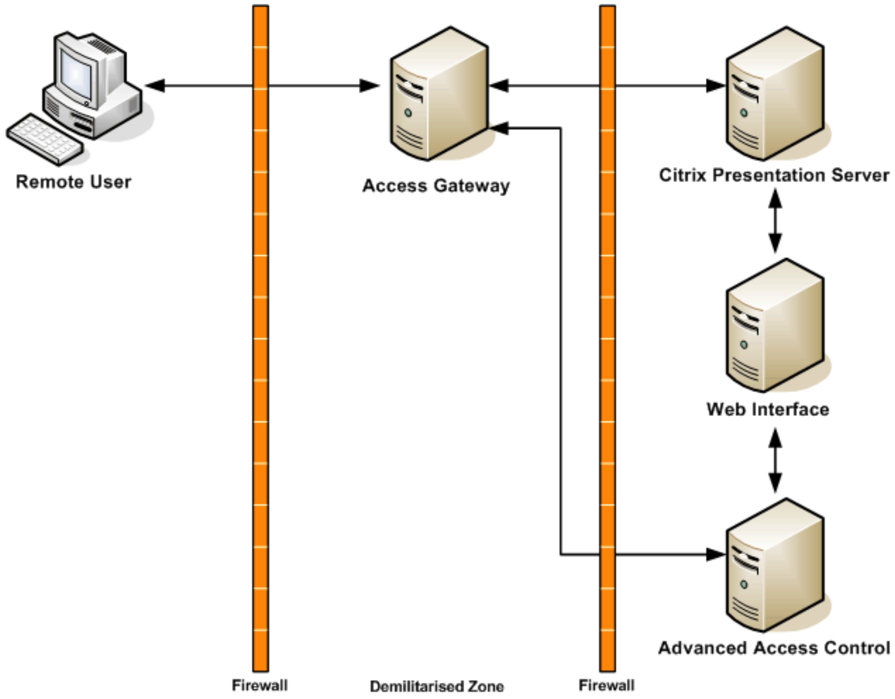
By default, pass-through authentication is enabled for users accessing the Web Interface using Advanced Access Control. Users log on using Advanced Access Control and do not have to reauthenicate to the Web Interface to access their applications. To increase security, you can disable pass-through authentication by selecting the **Prompt user for password before displaying the application list** check box.

You can update these settings at any time using the **Manage access method** task.

Note Support for Advanced Access Control is not available on UNIX platforms.

Recommended Deployment for Advanced Access Control

The recommended deployment for using Advanced Access Control with the Web Interface is illustrated below.



This diagram shows the recommended deployment for using Advanced Access Control with the Web Interface.

In this deployment Presentation Server, the Web Interface, and Advanced Access Control are all installed on servers within the internal network. Access Gateway is installed in the DMZ. When you install Advanced Access Control, an instance of the Logon Agent is also installed. The Logon Agent provides the user interface for logging on to a server in your server farm.

When a user logs on, they are authenticated by the Access Gateway and directed to their resources subject to the access policies configured in Advanced Access Control.

Making Resources Available to Users

With Advanced Access Control, users log on to a logon point to gain access to their resources. You make resources available to users by configuring a logon point to provide access to an Access Platform site.

Advanced Access Control provides several methods for integrating Access Platform sites created with the Web Interface including:

- Access Platform site embedded within the default navigation page. When the navigation page is selected as the default home page, an Access Platform site is displayed alongside file shares, access centers, and Web applications.

  Note This option is available only if you are running Citrix Access Gateway 4.2 with Advanced Access Control.

- Access Platform site configured as the default home page for a logon point. Once logged on, users are presented with the Access Platform site.

  Note This option is available only if you are running Access Gateway Enterprise 4.0 with the Access Gateway Enterprise hotfix AAC400W001 applied or Citrix Access Gateway 4.2 with Advanced Access Control.

To integrate an Access Platform site

Complete the following steps in Advanced Access Control.

1. Configure Presentation Server to communicate with Advanced Access Control.
2. Create a Web resource for the Access Platform site with the following settings:
   - Select **Citrix Web Interface 4.2 or later** as the application type
   - Select the **Publish for users in their list of resources** check box
3. Specify the appropriate policy settings for the Web resource referencing the Access Platform site.
4. Provide access to the Access Platform site in one of the following ways:
   - **Display the Access Platform site as the default home page.** Configure a logon point to display the application with the highest display priority as the home page. Then, configure the Access Platform site as the application with the highest priority.
   - **Embed an Access Platform site within the navigation page.** Configure a logon point to display the navigation page as the home

page. The Access Platform site is embedded as a frame within the navigation page.

Note Because the navigation page provided by Advanced Access Control can display only one Access Platform site (Web resources configured with the Web Interface 4.2 or later application type), you should configure no more than one Web resource of this type.

For more information about completing these steps, see the *Citrix Access Gateway Advanced Edition Administrator's Guide.*

Complete the following steps for the Web Interface.

1. Select **Using the Advanced Access Control** when specifying an access method for the site.
2. Enter the URL of the Advanced Access Control authentication service in the **Authentication service URL:** box.

In both Web Interface and Advanced Access Control, ensure the Workspace control, Client for Java fallback, and session time-out settings are configured properly.

Coordinating Web Interface and Advanced Access Control Settings

Certain Presentation Server settings are available for configuration within the Web Interface and Advanced Access Control. However, because an Access Platform site integrated with Advanced Access Control can be referenced by more than one logon point, it is possible for one logon point to embed an Access Platform site within its default navigation page while another logon point displays the site as its default home page. This can cause conflicts with certain published application settings. To ensure your settings work as intended, follow the instructions below.

- **Workspace control**. Disable all Advanced Access Control Workspace control settings for all logon points that have an Access Platform site as their home page. This ensures that the settings configured within the Web Interface are used. All other logon points can have Workspace control configured as desired.
- **Client for Java Fallback**. Ensure that logon points using the default navigation page as their home page have the same Client for Java fallback settings as the Access Platform site.
- **Session time-out**. Ensure all logon points use the same settings as the Access Platform site.

Using Site Tasks

To configure sites, select the site under the Web Interface node in the Access Management Console and use the tasks in the task pane. Alternatively, you can right-click a site name and select tasks from the **Context** menu.

Tasks that are available for each site type are displayed in the task pane. Tasks are either performed using wizards or by setting options in dialog boxes. To execute a task, either click a task name in the task pane or right-click the site you want to configure and select a task from the menu displayed.

Some tasks are available only for certain site types and configurations. This information is specified in the table below.

Task	Access Platform sites	Program Neighborhood Agent Services sites	Conferencing manager Guest Attendee sites	ADFS integrated sites	Sites running only streamed applications
Change display	◆	◆	◆	◆	◆
Change session options		◆			
Clean up configuration	◆	◆	◆	◆	◆
Configure authentication methods	◆	◆			◆
Control diagnostic logging	◆	◆	◆	◆	◆
Customize appearance for user	◆		◆	◆	◆
Edit client-side proxy	◆	◆	◆	◆	
Export configuration	◆	◆	◆	◆	◆
Export client configuration		◆			◆
Import configuration	◆	◆	◆	◆	◆
Local site tasks	◆	◆	◆	◆	◆
Manage access method	◆				◆
Manage application refresh		◆			◆

Task	Access Platform sites	Program Neighborhood Agent Services sites	Conferencing manager Guest Attendee sites	ADFS integrated sites	Sites running only streamed applications
Manage application shortcuts		◆			◆
Manage application types	◆	◆		◆	◆
Manage client deployment	◆		◆	◆	◆
Manage secure client access	◆			◆	
Manage server farms	◆	◆	◆	◆	◆
Manage server settings		◆			◆
Manage session preferences	◆		◆	◆	
Manage site grouping	◆	◆	◆	◆	◆
Manage workspace control	◆			◆	
Modify apply changes URL	◆	◆	◆	◆	◆
Upgrade configuration	◆	◆	◆	◆	◆

Using Local Site Tasks

Use **Local site tasks** to specify the configuration location for sites, how IIS hosts sites, and to repair or uninstall sites. These tasks are available only when the console is run on the server running the Web Interface. You can edit the information you entered when you created the site, and add servers for centralized configuration for the site.

Managing Configuration Sources

The **Manage configuration source** task allows you to specify whether or not the site uses local configuration (configuration for the site is held on the local computer) or centralized configuration (configuration for the site is held on a remote server running Presentation Server). The site's existing configuration is copied to the new configuration source.

If you are using a firewall between the server running the Web Interface and the server running Presentation Server, follow the procedure below to change the configuration source for a site from local configuration to centralized configuration.

To use centralized configuration for sites separated from Presentation Server by a firewall

1. Run the Access Management Console on the server running the Web Interface.
2. Use the **Export configuration** task and save the configuration to a file.
3. Use the **Manage configuration source** task to enable centralized configuration. Click **Yes** if a warning appears.
4. Run the Access Management Console on the server running Presentation Server and use the **Import configuration** task to import the saved configuration.

Repairing and Uninstalling Sites

You can use the **Repair site** and **Uninstall site** tasks to repair and remove sites. Uninstalling a site completely removes it from the system and you can no longer perform tasks on the site.

Important If custom scripts and images have been created for the site and you run the **Repair site** task, these customized files will be removed. Customized files are also removed when using the **Manage IIS Hosting task**. Citrix recommends that you back up any files you create before you use either of these tasks.

Grouping Sites

Use the **Manage site grouping** set of tasks to group sites so that they share the same configuration and can be used for load balancing across your network. Sites that use a centralized configuration source can be grouped together using this task.

To create a site group, use the **Create site group** task. Enter a name for the group and then select the sites you want to place in this group. Sites must use the same configuration source, technology (for example, Windows or UNIX), type (for example, Access Platform), and must be the same version to be included in a group.This task is not displayed for locally configured sites. Use the **Add sites to a group** task to add a site to existing group.

After a site is added to a group, you cannot perform local site tasks on that site and the site's configuration is removed. To use local site tasks, you must remove the site from the group using the **Remove sites from group** task; the group configuration is used for the site. Additionally, you can use the **Ungroup** task to remove all sites from the group.

Making the Web Interface Available to Users

When the Web Interface is installed and configured, inform your users of the URL for the **Login** page. If users want to bookmark this page in their browsers, Citrix recommends that the bookmark be set to http://*servername*/*site path* without specifying a particular page (such as login.aspx).

On UNIX Web servers, the site path (the portion of the URL after the host name and port number) is determined by the servlet engine. When installing the WAR file within the servlet engine, you can modify this path. The default is usually /*WAR file name*, where the file name is WARFileName.war. For WebLogic, a separate XML file must be created to modify this path. Example XML files with usage notes are generated with the WAR file, and are typically located in the directory from which you run the UNIX pre-install script.

Making the Login Page the Default on IIS

You can set the Web Interface **Login** page to be the default for users of the Web server, so that the URL is http://*servername*/. To do this, enable the **Set as the default page for the IIS site** option in the **Create site** task.

What to Do Next

- For more information about deploying Citrix Presentation Server clients to Web Interface users, see "Managing Client Deployment" on page 93.
- For information about security considerations, see "Configuring Web Interface Security" on page 121.

Managing Servers and Farms

Overview

This chapter describes how to configure the Web Interface to communicate with your server farms. It also describes how to configure and manage server settings and enable load balancing between sites. Topics include:

- Managing Server Farms
- Managing Server Settings

Managing Server Farms

Using the **Manage server farms** task, you can configure the Web Interface to communicate with one or more farms. Users must have an account that can authenticate to each farm specified in this task. On Windows, if the farms are on different domains, a two-way trust must be enabled between these domains. If a farm is on UNIX, each user must have a user name and password that matches the Windows farm. If the user name and password cannot be authenticated to all of the farms specified, users are presented with an invalid credentials error.

Multiple server farm functionality is transparent to users because they are not informed that their application set is an aggregation from multiple server farms. Applications from multiple server farms are displayed in the same way as a single farm; folders are displayed first, followed by application icons. Consequently, applications with the same name from multiple server farms appear in an arbitrary position in the user’s application set. Citrix recommends that you ensure application names are unique across the server farms, such as by publishing applications in folders with different names.

Note The Web Interface acquires application data from all server farms before displaying applications; each server farm is contacted in the order that it appears in the configurations. As a result, a server farm that is slow to respond impacts overall responsiveness when obtaining application sets.

Password Change Considerations

If there are differences among your server farms, there are additional issues that may prevent users from changing their passwords. For example:

- The domain policy may prevent users from changing passwords
- When Presentation Server for UNIX and Presentation Server for Windows are aggregated by a single site, only the Windows password can be changed

Citrix recommends that you disable user password changing in these situations.

You should also ensure, when aggregating multiple farms, that the first farm listed in the configuration is running MetaFrame XP, Service Pack 2 or later.

If necessary, it is possible to enable password changing in a mixed server farm deployment. The Web Interface contacts server farms in the order in which they are defined until a server farm reports that the password is successfully changed, at which point the process stops. This allows you to specify the server farm to which the change password request will be issued. However, use suitable password replication mechanisms between server farms to ensure that user passwords remain consistent. If the password change request fails, the next server farm in sequence is issued the change password request.

Configuring Server Settings

Server settings are configured for each server farm. To view and configure server farm settings, select the **Manage server farms** task. Using this task, you can create and edit server farm names and specify the order in which servers running the Citrix XML Service are used for load balancing. You can also configure individual farm settings such as XML and SSL server ports, transport types, and enable ticketing.

To add server farms

1. Click the **Manage server farms** task.
2. Click **Add**.
3. In the **Servers** area, click **Add** to create a server name.
4. If you specify more than one server name, highlight a name in the list and click **Move Up** or **Move Down** to place these in the appropriate failover order. To change a server name, click **Edit**. To remove a server name, highlight the name in the list and click **Remove**.
5. Enter a name for the server farm in the **Farm name** box.
6. Click **OK** to finish adding the farm.

Configuring Fault Tolerance

The Web Interface provides fault tolerance among servers running the Citrix XML Service. If an error occurs while communicating with a server, the failed server is bypassed for a specified time but communication continues with the remaining servers in the **Servers** list.

By default, a failed server is bypassed for one hour.

To configure fault tolerance

1. Click the **Manage server farms** task.
2. Click **Add** if you are adding a farm or **Edit** to configure an existing farm.
3. In the **Servers** list, place the servers in order of priority. Highlight a name in the list and click **Move Up** or **Move Down** to place these in the appropriate order.
4. Change the length of time a failed server is bypassed for in the **Bypass any failed server for** box.

Note If a server running the Citrix XML Service fails, the Web Interface does not attempt to communicate with the failed server until the time specified in the **Bypass any failed server for** box elapses. If all servers in the list fail to respond, the Web Interface retries the servers every 10 seconds.

Enabling Load Balancing between Servers

You can enable load balancing among servers running the Citrix XML Service. Enabling load balancing allows you to evenly distribute connections among these servers so that no one server becomes overloaded. By default, load balancing is enabled.

If an error occurs while communicating with a server, all further communication is load balanced among the remaining servers in the list. The failed server is bypassed for a specific time period (by default, one hour) but you can change this using the **Bypass any failed server for** box.

To enable load balancing

1. Click the **Manage server farms** task.
2. Click **Add** if you are adding a farm or **Edit** to configure an existing farm.
3. In the **Servers** list, add the servers that will be used for load balancing. For information about how to add servers, see “Configuring Server Settings” on page 62.

4. Select the **Use the server list for load balancing** option.
5. Change the length of time a failed server is bypassed for in the **Bypass any failed server for** box.

Configuring Settings for All Servers

You can use the **Manage server farms** task to specify the TCP/IP port used by the Citrix XML Service and the protocol used to transport Web Interface data between the Web server and the server running Presentation Server for those specified in the **Servers** list. The Citrix XML Service is a Presentation Server component that acts as the contact point between the server farm and the server running the Web Interface. By default, the port number is the value entered during site creation. This port number must match the port number used by the Citrix XML Service.

Additionally, you can specify an expiration time for the ticket generated by the server. Ticketing provides enhanced authentication security for explicit logons by eliminating user credentials from the ICA files sent from the Web server to the client devices.

Each Web Interface ticket has an expiration time of 200 seconds by default. If, for example, you want to adjust the time to your network's performance because expired tickets cannot successfully authenticate a user to the server farm, you can change the ticket time to live. If you change the IP address or addresses of a server running the Citrix XML Service, ticketing will not function until you restart the server. After changing a server's IP address or addresses, make sure you restart the machine.

To specify settings for all servers

1. Click the **Manage server farms** task.
2. Click **Add** if you are adding a farm or **Edit** to configure an existing farm.
3. In the **Communications settings** area, enter the port number in the **XML service port** box.
4. In the **Transport type** list, select one of the following options:
   - **HTTP**. Sends data over a standard HTTP connection. Use this option if you made other provisions for the security of this link.
   - **HTTPS**. Sends data over a secure HTTP connection using SSL (Secure Sockets Layer) or TLS (Transport Layer Security). You must

ensure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

- **SSL Relay**. Sends data over a secure connection that uses the Citrix SSL Relay running on a server running Presentation Server to perform host authentication and data encryption.

5. If you are using **SSL Relay**, specify the TCP port of the Citrix SSL Relay in the **SSL relay port** box (the default port is 443). The Web Interface uses root certificates when authenticating a Citrix SSL Relay server. Ensure all the servers running Citrix SSL Relay are configured to listen on the same port number.

Note If you are using **SSL Relay** or **HTTPS**, ensure the server names you specify match the names on the certificate for the computer running Presentation Server.

6. To configure ticketing, click **Ticketing Settings**.
7. Enter the lifetime of tickets for remote clients in the **ICA ticket lifetime** fields.
8. Enter the lifetime of tickets for the streaming client in the **Streaming ticket lifetime** fields.
9. Click **OK** to save your settings.

Specifying Advanced Server Settings

Using the **Advanced settings** in the **Manage Server Farms** dialog box, you can enable socket pooling and content redirection, specify the Citrix XML Service time-out duration, and specify the number of attempts made to contact the XML Service before it is considered failed.

Enabling Socket Pooling

When socket pooling is enabled, the Web Interface maintains a pool of sockets, rather than creating a socket each time one is needed and returning it to the operating system when the connection is closed. Enabling socket pooling enhances performance, particularly for SSL connections.

Socket pooling should not be used when the Web Interface is configured to use one or more Presentation Server for UNIX servers.

Note Socket pooling is not available for sites configured to use ADFS for authentication.

To enable socket pooling

1. In the **Manage Server Farms** dialog box, click **Advanced**.
2. In the **Socket Pooling** area, select the **Enable socket pooling** check box.

Enabling Content Redirection

You can use the **Enable content redirection** setting to enable and disable content redirection from client to server for individual Program Neighborhood Agent Services sites. This setting overrides any content redirection settings configured for Presentation Server.

When you enable content redirection from client to server, users running the Program Neighborhood Agent open published content and local files with applications published on servers. For example, a Program Neighborhood Agent user who receives an email attachment in a locally running email program opens the attachment in a published application. When you disable content redirection, users open published content and local files with locally installed applications.

By default, content redirection is enabled from client to server for Program Neighborhood Agent Services sites.

You configure content redirection from client to server by associating published applications with file types. For more information about file type association, see the *Citrix Presentation Server Administrator's Guide*.

To enable or disable content redirection

1. In the **Manage server farms** dialog box, click **Advanced**.
2. In the **Content redirection** area, do one of the following:
   - To enable content redirection, select the **Enable content redirection** check box.

   —Or—

   - To disable content redirection, clear the **Enable content redirection** check box.

Configuring XML Service Communication

By default contact with the Citrix XML Service times out after one minute and is considered failed after five attempts are made to communicate with it. You can change these settings by altering the default values.

To configure XML Service communication

1. In the **Manage server farms** dialog box, click **Advanced**.

2. To configure the Citrix XML Service time-out duration, enter appropriate values in the **Socket timeout** boxes.
3. To specify how many attempts are made to contact the Citrix XML Service before it is considered failed and will be bypassed, enter a value in the **Attempts made to contact the XML service:** box.

Managing Server Settings

Use the **Manage server settings** task to configure how the Program Neighborhood Agent communicates with a site and whether or not users are redirected to alternative sites in the event of failure.

Configuring Server Communication Settings

Use the server communication settings to:

- **Enable SSL/TLS for communication.** Smart card logon and SSL/TLS-secured communications between the client and the server running the Web Interface are not enabled by default. You can enable SSL/TLS communication from this dialog box, forcing URLs to apply the HTTPS protocol automatically. In addition, you must enable SSL on the server running Presentation Server.
- **Allow users to customize the server URL**. The server URL points the Program Neighborhood Agent to the correct configuration file. The default path is determined based on the server address entered by the user during installation. You can allow users to change the server URL, which enables the **Server URL** option on the **Server** tab of the **Program Neighborhood Agent Properties** dialog box.
- **Configure automatic refresh**. You can define how often the client should refresh its configuration settings.

To configure server communication settings

1. Click the **Manager server settings** task.
2. If you want to use secure communication between the Program Neighborhood Agent and a site, select **Use SSL/TLS for communications between clients and this site**.
3. If you want to allow users to customize the server URL that points the Program Neighborhood Agent to the correct configuration file to use, select **Allow users to customize server URL**.

4. If you want to configure how often the Program Neighborhood Agent refreshes its configuration settings select **Schedule an automatic refresh every:** and enter the refresh period in hours, days, weeks, or months.

Specifying Program Neighborhood Agent Backup URLs

You can specify backup servers for the Program Neighborhood Agent to contact if the primary Web Interface server is not available. Use the **Backup** settings available from the **Manage server settings** dialog box to specify URLs for backup servers. In the event of a server failure users are automatically connected to the backup server specified first in the Backup URL list. If this server fails, the Program Neighborhood Agent attempts to contact the next server in the list.

Important All Backup URLs must point to sites that are of the same type as the primary site specified. For example, if the primary site is an ASPX site any backup sites specified must also be ASPX sites.

To specify backup URLs

1. Click the **Manage server settings** task.
2. Click **Backup**.
3. Click **Add**.
4. Enter the URL for the site users are connected to in the **Backup URL** box.

   Note You can define a maximum of five backup URLs per site.

5. Click **OK**.
6. If you specify more than one backup server URL, highlight a URL in the list and click **Move Up** or **Move Down** to place these in the appropriate failover order.

Configuring Site Redirection

Use the **Redirection** settings to define when users are redirected to a different site. For example, you create a new site for your HR department and want to redirect all users from the old site to the new site without them having to enter the URL manually. You can specify details of the new site in the **Site Redirection** dialog box. Users are redirected to the new site immediately or the next time they launch the Program Neighborhood Agent.

To configure site redirection

1. Click the **Manage server settings** task.
2. Click **Redirection**.
3. Choose one of the following:
   - If you do not want to configure site redirection, select **Do not redirect**
   - If you want to redirect users to an alternative site immediately, select **Redirect immediately**
   - If you want to redirect users to an alternative site next time the client launches, select **Redirect the next time Program Neighborhood Agent starts**
4. Enter the URL of the alternative site in the **Redirect URL** box.
5. Click **OK**.

Configuring Authentication for the Web Interface

Overview

This chapter describes the authentication methods available to users of the Web Interface. It also explains how to configure authentication between the Web Interface, Presentation Server, and Program Neighborhood Agent.

Note This chapter is applicable to Access Platform and Program Neighborhood Agent Services sites only.

Topics in this chapter include:

- Authentication Methods
- Configuring Authentication
- Configuring Two-Factor Authentication

Authentication Methods

Authentication takes place when a user accesses applications. If authentication is successful, the user's application set is displayed. You can configure the following authentication methods for the Web Interface:

- **Explicit** (Access Platform sites) or **Prompt** (Program Neighborhood Agent Services sites). Users are required to log on by supplying a user name and password.User Principal Names (UPN), Microsoft domain-based authentication, and Novell Directory Service (NDS) are available. For

Access Platform sites, RSA SecurID, and SafeWord authentication are also available.

Note Novell authentication is not available on UNIX platforms.

- **Pass-through**. Users can authenticate using the credentials they provided when they logged on to their Windows desktop. Users do not need to reenter their credentials and their application set is displayed automatically. Additionally, you can use Kerberos authentication to connect to servers. If you specify the Kerberos authentication option and Kerberos fails, pass-through authentication also fails and users cannot log on. For more information about Kerberos, see the *Citrix Presentation Server Administrator’s Guide*.
- **Pass-through with smart card.** Users can authenticate by inserting a smart card into a smart card reader attached to the client device. The Program Neighborhood Agent prompts you for a smart card PIN when you log on. After logon, you can access your set of published applications and content without further logon prompts. Users connecting to Access Platform sites are not prompted for a PIN. If you are configuring a Program Neighborhood Agent Services site, you can use Kerberos authentication to connect to servers. If you specify the Kerberos authentication option and Kerberos fails, pass-through authentication also fails and users cannot log on. For more information about Kerberos, see the *Citrix Presentation Server Administrator’s Guide*.
- **Smart card**. Users can authenticate using a smart card. The user is prompted for a PIN.

Note Pass-through, pass-though with smart card, and smart card authentication methods are not available on UNIX platforms.

- **Anonymous**. Anonymous users can log on without supplying a user name and password, and launch applications published for anonymous users on the server.

Caution Web Interface anonymous users can obtain Secure Gateway tickets, despite not being authenticated by the Web Interface. Because the Secure Gateway relies on the Web Interface issuing tickets only to authenticated users, this compromises one of the security benefits of using the Secure Gateway in your installation.

Authentication Recommendations

Ensure users log on to their workstations and the Web Interface consistently, either explicitly (with a user name and password) or using smart cards, not a mixture of both methods. For example, if a user logs on to the Windows desktop using a smart card, and then logs on to the Web Interface explicitly, the credentials supplied by the client may be incorrect. In this case, the client may supply the PIN rather than the user name and password.

If you change the methods for authenticating to the Web Interface, error messages may be displayed to existing users. Users must close and restart any browsers used to access the Web Interface.

Configuring Authentication

Use the **Configure authentication methods** task to configure the ways in which users can authenticate to Presentation Server and the Program Neighborhood Agent.

Configuring Domain Restriction Settings

Use the **Domain Restriction** page to restrict access to sites to users from specific domains.

To configure domain restriction settings

1. Click the **Configure authentication methods** task.
2. Click **Properties**.
3. Select **Domain Restriction**.
4. Specify whether or not to restrict access to users in selected domains. Choose from the following:
   - If you do not want to restrict access based on domains, select **Allow any domains**
   - If you want to restrict access to users from selected domains, select **Restrict access to the following domains:**
5. Click **Add**.
6. Enter the name of the domain you want to add to the domain restriction list in the **Logon domain** box.
7. Click **OK**.

Configuring the Authentication Type

If you are using Explicit or Prompt authentication use the **Authentication Type** page to configure whether users authenticate using Windows or NDS.

To configure the authentication type

1. Click the **Configure authentication methods** task.
2. Click **Properties**.
3. Select **Authentication Type**.
4. Specify the type of authentication that explicit users must use:
   - If you want to use Microsoft domain-based authentication, select **Use Windows or NIS (UNIX) Authentication**. Go to step 5.
   - If you want to use Novell Directory Service (NDS) authentication, select **Use NDS authentication**. Go to step 9.
5. Specify the credential format for user logons. Choose one of the following:
   - To allow users to enter their logon details in either UPN or Domain username format, select **Domain user name and UPN**
   - To specify that users must enter their logon details in Domain username format only, select **Domain user name only**
   - To specify that users must enter their logon details in UPN format, select **UPN only**
6. Select **Settings**.
7. In the **Domain display** area, configure the following settings:
   - Specify whether or not to display the Domain box on the Login page.
   - Specify whether the Domain box is pre-populated with a list of domains for users to choose from or whether users must enter a value in the Domain box manually.

     Note If users receive a "Domain must be specified" error message during logon, this may be due to an empty domain box. To resolve this issue, select **Hide Domain field**. If your farm comprises only server running Presentation Server for UNIX, in the **Domain list** box select **Pre-populated** and add UNIX as the domain name.

   - Specify the domains you want to appear in the Domain box on the Login page.

8. In the **UPN restriction** area, configure the following settings:

   - Specify whether or not all User Principal Names (UPN) suffixes are accepted. By default, all UPN suffixes are permitted.

   - Specify the UPN suffixes you want to accept.

9. Enter a name in the **Default tree name** box.

10. Configure context restriction or contextless authentication.

    Note By default, eDirectory does not give anonymous connection access to the cn attribute, which is required for contextless logon. For information about how to reconfigure eDirectory, visit http://developer.novell.com/.

11. If you want the client to use the user's Windows NT credentials with pass-through authentication, select **Use Windows NT credentials to connect to the server farms**.

Enabling Explicit Authentication

If explicit authentication is enabled, users must have a user account and supply a user name, password, and a domain name to log on.

You can change the explicit authentication settings using the console. For example, you can configure whether or not users are allowed to change their logon passwords within a session.

Note Explicit authentication is available only for Access Platform sites.

To enable explicit authentication

1. Click the **Configure authentication methods** task.
2. Select the **Explicit** check box.
3. Click **Properties** to configure further settings for explicit authentication.

Configuring Password Settings

Use the **Password Settings** page to configure password change and password expiry reminder options for users.

To configure password settings

1. Select **Password Settings**.
2. If you want users to be able to change their logon password within a Web Interface session, select the **Allow user to change password** check box.
3. To specify when users can change their logon password choose one of the following options:
   - To enable users to change their logon password when it expires, select **Only when it expires**. When you enable this option, if a user fails to log on to the Web Interface due to an expired password, the user is redirected to the **Change password** dialog box. After changing their password, users are automatically logged on to the Web Interface using the new password.
   - To allow users to change their password as often as they want in the Web Interface, select **At any time**. When you enable this option, the change password icon appears on users' pages. When users click this icon, a dialog box appears where users can enter a new password.
4. To configure a reminder message for users to notify them before their password expires choose one of the following options:
   - If you do not want to notify users before their password expires, select **Do not remind**.
   - To use your current Windows policy reminder settings, select **Use reminder settings from Active Directory group policy**.
   - To remind users their password will expire in a set number of days, select **Use a customized reminder setting**. Specify the number of days in the **Remind user <n> days before expiry** box.

Enabling Two-Factor Authentication

Use the Two-Factor authentication page to enable two-factor authentication for users, if required.

To enable two- factor authentication

1. Select **Two-Factor Authentication**.
2. Select the type of two factor authentication you want to use from the **Two-Factor setting** list. For more information about configuring SafeWord authentication, see "Configuring Two-Factor Authentication" on page 85. For more information about configuring RSA SecurID authentication, see "Enabling RSA SecurID 6.0 Authentication on IIS" on page 86.

Configuring Account Self Service

Integration with the account self service feature available in Citrix Password Manager enables users to reset their network password and unlock their account by answering a series of simple security questions.

Important When setting up Password Manager, you specify which users are able to perform password resets and unlock their accounts. If you enable these features for the Web Interface, users may still be denied permission to perform these tasks based on the settings you configure for Password Manager.

Before configuring account self service for a site, you must ensure that:

- The site is configured to use explicit Windows-based authentication.
- The site is configured to allow users direct access. Account Self Service is not available for sites accessed using Advanced Access Control.
- The site is configured to use only one Password Manager Service. If the Web Interface is configured to use multiple farms within the same or trusted domains, Password Manager must be configured to accept credentials from all of those domains.
- The site is configured to allow users to change their password, if you want to enable password reset functionality.

To configure account self service

1. Select **Account Self Service**.
2. Specify whether or not you want users to be able to reset their logon password or unlock their account.
3. Enter the URL for Password Manager in the **Password Manager Service URL** box.

Enabling Prompt Authentication

If prompt authentication is enabled, users must have a user account and supply a user name, password, and a domain name to log on.

Note Prompt authentication is available only for Program Neighborhood Agent Services sites.

To enable prompt authentication

1. Click the **Configure authentication methods** task.
2. Select the **Prompt** check box.
3. Click **Properties** to configure further settings for Prompt authentication.

Configuring Password Settings

Use the **Password Settings** page to configure whether or not users can save their passwords.

To configure password settings

1. Select **Password Settings**.
2. To enable users to save their passwords, select the **Allow user to save password** option.

Enabling Pass-Through Authentication

Using the console, you can enable pass-through authentication for users logging on to their desktops with user name, password, and domain credentials. This feature allows users to authenticate using the credentials they provided when they logged on to their Windows desktop. Users do not need to reenter credentials and their application set is automatically displayed.

The following section provides information about pass-through authentication requirements and explains the steps you must perform to enable pass-through support.

Pass-Through Requirements

To use the pass-through authentication feature, your servers must be running MetaFrame Presentation Server with Feature Release 2 or later, the Web Interface must be running on IIS on Windows Server 2003, and users must be running Internet Explorer Version 5.5 or later.

Caution If the servers are running versions prior to MetaFrame Presentation Server with Feature Release 2, users may be able to view all applications when using pass-through.

If users are using clients earlier than Version 6.30 and ICA encryption (SecureICA) is enabled, pass-through will not work. To use pass-through with ICA encryption, you must have the latest clients and the server must be running MetaFrame Presentation Server with Feature Release 2 or later.

Caution When a user selects an application, a file is sent to the browser. The file can contain a setting that instructs the client to send the user's workstation credentials to the server. By default, the client does not honor this setting; however, there is a risk that if the pass-through feature is enabled on the Clients for Windows, an attacker could send the user a file that causes the user's credentials to be misrouted to an unauthorized or counterfeit server. Therefore, use pass-through authentication only in secure, trusted environments.

Step 1—Installing the Clients for Windows

You must install the Clients for Windows on your users' client devices, using an administrator account. Pass-through is available only in the Clients for Windows, available on the Components CD-ROM. For security reasons, the Web Client does not include this feature. This means that you cannot use Web-based client installation to deploy clients containing this feature to your users.

Step 2—Enabling Pass-Through on the Client

After installation, you must enable pass-through authentication on the client. You can:

- Configure Group Policy to enable pass-through for all clients.

  —Or—

- Edit the Appsrv.ini file. located in users' profiles, to enable pass-through for a single client. For example, if a user's profile is stored locally, this file is located in C:\Documents and Settings\user\Application Data\ICAClient.

  Note Application Data is a hidden folder.

To enable pass-through authentication for all clients

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the Group Policy Object you want to edit.
3. Right-click the **Administrative Templates** folder and choose **Add/ Remove Templates**.

4. Click **Add** and browse to the icaclient template on the Components CD.
5. Click **Open** to add the template and then click **Close** to return to the Group Policy Object Editor.

Note If you already added the icaclient template to the Group Policy Object Editor, you can omit Steps 3 to 5.

6. In the console tree expand the **Administrative Templates** folder.
7. Select **Citrix Components > Presentation Server > Client User Authentication**.
8. Select **Local user name and password**.
9. On the **Action** menu, click **Properties**.
10. Click the **Settings** tab.
11. In the **Local username and password** area, select **Enabled**.
12. Select the **Enable Pass-through authentication** check box and click **OK**.

To enable pass-through authentication for a single client

1. Open the Appsrv.ini file using a text editor such as Notepad.
2. In the [WFClient] section, add the following entries:

```
EnableSSOnThruICAFile=On
SSOnUserSetting=On
```

3. Save the updated file.

Caution If the servers are running versions prior to MetaFrame Presentation Server with Feature Release 2, users may be able to view all applications when using pass-through.

Step 3—Enabling Pass-Through Using the Console

Use the Access Management Console to enable pass-through authentication. When you enable this feature, users do not need to enter their credentials again and their application set is automatically displayed.

Additionally, you can enable Kerberos with pass-through authentication for Access Platform and Program Neighborhood Agent Services sites. For Program Neighborhood Agent Services sites you can also specify Kerberos for pass-through with smart card authentication.

To enable pass-through authentication

1. Click the **Configure authentication methods** task.
2. Select the **Passthrough** check box.
3. Select **Properties**.
4. Select **Kerberos Authentication**.
5. If you want to enable Kerberos authentication for Access Platform sites, select the **Use Kerberos authentication to connect to servers** check box.

Enabling Smart Card Authentication

The following section provides information about smart card requirements and explains the steps that you must perform to enable smart card support. For an example of how to configure smart card authentication in the Web Interface, see "Example—Enabling Smart Card Authentication" on page 84.

Smart Card Support Requirements

To use smart card authentication, the Web Interface must be running on IIS and users must be running Internet Explorer Version 5.5 or later Windows systems. Smart card support is not available on UNIX platforms.

Secure Sockets Layer (SSL) must be enabled on the Web server. Because SSL is the mechanism underlying smart card technology, SSL must be used between the browser and Web server. See the Web server documentation for further information.

If you want to enable smart card (with or without other authentication methods), you must configure the **Login** page so it is accessible using HTTPS connections only. If plain HTTP is used or HTTPS is misconfigured, all users receive an error message and cannot log on. To avoid this problem, publish the full HTTPS URL to all users; for example, https://www.yourcompany.com:449/Citrix/AccessPlatform.

For more information about client device requirements and server requirements for smart card support, see the *Clients for Windows Administrator's Guide* and the *Citrix Presentation Server Administrator's Guide*.

Step 1—Installing the Clients for Windows

You must install the Clients for Windows on your users' client devices, using an administrator account. The pass-through authentication feature is available only in the Clients for Windows on the Components CD-ROM. For security reasons, the Web Client does not include this feature. This means that you cannot use Web-based client installation to deploy clients containing this feature to your users.

Step 2—Enabling Pass-Through on the Client

After installation, you must enable pass-through authentication on the client. You can:

- Configure Group Policy to enable pass-through for all clients.

  —Or—

- Edit the Appsrv.ini file. located in users' profiles, to enable pass-through for a single client. For example, if a user's profile is stored locally, this file is located in C:\Documents and Settings*user*\Application Data\ICAClient.

Note Application Data is a hidden folder.

To enable pass-through authentication for all clients

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the Group Policy Object you want to edit.
3. Right-click the **Administrative Templates** folder and choose **Add/ Remove Templates**.
4. Click **Add** and browse to the icaclient template on the Components CD.
5. Click **Open** to add the template and then click **Close** to return to the Group Policy Object Editor.

Note If you already added the icaclient template to the Group Policy Object Editor, you can omit Steps 3 to 5.

6. In the console tree expand the **Administrative Templates** folder.
7. Select **Citrix Components > Presentation Server > Client User Authentication**.
8. Select **Local user name and password**.

9. On the **Action** menu, click **Properties**.
10. Click the **Settings** tab.
11. In the **Local username and password** area, select **Enabled**.
12. Select the **Enable Pass-through authentication** check box and click **OK**.

To enable pass-through authentication for a single client

1. Open the Appsrv.ini file using a text editor such as Notepad.
2. In the [WFClient] section, add the following entries:

```
EnableSSOnThruICAFile=On
SSOnUserSetting=On
```

3. Save the updated file.

Caution If the servers are running versions prior to MetaFrame Presentation Server with Feature Release 2, users may be able to view all applications when using pass-through.

Step 3—Enabling the Windows Directory Service Mapper

You must ensure the Windows Directory Service Mapper is enabled on the server running the Web Interface.

Web Interface authentication uses Windows domain accounts—that is, user name and password credentials. However, certificates are stored on smart cards. The Directory Service Mapper uses Windows Active Directory to map a certificate to a Windows domain account.

To enable the Windows Directory Service Mapper on IIS 6.0

1. Open Internet Information Service (IIS) Manager on the server running the Web Interface.
2. Right-click the Web Sites directory located under the server running the Web Interface and click **Properties**.
3. From the **Directory Security** tab, select **Enable the Windows directory service mapper** in the **Secure Communications** section.
4. Click **OK** to enable the Directory Service Mapper.

Step 4—Enabling Smart Card Authentication Using the Console

You must configure the Web Interface to enable smart card authentication (so that users can access the Web Interface and display their application sets) and authentication to the server (so that users can launch applications in a client session using the Web Interface).

To enable Smart Card authentication using the console

1. Click the **Configure authentication methods** task.
2. Do one of the following:
   - If you are enabling smart card authentication for an Access Platform site, select the **Smart Card** check box and click **OK** to close the **Configure authentication methods** dialog box.
   - If you are enabling smart card authentication for a Program Neighborhood Agent Services site, select the **Smart Card** check box. Go to step 3.
3. Click **Properties**.
4. Select **Roaming**.
5. Select the **Enable roaming** check box and choose one of the following options:
   - **Disconnect sessions on removal**. This option disconnects a user’s session when a smart card is removed.
   - **Log off sessions on removal**. This option logs off a user’s session when a smart card is removed.

Example—Enabling Smart Card Authentication

This example illustrates the steps required to allow a user to log on to the Web Interface and launch applications using a smart card.

You want to enable smart card authentication for the user Gary. Gary is using a Windows 2000 with Service Pack 4 client device. A smart card reader is attached to his client device and smart card support is configured on the server. Currently, the Web Interface is configured to allow only explicit authentication using a user name and password.

To enable smart card authentication

1. Use the Components CD-ROM to install the Clients for Windows on Gary’s client device. The installation of the client is performed using an

administrator account. During installation of the Clients for Windows respond **Yes** to the prompt "Would you like to enable and automatically use your local user name and password for Citrix sessions from this client?"

2. Edit the Appsrv.ini file in Gary's profile. This is located in C:\Documents and Settings\Gary\Application Data\ICAClient
   In the [WFClient] section, add the following entries:

   ```
   EnableSSOnThruICAFile=On
   ```

   ```
   SSOnUserSetting=On
   ```

3. Ensure that the Windows Directory Service Mapper is enabled. For more information, see "Step 3—Enabling the Windows Directory Service Mapper" on page 83.
4. Use the **Configure authentication methods** task in the Access Management Console to enable smart card authentication. When Gary selects Smart Card on the **Login** page, he enters his PIN to log on (assuming he logged on to his Windows desktop using his smart card).

Note If you do not want Gary to have to reenter his PIN when he logs on to the Web Interface, select **Pass-through with smart card**.

Configuring Two-Factor Authentication

You can configure the following two-factor authentication methods for Access Platform sites:

- **Secure Computing SafeWord for Citrix**. A two-factor authentication technology, using alphanumeric codes generated by SafeWord tokens and (optionally) PIN numbers to create a passcode. Users enter their domain credentials and SafeWord passcodes in the **Login** page before they can access applications on the server.
- **RSA SecurID**. A two-factor authentication method that uses numbers generated by RSA SecurID tokens (*tokencodes*) and PIN numbers to create a *PASSCODE*. Users enter their user names, domains, and RSA SecurID PASSCODES on the **Login** page before they can access applications on the

server. When creating users on the ACE/Server, user logon names must be the same as their domain user names.

Note When using RSA SecurID authentication, the system can generate and display a new PIN to the user. This PIN is displayed for 10 seconds or until the user clicks **OK** or **Cancel** to ensure that the PIN cannot be viewed by others. This feature is not available on PDAs.

Enabling Secure Computing SafeWord on IIS

The following section describes how to enable Secure Computing SafeWord support. By default, the SafeWord server port defaults to 5031, but this is configurable. The server running the Web Interface does not need to belong to the Active Directory domain where SafeWord is integrated.

SafeWord Requirements

To use SafeWord authentication with the Web Interface for IIS:

- Obtain the latest version of the SafeWord Agent from Secure Computing
- Ensure the SafeWord Agent for the Web Interface is installed on the server running the Web Interface
- Ensure the Web Interface is installed prior to installing the SafeWord Agent for the Web Interface

If you are using the Web Interface for MetaFrame XP Version 2.0 or earlier and are using SafeWord for Citrix 1.1, you can upgrade to the Web Interface for Citrix Presentation Server Version 4.0.

If you do not have earlier versions of the Web Interface integrated with SafeWord, you must obtain an updated version of the SafeWord Agent for the Web Interface from Secure Computing.

For more information about configuring your SafeWord product, see http://www.securecomputing.com/.

Enabling SafeWord Authentication Using the Console

You must configure the Web Interface to enable SafeWord authentication so that users can access and display their application set. To do this, use the **Configure authentication methods** task.

Enabling RSA SecurID 6.0 Authentication on IIS

The following sections describe how to enable RSA SecurID support.

SecurID Requirements

To use SecurID authentication with the Web Interface for IIS:

- The RSA ACE/Agent for Windows 6.0 must be installed on the server running the Web Interface
- The Web Interface must be installed after the installation of the ACE/Agent

Adding the Server Running the Web Interface as an Agent Host

You must create an Agent Host for the server running the Web Interface in the RSA ACE/Server database, so that the RSA ACE/Server recognizes and accepts authentication requests from the server running the Web Interface. When creating an Agent Host, select **Net OS Agent** from the **Agent type** list.

Copying the sdconf.rec File

Locate (or if necessary, create) the sdconf.rec file on the RSA ACE/Server and copy it to the %SystemRoot%\System32 directory on the server running the Web Interface. This file provides the server with the information necessary to connect to the RSA ACE/Server.

Enabling RSA SecurID Authentication Using the Console

You must configure the Web Interface to enable RSA SecurID authentication to the Web Interface so that users can access and display their application set. To do this, use the **Configure authentication methods** task.

Node Secret Registry Key Considerations

The node secret is used to ensure secure communication between the server running the Web Interface and the RSA ACE/Server.

The node secret can become out of sync between these two servers in the following circumstances:

- If the server running Web Interface is reinstalled
- If the Agent Host record for the server running the Web Interface is deleted and then added again
- If the **Node Secret Created** box is not selected in the **Edit Agent Host** dialog box on the RSA server
- If the RSA server is reinstalled
- If the node secret registry key is deleted on the server running the Web Interface

If the node secret on the server running the Web Interface and the RSA ACE/ Server does not match, RSA SecurID fails.You must reset the node secret on the server running the Web Interface and the RSA ACE/Server.

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

To reset the node secret on the server running the Web Interface

1. In the system registry, navigate to:

   HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT

2. Delete the NodeSecret key.

Note Reinstalling the Web Interface does not delete the node secret key. If the Agent Host entry remains unchanged on the RSA server, the node secret can be reused.

RSA SecurID Multiple Domain Support

If you have user accounts that share the same user name but exist in different Windows domains, you must identify them in the RSA ACE/Server database with a default login using the form *DOMAIN\username* (as opposed to *username* only), and configure the Web Interface to send the domain and user name to the ACE/Server, using the **Configure authentication methods** task available from the Access Management Console.

Enabling RSA SecurID 6.0 Windows Password Integration

The Web Interface supports the Windows password integration feature that is available with RSA SecurID 6.0. With this feature enabled, users of the Web Interface can log on and launch applications with their SecurID PASSCODE. Users need only supply a Windows password the first time they log on to the Web Interface or when their password needs to be changed.

To use SecurID 6.0 Windows password integration with the Web Interface for IIS:

- The RSA ACE/Agent Local Authentication Client for Windows 6.0 must be installed on the server running the Web Interface (administrators must log on to the Web Interface using local machine administrator credentials)
- The Web Interface must be installed after the installation of the ACE/Agent
- The RSA Authentication Agent Offline Local service must be running on the server running the Web Interface
- The Agent Host for the server running the Web Interface in the RSA ACE/Server 6.0 database must be configured to enable the Windows password integration feature
- The database system parameters must be configured to enable the Windows password integration feature at the system level

Enabling Two-Factor Authentication on UNIX

The following sections describe how to enable Secure Computing SafeWord and RSA SecurID support on UNIX.

For UNIX sites, the Web Interface uses the Remote Authentication Dial In User Service (RADIUS) authentication protocol (as opposed to the proprietary agent software that must be installed for IIS sites). Both SafeWord and SecurID can be installed and configured to be presented as a RADIUS server.

Enabling RADIUS with SafeWord

When installing the SafeWord server software, choose to install the IAS RADIUS Agent.

Follow the on-screen instructions regarding installation of the RADIUS client(s) with the Windows IAS snap-in. A new RADIUS client needs to be configured for each server running the Web Interface that authenticates users against the SafeWord server.

Each RADIUS client created must be provided with the following:

- The fully qualified domain name or IP address of the server running the Web Interface with which the RADIUS client is associated.
- A secret, that is known to the associated server running the Web Interface. For more information, see “Creating a Shared Secret for RADIUS” on page 91.
- The client type should be set to **RADIUS standard**.
- The **Request must contain the Message Authenticator attribute** option must be enabled for extra security.

Enabling RADIUS with RSA SecurID

RADIUS is enabled on the ACE/Server using the SecurID 6.0 Configuration Management Tool. For more information about this tool, see the RSA documentation provided with the SecurID software.

Adding the Web Interface and RADIUS Servers as Agent Hosts

Assuming the ACE/Server that authenticates users will also act as the RADIUS server, you must create an Agent Host for the local RADIUS server running in the RSA ACE/Server database. When creating the Agent Host, set the name and IP address to that of the local server, and select **Net OS Agent** from the **Agent type** list. The local server must be assigned as the acting server.

In addition, you must create an Agent Host for each server running the Web Interface in the RSA ACE/Server database so that the RSA ACE/Server recognizes and accepts authentication requests from the server running the Web Interface through the RADIUS server. When creating this Agent Host, select **Communication Server** from the **Agent type** list, and set the encryption key to the value of the secret that is shared with the Web Interface. For more information, see “Creating a Shared Secret for RADIUS” on page 91.

Creating a Shared Secret for RADIUS

The RADIUS protocol requires the use of a shared secret—data that is known only to the RADIUS client (that is, the Web Interface) and the RADIUS server against which it authenticates. The Web Interface stores this secret in a text file on the local file system. The location for this file is indicated in the web.xml file in the radius_secret_path parameter stored on the UNIX server. To create the shared secret, create a text file called radius_secret.txt containing any string. Move this file to the location specified in the web.xml file, and ensure that it is locked down and can be accessed only by the appropriate users or processes.

Enabling RADIUS Two-Factor Authentication Using the Console

You must enable two-factor authentication to the Web Interface so that users can access and display their application set. To do this, use the **Configure authentication methods** task in the Access Management Console. For UNIX sites, in addition to enabling two-factor authentication, you can specify one or more RADIUS server addresses (and optionally ports), the load balancing or failover behavior of the servers, and the response time-out.

Using RADIUS Challenge Mode

By default, the SecurID RADIUS server is in *RADIUS Challenge Mode*. In this mode:

- The Web Interface displays a generic challenge screen with a message, an HTML password box, and **OK** and **Cancel** buttons.
- Challenge messages are not localized by the Web Interface. Messages are in the language of the challenge messages set on the SecurID RADIUS server.

If users do not submit a response (for example, if they click **Cancel**), they are directed back to the **Login** page.

Citrix recommends that this mode is used only if software components or products other than the Web Interface also use the RADIUS server for authentication.

Using Customized Challenge Messages

You can configure customized challenge messages for the SecurID RADIUS server. When using custom messages that are known to the Web Interface, it can present user interface pages identical to those displayed by the Web Interface for IIS, and these pages are localized.

This feature requires changes to the RADIUS server configuration and must be implemented only if the RADIUS server is used solely to authenticate Web Interface users.

You can change challenge messages by launching the RSA RADIUS Configuration Utility. For more information about using this tool, see the RSA documentation provided with the SecurID software. To display the same messages to users accessing sites on IIS and UNIX servers, the following challenges must be updated:

Message For	**Packet**	**Updated Value**
Does User Want a System PIN	Challenge	CHANGE_PIN_EITHER
Is User Ready To Get System PIN	Challenge	SYSTEM_PIN_READY
Is User Satisfied With System PIN	Challenge	CHANGE_PIN_SYSTEM_[%s]
New Numeric PIN of Fixed Length	Challenge	CHANGE_PIN_USER
New Alphanumeric PIN of Fixed Length	Challenge	CHANGE_PIN_USER
New Numeric PIN of Variable Length	Challenge	CHANGE_PIN_USER
New Alphanumeric PIN of Variable Length	Challenge	CHANGE_PIN_USER
New PIN Accepted	Challenge	SUCCESS
Enter Yes or No	Challenge	FAILURE
Next Token Code Required	Challenge	NEXT_TOKENCODE

Managing Clients

This chapter provides information about deploying and using Citrix Presentation Server Clients and the Citrix Streaming Client with the Web Interface. It also explains how to set up secure client access. Topics include:

- Managing Client Deployment
- Configuring the Program Neighborhood Agent
- Managing Secure Client Access
- Editing Client-Side Proxy Settings

Managing Client Deployment

To access applications or log on to conferences, users must have a supported Web browser and a Citrix Presentation Server Client, Citrix Streaming Client, or Remote Desktop Connection software.

Use the **Manage client deployment** task to specify which clients are offered to users for download and installation. You can also use this task to specify which clients users can launch applications with.

You can:

- Configure Web-based client installation. This feature allows you to easily download and install the appropriate clients on your users' devices using *installation captions.* Installation captions are links that are presented to users who require a client. Users click a link to install the client on their client device.
- Configure the Web Interface to automatically install the full client for Windows users accessing applications through Internet Explorer.

Note Automatic client installation is available only for sites configured to run remote applications.

- Configure the Web Interface to offer the Citrix Streaming Client to users for installation.
- Specify which clients users can launch applications with.
- Enable users to choose how their applications are launched.
- Specify the components included in the Client for Java or allow users to select the components that they require.

Remote Client Types

The following clients are available for launching remote applications:

- **Native client**. The full client can automatically be installed for users. Seamless windows are supported; applications are launched in desktop windows that can be resized. If users are accessing applications through a PDA device, you must enable the native client.
- **Native embedded client (ActiveX or Netscape plugin)**. Users download and install this client when they launch applications. Seamless windows are not supported; applications are launched embedded in a browser window.
- **Client for Java**. Users download the Client for Java when they launch applications. This client supports seamless windows; applications are launched in desktop windows that can be resized.
- **Embedded Remote Desktop Connection software**. Users download and install Remote Desktop Connection software when they launch applications. Seamless windows are not supported; applications are launched in embedded browser windows.

You must specify a default client. To do this, select a client and click **Set as default**.

Note The native embedded client, Client for Java, and embedded Remote Desktop Connection software are not supported on Personal Digital Assistants (PDAs) running Pocket PC.

Citrix Streaming Client

The Citrix Streaming Client allows users to stream applications to their desktop and open them locally. The Citrix Streaming Client:

- Runs as a service on the user workstation to invoke applications the user selects using Program Neighborhood Agent or a Web browser
- Finds the correct package target for the user workstation, creates an isolation environment on the user workstation, and streams the necessary files for the application to run to the user desktop

You can install the Citrix Streaming Client with the Program Neighborhood Agent to provide the full set of application streaming features or alone on the user's desktop so the user can access published applications through a Web browser using an Access Platform site.

For more information about publishing streamed applications, see the *Citrix Presentation Server Administrator's Guide*.

For more information about the application streaming feature, see the *Citrix Application Streaming Guide*.

Using Web-Based Client Installation

To use the Web Interface, users must have a supported Web browser, a Citrix Presentation Server client, and the Citrix Streaming Client (to access streamed applications).

Copying Client Installation Files to the Web Server

To use Web-based client installation, the Web server must contain the client installation files.

During Web Interface installation, Setup prompts you to supply the Components CD-ROM or CD image. Setup copies the contents of the CD's Clients directory to a directory called \Clients in the common files root directory (for example, C:\Program Files\Citrix\Web Interface\4.5\Clients).

If you did not copy the client installation files to the Web server during Web Interface installation, make sure you copy these files to the Web server before using Web-based client installation.

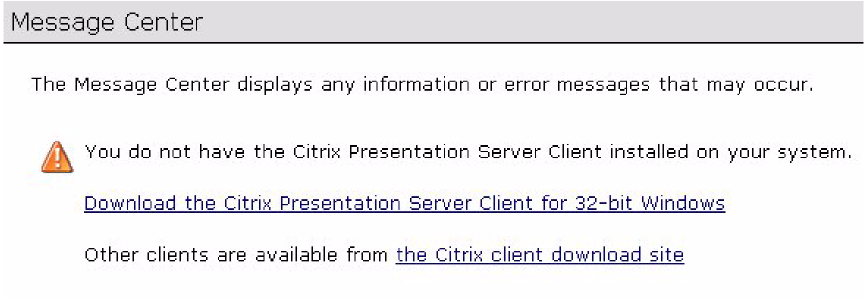
To copy the client files to the Web server

1. Locate the Clients directory where the Web Interface is installed. For example, C:\Program Files\Citrix\Web Interface\4.5\Clients.
2. Insert the Components CD-ROM in the Web server's CD-ROM drive or browse the network for a shared Components CD image.

3. Change directories to the CD's \Clients directory. Copy the contents from the \Clients directory on the CD to the \Clients directory on the server running the Web Interface. Make sure you copy the contents of the directory and not the \Clients directory itself.

Configuring Installation Captions

When a user logs on to a Web Interface site, the Web-based client installation feature checks the user's computer for the presence of client software. If the client software is not detected, the Web-based client installation feature presents the appropriate client software for download and setup. The user clicks this link to install the client on the user's client device. These links are called *installation captions*. For example:



Message Center

The Message Center displays any information or error messages that may occur.

You do not have the Citrix Presentation Server Client installed on your system.

Download the Citrix Presentation Server Client for 32-bit Windows

Other clients are available from the Citrix client download site

This screen capture shows an example of an installation caption that may appear in the user's Login page.

To configure an installation caption

1. Click the **Manage client deployment** task.
2. Click **Installation Caption**.
3. Specify when the installation caption is shown to users. Choose from the following:
   - **Automatically**. If the user does not have an appropriate client installed, the installation caption is displayed. This is the default setting.
   - **Always**. The installation caption is always displayed on all platforms.
   - **Never**. The installation caption is never displayed.

Configuring a Custom Installation Caption

The **OverrideClientInstallCaption** parameter in the WebInterface.conf file specifies a custom message that can be displayed along with the download links for the clients. By default, this parameter is commented out by a number sign (#) at the beginning of the line and the default messages are used. The default message is specific to the identified client platform, and is similar to the following:

"You do not have the Web Client installed on your system. You must install the client to launch the applications.
Select the icon below to install the client."

To display a custom message with the download links

1. Open the WebInterface.conf file.
2. Edit the **OverrideClientInstallCaption** parameter. For example:

   OverrideClientInstallCaption=Please install a client. Here are the clients we offer:

To configure the clients offered to users by installation captions, you must edit the WebInterface.conf file. For more information, see "Configuring Sites Using the Configuration File" on page 137.

Deploying Remote Desktop Connection Software

Remote Desktop Connection functionality is available on 32-bit Windows systems with Internet Explorer 5.5 or later.

Remote Desktop Connection Requirements

If you are configuring a Conferencing Manager Guest Attendee site and users will connect using Remote Desktop Software, ensure that conferences are created using a color depth of 256 or lower. Otherwise, users connecting with Remote Desktop Software will receive an error message and will be unable to log on.

If the client's browser does not place the Web Interface site in the intranet or the Trusted Sites zone, it will display an error message and refer the user to the online help for more information. In this instance, Citrix recommends that users be advised of the following procedure.

To add the server running the Web Interface to the Trusted Sites zone

1. In Internet Explorer, open the **Tools** menu.
2. Select **Internet Options**.
3. Open the **Security** page.

4. Select **Trusted Sites**.
5. Click **Sites**.
6. In the **Add this Web site to the zone** box, enter the name of the server running the Web Interface; for example, http://*servername*.
7. Click **Add** to add the server to the **Web sites** list.
8. Click **OK** twice to close the **Internet Options** dialog box.

Deploying the Client for Java

If you are deploying clients over a low-bandwidth network or you are not sure what platform your users are on, consider using the Client for Java. The Client for Java is an applet that is cross-platform compatible and can be deployed by the server running the Web Interface to any Java-compatible Web browser.

Customizing the Client for Java Deployment

You can configure the components included in the deployment of the Client for Java.

The size of the Client for Java download is determined by the packages you include in the download. The fewer packages selected, the smaller the download (the download can be as small as 540K). If you want to limit the size of the download for users on low bandwidth connections, you can deploy only a minimum set of components. Alternatively, you can enable users to control which components are required.

Note Some components that you make available in the Client for Java may require further configuration on the client device or on the server.

For more information about the Client for Java and its components, see the *Client for Java Administrator's Guide*.

The following table explains the options available:

Package	Description
Audio	Enables applications running on the server to play sounds through a sound device installed on the client device. You can control the amount of bandwidth used by the client audio mapping on the server—see the *Citrix Presentation Server Administrator's Guide* for information.
Clipboard	Enables users to copy text and graphics between server-based applications and applications running locally on the client device.
Local text echo	Accelerates the display of the input text on the client device.
SSL/TLS	Secures communication using Secure Sockets Layer (SSL) and TLS (Transport Layer Security). SSL/TLS provides server authentication, encryption of the data stream, and message integrity checks.
Encryption	Provides strong encryption to increase the privacy of client connections.
Client drive mapping	Enables users to access their local drives from within a client session. When users connect to the server, their client drives are mounted automatically, such as floppy disks, network drives, and CD-ROM drives. Users can access their locally stored files, work with them during their client sessions, and save them again on a local drive or on a drive on the server. To enable this setting, users must also configure client drive mapping in the Client for Java Settings dialog box. See the *Client for Java Administrator's Guide* for more information.
Printer mapping	Enables users to print to their local or network printers from within a client session.
Configuration UI	Enables the Client for Java Settings dialog box. This dialog box is utilized by users to configure the Client for Java.

Using Private Root Certificates with the Client for Java Version 9.*x*

If you configured the Secure Gateway or the Citrix SSL Relay service with a server certificate obtained from a private certificate authority (for example, if you issue your own certificates using Microsoft Certificate Services), you must import the root certificate into the Java keystore on each client machine. For more information, see the *Client for Java Administrator's Guide*.

Using Private Root Certificates with the Client for Java Version 8.*x*

To use private root certificates with Version 8.*x* of the client, select the **Use a private root certificate** option. Enter the file name of the certificate in the **Certificate file name** box. The certificate must be located in the same directory on the Web server as the Java Client packages (such as Clients\icajava in the common files directory on IIS).

Important This option does not verify that the root certificate is delivered over a secure connection. Because the root certificate could be transmitted over an unencrypted HTTP link, it is potentially vulnerable to attack. Citrix recommends that you configure the Web server to use HTTPS connections.

Deploying the Client for Java Using the Web Interface with Custom SSL/TLS Certificates

Use the following procedure to configure the Web Interface to use a single custom SSL root certificate if you are using the Client for Java Version 8.*x*.

The certificate is made available to the Client for Java as an individual file in the client’s codebase directory on the Web server. This can cause problems for .cer files because IIS sends these using MIME text and the file can become corrupted during transport (for example, line endings change). Also, some Java Virtual Machines (JVM), such as the IBM JVM on OS/2, will not retrieve certificates when specified as individual files.

Citrix recommends that you package custom root certificates into a single archive file to supply multiple certificates. This procedure is documented in the *Client for Java Administrator’s Guide*.

The following procedure describes how to configure custom certificates using the Web Interface and the Client for Java.

To configure custom certificates

1. Contact your Certificate Authority and obtain the root certificates that correspond to the server certificates being used on the servers.
2. In a text editor, locate and open the appembedJICA.inc file. Typically, this is C:\Inetpub\wwwroot\Citrix\SiteType\app_data\site\include.
3. Locate the section between the <applet> and </applet> HTML tags.

4. Before the </applet> tag, specify which SSL/TLS certificates the Client for Java should use. Use the following parameters:

   - **SSLNoCACerts**. The number of specified certificates in the client archive.
   - **SSLCACert0, SSLCert1...SSLCert*n***. The names of the root certificates to use when validating the name of the server certificate. The number of root certificates that you specify must match the number specified in the **SSLNoCACerts** parameter.

     For example, if you have three custom root certificates with filenames A.crt, B.crt, and C.cer, insert the following lines:

     <param name="SSLNoCACerts" value="3">

     <param name="SSLCACert0" value="A.crt">

     <param name="SSLCACert1" value="B.crt">

     <param name="SSLCACert2" value="C.cer">

5. If the client will be deployed in Microsoft Internet Explorer with the Microsoft JVM, package the certificates in a .cab file. For more information, see the *Client for Java Administrator's Guide*.

6. Search for the cabinets parameter. Add the name of the archive you created in Step 6. For example, if you named your archive MyCerts.cab, change the following:

   <param name=cabinets value="<%=jicaCabFiles%>">

   to

   <param name=cabinets value="<%=jicaCabFiles%>MyCerts.cab">

7. Copy your archive file to the directory on the Web server that contains the Client for Java files. For example, C:\Program Files\Citrix\Web Interface\4.5\Clients\icajava.

8. Save the appembedJICA.inc file.

9. On the client device, launch the Web browser and connect to the server running the Web Interface. All embedded Client for Java sessions to secured servers work transparently using SSL.

Automatically Deploying Clients

You can configure the Web Interface to automatically deploy the native client to users running Internet Explorer. You can also deploy the Client for Java automatically if, for example, the client is not installed on the users local machine.

Note Automatic client deployment is available for sites configured to only run remote applications.

Automatically Deploying the Native Client

You can automatically deploy the native client to users running Internet Explorer.

If you enable this feature, when users access the Web Interface, their client devices and Web browser are detected. If they are on a Windows platform and they do not have a client, or their current client is not up-to-date, the Web Interface attempts to install the specified client on their client devices automatically.

If users have administrative rights on their computers, they select whether to install any or all of the native client components. If users do not have administrative rights they install only the Web client.

Automatically Deploying the Client for Java

You can configure the Web Interface to automatically deploy the Client for Java if a client is not installed on the user’s local machine.

To enable automatic fallback to the Client for Java

1. Click the **Manage client deployment** task.
2. Select **Remote clients**.
3. Select the **Native client** and/or **Embedded native client** check boxes.
4. Select the **Client for Java** check box.
5. In the **Fallback to Client for Java** area, select the **Automatic fallback to the Client for Java** check box.
6. Click **Finish** to accept the changes.

Note The Client for Java must be deployed for users connecting with a Safari 1.x Web browser.

Compatibility with Asian Language Web Servers

You can configure the Web Interface to generate ICA files in Unicode, which increases the number of non-European language characters remote clients recognize. ICA files are text files that contain parameters and instructions for launching published applications. This feature works only with clients available with MetaFrame Presentation Server 3.0 and later; earlier versions of the clients do not support Unicode ICA files.

To ensure that ICA files are in Unicode

1. Click the **Manage client deployment** task.
2. Select **Version Support**.
3. Click **Support version 8 or later of the clients**.

Configuring Streaming Session Monitoring

You can use the **Manage client deployment** task to configure the Web Interface to provide information about user sessions to the Citrix administrator. The Web Interface provides this information by means of a session URL used to communicate with the Citrix Streaming Client. In most cases this URL is detected automatically. It may, however, need to be set manually; for example, if a client-side proxy is in use.

You can use the Access Management Console to view session information. You can view information for all user session in multiple farms, specific published application, sessions connecting to a specific server, or a specific user’s sessions and applications.

To configure streaming session monitoring

1. Click the **Manage client deployment** task.
2. Select **Citrix Streaming Client**.
3. Select how the Web Interface communicates with the Citrix Streaming Client. Choose from the following:
   - To automatically detect the session URL used to communicate with the client, select **Automatically detect the session URL**.
   - To set the session URL manually, select **Specify session URL** and enter the URL details.
4. Click **OK**.

Configuring the Program Neighborhood Agent

The Program Neighborhood Agent allows users to access remote and streamed applications directly from the Windows desktop without using a Web browser. You can remotely configure the placement of links to remote applications from the Start menu, on the Windows desktop, or in the Windows notification area. The Program Neighborhood Agent user interface can also be "locked down" to prevent user misconfiguration. You can use the Access Management Console or the config.xml file to configure the Program Neighborhood Agent.

Using the Access Management Console for Configuration

The Program Neighborhood Agent is configured with default presentation options, authentication methods, and server connection options. The Access Management Console provides a tool to change the default settings to prevent users from changing specific options.

For more information about using the console, see "Configuring Sites Using the Console" on page 43.

Using the Configuration Files

You can also configure the Program Neighborhood Agent using the config.xml and WebInterface.conf files. These files are typically located in the C:\Inetpub\wwwroot\Citrix\PNAgent\conf\ folder on the server running the Web Interface.

Managing Client Configuration Files

The Program Neighborhood Agent options configured with the console are stored in a configuration file on the server running the Web Interface (for sites using local configuration) or on a server in the farm running the configuration service (for sites using centralized configuration); typically this is also the server running the XML Service. The configuration file controls the range of parameters that appear as options in the users's **Program Neighborhood Agent Properties** dialog box. Users can choose from available options to set preferences for their ICA sessions, including logon mode, screen size, audio quality, and the locations of links to published resources.

For locally configured sites, a default configuration file, config.xml, is installed with default settings and is ready for use without modification in most network environments. The config.xml file is stored in the \conf folder for the site.

Use the **Export client configuration** task to save a copy of the selected config.xml file to another location.

Managing Secure Client Access

If you are using Access Gateway, the Secure Gateway, or a firewall in your deployment, you can use the **Manage secure client access** tasks to configure the Web Interface to include the appropriate settings. For example, you can configure the Web Interface to provide an alternate address, if the server is configured with an alternate address and the firewall is configured for Network Address Translation.

This section explains how to use the **Manage secure client access** tasks to edit demilitarized zone (DMZ) settings, configure gateway settings, edit address translations, and how to display your settings in the details pane.

Note The following sections are applicable to Access Platform and Conferencing Manager Guest Attendee sites only.

Editing DMZ Settings

You can configure client addresses, masks, and access methods using the **Edit DMZ settings** task. The order in which entries appear in the client address table is the order in which the rules are applied. If none of the rules are applicable, the default rule is applied.

To add or edit a client route

1. In the **Edit DMZ settings** dialog box, click **Add** to add a new client route or **Edit** to edit an existing client route.
2. Enter the network address and subnet mask that identify the client network.
3. Select an access method from the following options:
   - **Direct**. The address given to the client is the actual address of the server. This is the default setting.
   - **Alternate**. The alternate address is given to the client. The server must be configured with an alternate address and the firewall configured for network address translation.
   - **Translated**. The address given to the client is determined by the address translation mappings set in the Web Interface.

- **Gateway Direct**. The address given to the Gateway server is the actual address of the server.
- **Gateway Alternate**. The alternate address is given to the Gateway server. The server running Presentation Server must be configured with an alternate address and the firewall configured for network address translation.
- **Gateway Translated**. The address given to the Gateway server is determined by the address translation mappings set in the Web Interface.

4. Click **OK**.

Editing Gateway Settings

If you are using the Access Gateway or Secure Gateway in your deployment, you must configure the Web Interface for Gateway support. To do this, use the **Edit Gateway settings** task.

To edit gateway settings

1. In the **Edit Gateway Settings** dialog box, specify the fully qualified domain name (FQDN) of the Gateway server that clients must use in the **Gateway address (FQDN)** box. This must match what is on the certificate installed on the Gateway server.
2. Specify the port number on the Gateway server that clients must use in the **Gateway port** box. The default port number is 443.
3. To use session reliability, select the **Enable session reliability** option.
4. In the **Secure Ticket Authorities** area, click **Add** to specify the URL of a Secure Ticket Authority that the Web Interface can use. The Secure Ticket Authority is displayed in the **Secure Ticket Authority URLs** list. Secure Ticket Authorities are included with the XML service, for example, in http://mfsrv01/Scripts/CtxSta.dll. You can specify more than one Secure Ticket Authority for fault tolerance; however, Citrix recommends that you do not use an external load balancer for this purpose. You can specify up to 256 Secure Ticket Authorities in this list.
5. To place the Secure Ticket Authorities in order of priority, highlight a Secure Ticket Authority URL and click **Move Up** or **Move Down**. To remove a Secure Ticket Authority URL, highlight it in the list and click **Remove**.

6. Choose whether or not to enable load balancing between Secure Ticket Authorities using the **Use for load balancing** option. Enabling load balancing allows you to evenly distribute connections among servers so that no one server becomes overloaded. If an error occurs while communicating with a server, all further communication is load balanced among the remaining servers in the list.
7. The Web Interface provides fault tolerance among servers in the Secure Ticket Authority list. If an error occurs while communicating with a server, the failed server is bypassed for the time specified in the **Bypass any failed server for** box.
8. Click **OK** to finish making changes.

Editing Address Translations

Using the **Edit address translations** task, you can map the server address to the address and port translated by the internal firewall. Users can then launch applications if the address and port of the server is translated at the internal firewall.

You can use the Web Interface to define mappings from internal IP addresses to external IP addresses and ports. For example, if your server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address.

To configure internal firewall address translation

1. In the **Edit address translations** dialog box, click **Add** to add an address translation or **Edit** to edit an existing address translation.
2. In the **Access type** area, select one of the following:
   - **Client route translation**. The client uses the translated address to connect to the server.
   - **Gateway route translation**. The Gateway server uses the translated address to connect to the server.
   - **Client and Gateway route translation**. Both the client and the Gateway server use the translated address to connect to the server.
3. In the **Internal IP address** box, enter the normal (internal) IP address of the server.
4. In the **Internal port** box, enter the port number of the server.
5. In the **External address** box, enter the translated (external) IP address or host name that clients must use to connect to the server.
6. In the **External port** box, enter the port number of the server.

7. Click **OK**. The mapping appears in the **Address Translation** table.
8. To remove a mapping, select the mapping in the **Address Translation** table and click **Remove**.

Displaying Secure Client Access Settings

Use the **Display settings** task to view all secure client access settings that are currently configured for the site.

You can view the different configurations for each secure client access task using the **View** drop-down menu, and you can click the link in the display to launch the pages associated with that task.

Editing Client-Side Proxy Settings

If you are using a proxy server at the client-side of the Web Interface installation, you can configure whether or not clients must communicate with the server through the proxy server. You use the **Edit client-side proxy** task to do this.

A proxy server positioned at the client-side of a Web Interface installation provides security benefits that include:

- Information hiding, where system names inside the firewall are not made known to systems outside the firewall through DNS (Domain Name System)
- Channeling different TCP connections through one connection

Using the Access Management Console, you can set default proxy rules for clients. However, you can also configure exceptions to this behavior for individual clients. To configure exceptions, you associate the proxy server's external IP address with a Web Interface proxy setting.

You can also specify that proxy behavior is controlled by the client. For example, to use the Secure Proxy feature in Presentation Server, configure the Web Interface to use the proxy settings specified on the client and configure the client for Secure Proxy. For more information about using clients to control proxy behavior, see the relevant Administrator’s Guide.

To configure default proxy settings

1. Click the **Edit client-side proxy** task.
2. Click **Add** to create a new mapping or **Edit** to edit an existing mapping.
3. Enter the external address of the proxy in the I**P Address** box.
4. Enter the subnet mask in the **Subnet Mask** box.

5. In the **Proxy** list, select one of the following:

   - **User's browser setting**. The client auto-detects the Web proxy based on the client’s browser configuration.
   - **Web proxy auto detect**. The client auto-detects the Web proxy using the Web Proxy Auto Discovery (WPAD) protocol.
   - **Client defined**. The settings configured for the client by the user.
   - **None**. No proxy is used.
   - **SOCKS**. If this option is selected, you must enter the address of the proxy server in the **Proxy Address** box and the port number in the **Proxy Port** box. The proxy address can be an IP address or a DNS name.
   - **Secure (HTTPS)**. If this option is selected, you must enter the address of the proxy server in the **Proxy Address** box and the port number in the **Proxy Port** box. The proxy address can be an IP address or a DNS name.

6. Click **OK**. The mapping is added to the **Mapping** list.

7. You can control the order in which multiple mappings are applied. Select a mapping and click **Move Up** or **Move Down** to place the mappings in order of priority. To remove a mapping, select the mapping and click **Remove**.

Customizing the User Experience

Overview

This chapter describes how to customize the way in which the Web Interface is displayed to users. Topics in this chapter include:

- Customizing the Appearance for Users
- Managing Client Session Preferences
- Configuring Workspace Control
- Changing Session Options
- Managing Application Shortcuts
- Using Application Refresh Options

Customizing the Appearance for Users

You can customize the appearance of the user interface if, for example, you want the site to have a specific corporate look and feel.

Use the **Customize appearance for user** task to customize:

- **Layout**. Customize the user's overall screen layout or allow users to customize the layout. You can select auto, full display, or compact screen layout. A compact user interface may be useful, for example, for users accessing their applications on PDAs. This interface does not contain the welcome message and message center areas, and does not show client installation captions. Additionally, messages are displayed above the main page. Format the number of application icon columns that are displayed, and allow users to customize these settings.
- **Appearance**. Format the user's screen with a customized "look and feel" by displaying customized headers and footers, branding colors, header

images, and logo images. Additionally, you can create a hyperlink for logos.

- **Content.** Define custom welcome message and footer text. Specify any additional languages.

The graphics in these option pages update as you make your changes, and are reflected in the main **Customize appearance for user** page.

Managing Client Session Preferences

Use the **Manage session preferences** task to specify the settings that users can adjust. You can also use this task to specify the length of time after which inactive users are logged off from the Web Interface and whether or not the Web Interface should override the ICA client name.

Note This task is not available for sites configured to run only streamed applications.

For Access Platform sites, you can enable and specify whether or not users can adjust the following options:

- Bandwidth control
- Color depth
- Audio quality
- Printer mapping
- Window size
- PDA synchronization settings
- Windows key combinations
- Kiosk mode

You can also specify the following:

- Whether or not to display the Settings button to users on the Applications page
- The length of time a user session can be inactive before the user is logged off.
- Whether or not the Web Interface should override the ICA client name.

Important You must enable the **Web Interface should override the ICA client name** setting if you want to use Workspace control with versions 8.x and 9.x of the clients.

Bandwidth control allows users to select session settings based on their connection bandwidth. These options are displayed in the **Login** page under **Advanced Options** in the **Connection Speed** drop-down list. Bandwidth control provides control for color depth, audio, and printer mapping. To enable this feature, you must also select **Allow user to customize printer mapping** in the Manage session preferences task. Additionally, you can use ICA override files to control other ICA settings for bandwidth control:

File Name	Description
bandwidth_ high.ica	Contains the override ICA settings for high bandwidth connections.
bandwidth_ medium_high.ica	Contains the override ICA settings for medium high bandwidth connections.
bandwidth_ medium.ica	Contains the override ICA settings for medium bandwidth connections.
bandwidth_low.ica	Contains the override ICA settings for low bandwidth connections.
default.ica	Contains the override ICA settings used when no bandwidth is selected.

The ICA override files are located in the \conf folder for a site, typically C:\Inetpub\wwwroot\Citrix\SiteName\conf.

If the Client for Java is used, bandwidth control determines whether or not audio and printer mapping packages are downloaded. If Remote Desktop Connection software is used, audio quality is either mapped to On or Off and further quality control is not provided. Low bandwidth is recommended for wireless WAN connections.

Note If Remote Desktop Connection software is used in conjunction with bandwidth control, the Web Interface specifies parameters appropriate to the selected bandwidth. However, the actual behavior depends on the version of the Remote Desktop Software, Terminal Servers, and the server configuration.

By default, users can adjust the window size of client sessions.

For Conferencing Manager Guest Attendee sites, you can configure:

- Windows key combinations
- Kiosk mode

Kiosk mode is ideal for situations in which client devices are public terminals and used by a variety of users. When kiosk mode is enabled, users' settings are not stored and are retained only for the duration of their session.

If you prevent users from adjusting a setting, the setting is not displayed in the user interface and the Presentation Server settings specified for the published application are used.

Configuring Workspace Control

Use the **Manage workspace control** task to allow users to quickly disconnect all running applications, reconnect to disconnected applications, and log off from all running applications. This allows users to move between client devices and gain access to all of their applications (disconnected only or disconnected and active) either when they log on or manually at any time. For example, hospital workers may need to move between workstations and access the same set of applications each time they log on to Presentation Server.

Feature Requirements

The following requirements and recommendations apply to the Workspace control feature:

- To use Workspace control you must enable the **Web Interface should override the ICA client name** setting in the **Manage session preferences** task. This is the default setting.
- If the Web Interface detects that it is being accessed from within a client session, the Workspace control feature is disabled.
- To use pass-through, smart card, or pass-through with smart card, you must set up a trust relationship between the server running the Web Interface and the Citrix XML Service. For more information, see “Using Workspace Control with Integrated Authentication Methods” on page 116.
- Applications published for anonymous use are terminated when both anonymous and authenticated users disconnect, provided that the Citrix XML Service is set to trust Web Interface credentials. Thus, users cannot reconnect to anonymous applications after they disconnect.
- If client credential pass-through is not enabled, smart card users are prompted for their PINs for each session being reconnected. This is not an issue with pass-through or pass-through with smart cards because client credential pass-through is enabled with these options.
- Each session times out after a period of inactivity (typically 20 minutes). When the HTTP session times out, the **Login** screen appears; however, any applications launched or reconnected in that session are not disconnected. Users must manually disconnect, log off, or log back on to the Web Interface and use the **Log off** buttons or disconnect.

Limitations

Workspace control is not available for sites configured to run streamed applications. If you configure a site for dual mode streaming, workspace control works only with remote applications.

You cannot use workspace control with the Client for Win32 prior to version 8, or Remote Desktop Connection software.

Additionally, this feature works only with servers running MetaFrame Presentation Server Version 3.0 or later.

Using Workspace Control with Integrated Authentication Methods

If users log on using smart card, pass-through with smart card, or pass-through authentication, you must set up a trust relationship between the server running the Web Interface and any other server in the farm running the Citrix XML Service that the Web Interface contacts. The Citrix XML Service communicates information about published applications between the Web Interface and servers running Presentation Server. Without the trust relationship, the Disconnect, Reconnect, and Log Off commands fail for those users logging on with smart card or pass-through.

You do not need to set up a trust relationship if your users are authenticated by the server farm; that is, if users do not log on using smart card or pass-through authentication methods.

To set up the trust relationship

1. In the Access Management Console, select the server running Presentation Server in the left pane.
2. From the **Action** menu, select **Modify server properties > Modify all properties**.
3. From the **Properties** list, select **XML Service**.
4. Select the **Trust requests sent to the XML Service** check box.

If you configure a server to trust requests sent to the XML Service, consider these factors:

- When you set up the trust relationship, you depend on the Web Interface server to authenticate the user. To avoid security risks, use IPSec, firewalls, or any technology that ensures only trusted services communicate with the XML Service. If you set up the trust relationship without using IPSec, firewalls, or other security technology, it is possible for any network device to disconnect or terminate client sessions. The trust relationship is not necessary if sites are configured using explicit authentication only.
- Enable the trust relationship only on servers directly contacted by the Web Interface. These servers are listed on the **Manage server farms** page.
- Configure IPSec, firewalls, or other technology that you use to secure the environment to restrict access to the Citrix XML Service to only the Web Interface servers. For example, if the Citrix XML Service is sharing a port with Microsoft Internet Information Services (IIS), you can use the IP address restriction capability in IIS to restrict access to the Citrix XML Service.

Enabling Workspace Control

To enable Workspace control, use the **Manage workspace control** task.

Use this dialog box to:

- Enable automatic reconnection when users log on to allow users to reconnect to disconnected applications or both disconnected and active applications
- Enable the **Reconnect** button to allow users to reconnect to disconnected applications or both disconnected and active applications
- Allow users to log off from both the Web Interface and active sessions or from the Web Interface only

To enable automatic reconnection when users log on

1. Select the **Automatically reconnect to sessions when user logs in** option.
2. Choose one of the following:
   - To automatically reconnect both disconnected and active sessions, select **All sessions**
   - To automatically reconnect disconnected sessions only, select **Disconnected sessions only**
3. Select the **Allow user to customize** check box to allow users to select these options in the user interface.

To enable the Reconnect option

1. Select the **Automatically reconnect to sessions after user logs in** option.
2. Choose one of the following:
   - To configure the Reconnect button to reconnect users to both disconnected and active sessions, select **All sessions**
   - To configure the Reconnect button to reconnect users to disconnected sessions only, select **Disconnected sessions only**
3. Select the **Allow user to customize** check box to allow users to select these options in the user interface.

To configure log off behavior

1. In the **Log off** section, to log users off from the Web Interface and all active sessions, select **Log off all sessions when user logs off from the Web Interface**.

2. Select the **Allow user to customize** check box to allow users to select these options in the user interface.

Changing Session Options

For Program Neighborhood Agent Services sites you can use the **Change session options** task to configure the following settings for user sessions:

- **Window sizes**. Use these options to select the window sizes available for ICA sessions, and to define custom sizes in pixels or screen percentage.
- **Color**. Options enabled in this section are available for users to select.
- **Windows key combinations**. Use these options to enable the targets of Windows key combinations that users can select. Windows key combinations do not affect seamless connections. You can provide options in the user's **Connection Preference** screen for the following modes:
  - **Local**. Key combinations apply to the local desktop only; they are not passed to the ICA sessions.
  - **Remote**. Key combinations apply to the remote desktop in the ICA session.
  - **Full screen only**. Key combinations apply to the remote desktop in the ICA session only when it is in full screen mode.
- **Audio**. Options enabled in this section are available for users to select.
- **Workspace control options**. Use these options to configure Workspace control settings. For more information, see "Configuring Workspace Control" on page 114.

Note This task is not available for sites configured to run only streamed applications.

Managing Application Shortcuts

You can use the **Manage application shortcuts** task to specify how the Program Neighborhood Agent displays shortcuts for published applications.

You can create the following types of shortcuts:

- **Start menu**. You can use the settings specified in the **Manage application shortcuts** page, settings defined during application publishing in

Presentation Server, or use both settings. You can also define how and if shortcuts are displayed in the Start menu, and allow users to specify this setting. Additionally, you can create shortcuts in the Programs menu, create an additional submenu, and/or allow users to specify a submenu name.

- **Desktop**. You can use the settings specified in the **Manage application shortcuts** page, settings defined during application publishing in Presentation Server, or use both settings. You can also define how and if shortcuts are displayed on the desktop, and allow users to specify this setting. Additionally, you can use a custom folder name, allow users to select a name, and/or use a custom URL for icons.
- **Notification area**. You can display applications in the notification area and/or allow users to specify how applications are displayed.

Using the **Manage application shortcuts** task, you can also remove shortcuts. You can specify when shortcuts are removed (either when the Program Neighborhood Agent closes or when users log off from the Program Neighborhood Agent), and which shortcuts are removed (Program Neighborhood shortcuts or Program Neighborhood and user-created shortcuts). If you select both Program Neighborhood and user-created shortcuts, you can also specify the search folder depth to improve performance.

Using Application Refresh Options

Use the **Manage application refresh** task to specify when the user's list of published resources is refreshed and if users can customize these settings. You can enable refresh when the Program Neighborhood Agent starts up, when applications are launched, and specify how often the list is refreshed.

Configuring Web Interface Security

Overview

This chapter provides information about how to secure your data in a Web Interface environment. Topics include:

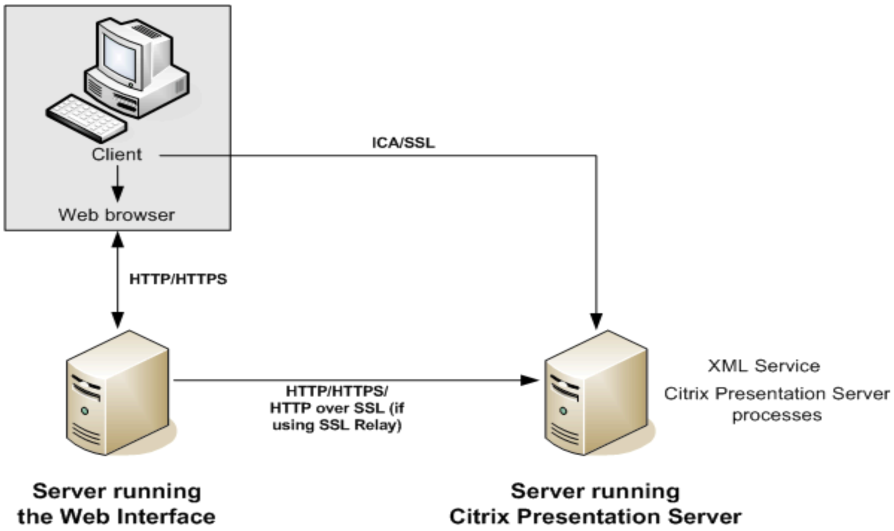
- Introduction to Web Interface Security
- Securing Web Interface Communication
- Securing the Program Neighborhood Agent with SSL
- Web Interface/Presentation Server Communication
- Client Session/Presentation Server Communication
- General Security Considerations

Introduction to Web Interface Security

A comprehensive security plan must include the protection of your data at all points in the application delivery process. This chapter describes Web Interface security risks and recommendations for each of the following communication links:

- **Client device/server running the Web Interface communication**. Explains risks associated with passing Web Interface data between browsers and servers and suggests strategies for protecting data in transit and data written on client devices.
- **Server running the Web Interface/Presentation Server communication**. Describes how to secure the authentication and published application information that passes between the server running the Web Interface and the server farm.
- **Client session/Presentation Server communication**. Explains risks associated with passing client session information between clients and

servers and discusses implementations of the Web Interface and Presentation Server security features that protect such data.



This diagram shows how the client device interacts with the server running Presentation Server and the server running the Web Interface.

Security Protocols and Citrix Security Solutions

This section introduces some of the security protocols and Citrix solutions you can use to secure your Web Interface deployment. It provides introductory information about the SSL and TLS security protocols, Citrix SSL Relay, Secure Gateway, and ICA encryption. It also tells you where to find more information about these technologies.

Secure Sockets Layer (SSL)

The SSL protocol provides the ability to secure data communications across networks. SSL provides server authentication, encryption of the data stream, and message integrity checks.

SSL uses cryptography to encode messages, authenticate their identity, and ensure the integrity of their contents. This guards against risks such as eavesdropping, misrouting, and data manipulation. SSL relies on public key certificates, issued by certificate authorities, to ensure proof of identity.

For more information about SSL, cryptography, and certificates, see the *Citrix Presentation Server Administrator’s Guide*, the *Citrix SSL Relay for UNIX Administrator’s Guide*, and the *Secure Gateway Administrator’s Guide*.

Transport Layer Security (TLS)

TLS is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when they took over responsibility for the development of SSL as an open standard. Like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks.

Support for TLS Version 1.0 is included in MetaFrame Presentation Server, Feature Release 2. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the server certificates you use for SSL in your installation also work for TLS.

Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS is a standard for cryptography.

Note On UNIX platforms, the maximum SSL/TLS certificate key size supported by the Web Interface is 2048 bits.

Citrix SSL Relay

Citrix SSL Relay is a Presentation Server component that uses SSL to secure communication between servers running the Web Interface and server farms. Citrix SSL Relay provides server authentication, data encryption, and message integrity for a TCP/IP connection. The SSL Relay is provided by the Citrix XTE Service.

Citrix SSL Relay operates as an intermediary in the communication between the server running the Web Interface and Citrix XML Service. When using Citrix SSL Relay, the Web server first verifies the identity of the Citrix SSL Relay by checking the relay's server certificate against a list of trusted certificate authorities.

After this authentication, the Web server and Citrix SSL Relay negotiate an encryption method for the session. The Web server then sends all information requests in encrypted form to Citrix SSL Relay. Citrix SSL Relay decrypts the requests and passes them to the Citrix XML Service. When returning the information to the Web server, the server sends all information through the Citrix SSL Relay server, which encrypts the data and forwards it to the Web server for decryption. Message integrity checks verify each communication was not tampered with.

For more information about Citrix SSL Relay, see the *Citrix Presentation Server Administrator's Guide* or the *Citrix SSL Relay for UNIX Administrator's Guide*.

ICA Encryption

Using ICA encryption, you can encrypt the information sent between a server and a client. This makes it difficult for unauthorized users to interpret an encrypted transmission.

Therefore, ICA encryption provides confidentiality to guard against the threat of eavesdropping. However, there are other security risks and using encryption is only one aspect of a comprehensive security policy. Unlike SSL/TLS, ICA encryption does not provide authentication of the server. Therefore information could, in theory, be intercepted as it crosses the network and rerouted to a counterfeit server. Also, ICA encryption does not provide integrity checking.

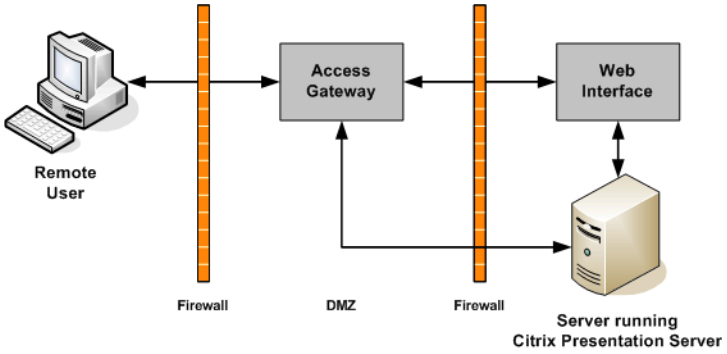
ICA encryption is not available for Presentation Server for UNIX servers.

Access Gateway

You can use the Access Gateway with the Web Interface and Secure Ticket Authority (STA) to provide authentication, authorization, and redirection to published resources hosted on a server running Presentation Server.

The Access Gateway is a universal Secure Socket Layer (SSL) virtual private network (VPN) appliance that provides secure, single point-of access to any information resource – both data and voice. The Access Gateway encrypts and supports all applications and protocols configured.

The Access Gateway provides remote users with seamless, secure access to authorized applications and network resources enabling them to work with files on network drives, email, intranet sites, and applications just as if they are working inside of their organization's firewall.



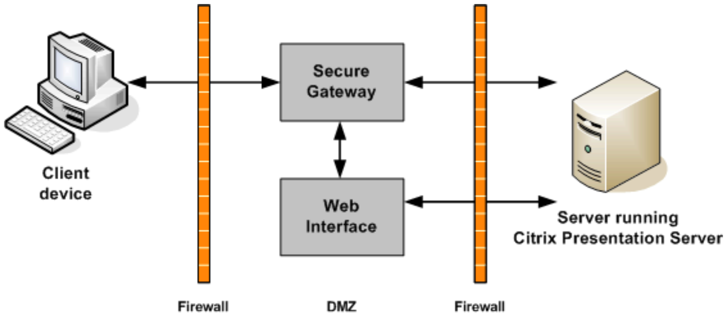
This diagram shows how the Access Gateway secures communication between SSL/TLS-enabled clients and servers.

For more information about the Access Gateway, see the *Access Gateway Administrator's Guide*. For information about how to configure the Web Interface for Access Gateway support using the Access Management Console, see "Editing Gateway Settings" on page 106.

Secure Gateway

You can use the Secure Gateway with the Web Interface to provide a single, secure, encrypted point of access through the Internet to servers on the internal corporate networks.

The Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled clients and servers, encrypting ICA traffic. The Internet portion of traffic between client devices and the Secure Gateway server is encrypted using SSL/TLS. This means that users can access information remotely without compromising security. The Secure Gateway also simplifies certificate management, because you require a certificate only on the Secure Gateway server, rather than on every server in the farm.



This diagram shows how the Secure Gateway secures communication between SSL/TLS-enabled clients and servers.

For more information about the Secure Gateway, see the *Secure Gateway Administrator's Guide*. For information about how to configure the Web Interface for Secure Gateway support using the Access Management Console, see “Editing Gateway Settings” on page 106.

Securing Web Interface Communication

When using the Web Interface, you can put in place the following to secure client-to-server communication:

- Instruct users to connect to Web Interface pages using HTTPS (secure HTTP). Internet Information Services must have an SSL certificate installed to establish a secure HTTP connection.
- Configure Web Interface ticketing to further secure the direct communication between the clients and the servers. A one time ticket is given to the client and the server verifies this ticket upon connection. When

the connection terminates, the ticket is discarded. This ensures that the usernames and passwords are never passed to the client.

- Configure the Web Interface to use Citrix SSL Relay for encryption between the server running the Web Interface and the servers running Presentation Server.

Securing the Program Neighborhood Agent with SSL

To use SSL to secure the communications between the Program Neighborhood Agent and the server running the Web Interface, change the URLs in the following parameters in the config.xml file to use HTTPS. Not all parameters may be specified in your version of the file.

- FolderDisplay/DesktopDisplay/Icon/Location
- ConfigurationFile/Location
- Request/Enumeration/Location
- Request/Resource/Location

To secure the connection between the Program Neighborhood Agent and the Web Interface using SSL, follow the instructions in "Managing Secure Client Access" on page 105 to configure the Web Interface to use SSL. Check the **Enable SSL and TLS Protocols** box on the **Client Options** page of the Application Properties dialog box in the Presentation Server Console.

Example

If the line specifying Request/Resource/Location is <*Location*>http://<SERVER_AND_PATH>/launch.<FILE_FORMAT></*Location*>, change it to <*Location*>https://<SERVER_AND_PATH>/launch.<FILE_FORMAT></*Location*>.

Client Device/Web Interface Communication

Communication between Citrix Presentation Server Clients and the server running the Web Interface consists of passing several different types of data. As users identify themselves, browse applications, and eventually select an application to execute, the Web browser and Web server pass user credentials, application set lists, and session initializing files. Specifically, this network traffic includes:

- **HTML form data**. Web Interface sites use a standard HTML form to transmit user credentials from the Web browser to the Web server at user logon time. The Web Interface form passes the user name and credentials in clear text.

- **HTML pages and session cookies**. After the user enters credentials in the **Login** page, the credentials are stored on the Web server and protected by a session cookie. The HTML pages sent from the Web server to the browser contain application sets. These pages list the applications available to the user.
- **ICA files**. When the user selects an application, the Web server sends an ICA file for that application to the browser. The ICA file contains a ticket that can be used to log on to the server.

Note ICA files do not include a ticket for pass-through or smart card authentication.

Risks

Attackers can exploit Web Interface data as it crosses the network between the Web server and browser and as it is written on the client device itself:

- An attacker can intercept logon data, the session cookie, and HTML pages in transit between the Web server and Web browser.
- Although the session cookie used by the Web Interface is transient and disappears when the user closes the Web browser, an attacker with access to the client device's Web browser can retrieve the cookie and possibly use credential information.
- Although the ICA file does not contain any user credentials, it contains a one-time use ticket that expires in 200 seconds, by default. An attacker may be able to use the intercepted ICA file to connect to the server before the authorized user can use the ticket and make the connection.
- If pass-through is enabled on the client, an attacker could send the user an ICA file that causes the user's credentials to be misrouted to an unauthorized or counterfeit server. This is because the client captures a user's credentials when they logon to the client machine and forwards them to any server if the appropriate setting is contained in the ICA file.

Recommendations

The following recommendations combine industry-standard security practices with Citrix-provided safeguards to protect data traveling between client devices and the Web server and data written to client devices.

Implementing SSL/TLS-Capable Web Servers and Web Browsers

Securing the Web server to the Web browser component of the Web Interface communication begins with implementing secure Web servers and Web browsers. Many secure Web servers rely upon SSL/TLS technology to secure Web traffic.

In a typical Web server to Web browser transaction, the Web browser first verifies the identity of the Web server by checking the Web server's certificate against a list of trusted certificate authorities. After verification, the Web browser encrypts user page requests and then decrypts the documents returned by the Web server. At each end of the transaction, TLS (Transport Layer Security) or Secure Sockets Layer (SSL) message integrity checks ensure that the data was not tampered with in transit.

In a Web Interface deployment, SSL/TLS authentication and encryption create a secure connection over which the user can pass credentials posted in the **Login** page. Data sent from the Web server, including the credentials cookie, ICA files, and HTML application list pages, is equally secure.

To implement SSL/TLS technology on your network, you must have an SSL/TLS-capable Web server and SSL/TLS-capable Web browsers. The use of these products is transparent to the Web Interface. You do not need to configure Web servers or browsers for the Web Interface. For information about configuring the Web server to support SSL/TLS, see the Web server's documentation.

Important Many SSL/TLS-capable Web servers use TCP/IP port 443 for HTTP communications. By default, the Citrix SSL Relay uses this port as well. If your Web server is also a server running the Citrix SSL Relay, make sure you configure either the Web server or Citrix SSL Relay to use a different port.

Do not Enable Pass-Through Authentication

To prevent the possible misrouting of user credentials to an unauthorized or counterfeit server, do not enable pass-through authentication in a secure installation. Use this feature only in a small, trusted environment.

Web Interface/Presentation Server Communication

Communication between the Web Interface and the server running Presentation Server involves the following:

- passing configuration data between the Web Interface and the configuration service (for sites using centralized configuration)
- passing user credential and application set information between the Web Interface and the Citrix XML Service in the server farm

In a typical session, the Web Interface passes credentials to the Citrix XML Service for user authentication and the Citrix XML Service returns application set information. The server and farm use a TCP/IP connection and the Citrix XML protocol to pass the information.

Risks

The Web Interface XML protocol and the configuration service use clear text to exchange all data with the exception of passwords, which pass using obfuscation. Communication is vulnerable to the following attacks:

- An attacker can intercept the XML traffic and steal application set information and tickets. An attacker with the ability to crack the obfuscation can obtain user credentials as well.
- An attacker can impersonate the server and intercept authentication requests.
- An attacker can intercept configuration data that may contain sensitive information.

Recommendations

Citrix recommends implementing one of the following security measures for securing the XML traffic and configuration data sent between the server running the Web Interface and the server farm:

- Use Citrix SSL Relay as a security intermediary between the server running the Web Interface and the server farm. Citrix SSL Relay performs host authentication and data encryption.
- In deployments that do not support running the Citrix SSL Relay, run the server running the Web Interface on the server running Presentation Server.

- Use the HTTPS protocol to send Web Interface data over a secure HTTP connection using SSL if IIS is installed on the server running the Web Interface for another purpose.

Using Citrix SSL Relay

Citrix SSL Relay is a default component of Presentation Server.

On the server side, you must install a server certificate on the Citrix SSL Relay server and verify the Citrix SSL Relay server's configuration. For information about installing a server certificate and configuring the Citrix SSL Relay on servers, see the *Citrix Presentation Server Administrator's Guide*. You can also consult the application help in the Citrix SSL Relay Configuration Tool. For Presentation Server for UNIX servers, see the *Citrix SSL Relay for UNIX Administrator's Guide*.

When configuring the Citrix SSL Relay, make sure the Citrix SSL Relay server permits passing SSL traffic to the servers you are using as the Citrix XML Service contacts. By default, the Citrix SSL Relay forwards traffic only to the server on which it is installed. You can, however, configure the Citrix SSL Relay to forward traffic to other servers. If the Citrix SSL Relay in your deployment is on a machine other than the machine to which you want to send Web Interface data, make sure the Citrix SSL Relay's server list contains the server to which you want to forward Web Interface data.

You can configure the Web Interface to use Citrix SSL Relay using the Access Management Console or the WebInterface.conf file. For information about using the console, see "Managing Server Farms" on page 61.

To configure the Web Interface to use Citrix SSL Relay using WebInterface.conf

1. Open the WebInterface.conf file.
2. Change the **SSLRelayPort** setting in the **Farm*n*** parameter to the port number of the Citrix SSL Relay on the server.
3. Change the value of the **Transport** setting in the **Farm*n*** parameter to **SSL**.

Adding Certificates to the Server Running the Web Interface

On UNIX, the Web Interface includes native support for the following certificate authorities:

- VeriSign, Inc., http://www.verisign.com/
- Baltimore Technologies, http://www.baltimore.com/

If you want to add support for other certificate authorities, you must add the certificate authority's root certificate to the server running the Web Interface.

To add a new root certificate to the server running the Web Interface

Copy the root certificate to your Web server.

- On Windows, the certificate is copied using the Certificate Microsoft Management Console (MMC) Snap-In.
- On UNIX, copy the certificate to the ./cacerts directory.

For information about certificates, see the installation chapter of the *Citrix Presentation Server Administrator's Guide*. For Presentation Server for UNIX servers, see the *Citrix SSL Relay for UNIX Administrator's Guide*.

Enabling the Web Interface on the Server Running Presentation Server

For those deployments that do not support the Citrix SSL Relay, you can eliminate the possibility of network attack by running a Web server on the server supplying the Web Interface data. Hosting your Web Interface sites on such a Web server routes all Web Interface requests to the Citrix XML Service and configuration service on the local host, thereby eliminating transmission of the Web Interface data across the network.

However, the benefit of eliminating network transmission must be weighed against the risk of exploitation of the Web server.

Note On Presentation Server systems, Setup lets you force the Citrix XML Service to share Internet Information Services's TCP/IP port instead of using a dedicated port. If you enable port sharing, the Citrix XML Service and the Web server use the same port by default.

At minimum, you can place both the Web server and the server running Presentation Server behind a firewall so that the communication between the two is not exposed to open Internet conditions. In this scenario, client devices must be able to communicate through the firewall to both the Web server and the server running Presentation Server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for client device to Web server communication. For client to server communication, the firewall must permit inbound ICA traffic on port 1494 and port 2598. See the server documentation for information about using ICA with network firewalls.

For information about using the Web Interface with network address translation, see the *Customizing the Web Interface* guide.

Using the HTTPS Protocol

You can use the HTTPS protocol to secure the Web Interface data passing between the Web server and the server running Presentation Server. HTTPS uses SSL/TLS to provide strong encryption of data.

The Web server makes an HTTPS connection to IIS running on the server running Presentation Server. This requires IIS port sharing at the server running Presentation Server, and for IIS running on the server running Presentation Server to have SSL enabled. The server name you specify (using the console, or in the **Farm** parameter in WebInterface.conf) must be a fully-qualified DNS name that matches the name of the IIS SSL server certificate. The Citrix XML Service is reached at https://*servername*/scripts/wpnbr.dll.

For information about how to configure the Web Interface to use the HTTPS protocol using the Access Management Console, see "Managing Secure Client Access" on page 105.

To configure the Web Interface to use HTTPS using the WebInterface.conf file

1. Open the WebInterface.conf file.
2. Change the value of the **Transport setting** in the **Farm*n*** parameter to **HTTPS**.

Client Session/Presentation Server Communication

The Web Interface communication between client devices and servers consists of passing several different types of client session data including initialization requests and client session information.

- **Initialization requests**. The first step in establishing a client session, called *initialization*, requires the client to request a client session and produce a list of session configuration parameters. These parameters control various aspects of the client session such as which user to log on, the size of the window to draw, and the program to execute in the session.
- **Client session information**. After client session initialization, information is passed between client and server through a number of virtual channels. For example, mouse input (from client to server) and graphical updates (from server to client).

Risks

To capture and interpret client to server network communications, an attacker must be able to crack the binary client protocol. An attacker with binary client protocol knowledge can:

- Intercept initialization request information sent from the client, including user credentials
- Intercept client session information including text and mouse clicks entered by users and screen updates sent from the server

Recommendations

Use SSL/TLS or ICA Encryption

Citrix recommends implementing SSL/TLS or ICA encryption to secure the traffic between your clients and servers. Both methods support 128-bit encryption of the data stream between the client and server, but SSL/TLS also supports verification of the identity of the server.

Support for SSL is included in Feature Release 1 for MetaFrame XP and higher, and Feature Release 1 for MetaFrame for UNIX and higher.

Support for SSL/TLS is included in Feature Release 2 for MetaFrame XP and higher.

Support for ICA encryption is included in Feature Release 1 for MetaFrame 1.8 and MetaFrame Presentation Server and higher.

See the client documentation or the Citrix download site for a list of clients that support each method. See the *Citrix Presentation Server Administrator's Guide* for more information about ICA encryption.

Use Secure Gateway

You can use the Secure Gateway to secure the traffic between your clients and servers over the Internet. The Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled clients and servers.

For more information about the Secure Gateway, see the *Secure Gateway Administrator's Guide*. For information about how to configure the Web Interface for Secure Gateway support using the Access Management Console, see “Configuring Secure Gateway Support” on page 154.

Controlling Diagnostic Logging

Use the **Control diagnostic logging** task to increase system security for error logging. You can suppress duplicate events from being logged repeatedly, and configure how many duplicate events will be logged and how often.

You can also use this task to specify the URL for error redirection. If you specify a customized error callback URL, you must handle all the error IDs with this URL and provide error messages to your users. In addition, this error callback URL will replace the user's **Log off** page, even when users are logged off successfully without any error.

General Security Considerations

You should also be aware of the following general security considerations when configuring your servers.

Ensuring Your Server is Configured Correctly

Citrix recommends that, as with any Windows-based server, you follow Microsoft standard guidelines for configuring the Windows server.

Always ensure that all components are up-to-date with all the latest patches. For details and to check for the latest download recommendations, see Microsoft's Web site at http://support.microsoft.com/.

Changing the Welcome Message

You may want to amend the default “Welcome” text displayed on the Web Interface Login Page. You can amend this text by editing the common_strings.properties file.

To change the default “Welcome” message

1. Open the common_strings.properties file. By default, this file is located in C:\Program Files\Citrix\Web Interface\4.5\languages.
2. Change the following line:

   ```
   Welcome=Welcome
   ```

   to

   ```
   Welcome=<customized text>
   ```

   Important Enter a space after the “=” character if you do not want to display customized “Welcome” text on the Login page.

3. Save the common_strings.properties file.
4. Repeat the same procedure for the following files:

   common_string_de.properties

   common_string_es.properties

   common_string_fr.properties

   common_string_ja.properties

5. Restart your Web server to apply the changes.

Configuring Sites Using the Configuration File

Locally configured sites include a configuration file, called WebInterface.conf, that contains a site's configuration data. You can use this file to perform day to day administration tasks and customize other settings for a site. For example, you can use WebInterface.conf to specify the settings that users can adjust on the **Settings** page or configure user authentication to the Web Interface.

Centrally configured sites store this data on the server running the Citrix XML Service. You can, however, export this data into a file using the **Export Configuration** task and edit the file manually.

Note If you enter an invalid value for a setting when you edit a configuration file, the Web Interface replaces the invalid value with the default value when the file is saved (for local configured sites) or imported (for centrally configured files).

The WebInterface.conf file is available on all platforms in the site configuration directory:

- On Windows this is typically found in C:\Inetpub\wwwroot\Citrix\AccessPlatform\conf
- On UNIX systems, this may be /usr/local/tomcat/webapps/Citrix/AccessPlatform/WEB-INF.

You can override some values in WebInterface.conf on a per-page basis in your Web server scripts. For more information about Web server scripts, see the *Customizing the Web Interface* guide.

Important For changes made to WebInterface.conf to take effect on UNIX platforms, you must stop and restart the server running the Web Interface. Additionally, ensure that you save your changes with UTF-8 encoding.

WebInterface.conf Parameters

The following table shows the parameters that WebInterface.conf can contain (in alphabetical order), Default values are shown in **bold** text. If a parameter is not specified in WebInterface.conf, its default value is used.

Parameter	Description	Values	Site Types
AccountSelfService URL	Specifies the URL for the Password Manager Service.	A valid URL using HTTPS.	Access Platform
AdditionalExplicit Authentication	Defines the explicit two-factor authentication that must be carried out, in addition to SAM, ADS or NDS. This replaces the deprecated setting of EnableSecurIDWithExplicit Authentication.	**None** | SecurID | SafeWord | RADIUS	Access Platform
AddressResolution Type	Specifies what type of address to use in the ICA launch file.	**Ipv4-port** | ipv4 | dns | dns-port	Access Platform Program Neighborhood Agent Services Conferencing Manager
AGEPromptPassword	Specifies whether or not a user is prompted to re-enter their password when logging in from the Advanced Access Control Login page.	**Off** | On	Access Platform
AGEWebServiceURL	The URL for the Advanced Access Control Authentication Service.	A valid URL	Access Platform
AllowBandwidth Selection	Specifies whether or not users can provide Presentation Server with the type of connection between their Web browser and Presentation Server, to optimize ICA settings.	**Off** | On	Access Platform
AllowCustomizeApp Columns	Specifies whether or not to allow users to specify the number of columns.	**On** | Off	Access Platform
AllowCustomize ApplicationAccess Method	Specifies whether or not the user can choose between remote and streaming as their preferred way of accessing applications.	**Off** | On	Access Platform
AllowCustomize Audio	Specifies whether or not the user is permitted to adjust the audio quality for ICA sessions.	**Off** | On	Access Platform

Parameter	Description	Values	Site Types
AllowCustomizeClientPrinterMapping	Specifies whether or not to allow users to enable/disable client printer mapping.	**Off** | On	Access Platform
AllowCustomizeClients	Specifies whether or not the user is permitted to change which client is used to launch the application.	**Off** | On	Access Platform Conferencing Manager
AllowCustomizeJavaClientPackages	Specifies whether or not the user is permitted to change the Client for Java packages that are downloaded.	**Off** | On	Access Platform
AllowCustomizeLayout	Specifies whether or not to allow users to choose which user interface to use.	**Off** | On	Access Platform
AllowCustomizeLogoff	Specifies whether or not users can override the behavior displayed by the workspace control feature when the user logs off from Presentation Server.	**On** | Off	Access Platform
AllowCustomizeReconnectAtLogin	Specifies whether or not the Presentation Server user is able to override the behavior of workspace control at logon.	**On** | Off	Access Platform
AllowCustomizeReconnectButton	Specifies whether or not the Presentation Server user is able to override the behavior of workspace control when **Reconnect** is clicked.	**On** | Off	Access Platform
AllowCustomizeSettings	Specifies whether or not the user can customize their Web Interface sessions.	**On** | Off	Access Platform
AllowCustomizeTransparentKeyPassthrough	Specifies whether or not to allow users to select the key combination pass-through behavior.	**Off** | On	Access Platform
AllowCustomizeVirtualCOMPortEmulation	Specifies whether or not to allow users to enable/disable PDA synchronization.	**On** | Off	Access Platform
AllowCustomizeWinColor	Specifies whether or not the user is permitted to change the color depth for ICA sessions.	**Off** | On	Access Platform
AllowCustomizeWinSize	Specifies whether or not the user is allowed to change the window size for ICA sessions.	**On** | Off	Access Platform

Parameter	Description	Values	Site Types
AllowUserAccountUnlock	Specifies whether or not a user can unlock their account using Account Self Service.	**Off** | On	Access Platform
AllowUserPasswordChange	Defines under what conditions users can change their password.	**Never** | Expired-Only | Always	Access Platform
AllowUserPasswordReset	Specifies whether or not a user can reset their password using Account Self Service.	**Off** | On	Access Platform
AlternateAddress	Specifies whether or not to return the alternate server address in the ICA file.	**Off** | Mapped | On	Access Platform Conferencing Manager
AppColumns	The number of columns of application icons in the Application screen.	Integer 1 - 300 (**3**)	Access Platform
ApplicationAccessMethods	Specifies whether users can access applications using the remote client, streaming client, or both.	**Remote**, Streaming	Access Platform Program Neighborhood Agent Services
AuthenticationMethods	Defines the permitted logon methods. This is a comma separated list and can contain any of the specified values in any order.	**Explicit**, Anonymous, CertificateSingleSignOn, Certificate, SingleSignOn | AGEPassthrough | Federated	Access Platform Program Neighborhood Agent Services
AutoDeployWebClient	Specifies whether or not the full native client should be downloaded to users with no client, or one that is out of date.	**Off** | On	Access Platform
AutoDeployWebClientPackage	Filename of the client auto-deployed to users when AutoDeployWebClient is set to On.	Filename of the full native client package	Access Platform
AutoFallbackToJavaClient	Specifies whether or not to use the Client for Java to launch applications if no native client is detected on Win32 platforms.	**Off** | On	Access Platform Conferencing Manager
BrandingColor	Specifies the color for the lines and bars in the header and footer areas.	Hex color number or color name	Access Platform Conferencing Manager
BypassFailedRadiusServerDuration	Time before a failed RADIUS server is considered for reuse.	A number in minutes(**60**)	Access Platform

Parameter	Description	Values	Site Types
BypassFailedSTA Duration	Time before a failed STA server is considered for reuse.	A number in minutes (**60**)	Access Platform Program Neighborhood Agent Services Conferencing Manager
ClientAddressMap	Part of the server side firewall configuration. A list of client address, address type pairings. The first can be a partial address, or a subnet address and mask, while the latter takes the values: Normal, Alternate, Translated, SG, SGAlternate, and SGTranslated. Using an asterisk (*) in place of a client address or subnet indicates the default for all otherwise unspecified clients.	<Subnet Address>/ <Subnet Mask> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …	Access Platform Conferencing Manager
ClientProxy	Client side firewall option. Specifies a list of client subnet addresses and masks and associated proxy settings. The client address in the returned ICA file is determined by these settings. Each entry comprises of three fields. The first can be a subnet address and mask. Using an asterisk (*) indicated the default for all otherwise unspecified clients. The second is one of six proxy types. The value of the third field (proxy address) in each set of three is ignored unless the second field (proxy type) is an explicit proxy type (SOCKS or Secure), but it must always be present; the default value for this field is the minus sign (-).	<ClientAddress>| <Subnet Address>/ <Subnet Mask> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <ProxyAddress> | <ProxyAddress>: <ProxyPort>, …	Access Platform Conferencing Manager
CompanyHomePage	A URL to be used as the hyperlink for the company logo if **CompanyLogo** is specified.	A valid URL	Access Platform Conferencing Manager
CompanyLogo	A URL to the company logo image.	A valid URL	Access Platform Conferencing Manager
CredentialFormat	Specifies the credential formats accepted for explicit Windows and NIS logins.	**All** | UPN | DomainUsername	Access Platform Program Neighborhood Agent Services

Parameter	Description	Values	Site Types
CSG_EnableSession Reliability	Specifies whether or not to use session reliability through the Secure Gateway or Access Gateway.	**Off** | On	Access Platform Conferencing Manager
CSG_Server	Specifies the address of the Secure Gateway or Access Gateway.	**None**. Server address as a FQDN	Access Platform Conferencing Manager
CSG_ServerPort	Specifies the port of the Secure Gateway or Access Gateway.	**None**. Server port	Access Platform Conferencing Manager
CSG_STA_URL<n>	Server providing the Secure Ticket Authority function.	**None**. A URL to an STA	Access Platform Conferencing Manager
DefaultApplication AccessMethod	Specifies whether the remote or streaming client is used to access applications by default.	**Remote**| Streaming	Access Platform
DefaultClient	Specifies whether or not to show all clients available for download when platform cannot be auto detected. Only relevant if install captions are to be shown.	**On** | Off	Access Platform Conferencing Manager
DefaultCustomText Locale	The default locale to use for customized text. This must be the same locale specified for <*lang_code*> in the WelcomeMessage <*lang_code*> and FooterText <*lang_code*> settings.	**None**. en | fr | de | es | ja | any other supported language identifier	Access Platform Conferencing Manager
DisplayFooter	Specifies whether or not to display the footer defined in footer.inc.	**On** | Off	Access Platform Conferencing Manager
DisplayHeader	Specifies whether or not to display the header defined in header.inc.	**On** | Off	Access Platform Conferencing Manager
DisplayMainBoxTitle BarBgImage	Specifies whether or not to use background image or simple background color for the main box title bar.	**On** | Off	Access Platform Conferencing Manager
DisplaySiteLogo	Specifies whether or not the site identifier logo is displayed	**On** | Off	Access Platform Conferencing Manager
DomainSelection	Specifies the domain names listed on the Login page for explicit authentication.	List of NetBios domain names.	Access Platform

Parameter	Description	Values	Site Types
DuplicateLogInterval	Specifies the time period over which **DuplicateLogLimit** log entries will be monitored.	A number in seconds (**60**)	Access Platform Program Neighborhood Agent Services Conferencing Manager
DuplicateLogLimit	Specifies the number of duplicate log entries allowed in the time period **DuplicateLogInterval**.	Integer greater than 0 (**10**)	Access Platform Program Neighborhood Agent Services Conferencing Manager
EnableFileType Association	Specifies whether or not file type association is enabled or disabled for a site. If this is Off, content redirection is not available for the site.	**On** | Off	Program Neighborhood Agent Services
EnableKerberosTo MPS	Specifies whether or not to enable Kerberos authentication.	**Off** | On	Access Platform
EnableLegacyICA ClientSupport	Specifies whether or not older Citrix Presentation Server Clients that cannot read UTF-8 ICA files are supported. If this is Off, Presentation Server will produce ICA files in UTF-8 encoding.	**On** | Off	Access Platform Program Neighborhood Agent Services Conferencing Manager
EnableLogoff Applications	Specifies whether or not the workspace control feature should logoff Active applications when the user logs off from Presentation Server.	**On** | Off	Access Platform
EnablePassthrough URLs	Specifies whether or not users can create persistent links to published applications accessed using the Web Interface.	**Off** | On	Access Platform
EnableRadiusServer LoadBalancing	Turn this on to permit sessions on multiple RADIUS servers to be load balanced in a random-access manner. Failover between the servers still occurs regardless of whether this is On or Off.	**On** | Off	Access Platform

Parameter	Description	Values	Site Types
EnableSTALoad Balancing	Turn this on to permit requests to multiple Secure Gateway STA servers to be load balanced.	**On** | Off	Access Platform Program Neighborhood Agent Services Conferencing Manager
EnableVirtualCOM PortEmulation	Specifies whether or not to enable PDA synchronization through tethered USB connection.	**Off** | On	Access Platform
EnableWorkspace Control	Specifies whether or not the workspace control feature is available to Presentation Server users.	**On** | Off	Access Platform
ErrorCallbackURL	Specifies a URL for Web Interface to redirect to when an error occurs. It takes four query string parameters: NFuse_MessageType NFuse_MessageKey NFuse_MessageArgs NFuse_LogEventID	A valid URL	Access Platform
Farm<n>	Specifies all the information for a farm.	XML service address [,XML service address,...] [,Name:<name>] [,XMLPort:<port>] [,Transport:<HTTP | HTTPS | SSL>] [,SSLRelayPort: <port>] [,BypassDuration: <duration>] [,LoadBalance: <on | off>] [,ECSUrlURL>] [,TicketTimeToLive: <seconds (200)>] [,RADETicketTime ToLive:<seconds (200)>]	Access Platform Program Neighborhood Agent Services Conferencing Manager
FooterText_<lang-code>	Localized footer text to be displayed in the footer area of all screens. *lang-code* is en, fr, de, es, ja or any other standard language code.	**None**. Plain text plus any number of new line HTML tags.	Access Platform Conferencing Manager

Parameter	Description	Values	Site Types
HeadingImage	A URL to the image to be displayed as the heading of Web Interface.	A valid URL	Access Platform Conferencing Manager
HideDomainField	Controls whether the domain field is displayed on the Login screen.	**Off** | On	Access Platform
HpUxUnixClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
IbmAixClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
ICAWebClient	File name of the Web Client.	**ica32pkg.msi**	Access Platform Conferencing Manager
IcaWebClientClassID	Class ID of the ActiveX client.	**238f6f83-b8b4-11cf-8771-00a024541ee3**	Access Platform Conferencing Manager
ICAWebClientVersion	Version number of client (from the Client CD-ROM). Used with **AutoDeployWebClient**.	The latest client version	Access Platform Conferencing Manager
IgnoreClientProvided ClientAddress	Ignore the client-provided client address when set.	**Off** | On	Access Platform Program Neighborhood Agent Services Conferencing Manager
InternalServer AddressMap	A list of normal, translated address pairings. The normal address identifies the Secure Gateway server address and the translated address is that which should be returned to the Citrix Presentation Server Client.	NormalAddress = TranslatedAddress, …	Access Platform Program Neighborhood Agent Services Conferencing Manager
JavaClientPackages	The default set of Client for Java packages to download. Consists of a comma-separated list in arbitrary order.	**ConfigUI**, **PrinterMapping**, **SecureICA**, Audio, ClientDriveMapping, ClipBoard, SSL, Thinwire1, ZeroLatency	Access Platform Conferencing Manager

Parameter	Description	Values	Site Types
JavaClientRoot Certificate	The file name of a private root certificate for the Client for Java. The certificate must be located in the same directory as the Client for Java packages.	**None**. A valid filename	Access Platform Conferencing Manager
KioskMode	Controls whether or not user settings should be persistent or last only for the lifetime of the session. When kiosk mode is enabled, user settings will not persist from one session to another.	**Off** | On	Access Platform Conferencing Manager
LaunchClients	Defines from which clients the user is allowed to select. Used in conjunction with **AllowCustomizeClients**.	**Ica-Local**, **Ica-Java**, **Ica-Embedded**, Rdp-Embedded	Access Platform Conferencing Manager
LaunchMethod	Preferred client to use for launches.	**Ica-Local** | Ica-Java |On | Off | Ica-Embedded | Rdp-Embedded	Access Platform Conferencing Manager
LinuxClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
LoginDomains	Specifies the domain names used for access restriction.	List of NetBIOS domain names	Access Platform Program Neighborhood Agent Services
LoginType	Specifies which Login screen is displayed. May be either domain-based, or NDS.	**Default** | NDS	Access Platform Program Neighborhood Agent Services
LogoffFederation Service	Specifies whether or not to log a user out of an Access Platform site only or globally from the ADFS when a user clicks on the Logoff button of an ADFS integrated site.	**On** | Off	Access Platform
MacClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
MainBoxTitleBarBg Color	Specifies the background color for the main box title bar.	Hex color number or color name	Access Platform Conferencing Manager
MainBoxTitleBarBg Image	Specifies a URL to the background image for the main box title bar.	A valid URL.	Access Platform Conferencing Manager

Parameter	Description	Values	Site Types
MainBoxTitleFont Color	Font color for the main box title bar.	Hex color number or color name	Access Platform Conferencing Manager
MessageHeadingBg Color	Background color for the headings of the welcome area and the message center.	Hex color number or color name	Access Platform Conferencing Manager
MessageHeadingFont Color	Font color for the headings of the welcome area and the message center.	Hex color number or color name	Access Platform Conferencing Manager
NDSContextLookup Loadbalancing	Specifies whether or not to load balance the configured LDAP servers.	**On** | Off	Access Platform Program Neighborhood Agent Services
NDSContextLookup Servers	Specifies the LDAP servers to use. If the port is not specified, it is inferred from the protocol: ldap for the default LDAP port (389), or ldaps for the default LDAP over SSL port (636). A maximum of 512 servers is supported. If this parameter is empty or not present, the contextless logon functionality is disabled.	**None**. ldap://[:] | ldaps://[:], ...	Access Platform Program Neighborhood Agent Services
NDSTreeName	When using NDS authentication, this specifies the NDS tree to use.	**None**. NDS tree	Access Platform Program Neighborhood Agent Services
OtherClient	Specifies download caption and links for unrecognized client platforms.	"**Default**". Caption and links	Access Platform Conferencing Manager
OverlayAutologon CredsWithTicket	Specifies that a logon ticket must be duplicated in a logon ticket entry or placed in a separate ICA launch file ticket entry.	**On** | Off	Access Platform
OverrideClientInstall Caption	Specifies a custom message to be displayed along with the download links for the clients.	**None**. Custom message text	Access Platform Conferencing Manager
OverrideIca Clientname	Specifies whether or not a Web Interface generated ID must be passed in the clientname entry of an ICA launch file	**On** | Off	Access Platform

Parameter	Description	Values	Site Types
PasswordExpiry Warning Period	Specifies the number of days before password expiry that a user is prompted to change their password	Integer between 0 and 999 (**14**)	Access Platform
PooledSockets	Specifies whether or not to use socket pooling.	**Off** | On	Access Platform Program Neighborhood Agent Services Conferencing Manager
RADEClientClassID	ClassID of Citrix Streaming client		Access Platform
RadiusRequest Timeout	Specifies the time-out value to use when waiting for a response from the session's RADIUS server.	Time-out in seconds (30)	Access Platform
RadiusServers	A comma-separated list of RADIUS servers and optionally the ports on which they listen. Servers can be specified using IPs or names, and the server and port for each element are separated using a colon. If the port is omitted, Presentation Server assumes the RADIUS default of 1812. A maximum of 512 RADIUS servers can be configured.	server[:port][,…]	Access Platform
RdpWebClient	Filename of the Remote Desktop Connection software used for embedded launches and auto-deployment of this client.	**msrdp.cab**	Access Platform Conferencing Manager
RdpWebClientClassID	Class ID of the Remote Desktop Connection ActiveX client shipped with Windows Server 2003.	**7584c670-2274-4efb-b00b-d6aaba6d3850**	Access Platform Conferencing Manager
RDPWebClient Version	Version number of the Remote Desktop Connection software shipped with Windows Server 2003.	**5,2,3790,0**	Access Platform Conferencing Manager
ReconnectAtLogin	Specifies whether or not workspace control should reconnect to applications at logon, and if so, whether to reconnect all applications, or disconnected applications only.	**DisconnectedAnd Active** | Disconnected | None	Access Platform

Parameter	Description	Values	Site Types
ReconnectButton	Specifies whether or not workspace control should reconnect to applications when Presentation Server users click **Reconnect**, and if so, whether to reconnect to all applications, or disconnected applications only.	**DisconnectedAnd Active** | Disconnected | None	Access Platform
RequestICAClient SecureChannel	Controls TLS settings.	**Detect-AnyCiphers**, TLS-GovCiphers, SSL-AnyCiphers	Access Platform Program Neighborhood Agent Services Conferencing Manager
RestrictDomains	Specifies whether or not the **LoginDomains** setting is used to restrict user access.	**Off** | On	Access Platform Program Neighborhood Agent Services
RetryCount	The number of times a failed request to the XML Service is retried before the service is deemed to have failed.	Integer greater than 0 (**5**)	Access Platform Program Neighborhood Agent Services Conferencing Manager
ScoUnixClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
SearchContextList	An optional comma-separated list of context names for use with NDS authentication.	**None**. Comma delimited list of context names	Access Platform
ServerAddressMap	Part of server side firewall support. A list of normal, translated address pairings. The normal address identifies the server address and the translated address is returned to the client.	NormalAddress, TranslatedAddress, …	Access Platform Conferencing Manager
SgiUnixClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
ShowClientInstall Caption	Controls the display of download captions. Auto specifies that the download caption is shown if the user does not have a client installed and automatic Web installation is disabled. On other platforms, the caption is always shown.	**Auto** | Off | On	Access Platform Conferencing Manager

Parameter	Description	Values	Site Types
ShowPasswordExpiry Warning	Controls whether or not users are prompted to change their password before it expires and determines what the warning period should be.	**Never** | WindowsPolicy | Custom	Access Platform
SolarisUnixClient	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
Timeout	Specifies the time-out value to use when communicating with the XML service.	Time-out in seconds (**60**)	Access Platform Program Neighborhood Agent Services Conferencing Manager
TransparentKey Passthrough	Specify the mode of Windows key combinations pass-through.	Local | Remote | **FullScreenOnly**	Access Platform Conferencing Manager
Tru64Client	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
TwoFactorPassword Integration	Specify whether or not to enable password integration with RSA SecurID 6 or later.	**Off** | On	Access Platform
TwoFactorUseFully QualifiedUserNames	Specify whether or not to pass fully qualified usernames to the authentication server during two-factor authentication.	**Off** | On	Access Platform
UPNSuffixes	Restrict UPN authentication to these suffixes for explicit authentication.	List of UPN suffixes	Access Platform Program Neighborhood Agent Services
UserInterfaceLayout	Specifies whether or not to use the compact user interface.	**Auto** | Normal | Compact	Access Platform Conferencing Manager
WebSessionTimeout	Specifies the time-out value for for idle browser sessions.	Time-out in minutes (**25**)	Access Platform Conferencing Manager

Parameter	Description	Values	Site Types
WelcomeMessage_<lang-code>	Localized welcome message text to be displayed in the welcome area of the Login screen and Application List screen. *lang-code* is en, fr, de, es, ja or any other standard language code.	**None**. HTML formatted text.	Access Platform Conferencing Manager
Win16Client	Specifies download caption and links for the associated platform.	"**Default**". Caption and links	Access Platform Conferencing Manager
Win32Client	Specifies download caption and links for the associated platform. If the value is set to default, the default Citrix Presentation Server Client links for this platform are displayed in the Message Center of the Web Interface Login page. The links are to the Web Client typically located at C:\\Program Files\Citrix\Web Interface\4.5\Clients\ica 32. Captions and links can be customized using the format: caption1&url,caption2&url2, …, and so on, where caption is the display text and url is the URL for the client. The caption is shown in the Message Center of the Web Interface Login page as a hyperlink to the specified URL.	"**Default**". Caption and links	Access Platform Conferencing Manager

Program Neighborhood Agent Considerations

Specific WebInterface.conf parameter settings affect the validation of Program Neighborhood Agent requests. Citrix recommends that the settings in WebInterface.conf be consistent with settings in the config.xml file in the Program Neighborhood Agent.

Contents of the config.xml File

The config.xml file contains a number of parameters divided into a number of different categories. You can edit parameters in the following categories:

- **FolderDisplay**. Specifies where to display application icons: in the Start menu, on the Windows desktop, or in the notification area. There are also additional parameters to specify a particular folder in the Start menu and the icon to use on the Windows desktop. This corresponds to the options on the **Application Display** tab of the **PN Agent Properties** dialog box.

- **DesktopIntegration**. Specifies whether or not to add shortcuts to the Start menu, desktop, or notification area.
- **ConfigurationFile**. Allows you to specify a different URL for config.xml for the client to use in the future. This facilitates moving users to a different server running the Web Interface.
- **Request**. Specifies where the client should request published application data from, and how often to refresh the information.
- **Failover**. Specifies a list of backup server URLs to contact if the primary server is unavailable.
- **Logon**. Specifies the logon method to use.
- **UserInterface**. Specifies whether to hide or display certain groups of options presented to the user as part of the Program Neighborhood Agent interface.
- **ReconnectOptions**. Specifies whether or not workspace control functionality is available to users.
- **FileCleanup**. Specifies whether or not shortcuts are deleted when a user logs off from Program Neighborhood Agent.
- **ICA_Options**. Specifies the display and sound options for client connections. This corresponds to the settings on the **Session Options** tab of the **Program Neighborhood Agent Properties** dialog box.
- **AppAccess**. Specifies the types of applications available to users.

For more information about using the config.xml file, see the *Clients for Windows Administrator's Guide.*

Settings in the WebInterface.conf file

The following table contains the parameters in WebInterface.conf that must be consistent with those in the config.xml file. It also explains the values that affect the Program Neighborhood Agent settings and their recommended settings:

Parameter	Recommended Setting
AuthenticationMethods	Use the same authentication method configured in the WebInterface. conf file. Authentication will fail if this method differs in config.xml.
LoginType	NDS must be enabled in config.xml.
NDSTreeName	DefaultTree in the Logon section of config.xml must contain the same setting.

To configure the Web Interface when using the Program Neighborhood Agent

1. Open the WebInterface.conf file.
2. Locate the following parameters:
   - AuthenticationMethods
   - LoginType
   - NDSTreeName
3. Amend the settings for these parameters as described in the table above.
4. Restart the server running the Web Interface to apply the changes.

For more information about WebInterface.conf file settings, see “Configuring Sites Using the Configuration File” on page 137.

Examples

This section provides typical examples of how to configure the Web Interface using the WebInterface.conf file.

Configuring Communication with Presentation Server

In this example, you want to specify the name of an additional server running the Citrix XML Service. The Citrix XML Service acts as a communication link between the server farm and the server running the Web Interface.

Communication is currently with a server called "marx" but you want to add a server called "engels" in case marx fails. To do this:

1. Locate the following line in WebInterface.conf:

   ```
   Farm1=marx,Name:Farm1,XMLPort:80,Transport:HTTP,
   SSLRelayPort:443,…
   ```

2. Edit this line to include the additional server, as follows:

   ```
   Farm1=marx,engels,Name:Farm1,XMLPort:80,Transport:HTTP,
   SSLRelayPort:443,…
   ```

Configuring Citrix SSL Relay Communication

In this example, you want to secure communication between the Web server and the server running Presentation Server, using Secure Sockets Layer (SSL). Citrix SSL Relay is installed on the server running Presentation Server that has a FQDN of marx.company-name.com. Citrix SSL Relay listens for connections on TCP port 443.

Communication is currently with the server marx but you want to replace marx with www.hegel.company-name.com. To do this:

1. Open WebInterface.conf and locate the following line:

   ```
   Farm1=marx,Name:Farm1,XMLPort:80,Transport:HTTP,
   SSLRelayPort:443
   ```

2. Change the Transport to SSL, as follows:

   ```
   Farm1=marx.company-name.com,Name:Farm1,XMLPort:80,
   Transport:SSL,SSLRelayPort:443
   ```

Note The server name specified must match the name on the server's certificate.

Configuring Secure Gateway Support

In this example, you want to specify a Secure Gateway server called "csg1.citrix.com" on which Citrix Presentation Server Clients use port 443, using the following two Secure Ticket Authority addresses:

- http://server1.citrix.com/scripts/CtxSta.dll
- http://server2.citrix.com/scripts/CtxSta.dll

Include the following lines in WebInterface.conf:

```
CSG_STA_URL1=http://server1.citrix.com/scripts/CtxSta.dll

CSG_STA_URL2=http://server2.citrix.com/scripts/CtxSta.dll
```

```
CSG_Server=csg1.citrix.com

CSG_ServerPort=443

ClientAddressMap=*,CSG
```
(to enable the Secure Gateway for all users)

Settings in bootstrap.conf

The following table lists the settings found in the bootstrap.conf file.

Parameter	Description	Values	Site Types
Configuration Location	Specifies from where Web Interface should load the configuration.	Path to configuration file within the web app | [ConfigSvrDef] ConfigSvrDef = ConfigSvr [;ConfigSvr]* [,Port:<port>] [,Transport:<HTTP|HTTPS|SSL>] [,SSLRelayPort:<port>] where ConfigSvr is either the DNS name or an IP address of the Configuration Proxy	Access Platform Program Neighborhood Agent Services Conferencing Manager
ConfigurationSource Type	Which type of configuration is used by the site.	**Local** | ConfigurationService	Access Platform Program Neighborhood Agent Services Conferencing Manager
DefaultLocale	The default language to be used if a browser requests a non-supported language.	**en** | fr | de | es | ja | any other supported language identifier	Access Platform Program Neighborhood Agent Services Conferencing Manager
SiteIDRoot	A string that provides the basis of a unique site identifier. For windows the **SiteIDRoot** is used directly as the site identifier when communicating with the configuration service. For UNIX, runtime information is added to the **SiteIDRoot** to form the site identifier for the configuration service.	This is a random number generated by the installer	Access Platform Program Neighborhood Agent Services Conferencing Manager

Configuring ADFS Support for the Web Interface

Overview

ADFS support for the Web Interface enables the resource partner of an ADFS deployment to use Presentation Server. Administrators can create ADFS sites to provide users with access to published applications on the resource partner.

Important ADFS requires secure communications between client, Web server, and federation servers. Web Interface users must use **HTTPS/SSL** to access the site.

What is ADFS?

Active Directory Federation Services (ADFS) is a feature of Microsoft Windows Server 2003 R2 Enterprise Edition. ADFS provides single-sign on technology to authenticate a user into multiple Web applications in a single session.

ADFS extends the existing Active Directory infrastructures to provide access to resources offered by trusted partners across the Internet. These trusted partners can include external third parties or other departments in your organization.

For two organizations to establish ADFS trust relationships, ADFS must be deployed in both organizations. ADFS trust relationships are explicit, one-way, and nontransitive. In a trust relationship, the party hosting the user accounts is the account partner and the party hosting the applications accessed by users is the resource partner.

Using ADFS requires a federation server on each partner. For additional security, you can locate these federation servers inside the trusted network of each organization and deploy federation server proxies. A federation server proxy relays federation requests from outside the organization to your federation server.

ADFS Terminology

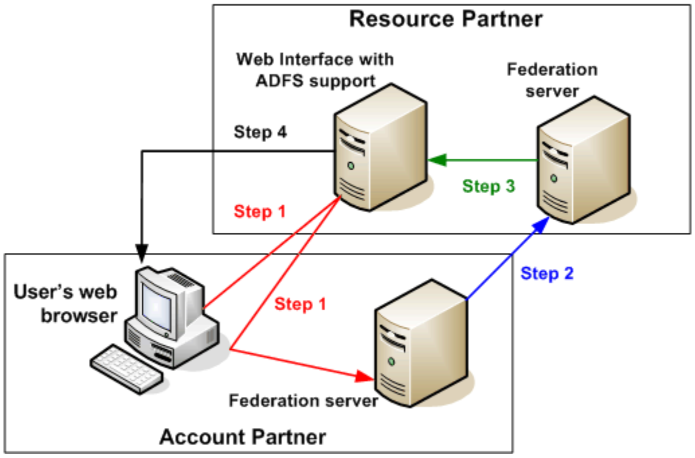
The following table contains basic terms used when describing ADFS.

Term	Definition
account partner	Client organization that wants to use the Web applications from the resource partner. The account partner provides the identities (user accounts).
federation server	Federation servers host the Federation Service component of ADFS, which controls access to your systems based on identification, authentication, and authorization through the federation trust. Federation servers authenticate requests from trusted partners based on the credentials of the partners. Representations of the credentials are exchanged in the form of security tokens.
federation server proxy	Federation server proxies host the Federation Service proxy component of ADFS. You can deploy federation server proxies in the demilitarized zone (DMZ) to forward requests to federation servers that are not accessible from the Internet.
Federation Service	A security token service in Windows Server 2003 R2 that provides tokens in response to requests for security tokens.
Federation Service proxy	Federation Service proxies collect user credential information from browser clients and Web applications and send the information to the Federation Service.
resource partner	Organization that makes services or Web applications available over the Internet.
shadow account	Shadow accounts are created in Active Directory on the *resource partner*. They mirror user accounts existing on the *account partner.* Do not enable shadow accounts for interactive logon, because they are never used for that purpose.

How ADFS Integrated Sites Work

The following steps occur when a user on an account partner accesses a published Web application on a resource partner.

1. A user opening the Web Interface home page on the resource partner is redirected to the account partner’s authentication page.
2. The account partner authenticates the user and sends a security token back to the resource partner.
3. ADFS on the resource partner validates the security token, transforms it to a Windows identity (representing a shadow account), and redirects the user to the Web Interface logon page.
4. Web Interface displays the application list page for the user.



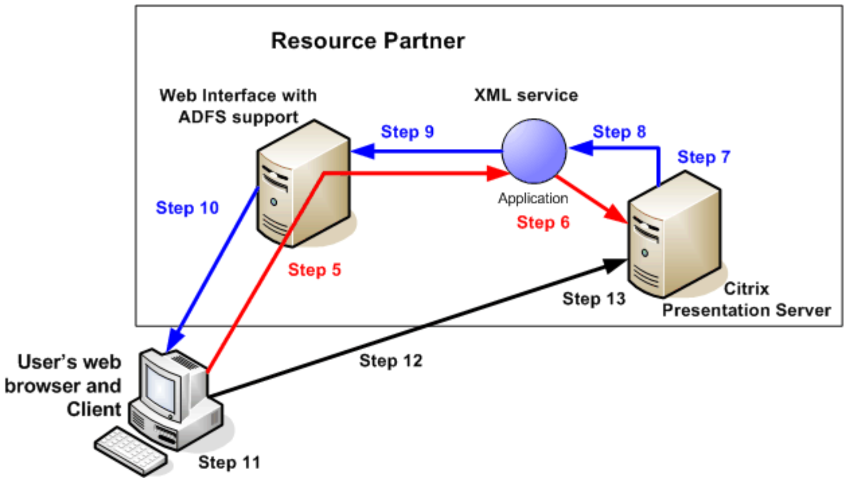
This diagram shows the steps that occur when a user tries to access an application list.

5. The user launches an application by clicking a hyperlink on the page. Web Interface contacts the Citrix XML service to request a launch.

Note For applications to be accessible by ADFS users, you must publish the applications on the resource partner's server for one or more of the shadow accounts.

6. The Citrix XML service generates Security Support Provider Interface data and sends it to Presentation Server.
7. Presentation Server uses the Security Support Provider Interface data to authenticate the user and stores a logon token in Presentation Server for future authentication.
8. Presentation Server generates a launch ticket to uniquely represent the stored logon token and returns this ticket to the Citrix XML service.
9. The Citrix XML Service returns the launch ticket to Web Interface.
10. Web Interface creates an ICA file containing the launch ticket and sends it to the user's browser.
11. The client on the user's computer opens the ICA file and attempts an ICA connection to Presentation Server.
12. The client sends the launch ticket to Presentation Server.
13. Presentation Server receives the launch ticket, matches it to the logon token that was generated previously, and uses this logon token to log the user onto

the ICA session on the server. The ICA session runs under the identity of the shadow account.



This diagram shows the steps that occur when the user clicks a link on the application list.

Depending on the settings configured for a site, when a user logs off, they log off from either:

- The Web Interface

—Or—

- The Web Interface and ADFS

If they log off from the Web Interface and ADFS, they log off from all ADFS Web applications.

Software Requirements

The following software must be installed and configured in your environment:

- Microsoft Windows Server 2003 R2 for federation and Web servers
- Microsoft Active Directory Federation Services (ADFS) on the resource and account partners

Before Creating ADFS Sites

Before you create an ADFS site, you must carry out the following steps. Disregarding any of them can cause failure.

- Synchronize the clocks on the account partner federation server and the resource partner federation server to within five minutes of each other. If not, the security tokens generated by the account partner may not be accepted by the resource partner because the tokens appear to have expired. To avoid this problem, both organizations should synchronize their servers with the same Internet time server. For more information, see “Setting Up the Relationships Between Domains” on page 162.
- Ensure the resource federation and Web servers can access the Certificate Authority’s Certificate Revocation Lists (CRLs). ADFS may fail if the servers cannot ensure that a certificate has not been revoked. For more information, see “Setting Up the Relationships Between Domains” on page 162.
- Ensure all servers within your deployment are trusted for delegation. For more information, see “Configuring Delegation for the Servers in Your Deployment” on page 164.
- Set up shadow accounts in the resource partner domain for each external user that can authenticate to the Web Interface through ADFS. For more information, see “Setting Up Shadow Accounts” on page 168.
- Install Citrix Presentation Server 4.5, ensuring that the XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

Important This guide does not document how to install ADFS. You should have a working ADFS installation, with external account users able to access ADFS-enabled Web applications in a resource partner.

- Set up a trust relationship between the server running the Web Interface and any other servers in the farm running the Citrix XML Service that the Web Interface contacts. For more information see, “Setting Up a Trust Relationship” on page 116.

Setting Up the Relationships Between Domains

The deployment documented in this appendix consists of two domains (in their own forests), one for the account partner and one for the resource partner.

Note The required components do not have to be on separate computers.

To set up the relationships between domains

1. Ensure you have the following components:

Account Partner	**Resource Partner**
Domain controller	Domain controller
Federation Server*	Federation Server*
Client computers	Web Server*
	One or more servers for a Presentation Server farm
Components marked with an asterisk (*) must be on computers running Windows 2003 R2 and have the **Active Directory Federation Services** component installed.	

2. Obtain separate server certificates for the Web server and both federation servers.

   - Certificates must be signed by a trusted entity called a Certificate Authority (CA).
   - The server certificate identifies a specific computer, so you must know the fully qualified domain name (FQDN) of each server; for example, cpsserver1.mydomain.com.
   - Install the Web server certificate into Internet Information Services (IIS) to enable the IIS default Web site for SSL traffic.
   - Install federation server certificates using the Microsoft Management Console (MMC) Certificate snap-in. See the *Step-by-Step Guide to the Microsoft Management Console* at www.microsoft.com for more information.

3. To ensure the resource partner’s federation server trusts the account partner’s federation server, install the account partner’s federation server root certificate into the Trusted Certification Authorities area of the resource partner’s federation server.

4. To ensure the Web server trusts the resource partner’s federation server, install the resource partner’s federation server root certificate into the Trusted Certification Authorities area of the Web server.

Important The resource federation and Web servers must be able to access the CA’s Certificate Revocation Lists (CRLs). The resource federation server must have access to the account partner Certificate Authority and the web server must have access to the resource partner Certificate Authority. ADFS might fail if the servers cannot ensure that a certificate has not been revoked.

5. On the resource partner federation server, open the MMC Active Directory Federation Services snap-in.
6. In the left pane, select **Federation Service > Trust Policy > Partner Organizations > Account Partners**, and then select the account partner name.
7. On the **Action** menu, click **Properties**.
8. On the **Resource Accounts** tab, select **Resource accounts exist for all users** and click **OK**.
9. Using the same Internet time server, synchronize the clocks on the account partner federation server and the resource partner federation server to within five minutes of each other. If not, the security tokens generated by the account partner may not be accepted by the resource partner because the tokens appear to have expired.

   The resource and account partners can be in different time zones, but they must be correctly synchronized. For example, the account partner is in New York and is set to 4:00 p.m. Eastern Standard Time (EST). The resource partner in California has to be set to within 12:55 to 1:05 p.m. Pacific Standard Time (PST). (There is a three-hour difference between EST and PST zones.)

Configuring Delegation for the Servers in Your Deployment

You must ensure that all servers within your deployment are trusted for delegation. To do this, you must complete the following tasks. Procedures for each task are included in this section.

- Ensure the resource partner domain’s functional level is correct
- Trust the server running the Web Interface for delegation
- Trust the server running the XML Service for delegation
- Determine which resources are accessible from the server running Presentation Server

Important To complete the procedures in this step, log on as an administrator to the resource partner domain controller, and then use the MMC Active Directory Users and Computers snap-in.

To ensure the resource partner domain is at the Windows Server 2003 functional level

Note To raise the domain level, all domain controllers in the domain must be running Windows Server 2003.

1. From the MMC Active Directory Users and Computers snap-in, select the domain name.
2. On the **Action** menu, click **Properties**.
3. If the domain is not at the Windows Server 2003 functional level, select the domain name and select **Raise domain functional level**.

To trust the server running the Web Interface for delegation

1. In the MMC Active Directory Users and Computers snap-in **View** menu, enable **Advanced Features.**
2. In the Computers folder under the domain name, select the server running the Web Interface.
3. On the **Action** menu, click **Properties**.

4. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.
5. On the **Add Services** screen, click **Users or Computers**.
6. On the **Select Users or Computers** screen, type the name of the server running the XML Service in the **Enter the object names to select** text box, and then click **OK**.
7. Select the **http** service type from the list and then click **OK**.
8. On the **Delegation** tab, verify the **http** service type for the server running Presentation Server appears in the **Services to which this account can present delegated credentials** list, and then click **OK**.

Note Repeat the process for each server in the farm running the XML Service that the Web Interface is configured to contact.

To trust the server running the XML Service for delegation

1. In the Computers folder under the MMC Active Directory Users and Computers snap-in, select the name of the server running the XML Service that the Web Interface is configured to contact.
2. On the **Action** menu, click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use Kerberos only**, and then click **Add**.
4. On the **Add Services** screen, click **Users or Computers**.
5. On the **Select Users or Computers** screen, type the name of the server running the XML Service in the **Enter the object names to select** text box, and then click **OK**.
6. Select the **HOST** service type from the list and then click **OK**.
7. On the **Delegation** tab, verify the **HOST** service type for the server running the XML Service appears in the **Services to which this account can present delegated credentials** list, and then click **OK**.
8. For a multiserver farm, repeat Steps 3 to 7 for each server running Presentation Server.

Note Repeat the process for each server in the farm running the XML Service that the Web Interface is configured to contact.

To determine which resources are accessible from the server running Presentation Server

1. In the Computers folder under the MMC Active Directory Users and Computers snap-in, select the name of the server running Presentation Server.
2. On the **Action** menu, click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use Kerberos only**, and then click **Add**.
4. On the **Add Services** screen, click **Users or Computers**.
5. On the **Select Users or Computers** screen, type the name of the resource partner domain controller in the **Enter the object names to select** text box, and then click **OK**.
6. From the list, select the **cifs** and **ldap** service types for the resource partner domain controller and click **OK**.

   Note The **cifs** service type applies to network shares. Add the cifs service to the list for any computers on which users can access network shares.

   If two choices appear for the **ldap** service, select the one that matches the FQDN of your domain controller.

7. On the **Delegation** tab, verify the **cifs** and **ldap** services for the resource partner domain controller appear in the **Services to which this account can present delegated credentials** list, and then click **OK**.

Note If you are using multiserver farms, repeat the procedure for each server running Presentation Server.

Configuring Servers for Constrained Delegation

For security reasons, you must configure all servers running Presentation Server for constrained delegation. To provide users with access to resources on those servers you must add the relevant services to the Services list using the MMC Active Directory Users and Computers snap-in. For example, to enable users to authenticate to a Web server on host foo, add the http service for server foo; to enable users to authenticate to an SQL server on host bar, add the MSSQLSvc service for server bar.

For more detailed information, see the *Service Principal Names and Delegation* whitepaper in the Citrix Knowledge Base.

Configuring a Time Limit for Access to Resources

By default, ADFS users have access to resources on a network for 15 minutes. You can increase this time limit by modifying the following registry entry on the server running the XML service:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\
Parameters\S4UTicketLifetime

This value specifies the number of minutes users have access to resources for after a session starts.

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

The domain security policy governs the maximum value you can set for the S4ULifetime parameter. If you specify a value for the S4UTicketLifetime parameter that is greater than the value specified at domain level, the domain level setting takes precedence.

To configure a time limit for access to resources at domain level

1. Log on to the domain controller as a domain administrator.
2. On the **Start** Menu, click **All Programs > Administrative Tools > Domain Security Policy**.
3. In the console tree, expand **Account Policies**.
4. Select **Kerberos Policy**.
5. In the details pane, click **Maximum lifetime for a service ticket**.
6. On the **Actions** menu, click **Properties**.
7. Enter a value (in minutes) in the **Ticket expires in:** box.
8. Click **OK**.
9. Close the **Domain Security Policy** dialog box.

If you do not want to configure a time limit for access to resources, select **Use any authentication protocol** when determining which resources are accessible from the server running Presentation Server. If you select this option, any value specified for the S4UTicketLifetime parameter is ignored.

For more information, see Microsoft’s Web site at http://support.microsoft.com/.

Setting Up Shadow Accounts

To launch applications, Presentation Server requires real Windows accounts. Therefore, you must manually create a shadow account in the resource partner domain for each external user that authenticates to the Web Interface through ADFS.

Note If you have a large number of users in the account partner domain that will access applications in the resource partner domain, you can use a third-party account-provisioning product to enable rapid creation of user shadow accounts in Active Directory.

To create shadow accounts, complete the following tasks as an administrator on the domain controller for the resource partner domain. Procedures for each task are included in this section.

- Add user principal name (UPN) suffixes for all external *account partners.*
- Define the shadow account user.

To add UPN suffixes

1. Open the MMC Active Directory Domains and Trusts snap-in.
2. In the left pane, select **Active Directory Domains and Trusts.**
3. On the **Action** menu, click **Properties**.
4. Add a UPN suffix for each external *account partner.* For example, if the Active Directory domain of the account partner is adatum.com, add adatum.com as the UPN suffix.
5. Click **OK**.

To define the shadow account user

1. Open the MMC Active Directory Users and Computers snap-in.
2. In the left pane, select the domain name.
3. On the **Action** menu, click **Users** > **New user**.
4. Type the user’s first name, initials, and last name in the corresponding text boxes.
5. In the **User logon name** text box, type the account name. Make sure this name matches the name on the account partner.
6. From the drop-down list, choose the external UPN suffix, and then click **Next**.

7. In the **Password** and **Confirm password** text boxes, type a password that meets your password policy. This password is never used because the user authenticates through ADFS.
8. Clear the **User must change password at next logon** check box.
9. Select the **User cannot change password** and **Password never expires** check boxes.
10. Click **Next**, and then click **Finish**.

Creating ADFS Integrated Sites

Run the **Create site** task from the Access Management Console and configure the site to use ADFS for authentication.

To create an ADFS integrated site

1. Click the **Create site** task.
2. Select **Access Platform site**.
3. On the **Specify IIS location** page, enter your required settings, and then click **Next**.
4. On the **Configuration Source** page, enter your required settings, and then click **Next**.
5. Select **Use Microsoft ADFS integration**, enter your required settings, and then click **Next**.
6. Confirm the settings for the new site and then click **Next**.
7. Click **Finish** to create the site.

Configuring Your Site as an ADFS Application

After creating your site you must configure it as an ADFS application so the federation server recognizes it.

To configure your site as an ADFS application

1. Open the MMC Active Directory Federation Services snap-in on the resource partner federation server.
2. In the left pane, select **Federation Service >Trust Policy > My Organization > Applications.**
3. On the **Action** menu, click **New** > **Applications**.
4. Click **Claims-aware application** and then click **Next**.

5. In the **Application display name** box, type **Citrix Web Interface**.
6. In the **Application URL** box, enter the URL of your Web Interface site, and then click **Next**.

Important Make sure you use HTTPS and the FQDN of your Web server.

---

7. Depending on how you configured ADFS (which is usually PKI), select **Public Key Infrastructure** or **Domain Service Account**, and then click **Next**.
8. Click **User Principal Name (UPN)** and then click **Next**.
9. Select the **Enable this application** check box and then click **Next**.
10. Click **Finish**.

Testing Your Deployment

After configuring your site as an ADFS application, test your deployment to ensure everything is working correctly between the account partner and the resource partner.

To test the Web Interface ADFS deployment

1. Log on to your client computer on the account partner.
2. Open a Web browser and type the FQDN URL of the Web Interface site that you previously created.

   The Web Interface application list page appears.

Note If you have not configured ADFS for integrated authentication, you may be prompted to enter your credentials or insert a smart card.

---

3. If you have not installed the Citrix Presentation Server client, do so now. For more information, see the *Clients for Windows Administrator's Guide.*

Note The Client for Java or Remote Desktop Connection software are not supported on ADFS integrated sites.

---

4. Click on an application to launch it.

Logging Off From ADFS Integrated Sites

Use the **Configure Authentication Method** task to specify whether users clicking the Logoff or Disconnect buttons in a browser log off from:

- The Web Interface only
- The Web Interface and the ADFS Federation Service

If you specify that users log off from the Web Interface only, they are directed to the Web Interface logoff page. If you specify that users log off from the Web Interface and the ADFS Federation Service, they are directed to the federation service logoff page and logged off from all ADFS Web applications.

To specify which services a user logs off from

1. Click the **Configure Authentication Method** task.
2. To specify that users log off from the Web Interface and ADFS federation service, select the **Perform global logoff** check box.
3. To specify that users log off from the Web Interface only, clear the **Perform global logoff** check box.

Index