Web Interface Administrator’s Guide

Citrix® Web Interface 5.0.1
Contents

1 Introduction ................................................................. 9
   How to Use This Guide .................................................. 9
   Finding Documentation .................................................. 9
   Documentation Conventions ......................................... 10
   Getting Support and Training ....................................... 10
   New Names for Citrix Presentation Server Components ......... 11
   Introducing the Web Interface ....................................... 11
   Web Interface Features ................................................. 12
   Management Features .................................................. 12
   Published Resource Access Features .............................. 13
   Security Features ...................................................... 13
   Plugin Deployment Features ......................................... 14
   New in This Release .................................................... 15
   Web Interface Components .......................................... 16
   Server Farms ........................................................... 16
   Web Server ............................................................ 16
   Client Device .......................................................... 17
   How the Web Interface Works ....................................... 17
   What to Do Next ...................................................... 18

2 Deploying the Web Interface ........................................... 19
   System Requirements .................................................. 19
   Server Requirements .................................................. 19
   Web Server Requirements ........................................... 22
   User Requirements .................................................... 24
   Client Device Requirements ......................................... 26
   Installing the Web Interface ......................................... 26
   Installation Overview .................................................. 26
   Installing the Web Interface on Internet Information Services .... 27
   Installing the Web Interface on Java Application Servers ........ 30
3 Getting Started with the Web Interface. ................................................. 37
   Deciding Which Configuration Method to Use .................................... 37
   Using the Access Management Console ........................................... 37
   Using Configuration Files .......................................................... 38
   Site Configuration Sources .......................................................... 38
   Centralized Configuration ............................................................ 39
   Configuring Sites Using the Console .............................................. 39
   Getting Help. .............................................................................. 40
   Getting Started with the Access Management Console ....................... 40
   Configuring and Running Discovery .............................................. 40
   To configure and run discovery ..................................................... 41
   Creating Sites ............................................................................. 42
   Creating Sites on Internet Information Services ................................. 42
   Creating Sites on Java Application Servers .................................... 42
   Specifying the Authentication Point ................................................ 43
   Authentication at the Web Interface ............................................... 43
   Authentication at an Active Directory Federation Services Account Partner .................................................. 43
   Authentication at Access Gateway ................................................ 44
   Authentication at a Third Party Using Kerberos ................................ 47
   Authentication at the Web Server ................................................... 47
   Specifying Initial Configuration Settings for a Site ............................. 47
   Specifying Server Farms ................................................................ 48
   Specifying Authentication Methods ............................................... 48
   Specifying Domain Restrictions ..................................................... 48
   Specifying the Appearance of the Logon Screen ............................... 48
   Specifying the Types of Published Resources Available to Users ........ 49
Enabling Pass-Through Authentication .......................................................... 73
  Pass-Through Requirements ........................................................................ 73
  Step 1: Installing the Citrix XenApp Plugin for Hosted Apps ..................... 74
  Step 2: Enabling Pass-Through for the Plugins ......................................... 74
  Step 3: Enabling Pass-Through Using the Console ..................................... 75
Enabling Smart Card Authentication ............................................................... 75
  Smart Card Support Requirements ............................................................ 76
  Step 1: Installing the Citrix XenApp Plugin for Hosted Apps ..................... 76
  Step 2: Enabling Pass-Through for the Plugins ......................................... 76
  Step 3: Enabling the Windows Directory Service Mapper .......................... 77
  Step 4: Enabling Smart Card Authentication on the Web Interface ............. 78
  Example: Enabling Smart Card Authentication for Users ......................... 79
Configuring Two-Factor Authentication .......................................................... 80
  Enabling Secure Computing SafeWord on Internet Information Services ...... 80
  Enabling RSA SecurID 6.0 Authentication on Internet Information Services 6.0 . 81
  Enabling RADIUS Authentication ............................................................... 84

6 Managing Plugins ......................................................................................... 87
  Managing Plugin Deployment ...................................................................... 87
  Remote Plugin Types .................................................................................. 88
  Citrix XenApp Plugin for Streamed Apps ................................................... 88
  Using Web-Based Plugin Installation ......................................................... 89
  Deploying Remote Desktop Connection Software ..................................... 92
  Deploying the Client for Java .................................................................... 93
  Configuring Support for Older Plugins ..................................................... 97
Configuring Streaming Session Monitoring .................................................... 97
  To configure streaming session monitoring .............................................. 97
Configuring Citrix XenApp ............................................................................ 98
  Using the Access Management Console for Configuration ..................... 98
  Using the Configuration Files ................................................................... 98
  Managing Plugin Configuration Files ....................................................... 98
Managing Secure Access ............................................................................... 99
  Editing Direct Access Routes .................................................................... 99
  Editing Alternate Address Settings .......................................................... 99
  Editing Address Translations ................................................................. 100
  Editing Gateway Settings ....................................................................... 101
  Editing Default Access Settings .............................................................. 102
  Editing Client-Side Proxy Settings ............................................................ 104
  To configure default proxy settings .......................................................... 104
7 Customizing the User Experience ........................................... 107
    Customizing the Appearance for Users ................................. 107
    Managing Session Preferences ....................................... 109
    Bandwidth Control ..................................................... 110
    ClearType Font Smoothing ............................................. 111
    Special Folder Redirection ........................................... 112
    Configuring Workspace Control ..................................... 113
    Feature Requirements ............................................... 113
    Limitations ................................................................ 114
    Using Workspace Control with Integrated Authentication Methods ........................................ 114
    Enabling Workspace Control ............................................ 115
    Changing Session Options .............................................. 117
    Managing Shortcuts to Published Resources ......................... 118
    Using Published Resource Refresh Options ......................... 118

8 Configuring Web Interface Security ..................................... 119
    Introduction to Web Interface Security ............................... 119
    Security Protocols and Citrix Security Solutions ................. 120
    Securing Web Interface Communication ............................... 124
    Securing Citrix XenApp with SSL ..................................... 124
    Client Device/Web Interface Communication ......................... 124
        Security Issues ....................................................... 125
        Recommendations .................................................. 125
    Web Interface/Citrix Server Communication ........................ 126
        Security Issues ....................................................... 127
        Recommendations .................................................. 127
    Client Session/Server Communication ................................ 130
        Security Issues ....................................................... 130
        Recommendations .................................................. 130
    Controlling Diagnostic Logging ........................................ 131
    General Security Considerations ..................................... 131

9 Configuring Sites Using the Configuration File .......................... 133
    Site Configuration Files ............................................... 133
    Disabling Error Messages ............................................. 134
    WebInterface.conf Parameters ....................................... 134
    Citrix XenApp Considerations ....................................... 150
        Contents of the config.xml File ................................ 150
        Settings in the WebInterface.conf File ......................... 151
Examples .................................................................152
Configuring Communication with the Server ....................................152
Configuring Citrix SSL Relay Communication .......................................153
Configuring Secure Gateway Support ..................................................153
Settings in the bootstrap.conf File ......................................................154

10 Configuring Active Directory Federation Services Support for the Web Interface. ........155
About Active Directory Federation Services ........................................155
What Is Active Directory Federation Services? ......................................155
Active Directory Federation Services Terminology .................................156
How Active Directory Federation Services Integrated Sites Work ...............157
Software Requirements for Active Directory Federation Services ...............159
Before Creating Active Directory Federation Services Sites ......................159
Setting up the Relationships Between Domains .....................................160
Configuring Delegation for the Servers in Your Deployment .......................162
Setting up Shadow Accounts ................................................................166
Creating Active Directory Federation Services Integrated Sites ..................168
To create an Active Directory Federation Services integrated site ...............168
Configuring Your Site as an Active Directory Federation Services Application ....168
To configure your site as an Active Directory Federation Services application ....168
Testing Your Deployment ....................................................................169
To test the Web Interface Active Directory Federation Services deployment ......169
Logging off from Active Directory Federation Services Integrated Sites ........170
To specify which services users log off from ......................................170

Index ..................................................................................171
Introduction

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

- How to Use This Guide
- Introducing the Web Interface
- New in This Release

How to Use This Guide

The *Web Interface Administrator’s Guide* is for Citrix administrators and webmasters responsible for installing, configuring, and maintaining XenApp Web and XenApp Services sites.

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

This guide assumes knowledge of XenApp and/or XenDesktop.

Finding Documentation

Read Me First.html, which is included on the XenApp and XenDesktop installation media, contains links to documents that will help get you started. It also contains links to the most up-to-date product documentation for XenApp/XenDesktop and their components, plus related technologies.

The Citrix Knowledge Center Web site, [http://support.citrix.com](http://support.citrix.com), contains links to all product documentation, organized by product. Select the product you want to access and then click the **Documentation** tab on the product information page.

Known issues information is included in the readme.

To provide feedback about the documentation, click the **Article Feedback** link located on the right side of the product documentation page.
Documentation Conventions

For consistency, Windows Vista and Windows Server 2008 (x64) terminology is used throughout the documentation set; for example, “Documents” rather than “My Documents” and “Computer” rather than “My Computer” are used.

Web Interface documentation uses the following typographic conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Commands, names of interface items such as boxes, option buttons, and user input.</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Placeholders for information you provide. For example, <em>file name</em> means you type the actual name of a file. Italics also are used for new terms and titles of books.</td>
</tr>
<tr>
<td>%SystemRoot%</td>
<td>The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or any other name you specify when you install Windows.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Text displayed in a text file.</td>
</tr>
<tr>
<td>{ braces }</td>
<td>In a command, a series of items, one of which is required. For example, {yes</td>
</tr>
<tr>
<td>[ brackets ]</td>
<td>In a command, optional items. For example, [ ping ] means you can type ping with the command. Do not type the brackets themselves.</td>
</tr>
<tr>
<td></td>
<td>In a command, a separator between items in braces or brackets. For example, /hold</td>
</tr>
<tr>
<td>… (ellipsis)</td>
<td>The previous item(s) in the command can be repeated. For example, /route:DeviceName[….] means you can type additional device names separated by commas.</td>
</tr>
</tbody>
</table>

UNIX Command-Line Conventions

Web Interface 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 Support and Training

The Citrix Knowledge Center (http://support.citrix.com) offers a variety of technical support services, tools, and developer resources.

New Names for Citrix Presentation Server Components

*Citrix XenApp* is the new name for Citrix Presentation Server. The following clients and components have been updated to reflect that product name:

- *Citrix XenApp Plugin for Hosted Apps* is the new name for the plugin for server-side virtualization (formerly named Citrix Presentation Server Clients for Windows), which contains the following plugins:
  - *Citrix XenApp*, formerly named the Program Neighborhood Agent
  - *Citrix XenApp Web Plugin*, formerly named the Web Client
  - Program Neighborhood

- *Citrix XenApp Plugin for Streamed Apps* is the new name for the plugin for client-side virtualization, formerly named the Citrix Streaming Client

- *XenApp Web sites* is the new name for access platform sites

- *XenApp Services sites* is the new name for Program Neighborhood Agent Services sites

Introducing the Web Interface

The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their published resources through a standard Web browser or through Citrix XenApp (the new name for the Program Neighborhood Agent).

The Web Interface employs Java and .NET technology executed on a Web server to dynamically create an HTML depiction of server farms for XenApp Web sites. Users are presented with all the resources (applications, content, and desktops) published in the server farm(s) you make available. You can create stand-alone Web sites for access to published resources or Web sites that can be integrated into your corporate portal. Additionally, the Web Interface allows you to configure settings for users accessing published resources through Citrix XenApp.

You can configure Web Interface sites created on Windows platforms using the Access Management Console. The Access Management Console can be installed on Windows platforms only. For more information about using this tool, see “Configuring Sites Using the Console” on page 39.
You can also edit the configuration file (WebInterface.conf) to manage and administer Web Interface sites. For more information, see “Configuring Sites Using the Configuration File” on page 133.

In addition, you can customize and extend XenApp Web sites. The documentation for the Web Interface SDK explains how to configure sites using these methods.

**Web Interface Features**

This section provides information about the features of the Web Interface. For information about the software requirements of particular Web Interface features, see “Minimum Software Requirements” on page 20.

**XenApp Web Sites**

The Web Interface provides functionality to create and manage XenApp Web sites (the new name for access platform sites). Users access remote published resources and streamed applications using a Web browser and a plugin.

**XenApp Services Sites**

Citrix XenApp is a plugin designed for flexibility and ease of configuration. Using Citrix XenApp in conjunction with XenApp Services sites (the new name for Program Neighborhood Agent Services sites) on the Web Interface, you can integrate published resources with users’ desktops. Users access remote and streamed applications, and remote desktops and content by clicking icons on their desktop or the Start menu, or by clicking in the notification area of their computer desktop. You can determine what, if any, configuration options your users can access and modify, such as audio, display, and logon settings.

**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.

**Multiple server farm support.** You can configure multiple server farms and provide users with a display of the published resources 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 the Server” on page 152.

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

Support for UNIX farms. Support for XenApp for UNIX farms allows the Web Interface to display and serve applications running on UNIX platforms to your users’ client devices.

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

Active Directory and user principal name support. All Web Interface components are compatible with Microsoft Active Directory. Users visiting XenApp Web sites can log on to server farms that are part of an Active Directory deployment and seamlessly access published applications and content. The logon screens are compatible with Active Directory’s use of user principal names (UPNs).

Anonymous users. The Web Interface allows users to access XenApp applications by logging on to XenApp Web sites using an anonymous account.

Accessing published content. The Web Interface supports the content publishing features of XenApp.

Security Features

Secure Sockets Layer/Transport Layer Security support. The Web Interface supports the Secure Sockets Layer (SSL) protocol to secure communication between the Web Interface server 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 .NET Framework to implement SSL and cryptography.

Citrix Access Gateway support. Access Gateway is a universal SSL virtual private network (VPN) appliance that, together with the Web Interface, provides a single, secure point of access to any information resource—both data and voice. 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 published resources and protocols.

Secure Gateway support. Secure Gateway, together with the Web Interface, provide a single, secure, encrypted point of access through the Internet to servers on your internal corporate networks. Secure Gateway simplifies certificate management because a server certificate is required only on the Secure Gateway server, rather than on every server in the farm.
**Ticketing.** This feature provides enhanced authentication security. The Web Interface obtains tickets that authenticate users to published resources. 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 published resources. Use of ticketing eliminates the explicit inclusion of credentials in the .ica files that the Web Interface uses to connect to published resources.

**Change password.** Users logging on to the Web Interface or Citrix XenApp using explicitly supplied domain credentials now have the option of changing their Windows password if it expires. Users can change their password regardless of whether or not their computer is in the domain to which they are attempting to authenticate.

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

## Plugin Deployment Features

**Web-based plugin installation.** When a user visits a XenApp Web site, the Web Interface detects the device and Web browser types and prompts the user to install an appropriate plugin, if one is available. Increased security restrictions in modern operating systems and Web browsers can make it difficult for users to download and deploy Citrix plugins, so the Web Interface provides a plugin detection and deployment process that guides users through the plugin deployment procedure, including, where appropriate, reconfiguring their Web browser. This ensures that users get an optimal experience when accessing their published resources, even from the most restricted environments.

**Citrix XenApp support.** Citrix XenApp allows users to access published resources directly from their desktops without using a Web browser. The Citrix XenApp user interface can also be “locked down” to prevent user misconfiguration.

**Citrix XenApp Plugin for Streamed Apps support.** The Citrix XenApp Plugin for Streamed Apps allows users to stream XenApp applications to their desktops and open them locally. You can either install the plugin with Citrix XenApp to provide the full set of Citrix client-side application virtualization features or install the plugin alone on users’ desktops so users can access published applications through a Web browser using a XenApp Web site.
New in This Release

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

**Redesigned user interface.** The end-user interface has been redesigned to provide more functionality and an enhanced user experience. The new user interface offers different view styles so that users can choose the way in which they would prefer to see their published resources represented. Search functionality has been added to help users more easily find the published resource they are looking for. Hints are available to highlight the features of the user interface. In addition, a low graphics version is introduced for users of hand-held devices and for integration with Access Gateway and third-party portals.

**Support for Windows Server 2008.** The Web Interface is supported for installation on both the x86 and x64 editions of Windows Server 2008 and is fully compatible with Microsoft Internet Information Services (IIS) 7.0.

**Special Folder Redirection.** The Web Interface allows users to map the Documents and Desktop folders for the server to their local computer. This enhancement makes it easier for users to find their local folders in, for example, the **Save As** dialog box of a published application. Special Folder Redirection support is provided through a combination of a server policy rule, client drive mapping, and session options configured with the Access Management Console.

**Font smoothing.** This feature improves the user experience by supporting ClearType font smoothing in published applications. ClearType is a software technology developed by Microsoft that improves the readability of text on LCD screens commonly found on laptops, hand-held devices, and flat panel monitors. Font smoothing must be enabled on XenApp, the Web Interface, users’ plugins, and users’ Windows operating systems.

**Secure access methods with Citrix XenApp.** XenApp Services sites for Citrix XenApp now support the full range of secure access methods available in the Web Interface. This allows Citrix XenApp users to connect to their published resources through a secure access solution such as Access Gateway.

**Java-based installer.** The Web Interface for Java Application Servers distributable has been upgraded to a Java application, making it platform independent and also allowing it to be run on Windows operating systems where Microsoft Internet Information Services is not being used as the Web server.
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 Web browser and a Citrix plugin

Server Farms

A group of servers that are managed as a single entity and operates together to serve published resources to users are collectively known as a server farm. A server farm is composed of a number of servers all running either XenApp (the new name for Presentation Server) or Desktop Delivery Controller, but not a mixture of both.

One of a server farm’s most important functions is resource publishing. This is a process that lets administrators make available to users specific resources (applications, content, and desktops) hosted by the server farm. When an administrator publishes a resource for a group of users, that resource becomes available as an object to which plugins can connect and initiate sessions.

Using the Web Interface, users can log on to the server farm and receive a customized list of resources published for their individual user name. This list of resources is called a resource set. The Web Interface server functions as an access point for connecting to one or more server farms. The Web Interface server queries server farms for resource set information and then formats the results into HTML pages that users can view in a Web browser.

To obtain information from server farms, the Web Interface server communicates with the Citrix XML Service running on one or more servers in the farm. The Citrix XML Service is a component of XenApp and Desktop Delivery Controller that provides published resource information to plugins and Web Interface servers using TCP/IP and HTTP. This service functions as the point of contact between the server farm and the Web Interface server. The Citrix XML Service is installed with XenApp and Desktop Delivery Controller.

Web Server

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

- Authenticates users to a server farm or farms
- Retrieves information about published resources, including a list of resources the user can access
Client Device

A client device is any computing appliance capable of running a Citrix plugin and a Web browser. Client devices include desktop PCs, laptops, network computers, terminals, and hand-held computers, among others.

In a client device, the browser and plugin work together as the viewer and the engine. The browser lets users view resource sets (created by server-side scripting on the Web Interface server) while the plugin acts as the engine that allows users to access published resources.

The Web Interface provides Web-based plugin deployment, which is a method of deploying plugins from a Web site. When a user visits a site created with the Web Interface, the Web-based plugin detection and deployment process detects the device and the user is prompted to deploy an appropriate plugin. For some environments, the plugin detection and deployment process can also detect the presence or absence of an installed plugin and prompts the user only when necessary. See “Configuring Plugin Deployment and Installation Captions” on page 90 for more information.

The Web Interface supports many browser/plugin combinations. For a complete list of supported browser/plugin combinations, see “Client Device Requirements” on page 26.

How the Web Interface Works

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

The figure 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 published resources.
Client device users authenticate to the Web Interface through a Web browser.

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 the other servers in the farm.

The Citrix XML Service on the designated server retrieves from the servers a list of published resources that users can access. These resources comprise the user’s resource set. The Citrix XML Service retrieves the resource set from the Independent Management Architecture (IMA) system.

In a XenApp for UNIX farm, 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 resource set information to the Web Interface running on the server.

The user clicks an icon that represents a published resource on the HTML page.

The Citrix XML Service is contacted to locate the server in the farm that is least busy. The Citrix XML Service identifies the least busy server and returns the address of this server to the Web Interface.

The Web Interface communicates with the plugin (in some cases using the Web browser as an intermediary).

The plugin initiates a session with the server in the farm according to the connection information supplied by the Web Interface.

**What to Do Next**

For information about system requirements, instructions for installing the Web Interface, and configuring the Web Interface server, see “Deploying the Web Interface” on page 19.
Deploying the Web Interface

This section 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 Server Versions

The Web Interface supports the following product versions:

• Citrix XenApp 5.0 for Microsoft Windows Server 2008 x64 Edition
• Citrix XenApp 5.0 for Microsoft Windows Server 2008
• Citrix XenApp 5.0 for Microsoft Windows Server 2003 x64 Edition
• Citrix XenApp 5.0 for Microsoft Windows Server 2003
• Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
• Citrix XenDesktop 2.0
• Citrix Presentation Server 4.5, with Feature Pack 1, for Windows Server 2003 x64 Edition
• Citrix Presentation Server 4.5, with Feature Pack 1, for Windows Server 2003
• Citrix Presentation Server 4.5 for Windows Server 2003 x64 Edition
• Citrix Presentation Server 4.5 for Windows Server 2003
• Citrix Presentation Server 4.0 for Windows Server 2003
• Citrix Presentation Server 4.0 for Windows 2000 Server
• Citrix Presentation Server 4.0 for UNIX Operating Systems

The Web Interface operates with these products on all of their supported platforms. For a list of supported platforms, see the appropriate Administrator’s Guide. Citrix recommends that you install the latest service pack for the operating system on your servers.

**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 XenApp Administrator’s Guide*.

**Minimum Software Requirements**

Without the latest release, some new features are not available. For example, to support Special Folder Redirection, you must have Citrix XenApp 5.0 installed on all servers in the farm.

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

<table>
<thead>
<tr>
<th>Web Interface feature</th>
<th>Software requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special Folder Redirection</td>
<td>Citrix XenApp 5.0</td>
</tr>
<tr>
<td></td>
<td>Citrix XenApp Plugin for Hosted Apps</td>
</tr>
<tr>
<td>Font smoothing</td>
<td>Citrix XenApp 5.0</td>
</tr>
<tr>
<td></td>
<td>Citrix XenApp Plugin for Hosted Apps</td>
</tr>
<tr>
<td>Support for Citrix XenDesktop</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Desktop Receiver Embedded Edition 10.250</td>
</tr>
<tr>
<td>Support for Windows Vista and Internet Explorer 7.0</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server Clients 10.1 for Windows</td>
</tr>
<tr>
<td>Web Interface feature</td>
<td>Software requirements</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User change password</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Program Neighborhood Agent 10.1</td>
</tr>
<tr>
<td>Support for streamed applications</td>
<td>Citrix Presentation Server 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Streaming Client 1.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Program Neighborhood Agent 10.0</td>
</tr>
<tr>
<td>AD FS support</td>
<td>Citrix Presentation Server 4.5</td>
</tr>
<tr>
<td>Access Control Policy support</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Access Gateway 4.2 with Advanced Access Control</td>
</tr>
<tr>
<td></td>
<td>Citrix MetaFrame Presentation Server Clients for 32-bit Windows, Version 9.0</td>
</tr>
<tr>
<td>Account self-service</td>
<td>Citrix Password Manager 4.0</td>
</tr>
<tr>
<td>Session reliability</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix MetaFrame Presentation Server Clients for 32-bit Windows, Version 9.0</td>
</tr>
<tr>
<td>Workspace control</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix MetaFrame Presentation Server Client for 32-bit Windows, Version 8.0</td>
</tr>
<tr>
<td>Smart card support</td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix ICA Client for 32-bit Windows 6.30</td>
</tr>
<tr>
<td>Secure Gateway support</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0 for UNIX Operating Systems</td>
</tr>
<tr>
<td></td>
<td>Citrix ICA Client for 32-bit Windows 6.20</td>
</tr>
<tr>
<td>NDS authentication</td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix ICA Client for 32-bit Windows 6.20</td>
</tr>
<tr>
<td>DNS addressing</td>
<td>Citrix XenDesktop 2.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.0 for UNIX Operating Systems</td>
</tr>
<tr>
<td></td>
<td>Citrix ICA Client for 32-bit Windows 6.20</td>
</tr>
</tbody>
</table>
### General Configuration Requirements

Servers must be members of a server farm. The servers in the farm must have resources (applications, content, and/or desktops) published. For information about server farm membership and publishing resources in a server farm, see the appropriate Administrator’s Guide.

XenApp for UNIX servers must also have applications published. In addition, these applications must be configured for use with the Web Interface. See the *Citrix XenApp 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

The Citrix plugins must be present on the server for Web-based installation of the plugins. See “Client Device Requirements” on page 26 for information about supported plugin versions and “Copying Plugin Installation Files to the Web Site” on page 89 for information about copying the plugins to the Web Interface server.
On Windows Platforms

You can install the Web Interface on the following Windows platforms:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web server</th>
<th>Runtime/JDK</th>
<th>Servlet engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 x64 Editions</td>
<td>Internet Information Services 7.0</td>
<td>.NET Framework 3.5* Visual J#.NET 2.0 Second Edition*</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 x64 Editions with Service Pack 2</td>
<td>Internet Information Services 6.0 in 32-bit mode</td>
<td>ASP.NET 2.0</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 with Service Pack 2</td>
<td>Internet Information Services 6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apache 2.2.x</td>
<td>Sun 1.6.x</td>
<td>Apache Tomcat 6.0.x</td>
</tr>
</tbody>
</table>

*The Web Interface is also compatible with existing installations of .NET Framework 2.0 with Service Pack 1 and Visual J#.NET 2.0 on both x86 and x64 editions of Windows Server 2003 with Service Pack 2 running Internet Information Services 6.0.

If you want to use Microsoft Internet Information Services (IIS), you must configure your server to add the appropriate server role and install IIS and ASP.NET (which is a subcomponent of IIS). If IIS is not installed when you install .NET Framework, you must install IIS and reinstall the Framework, or install IIS and run the aspnet_regiis.exe -i command in the C:\Windows\Microsoft.NET\Framework\Version directory. The .NET Framework and J# redistributable files are included in the \Support folder on the XenApp and XenDesktop installation media.

On UNIX Platforms

You can install the Web Interface on the following UNIX platforms:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web server</th>
<th>JDK</th>
<th>Servlet engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 5 Advanced Platform 32-bit</td>
<td>Apache 2.2.x</td>
<td>Sun 1.6.x</td>
<td>Apache Tomcat 6.0.x</td>
</tr>
<tr>
<td>IBM AIX 5L Version 5.3</td>
<td>IBM WebSphere Application Server 6.1</td>
<td>IBM Version 5.0</td>
<td>IBM WebSphere</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>Sun Java System Application Server Platform Edition 9.0</td>
<td>Sun 1.5.x</td>
<td>Sun Java System Application Server</td>
</tr>
</tbody>
</table>
## User Requirements

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 7.x (32-bit mode)</td>
<td>Windows Vista 64-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional x64 Edition</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 x64 Editions</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 x64 Editions with Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 with Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Fundamentals for Legacy PCs</td>
</tr>
<tr>
<td>Internet Explorer 6.x (32-bit mode)</td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td>Mozilla Firefox 3.0</td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 with Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 5 Desktop</td>
</tr>
<tr>
<td></td>
<td>Mac OS X Leopard</td>
</tr>
<tr>
<td>Mozilla Firefox 2.0</td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 with Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 5 Desktop</td>
</tr>
<tr>
<td></td>
<td>Mac OS X Leopard</td>
</tr>
<tr>
<td>Safari 3.0</td>
<td>Mac OS X Leopard</td>
</tr>
<tr>
<td>Safari 2.0</td>
<td>Mac OS X Tiger</td>
</tr>
<tr>
<td>Mozilla 1.7</td>
<td>Solaris 10</td>
</tr>
</tbody>
</table>
Requirements for Access to Streamed Applications

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 7.x (32-bit mode)</td>
<td>Windows Vista 64-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional x64 Edition</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 x64 Editions</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 x64 Editions with Service Pack 2</td>
</tr>
<tr>
<td>Internet Explorer 6.x (32-bit mode)</td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td>Mozilla Firefox 3.0</td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 with Service Pack 2</td>
</tr>
<tr>
<td>Mozilla Firefox 2.0</td>
<td>Windows Vista 32-bit Editions</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 with Service Pack 2</td>
</tr>
</tbody>
</table>

Requirements for Other Client Devices

Users can access the Web Interface on Windows-based terminals, personal digital assistants (PDAs), and hand-held devices with the following configurations:

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating system</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-TEN Glofiish X500</td>
<td>Windows Mobile 6</td>
<td>Pocket Internet Explorer</td>
</tr>
<tr>
<td>HP iPAQ rx1950</td>
<td>Windows Mobile 2005</td>
<td></td>
</tr>
<tr>
<td>HP t5530</td>
<td>WinCE 6.0</td>
<td>Internet Explorer 6.0</td>
</tr>
<tr>
<td>WYSE V30</td>
<td>WinCE 5.0</td>
<td></td>
</tr>
<tr>
<td>WYSE V90</td>
<td>Windows XP Embedded with Service Pack 1</td>
<td></td>
</tr>
<tr>
<td>Symbian Nokia E61/E70</td>
<td>Symbian Nokia</td>
<td>Symbian Browser</td>
</tr>
</tbody>
</table>
Client Device Requirements

To operate with the Web Interface, your client devices must have, at minimum, either a supported plugin or a supported Web browser with the Java Runtime Environment. All plugins that ship on the XenApp and XenDesktop installation media are compliant with the Web Interface. The plugins are also available for free download from the Citrix Web site.

Citrix recommends that you deploy the most recent plugins to your users to ensure that they can take advantage of the latest features. The features and capabilities of each plugin differ—for information about supported plugin features, see the appropriate Administrator’s Guide for the plugin 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 for installing the Web Interface on each supported platform.

Installation Overview

You install the Web Interface using the XenApp or XenDesktop installation media.

You can install the Web Interface on the following platforms:

- A supported Windows operating system running:
  - Microsoft Internet Information Services (IIS)
  - Apache Tomcat
- A supported UNIX operating system running:
  - Apache Tomcat
  - IBM WebSphere
  - Sun Java System Application Server

For more information about how to install the Web Interface, see “Installing the Web Interface on Internet Information Services” on page 27 and “Installing the Web Interface on Java Application Servers” on page 30.

Security Considerations

If you plan to install the Web Interface on a Windows-based server, Citrix recommends that you follow Microsoft standard guidelines for configuring your Windows server. For UNIX implementations, follow the manufacturer’s recommendations for your particular operating system.
Viewing the Citrix XML Service Port Assignment
During Web Interface site creation (IIS) or .war file generation (Java), you are prompted for the port number that the Citrix XML Service is using. The Citrix XML Service is the communication link between the server farm and the Web Interface server. This section explains how to view the port number that the Citrix XML Service is using.

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 Action menu, click Properties.
4. Select XML Service to view the port assignment.

If during XenApp or XenDesktop installation you choose the option to share Internet Information Services’ TCP/IP port with the Citrix 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 Services’ WWW Service. By default, the WWW Service uses port 80.

To view the Citrix XML Service port assignment on UNIX platforms
On XenApp for UNIX servers, type ctxnfusesrv -l at a command prompt to view port information.

Note: If necessary, you can change the port used by the Citrix XML Service on the server. For more information, see the appropriate Administrator’s Guide.

Installing the Web Interface on Internet Information Services
Before installing the Web Interface, you must configure your server to add the Web server role and install IIS and ASP.NET.

To use IIS 7.0 on Windows Server 2008, install the Web Server (IIS) role and then enable the following role services:

- Web Server > Application Development > ASP.NET
- Web Server > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility
If you plan to enable pass-through, pass-through with smart card, and/or smart card authentication, you will also need to install the following role services:

- For pass-through and pass-through with smart card authentication, enable **Web Server > Security > Windows Authentication**
- For smart card authentication, enable **Web Server > Security > Client Certificate Mapping Authentication**

To use IIS 6.0 on Windows Server 2003, add the **Application server (IIS, ASP.NET)** role and enable ASP.NET.

On IIS, 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 one, you might not be able to run the Web Interface.

After configuring your server role, ensure that .NET Framework 3.5 and Visual J#.NET 2.0 Second Edition are installed and then install the Access Management Console. For more information about installing the Access Management Console, see the *Citrix XenApp Administrator’s Guide*.

Although Citrix recommends that you upgrade to .NET Framework 3.5 and Visual J#.NET 2.0 Second Edition, the Web Interface can also be installed on Windows Server 2003/IIS 6.0 deployments with existing installations of .NET Framework 2.0 with Service Pack 1 and Visual J#.NET 2.0.

If you are upgrading from an earlier version of the Web Interface, back to and including Version 4.0, the installer prompts you to back up your existing sites before upgrading them.

**Important:** Starting from Version 5.0 of the Web Interface, Conferencing Manager Guest Attendee sites are no longer supported. If you upgrade from an earlier version of the Web Interface, the installer will remove any existing Conferencing Manager Guest Attendee sites on your server.

---

**To install the Web Interface on Internet Information Services**

1. Log on as an administrator.

   If you are installing the Web Interface from the XenApp or XenDesktop installation media, insert the disc in your Web server’s optical drive.

   If you downloaded the Web Interface from a download site, copy the file WebInterface.exe to your Web server. Double-click the file.

2. Select your language from the list. The language of your operating system is detected and appears as the default selection. Click **OK**.

3. On the **Welcome** page, click **Next**.
4. On the **License Agreement** page, select **I accept the license agreement** and click **Next**.

5. On the **Common Components** page, browse to a location for the common Web Interface components (the default is `C:\Program Files (x86)\Citrix\Web Interface\Version`). Click **Next**.

6. On the **Clients** page, select **Copy the clients to this computer**. Click **Browse** to search the installation media or your network for the plugin setup files.

   Setup copies the contents of the `\Clients` directory on the installation media or network share to the Web Interface `\Clients` directory, typically `C:\Program Files (x86)\Citrix\Web Interface\Version\Clients`. All Web sites created by the installation process assume that the Web server contains the plugin files in this directory structure.

   If you do not want to copy the plugins to the Web server during Web Interface installation, select **Skip this step**. You can copy the plugins to the server later.

7. Click **Next** to continue and click **Next** again to confirm that you are ready to begin the installation.

8. When the installation is complete, click **Finish**.

9. 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 40.

**Compatibility with Other Components on 64-bit Windows Platforms**

On 64-bit versions of Windows Server 2003, installation of Web Interface for Windows enables 32-bit Web extension support in IIS 6.0 and this disables 64-bit extension support. To avoid this issue, ensure that if you are installing Web Interface for Windows on a 64-bit version of Windows Server 2003, you install the Web Interface prior to installing any other Citrix software, including XenApp, XenDesktop, and the License Management Console. This particular order of installation allows the products to adapt to the 32-bit support in IIS 6.0. If you install these products in an incorrect order, the Web server may produce error messages when it is accessed, such as “Service unavailable.”

On 64-bit Windows Server operating systems, Web Interface for Windows may not be compatible with other software products that require 64-bit ISAPI filters, such as the Windows component RPC over HTTP proxy. You must uninstall RPC over HTTP proxy before installing the Web Interface.
To uninstall RPC over HTTP proxy on Windows Server 2008 x64 Editions
1. On the Windows Start menu, click Administrative Tools > Server Manager.
2. Select Features in the left pane.
3. On the Action menu, click Remove Features.
4. Clear the RPC over HTTP Proxy check box and click Next.
5. Click Remove to uninstall RPC over HTTP proxy and then restart your server.

To uninstall RPC over HTTP proxy on Windows Server 2003 x64 Editions
1. On the Windows Start menu, click Control Panel > Add or Remove Programs.
2. Select Add/Remove Windows Components.
3. Select Networking Services and click Details.
4. Select the RPC over HTTP Proxy check box and click OK.
5. Click Next to uninstall RPC over HTTP proxy and then restart your server.

Installing the Web Interface on Java Application Servers

This section describes how to install the Web Interface on Apache Tomcat. For other configurations, see the server documentation and any documentation for the server’s administration tool.

**Note:** If you are installing the Web Interface on IBM 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 file in accordance with the WebSphere Java 2 Security policy, otherwise, the Web Interface may not function correctly. This policy file is located in WEBSPHERE_HOME/AppServer/installedApps/NodeName/WARFileName.ear/META-INF.

Web Interface for Java Application Servers requires a servlet engine to function. To support the Web Interface, the Apache Web server requires an additional servlet engine such as Tomcat (note that Tomcat can be used as a stand-alone Web server or as a servlet engine).
To install the Web Interface on Tomcat

1. Copy the WebInterface.jar file from the Web Interface directory on the installation media to a temporary location.

2. From a command prompt, navigate to the directory where the installation file was downloaded and run the installer by typing `java -jar WebInterface.jar`.

3. Press ENTER to read the license agreement.

4. Type `Y` to accept the license agreement.

5. Select a site type from the list provided.

6. Specify the initial configuration for the site by answering the questions that appear on the screen.

7. A summary of the options you selected appears. If the site details are correct, type `Y` to create the .war file.
   The .war file is created and the plugins are copied from the installation media, if required.

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

Configuring the Security Policy on Sun Java System Application Servers

Before you can create XenApp Web sites configured to allow account self-service 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 configuration directory. For example, if Sun Java System Application Server is installed under `SunJavaApplicationServerRoot/AppServer` and the site is deployed in “domain1,” the file resides in `SunJavaApplicationServerRoot/AppServer/domains/domain1/config`. 
4. Add the following configuration before any generic grant blocks:

```java
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 file name of your site’s .war file; for example, “XenApp.”

5. Edit the launcher.xml file located in SunJavaApplicationServerRoot/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, visit the Knowledge Center at [http://support.citrix.com/](http://support.citrix.com/).

### Using Language Packs

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

- Resource files for sites
- User help
- Localized icons and images

On Windows, language packs can be added to a Web Interface installation by copying the tree or unpacking the files in the \languages directory, typically C:\Program Files (x86)\Citrix\Web Interface\Version\languages. To customize a language for a specific site, you can copy the language pack to the site’s location and modify it. The site then uses the modified language pack and other sites continue to use the default.

**Note:** To display Windows error messages in the correct language on IIS, you must install the appropriate language pack for Microsoft .NET Framework.
On Java application servers, extra language packs can be installed by moving them to the appropriate directory within the site and extracting the files.

The English language pack is used as the fallback language and must always be present on your server. Language packs are specific to the version of the Web Interface that the packs are supplied with and cannot be used with earlier or later versions.

For more information about using language packs, see the Web Interface SDK.

**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 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 sites on IIS, remove LanguageCode.lang (for example, ja.lang) from the \languages directory, typically C:\Program Files (x86)\Citrix\Web Interface\Version\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 sites on Java application servers, 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.

**Upgrading an Existing Installation**

You can upgrade from Version 4.0 or later of the Web Interface to the most recent version by installing the Web Interface from either the XenApp or XenDesktop installation media, or from Web download files.

You cannot downgrade to an earlier version of the Web Interface.

---

**Important:** Starting from Web Interface 5.0, Conferencing Manager Guest Attendee sites are no longer supported. If you upgrade from an earlier version of the Web Interface, the installer will remove any existing Conferencing Manager Guest Attendee sites on your server.

---

**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 to interact with 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 153
- For information about how to configure the Web Interface using the console or WebInterface.conf file, see “Configuring Sites Using the Console” on page 39 or “Configuring Sites Using the Configuration File” on page 133
- For information about configuring the Web Interface to use AD FS, see “Configuring Active Directory Federation Services Support for the Web Interface” on page 155
- For information about security considerations, see “Configuring Web Interface Security” on page 119
- To extend and customize Web Interface functionality, see the Web Interface SDK

### Troubleshooting the Web Interface Installation

On Windows platforms with IIS, you can use the Repair option to troubleshoot Web Interface installation. If the Repair option does not fix the problem or this option is unavailable (for example, on Java application server installations), try uninstalling and then reinstalling the Web Interface. For more information, see “Uninstalling the Web Interface” on page 35. You must recreate all your sites after reinstalling the Web Interface.

#### 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 the screen.
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 them 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 Internet Information Services

To uninstall the Web Interface on Internet Information Services

1. On the Windows Start menu, click Control Panel > Programs and Features.
2. Select Citrix Web Interface and click Uninstall.
3. Follow the instructions on the screen.

Uninstalling the Web Interface on Java Application Servers

If your Web server provides a tool to help you uninstall Web applications, follow the recommended procedure to uninstall the Web Interface. Alternatively, you can uninstall the Web Interface manually.

To uninstall the Web Interface on Tomcat

1. From a command prompt, navigate to the directory to which you originally copied the .war file.
2. Stop your Web server and delete the .war file.
   You may also need to delete the directory in which the .war file is expanded. Normally, this is in the same directory as the .war file and has the same name. For example, the contents of “mysite.war” is expanded into a directory called /mysite.

Note: When you uninstall the Web Interface, some files may remain on the server. For more information about which files remain, see the Citrix XenApp Readme file.
Getting Started with the Web Interface

This section explains how to configure the Web Interface using the Access Management Console or the Web Interface configuration file. Topics include:

- Deciding Which Configuration Method to Use
- Site Configuration Sources
- 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.

Using the Access Management Console

You can use the Access Management Console to configure sites created on Windows platforms. 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 install the Access Management Console on computers running:

- Windows Server 2008/Windows Server 2008 x64 Editions
- Windows Server 2003 R2/Windows Server 2003 R2 x64 Editions
- Windows Server 2003 with Service Pack 1/Windows Server 2003 x64 Editions with Service Pack 1
- Windows Vista 32-bit Editions
- Windows XP Professional with Service Pack 2
- Windows 2000 Professional with Service Pack 4

**Note:** You must ensure either .NET Framework 3.5 or .NET Framework 2.0 with Service Pack 1 is installed on the computer on which you install the Access Management Console.

For information about configuring the Web Interface using the console, see “Configuring Sites Using the Console” on page 39 and the console Help system.

### Using Configuration Files

You can use the following configuration files:

- **Web Interface configuration file.** The Web Interface configuration file, WebInterface.conf, allows you to change many Web Interface properties; it is available on both Microsoft Internet Information Services (IIS) and Java application servers. You can use this file to perform day-to-day administration tasks and customize many more settings. Edit the values in the WebInterface.conf file and save the updated file to apply the changes.

  For information about configuring the Web Interface using the WebInterface.conf file, see “Configuring Sites Using the Configuration File” on page 133.

- **Citrix XenApp configuration file.** You can configure Citrix XenApp using the config.xml file located on the Web Interface server.

### Site Configuration Sources

The Web Interface stores the configuration for new sites in local files on the Web Interface server. If you are using the Access Management Console for site management, you must install the console on the Web Interface server.
Throughout this guide, sites storing their configuration data in local files are referred to as *locally configured sites*.

**Note:** On Java application servers, you manage locally configured sites by editing the WebInterface.conf file.

---

**Centralized Configuration**

In previous versions of the Web Interface, the Configuration Service provided a mechanism for retrieving and persisting site configuration data by storing it in a centralized location on any server in a farm.

Throughout this guide, sites using the Configuration Service are referred to as sites using *centralized configuration*.

In the current version of the Web Interface, centralized configuration is deprecated and the creation of centrally configured sites is no longer supported, although you can still administer and upgrade existing sites. Citrix recommends that you convert your existing centrally configured sites to use local configuration.

To access existing site configurations stored in a centralized location, you must log on to the computer running the Access Management Console as a Citrix administrator who has been granted permission to edit centrally configured Web Interface sites. Full administrators have these permissions by default, but for custom administrators, you may need to assign them using the **Modify administrator properties** task in the XenApp snap-in to the Access Management Console. For more information about modifying administrator permissions for XenApp, see the *Citrix XenApp Administrator’s Guide*.

---

**Configuring Sites Using the Console**

The Access Management Console allows you to create and configure XenApp Web and XenApp Services sites. The console allows you to modify many of the settings quickly and easily. You can also use the console to manage legacy Conferencing Manager Guest Attendee sites, but you cannot create new sites.

When using the console, some Web Interface settings may be disabled if their values are not relevant to the current configuration and the corresponding WebInterface.conf settings are reset to their default values. Citrix recommends that you create regular backups of the WebInterface.conf and config.xml files for your sites.
Getting Help
You can display the Help system for the Access Management Console by clicking Help > Help Topics or by clicking Help on the toolbar. Alternatively, you can access the Help system at any time by pressing F1 or by right-clicking any node in the left pane and selecting Help.

Getting Started with the Access Management Console
Run the console from Start > All Programs > Citrix > Management Consoles > Access Management Console.
For more information about the Access Management Console, see the Citrix XenApp 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 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 specify the following:

• The component products you want discovery to search for new items
• Whether or not to retrieve centralized configuration for sites on your computer
• Details of farms running XenApp and Desktop Delivery Controller

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

Note: After installing the latest version of the Web Interface, earlier versions of the Access Management Console no longer discover centrally configured sites. To avoid this issue, update all your console installations to the latest version and then run the discovery process to discover previously created sites.
To configure and run discovery

1. On the Start menu, click All Programs > Citrix > Management Consoles > Access Management Console.

2. On the Welcome page of the Configure and Run Discovery wizard, click Next. If this page does not appear automatically, click Configure and run discovery.

3. On the Select Products or Components page, ensure that the Web Interface check box is selected and click Next.

4. On the Configuration Servers page, choose one of the following options:
   • If you want to discover and create sites whose configuration is stored in local files or if the servers running the Configuration Service are behind a firewall, select Discover sites installed on this computer.
   • If you want to discover and/or upgrade sites whose configuration is stored in a centralized location, select Contact the following servers running the Configuration Service. List the servers running the Configuration Service in the Servers box.

   **Note:** Centralized configuration is deprecated. The creation of centrally configured sites is no longer supported, although you can still administer and upgrade existing sites. Citrix recommends that you convert your existing centrally configured sites to use local configuration.

5. Click Next.

6. On the Preview Discovery page, click Next.

7. If the Configure and Run Discovery wizard does not close automatically, click Finish.

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

You can create sites using only the instance of the Access Management Console installed on the Web Interface server. To perform remote discovery of centrally configured sites, you must use an instance of the Access Management Console installed on a computer that is a member of the same domain or workgroup that contains the Configuration Service.

When discovery is complete, existing sites appear under the Web Interface node in the left pane and you are ready to create new sites and administer existing sites.
Creating Sites

After running discovery, you can use the console to create sites to provide users with access to published resources using either a Web browser or Citrix XenApp.

Creating Sites on Internet Information Services

Use the Create site task to create one of the following sites:

- **XenApp Web.** For users accessing published resources using a Web browser.
- **XenApp Services.** For users accessing published resources using Citrix XenApp.

You use this task to specify the IIS location in which the site is hosted, 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.

**To create a site**

1. Click Web Interface in the left pane.
2. Click Create site.
3. Select the type of site you want to create.
4. Specify the URL for the site.
5. Follow the instructions on the screen to create the site.
6. Click Finish.

Creating Sites on Java Application Servers

On Java application servers, run the Web Interface installer before creating each site. The installer 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). You can modify sites by editing the contents of the unpacked .war file and remove sites by deleting the .war file.
Specifying the Authentication Point

When creating a XenApp Web site using the console, you must specify the authentication point, which is the point in your deployment where user authentication takes place.

Authentication at the Web Interface

You can enable authentication of users by the Web Interface using a range of built-in authentication methods, including explicit, pass-through, and smart card authentication.

For more information about Web Interface authentication methods, see “Configuring Authentication for the Web Interface” on page 63.

Authentication at an Active Directory Federation Services Account Partner

You can enable the resource partner of an Active Directory Federation Services (AD FS) deployment to launch XenApp applications. This allows you to provide users on the resource partner with access to published applications.

If you are planning to create AD FS integrated sites, be aware of the following:

- XenDesktop does not support AD FS authentication.
- AD FS support is not available with Web Interface for Java Application Servers.
- The Client for Java and embedded Remote Desktop Connection (RDP) software are not supported for accessing AD FS integrated sites.
- AD FS integrated sites support authentication using AD FS only. Other methods of authentication are not supported.
- After an AD FS integrated site is created, you cannot configure that site to use built-in authentication or authentication by Access Gateway instead of AD FS.

For more information, see “Configuring Active Directory Federation Services Support for the Web Interface” on page 155.
Authentication at Access Gateway

You can enable authentication and single sign-on of users by Access Gateway Advanced or Enterprise Edition. User access to published resources is controlled through the use of access control policies and conditions.

By default, pass-through authentication is enabled for users who access the Web Interface using Access Gateway. Users log on using Access Gateway and do not have to reauthenticate to the Web Interface to access their published resources. To increase security, you can disable pass-through authentication by selecting the **Prompt users for password before displaying published resource set** check box.

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

**Note:** Support for Access Gateway authentication is not available with Web Interface for Java Application Servers.

Recommended Deployment for Access Gateway

The recommended configuration for a deployment of Access Gateway Advanced Edition in combination with the Web Interface is illustrated below.

*The figure shows the recommended deployment for using Access Gateway Advanced Edition with the Web Interface.*
In this deployment, XenApp/Desktop Delivery Controller, the Web Interface, and Advanced Access Control (a component of Access Gateway Advanced Edition) are all installed on servers within the internal network. The Access Gateway appliance is installed in the demilitarized zone (DMZ). For Access Gateway Advanced Edition, an instance of the Logon Agent is installed when Advanced Access Control is installed. The Logon Agent provides the user interface for logging on to a server in your farm.

A typical deployment using Access Gateway Enterprise Edition is configured similarly to the diagram above, except that there is no need for a server running the Advanced Access Control software. In this case, the Access Gateway appliance is installed in the DMZ and communicates directly with the Web server located within the internal network.

When users log on, they are authenticated by Access Gateway and directed to their published resources, subject to the access policies that you configure.

**Making Published Resources Available to Users**

With Access Gateway, users log on to a logon point to gain access to their published resources. You make published resources available to users by configuring a logon point to provide access to a XenApp Web site.

Access Gateway provides several methods for integrating XenApp Web sites created with the Web Interface, including:

- A XenApp Web site embedded within the Access Interface. When the Access Interface is selected as the default home page, a XenApp Web site appears alongside file shares, access centers, and Web applications.

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

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

  This option is available only if you are running Access Gateway Enterprise 4.0 with Access Gateway Enterprise Hotfix AAC400W001 applied or Citrix Access Gateway 4.2 with Advanced Access Control or later.
To integrate a XenApp Web site

Complete the following steps:

1. Configure XenApp or Desktop Delivery Controller to communicate with Access Gateway.

2. In Access Gateway, create a Web resource for the XenApp Web 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 XenApp Web site.

4. Provide access to the XenApp Web site in one of the following ways:
   - If you want to display the site as the default home page, configure a logon point to show the application with the highest display priority as the home page. Then, configure the XenApp Web site as the application with the highest priority.
   - If you want to embed the site within the Access Interface, configure a logon point to show the Access Interface as the home page. The XenApp Web site is embedded as a frame within the Access Interface.

Note: Because the Access Gateway Access Interface can display only one XenApp Web 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 Administrator’s Guide.

Complete the following steps for the Web Interface.

1. Select At Access Gateway when specifying the point of authentication for the site.

2. Type the URL of the Access Gateway authentication service in the Authentication service URL box.

In both the Web Interface and Access Gateway, ensure the workspace control and session time-out settings are configured correctly.
Coordinating Web Interface and Access Gateway Settings

Certain XenApp and XenDesktop settings can be configured within the Web Interface and Access Gateway. However, because a XenApp Web site integrated with Access Gateway can be referenced by more than one logon point, it is possible for one logon point to embed a XenApp Web site within its Access Interface while another logon point displays the site as its default home page. This can cause conflicts with certain published resource settings.

To ensure your settings work as intended, follow the instructions below:

• **Workspace control.** Disable all Access Gateway workspace control settings for logon points that have a XenApp Web 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 required.

• **Session time-out.** Ensure all logon points use the same settings as the XenApp Web site.

Authentication at a Third Party Using Kerberos

You can use a third-party federation or single sign-on product to authenticate users and map their identities to Active Directory user accounts. Kerberos can then be used for single sign-on to the Web Interface.

For more information about Kerberos, see the *Citrix XenApp Administrator’s Guide*.

Authentication at the Web Server

You can enable authentication of users at the Web server using Kerberos.

For more information about Kerberos, see the *Citrix XenApp Administrator’s Guide*.

Specifying Initial Configuration Settings for a Site

After creating a site with the console, 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 the Specify Initial Configuration wizard to configure communication with one or more server farms and specify the types of published resources available to users.
Specifying Server Farms
When configuring a new site, you must enter details of the server farms that will provide published resources for users of the site.
You can update these settings at any time using the Manage server farms task.
For more information about configuring communication with server farms, see “Managing Servers and Farms” on page 55.

Specifying Authentication Methods
When configuring a new XenApp Web site created with the authentication point At Web Interface, you can specify how users will authenticate when logging on to the Web Interface.
You can update these settings at any time using the Configure authentication methods task.
For more information about configuring authentication, see “Configuring Authentication for the Web Interface” on page 63.

Specifying Domain Restrictions
When configuring a new XenApp Web site created with the authentication point At Web Interface, you can restrict access to users in particular domains.
You can update these settings at any time using the Configure authentication methods task.
For more information about configuring domain restrictions, see “Configuring Domain Restriction Settings” on page 65.

Specifying the Appearance of the Logon Screen
When configuring a new XenApp Web site, you can specify the style for users’ logon screens. Choose between a minimalistic layout where only the appropriate logon fields appear and a layout that includes the navigation bar.
You can update this setting at any time using the Customize Web site appearance task.
For more information about customizing the appearance of the user interface, see “Customizing the Appearance for Users” on page 107.
Specifying the Types of Published Resources Available to Users

When configuring a new site, you must specify the types of published resources that you want to make available on the site. The Web Interface provides users with access to published resources (applications, content, and desktops) through a standard Web browser or through Citrix XenApp. Integration with the Citrix application streaming feature allows users to stream applications to their desktops and open them locally.

You can grant users access to published resources as follows:

- **Remote.** Users access applications, content, and desktops hosted on remote servers.
- **Streaming.** Users stream applications to their desktops and open them locally.
- **Dual mode streaming.** Users stream applications to their desktops and open them locally or, alternatively, virtualize them from XenApp. If streamed applications are not available, remote versions are accessed.

You can update this setting at any time using the Manage published resource types task.

For more information about plugin types, see “Managing Plugin Deployment” on page 87.

Upgrading Existing Sites

If you are upgrading your installation from an earlier version of the Web Interface, back to and including Version 4.0, support is provided for upgrading existing access platform and Program Neighborhood Agent Services sites.

**Note:** The Web Interface no longer supports Conferencing Manager Guest Attendee sites. If you upgrade from an earlier version of the Web Interface, any existing Conferencing Manager Guest Attendee sites are removed by the Web Interface installer.
Existing access platform and Program Neighborhood Agent Services sites are upgraded 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.** Although you can upgrade your existing centrally configured sites, Citrix recommends that you convert them to use local configuration rather than simply upgrading because the creation of centrally configured sites is no longer supported.

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

- **Grouped sites.** Because grouped sites use centralized configuration, which is deprecated, Citrix recommends that you ungroup the sites and convert them to use local configuration rather than simply upgrading.

Upgrading a site group is carried out in the same way as for other centrally configured sites. However, because sites in a group may exist on different servers, after installation, you may find either of the following occurs:

- **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 message 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 message appears in the console. You can complete the upgrade process by either running the installer and upgrading the remaining sites or removing the sites that were not upgraded from the group.
Converting Centrally Configured Sites to Local Configuration

Because centralized configuration is deprecated and the creation of centrally configured sites is no longer supported, Citrix recommends that you convert your existing centrally configured sites to use local configuration. You can edit a centrally configured site to change its configuration source to local files. When you switch to local configuration, the existing configuration is obtained from the centralized configuration location and populates the new local files accordingly.

For more information about specifying site configuration sources in the Access Management Console, see “Using Local Site Tasks” on page 53.

On IIS, you can also import and export existing configuration files to use with other sites using the **Import configuration** and **Export configuration** tasks. On Java application servers, however, the installer cannot create sites using local configuration files based on existing site configurations.

To convert grouped sites, you must remove sites from the group using the **Remove sites from group** task; the group configuration is used for the removed site. Alternatively, use the **Ungroup** task to remove all sites from the group.

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 appear in the task pane. Tasks are either performed using wizards or by setting options in dialog boxes. To run a task, either click the task name in the task pane or right-click the site you want to configure and select a task from the context menu.
Some tasks are available only for certain site types and configurations. Details of which tasks are available for which site are given in the table below.

<table>
<thead>
<tr>
<th>Task</th>
<th>XenApp Web sites</th>
<th>XenApp Services sites</th>
<th>AD FS integrated sites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remote and dual mode</td>
<td>Streaming only</td>
<td>Remote and dual mode</td>
</tr>
<tr>
<td>Change session options</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Clean up configuration</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Configure authentication methods</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Control diagnostic logging</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Customize Web site appearance</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Edit client-side proxy</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Export configuration</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Export client configuration</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Edit secure client access settings</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Import configuration</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Local site tasks</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manage access method</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Manage published resource refresh</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Manage shortcuts</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Manage published resource types</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manage client deployment</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Manage server farms</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manage server settings</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Manage session preferences</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manage site grouping</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manage workspace control</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Modify apply changes URL</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Upgrade configuration</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
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 Web Interface server. 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 configure sites using centralized configuration (the configuration files for the site are stored on a remote server) to use local configuration (the configuration files for the site are stored on the local computer.) The site’s existing configuration is copied to the new configuration source.

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 were created for the site and you run the Repair site task, these customized files are 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.

Making the Web Interface Available to Users

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

On Java application 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 /WARFileName, where WARFileName is the first part of the file name of your site’s .war file.
Accessing a Site Directly

If users access a site directly or through Access Gateway Enterprise Edition, you can enable published resource URL support. This allows users to create persistent links to published resources accessed using the Web Interface. These links can be added to the user’s shortcuts list or desktop. Enable support for published resource URLs by clicking Manage access method and selecting the Allow users to access published resources using browser bookmarks check box.

**Important:** Enabling this feature for users disables cross-site request forgery protection.

Making the Logon Screen the Default on Internet Information Services

You can set the Web Interface logon screen to be the default for users of the Web server so that the URL is http://ServerName/. To do this, select the Set as the default page for the IIS site check box when you create the site or at any time thereafter in the Manage IIS hosting task.

What to Do Next

- For more information about deploying Citrix plugins to Web Interface users, see “Managing Plugin Deployment” on page 87
- For information about security considerations, see “Configuring Web Interface Security” on page 119
Managing Servers and Farms

This section 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 servers running the Citrix XML Service. 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 in different domains, a two-way trust must be enabled between these domains. If a farm is running on UNIX, each user must have the same user name and password for all the farms in the deployment. If the user name and password cannot be authenticated to all of the farms specified, users receive an invalid credentials error message.

Multiple server farm functionality is transparent to users because they are not informed that their resource set is an aggregation from multiple server farms. Published resources (applications, content, and desktops) from multiple server farms appear in the same way as a single farm; folders appear first, followed by the icons. Consequently, published resources with the same name from multiple server farms appear in an arbitrary position in the user’s resource set. Citrix recommends that you ensure published resource names are unique across the server farms; for example, by publishing resources in folders with different names.

The Web Interface acquires resource data from all server farms before displaying published resources; each server farm is contacted in the order in which it appears in the configurations. As a result, a server farm that is slow to respond impacts overall responsiveness when obtaining resource 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 XenApp for UNIX farms are aggregated by a single site with XenApp for Windows and/or Desktop Delivery Controller farms, only the Windows password can be changed

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

When aggregating multiple farms, ensure that the first farm listed in the configuration is running either Citrix Presentation Server 4.0 or later, Citrix Desktop Server 1.0, or Citrix XenDesktop 2.0.

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 is 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 and transport types.

To add a server farm

1. Click Manage server farms.
2. Click Add.
3. Enter a name for the server farm in the Farm name box.
4. In the Server Settings area, click Add to specify a server name. To change a server name, select the name from the list and click Edit. To remove a server name, select the name and click Remove.
5. If you specify more than one server name, select a name from the list and click Move Up or Move Down to place these in the appropriate failover order.
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 Web Interface does not attempt to contact with the failed server until the time specified in the Bypass any failed server for box elapses, but communication continues with the remaining servers on the Servers list.

By default, a failed server is bypassed for one hour. If all servers on the list fail to respond, the Web Interface retries the servers every 10 seconds.

To configure fault tolerance
1. Click Manage server farms.
2. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.
3. On the Servers list, place the servers in order of priority. Select a name from 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.

Enabling Load Balancing Among 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 on 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 Manage server farms.
2. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.
3. On the Servers list, add the servers that you want to use for load balancing. For information about how to add servers, see “Configuring Server Settings” on page 56.
4. Select the Use the server list for load balancing check box.
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 in a Farm

You can use the Manage server farms task to specify how the Citrix XML Service transports data between the Web Interface and the server running XenApp or Desktop Delivery Controller. The Citrix XML Service is a component of XenApp and Desktop Delivery Controller that acts as the contact point between the server farm and the Web Interface server. 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 users to the server farm, you can change the ticket lifetime. 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 server.

To specify settings for all servers

1. Click Manage server farms.
2. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.
3. In the Communications Settings area, enter the port number in the XML Service port box. This port number must match the port number used by the Citrix XML Service.
4. From the Transport type list, choose 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 Secure Sockets Layer (SSL) or Transport Layer Security (TLS). You must ensure that the Citrix XML Service is set to share its port with Internet Information Services (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 XenApp or Desktop Delivery Controller 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 server running the Citrix SSL Relay. Ensure all the servers running the 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 server running XenApp or Desktop Delivery Controller.

6. To configure ticketing, click Ticketing Settings.
7. Enter the lifetime of tickets for remote plugins in the ICA ticket lifetime boxes.
8. Enter the lifetime of tickets for the Citrix XenApp Plugin for Streamed Apps in the Streaming ticket lifetime boxes.
9. Click OK to save your settings.

## Specifying Advanced Server Settings

Using the Advanced Farm Settings 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 Citrix 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 is available only for sites created with the authentication points At Web Interface or At Access Gateway. Socket pooling should not be used when the Web Interface is configured to use one or more servers running XenApp for UNIX.

**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 plugin to server for individual XenApp Services sites. This setting overrides any content redirection settings configured for XenApp.

When you enable content redirection from plugin to server, users running Citrix XenApp open published content and local files with applications published on servers. For example, a Citrix XenApp 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 plugin to server for XenApp Services sites.

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

**To enable content redirection**

1. In the **Manage Server Farms** dialog box, click **Advanced**.
2. In the **Content Redirection** area, select the **Enable content redirection** check box.

Configuring Citrix XML Service Communication

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

**To configure Citrix 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 is 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 Citrix XenApp 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 plugin and the Web Interface server 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 XenApp or Desktop Delivery Controller.

- **Allow users to customize the server URL.** The server URL points Citrix XenApp 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 box on the Server Options page of the XenApp plugin Options dialog box.

- **Configure automatic refresh.** You can define how often the plugin should refresh its configuration settings.

**To configure server communication settings**

1. Click **Manage server settings**.

2. To use secure communication between Citrix XenApp and a site, select **Use SSL/TLS for communication between clients and this site**.

3. To allow users to customize the server URL that points Citrix XenApp to the correct configuration file to use, select **Allow users to customize server URL**.

4. To configure how often Citrix XenApp refreshes its configuration settings, select **Schedule an automatic refresh every** and enter the refresh period in hours, days, weeks, or years.

**Specifying Citrix XenApp Backup URLs**

You can specify backup servers for Citrix XenApp 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 connected automatically to the backup server specified first on the **Backup site paths** list. If this server fails, Citrix XenApp attempts to contact the next server on 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 a Web Interface for Windows site, any backup sites must also be Web Interface for Windows sites.
To specify backup URLs
1. Click Manage server settings.
2. Click Backup.
3. Click Add.
4. Enter the URL for the site users are connected to in the Backup URL box. You can define a maximum of five backup URLs per site.
5. Click OK.
6. If you specify more than one backup server URL, select a URL from 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 Citrix XenApp.

To configure site redirection
1. Click Manage server settings.
2. Click Redirection.
3. Choose one of the following options:
   - 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 plugin launches, select Redirect the next time Citrix XenApp plugin starts
4. Enter the URL of the alternative site in the Redirect URL box.
5. Click OK.
Configuring Authentication for the Web Interface

This section describes the authentication methods available to users of the Web Interface. It also explains how to configure authentication between the Web Interface, XenApp/XenDesktop, and the XenApp plugin.

Topics in this section include:

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

Authentication Methods

Authentication takes place when a user accesses published resources (applications, content, and desktops). If authentication is successful, the user’s resource set appears.

You can configure the following authentication methods for the Web Interface:

• **Explicit (XenApp Web sites) or prompt (XenApp Services sites).** Users are required to log on by supplying a user name and password. User principal name (UPN), Microsoft domain-based authentication, and Novell Directory Services (NDS) are available. For XenApp Web sites, RSA SecurID and SafeWord authentication are also available.

  **Note:** Novell authentication is not available with Web Interface for Java Application Servers and is not supported by XenDesktop. Novell eDirectory is not supported for installation on Windows Server 2008.

• **Pass-through.** Users can authenticate using the credentials they provided when they logged on to their physical Windows desktop. Users do not need to reenter their credentials and their resource set appears 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 XenApp Administrator’s Guide*.

- **Pass-through with smart card.** Users can authenticate by inserting a smart card in a smart card reader attached to the client device. Citrix XenApp prompts users for their smart card PIN when they log on to the client device. After logging on, users can access their published applications and content without further logon prompts. Users connecting to XenApp Web sites are not prompted for a PIN. If you are configuring a XenApp 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 XenApp Administrator’s Guide*.

  **Note:** Because of the security enhancements introduced in Windows Vista, smart card users running Vista are required to provide their PINs when they launch an application, even if you enable pass-through with smart card authentication.

- **Smart card.** Users can authenticate using a smart card. The user is prompted for the smart card PIN.

  **Note:** Pass-through, pass-through with smart card, and smart card authentication are not available with Web Interface for Java Application Servers. XenDesktop does not support pass-through with Kerberos, pass-through with smart card, or smart card authentication.

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

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

  **Note:** XenDesktop does not support anonymous users.
Authentication Recommendations

If you plan to enable pass-through, pass-through with smart card, or smart card authentication, be aware of the following:

- If users log on to their computers using explicit credentials, do not enable smart card or pass-through with smart card authentication for those users to access the Web Interface.
- If users log on to their computers using smart cards and you want to enable pass-through authentication, select the option to use Kerberos authentication.

If you change the methods for authenticating to the Web Interface, error messages may appear to any users who are currently logged on. If any of these users are accessing the Web Interface through a Web browser, they must close and restart their browsers before attempting to log on again.

Configuring Authentication

Use the Configure authentication methods task to configure the ways in which users can authenticate to XenApp, XenDesktop, and the XenApp plugin.

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 Configure authentication methods.
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 to the following domains.
5. Click Add.

6. Enter the names of any domains you want to add to the domain restriction list in the Logon domain box.

   **Note:** To restrict access to users from specific domains, you must enter the same domain names on both the Domain Restriction and UPN Restriction lists. For more information, see “Configuring the Authentication Type” on page 66.

7. Click OK.

**Configuring Automatic Logon**

Use the Automatic Logon page to configure automatic logon settings for users accessing their published resources using pass-through, pass-through with smart card, and smart card authentication.

If anonymous authentication is the only authentication method enabled for users, they are logged on automatically regardless of the settings configured by either the administrator or the user.

**To configure automatic logon settings**

1. Click Configure authentication methods.

2. Click Properties.


4. Specify whether or not you want to allow users to log on automatically and whether or not they will be presented with the option to enable and disable automatic logon on their Account Settings screen.

5. 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 Novell Directory Services (NDS).

**To configure the authentication type**

1. Click Configure authentication methods.

2. Click Properties.
3. Select Authentication Type.
4. Specify the type of authentication that explicit users must use:
   • If you want to use either Microsoft domain-based authentication or UNIX authentication, select Windows or NIS (UNIX). See “To use domain-based authentication” on page 67.
   • If you want to use NDS authentication, select NDS. See “To use Novell Directory Services authentication” on page 68.

To use domain-based authentication
1. Specify the credential format for user logons. Choose one of the following options:
   • To allow users to enter their logon details in either user principal name (UPN) or domain user name format, select Domain user name and UPN
   • To specify that users must enter their logon details in domain user name format only, select Domain user name only
   • To specify that users must enter their logon details in UPN format only, select UPN only
2. Click Settings.
3. In the Domain Display area, configure the following settings:
   • Specify whether or not to display the Domain box on the logon screen
   • Specify whether the Domain box is prepopulated 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 box. If your farm comprises only XenApp for UNIX servers, 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 logon screen
4. In the **UPN Restriction** area, configure the following settings:
   - Specify whether or not all UPN suffixes are accepted. By default, all UPN suffixes are permitted.
   - Specify the UPN suffixes you want to accept.

   **Note:** To restrict access to users from specific domains, you must enter the same domain names on both the **Domain Restriction** and **UPN Restriction** lists. For more information, see “Configuring Domain Restriction Settings” on page 65.

---

**To use Novell Directory Services authentication**

1. Enter a name in the **Default tree name** box.
2. Click **Settings** and configure context restriction or contextless authentication, as appropriate.


3. If your users’ client devices have the Novell client installed and you want them to use their Windows credentials for pass-through authentication, select **Use Windows credentials**.

---

**Enabling Explicit Authentication**

If explicit authentication is enabled, users must have a user account and supply appropriate credentials to log on.

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

Explicit authentication is available only for XenApp Web sites.

**To enable explicit authentication**

1. Click **Configure authentication methods**.
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 expiration reminder options for users.

Some password settings are affected by other authentication settings you configure for a site:

- The At any time option is disabled if you select the RSA SecurID and Use Windows password integration options on the Two-Factor Authentication page.

- Selecting the Use reminder settings from Active Directory group policy option may mean that reminder settings are configured according to your current Windows policy. If your current Windows policy does not have a reminder period set, users will not receive a reminder to change their current password before it expires.

To configure password settings

1. Select Password Settings.

2. If you want users to be able to change their password within a Web Interface session, select the Allow users to change password check box.

3. To specify when users can change their password, choose one of the following options:

   - To allow users to change their password when it expires, select Only when it expires. When you enable this option, if users fail to log on to the Web Interface due to an expired password, they are redirected to the Change Password dialog box. After changing their password, users are logged on automatically 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 button appears on users’ Applications and Account Settings screens. When users click this button, a dialog box appears where users can enter a new password.
4. To configure a reminder message to notify users 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, weeks, or years in the **Remind users before expiry** boxes.

**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 “Enabling Secure Computing SafeWord on Internet Information Services” on page 80. For more information about configuring RSA SecurID authentication, see “Enabling RSA SecurID 6.0 Authentication on Internet Information Services 6.0” on page 81. For more information about configuring RADIUS authentication, see “Enabling RADIUS Authentication” on page 84.

**Configuring Account Self-Service**

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

Account self-service is available only to users accessing the Web Interface using HTTPS connections. If a user attempts to access the Web Interface using an HTTP connection, account self-service is unavailable. Users must restart their browser and access the Web Interface using an HTTPS connection.
Account self-service does not support UPN logons, such as username@domain.com.

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 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 at any time if you want to enable password reset functionality.
- For deployments that include Access Gateway, the site is configured to allow users direct access. Account self-service is not available for sites accessed using Advanced Access Control.
- For deployments that include Access Gateway, it is configured to use HTTPS when connecting to the Web Interface. This is necessary because information collected during the account self-service process may be sent from Access Gateway to the Web Interface as clear text. For more information, see the Citrix Access Gateway Administrator’s Guide.

Security Policy Considerations

Enabling account self-service for a site exposes sensitive security functions to anyone who can access it. If your site is accessible from the Internet, there are no restrictions on who can access these functions. If your organization has a security policy that restricts these functions for internal use only, you must ensure the site is not accessible outside of your internal network.

To configure account self-service

1. Select Account Self-Service.

2. Specify whether or not you want users to be able to reset their passwords or unlock their accounts.

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 appropriate credentials to log on.

Prompt authentication is available only for XenApp Services sites.
To enable prompt authentication

1. Click **Configure authentication methods**.
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 specify whether or not users can save their passwords and to configure password change options for users.

**To configure password settings**

1. Select **Password Settings**.
2. To allow users to save their passwords, select the **Allow users to save password** option.
3. If you want users to be able to change their password when it expires, select the **Allow users to change expired passwords by contacting** check box.
4. Specify the path through which the change password request is routed by choosing one of the following options:

   - If you want Citrix XenApp users to change their passwords by connecting directly to the domain controller, select **Domain controller directly**. This is the most secure option because the password change request is routed directly from the XenApp plugin to the domain controller, bypassing the Web Interface and XenApp/Desktop Delivery Controller.

   - If you would prefer Citrix XenApp users to change their passwords by connecting directly to the domain controller, but want to enable connections through the Web Interface and XenApp/Desktop Delivery Controller if the preferred connection method fails, select **Domain controller directly, with fallback to server farm**.

   - If you want Citrix XenApp users to change their passwords by connecting to the domain controller through the Web Interface and XenApp/Desktop Delivery Controller, select **Server farm**. This option ensures that when users change their passwords, Web Interface plus XenApp and/or Desktop Delivery Controller are updated with the new password. However, it is potentially less secure because the new password is routed through a greater number of network connections.
Enabling Pass-Through Authentication

Using the console, you can enable pass-through authentication for users logging on to their physical 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 physical Windows desktop. Users do not need to reenter credentials and their resource set appears automatically.

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, the Web Interface must be running on IIS and users must be running Internet Explorer 6.x or 7.x. For IIS 7.0 running on Windows Server 2008, ensure that the Web Server > Security > Windows Authentication role service is enabled for the Web Server (IIS) role.

**Important:** If your servers are running versions prior to Citrix MetaFrame XP Feature Release 2, users may be able to view all the published applications and content when using pass-through.

If users are using Clients for Windows versions prior to Version 6.30 and ICA encryption (SecureICA) is enabled, pass-through does not work. To use pass-through with ICA encryption, you must have the latest plugins. Pass-through authentication is not available with Web Interface for Java Application Servers.

**Important:** When a user accesses a resource, a file is sent to the plugin (in some cases using the Web browser as an intermediary). The file can contain a setting that instructs the plugin to send the user’s workstation credentials to the server. By default, the plugin does not honor this setting; however, there is a risk that if the pass-through feature is enabled on the Citrix XenApp Plugin for Hosted Apps, 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 Citrix XenApp Plugin for Hosted Apps

You must install the Citrix XenApp Plugin for Hosted Apps on your users’ client devices using an administrator account. The pass-through authentication feature is available only in the Citrix XenApp Plugin for Hosted Apps, which is included on the XenApp installation media. For security reasons, the Citrix XenApp Web Plugin does not include this feature. This means that you cannot use Web-based plugin installation to deploy plugins containing this feature to your users.

Step 2: Enabling Pass-Through for the Plugins

After installation, you must enable pass-through authentication for all plugins using group policy. Enabling pass-through authentication for the plugins is a two-step process. First, you add the icaclient template to the Group Policy Object Editor. Once added, you use this template to enable pass-through authentication for all plugins.

To add the icaclient template to the Group Policy Object Editor

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. Select the Administrative Templates node and, on the Action menu, click Add/Remove Templates.
4. Click Add and browse to the icaclient template file, icaclient.adm. This file is installed in the Configuration directory for the plugins, typically C:\Program Files\Citrix\ICA Client\Configuration.
5. Click Open to add the template and then click Close.

To enable pass-through authentication for all plugins

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. In the left pane, expand the Administrative Templates node.
5. Select Local user name and password.
7. Click the Setting tab and, in the Local user name and password area, select Enabled.

8. Verify that the Enable pass-through authentication check box is selected and click OK.

9. Ensure that all the above steps are completed for both the user and the computer in the Group Policy Object Editor.

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 resource set appears automatically.

Additionally, you can enable Kerberos with pass-through authentication for XenApp Web and XenApp Services sites. For XenApp Services sites, you can also specify Kerberos for pass-through with smart card authentication.

Note: XenDesktop does not support pass-through with Kerberos or pass-through with smart card authentication.

To enable pass-through authentication

1. Click Configure authentication methods.

2. Select the Pass-through check box.

3. Click Properties.

4. Select Kerberos Authentication.

5. If you want to enable Kerberos authentication for XenApp Web 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 authentication. For an example of how to configure smart card authentication in the Web Interface, see “Example: Enabling Smart Card Authentication for Users” on page 79.
Smart Card Support Requirements

To use smart card authentication, the Web Interface must be running on IIS and users must be running Internet Explorer 6.x or 7.x. For IIS 7.0 running on Windows Server 2008, ensure that the **Web Server > Security > Client Certificate Mapping Authentication** role service is enabled for the **Web Server (IIS)** role. Smart card authentication is not available with Web Interface for Java Application Servers or XenDesktop.

Secure Sockets Layer (SSL) must be enabled on the Web server because SSL must be used to secure communication between the browser and Web server. See the Web server documentation for further information.

If you want to enable smart card authentication (with or without other authentication methods), you must configure the logon screen 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.MyCompany.com:443/Citrix/XenApp.

For more information about client device requirements and server requirements for smart card authentication, see the **XenApp Plugin for Hosted Apps Administrator’s Guide** and the **Citrix XenApp Administrator’s Guide**.

Step 1: Installing the Citrix XenApp Plugin for Hosted Apps

You must install the Citrix XenApp Plugin for Hosted Apps on your users’ client devices using an administrator account. Smart card authentication is available only in the Citrix XenApp Plugin for Hosted Apps, which is included on the XenApp installation media. For security reasons, the Citrix XenApp Web Plugin does not include this feature. This means that you cannot use Web-based plugin installation to deploy plugins containing this feature to your users.

Step 2: Enabling Pass-Through for the Plugins

After installation, you must enable pass-through authentication for all plugins using group policy. Enabling pass-through authentication for the plugins is a two-step process. First, you add the icaclient template to the Group Policy Object Editor. Once added, you use this template to enable pass-through authentication for all plugins.

To add the icaclient template to the Group Policy Object Editor

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. Select the Administrative Templates node and, on the Action menu, click Add/Remove Templates.

4. Click Add and browse to the icaclient template file, icaclient.adm. This file is installed in the 'Configuration directory for the plugins, typically C:\Program Files\Citrix\ICA Client\Configuration.

5. Click Open to add the template and then click Close.

6. Ensure that all the above steps are completed for both the user and the computer in the Group Policy Object Editor.

To enable pass-through authentication for all plugins

1. Open the MMC Group Policy Object Editor snap-in.

2. Select the group policy object you want to edit.

3. In the left pane, expand the Administrative Templates node.


5. Select Local user name and password.


7. Click the Setting tab and, in the Local user name and password area, select Enabled.

8. Verify that the Enable pass-through authentication check box is selected and click OK.

Step 3: Enabling the Windows Directory Service Mapper

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

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 Internet Information Services 7.0

1. Ensure that the Web Server > Security > IIS Client Certificate Mapping Authentication role service is not installed for the Web Server (IIS) role.

2. Open the MMC Internet Information Services (IIS) Manager snap-in on the Web Interface server.
3. Select your Web server in the left pane and, in the **Features View**, double-click **Authentication**.

4. On the **Authentication** page, enable the following authentication methods:
   - **Active Directory Client Certificate Authentication**
   - **Anonymous Authentication**
   - **Windows Authentication** (if you plan to enable pass-through with smart card authentication)

**To enable the Windows Directory Service Mapper on Internet Information Services 6.0**

1. Open the MMC Internet Information Services (IIS) Manager snap-in on the Web Interface server.

2. Select the **Web Sites** node located under the Web Interface server and, on the **Action** menu, click **Properties**.

3. From the **Directory Security** tab, select **Enable the Windows directory service mapper** in the **Secure communications** area.

4. Click **OK** to enable the Directory Service Mapper.

**Step 4: Enabling Smart Card Authentication on the Web Interface**

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

**To enable smart card authentication for XenApp Web sites**

1. Click **Configure authentication methods**.

2. Select the **Smart card** check box.

**To enable smart card authentication for XenApp Services sites**

1. Click **Configure authentication methods**.

2. Select the **Smart card** check box.

3. Click **Properties**.
4. Select **Roaming**.

5. To configure the behavior of the Web Interface when a smart card is removed, select **Enable roaming** and choose one of the following options:
   - To disconnect a user’s session when the smart card is removed, select **Disconnect sessions when smart card removed**
   - To log off a user’s session when the smart card is removed, select **Log off sessions when smart card removed**

**Example: Enabling Smart Card Authentication for Users**

This example illustrates the steps required to allow users to log on to the Web Interface using smart cards and access published applications and content.

You want to enable smart card authentication for a user. The user is using a computer running Windows XP. A smart card reader is attached to the computer and smart card support is configured on the XenApp 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 XenApp installation media to install the Citrix XenApp Plugin for Hosted Apps on the user’s computer. The installation of the plugin is performed using an administrator account. During installation of the Citrix XenApp Plugin for Hosted Apps, respond **Yes** to the prompt “Would you like to enable and automatically use your local user name and password for Citrix sessions from this plugin?”

2. Enable pass-through authentication for all plugins using group policy. For more information, see “Step 2: Enabling Pass-Through for the Plugins” on page 74. You must also ensure that pass-through authentication is enabled on the XenApp server. For more information, see the *Citrix XenApp Administrator’s Guide*.

3. Ensure that the Windows Directory Service Mapper is enabled. For more information, see “Step 3: Enabling the Windows Directory Service Mapper” on page 77.

4. Use the **Configure authentication methods** task to enable smart card authentication. When the user selects **Smart card** on the logon screen, the user enters the PIN to log on (assuming the user logged on to the physical Windows desktop using the smart card). If you do not want the user to have to reenter the PIN when logging on to the Web Interface, enable pass-through with smart card authentication.
Configuring Two-Factor Authentication

You can configure the following two-factor authentication methods for XenApp Web sites:

- **Secure Computing SafeWord for Citrix.** An authentication method that uses alphanumeric codes generated by SafeWord tokens and, optionally, PIN numbers to create a passcode. Users enter their domain credentials and SafeWord passcodes on the logon screen before they can access applications on the server.

- **RSA SecurID.** An authentication method that uses numbers generated by RSA SecurID tokens (tokencodes) and PIN numbers to create a PASSCODE. Users enter their user names, domains, passwords, and RSA SecurID PASSCODES on the logon screen before they can access published resources 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 appears 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.

- **RADIUS server.** An authentication method that uses the Remote Authentication Dial-in User Service (RADIUS) authentication protocol (as opposed to proprietary agent software). Both SafeWord and SecurID can be installed and configured to be presented as a RADIUS server. For Web Interface for Java Application Servers, RADIUS authentication is the only option available.

Enabling Secure Computing SafeWord on Internet Information Services

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 Web Interface server 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 Windows:

- Obtain the latest version of the SafeWord Agent from Secure Computing. If support for UPN authentication is required, ensure you apply the latest auto-updates for the SafeWord Agent for the Web Interface and for the SafeWord server.
- Ensure the Web Interface is installed prior to installing the SafeWord Agent for the Web Interface.
- Ensure the SafeWord Agent for the Web Interface is installed on the Web Interface server.

For more information about configuring your SafeWord product, visit 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 resource set. To do this, use the Configure authentication methods task.

Enabling RSA SecurID 6.0 Authentication on Internet Information Services 6.0
The following sections describe how to enable RSA SecurID support.

SecurID Requirements
To use SecurID authentication with the Web Interface for Windows:

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

Note: The RSA ACE/Agent for Windows 6.0 is not supported on Windows Server 2008. If you want to integrate RSA SecurID into your environment, you must either install the Web Interface and the RSA ACE/Agent on a server running Windows Server 2003 or configure your RSA ACE/Server to be presented as a RADIUS server.
Adding the Web Interface Server as an Agent Host
You must create an Agent Host for the Web Interface server in the RSA ACE/Server database so that the RSA ACE/Server recognizes and accepts authentication requests from the Web Interface server. 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 Web Interface server. 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 so that users can access and display their resource set. To do this, use the **Configure authentication methods** task.

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

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

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

If the node secret on the Web Interface server and the RSA ACE/Server do not match, RSA SecurID fails. You must reset the node secret on the Web Interface server 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 Web Interface server
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 NodeSecret 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 logon using the form `DOMAIN\username` (as opposed to user name only) and configure the Web Interface to send the domain and user name to the ACE/Server using the **Configure authentication methods** task.

**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 access published resources 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 Windows:

- The RSA ACE/Agent Local Authentication Client for Windows 6.0 must be installed on the Web Interface server (administrators must log on to the Web Interface using local server 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 Web Interface server
- The Agent Host for the Web Interface server 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 RADIUS Authentication

The following sections describe how to install and configure Secure Computing SafeWord and RSA SecurID to be presented as a RADIUS server. RADIUS authentication is the only two-factor authentication option available for Web Interface for Java Application Servers.

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 Internet Authentication Service (IAS) snap-in to the Microsoft Management Console. A new RADIUS client needs to be configured for each Web Interface server 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 Web Interface server with which the RADIUS client is associated.
- A secret that is available to the associated Web Interface server. For more information, see “Creating a Shared Secret for RADIUS” on page 85.
- The client type must be set to RADIUS standard.
- The Request must contain the Message Authenticator attribute option must be selected 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 also acts 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 Web Interface server in the RSA ACE/Server database so that the RSA ACE/Server recognizes and accepts authentication requests from the Web Interface server 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.
Creating a Shared Secret for RADIUS
The RADIUS protocol requires the use of a shared secret—data that is available only to the RADIUS client (that is, the Web Interface) and the RADIUS server against which it authenticates. The Web Interface stores the shared secret in a text file on the local file system. On IIS, the location for this file is given by the RADIUS_SECRET_PATH configuration value in the web.config file. The location given is relative to the ‘conf’ folder for the site. On Java application servers, the location for the shared secret file is indicated by the radius_secret_path parameter in the web.xml file. The location given is relative to the /WEB-INF directory for the site.

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 relevant configuration 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 resource set. To do this, use the Configure authentication methods task. 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 logon screen.

Citrix recommends that this mode be 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 recognized by the Web Interface, the RADIUS server can present user interface pages identical to those displayed by the Web Interface for Windows, 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 Java application servers, the following challenges must be updated:

<table>
<thead>
<tr>
<th>Message for</th>
<th>Packet</th>
<th>Updated value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does User Want a System PIN</td>
<td>Challenge</td>
<td>CHANGE_PIN_EITHER</td>
</tr>
<tr>
<td>Is User Ready to Get System PIN</td>
<td>Challenge</td>
<td>SYSTEM_PIN_READY</td>
</tr>
<tr>
<td>Is User Satisfied with System PIN</td>
<td>Challenge</td>
<td>CHANGE_PIN_SYSTEM_[%s]</td>
</tr>
<tr>
<td>New Numeric PIN of Fixed Length</td>
<td>Challenge</td>
<td>CHANGE_PIN_USER</td>
</tr>
<tr>
<td>New Alphanumeric PIN of Fixed Length</td>
<td>Challenge</td>
<td>CHANGE_PIN_USER</td>
</tr>
<tr>
<td>New Numeric PIN of Variable Length</td>
<td>Challenge</td>
<td>CHANGE_PIN_USER</td>
</tr>
<tr>
<td>New Alphanumeric PIN of Variable Length</td>
<td>Challenge</td>
<td>CHANGE_PIN_USER</td>
</tr>
<tr>
<td>New PIN Accepted</td>
<td>Challenge</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Enter Yes or No</td>
<td>Challenge</td>
<td>FAILURE</td>
</tr>
<tr>
<td>Next Token Code Required</td>
<td>Challenge</td>
<td>NEXT_TOKENCODE</td>
</tr>
</tbody>
</table>
Managing Plugins

This section provides information about deploying and using Citrix plugins with the Web Interface. It also explains how to set up secure access. Topics include:

- Managing Plugin Deployment
- Configuring Citrix XenApp
- Managing Secure Access
- Editing Client-Side Proxy Settings

Managing Plugin Deployment

To access published resources (applications, content, and desktops), users must have, at minimum, either a supported plugin or a supported Web browser with the Java Runtime Environment.

Use the Manage client deployment task to specify which plugins are offered to users for download and installation. You can also use this task to specify with which plugins users can access published resources.

You can:

- Configure Web-based plugin deployment
- Specify which plugins the Web Interface offers to users for installation
- Specify the plugins with which users can access published resources
- Allow users to choose whether they want to launch remote or streamed applications
- Specify the components included in the Client for Java or allow users to select the components that they require
Remote Plugin Types

The following plugins are available for accessing remote resources:

- **Native plugin.** Users download and deploy the Citrix XenApp Web Plugin using the plugin detection and deployment process. Seamless windows are supported; published resources are presented in desktop windows that can be resized. If users are accessing applications through a PDA device, you must enable the native plugin.

- **Native embedded plugin (ActiveX or Netscape plugin).** Users download and deploy this plugin using the plugin detection and deployment process. Seamless windows are not supported; published resources are presented in embedded browser windows.

- **Client for Java.** Users download the Client for Java when the published resource is accessed. This plugin supports seamless windows; published resources are presented in desktop windows that can be resized.

- **Embedded Remote Desktop Connection (RDP) software.** If it is not already installed with their Windows operating system, users download and deploy Remote Desktop Connection (RDP) software using the plugin detection and deployment process. Seamless windows are not supported; applications are presented in embedded browser windows.

---

**Note:** The native embedded plugin, Client for Java, and embedded Remote Desktop Connection (RDP) software are not supported on devices running Windows CE or Windows Mobile. XenDesktop virtual desktops cannot be accessed using embedded Remote Desktop Connection (RDP) software or using PDAs and other hand-held devices. The Client for Java and embedded Remote Desktop Connection (RDP) software are not supported for accessing AD FS integrated sites.

---

Citrix XenApp Plugin for Streamed Apps

The Citrix XenApp Plugin for Streamed Apps allows users to stream applications to their desktops (both physical and virtual) and open them locally. The Citrix XenApp Plugin for Streamed Apps:

- Runs as a service on the user’s computer to invoke applications the user selects using Citrix XenApp or a Web browser

- Finds the correct package target for the user’s computer, creates an isolation environment on the computer, and streams the necessary files for the application to run to the user’s desktop
You can either install the Citrix XenApp Plugin for Streamed Apps with Citrix XenApp to provide the full set of Citrix client-side application virtualization features or alone on users’ desktops so users can access published applications through a Web browser using a XenApp Web site.

To be able to stream applications through a XenApp Web site, both Internet Explorer and Firefox users must add the site to the Windows Trusted sites zone using Internet Explorer. For instructions on how to do this, see “To add a XenApp Web site to the Trusted sites zone in Internet Explorer” on page 92.

For security reasons, neither the Web Interface nor the Citrix XenApp Plugin for Streamed Apps warn users if the XenApp Web site they are accessing is not in the correct Windows security zone. Users who have not added their XenApp Web sites to the Trusted sites zone cannot launch applications and do not receive error messages informing them that the application launch has been blocked. For this reason, it is important that users are made aware of the need to add their XenApp Web sites to the appropriate Windows security zone.

**Note:** XenDesktop virtual desktops cannot be accessed using the Citrix XenApp Plugin for Streamed Apps.

For more information about publishing streamed applications, see the *Citrix XenApp Administrator’s Guide*.

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

### Using Web-Based Plugin Installation

To use the Web Interface, users must have, at minimum, either a supported plugin or a supported Web browser with the Java Runtime Environment.

### Copying Plugin Installation Files to the Web Site

To use Web-based plugin installation, the XenApp Web site must contain the plugin installation files.

During Web Interface installation, Setup prompts you to access the installation media. On IIS, Setup copies the contents of the \Clients directory on the installation media to a directory called \Clients in the root directory (for example, C:\Program Files (x86)\Citrix\Web Interface\Version\Clients). On Java application servers, Setup copies the plugins from the installation media and packages them in the .war file.

If you did not copy the plugin installation files to the Web server during Web Interface installation, make sure you copy these files to the Web server before using Web-based plugin installation.
To copy the plugin files to the XenApp Web site on Internet Information Services
1. Locate the \Clients directory where the Web Interface is installed; for example, C:\Program Files (x86)\Citrix\Web Interface\Version\Clients.
2. Insert the installation media in the Web server’s optical drive or browse the network for a shared image of the installation media.
3. Change directories to the \Clients directory on the installation media. Copy the contents of the directory on the installation media to the directory on the Web Interface server. Make sure you copy only the contents of the directory and not the \Clients directory itself.

To copy the plugin files to the XenApp Web site on Java application servers
1. In the expanded .war file for the site, locate the /Clients directory.
2. Insert the installation media in the Web server’s optical drive or browse the network for a shared image of the installation media.
3. Change directories to the /Clients directory of the installation media. Copy the contents from the directory on the installation media to the directory on the Web Interface server. Make sure you copy only the contents of the directory and not the /Clients directory itself.

Configuring Plugin Deployment and Installation Captions
The Web Interface provides a plugin detection and deployment process that detects which plugins can be deployed within the user’s environment and then guides them through the deployment procedure, including, where appropriate, reconfiguring their Web browser.

You can allow users to access the plugin detection and deployment process in up to three ways:

- You can configure the plugin detection and deployment process to run automatically when users access a XenApp Web site. When users log on to the Web Interface, the plugin deployment process starts automatically, helping users to identify and deploy the appropriate plugin to access their published resources. For some environments, the plugin detection and deployment process can also detect the presence or absence of an installed plugin and prompt the user only when necessary.

- You can allow users to specify their preferred plugin for accessing remote published resources. This adds the Change Client button to the Connection Preferences screen, enabling users to start the plugin detection and deployment process manually.

- You can provide users with installation captions, which are links that are presented to users on the Messages screen. Users click a link to start the plugin detection and deployment process.
When a user accesses a XenApp Web site, the Web-based plugin detection and deployment process attempts to determine whether or not any plugin software is installed on the user’s computer. If a user for which the appropriate plugin software could not be detected subsequently logs on to a XenApp Web site configured for automatic plugin detection and deployment, the process starts automatically and guides the user through the procedure for identifying and deploying a suitable plugin to access their published resources, including, where appropriate, reconfiguring their Web browser.

Users can also access the plugin deployment process using links that appear on their Messages screens. Users click a link to start the plugin detection and deployment process. These links are called installation captions. For example:

The figure shows an example of an installation caption that may appear on the user’s Messages screen.

Installation captions can be provided for users who do not have a suitable plugin; they can also be used to allow users to access the plugin deployment process to upgrade their plugins to a newer version or to an alternative type of plugin that offers greater functionality.

You can use the Manage client deployment task to specify the circumstances under which users can access the plugin detection and deployment process.

**To configure plugin deployment and installation captions**

1. Click Manage published resources and clients > Manage client deployment.
2. Click Client Detection.
3. If you want the plugin detection and deployment process to start automatically when users without a suitable plugin log on to the Web Interface, select the **Perform client detection at logon** check box.

4. Specify when installation captions are shown to users by choosing one of the following options:

   - To notify the user if an appropriate plugin cannot be detected or if a more suitable plugin is available, select **Whenever a client is needed**. This is the default setting.
   
   - To notify the user only if an appropriate plugin cannot be detected, select **Only if published resources cannot be accessed**.
   
   - If you do not want installation captions to appear under any circumstances, select **Never**.

### Deploying Remote Desktop Connection Software

Remote Desktop Connection (RDP) functionality is available on 32-bit Windows systems with Internet Explorer 6.x or 7.x.

#### Remote Desktop Connection Requirements

If Internet Explorer does not place the XenApp Web site in the Local intranet or Trusted sites zone, it displays an error message and refers the user to the Help system for more information. In this instance, Citrix recommends that users be advised of the following procedures.

**To add a XenApp Web site to the Trusted sites zone in Internet Explorer**

1. From the Internet Explorer **Tools** menu, select **Internet Options**.

2. Click the **Security** tab.

3. Select **Trusted sites** and click **Sites**.

4. If necessary, type the URL of the Web Interface server in the **Add this website to the zone** box; for example, http://ServerName.

5. If the XenApp Web site is accessed using an HTTP connection, ensure that the **Require server verification (https:) for all sites in this zone** check box is cleared.

6. Click **Add** to add the XenApp Web site to your list of trusted sites.
To add a XenApp Web site to the Local intranet zone in Internet Explorer
1. From the Internet Explorer Tools menu, select Internet Options.
2. Click the Security tab.
3. Select Local intranet and click Sites.
4. Click Advanced.
5. If necessary, type the URL of the Web Interface server in the Add this website to the zone box; for example, http://ServerName.
6. If the XenApp Web site is accessed using an HTTP connection, ensure that the Require server verification (https:) for all sites in this zone check box is cleared.
7. Click Add to add the XenApp Web site to your list of intranet sites.

Deploying the Client for Java
If you are deploying plugins 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 Web Interface server 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 540 KB). 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 allow 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:

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>Allows published resources 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 XenApp Administrator’s Guide for information.</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Allows users to copy text and graphics between server-based resources and applications running locally on the client device.</td>
</tr>
<tr>
<td>Local text echo</td>
<td>Accelerates the display of the input text on the client device.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>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.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Provides strong encryption to increase the privacy of plugin connections.</td>
</tr>
<tr>
<td>Client drive mapping</td>
<td>Allows users to access their local drives from within a session. When users connect to the server, their client drives, such as floppy disks, network drives, and optical drives, are mounted automatically. Users can access their locally stored files, work with them during their 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.</td>
</tr>
<tr>
<td>Printer mapping</td>
<td>Allows users to print to their local or network printers from within a session.</td>
</tr>
<tr>
<td>Configuration UI</td>
<td>Enables the Client for Java Settings dialog box. This dialog box is utilized by users to configure the Client for Java.</td>
</tr>
</tbody>
</table>

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

If you configured 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 device. 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 for Java, 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 Client for Java packages (such as the C:\Program Files (x86)\Citrix\Web Interface\Version\Clients\ica\java 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
If you are using the Client for Java Version 8.x, configure the Web Interface to use a single custom SSL root certificate.

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 (JVMs), such as the IBM JVM on OS/2, do 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. Using a text editor, open the appEmbedClient.js file, which is typically located at C:\inetpub\wwwroot\Citrix\SiteName\site\clientscripts.
3. Locate the line of the JavaScript code that writes out the first `<applet>` HTML tag.
4. After this line, specify which SSL/TLS certificates the Client for Java should use. The following parameters (enclosed in JavaScript) are required:

- **SSLNoCACerts.** The number of specified certificates in the Client for Java archive.

- **SSLCACert0, SSLCACert1...SSLCACertn.** 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:

```javascript
document.write('<param name="SSLNoCACerts" value="3">');
document.write('<param name="SSLCACert0" value="A.crt">');
document.write('<param name="SSLCACert1" value="B.crt">');
document.write('<param name="SSLCACert2" value="C.cer">');
```

5. If you want to deploy the Client for Java 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 line in the JavaScript code that writes out the cabinets parameter. Add the name of the archive you created in Step 5. For example, if you named your archive mycerts.cab, change the following:

```javascript
document.write('<param name="cabinets" value="'+Cabs+'">');
```

to:

```javascript
document.write('<param name="cabinets" value="'+Cabs+',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 (x86)\Citrix\Web Interface\Version\Clients\icajava.

8. On the client device, launch the Web browser and connect to the Web Interface. All embedded Client for Java sessions to secured servers work transparently using SSL.
Configuring Support for Older Plugins

ICA files are text files that contain parameters and instructions for accessing published resources. By default, the Web Interface is configured to generate .ica files in Unicode, which increases the number of non-European language characters that remote plugins recognize. However the plugins available with releases prior to Citrix MetaFrame Presentation Server 3.0 do not support Unicode .ica files, so you may want to configure the Web Interface to support all versions of the plugins.

To configure support for older plugins
1. Click Manage published resources and clients > Manage client deployment.
2. Select Version Support.
3. Click Support all versions 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 the session URL, which enables communication with the Citrix XenApp Plugin for Streamed Apps. 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 sessions in multiple farms, specific published applications, sessions connecting to a specific server, or a specific user’s sessions and applications.

To configure streaming session monitoring
1. Click Manage published resources and clients > Manage client deployment.
2. Select Streaming Client.
3. Select how the Web Interface communicates with the Citrix XenApp Plugin for Streamed Apps. Choose from the following:
   - To automatically detect the session URL used to communicate with the plugin, select Automatically detect session URL.
   - To set the session URL manually, select Specify session URL and enter the URL details.
Configuring Citrix XenApp

Citrix XenApp allows users to access remote and streamed applications, and remote desktops and content directly from physical Windows desktops without using a Web browser. You can remotely configure the placement of links to remote resources on the Start menu, on the Windows desktop, or in the Windows notification area. The Citrix XenApp 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 Citrix XenApp.

Using the Access Management Console for Configuration

Citrix XenApp 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 39.

Using the Configuration Files

You can also configure Citrix XenApp using the config.xml and WebInterface.conf files. These files are typically located in the C:\inetpub\wwwroot\Citrix\PNAgent\conf directory on the Web Interface server.

Managing Plugin Configuration Files

The Citrix XenApp options configured with the console are stored in a configuration file on the Web Interface server (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 Citrix XML Service. The configuration file controls the range of parameters that appear as options in the user’s XenApp plugin Options 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 directory for the site.

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

All new Web Interface sites are configured by default for direct access, where the actual address of the Citrix server is given to all plugins. However, if you are using Access Gateway, Secure Gateway, or a firewall in your deployment, you can use the Edit secure client access settings task to configure the Web Interface to include the appropriate settings. You can also configure different access methods for different groups of users. For example, internal users logging on over the corporate LAN can be configured for direct access, while external users logging on through the Internet access the Web Interface through Access Gateway.

This section explains how to use the Edit secure client access settings task to specify access settings, edit address translations, and configure gateway settings.

Editing Direct Access Routes

If you want the actual address of the Citrix server to be given to a particular set of plugins, you can specify plugin addresses and masks using the Edit secure client access settings task.

To configure direct access
1. Click Manage secure client access > Edit secure client access settings.
2. On the Specify Access Methods page, click Add to add a new access route or select an entry from the list and click Edit to edit an existing route.
3. From the Access method list, select Direct.
4. Enter the network address and subnet mask that identify the client network.
5. Use the Move Up and Move Down buttons to place the access routes in order of priority in the Client addresses table.

Editing Alternate Address Settings

If you want the alternate address of the Citrix server to be given to a particular set of plugins, you can specify plugin addresses and masks using the Edit secure client access settings task. The server must be configured with an alternate address and the firewall must be configured for network address translation.

Note: XenDesktop virtual desktops cannot be accessed if alternate addresses are used.
To configure alternate address settings
1. Click Manage secure client access > Edit secure client access settings.
2. On the Specify Access Methods page, click Add to add a new access route or select an entry from the list and click Edit to edit an existing route.
3. From the Access method list, select Alternate.
4. Enter the network address and subnet mask that identify the client network.
5. Use the Move Up and Move Down buttons to place the access routes in order of priority in the Client addresses table.

Editing Address Translations
If you are using a firewall in your deployment, you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your Citrix server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to the plugin. To do this, use the Edit secure client access settings task.

To configure internal firewall address translation
1. Click Manage secure client access > Edit secure client access settings.
2. On the Specify Access Methods page, click Add to add a new access route or select an entry from the list and click Edit to edit an existing route.
3. From the Access method list, select Translated.
4. Enter the network address and subnet mask that identify the client network. Use the Move Up and Move Down buttons to place the access routes in order of priority in the Client addresses table and click Next.
5. On the Specify Address Translations page, click Add to add a new address translation or select an entry from the list and click Edit to edit an existing address translation.
6. In the Access Type area, select one of the following options:
   - If you want the plugin to use the translated address to connect to the Citrix server, select Client route translation
   - If you already configured a gateway translated route in the Client addresses table and want both the plugin and the gateway server to use the translated address to connect to the Citrix server, select Client and gateway route translation
7. Enter the internal and external (translated) port numbers and addresses for the Citrix server. Plugins connecting to the server use the external port number and address. Ensure that the mappings you create match the type of addressing being used by the Citrix server.
Editing Gateway Settings

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

**To configure gateway settings**

1. Click **Manage secure client access > Edit secure client access settings**.

2. On the **Specify Access Methods** page, click **Add** to add a new access route or select an entry from the list and click **Edit** to edit an existing route.

3. From the **Access method** list, select one of the following options:
   - If you want the actual address of the Citrix server to be given to the gateway server, select **Gateway direct**.
   - If you want the alternate address of the XenApp server to be given to the gateway server, select **Gateway alternate**. The XenApp server must be configured with an alternate address and the firewall must be configured for network address translation.

4. Enter the network address and subnet mask that identify the client network. Use the **Move Up** and **Move Down** buttons to place the access routes in order of priority in the **Client addresses** table and click **Next**.

5. If you are not using gateway address translation, continue to Step 8. If you are using gateway address translation, click **Add** on the **Specify Address Translations** page to add a new address translation or select an entry from the list and click **Edit** to edit an existing address translation.

6. In the **Access Type** area, select one of the following options:
   - If you want the gateway server to use the translated address to connect to the Citrix server, select **Gateway route translation**.
   - If you already configured a plugin translated route in the **Client addresses** table and want both the plugin and the gateway server to use the translated address to connect to the Citrix server, select **Client and gateway route translation**.

---

**Note:** XenDesktop virtual desktops cannot be accessed if alternate addresses are used.
7. Enter the internal and external (translated) port numbers and addresses for the Citrix server and click Next. When the gateway server connects to the Citrix server, it uses the external port number and address. Ensure that the mappings you create match the type of addressing being used by the server farm.

8. On the Specify Gateway Settings page, specify the fully qualified domain name (FQDN) and port number of the gateway server that plugins must use. The FQDN must match what is on the certificate installed on the gateway server.

9. If you want the Citrix server to keep disconnected sessions open while the plugin attempts to reconnect automatically, select the Enable session reliability check box. Click Next.

10. On the Specify Secure Ticket Authority Settings page, click Add to specify the URL of a Secure Ticket Authority (STA) that the Web Interface can use or select an entry from the list and click Edit to edit existing STA details. STAs are included with the Citrix XML Service; for example, in http://ServerName/scripts/ctxsta.dll. You can specify more than one STA for fault tolerance; however, Citrix recommends that you do not use an external load balancer for this purpose. Use the Move Up and Move Down buttons to place the STAs in order of priority.

11. Choose whether or not to enable load balancing between STAs 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.

12. Specify the length of time that uncontactable STAs should be bypassed for in the Bypass failed servers for boxes. The Web Interface provides fault tolerance among the servers on the Secure Ticket Authority URLs list so that if a communication error occurs, the failed server is bypassed for the specified time period.

**Editing Default Access Settings**

The order in which the entries appear in the Client addresses table is the order in which the rules are applied. If the plugin address does not match any explicitly defined rules for access, the default rule is applied. When you create a site, the default route is configured automatically for direct access. You can specify a default access method appropriate to your deployment using the Edit secure client access settings task.
To configure default access settings
1. Click Manage secure client access > Edit secure client access settings.
2. On the Specify Access Methods page, select the entry from the list labeled Default and click Edit.
3. From the Access method list, select one of the following options:
   - If you want the actual address of the Citrix server to be given to the plugin, select Direct.
   - If you want the alternate address of the XenApp server to be given to the plugin, select Alternate. The XenApp server must be configured with an alternate address and the firewall must be configured for network address translation.

   Note: XenDesktop virtual desktops cannot be accessed if alternate addresses are used.

   - If you want the address given to the plugin to be determined by the address translation mappings set in the Web Interface, select Translated.
   - If you want the actual address of the Citrix server to be given to the gateway server, select Gateway direct.
   - If you want the alternate address of the XenApp server to be given to the gateway server, select Gateway alternate. The XenApp server must be configured with an alternate address and the firewall must be configured for network address translation.

   Note: XenDesktop virtual desktops cannot be accessed if alternate addresses are used.

   - If you want the address given to the gateway server to be determined by the address translation mappings set in the Web Interface, select Gateway translated.
4. Enter the network address and subnet mask that identify the client network. Use the Move Up and Move Down buttons to place the access routes in order of priority in the Client addresses table.

5. If you are using address translation or a gateway in your deployment, click Next and specify the appropriate additional settings for your default configuration. See “To configure internal firewall address translation” on page 100 and “To configure gateway settings” on page 101 for more information.

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 plugins must communicate with the server running XenApp or Desktop Delivery Controller 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 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 plugins. However, you can also configure exceptions to this behavior for individual client devices. 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 be controlled by the plugin. For example, to use the Secure Proxy feature in XenApp and XenDesktop, configure the Web Interface to use the proxy settings specified on the plugin and configure the plugin for Secure Proxy. For more information about using plugins to control proxy behavior, see the relevant administrator’s guide.

To configure default proxy settings

1. Click Edit client-side proxy.
2. Click Add to create a new mapping or select an entry from the list and click Edit to edit an existing mapping.
3. Enter the external address of the proxy and the plugin subnet mask in the IP address and Subnet mask boxes, respectively.
4. From the **Proxy** list, choose one of the following options:

- If you want the plugin to detect the Web proxy automatically based on the client computer’s browser configuration, select **User’s browser setting**.

- If you want the plugin to detect the Web proxy automatically using the Web Proxy Auto Discovery (WPAD) protocol, select **Web Proxy Auto Detect**.

- If you want to use the settings configured for the plugin by the user, select **Client defined**.

- If you want to use a SOCKS proxy server, select **SOCKS**. If you choose this option, you must enter the address and port number of the proxy server. The proxy address can be an IP address or a DNS name.

- If you want to use a secure proxy server, select **Secure (HTTPS)**. If you choose this option, you must enter the address and port number of the proxy server. The proxy address can be an IP address or a DNS name.

- If you do not want to use a proxy, select **None**.

5. If you entered more than one mapping, use the **Move Up** and **Move Down** buttons to place the mappings in order of priority in the table.
Customizing the User Experience

This section describes how to customize the way in which the Web Interface appears to users. Topics include:

- Customizing the Appearance for Users
- Managing Session Preferences
- Configuring Workspace Control
- Changing Session Options
- Managing Shortcuts to Published Resources
- Using Published Resource 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 Web site appearance** task to customize:

- **Layout.** Specify the controls available to users and define the way in which the Web site is presented. You can:
  
  - Select auto, full graphics, or low graphics screen layout for the XenApp Web site. The low graphics user interface is a compact version designed for users accessing their published resources on small form factor devices or over slow network connections. The **Auto** option allows the system to choose the most appropriate site layout for each user according to the size of the user’s computer screen.
  
  - Configure the features and controls available on users’ **Applications** screens, including searching and hints, and specify whether or not users are permitted to customize their own screens.
• Set the default view styles for users’ published resource sets in the full graphics and low graphics screen layouts. You can also specify which of the view styles are available for users to select from.

• Specify how published resources should be grouped on users’ Applications screens. You can either configure separate tabs for applications, content, and desktops or you can collect all published resources together on a single tab.

• **Appearance.** Rebrand the user interface with a customized “look and feel” by displaying different images and colors throughout the site. You can:
  
  • Specify the style for users’ logon screens. Choose between a minimalistic layout where only the appropriate logon fields appear and a layout that includes the navigation bar, providing users with access to the Messages and pre-logon Preferences screens.
  
  • Use customized site branding images for the full graphics and low graphics layouts and, optionally, hyperlink the images. You can also change the background image displayed in the header area of the site or simply use a particular color.
  
  • Restyle the navigation bar to use different background images and colors that conform to your corporate color scheme.
  
  • Use a different background image or color for the central content area of the site and choose a complementary color for the text.

• **Content.** Define custom messages and screen text, and specify any additional languages in which the site is available. You can specify page titles and messages for users’ logon, Applications, and Messages screens, and common footer text to appear on all screens. In addition, you now have the option to configure a pre-logon disclaimer that users must accept before they can log on.
Managing 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 remote plugin name.

For XenApp Web sites, you can configure the following settings for user sessions:

- **User customizations.** Enable or disable kiosk mode and specify whether or not to display the Preferences button to users on their Applications screens.

- **Web sessions.** Specify the length of time a user session can be inactive before the user is logged off.

- **Connection performance.** Specify whether or not users are permitted to customize their bandwidth control, color depth, audio quality, and printer mapping settings.

- **Display.** Specify whether or not users can control their window sizes in remote sessions and allow the Web Interface to use ClearType font smoothing, providing the corresponding settings are configured for users’ Windows operating systems, users’ plugin software, and the server farm.

- **Local resources.** Configure settings for Windows key combinations, PDA synchronization, and Special Folder Redirection.

- **Client name.** Specify whether or not the Web Interface should override the remote plugin name.

**Important:** You must enable the Web Interface should override the remote client name setting if you want to use workspace control with Versions 8.x and 9.x of the Clients for Windows or with Citrix Presentation Server 4.0.
Bandwidth Control

Bandwidth control allows users to select session settings based on their connection bandwidth. These options appear on the pre-logon Preferences and Session Settings screens. Bandwidth control enables adjustment of color depth, audio quality, and printer mapping. Additionally, you can use .ica override files to manage other ICA settings for bandwidth control:

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth_high.ica</td>
<td>Contains the override ICA settings for high speed connections, such as broadband or LAN connections.</td>
</tr>
<tr>
<td>bandwidth_medium_high.ica</td>
<td>Contains the override ICA settings for medium high speed connections, such as connections through modems with speeds of greater than 33 kbps.</td>
</tr>
<tr>
<td>bandwidth_medium.ica</td>
<td>Contains the override ICA settings for medium speed connections, such as connections through modems with speeds of less than 33 kbps.</td>
</tr>
<tr>
<td>bandwidth_low.ica</td>
<td>Contains the override ICA settings for low speed connections, such as wireless connections.</td>
</tr>
<tr>
<td>default.ica</td>
<td>Contains the override ICA settings used when no connection speed is specified.</td>
</tr>
</tbody>
</table>

To specify particular settings that plugins should use regardless of the published resource being accessed and the user’s settings, open the appropriate .ica override file using a text editor and insert the required ICA settings. 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 (RDP) software is used, audio quality is mapped to either on or off and further quality control is not provided. Low bandwidth settings are recommended for wireless WAN connections.

**Note:** If Remote Desktop Connection (RDP) 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 Connection (RDP) software, the terminal servers, and the server configuration.

By default, users can adjust the window size of sessions. If you prevent users from adjusting a setting, the setting does not appear in the user interface and the server settings specified for the published resource are used.
Disabling Automatic Reconnection

The Auto Reconnect feature allows the Citrix XenApp Plugin for Hosted Apps, the Client for Windows CE, and the Client for Java to detect broken connections and automatically reconnect users to disconnected sessions. When a plugin detects an involuntary disconnection of a session, it attempts to reconnect to the session, enabling users to resume working at the point at which they were interrupted when the connection was broken.

By default, the Auto Reconnect feature is enabled at the server farm level, and can be disabled by editing the .ica override files for the site.

To disable automatic reconnection
1. Using a text editor, open the default.ica file in the \conf directory for the site, which is typically located at C:\inetpub\wwwroot\Citrix\SiteName\conf.
2. In the WFClient section, add the following line:
   TransportReconnectEnabled=False
3. Repeat the same procedure for the other ICA settings files:
   bandwidth_high.ica
   bandwidth_medium_high.ica
   bandwidth_medium.ica
   bandwidth_low.ica

ClearType Font Smoothing

ClearType is a subpixel anti-aliasing technology developed by Microsoft that improves the rendering of text on LCD screens, reducing visible artifacts and making the text appear less jagged. ClearType font smoothing is a feature of both Windows XP and Vista, although it is not enabled by default in Windows XP.

The Web Interface and the Citrix XenApp Plugin for Hosted Apps support ClearType font smoothing during ICA sessions. When a user running Windows XP or Vista connects to the server, the plugin automatically detects the font smoothing setting on the user’s computer and sends it to the server. This setting is then used for the duration of the session.

Font smoothing must be enabled on users’ operating systems, the Citrix XenApp Plugin for Hosted Apps, the Web Interface site, and the server farm. Use the Manage session preferences task to enable font smoothing for XenApp Web sites and the Change session options task for XenApp Services sites.

Font smoothing applies to remote published resources only. This feature is not available for streamed applications.
Special Folder Redirection

The Special Folder Redirection feature allows users to map Windows special folders for the server to those on their local client computer so that they are easier to use with published resources. The term *special folders* refers specifically to standard Windows folders, such as Documents and the Desktop, that are always presented in the same way, regardless of the operating system.

**Note:** Prior to Windows Vista, the word “My” was prepended to the names of special folders, so the “Documents” folder is referred to as the “My Documents” folder in Windows XP, for example.

When users open, close, or save files in a session without Special Folder Redirection enabled, the **Documents** and **Desktop** icons that appear in the navigation dialog boxes within users’ published resources represent the users’ Documents and Desktop folders on the server. Special Folder Redirection redirects actions, such as opening or saving a file, so that when users open or save files to their Documents and Desktop folders, they are accessing the folders on their local computers. Currently, only the Documents and Desktop folders are supported for redirection.

Special Folder Redirection applies to remote published resources only. This feature is not available for streamed applications.

**Enabling Special Folder Redirection**

Special Folder Redirection support is disabled by default for both XenApp Web and XenApp Services sites, and requires that a corresponding policy is configured on the Citrix server. In addition, you must ensure that none of the existing policy rules prevent users from accessing or saving to their local drives.

Use the **Manage session preferences** task to enable Special Folder Redirection for XenApp Web sites and the **Change session options** task for XenApp Services sites. You can also allow users to choose whether or not to enable this feature on the Session Settings screen.

When Special Folder Redirection is enabled, users should always grant published resources full read and write access to local files and folders by selecting **Full Access** in the **Client File Security** dialog box for the Program Neighborhood Connection Center. Users must log off from any active sessions before starting a new session on another client device. Citrix recommends that you do not enable Special Folder Redirection for users who connect to the same session simultaneously from multiple client devices.
Configuring Workspace Control

Use workspace control to allow users to disconnect quickly from all published resources (applications, content, and desktops), reconnect to disconnected resources, and log off from all resources. This allows users to move between client devices and gain access to all of their published resources (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 published resources each time they log on.

Feature Requirements

The following features, requirements, and recommendations apply to the workspace control feature:

- To use workspace control with Versions 8.x and 9.x of the Clients for Windows or Citrix Presentation Server 4.0, you must enable the Web Interface should override the remote 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 session, the workspace control feature is disabled.
- Depending on the security settings, Internet Explorer 7.0 can block the download of files that do not appear to be directly initiated by the user, so attempts to reconnect to published resources using the native plugin can be blocked. In situations where reconnection is not possible, a warning message appears and users are given the option of reconfiguring their Internet Explorer security settings.
- Each Web session times out after a period of inactivity (typically 20 minutes). When the HTTP session times out, the logoff screen appears; however, any published resources accessed 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 or Disconnect buttons.
- Resources 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 published resources after they disconnect.
• To use pass-through, smart card, or pass-through with smart card authentication, you must set up a trust relationship between the Web Interface server and the Citrix XML Service. For more information, see “Using Workspace Control with Integrated Authentication Methods” on page 114.

• If 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 card authentication because credential pass-through is enabled with these options.

Limitations
If you are planning to enable workspace control, be aware of the following:

• 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 published resources.

• You cannot use workspace control with the Client for 32-bit Windows prior to Version 8 or Remote Desktop Connection (RDP) software. Additionally, this feature works only with servers running Citrix Presentation Server 4.0 or later.

• Workspace control enables reconnection only to disconnected XenDesktop virtual desktops. Users cannot reconnect to virtual desktops that are suspended.

Using Workspace Control with Integrated Authentication Methods
If users log on using pass-through, smart card, or pass-through with smart card authentication, you must set up a trust relationship between the Web Interface server 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 resources among the Web Interface and servers running XenApp and Desktop Delivery Controller. Without the trust relationship, the Disconnect, Reconnect, and Log Off buttons will not work for those users logging on with smart card or pass-through authentication.

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 from the left pane that is running XenApp or Desktop Delivery Controller.

2. On the Action menu, click 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 Citrix 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 Citrix 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 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 in the Manage Server Farms dialog box.

- 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 server. 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 for XenApp Web sites, use the Manage workspace control task. To enable workspace control for XenApp Services sites, click Change session options > Workspace Control.

You can:

- Configure automatic reconnection when users log on, which allows users to reconnect to disconnected published resources or both disconnected and active resources

- Configure the Reconnect button, which allows users to reconnect to disconnected published resources or both disconnected and active resources

- Allow users of XenApp Web sites 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 users log on** option.
2. Choose one of the following options:
   - To reconnect both disconnected and active sessions automatically, select **Reconnect to all sessions**
   - To reconnect only disconnected sessions automatically, select **Reconnect only to disconnected sessions**
3. Select the **Allow users to customize** check box to allow users to configure this setting for themselves. Users can change this setting on the **Account Settings** screen of XenApp Web sites or in the XenApp plugin **Options** dialog box for XenApp Services sites.

To enable the Reconnect button
1. Select the **Enable the Reconnect button** option.
2. Choose one of the following options:
   - To configure the **Reconnect** button to reconnect users to both disconnected and active sessions, select **Reconnect to all sessions**
   - To configure the **Reconnect** button to reconnect users to disconnected sessions only, select **Reconnect only to disconnected sessions**
3. Select the **Allow users to customize** check box to allow users to configure this setting for themselves on the **Account Settings** screen of the site.

To configure logoff behavior
1. For XenApp Web sites only, select the **Log off active sessions when users log off from the Web Interface** check box to log users off from the Web Interface and all active sessions. If you do not select this option, users’ sessions remain active after they log off.
2. Select the **Allow users to customize** check box to allow users to configure this setting for themselves on the **Account Settings** screen of the site.
Changing Session Options

For XenApp Services sites configured to run either remote applications only or in dual mode, you can use the Change session options task to configure the following settings for user sessions:

- **Display.** Select the window sizes available for ICA sessions and define custom sizes in pixels or screen percentage. In addition, you can allow the Web Interface to use ClearType font smoothing, providing the corresponding settings are configured for users’ Windows operating systems, Citrix XenApp, and the server farm.

- **Color and sound.** Options enabled in this section are available for users to select.

- **Local resources.** Enable the targets of Windows key combinations that users can select. Windows key combinations do not affect seamless connections. You can enable the following targets:
  - **Local desktop.** Key combinations apply to the local physical desktop only; they are not passed to the ICA sessions.
  - **Remote desktop.** Key combinations apply to the virtual desktop in the ICA session.
  - **Full screen desktops only.** Key combinations apply to the virtual desktop in the ICA session only when it is in full screen mode.

Enable Special Folder Redirection so that when users open, close, or save to the Documents or Desktop folders from within a remote published resource, their actions are redirected to the folders on their local client computers. For more information, see “Special Folder Redirection” on page 112.

- **Workspace control.** Configure reconnection and logoff behavior. For more information, see “Configuring Workspace Control” on page 113.
Managing Shortcuts to Published Resources

You can use the **Manage shortcuts** task to specify how Citrix XenApp displays shortcuts for published resources.

You can create the following types of shortcuts:

- **Start menu.** You can use the settings specified in the **Manage shortcuts** task, the settings defined when resources are published on XenApp and Desktop Delivery Controller, or both settings. You can also define whether and how shortcuts appear in the **Start** menu, and allow users to specify this setting. Additionally, you can create shortcuts in the **All 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 shortcuts** task, the settings defined when resources are published on XenApp and Desktop Delivery Controller, or both settings. You can also define how and if shortcuts appear 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 published resources in the notification area and/or allow users to specify how published resources appear.

Using the **Manage shortcuts** task, you can also remove shortcuts. You can specify when shortcuts are removed (either when the Citrix XenApp plugin closes or when users log off from Citrix XenApp) and, for users running Windows CE or Linux, whether or not user-created shortcuts are removed in addition to Citrix XenApp shortcuts. If you choose to remove both Citrix XenApp and user-created shortcuts, you can also limit the folder depth of the search to improve performance.

Using Published Resource Refresh Options

Use the **Manage published resource refresh** task to specify when users’ lists of published resources are refreshed and whether or not they can customize these settings. You can enable refreshes when Citrix XenApp starts up or when published resources are accessed, and you can specify how often the list is refreshed.
Configuring Web Interface Security

This section 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 Citrix XenApp with SSL
- Web Interface/Citrix Server Communication
- Client Session/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 published resource delivery process. This section describes Web Interface security issues and recommendations for each of the following communication links:

- **Client device/Web Interface communication.** Discusses issues associated with passing Web Interface data between browsers and servers and suggests strategies for protecting data in transit and data written on client devices.

- **Web Interface/server communication.** Describes how to secure the authentication and published resource information that passes between the Web Interface server and the server farm.

- **Client session/server communication.** Considers issues associated with passing session information between plugins and servers. Discusses implementations of the Web Interface and XenApp/XenDesktop security features that protect such data.
The figure shows how the client device interacts with the server running XenApp or Desktop Delivery Controller and the Web Interface server.

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, the Citrix SSL Relay, Secure Gateway, and ICA encryption. It also tells you where to find more information about these technologies.

Secure Sockets Layer

The Secure Sockets Layer (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.

Transport Layer Security

Transport Layer Security (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 Citrix Presentation Server 4.0 and later, Citrix Desktop Server 1.0, and Citrix XenDesktop 2.0. 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: The maximum SSL/TLS certificate key size supported by the Web Interface for Java Application Servers is 2048 bits.

Citrix SSL Relay

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

The Citrix SSL Relay operates as an intermediary in the communication between the Web Interface server and Citrix XML Service. When using the 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 the Citrix SSL Relay negotiate an encryption method for the session. The Web server then sends all information requests in encrypted form to the Citrix SSL Relay. The Citrix SSL Relay decrypts the requests and passes them to the Citrix XML Service. When returning the information to the Web server, the XML Service sends all information through the server running the Citrix SSL Relay, 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 the Citrix SSL Relay, see the Citrix XenApp Administrator’s Guide or the Citrix XenApp SSL Relay for UNIX Administrator’s Guide.
ICA Encryption

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

ICA encryption provides confidentiality, which helps 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 XenApp for UNIX servers.

Access Gateway

You can use Access Gateway with the Web Interface and Secure Ticket Authority (STA) to provide authentication, authorization, and redirection to published resources (applications, content, and desktops) hosted on a server running XenApp or Desktop Delivery Controller.

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

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

The figure shows how Access Gateway secures communication between SSL/TLS-enabled plugins and servers.
For more information about Access Gateway, see the *Citrix 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 101.

**Secure Gateway**

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

Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled plugins 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. 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.

The figure shows how Secure Gateway secures communication between SSL/TLS-enabled plugins and servers.

For more information about 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 101.
Securing Web Interface Communication

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

- Instruct users to connect to Web Interface pages using HTTPS (HTTP secured with SSL/TLS). Your Web server must have an SSL certificate installed to establish a secure HTTP connection.

- Configure the Web Interface to use the Citrix SSL Relay for encryption between the Web Interface server and the servers running XenApp and Desktop Delivery Controller. Alternatively, if IIS is installed on the server running XenApp or Desktop Delivery Controller, use HTTPS to secure the connection.

Securing Citrix XenApp with SSL

To use SSL to secure the communications between Citrix XenApp and the Web Interface server, select the Use SSL/TLS for communication between clients and this site check box in the Manage server settings task.

Ensure that the Enable SSL and TLS protocols check box is selected on the Client options page of the Application Properties dialog box in XenApp Advanced Configuration.

Client Device/Web Interface Communication

Communication between Citrix plugins and the Web Interface server consists of passing several different types of data. As users identify themselves, browse published resources, and eventually select a resource to access, the Web browser and Web server pass user credentials, resource sets, and session initialization 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 when users log on. 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 logon screen, 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 resource sets. These pages list the published resources available to the user.

- **ICA files.** When the user selects a published resource, the Web server sends an .ica file for that resource to the plugin (in some cases using the Web browser as an intermediary). The .ica file contains a ticket that can be used to log on to the server. ICA files do not include a ticket for pass-through or smart card authentication.

### Security Issues

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:

- Attackers 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, attackers 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. Attackers 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 Internet Explorer users accessing the Web server using an HTTPS connection select the option to prevent encrypted pages being cached, the .ica file is saved as a plain text file in the Windows \Temporary Internet Files folder. Attackers with access to a user’s Internet Explorer cache could retrieve the .ica file to obtain network information.

- If pass-through is enabled on the plugin, attackers could send the user an .ica file that causes the user’s credentials to be misrouted to an unauthorized or counterfeit server. This occurs when the plugin captures users’ credentials when they log on to the client device 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.
Implement 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 browser first verifies the identity of the server by checking the 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 or 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 on the logon page. Data sent from the Web server, including the credentials cookie, .ica files, and HTML resource set 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 server 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 running the Citrix SSL Relay, make sure you configure either the Web server or the 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/Citrix Server Communication**

Communication between the Web Interface and the server running XenApp or Desktop Delivery Controller involves the following:

- Passing configuration data between the Web Interface and the Configuration Service (for sites using centralized configuration)
- Passing user credential and resource 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 resource set information. The server and farm use a TCP/IP connection and the Citrix XML protocol to pass the information.

**Security Issues**

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

- Attackers can intercept the XML traffic and steal resource set information and tickets. Attackers with the ability to crack the obfuscation can obtain user credentials as well.
- Attackers can impersonate the server and intercept authentication requests.
- Attackers 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 Web Interface server and the server farm:

- Use the Citrix SSL Relay as a security intermediary between the Web Interface server and the server farm. The Citrix SSL Relay performs host authentication and data encryption.
- In deployments that do not support the Citrix SSL Relay, install the Web Interface on the server running XenApp or Desktop Delivery Controller.
- Use the HTTPS protocol to send Web Interface data over a secure HTTP connection using SSL if IIS is installed on the server running XenApp or Desktop Delivery Controller.

**Use the Citrix SSL Relay**

The Citrix SSL Relay is a default component of XenApp and XenDesktop.

On the server side, you must install a server certificate on the server running the Citrix SSL Relay and verify the server’s configuration. For information about installing a server certificate and configuring the Citrix SSL Relay on servers, see the *Citrix XenApp Administrator’s Guide*. You can also consult the application Help in the Citrix SSL Relay Configuration Tool. For XenApp for UNIX servers, see the *Citrix XenApp SSL Relay for UNIX Administrator’s Guide*. 
When configuring the Citrix SSL Relay, make sure the server running the Citrix SSL Relay 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 server other than the server 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 the 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 55.

To configure the Web Interface to use Citrix SSL Relay using WebInterface.conf
1. Using a text editor, 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 Web Interface Server
To add support for a certificate authority, you must add the certificate authority’s root certificate to the Web Interface server.

To add a new root certificate to the Web Interface server
Copy the root certificate to your Web server.

- On IIS, the certificate is copied using the Microsoft Management Console (MMC) Certificate Manager snap-in.
- On Java application servers, use the keytool command-line tool to copy the certificate to the appropriate keystore directory for your particular platform. The certificate must be added to the keystore associated with the Java Virtual Machine that is serving the Web pages. The keystore is typically in one of the following locations:
  - {javax.net.ssl.trustStore}
  - {java.home}/lib/security/jssecacerts
  - {java.home}/lib/security/cacerts

For information about certificates, see the installation section of the Citrix XenApp Administrator’s Guide. For XenApp for UNIX servers, see the Citrix XenApp SSL Relay for UNIX Administrator’s Guide.
Enable the Web Interface on the Server Running XenApp or Desktop Delivery Controller

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 systems running XenApp, Setup lets you force the Citrix XML Service to share Internet Information Services’ TCP/IP port instead of using a dedicated port. With Desktop Delivery Controller, the installer enables port sharing automatically. When port sharing is enabled, the Citrix XML Service and the Web server use the same port by default.

As a first step, you can place both the Web server and the server running XenApp or Desktop Delivery Controller 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 XenApp or Desktop Delivery Controller. 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 plugin to server communication, the firewall must permit inbound ICA traffic on ports 1494 and 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 Web Interface SDK.

Use the HTTPS Protocol

You can use the HTTPS protocol to secure the Web Interface data passing between the Web server and the server running XenApp or Desktop Delivery Controller. HTTPS uses SSL/TLS to provide strong data encryption.

The Web server makes an HTTPS connection to IIS running on the server running XenApp or Desktop Delivery Controller. This requires IIS port sharing on the server running XenApp or Desktop Delivery Controller, and for IIS running on this server to have SSL enabled. The server name you specify (using the console, or in the Farm<n> 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 accessible 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 Access” on page 99.

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

1. Using a text editor, open the WebInterface.conf file.
2. Change the value of the **Transport** setting in the **Farm<n>** parameter to **HTTPS**.

### Client Session/Server Communication

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

- **Initialization requests.** The first step in establishing a session, called *initialization*, requires the plugin to request a session and produce a list of session configuration parameters. These parameters control various aspects of the session, such as which user to log on, the size of the window to draw, and the program to execute in the session.

- **Session information.** After session initialization, information is passed between the plugin and server through a number of virtual channels; for example, mouse input (from plugin to server) and graphical updates (from server to plugin).

### Security Issues

To capture and interpret plugin to server network communications, attackers must be able to crack the binary plugin protocol. Attackers with binary plugin protocol knowledge can:

- Intercept initialization request information sent from the plugin, including user credentials
- Intercept 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 plugins and servers. Both methods support 128-bit encryption of the data stream between the plugin and server, but SSL/TLS also supports verification of the identity of the server.
Support for SSL is included in Citrix Presentation Server 4.0 and later, Citrix Presentation Server 4.0 for UNIX Operating Systems, Citrix Desktop Server 1.0, and Citrix XenDesktop 2.0.

Support for SSL/TLS and ICA encryption is included in Citrix Presentation Server 4.0 and later, Citrix Desktop Server 1.0, and Citrix XenDesktop 2.0.

See the plugin documentation or the Citrix download site for a list of plugins that support each method. See the *Citrix XenApp Administrator’s Guide* for more information about ICA encryption.

**Use Access Gateway**

You can use Access Gateway to secure the traffic between your plugins and servers over the Internet. Access Gateway is a universal SSL VPN appliance that provides a single, secure point of access to all published resources.

For more information about Access Gateway, see the *Citrix 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 101.

**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 are 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 replaces users’ logoff screens, even when users are logged off successfully without any error.

**General Security Considerations**

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

Always ensure that all components are up-to-date with all the latest patches. For more information and to check for the latest download recommendations, see Microsoft’s Web site at [http://support.microsoft.com/](http://support.microsoft.com/).
Configuring Sites Using the Configuration File

This section describes how to administer locally configured sites using the configuration files. It also lists all the parameters that the configuration files can contain. Topics include:

- WebInterface.conf Parameters
- Settings in the bootstrap.conf File

Site Configuration Files

Locally configured sites include a file named WebInterface.conf that contains the 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 customize 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.

If you enter an invalid value for a setting when you edit a configuration file and then subsequently use the Access Management Console, the console replaces the invalid value with the default value when the file is saved (for locally configured sites) or imported (for centrally configured files).

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

- On Microsoft Internet Information Services (IIS), this is typically in C:\inetpub\wwwroot\Citrix\SiteName\conf
- On Java application servers such as Apache Tomcat, this may be /usr/local/tomcat/webapps/Citrix/XenApp/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 Web Interface SDK.

**Note:** You may need to stop and restart the Web Interface server for changes made to WebInterface.conf to take effect on Java application servers. Additionally, ensure that you save your changes with UTF-8 encoding.

### Disabling Error Messages

On IIS, you can disable the error messages provided with the Web Interface and display the underlying error that occurred. To do this, edit the web.config file located in the site’s root directory. Change the following line:

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

to:

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

You can also display your own customized error messages. To do this change the line to:

```xml
<customErrors mode="On" defaultRedirect="/html/CustomErrorPage"/>
```

where *CustomErrorPage* is the file name of your customized error page.

### 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Site types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AccountSelfServiceUrl</strong></td>
<td>Specifies the URL for the Password Manager Service.</td>
<td>Valid URL using HTTPS</td>
<td>XenApp Web</td>
</tr>
<tr>
<td><strong>AdditionalExplicitAuthentication</strong></td>
<td>Specifies the explicit two-factor authentication that must be carried out, in addition to SAM, ADS, or NDS.</td>
<td><strong>None</strong></td>
<td>SecurID</td>
</tr>
<tr>
<td><strong>AddressResolutionType</strong></td>
<td>Specifies the type of address to use in the .ica launch file.</td>
<td><strong>dns-port</strong></td>
<td><strong>dns</strong></td>
</tr>
<tr>
<td><strong>AGEPromptPassword</strong></td>
<td>Specifies whether or not users are prompted to reenter their passwords when logging on from the Access Gateway logon page.</td>
<td><strong>Off</strong></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>AGEWebServiceUrl</td>
<td>Specifies the URL for the Access Gateway authentication service.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AllowBandwidth Selection</td>
<td>Specifies whether or not users can indicate the speed of their network connection so that ICA settings can be optimized.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomize ApplicationAccess Method</td>
<td>Specifies whether or not users are permitted to choose between remote and streaming as their preferred way of accessing applications.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeAudio</td>
<td>Specifies whether or not users are permitted to adjust the audio quality for ICA sessions.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeAutoLogin</td>
<td>Specifies whether or not users are permitted to enable/disable automatic logon.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowCustomizeClientPrinterMapping</td>
<td>Specifies whether or not users are permitted to enable/disable client printer mapping.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeClients</td>
<td>Specifies whether or not users are permitted to change which plugin is used to access a published resource.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeJavaClientPackages</td>
<td>Specifies whether or not users are permitted to choose which Client for Java packages they want to download.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeLayout</td>
<td>Specifies whether or not users are permitted to choose whether to use the low graphics or full graphics user interface. When this parameter is set to On, users can also access the low graphics version of a site by appending /mobile or /m to the site path.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeLogoff</td>
<td>Specifies whether or not users are permitted to override the behavior of the workspace control feature when they log off from the server.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowCustomizePersistFolderLocation</td>
<td>Specifies whether or not users are permitted to enable/disable the feature that returns them to the last folder they visited on the Applications screen when they log on again.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeReconnectAtLogin</td>
<td>Specifies whether or not users are permitted to override the behavior of the workspace control feature at logon.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>AllowCustomizeReconnectButton</td>
<td>Specifies whether or not users are permitted to override the behavior of the workspace control feature when the Reconnect button is clicked.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowCustomizeSettings</td>
<td>Specifies whether or not users are permitted to customize their Web Interface sessions. When this parameter is set to Off, the Preferences button is not shown on users’ logon and Applications screens.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowCustomizeShowHints</td>
<td>Specifies whether or not users are permitted to show/hide hints on the Applications screen.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowCustomizeShowSearch</td>
<td>Specifies whether or not users are permitted to enable/disable searching on the Applications screen.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeSpecialFolderRedirection</td>
<td>Specifies whether or not users are permitted to enable/disable the Special Folder Redirection feature.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeTransparentKeyPassthrough</td>
<td>Specifies whether or not users are permitted to select the key combination pass-through behavior.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeVirtualCOMPortEmulation</td>
<td>Specifies whether or not users are permitted to enable/disable PDA synchronization.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeWinColor</td>
<td>Specifies whether or not users are permitted to change the color depth for ICA sessions.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowCustomizeWinSize</td>
<td>Specifies whether or not users are permitted to change the window size for ICA sessions.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowFontSmoothing</td>
<td>Specifies whether or not font smoothing is permitted for ICA sessions.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>AllowUserAccountUnlock</td>
<td>Specifies whether or not users are permitted to unlock their accounts using account self-service.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AllowUserPasswordChange</td>
<td>Specifies the conditions under which users can change their passwords.</td>
<td>Never</td>
<td>Expired-Only</td>
</tr>
<tr>
<td>AllowUserPasswordReset</td>
<td>Specifies whether or not users are permitted to reset their passwords using account self-service.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>AlternateAddress</td>
<td>Specifies whether or not to return the alternate server address in the .ica file.</td>
<td>Off</td>
<td>Mapped</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>ApplicationAccessMethods</td>
<td>Specifies whether users can access applications using a remote plugin, the Citrix XenApp Plugin for Streamed Apps, or both.</td>
<td>Remote, Streaming</td>
<td>XenApp Web, XenApp Services</td>
</tr>
<tr>
<td>AppNavLinkTitle_&lt;LanguageCode&gt;</td>
<td>Specifies a localized name for the Applications screen to appear as a button on the navigation bar. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>Applications. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AppSysMessage_&lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear at the bottom of the main content area of the Applications screen. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AppTab_&lt;n&gt;</td>
<td>Specifies tabs to be displayed on the Applications screen. Multiple instances can be used to define multiple tabs. Alternatively, a single tab containing all the published resources available to the user can be defined using the AllResources value, which is the default setting.</td>
<td>AllResources</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AppWelcomeMessage_&lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear at the top of the main content area of the Applications screen. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AuthenticationPoint</td>
<td>Specifies where user authentication takes place.</td>
<td>WebInterface</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AutoLaunchDesktop</td>
<td>Specifies whether or not the automatic launching of desktops is enabled. When this parameter is set to On, the Web Interface will automatically launch a user’s desktop if it is the only published resource available to them from all farms.</td>
<td>Off</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AutoLoginDefault</td>
<td>Specifies whether or not automatic logons are enabled by default for users accessing their published resources using pass-through, pass-through with smart card, and smart card authentication.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>BrandingColor</td>
<td>Specifies the color for the header and footer areas.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>BrandingImage</td>
<td>Specifies the URL for the branding gradient image for the header and footer areas.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>BypassFailedRadius ServerDuration</td>
<td>Specifies the time before a failed RADIUS server is considered for reuse.</td>
<td>Time in minutes (60)</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>BypassFailedSTA Duration</td>
<td>Specifies the time before a failed server running the Secure Ticket Authority is considered for reuse.</td>
<td>Time in minutes (60)</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ClientAddressMap</td>
<td>Specifies plugin address/address type pairings for the server-side firewall configuration. The first field in the entry is a subnet address and mask, while the second takes the values: Normal, Alternate, Translated, SG, SGAlternate, and SGTranslated. Using an asterisk (*) in place of a plugin address or subnet indicates the default for all otherwise unspecified plugins.</td>
<td><code>&lt;SubnetAddress&gt;/</code> <code>&lt;SubnetMask&gt;</code></td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ClientProxy</td>
<td>Specifies plugin subnet addresses and masks and associated proxy settings for a client-side firewall. The plugin address in the returned ICA file is determined by these settings. Each entry is comprised of three fields. The first is a subnet address and mask. Using an asterisk (*) indicates the default for all otherwise unspecified plugins. The second field 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 (-).</td>
<td><code>&lt;SubnetAddress&gt;/</code> <code>&lt;SubnetMask&gt;</code></td>
<td>XenApp Web</td>
</tr>
<tr>
<td>CompactHeaderImage</td>
<td>Specifies the URL for the header image for the low graphics version of the user interface.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>CompactViewStyles</td>
<td>Specifies the view styles available to users on the Applications screen of the low graphics user interface.</td>
<td>Icons, List</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ContentBgColor</td>
<td>Specifies the background color for the content area.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ContentBgImage</td>
<td>Specifies the URL for the background image for the content area.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ContentFontColor</td>
<td>Specifies the font color for the content area.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>CredentialFormat</td>
<td>Specifies the credential formats accepted for explicit Windows and NIS logons.</td>
<td>All</td>
<td>UPN</td>
</tr>
</tbody>
</table>

Parameter Description Values Site types
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Site types</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSG_EnableSession Reliability</td>
<td>Specifies whether or not to use session reliability through the Secure Gateway or Access Gateway.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>CSG_Server</td>
<td>Specifies the address of the Secure Gateway server or the Access Gateway appliance.</td>
<td>None. Server address as an FQDN</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>CSG_ServerPort</td>
<td>Specifies the port for the Secure Gateway server or the Access Gateway appliance.</td>
<td>None. Server port</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>CSG_STA_URL&lt;n&gt;</td>
<td>Specifies the URL of the server running the Secure Ticket Authority.</td>
<td>None. URL of an STA</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>DefaultApplication AccessMethod</td>
<td>Specifies whether a remote plugin or the Citrix XenApp Plugin for Streamed Apps is used to access applications by default.</td>
<td>Remote</td>
<td>Streaming</td>
</tr>
<tr>
<td>DefaultCompact ViewStyle</td>
<td>Specifies the default view style on the Applications screen of the low graphics user interface.</td>
<td>List</td>
<td>Icons</td>
</tr>
<tr>
<td>DefaultCustomText Locale</td>
<td>Specifies the default locale to use for customized text. The same locale must be specified in any customized text parameters (*.&lt;LanguageCode&gt;) that are defined.</td>
<td>None. en fr de es ja any other supported language identifier</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>DefaultViewStyle</td>
<td>Specifies the default view style on the Applications screen of the full graphics user interface.</td>
<td>Icons Details List Tree Groups</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>DisplayBrandingImage</td>
<td>Specifies whether or not to display the branding gradient image for the header and footer areas.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DisplayContentBgImage</td>
<td>Specifies whether or not to display the background image for the content area.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DisplayHeader</td>
<td>Specifies whether or not to display the header defined in header.inc.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DisplayNavCurrentLinkBgImage</td>
<td>Specifies whether or not to display the background image for the currently selected button on the navigation bar.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DisplayNavLinkBgImage</td>
<td>Specifies whether or not to display the background image for the unselected buttons on the navigation bar.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DomainSelection</td>
<td>Specifies the domain names listed on the logon screen for explicit authentication.</td>
<td>List of NetBios domain names</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>DuplicateLogInterval</td>
<td>Specifies the time period over which DuplicateLogLimit log entries are monitored.</td>
<td>Time in seconds (60)</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>DuplicateLogLimit</td>
<td>Specifies the number of duplicate log entries permitted in the time period given by DuplicateLogInterval.</td>
<td>Integer greater than 0 (10)</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>EnableFileType Association</td>
<td>Specifies whether or not file type association is enabled for a site. If this parameter is set to Off, content redirection is not available for the site.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>EnableKerberosToMPS</td>
<td>Specifies whether or not Kerberos authentication is enabled.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>EnableLegacyICA ClientSupport</td>
<td>Specifies whether or not older plugins that cannot read UTF-8 .ica files are supported. If this parameter is set to Off, the server produces .ica files in UTF-8 encoding.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>EnableLogoff Applications</td>
<td>Specifies whether or not the workspace control feature logs off active published resources when users log off from the server.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>EnablePassthroughURLs</td>
<td>Specifies whether or not users are permitted to create persistent links to published resources accessed using the Web Interface.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>EnableRadiusServer LoadBalancing</td>
<td>Specifies whether or not to permit sessions on multiple RADIUS servers to be load balanced in a random-access manner. Failover between the servers still occurs regardless of the setting for this parameter.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>EnableSTALoadBalancing</td>
<td>Specifies whether or not to permit requests to multiple servers running the Secure Gateway Secure Ticket Authority to be load balanced.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>EnableVirtualCOMPort Emulation</td>
<td>Specifies whether or not to enable PDA synchronization through tethered USB connections.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>EnableWizardAutoMode</td>
<td>Specifies whether or not the plugin detection and deployment process runs in auto mode.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>EnableWorkspace Control</td>
<td>Specifies whether or not the workspace control feature is available to users.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>ErrorCallbackURL</td>
<td>Specifies a URL for the Web Interface to redirect to when an error occurs. This setting takes four query string parameters: NFuse_MessageType, NFuse_MessageKey, NFuse_MessageArgs, NFuse_LogEventID</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>FooterText &lt;LanguageCode&gt;</td>
<td>Specifies localized footer text to appear in the footer area of all pages. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>HeadingHomePage</td>
<td>Specifies the URL for the image to appear as the heading of the home page.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>HeadingImage</td>
<td>Specifies the URL for the image to appear as the heading of the Web Interface.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>HideDomainField</td>
<td>Specifies whether or not the Domain field appears on the logon screen.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>HpUxUnixClient</td>
<td>Specifies the installation caption and link for the associated platform. Captions and links can be customized using the format Caption&amp;URL, where Caption is the display text and URL is the URL for the plugin. The specified URL is linked from the Download button on the Download Client Software page of the plugin detection and deployment process.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>IbmAixClient</td>
<td>Specifies the installation caption and link for the associated platform.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td>Captions and links can be customized using the format Caption&amp;URL, where Caption is the display text and URL is the URL for the plugin. The specified URL is linked from the Download button on the Download Client Software page of the plugin detection and deployment process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IcaClientVersion</td>
<td>Specifies the version number of the plugin (from the 'Clients directory on the installation media). Used to determine if there is a newer version of the native plugin than is currently installed on users' computers. The version number specified here will override the version number automatically detected by the Web Interface when users log on.</td>
<td>None. Latest plugin version</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>IcaWebClientClassID</td>
<td>Specifies the class ID of the ActiveX plugin.</td>
<td>238f6f83-b8b4-11cf-8771-00a024541ee3</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>IgnoreClientProvided</td>
<td>Specifies whether or not to ignore the address provided by the plugin.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>ClientAddress</td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>InternalServer</td>
<td>Specifies normal/translated address pairings. The normal address identifies the server with which the gateway communicates and the translated address is returned to the plugin.</td>
<td>NormalAddress, TranslatedAddress, …</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>AddressMap</td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>JavaClientPackages</td>
<td>Specifies the default set of Client for Java packages to download.</td>
<td>ConfigUI, PrinterMapping, SecureICA, Audio, ClientDriveMapping, Clipboard, SSL, Thinwire1, ZeroLatency</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>JavaClientRoot</td>
<td>Specifies 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.</td>
<td>None. Valid filename</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KioskMode</td>
<td>Specifies whether user settings should be persistent or last only for the lifetime of the session. When kiosk mode is enabled, user settings do not persist from one session to another.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>LaunchClients</td>
<td>Specifies the plugins from which users are permitted to select. Used in conjunction with AllowCustomizeClients.</td>
<td>Ica-Local, Ica-Embedded, Ica-Java, Rdp-Embedded</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinuxClient</td>
<td>Specifies the installation caption and link for the associated platform.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LoginDomains</td>
<td>Specifies the domain names used for access restriction.</td>
<td>List of NetBIOS domain names</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>LoginSysMessage_&lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear at the bottom of the main content area of the logon screen. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>LoginTitle_&lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear above the welcome message on the logon screen. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>LogoffFederationService</td>
<td>Specifies whether to log users off from XenApp Web sites only or globally from the Federation Service when the Log Off button is clicked in an AD FS integrated site.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>MacClient</td>
<td>Specifies the installation caption and link for the associated platform.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>MessagesNavLinkTitle_ &lt;LanguageCode&gt;</td>
<td>Specifies a localized name for the Messages screen to appear as a button on the navigation bar. <em>LanguageCode</em> is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>Messages. Plain text plus any number of new line HTML <code>&lt;br&gt;</code> tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Messages WelcomeMessage_ &lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear at the top of the main content area of the Messages screen. <em>LanguageCode</em> is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML <code>&lt;br&gt;</code> tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavCurrentLinkBgColor</td>
<td>Specifies the background color for the currently selected button on the navigation bar.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavCurrentLinkBgImage</td>
<td>Specifies the URL for the background image for the currently selected button on the navigation bar.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavCurrentLinkFontColor</td>
<td>Specifies the font color for the currently selected button on the navigation bar.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavLinkBgColor</td>
<td>Specifies the background color for the unselected buttons on the navigation bar.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavLinkBgImage</td>
<td>Specifies the URL for the background image for the unselected buttons on the navigation bar.</td>
<td>Valid URL</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NavLinkFontColor</td>
<td>Specifies the font color for the unselected buttons on the navigation bar.</td>
<td>Hex color number or color name</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>NDSContextLookup Loadbalancing</td>
<td>Specifies whether or not to load balance the configured LDAP servers.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>NDSContextLookup Servers</td>
<td>Specifies the LDAP servers to use. If the port is not specified, it is inferred from the protocol; if this parameter is set to ldap, the default LDAP port (389) is used; if the setting is ldaps, the default LDAP over SSL port (636) is used. A maximum of 512 LDAP servers can be configured. If this parameter is undefined or not present, the contextless logon functionality is disabled.</td>
<td>None. ldap://[:][:]</td>
<td>ldaps://[:][:]</td>
</tr>
</tbody>
</table>
| NDSTreeNodeName                 | Specifies the NDS tree to use when using NDS authentication.               | None. NDS tree                                                         | XenApp Web | XenApp Services
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Site types</th>
</tr>
</thead>
<tbody>
<tr>
<td>OverlayAutologon</td>
<td>Specifies whether a logon ticket must be duplicated in a logon ticket entry or placed in a separate.ica launch file ticket entry only. When credential overlay is enabled, logon tickets are duplicated.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>CredsWithTicket</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OverrideIcaClientname</td>
<td>Specifies whether or not a Web Interface-generated ID must be passed in the clientname entry of an .ica launch file.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>PasswordExpiry</td>
<td>Specifies the number of days before password expiration when users are prompted to change their passwords.</td>
<td>Integer between 0 and 999 (14)</td>
<td></td>
</tr>
<tr>
<td>WarningPeriod</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PersistFolderLocation</td>
<td>Specifies whether or not users are returned to the last folder they visited on the Applications screen when they log on again.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>PNAChangePasswordMethod</td>
<td>Specifies how Citrix XenApp deals with change password requests from users. If this parameter is set to Direct-Only, the plugin changes the password by communicating directly with the domain controller. Direct-With-Fallback indicates that the plugin initially tries to contact the domain controller, but uses the XenApp Services site if this fails. The Proxy option indicates that the plugin changes passwords by contacting the XenApp Services site.</td>
<td>Direct-Only</td>
<td>Direct-With-Fallback</td>
</tr>
<tr>
<td>PooledSockets</td>
<td>Specifies whether or not to use socket pooling.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>PreLoginMessageButton_&lt;LanguageCode&gt;</td>
<td>Specifies a localized name for the pre-logon message confirmation button. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>PreLoginMessageText_&lt;LanguageCode&gt;</td>
<td>Specifies localized text to appear on the pre-logon message page. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>PreLoginMessageTitle_&lt;LanguageCode&gt;</td>
<td>Specifies a localized title for the pre-logon message page. LanguageCode is en, fr, de, es, ja, or any other supported language identifier.</td>
<td>None. Plain text plus any number of new line HTML &lt;br&gt; tags and hyperlinks</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RADEClientClassID</td>
<td>Specifies the classID of the Citrix XenApp Plugin for Streamed Apps.</td>
<td>4384F3C5-4A9E-4E81-9AAE-4251C2813861</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>RADEClientVersion</td>
<td>Specifies the version number of the plugin (from the <code>Clients</code> directory on the installation media). Used to determine if there is a newer version of the Citrix XenApp Plugin for Streamed Apps than is currently installed on users' computers. The version number specified here will override the version number automatically detected by the Web Interface when users log on.</td>
<td>None. Latest plugin version</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RADESessionURL</td>
<td>Specifies the URL for the RADE session page. If this parameter is set to auto, the URL is generated automatically.</td>
<td>auto. Valid URL</td>
<td>XenApp Web XenApp Services</td>
</tr>
<tr>
<td>RadiusRequestTimeout</td>
<td>Specifies the time-out value to use when waiting for a response from the session's RADIUS server.</td>
<td>Time in seconds (30)</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RadiusServers</td>
<td>Specifies the RADIUS servers to use and, optionally, the ports on which they listen. Servers can be specified using IP addresses or names, and the server and port for each element are separated using a colon. If the port is not specified, the default RADIUS port (1812) is assumed. A maximum of 512 RADIUS servers can be configured.</td>
<td>$Server[,Port][,…]$</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RdpWebClient</td>
<td>Specifies the file name of the Remote Desktop Connection (RDP) software used for embedded launches and auto-deployment of this plugin.</td>
<td>msrdp.cab</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RdpWebClientClassID</td>
<td>Specifies the class ID of the Remote Desktop Connection (RDP) ActiveX plugin.</td>
<td>7584c670-2274-4efb-b00b-d6aaba6d3850</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>RdpWebClientVersion</td>
<td>Specifies the version number of the Remote Desktop Connection (RDP) software shipped with Windows.</td>
<td>5,2,3790,0</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>ReconnectAtLogin</td>
<td>Specifies whether or not workspace control should reconnect to published resources when users log on, and if so, whether to reconnect all resources or disconnected resources only.</td>
<td>DisconnectedAndActive</td>
<td>None</td>
</tr>
<tr>
<td>ReconnectButton</td>
<td>Specifies whether or not workspace control should reconnect to published applications when users click the Reconnect button, and if so, whether to reconnect to all resources or disconnected resources only.</td>
<td>DisconnectedAndActive</td>
<td>None</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>RequestICAClientSecure</td>
<td>Specifies TLS settings.</td>
<td>Detect-AnyCiphers,</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>Channel</td>
<td></td>
<td>TLS-GovCiphers,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL-AnyCiphers</td>
<td></td>
</tr>
<tr>
<td>RequestedHighColor Icons</td>
<td>Specifies whether or not high color depth 32-bit icons are requested from</td>
<td>None. 16, 32, 48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Citrix XML Service, and if so, lists the icon sizes in pixels. If this</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>parameter is set to None, only the standard 4-bit 32 x 32 icons are</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>requested. The default setting varies according to the site type and its</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequireLaunch Reference</td>
<td>Specifies whether or not the use of launch references is enforced.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RestrictDomains</td>
<td>Specifies whether or not the LoginDomains parameter is used to restrict user</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RetryCount</td>
<td>Specifies the number of times a failed request to the Citrix XML Service is</td>
<td>Integer greater than 0 (5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>retried before the service is deemed to have failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ScoUnixClient</td>
<td>Specifies the installation caption and link for the associated platform.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Captions and links can be customized using the format Caption&amp;URL, where</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Caption is the display text and URL is the URL for the plugin. The specified</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL is linked from the Download button on the Download Client Software page</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the plugin detection and deployment process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SearchContextList</td>
<td>Specifies context names for use with NDS authentication.</td>
<td>None. Comma-separated list of context names</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServerAddressMap</td>
<td>Specifies normal/translated address pairings for the server-side firewall</td>
<td>NormalAddress,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration. The normal address identifies the server and the translated</td>
<td>TranslatedAddress, …</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address is returned to the plugin.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SgiUnixClient</td>
<td>Specifies the installation caption and link for the associated platform.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Captions and links can be customized using the format Caption&amp;URL, where</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Caption is the display text and URL is the URL for the plugin. The specified</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL is linked from the Download button on the Download Client Software page</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the plugin detection and deployment process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>ShowClientInstallCaption</td>
<td>Specifies how and when installation captions appear. Setting this parameter to Auto causes installation captions to be shown if users do not have a plugin installed or if a better plugin is available. If the parameter is set to Quiet, installation captions are shown only if users do not have a plugin. The behavior of the logon screen is slightly different in that captions are shown only for remote plugins and only if no plugin is detected. Hence, there is no difference between the Auto and Quiet settings for the logon screen.</td>
<td>Auto</td>
<td>Quiet</td>
</tr>
<tr>
<td>ShowHints</td>
<td>Specifies whether or not hints appear on the Applications screen.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>ShowPasswordExpiryWarning</td>
<td>Specifies whether or not users are prompted to change their passwords before they expire, and if so, what the warning period should be.</td>
<td>Never</td>
<td>WindowsPolicy</td>
</tr>
<tr>
<td>ShowRefresh</td>
<td>Specifies whether or not the Refresh button is available for users on the Applications screen.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>ShowSearch</td>
<td>Specifies whether or not the Search control is available for users on the Applications screen.</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>SolarisUnixClient</td>
<td>Specifies the installation caption and link for the associated platform. Captions and links can be customized using the format Caption&amp;URL, where Caption is the display text and URL is the URL for the plugin. The specified URL is linked from the Download button on the Download Client Software page of the plugin detection and deployment process.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td></td>
</tr>
<tr>
<td>SpecialFolderRedirection</td>
<td>Specifies whether or not the Special Folder Redirection feature is enabled. If this parameter is set to On, published resources are directed to use the Documents and Desktop folders on users’ local computers. Setting the parameter to Off indicates that the Documents and Desktop folders available in published applications will be those on the server.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Site types</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the time-out value to use when communicating with the Citrix XML service.</td>
<td>Time in seconds (60)</td>
<td>XenApp Web XenApp Services</td>
</tr>
<tr>
<td>TransparentKey Passthrough</td>
<td>Specifies the mode of Windows key combinations pass-through.</td>
<td>Local</td>
<td>Remote</td>
</tr>
<tr>
<td>Tru64Client</td>
<td>Specifies the installation caption and link for the associated platform. Captions and links can be customized using the format Caption&amp;URL, where Caption is the display text and URL is the URL for the plugin. The specified URL is linked from the Download button on the Download Client Software page of the plugin detection and deployment process.</td>
<td>&quot;Default&quot;. Caption and link</td>
<td>XenApp Web</td>
</tr>
<tr>
<td>TwoFactorPassword Integration</td>
<td>Specifies whether or not to enable password integration with RSA SecurID 6.0.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>TwoFactorUseFully QualifiedUserNames</td>
<td>Specifies whether or not to pass fully qualified user names to the authentication server during two-factor authentication.</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>UPNSuffixes</td>
<td>Specifies suffixes to which UPN authentication is restricted for explicit authentication.</td>
<td>List of UPN suffixes</td>
<td>XenApp Web XenApp Services</td>
</tr>
<tr>
<td>UserInterfaceBranding</td>
<td>Specifies the branding focus for the site.</td>
<td>Applications</td>
<td>Desktops</td>
</tr>
<tr>
<td>UserInterfaceLayout</td>
<td>Specifies whether or not to use the compact user interface.</td>
<td>Auto</td>
<td>Normal</td>
</tr>
<tr>
<td>UserInterfaceMode</td>
<td>Specifies the appearance of the logon screen. If this parameter is set to Simple, only the logon fields for the selected authentication method are shown. Setting the parameter to Advanced displays the navigation bar, which provides access to the pre-logon Messages and Preferences screens.</td>
<td>Simple</td>
<td>Advanced</td>
</tr>
<tr>
<td>ViewStyles</td>
<td>Specifies the view styles available to users on the Applications screen of the full graphics user interface.</td>
<td>Icons</td>
<td>Details</td>
</tr>
<tr>
<td>WebSessionTimeout</td>
<td>Specifies the time-out value for idle browser sessions.</td>
<td>Time in minutes (20)</td>
<td>XenApp Web</td>
</tr>
</tbody>
</table>
Specific WebInterface.conf parameter settings affect the validation of Citrix XenApp requests. Citrix recommends that the settings in WebInterface.conf be consistent with settings in the config.xml file in Citrix XenApp.

### 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 icons for published resources: in the **Start** menu, on the physical 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 controls on the Application Display page of the XenApp plugin **Options** dialog box.

- **DesktopIntegration**: Specifies whether or not to add shortcuts to the **Start** menu, desktop, or notification area.

- **ConfigurationFile**: Specifies a different URL for config.xml for the plugin to use in the future. This facilitates moving users to a different Web Interface server.
• **Request.** Specifies from where the plugin should request published resource data 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.

• **ChangePassword.** Specifies under what circumstances Citrix XenApp users are permitted to change their passwords and the path through which the request is routed.

• **UserInterface.** Specifies whether to hide or display certain groups of options presented to users as part of the Citrix XenApp interface.

• **ReconnectOptions.** Specifies whether or not workspace control functionality is available to users.

• **FileCleanup.** Specifies whether or not shortcuts are deleted when users log off from Citrix XenApp.

• **ICA_Options.** Defines the display and sound options for plugin connections. This corresponds to the settings on the Session Options page of the XenApp plugin Options dialog box.

• **AppAccess.** Specifies the types of published resources available to users.

For more information about using the config.xml file, see the *XenApp Plugin for Hosted Apps 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 parameters that affect Citrix XenApp and their recommended settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginType</td>
<td>NDS must be enabled in config.xml.</td>
</tr>
<tr>
<td>NDSTreeName</td>
<td>DefaultTree in the Logon section of config.xml must contain the same setting.</td>
</tr>
<tr>
<td>PNAChangePasswordMethod</td>
<td>Method in the ChangePassword section of config.xml must contain the same setting.</td>
</tr>
<tr>
<td>WIAuthenticationMethods</td>
<td>Use the same authentication method configured in the WebInterface.conf file. Authentication fails if this method differs in config.xml.</td>
</tr>
</tbody>
</table>
To configure the Web Interface when using Citrix XenApp

1. Using a text editor, open the WebInterface.conf file.
2. Locate the following parameters:
   - LoginType
   - NDSTreeName
   - PNACChangePasswordMethod
   - WIAuthenticationMethods
3. Amend the settings for these parameters as described in the table above.
4. Restart the Web Interface server to apply the changes.

For more information about WebInterface.conf file settings, see “Configuring Sites Using the Configuration File” on page 133.

Examples

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

Configuring Communication with the 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 Web Interface server.

Communication is currently with a server called “rock,” but you want to add a server called “roll” in case rock fails. To do this:

1. Using a text editor, open the WebInterface.conf file and locate the following line:

   Farm1=rock,Name:Farm1,XMLPort:80,Transport:HTTP,
   SSLRelayPort:443,…

2. Edit this line to include the additional server, as follows:

   Farm1=rock,roll,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 XenApp or Desktop Delivery Controller using Secure Sockets Layer (SSL). The Citrix SSL Relay is installed on the server running XenApp or Desktop Delivery Controller, which has a fully qualified domain name of “blues.mycompany.com.” The Citrix SSL Relay listens for connections on TCP port 443.

Communication is currently with a server called “rhythm,” but you want to replace rhythm with blues.mycompany.com. To do this:

1. Using a text editor, open the WebInterface.conf file and locate the following line:
   
   Farm1=rhythm,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443

2. Change the transport to SSL, as follows:

   Farm1=blues.mycompany.com,Name:Farm1,XMLPort:80,Transport:SSL,SSLRelayPort:443

**Note:** The specified server name 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.mycompany.com” on which Citrix plugins use port 443, using the following two Secure Ticket Authority addresses:


Include the following lines in WebInterface.conf:

```
AlternateAddress=Mapped
CSG_STA_URL1=http://country.mycompany.com/scripts/ctxsta.dll
CSG_STA_URL2=http://western.mycompany.com/scripts/ctxsta.dll
CSG_Server=csg1.mycompany.com
CSG_ServerPort=443
ClientAddressMap=*,SG
```

The final line enables the Secure Gateway for all users.
## Settings in the bootstrap.conf File

The following table lists the settings in the bootstrap.conf file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Site types</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConfigurationLocation</td>
<td>Specifies from where Web Interface</td>
<td>Path to configuration file within the web app</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td>should load the configuration.</td>
<td>[ConfigSvrDef]</td>
<td>XenApp Services</td>
</tr>
<tr>
<td></td>
<td>ConfigSvr is either the DNS name or an IP address of the configuration proxy.</td>
<td>ConfigSvrDef = ConfigSvr [;ConfigSvr]* [;Port:&lt;Port&gt;] [;Transport:&lt;HTTP</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTPS</td>
<td>SSL&gt;] [;SSLRelayPort:&lt;Port&gt;]</td>
</tr>
<tr>
<td>ConfigurationSource</td>
<td>Specifies which type of configuration is</td>
<td>Local</td>
<td>ConfigurationService</td>
</tr>
<tr>
<td>Type</td>
<td>used by the site.</td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>DefaultLocale</td>
<td>Specifies the default language to be used</td>
<td>en</td>
<td>fr</td>
</tr>
<tr>
<td></td>
<td>if a browser requests a non-supported language.</td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td>SiteIDRoot</td>
<td>A string that provides the basis of a</td>
<td>Random number generated by the installer</td>
<td>XenApp Web</td>
</tr>
<tr>
<td></td>
<td>unique site identifier. On IIS, this is used</td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td></td>
<td>directly as the site identifier when</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>communicating with the Configuration Service. On</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Java application servers, runtime information is</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>added to form the site identifier.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SiteName</td>
<td>Specifies the name of the site that appears in</td>
<td>Valid string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Access Management Console. The default</td>
<td></td>
<td>XenApp Services</td>
</tr>
<tr>
<td></td>
<td>setting uses the URL of the site.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Active Directory Federation Services Support for the Web Interface

This section describes how to create and configure Microsoft Active Directory Federation Services (AD FS) integrated Web Interface sites. Topics include:

• Before Creating Active Directory Federation Services Sites
• Creating Active Directory Federation Services Integrated Sites
• Configuring Your Site as an Active Directory Federation Services Application

About Active Directory Federation Services

Microsoft Active Directory Federation Services support for the Web Interface allows the resource partner of an AD FS deployment to use XenApp. Administrators can create AD FS sites to provide users with access to published applications and content on the resource partner.

Important: AD FS requires secure communications between the Web browser, Web server, and federation servers. Web Interface users must use HTTPS/SSL to access the site.

What Is Active Directory Federation Services?

Active Directory Federation Services is a feature of Windows Server 2008 and Windows Server 2003 R2. AD FS provides single sign-on technology to authenticate users to multiple applications in a single session.
AD FS 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 AD FS trust relationships, AD FS must be deployed in both organizations. AD FS 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 AD FS requires a federation server for 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.

**Active Directory Federation Services Terminology**

The following table contains basic terms used when describing AD FS.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account partner</td>
<td>Client organization that wants to use the applications from the resource partner. The account partner provides the identities (user accounts).</td>
</tr>
<tr>
<td>Federation server</td>
<td>Federation servers host the Federation Service component of AD FS, 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.</td>
</tr>
<tr>
<td>Federation server proxy</td>
<td>Federation server proxies host the Federation Service proxy component of AD FS. You can deploy federation server proxies in the demilitarized zone (DMZ) to forward requests to federation servers that are not accessible from the Internet.</td>
</tr>
<tr>
<td>Federation Service</td>
<td>A service in Windows Server 2008 and Windows Server 2003 R2 that uses Active Directory to provide tokens in response to requests by trusted partners.</td>
</tr>
<tr>
<td>Federation Service proxy</td>
<td>Federation Service proxies collect user credential information from browser plugins and applications and send the information to the Federation Service.</td>
</tr>
<tr>
<td>Resource partner</td>
<td>Organization that makes services or applications available over the Internet.</td>
</tr>
<tr>
<td>Shadow account</td>
<td>Shadow accounts are created in Active Directory on the resource partner. They mirror user accounts existing on the account partner.</td>
</tr>
</tbody>
</table>
How Active Directory Federation Services Integrated Sites Work

The following steps occur when a user on an account partner accesses a published application on a resource partner:

- **Step 1.** A user opening the Web Interface home page on the resource partner is redirected to the account partner’s authentication page.

- **Step 2.** The account partner authenticates the user and sends a security token back to the resource partner.

- **Step 3.** AD FS 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 screen.

- **Step 4.** The Web Interface displays the application set for the user.

The figure shows the steps that occur when users from the account partner domain log on to access their application sets.

- **Step 5.** The user launches an application by clicking a hyperlink on the page. Web Interface contacts the Citrix XML Service to request a launch.

- **Step 6.** The Citrix XML Service generates Security Support Provider Interface data and sends it to a XenApp server.
• **Step 7.** The server uses the Security Support Provider Interface data to authenticate the user and stores a logon token for future authentication.

• **Step 8.** The server generates a launch ticket to uniquely represent the stored logon token and returns this ticket to the Citrix XML Service.

• **Step 9.** The Citrix XML Service returns the launch ticket to the Web Interface.

• **Step 10.** The Web Interface creates an .ica file containing the launch ticket and sends it to the user’s browser.

• **Step 11.** The client device opens the .ica file and attempts an ICA connection to the server.

• **Step 12.** The plugin sends the launch ticket to the XenApp server.

• **Step 13.** The 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.

*The figure shows the steps that occur when users from the account partner domain launch published applications.*
Depending on the settings configured for a site, when users log off, they log off from either the Web Interface or the Web Interface and AD FS. If they log off from the Web Interface and AD FS, they log off from all AD FS applications.

Software Requirements for Active Directory Federation Services

The following software must be installed and configured in your environment:

- Windows Server 2008 or Windows Server 2003 R2 for the federation and Web servers.
- Active Directory Federation Services on the resource and account partners. Both the claims-aware and Windows token-based AD FS Web Agents should be installed.

Before Creating Active Directory Federation Services Sites

Before you create an AD FS site, you must carry out the following steps. Disregarding any of them could mean that you are unable to create a site.

- 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 could appear to have expired. To avoid this problem, both organizations must synchronize their servers with the same Internet time server. For more information, see “Setting up the Relationships Between Domains” on page 160.

- Ensure the resource partner federation and Web servers can access the Certificate Authority’s certificate revocation lists (CRLs). AD FS may fail if the servers cannot ensure that a certificate is not revoked. For more information, see “Setting up the Relationships Between Domains” on page 160.

- Ensure all servers within your deployment are trusted for delegation. For more information, see “Configuring Delegation for the Servers in Your Deployment” on page 162.

- Set up shadow accounts in the resource partner domain for each external user who can authenticate to the Web Interface through AD FS. For more information, see “Setting up Shadow Accounts” on page 166.
• Install XenApp, ensuring that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

• Set up a trust relationship between the Web Interface server and any other servers in the farm running the Citrix XML Service that the Web Interface contacts. For more information see, “To set up the trust relationship” on page 115.

**Important:** This guide does not document how to install AD FS. You must have a working AD FS installation, with external account users able to access AD FS-enabled applications in a resource partner, before you attempt to create an AD FS site.

### Setting up the Relationships Between Domains

The deployment documented here consists of two domains (in their own forests), one for the account partner and one for the resource partner. Note that 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.

   The account partner requires:
   - Domain controller
   - Federation server*
   - Client devices

   The resource partner requires:
   - Domain controller
   - Federation server*
   - Web server*
   - One or more servers for a XenApp farm

Components marked with an asterisk (*) must be on computers running Windows Server 2008 or Windows Server 2003 R2 and have the **Active Directory Federation Services** server role installed. In the case of the Web server, the **Claims-aware Agent** and **Windows Token-based Agent** role services need to be installed in addition to all the role services for the **Web Server (IIS)** server role.
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.
   - The server certificate identifies a specific computer, so you must know the fully qualified domain name (FQDN) of each server; for example, “xenappserver1.mydomain.com.”
   - Install the Web server certificate into Microsoft Internet Information Services (IIS) to enable the IIS default Web site for SSL traffic.

3. To ensure the resource partner’s federation server trusts the account partner’s federation server, install the account partner’s federation certificate into the Trusted Root Certification Authorities store on 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 certificate into the Trusted Root Certification Authorities store on the Web server.

**Important:** The resource federation and Web servers must be able to access the Certificate Authority’s CRLs. The resource federation server must have access to the account partner’s Certificate Authority and the Web server must have access to the resource partner’s Certificate Authority. AD FS may fail if the servers cannot ensure that a certificate is not 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**, 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 could 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 16:00 Eastern Standard Time (EST). The resource partner in California has to be set to within 12:55 to 13:05 Pacific Standard Time (PST). (There is a three hour difference between the EST and PST time zones.)

10. On the Web server, open the MMC Internet Information Services (IIS) Manager snap-in.

11. Select your Web server in the left pane and, in the **Features View**, double-click **Federation Service URL**.

12. On the **Federation Service URL** page, enter the URL for the resource partner federation server and click **Apply** in the **Actions** pane.

## Configuring Delegation for the Servers in Your Deployment

You must ensure that all servers within your deployment are trusted for delegation. To do this, complete the following tasks while logged on as a domain administrator on the domain controller for the resource partner domain. Procedures for each task are included in this section.

- Ensure the resource partner domain is at the correct functional level
- Trust the Web Interface server for delegation
- Trust the server running the Citrix XML Service for delegation
- Determine which published resources are accessible from the XenApp server
To ensure the resource partner domain is at the correct functional level

**Important:** To raise the domain level, all domain controllers in the domain must be running either Windows Server 2008 or Windows Server 2003. Do not raise the domain functional level to Windows Server 2008 if you have or plan to add domain controllers running Windows Server 2003. After the domain functional level is raised, it cannot be rolled back to a lower level.

1. On the resource partner domain controller, open the MMC Active Directory Domains and Trusts snap-in.
2. In the left pane, select the resource partner domain name and, on the **Action** menu, click **Properties**.
3. If the domain is not at the highest possible functional level, select the domain name and, on the **Action** menu, click **Raise Domain Functional Level**.
4. To raise the domain functional level, click the appropriate level and click **Raise**.

To trust the Web Interface server for delegation

1. On the resource partner domain controller, open the MMC Active Directory Users and Computers snap-in.
2. On the **View** menu, click **Advanced Features**.
3. In the left pane, click the **Computers** node under the resource partner domain name and select the Web Interface server.
4. On the **Action** menu, click **Properties**.
5. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.
6. In the **Add Services** dialog box, click **Users or Computers**.
7. In the **Select Users or Computers** dialog box, type the name of the server running the Citrix XML Service in the **Enter the object names to select** box and click **OK**.
8. Select the **http** service type from the list and click **OK**.
9. On the Delegation tab, verify the http service type for the XenApp server appears on the Services to which this account can present delegated credentials list and click OK.

10. Repeat the process for each server in the farm running the Citrix XML Service that the Web Interface is configured to contact.

To trust the server running the Citrix XML Service for delegation
1. On the resource partner domain controller, open the MMC Active Directory Users and Computers snap-in.
2. In the left pane, click the Computers node under the resource partner domain name and select the server running the Citrix XML Service that the Web Interface is configured to contact.
3. On the Action menu, click Properties.
4. On the Delegation tab, click Trust this computer for delegation to specified services only and Use Kerberos only, and then click Add.
5. In the Add Services dialog box, click Users or Computers.
6. In the Select Users or Computers dialog box, type the name of the server running the Citrix XML Service in the Enter the object names to select box and click OK.
7. Select the HOST service type from the list and click OK.
8. On the Delegation tab, verify the HOST service type for the server running the Citrix XML Service appears on the Services to which this account can present delegated credentials list and click OK.
9. Repeat the process for each server in the farm running the Citrix XML Service that the Web Interface is configured to contact.

To determine which resources are accessible from the XenApp server
1. On the resource partner domain controller, open the MMC Active Directory Users and Computers snap-in.
2. In the left pane, click the Computers node under the resource partner domain name and select the XenApp server.
3. On the Action menu, click Properties.
4. On the Delegation tab, click Trust this computer for delegation to specified services only and Use Kerberos only, and then click Add.
5. In the Add Services dialog box, click Users or Computers.
6. In the **Select Users or Computers** dialog box, type the name of the resource partner federation server in the **Enter the object names to select** box and click **OK**.

7. Select the **cifs** and **ldap** service types from the list and click **OK**.

   **Note:** If two choices appear for the **ldap** service, select the one that matches the FQDN of the domain controller.

8. On the **Delegation** tab, verify the **cifs** and **ldap** service types for the resource partner domain controller appear on the **Services to which this account can present delegated credentials** list and click **OK**.

9. Repeat the process for each XenApp server in the farm.

**Configuring Servers for Constrained Delegation**

For security reasons, you must configure all XenApp servers for constrained delegation. To provide users with access to resources on those servers, you must add the relevant services to the **Services to which this account can present delegated credentials** list using the MMC Active Directory Users and Computers snap-in. For example, to allow users to authenticate to a Web server on host “peter,” add the **http** service for server peter; to allow users to authenticate to an SQL server on host “lois,” add the **MSSQLSvc** service for server lois.

For more detailed information, see the **Service Principal Names and Delegation in Presentation Server** white paper ([CTX110784](#)) in the Citrix Knowledge Center.

**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.

**Configuring a Time Limit for Access to Resources**

By default, AD FS 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 Citrix XML Service:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\S4UTicketLifetime
```
This value specifies the number of minutes for which users have access to resources after a session starts.

The domain security policy governs the maximum value you can set for S4ULifetime. If you specify a value for S4UTicketLifetime 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. On the resource partner domain controller, open the MMC Domain Security Policy snap-in.
2. In the left pane, select Account Policies > Kerberos Policy.
3. In the details pane, select Maximum lifetime for service ticket.
4. On the Action menu, click Properties.
5. Enter the required time limit (in minutes) in the Ticket expires in box and click OK.

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 XenApp server. If you select this option, any value specified for S4UTicketLifetime is ignored.

For more information, see Microsoft’s Web site at http://support.microsoft.com/.

Setting up Shadow Accounts

To launch applications, XenApp requires real Windows accounts. Therefore, you must manually create a shadow account in the resource partner domain for each external user who authenticates to the Web Interface through AD FS.

If you have a large number of users in the account partner domain who access applications and content 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 while logged on as a domain 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 user principal name suffixes
1. On the resource partner domain controller, 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 “adomain.com,” add **adomain.com** as the UPN suffix. Click **OK**.

To define the shadow account user
1. On the resource partner domain controller, open the MMC Active Directory Users and Computers snap-in.
2. In the left pane, select the resource partner domain name.
3. On the **Action** menu, click **New > User**.
4. Type the user’s first name, initials, and last name in the corresponding boxes.
5. In the **User logon name** box, type the account name. Make sure this name matches the name on the account partner domain controller.
6. From the list, choose the external UPN suffix and click **Next**.
7. In the **Password** and **Confirm password** boxes, type a password that meets your password policy. This password is never used because the user authenticates through AD FS.
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 Active Directory Federation Services Integrated Sites

Run the Create site task from the Access Management Console and configure the Web Interface site to use AD FS for authentication.

**Note:** The delivery of XenDesktop virtual desktops in an AD FS environment is not supported. Additionally, the Client for Java and embedded Remote Desktop Connection (RDP) software are not supported for accessing AD FS integrated sites.

**To create an Active Directory Federation Services integrated site**

1. Click Create site.
2. Select XenApp Web and click Next.
3. On the Specify IIS Location page, enter your required settings and click Next.
4. On the Specify Point of Authentication page, select At Microsoft AD FS account partner. Set the return URL for the Web Interface and click Next.
5. Confirm the settings for the new site and click Next.
6. Click Finish to exit the wizard.

Configuring Your Site as an Active Directory Federation Services Application

After creating your site, you must configure it as an AD FS application so the federation server recognizes it.

**To configure your site as an Active Directory Federation Services application**

1. On the resource partner federation server, open the MMC Active Directory Federation Services snap-in.
2. In the left pane, select Federation Service > Trust Policy > My Organization > Applications.
4. Click Next, select **Claims-aware application**, and click Next again.

5. Enter a name for your site in the **Application display name** box.

6. In the **Application URL** box, enter the URL of your Web Interface site *exactly* as it appeared in the **Web Interface return URL** box when you created the site and click Next.

   **Important:** Make sure you use HTTPS and the FQDN of your Web server.

7. Select the **User principal name (UPN)** check box and click Next.

8. Ensure that the **Enable this application** check box is selected and click Next.

9. Click **Finish** to add your site as an AD FS application.

**Testing Your Deployment**

After configuring your site as an AD FS application, test your deployment to ensure everything is working correctly between the account partner and the resource partner.

**To test the Web Interface Active Directory Federation Services deployment**

1. Log on to a client device in the account partner domain.

2. Open a Web browser and type the FQDN URL of the AD FS integrated Web Interface site that you previously created. Your application set appears.

   **Note:** If you did not configure AD FS for integrated authentication, you may be prompted to enter your credentials or insert a smart card.

3. If you did not install the Citrix XenApp Plugin for Hosted Apps, do so now. For more information, see the *XenApp Plugin for Hosted Apps Administrator’s Guide.*

4. Click an application to launch it.
Logging off from Active Directory Federation Services Integrated Sites

Use the **Configure authentication methods** task in the Access Management Console to specify whether users clicking the **Log Off** or **Disconnect** buttons on the Web site log off from:

- The Web Interface only
- The Web Interface and the AD FS Federation Service

If you specify that users log off from the Web Interface only, they are directed to the Web Interface logoff screen. If you specify that users log off from the Web Interface and the AD FS Federation Service, they are directed to the federation service logoff page and logged off from all AD FS applications.

**Note:** Users who authenticate using AD FS cannot unlock their XenApp sessions because they do not know their passwords. To unlock sessions, users must log off from the Web Interface, then log back on using AD FS authentication and relaunch their applications. When they do this, the previous session unlocks and the new launch window closes.

**To specify which services users log off from**

1. Click **Configure authentication methods**.

2. To specify that users log off from the Web Interface and AD FS federation service, select the **Perform global logoff** check box. To specify that users log off from the Web Interface only, clear the **Perform global logoff** check box.
Index

A
Access Gateway
  about 13
  configuring the Web Interface for 101
  deploying with the Web Interface 44
  integrating XenApp Web sites 45
  making resources available to users 45
  overview 122
  support 13
Access Management Console 12, 37
  about 37
  getting started 40
  using 39
account partner 156
account self-service 14
  account unlock 70
  configuring 70
  password reset 70
account unlock
  configuring 70
Active Directory Federation Services, see AD FS
AD FS 159
  overview 155
  software requirements 159
  terminology 156
adding
  server farms 56
address translations
  editing 100
alerts 16
alternate address settings
  editing 99
anonymous authentication 64
  security considerations 64
application refresh options
  managing 118
application shortcuts
  managing 118
authentication
  anonymous 64
  explicit 63, 68
  methods 63
  pass-through 63, 73
  pass-through with smart card 64
  prompt 63
  recommendations 65
  smart card 64
  two-factor 80
authentication settings
  specifying 43
authentication type
  configuring 66
automatic logon settings
  configuring 66
automatic refresh
  configuring 61
B
backup URLs
  specifying 61
bandwidth control 110
bootstrap.conf
  parameters 154
C
centrally configured sites
  upgrading 50
certificate key size 121
changing
  session options 117
Citrix documentation set 9
Citrix SSL Relay 58
  configuring the Web Interface for 153
  overview 121
  see also SSL
Citrix XenApp
configuration settings 150
configuring 38, 98
config.xml 98
password reset 14, 72
securing 124
Citrix XenApp for UNIX
viewing XML service port assignment 27
Citrix XenApp for Windows
viewing XML service port assignment 27
Citrix XenApp Plugin for Hosted Apps
configuring for pass-through 74
configuring for smart card 76
Citrix XenApp Plugin for Streamed Apps 88
Citrix XML Service
configuring communication with 60, 152
configuring fault tolerance 57
role in the Web Interface 16
TCP/IP port configuration 58
viewing the port assignment 27
client devices
requirements 26
role in the Web Interface 17
security 124, 130
Client for Java
deploying with custom certificates 95
deployment of components 93
overview 93
using private root certificates with 94
client-side proxy settings
editing 104
command line 32
configuration source
managing 53
configure and run discovery 40
configuring
account self-service 70
account unlock 70
authentication type 66
automatic logon settings 66
automatic refresh 61
communication with the Citrix XML Service 60
constrained delegation 165
domain restriction settings 65
fault tolerance 102
password reset 70
password settings 69, 72
site redirection 62
SSL/TLS communication 61
using the Access Management Console 12, 37
using WebInterface.conf 38
workspace control 113
config.xml 38
about 98
constrained delegation
configuring 165
content publishing 13
content redirection
disabling 60
enabling 60
context-sensitive Help 40
controlling
diagnostic logging 131
cookies 125
creating sites 42
customizing
appearance for users 107
screen appearance 108
screen content 108
screen layout 107
server URL 61
D
default access settings
editing 102
deploying
Web Interface and Access Gateway 44
diagnostic logging
controlling 131
direct access routes
editing 99
disabling
content redirection 60
error messages 134
discovery
configuring 40
running 40
domain restriction settings
configuring 65
domains
correct functional level 163
setting up relationships between 160
E
editing
address translations 100
alternate address settings 99
client-side proxy settings 104
default access settings 102
direct access routes 99
gateway settings 101

enabling
content redirection 60
pass-through authentication 73
prompt authentication 71
socket pooling 59
two-factor authentication 70
workspace control 115

error messages
disabling 134
expiry time
tickets 58
explicit authentication 63
configuring password settings 69
enabling 68

fault tolerance
configuring 57, 102

Federation
server 156
server proxy 156
Service 156
Service proxy 156

firewall
address translation 99
font smoothing 15, 111

functional level for resource partner domain 163

G
gateway settings 101

H
Help
displaying 40
HTTP 58
HTTPS 58, 129

I
ICA encryption 130
overview 122
ICA files 125
IIS
installing on 27
initial configuration settings
specifying 47
initialization 130

installation captions 91
installing
on 64-bit Windows 29
on IIS 27
on Java application servers 30
overview 26
security considerations 26
using the command line 32

Internet Information Services
requirements 23

J
Java application servers
installing on 30
Java installer 15

L
language packs 32
removing 33
legacy support 97
load balancing
between Secure Ticket Authorities 102
XML requests 57
local site tasks 53
locally configured sites
upgrading 50
logon page
making the default on IIS 54

M
managing
application refresh options 118
application shortcuts 118
configuration sources 53
plugin configuration files 98
plugin deployment 87, 91
secure access 99
server farms 55
server settings 60
session preferences 109
Microsoft domain-based authentication 67

N
NDS
authentication 67
new features 15
alerts 16
font smoothing 15
Java installer 15
secure access with Citrix XenApp 15
Special Folder Redirection 15
user interface redesign 15
Windows Server 2008 support 15

O
online Help 40
other client devices
requirements 25
overview
AD FS 155
installing the Web Interface 26

P
partners
account 156
resource 156
pass-through authentication 63
enabling 73
requirements 73
pass-through with smart card 64
password reset
Citrix XenApp 14, 72
configuring 70
password settings
configuring 69, 72
plugin configuration files
managing 98
plugin deployment
managing 87, 91
plugin files
copying to the server 89
plugins
obtaining 26
user customization 109
Web-based installation 89
private root certificates 94
prompt authentication 63
configuring password settings 72
enabling 71
proxy
federation server 156
Federation Service 156
published application URLs
support 54
publishing content 13
publishing resources 16

R
Remote Desktop Connection (RDP)
and the Trusted Sites zone 92–93
requirements 92
remote plugins
Client for Java 88
native embedded plugin 88
native plugin 88
Remote Desktop Connection (RDP) software 88
types 88
removing
language packs 33
server farms 56
Repair option 34
repairing sites 53
requirements
AD FS 159
pass-through authentication 73
Remote Desktop Connection (RDP) 92
smart card authentication 76
workspace control 113
resource partner 156
resource publishing 16
resource sets 16
resource types
dual mode streaming 49
remote 49
specifying 49
streamed 49
RSA SecurID
PASSCODES 80
tokencodes 80

S
screen appearance
customizing 108
screen content
customizing 108
screen layout
customizing 107
secure access
managing 99
secure access with Citrix XenApp 15
Secure Gateway
about 13
between plugins and servers 131
configuring the Web Interface for 101
dual mode streaming 49
example of how to configure 153
overview 123
support 13
Secure Sockets Layer
see SSL
SecureICA
see ICA encryption
securing the Web Interface 124
security 119
Access Gateway
configuring the Web Interface for 101
Access Gateway overview 122
and anonymous authentication 64
Citrix SSL Relay overview 121
configuring the Citrix SSL Relay 127
ICA encryption overview 122
network communication 124, 126
plugin and server 130
plugin-to-server communication 124
protocols and Citrix solutions 120
Secure Gateway
between plugins and servers 131
configuring the Web Interface for 101
Secure Gateway overview 123
SSL
between plugins and servers 130
between Web server and Web browser 126
SSL overview 120
TLS
between plugins and servers 130
between Web server and Web browser 126
TLS overview 121
when installing the Web Interface 26
server clocks
synchronizing 159
server farms
adding 56
managing 55
password change considerations 56
removing 56
role in the Web Interface 16
specifying settings for all servers 58
server settings
managing 60
specifying advanced 59
server URL
customizing 61
servers
configuring communication with 152
federation 156
role in the Web Interface 16
security 126
security considerations 130
synchronizing clocks 159, 162
Service
Federation 156
session options
changing 117
session preferences
managing 109
setting up
domain relationships 160
shadow accounts 156
site configuration
central 39
local 38
site redirection
configuring 62
site tasks
available for site types 52
using 51
using local 53
site types
tasks available for 52
sites
AD FS integrated 43, 114
configuring using the Access Management Console 39
creating 42
creating on Java application servers 42
repairing 53
specifying authentication settings 43
specifying initial configuration settings 47
specifying resource types 49
uninstalling 53
smart card
example of how to configure 79
smart card authentication 64
requirements 76
socket pooling
enabling 59
Special Folder Redirection 15
specifying
advanced server settings 59
authentication settings 43
backup URLs 61
initial configuration settings 47
resource types 49
settings for all servers 58
SSL
  between plugins and servers 130
certificate key size 121
configuring the Citrix SSL Relay 127
overview 120
secure Web servers 126
support
SSL/TLS communication
configuring 61
streamed applications
requirements 25
synchronizing
server clocks 159, 162
system requirements 19–26
client device 26
Internet Information Services 23
Web server 23

T
terminology
  AD FS 156
ticketing 125
  about 14
  configuring ticket expiry time 58
TLS
  between plugins and servers 130
certificate key size 121
overview 121
secure Web servers 126
troubleshooting
  installation 34
two-factor authentication 80
  enabling 70

U
Unicode ICA files 97
uninstalling 35
uninstalling sites 53
upgrading
  centrally configured sites 50
  existing installation 33
  existing sites 49
  groups of sites 50
  locally configured sites 50
upgrading sites 16
UPN
  authentication 67
  restricting suffixes 67
  support
user appearance
  customizing 107
user interface redesign 15
user principal name
  see UPN
user requirements 24

W
Web Interface
  AD FS support 157
  configuring with the Citrix XenApp 151
deploying with Access Gateway 44
deployment 157
features 12
how it works 17
installing 26
introduction 11
making available to users 53
overview 17
running on a server 129
security 119
uninstalling 35
Web server
  requirements 23
Web-based plugin installation
  copying plugins to the server 89
WebInterface.conf
  about 38
  configuring the Web Interface using 133
  parameters 134
Windows authentication 67
Windows Directory Service Mapper 77
Windows platforms
  installing on 64-bit versions 29
Windows Server 2008 support 15
Windows-based terminals 25
workspace control
  automatic reconnection 116
  configuring 113
  enabling 115
  overview 113
  reconnect option 116
  requirements 113
  using with integrated authentication 114

X
XenApp Services sites 12
XenApp Web sites 12