Web Interface 5.4

2015-05-03 05:26:50 UTC

Contents

Web Interface 5.4

The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their resources through a standard Web browser or through the Citrix online plug-in.

In This Section

This section of the library provides up-to-date information about installing, configuring, and administering the Web Interface, including the following:

Readme for Web Interface 5.4	Information about last-minute updates and known issues.
Issues Fixed in Web Interface 5.4	Details of issues that have been fixed since the previous release of the Web Interface.
Web Interface Features	Introducing the Web Interface.
New in This Release	An overview of new features.
Web Interface Components	A description of a Web Interface deployment.
System Requirements for the Web Interface	Software, configuration, Web server, user, and device requirements.
Installing the Web Interface	Installing the Web Interface and configuring your Web server.
Getting Started with the Web Interface	Creating and configuring Web Interface sites.
Managing Servers and Farms	Configuring and managing server settings and communication with server farms.
Configuring Authentication for the Web Interface	Configuring authentication between the Web Interface, server farms, and Citrix plugins.
Managing Clients	Deploying and use Citrix plugins with the Web Interface.
Managing Secure Access	Configuring and managing access to sites.
Editing Client-Side Proxy Settings	Configuring Citrix clients and servers running XenApp or XenDesktop through proxy servers.
Customizing the Apperance for Users	Customize the way in which the Web Interface appears to users.
Managing Session Preferences	Specify the settings that users can adjust.
Configuring Workspace Control	Allow users to disconnect, reconnect, and log off from resources quickly.
Configuring Web Interface Security	Secure your data in a Web Interface environment.

Configuring Sites Using the Configuration File	Administer Web Interface sites using the configuration files.
Configuring AD FS Support for the Web Interface	Create and configure Microsoft Active Directory Federation Services (AD FS) integrated Web Interface sites.

Readme for Web Interface 5.4

Readme Version: 1.0

Contents

Related Documentation

For client-related issues that may affect Web Interface users, see the Readme files for the Citrix clients currently deployed to your users.

For a list of issues resolved in this release, see Knowledge Center article http://support.citrix.com/article/CTX124164.

To access licensing documentation, go to Licensing Your Product.

Getting Support

Citrix provides technical support primarily through Citrix Solutions Advisor. Contact your supplier for first-line support or use Citrix Online Technical Support to find the nearest Citrix Solutions Advisor.

Citrix offers online technical support services on the Citrix Support Web site. The Support page includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

Known Issues in This Release

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

- Icons are not displayed properly on devices running WinCE 6.0 WFR3 and Internet Explorer 6
- User error may occur when published desktops are added to Internet Explorer Favorites
- Error message when attempting to connect using deprecated clients

- Citrix online plug-in cannot be upgraded on devices running Windows Embedded operating systems

- Using Kerberos fails when configuring delegation on XenApp servers running Windows Server 2008

- Virtual desktop fails to start when accessing the Web Interface from some devices running Windows Embedded CE 6.0

- Workspace control and client upgrade unavailable for Firefox 3.6 users

- Workspace control unavailable on some devices running Windows Mobile 6.1

- Workspace control intermittently unavailable on some devices running Windows Embedded CE 6.0 R2

- Pass-through with smart card from Access Gateway cannot be used with XenApp 6.0

Icons are not displayed properly on devices running WinCE 6.0 WFR3 and Internet Explorer 6

Icons in .png format are not displayed properly when viewed on devices running Internet Explorer 6 with WinCE 6.0 WFR3 (Hot Fix 3 build 664). To resolve this issue, use Internet Explorer version 5 or earlier. Alternatively, to display .png files in Internet Explorer 6, refer to the workaround described in the Microsoft article http://support.microsoft.com/kb/294714.

[#41839]

Users may be unable to add published desktops and applications to Internet Explorer Favorites

Users may experience problems adding published desktops and applications to Internet Explorer Favorites. In some situations, the resulting Favorites link will have an incorrect title and will not work correctly when clicked. To add applications to Favorites, right-click the application's icon. To add desktops, right-click the desktop title text.

[#244446]

Error message when attempting to connect using deprecated clients

This release of the Web Interface does not support the use of clients prior to Version 7.0. When attempting to connect to a remote application with an earlier client, users may encounter the error “50: Cannot connect to server.” Users can avoid this issue by upgrading to the latest versions of the clients. If this is not possible, you can prevent the error from occurring by editing the template .ica files as follows:

1. Using a text editor such as Notepad, open the following files: default.ica, bandwidth_high.ica, bandwidth_low.ica, bandwidth_medium.ica, and bandwidth_medium_high.ica. These files are typically located in the C:\inetpub\wwwroot\Citrix\SiteName\conf directory on IIS and the /WEB-INF directory of the Web Interface site on Java application servers.

2. Locate and delete the following lines in each file:

```
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
```

[#163695]

Citrix online plug-in cannot be upgraded on devices running Windows Embedded operating systems

The Web Interface may offer to install or upgrade the Citrix online plug-in on devices running Windows Embedded operating systems; however, the installation will fail. You can avoid this issue by manually installing the latest version of the Citrix online plug-in on the embedded device. If this is not possible, you can modify settings for the site to prevent these installation captions from appearing:

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Client Deployment. For sites that offer only online applications, select the Native client checkbox and click Properties.

4. Click Client Detection.

5. Clear the Offer upgrades for clients check box and select either Only if resources cannot be accessed or Never.

[#164709]

Using Kerberos fails when configuring delegation on XenApp servers running Windows Server 2008

Because of an issue with Windows Server 2008, configuring Active Directory to use Kerberos only for authentication when trusting XenApp servers for delegation causes authentication to fail. This issue occurs on XenApp servers running Windows Server 2008 with Service Pack 2, Windows Server 2008 x64 Editions with Service Pack 2, and Windows Server 2008 R2. To enable AD FS integration and pass-through with smart card from Access Gateway with XenApp servers running Windows Server 2008, select the Use any authentication protocol setting instead of the Use Kerberos only setting indicated in the documentation. [#169269]

Virtual desktop fails to start when accessing the Web Interface from some devices running Windows Embedded CE 6.0

In some cases, users of WYSE V30LE thin clients running Windows Embedded CE 6.0 and Internet Explorer 6.*x* may find that when they log on to XenApp Web sites and click on a text link to start a virtual desktop, the desktop fails to start. Users can avoid this issue by clicking on the icon displayed next to the text link to start the desktop. [#218317]

Workspace control and client upgrade unavailable for Firefox 3.6 users

Because of a change in Mozilla Firefox 3.6, workspace control is automatically disabled for users accessing the Web Interface with this browser. In addition, the client detection and deployment process cannot detect the version numbers of Citrix clients installed by Firefox 3.6 users and so is unable to offer these users the opportunity to upgrade their clients.

[#230068]

Workspace control unavailable on some devices running Windows Mobile 6.1

In some cases, users of HP iPAQ 910c handheld devices running Windows Mobile 6.1 Professional and Internet Explorer Mobile may find that when they log on to XenApp Web sites, workspace control fails to function correctly. [#230580]

Workspace control intermittently unavailable on some devices running Windows Embedded CE 6.0 R2

In some cases, users of HP t5540 thin clients running Windows Embedded CE 6.0 R2 and Internet Explorer 6.*x* may find that when they log on to XenApp Web sites, workspace control sometimes fails to function when they click the Reconnect button. [#230654]

Pass-through with smart card from Access Gateway cannot be used with XenApp 6.0

Because of an issue with XenApp 6.0, smart card users logging on to Access Gateway integrated sites are unable to access resources when the pass-through with smart card from Access Gateway feature is enabled. Users clicking on a link to access a resource delivered by XenApp 6.0 encounter the error message “An error occurred while making the requested connection.” You can avoid this issue by configuring the site to prompt smart card users for their PIN each time they access a resource. [#230942]

http://www.citrix.com/

Web Interface Administration

The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their resources through a standard Web browser or through the Citrix online plug-in.

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 resources or Web sites that can be integrated into your corporate portal. Additionally, the Web Interface enables you to configure settings for users accessing resources through the Citrix online plug-in.

You can create and configure Web Interface sites on Microsoft Internet Information Services (IIS) using the Citrix Web Interface Management console. The console is installed only with Web Interface for Microsoft Internet Information Services. For more information about using this tool, see Configuring Sites Using the Citrix Web Interface Management Console.

You can also edit the site configuration file (WebInterface.conf) to manage and administer Web Interface sites. For more information, see Configuring Sites Using Configuration Files.

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

The two Web Interface site types enable you to provide your users with different methods of accessing their resources, according to their needs.

XenApp Web sites. You can provide users with a Web site to which they can log on using a Web browser. Once authenticated, users can access online resources and offline applications using a Citrix client.

XenApp Services sites. You can use the Citrix online plug-in in conjunction with the Web Interface to integrate resources with users' desktops. Users access applications, virtual desktops, and online 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

Multiple server farm support. You can configure multiple server farms and provide users with a display of the resources available to them from all farms. You can configure each server farm individually using the Server Farms task in the Citrix Web Interface Management console. For more information, see To configure communication with the server.

Disaster recovery. You can specify XenApp and XenDesktop server farms for emergency use when users cannot access any of their production farms, perhaps due to a power failure or network outage. This enables you to make provisions to deal with the loss of access to all production servers so that line-of-business applications or desktops do not suddenly become unavailable.

Shared site configuration. Web Interface for Microsoft Internet Information Services enables you to specify a “master” site that shares its configuration file over the network. Other sites can then be configured to use the master site’s configuration rather than a local file.

Integration with popular Web technologies. The Web Interface’s API can be accessed from Microsoft’s ASP.NET and Sun Microsystems’ JavaServer Pages. The Web Interface for Java Application Servers is platform independent, so it can be installed on Windows operating systems where Microsoft Internet Information Services (IIS) is not being used as the Web server.

Resource Access Features

XenApp VM hosted apps. XenApp has the capability to deliver online applications from virtual machines. This enables you to publish applications that are incompatible with or not yet validated for Remote Desktop Services, or applications that are not supported for installation on Windows Server operating systems.

User roaming. You can associate user groups with specific server farms to provide a consistent experience for users, regardless of their current location or the server to which they are logging on. This enable users who travel abroad on business, for example, to log on to a local Web Interface server and automatically receive resources in their native language from a farm in their home country.

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

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 applications and content. The logon screens are compatible with Active Directory's use of user principal names (UPNs).

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

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.

Access Gateway support. Citrix 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. The Access Gateway combines the best features of Internet Protocol Security (IPSec) and SSL VPN without the costly and cumbersome implementation and management, works through any firewall, and supports all 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.

Smart card support. The Web Interface supports the use of smart cards for user authentication to provide secure access to applications, content, and desktops. Using smart cards simplifies the authentication process for users while at the same time enhancing logon security.

Ticketing. This feature provides enhanced authentication security. The Web Interface obtains tickets that authenticate users to 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 resources. Use of ticketing eliminates the explicit inclusion of credentials in the .ica files that the Web Interface uses to connect to resources.

Secure Ticket Authority redundancy. You can configure multiple redundant Secure Ticket Authorities (STAs) for users accessing their resources through the Access Gateway. This enables you to mitigate against the possibility of the STA becoming unavailable midway through a user's session, preventing reconnection to the session. When redundancy is enabled, the Web Interface attempts to obtain and deliver to the gateway two tickets from two different STAs. If one of the STAs cannot be contacted during a user session, the session continues uninterrupted using the second STA.

Change password. Users logging on to the Web Interface or the Citrix online plug-in using explicitly supplied domain credentials 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 enables users to reset their network password and unlock their account by answering a series of security questions.

Client Deployment Features

Web-based client 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 Citrix client, 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 clients, so the Web Interface provides a client detection and deployment process that guides users through the client deployment procedure, including, where appropriate, reconfiguring their Web browser. This ensures that users get an optimal experience when accessing their resources, even from the most restricted environments.

Citrix online plug-in support. The Citrix online plug-in enables users to access resources directly from their desktops without using a Web browser. The user interface of the Citrix online plug-in can also be “locked down” to prevent user misconfiguration.

Citrix offline plug-in support. The Citrix offline plug-in enables users to stream XenApp applications to their desktops and open them locally. You can either install the plug-in with the Citrix online plug-in to provide the full set of Citrix client-side application virtualization features or install the plug-in alone on users’ desktops so users can access 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:

Updated end user interface. The layout and color scheme for end users has been updated to help improve navigation and readability.

Session sharing for VM hosted applications. The Web Interface now supports session sharing for Virtual Machine (VM) hosted apps. This feature is only available for seamless applications and non-anonymous users.

Multiple desktop access for users. In previous versions of the Web Interface, users could only access a single instance of a desktop per desktop group. Now, users can access multiple instances of desktops in desktop groups. For more information about assigning desktops to users, see the XenDesktop version 5 documentation.

Improved smart card support for Access Gateway. Smart card authentication to the Web Interface is now compatible with more environments. The Web Interface can now accept User Principal Names (UPNs) from Access Gateway as well as the user name and domain. Additionally, the Web Interface has been updated to comply with FIPS. This new functionality can only be used with the pass-through authentication for smart card option and you must be logged on as a domain administrator. For more information about configuring smart card support for Access Gateway, see the Access Gateway documentation.

Ability to set additional default values. Administrators can configure default values for all bandwidth-related settings, such as audio quality, color depth, bandwidth profile, printer mapping, and window size.

ICA File Signing. The Web Interface digitally signs generated ICA files, to allow compatible Citrix clients and plug-ins to validate that the file originates from a trusted source.

Web Interface Components

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

- One or more server farms
- A Web server
- A user device with a Web browser and a Citrix client

Server Farms

A group of servers that are managed as a single entity and operate together to serve resources to users are collectively known as a *server farm*. A server farm is composed of a number of servers all running either XenApp or XenDesktop, 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) delivered from the server farm. When an administrator publishes a resource for a group of users, that resource becomes available as an object to which Citrix clients 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 XenDesktop that provides resource information to Citrix clients 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 XenDesktop.

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 available resources, including a list of resources the user can access

User Device

A *user device* is any computing appliance capable of running a Citrix client and a Web browser. User devices include desktop PCs, laptops, network computers, terminals, and handheld computers, among others.

In a user device, the browser and Citrix client 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 client acts as the engine that enables users to access resources.

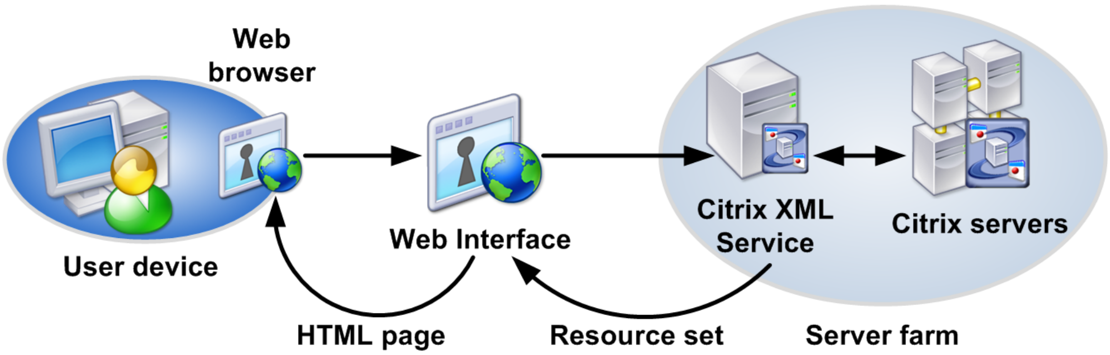
The Web Interface provides *Web-based client deployment*, which is a method of deploying Citrix clients from a Web site. When a user visits a site created with the Web Interface, the Web-based client detection and deployment process detects the device and the user is prompted to deploy an appropriate Citrix client. For some environments, the client detection and deployment process can also detect the presence or absence of an installed client and prompts the user only when necessary. For more information, see Configuring Client Deployment and Installation Captions.

The Web Interface supports many browser and Citrix client combinations. For a complete list of supported browser and client combinations, see User Device Requirements.

How the Web Interface Works

Typical interactions between a server farm, a server running the Web Interface, and a user device are described below.

The figure shows an example of a typical Web Interface interaction. The Web browser on the user's device sends information to the Web server, which communicates with the server farm to provide the user with access to the resources.



- A user authenticates to the Web Interface through a Web browser.
- The Web server reads the user's 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 resources that the user 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 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 Citrix client (in some cases using the Web browser as an intermediary).
- The Citrix client initiates a session with the server in the farm according to the connection information supplied by the Web Interface.

System Requirements for the Web Interface

To run the Web Interface, your servers must run a supported Citrix product.

The Web Interface supports the following product versions:

- Citrix XenApp 7.6 and XenDesktop 7.6
- Citrix XenApp 7.5 and XenDesktop 7.5
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7
- Citrix XenDesktop 5.6 Service Pack 1
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenDesktop 5.0 Service Pack 1
- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2008
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003
- 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 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

Important: For compatibility with XenApp 4.0, with Feature Pack 1, for UNIX, an additional manual site configuration step is required. For more information, see To configure support for XenApp 4.0, with Feature Pack 1, for UNIX.

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

Minimum Software Requirements

Without the latest release, some new features are not available. For example, seamless farm migration is only available when upgrading to XenApp 6.0.

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

Note: To confirm support for Web Interface 5.4 in specific releases of Citrix products, refer to the System Requirements for that product.

Web Interface feature	Software requirements
XenApp farm migration	Citrix XenApp 6.0
User roaming	Citrix XenDesktop 4.0 Citrix XenApp 6.0
XenApp VM hosted apps	Citrix XenApp 5.0 with Feature Pack 2
Disaster recovery	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2
Secure Ticket Authority redundancy	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2 Citrix Access Gateway 4.6, Standard Edition
Support for Windows 7 and Internet Explorer 8.0	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2 Citrix online plug-in 11.2 Citrix offline plug-in 5.2
Virtual desktop restart	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
Special Folder Redirection	Citrix XenApp 5.0 Citrix XenApp Plugin for Hosted Apps 11.0 for Windows
Font smoothing	Citrix XenApp 5.0 Citrix XenApp Plugin for Hosted Apps 11.0 for Windows
Support for XenDesktop	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition 10.250

Support for Windows Vista and Internet Explorer 7.0	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Presentation Server Clients 10.1 for Windows
Support for offline applications	Citrix Presentation Server 4.5 Citrix Streaming Client 1.0 Citrix Program Neighborhood Agent 10.0
AD FS support	Citrix Presentation Server 4.5
Access control policy support	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Access Gateway 4.2 with Advanced Access Control Citrix MetaFrame Presentation Server Clients for 32-bit Windows, Version 9.0
Account self-service	Citrix Password Manager 4.0
User change password	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Program Neighborhood Agent 10.1
Session reliability	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Clients for 32-bit Windows, Version 9.0
Workspace control	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Client for 32-bit Windows, Version 8.0
Smart card support	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 Citrix ICA Client for 32-bit Windows 7.0

Secure Gateway support	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems Citrix ICA Client for 32-bit Windows 7.0
NDS authentication	Citrix Presentation Server 4.5 Citrix ICA Client for 32-bit Windows 7.0
DNS addressing	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems Citrix ICA Client for 32-bit Windows 7.0
Enhanced Content Publishing	Citrix Presentation Server 4.5 Citrix ICA Client for 32-bit Windows 7.0
Load balancing	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
Server-side firewall support	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
Client-side firewall support	Citrix ICA Client for 32-bit Windows 7.0
Pass-through authentication	Citrix Presentation Server 4.5 Full Program Neighborhood Client for 32-bit Windows Citrix Program Neighborhood Agent 7.0
Remote Desktop Connection (RDP)	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

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 more information about server farm membership and publishing resources in a server farm, see the documentation for your Citrix server.

XenApp for UNIX servers must also have applications published. In addition, these applications must be configured for use with the Web Interface. For more information about installing the Citrix XML Service for UNIX and configuring applications for use with the Web Interface, see the XenApp for UNIX documentation.

Web Server Requirements

The Citrix clients must be present on the server for Web-based deployment of the clients. For more information about supported client versions, see User Device Requirements. For more information about copying the clients to the Web Interface server, see Copying Client Installation Files to the Web Interface.

On Windows Platforms

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

Operating system	Web server	Runtime/JDK	Servlet engine
Windows Server 2008 R2 x64 Windows Server 2008 R2 with Service Pack 1	Internet Information Services 7.5	.NET Framework 3.5 with Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	N/A
Windows Server 2008 x64 Editions with Service Pack 2 Windows Server 2008 x86 with Service Pack 2	Internet Information Services 7.0		
Windows Server 2003 R2 x86 with Service Pack 2 Windows Server 2003 Standard Edition x86 with Service Pack 2 Windows Server 2003 Enterprise Edition x86 with Service Pack 2 Windows Server 2003 R2 Standard Edition x86 with Service Pack 2 Windows Server 2003 R2 Standard Edition x64 with Service Pack 2	Internet Information Services 6.0		

Windows Server 2003 Standard Edition x86 with Service Pack 2	Apache 2.2.*x*	Java 1.6.*x*	Apache Tomcat 6.0.*x*

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.

User Requirements

The following Web browser and operating system combinations are supported for users to access Web Interface sites:

Browser	Operating system
Internet Explorer 11	Windows 8.1 32-bit Windows 8.1 64-bit Windows 8 32-bit Windows 8 64-bit Windows 2012 64-bit Windows 2012 R2 64-bit Windows 7 32-bit with Service Pack 1 (SP1) Windows 7 64-bit with Service Pack 1 (SP1) Windows Server 2008 R2 with Service Pack 1 (SP1) 64-bit
Internet Explorer 10	Windows 7 32-bit with Service Pack 1 (SP1) Windows 7 64-bit with Service Pack 1 (SP1) Windows Server 2008 R2 with Service Pack 1 (SP1) 64-bit
Internet Explorer 9.*x* (32-bit mode)	Windows Vista 32-bit Editions with Service Pack 2 or higher Windows Vista 64-bit Editions with Service Pack 2 or higher Windows 7 32-bit RTM or higher Windows 7 64-bit RTM or higher Windows Server 2008 32-bit with Service Pack 2 or higher Windows Server 2008 64-bit with Service Pack 2 or higher Windows Server 2008 R2 64-bit

Internet Explorer 8.*x* (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows XP Professional with Service Pack 3 Windows XP Professional x64 Edition with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Vista 64-bit Editions with Service Pack 2 Windows Server 2008 R2 Windows Server 2008 with Service Pack 2 Windows Server 2003 with Service Pack 2
Internet Explorer 7.*x* (32-bit mode)	Windows Vista 64-bit Editions with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Server 2008 with Service Pack 2 Windows Server 2003 with Service Pack 2
Safari 5.*x*	Mac OS X Snow Leopard 10.6
Safari 4.*x*	Mac OS X Leopard 10.5
Mozilla Firefox 4.*x* (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows XP Professional with Service Pack 3 Windows XP Professional x64 Edition with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Vista 64-bit Editions with Service Pack 2 Windows Server 2003 with Service Pack 2
Mozilla Firefox 3.*x*	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x32 Edition with Service Pack 3 Windows Vista 32-bit Editions with Service Pack 2 Windows 7 32-bit Editions Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003 with Service Pack 2

Mozilla 1.7	Solaris 10

Note: Web Interface 5.4 is supported only for the software versions listed on this page. Although newer software versions might work, they have not been tested and are not supported.

Requirements for Access to Offline Applications

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

Browser	Operating system
Internet Explorer 8.*x* (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows Vista 64-bit Editions with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows XP Professional x64 Edition with Service Pack 2 Windows XP Professional with Service Pack 3 Windows Server 2008 R2 Windows Server 2008 x64 Editions with Service Pack 2 Windows Server 2008 with Service Pack 2 Windows Server 2003 x64 Editions with Service Pack 2 Windows Server 2003 with Service Pack 2
Internet Explorer 7.*x* (32-bit mode)	Windows Vista 64-bit Editions with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows XP Professional x64 Edition with Service Pack 2 Windows XP Professional with Service Pack 3 Windows Server 2008 x64 Editions with Service Pack 2 Windows Server 2008 with Service Pack 2 Windows Server 2003 x64 Editions with Service Pack 2 Windows Server 2003 with Service Pack 2

Mozilla Firefox 3.*x*	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows Vista 64-bit Editions with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows XP Professional x64 Edition with Service Pack 2 Windows XP Professional with Service Pack 3 Windows Server 2003 with Service Pack 2

Requirements for Other User Devices

Users can access the Web Interface on thin clients, personal digital assistants (PDAs), and handheld devices with the following configurations:

Device	Operating system	Browser
iPhone	N/A	Safari 5.*x*
iPad	N/A	Safari 5.*x*
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSE V90	Windows XP Embedded with Service Pack 2	Internet Explorer 6.*x*
HP T5730	Windows Embedded Standard 2009	Internet Explorer 7.*x*
HP T5540	Windows Embedded CE 6.0 R2	Internet Explorer 6.*x*
HP RK270 WYSE V30	Windows Embedded CE 6.0	Internet Explorer 6.*x*
HP GY231	Debian Linux 4.0	Debian Iceweasel 2.0
Symbian E61/E70	Symbian	Symbian browser

User Device Requirements

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

Citrix recommends that you deploy the most recent clients to your users to ensure that they can take advantage of the latest features. The features and capabilities of each client differ—for more information about supported client features, see the documentation for the client in question.

Installing the Web Interface

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 GlassFish Enterprise Server

For more information about how to install the Web server requirements, see Web Server Requirements.

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.

For more information about how to install the Web Interface, see To install the Web Interface on Microsoft Internet Information Services and Installing the Web Interface on Java Application Servers.

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 that the Citrix XML Service is using. The Citrix XML Service is the communication link between the server farm and the Web Interface server.

On Windows platforms, the Citrix XML Service can be configured to share Internet Information Services' TCP/IP port. If this is the case, you must locate the port used by Internet Information Services' WWW Service to determine the Citrix XML Service port. By default, the WWW Service uses port 80. If a dedicated port is required for the Citrix XML Service, Citrix recommends using port 8080.

For a list of ports in use on Windows platforms, type netstat -a at a command prompt. 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 documentation for your Citrix server.

To install the Web Interface on Microsoft 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.*x* on Windows Server 2008, install the Web Server (IIS) role and then enable the following role services:

- Web Server > Application Development > ASP.NET
- 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 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 with Service Pack 1 and Visual J#.NET 2.0 Second Edition are installed.

If you are upgrading from an earlier version of the Web Interface, back to and including Version 4.5, the installer prompts you to back up your existing sites before upgrading them.

Important: Centrally configured sites and 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 Web server. Any existing centrally configured sites will be upgraded and converted to use local configuration.

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 the Citrix Web site, copy the file WebInterface.exe to your Web server.

2. Navigate to and double-click the file WebInterface.exe.

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

4. On the Welcome page, click Next.

5. On the License Agreement page, select I accept the license agreement and click Next.

6. On the Installation Location page, browse to an installation location for the Web Interface (the default is C:\Program Files (x86)\Citrix\Web Interface\). Click Next.

7. On the Location of Clients page, select Copy the clients to this computer. Click Browse to search the installation media or your network for the Citrix client setup files.

   Setup copies the contents of the \Citrix Receiver and Plug-ins folder on the installation media or network share to the Web Interface \Clients folder, 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 client files in this directory structure.

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

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

9. When the installation is complete, click Finish.

10. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management to access the Citrix Web Interface Management console and begin creating and configuring your sites.

Compatibility with Other Components on Windows Server 2003 x64 Editions

On 64-bit versions of Windows Server 2003, installation of Web Interface for Microsoft Internet Information Services enables 32-bit Web extension support in IIS 6.0 and this disables 64-bit extension support. If you are installing Web Interface for Microsoft Internet Information Services on a 64-bit version of Windows Server 2003, ensure that 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.”

When installed on Windows Server 2003 x64 Editions, Web Interface for Microsoft Internet Information Services may not be compatible with 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

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 restart your server.

Installing the Web Interface on Java Application Servers

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 Citrix clients are copied from the installation media, if required.
8. Follow the instructions on the screen to complete the installation of the .war file.

To configure the security policy on Sun GlassFish Enterprise Server

Before you can create XenApp Web sites configured to allow account self-service on a Sun GlassFish Enterprise Server, you must manually configure the server's security policy.

1. Deploy the site's .war file on the server.

2. Stop the Web server.

3. Edit the server.policy file under the deployed domain configuration directory. For example, if Sun GlassFish Enterprise Server is installed under *SunGlassFishEnterpriseServerRoot*/AppServer and the site is deployed in “domain1,” the file resides in *SunGlassFishEnterpriseServerRoot*/AppServer/domains/domain1/config.

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

   ```
    grant codeBase
   "file:${com.sun.aas.instanceRoot}/applications/
   j2ee-modules/WARFileName/-"{
   permission java.lang.RuntimePermission
   "getClassLoader";
   permission java.lang.RuntimePermission
   "createClassLoader";
   permission java.util.PropertyPermission
   "java.protocol.handler.pkgs", "read, write";
    };
   ```

   where *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 *SunGlassFishEnterpriseServerRoot*/ApplicationServer/lib to add javax.wsdl to the list of values for the sysproperty key="com.sun.enterprise.overrideablejavaxpackages" element.

6. Start the Web server.

Using Language Packs

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

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

On IIS, language packs can be added to a Web Interface installation by copying the tree or unpacking the files in the \languages folder, 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 devices, such as those running Windows CE, 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 specific sites only.

For sites on IIS, remove *LanguageCode*.lang (for example, ja.lang) from the \languages folder, 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 4.5 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: Centrally configured sites and 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 Web server. Any existing centrally configured sites will be upgraded and converted to use local configuration.

The directory structure of the \Clients folder, which is used for Web-based client deployment to users, is different in version 5.1 and earlier of the Web Interface. If you upgrade your Web Interface installation using the XenApp or XenDesktop installation media, copy the directory structure from the installation media when you upgrade your installation. If you upgrade using a Web download, you must manually recreate the required directory structure for your Web Interface installation. You can then download the clients that you need from the Citrix Web site. For more information on the \Clients directory structure, see Copying Client Installation Files to the Web Interface.

By default, the Web Interface assumes that the file names of the client installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download clients from the Citrix Web site or if you plan to deploy older clients, check that the appropriate client installation file names are specified for the ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, and ClientStreamingWin32 parameters in the configuration files for your XenApp Web sites. For more information on Web Interface configuration file parameters, see WebInterface.conf Parameters.

What to Do After Installation

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 Citrix Web Interface 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 using the console or WebInterface.conf file, see Configuring Sites Using the Citrix Web Interface Management Console or Configuring Sites Using Configuration Files, respectively

- For information about how to configure the Web Interface for Access Gateway or Secure Gateway using the Citrix Web Interface Management console, see To configure gateway settings

- For information about configuring the Web Interface to use AD FS, see Configuring AD FS Support for the Web Interface

- For information about security considerations, see Configuring Web Interface Security

- For information about extending and customizing 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 your 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. You must recreate all your sites after reinstalling the Web Interface.

To use the Repair option

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

Important: If your Web interface installation includes customized code and you select the Repair option, this customized code is removed. Citrix recommends that you back up any files you customize before you use this option.

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 folder. Therefore, if you want to keep any Web Interface files, copy them to another location before you uninstall the Web Interface.

Occasionally, 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

To uninstall the Web Interface on Microsoft 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.

To uninstall the Web Interface on Java application servers

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

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 the files that remain, see the Citrix XenApp Readme file.

Getting Started with the Web Interface

Deciding Which Configuration Method to Use

You can configure and customize the Web Interface using either the Citrix Web Interface Management console or the configuration files.

Using the Citrix Web Interface Management Console

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

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

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

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

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

Using Configuration Files

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

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

- **Citrix online plug-in configuration file.** You can configure the Citrix online plug-in using the config.xml file on the Web Interface server.

Configuring Sites Using the Citrix Web Interface Management Console

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

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

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

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

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

Configuring Sites Using Configuration Files

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

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

Shared Configuration

For sites hosted on IIS, you can specify that a Web Interface site should obtain its configuration from a “master” site that you have configured to share its configuration files over the network. Once you have set up the appropriate file permissions, you can allow other sites to share the configuration of the master site by specifying the absolute path to the master site configuration file (WebInterface.conf) in the bootstrap.conf file of the local site. In the case of XenApp Services sites that use shared configuration, the Web Interface also attempts to read the Citrix online plug-in configuration file (config.xml) from the same directory as that specified for WebInterface.conf.

Once a site has been modified to obtain its configuration from a shared file, you will not be able to manage that site’s configuration directly. Instead, you must alter the configuration of the master site using the console or by directly editing the configuration files on the Web server hosting the master site. Any changes made to the configuration of the master site affect all the other sites that share the master site’s configuration file. Shared configuration is not available for sites hosted on Java application servers.

To share site configurations

1. Set up appropriate file sharing permissions to allow access over the network to the \conf folder (typically C:\inetpub\wwwroot\Citrix\SiteName\conf) of the master site and the site configuration file (WebInterface.conf), which is typically located in the \conf folder. For XenApp Services master sites, the same permissions need to be set up for the Citrix online plug-in configuration file (config.xml), which is also typically located in the \conf folder for the site.

2. Using a text editor, open the bootstrap.conf file (typically located in the \conf folder) for the site that will obtain its configuration from the shared configuration file.

3. Change the setting of the ConfigurationLocation parameter to specify the absolute network path to the master site’s configuration file, for example:

   ```
   ConfigurationLocation=\\ServerName\ShareName\WebInterface.conf
   ```

To create a site on Microsoft Internet Information Services

Use the Create Site task in the Citrix Web Interface Management console to create one of the following sites:

- **XenApp Web Sites.** For users accessing resources using a Web browser.
- **XenApp Services Sites.** For users accessing resources using the Citrix online plug-in.

You use this task to specify the IIS location in which the site is hosted, the URL to apply changes, and authentication settings for the site. You can update these settings later using the Site Maintenance tasks. You must be a local administrator on the server running the Web Interface to create sites.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click the Citrix Web Interface container.
3. In the Action pane, click Create Site.
4. Select the type of site you want to create.
5. Specify the URL and a name for the site.
6. Follow the instructions on the screen to create the site.

Microsoft Internet Information Services Hosting

Use the Manage IIS Hosting task under Site Maintenance in the Citrix Web Interface Management console to change the location of your Web Interface site on IIS.

Creating Sites on Java Application Servers

On Java application servers, run the Web Interface installer to create new sites. The installer creates a customized .war file for the site that you can then install (typically by placing the .war file in the appropriate location for your 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 Citrix Web Interface Management 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.

Authentication at an Active Directory Federation Services Account Partner

You can enable the account partner of an Active Directory Federation Services (AD FS) deployment to access XenApp applications. This enables you to provide users on the account partner with access to 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 the Access Gateway instead of AD FS.

For more information, see Configuring AD FS Support for the Web Interface.

Authentication at the Access Gateway

You can enable authentication and pass-through of users' credentials by the Access Gateway for explicit and smart card authentication. User access to resources is controlled through the use of policies.

If your users log on to the Access Gateway using explicit credentials, pass-through authentication is enabled by default. Users log on to the Access Gateway and do not have to authenticate again to the Web Interface to access their resources. To increase security, you can disable pass-through authentication so that users are prompted for a password before the resource set is displayed.

If your users log on to the Access Gateway with a smart card, they do not need to authenticate again to the Web Interface. By default, users are, however, prompted for a PIN when accessing a resource. You can configure the site to enable users to access their XenApp resources without having to provide a PIN. This feature is not supported by XenDesktop.

You can update these settings at any time using the Authentication Method task in the Citrix Web Interface Management console.

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 XenApp Administration.

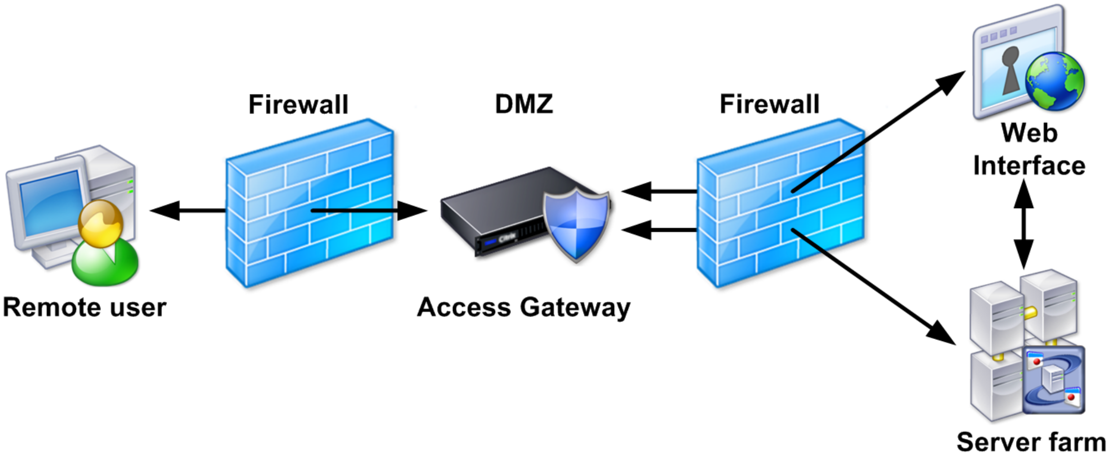
Authentication at the Web Server

You can enable authentication of users at the Web server using Kerberos. For more information about Kerberos, see XenApp Administration.

Deploying Access Gateway with the Web Interface

When deploying Access Gateway in combination with the Web Interface, Citrix recommends that XenApp/XenDesktop and the Web Interface are all installed on servers within the internal network, with Access Gateway appliance in the demilitarized zone (DMZ).

The figure shows the recommended configuration for deploying Access Gateway with the Web Interface.



A DMZ is a subnet that lies between the secure internal network and the Internet (or any external network). When Access Gateway is deployed in the DMZ, users access it using the Citrix secure access plug-in or a Citrix client. Users log on, are authenticated by Access Gateway, and are then directed to their resources, subject to the access policies that you configure.

Making Resources Available to Users

With Access Gateway, users log on to a realm (for Access Gateway Standard Edition), logon point (for Access Gateway Advanced Edition and Access Gateway 5.0), or virtual server (for Access Gateway Enterprise Edition) to gain access to their resources. You make resources available to users by configuring a realm, logon point, or virtual server 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 configured as the default home page for a realm, logon point, or virtual server. Once logged on, users are presented with the XenApp Web site.

- 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. The Access Interface is only available with Access

Gateway Advanced Edition and Enterprise Edition.

Integrating a XenApp Web Site with the Access Gateway

To integrate a site with the Access Gateway, create a XenApp Web site and configure a Web resource for the site in the Access Gateway.

To create an Access Gateway integrated site

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click the Citrix Web Interface container.

3. In the Action pane, click Create Site.

4. Select XenApp Web and click Next.

5. On the Specify IIS Location page, specify the IIS location, the path, and a name for the site. Click Next.

6. On the Specify Point of Authentication page, select At Access Gateway and click Next.

7. On the Specify Access Gateway Settings page, type the URL of the Access Gateway authentication service in the Authentication service URL box.

8. Specify how your users log on to the Access Gateway and click Next:

   - If your users log on to the Access Gateway with a user name and password, select Explicit. To increase security by disabling pass-through of users' credentials from the Access Gateway to the Web Interface, select the Prompt users for password before displaying applications and desktops check box.

   - If your users log on to the Access Gateway with a smart card, select Smart card. Ensure you are logged on as a domain administrator before enabling the pass-through authentication for smart card option.

   Important: Access Gateway integrated XenApp Web sites can support either explicit or smart card authentication, but not both. If you have a mixture of users logging on to the Access Gateway with both explicit and smart card authentication, you must create and configure separate sites for each authentication method. Then, configure the Access Gateway to direct users to the appropriate site for their authentication method.

9. If you are configuring the site for explicit authentication, continue to Step 10. If you are configuring smart card authentication, on the Specify Smart Card Settings page, specify whether or not users are required to provide their PIN before they can access a resource.

   - If you want users to enter a PIN each time they access a resource, select Prompt users for PIN. Additional configuration steps are required to enable this feature. For more information, see To enable smart card users to access their resources through the Access Gateway by providing a PIN.

     Note: You can enable Windows XP users who log on to their desktops using the same smart card that they use to log on to the Access Gateway to access their resources without having to provide a PIN. For more information, see To enable smart card users to access their resources through the Access Gateway by providing a PIN.

- If you want to enable all users to access their XenApp resources without having to provide a PIN, select Enable Smart Card pass-through. This feature is not supported by XenDesktop and can be used only when the Web server is within the same domain as your users. You may need to restart the Web server to enable the pass-through with smart card from Access Gateway service. Additional configuration steps are required to enable this feature. For more information, see To enable smart card users to access their resources through the Access Gateway without providing a PIN.

  Note: By default, pass-through with smart card from the Access Gateway is enabled for all domain users. To restrict the list of allowed users, edit the user permissions for the file PTSAccess.txt, which is typically located in the C:\Program Files (x86)\Citrix\DeliveryServices\ProtocolTransitionService\ directory.

10. Confirm the settings for the new site and click Next to create the site.

To provide access to the site through the Access Gateway

These steps provide an overview of how to provide access to the site through Access Gateway. For more information, see the documentation for your Access Gateway edition, archived here.

1. Configure XenApp or XenDesktop to communicate with the Access Gateway.
2. Configure the Access Gateway to provide access to the XenApp Web site.

   Important: Specify the domain in the format *domain* rather than *domain.com*. The Web Interface pass-through with smart card from Access Gateway service does not recognize domains in the format *domain.com*, so users cannot log on if you specify the domain in this way.

3. Ensure the workspace control (for Access Gateway Advanced Edition only) and session time-out settings are configured correctly for both the Access Gateway and the Web Interface.

To enable smart card users to access their resources through the Access Gateway without providing a PIN

If you want to enable all users to access their XenApp resources without having to provide a PIN, you must enable Secure Sockets Layer (SSL) for the IIS site hosting the XenApp Web site. For more information, see the Microsoft documentation for IIS 7.*x* and IIS 6.0.

After enabling SSL, ensure that the Web server is within the same domain as your users and configure Active Directory to allow constrained delegation.

To ensure the 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. Log on to the domain controller as a domain administrator and open the MMC Active Directory Domains and Trusts snap-in.
2. In the left pane, select the domain name and, in the Action pane, click Properties.
3. If the domain is not at the highest possible functional level, select the domain name and, in the Action pane, click Raise Domain Functional Level.
4. To raise the domain functional level, click the appropriate level and click Raise.

To trust the servers running the Web Interface and the Citrix XML Service for delegation

1. Log on to the domain controller as a domain administrator and 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 and select the Web server.

4. In the Action pane, 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 server running the Citrix XML Service appears on the Services to which this account can present delegated credentials list and click OK.

10. Repeat Steps 3-9 for each server in the farm running the Citrix XML Service that the Web Interface is configured to contact.

11. In the left pane, click the Computers node and select the server running the Citrix XML Service that the Web Interface is configured to contact.

12. In the Action pane, click Properties.

13. On the Delegation tab, click Trust this computer for delegation to specified services only and Use Kerberos only, and then click Add.

14. In the Add Services dialog box, click Users or Computers.

15. 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.

16. Select the HOST service type from the list and click OK.

17. 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.

18. Repeat Steps 11–17 for each server in the farm running the Citrix XML Service that the Web Interface is configured to contact.

19. For security reasons, you must configure all servers in the farm for constrained delegation. To provide users with access to resources on those servers, you must add the relevant services, such as the http service for a Web server, to the Services to

which this account can present delegated credentials list.

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

To determine which resources are accessible from the server farm

1. Log on to the domain controller as a domain administrator and open the MMC Active Directory Users and Computers snap-in.

2. In the left pane, click the Computers node and select a server from the farm.

3. In the Action pane, 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 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 domain controller appear on the Services to which this account can present delegated credentials list and click OK.

9. Repeat the procedure for each server in the farm.

To configure a time limit for access to resources at domain level

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.

By default, 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.

1. Log on to the domain controller as a domain administrator and open the MMC Domain Security Policy snap-in.

2. In the left pane, select Account Policies > Kerberos Policy.

3. In the results pane, select Maximum lifetime for service ticket.

4. In the Action pane, click Properties.

5. Enter the required time limit (in minutes) in the Ticket expires in box.

If you do not want to configure a time limit for access to resources, select Use any authentication protocol when determining which resources are accessible from the server farm. If you select this option, any value specified for S4UTicketLifetime is ignored. For more information, visit the Microsoft Web site at http://support.microsoft.com/.

To enable smart card users to access their resources through the Access Gateway by providing a PIN

If you want smart card users to enter a PIN each time they access a resource through the Access Gateway, you must enable enumeration of users' security identifiers (SIDs) on the Citrix XML Service.

> **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.

1. If the user accounts exist in a different domain to that containing the server farm, ensure that the domains share a two-way trust relationship.

2. Verify that the Citrix XML Service can resolve the IP address and contact the domain controller of the user account domain. Requests to the Citrix XML Service may time out if it cannot communicate with the domain controllers.

3. Grant the Windows account under which the Citrix XML Service runs read access to the TGGAU attribute in Active Directory for each domain. For more information on the TGGAU attribute, see Microsoft Knowledge Base article 331951. By default, the Citrix XML Service is configured to run as the Network Service account. The required permissions can be granted by adding this account to the following built-in Active Directory groups:

   - Pre-Windows 2000 Compatibility Access

   - Windows Authorization Access
4. On the server running the Citrix XML Service, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\XMLService\ in the system registry.

5. Under the XMLService node, add a DWORD value named EnableSIDEnumeration and set the value set to 1.

   Note: For XenDesktop 5 and later, the registry key is:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer]
   "EnableXmlServiceSidEnumeration"=REG_DWORD:1

6. Restart IIS on the Web server. If you want the new permissions to take effect immediately rather than waiting for the Kerberos ticket cache period to expire, restart the server running the Citrix XML Service.

7. For Windows XP users who log on to their desktops using the same smart card that they use to log on to the Access Gateway, you can enable them to access their resources without having to provide a PIN by configuring pass-through with smart card

authentication:

a. Install the Citrix online plug-in or Citrix Desktop Viewer on your users' devices using an administrator account.

b. Add the client template to the Group Policy Object Editor. For more information, see Step 1: Installing the Plugin for Smart Card Authentication.

c. Enable pass-through authentication for all Citrix clients using group policy. For more information, see Step 1: Installing the Plugin for Smart Card Authentication.

Coordinating Web Interface and Access Gateway Settings

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

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

- **Session time-out.** Ensure all realms, logon points, or virtual servers use the same settings as the XenApp Web site.
- **Workspace control.** For Access Gateway Advanced Edition, disable all 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.

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 resources available to users.

Specifying Server Farms

When configuring a new site, you must enter details of the server farms that will provide resources for users of the site.

You can update these settings at any time using the Server Farms task in the Citrix Web Interface Management console. For more information about configuring communication with server farms, see Managing Servers and Farms.

Important: For compatibility with XenApp 4.0, with Feature Pack 1, for UNIX, an additional manual site configuration step is required. For more information, see To configure support for XenApp 4.0, with Feature Pack 1, for UNIX.

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 Authentication Methods task in the Citrix Web Interface Management console. For more information about configuring authentication, see Configuring Authentication for the Web Interface.

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 Authentication Methods task in the Citrix Web Interface Management console. For more information about configuring domain restrictions, see To configure domain restriction settings.

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 Web Site Appearance task in the Citrix Web Interface Management console. For more information about customizing the appearance of the user interface, see Customizing the Appearance for Users.

Specifying the Types of Resources Available to Users

When configuring a new site, you must specify the types of resources that you want to make available. The Web Interface provides users with access to resources (applications, content, and desktops) through a Web browser or the Citrix online plug-in. Integration with the offline application feature enables users to stream applications to their desktops and open them locally.

You can grant users access to resources as follows:

- **Online.** Users access applications, content, and desktops hosted on remote servers. Users need a network connection in order to work with their resources.
- **Offline.** Users stream applications to their desktops and open them locally. For XenApp Services sites, once applications have been delivered, users can run these applications at any time without connecting to the network. With XenApp Web sites, users need network connections to log on to the site and start their applications. Once the applications are running, the connection does not need to be maintained.
- **Dual mode.** Users access both offline applications and online applications, content, and desktops, all on the same site. If offline applications are not available, online versions are delivered, where possible.

You can update this setting at any time using the Resource Types task in the Citrix Web Interface Management console. For more information about Citrix client types, see Managing Clients.

Upgrading Existing Sites

If you are upgrading your installation from an earlier version of the Web Interface, back to and including Version 4.5, support is provided for upgrading existing sites (excluding Conferencing Manager Guest Attendee sites).

Important: 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 Web server.

Existing access platform/XenApp Web and Program Neighborhood Agent Services/XenApp Services sites are treated as follows:

- **Locally configured sites.** During installation, the Web Interface installer automatically upgrades all locally configured sites to the latest version.
- **Centrally configured and grouped sites.** During installation, the Web Interface installer automatically converts any existing centrally configured or grouped sites to use local configuration. The converted sites are then upgraded to the latest version.

By default, the Web Interface assumes that the file names of the client installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download clients from the Citrix Web site or if you plan to deploy older clients, check that the appropriate client installation file names are specified for the ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, and ClientStreamingWin32 parameters in the configuration files for your XenApp Web sites. For more information on Web Interface configuration file parameters, see WebInterface.conf Parameters.

Using Site Tasks

To configure a site, select the site type in the left pane of the Citrix Web Interface Management console, then click the site in the results pane and select from the available tasks in the Action pane or the Action menu. Alternatively, you can right-click a site name in the results pane and select tasks from the context menu.

Some tasks are available only for certain site types and configurations. Details of the tasks available for each site type are given in the table below.

Task	XenApp Web sites		XenApp Services sites		AD FS integrated sites
	Online/dual mode	Offline only	Online/dual mode	Offline only	
Authentication Method	*	*			
Authentication Methods	*	*	*	*	*
Client-Side Proxy	*		*		*
Client Deployment	*	*			*
Resource Refresh			*	*	
Resource Types	*	*	*	*	*
Secure Access	*		*		*
Server Farms	*	*	*	*	*
Server Settings			*	*	
Session Options			*		
Session Preferences	*	*			*
Shortcuts			*	*	
Site Maintenance	*	*	*	*	*
Web Site Appearance	*	*			*
Workspace Control	*				*

Repairing and Uninstalling Sites

Use the Repair Site and Uninstall Site tasks under Site Maintenance in the Citrix Web Interface Management console to repair and remove sites, respectively. 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 Web 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) 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 Sites Directly

If users access XenApp Web sites directly or through Access Gateway Enterprise Edition using the Citrix secure access plug-in, you can enable support for resource URLs. This enables users to create persistent links to resources accessed using the Web Interface.

Note: Resource URLs are not supported for users accessing sites through Access Gateway Standard Edition or Advanced Edition, or those using clientless access through Access Gateway Enterprise Edition.

Users can add persistent links to their shortcuts list or desktop. To enable support for resource URLs using the Citrix Web Interface Management console, click XenApp Web Sites in the left pane, select the site in the results pane, click Session Preferences in the Action pane, click Persistent URLs, and select the Enable users to access resources using browser bookmarks check box.

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

Making the Logon Screen the Default on Microsoft 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 under Site Maintenance in the Citrix Web Interface Management console.

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.

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 XenDesktop 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 site configuration file is running either Presentation Server 4.5 or later, or XenDesktop.

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 enables you to specify the server farm to which the change password request is issued. If the password change request fails, the next server farm in the sequence is issued the change password request. Use suitable password replication mechanisms between server farms to ensure that user passwords remain consistent.

To add a server farm

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Add.
5. Enter a name for the server farm in the Farm name box.
6. 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.
7. 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.

Important: For compatibility with XenApp 4.0, with Feature Pack 1, for UNIX, an additional manual site configuration step is required. For more information, see To configure support for XenApp 4.0, with Feature Pack 1, for UNIX.

To configure fault tolerance

The Web Interface provides fault tolerance among servers running the Citrix XML Service. Use the Server Farms task in the Citrix Web Interface Management console to configure fault tolerance. 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.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.
5. 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.
6. Change the length of time a failed server is bypassed for in the Bypass any failed server for box.

To enable 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 disabled.

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 Server Farms task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the CItrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.
5. On the Servers list, add the servers that you want to use for load balancing.
6. Select the Use the server list for load balancing check box.
7. 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 Server Farms task in the Citrix Web Interface Management console to specify how the Citrix XML Service transports data between the Web Interface and the server running XenApp or XenDesktop. The Citrix XML Service is a component of XenApp and XenDesktop that acts as the point of contact 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 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 users' 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. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.

3. In the Action pane, click Server Farms.

4. Click Add if you are adding a farm or select a name from the list and click Edit to configure an existing farm.

5. In the Communications Settings area, enter the port number in the XML Service port box. This port number must match the port used by the Citrix XML Service.

6. 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 SSL Relay running on a server running XenApp or XenDesktop to perform host authentication and data encryption.

7. If you are using SSL Relay, specify the TCP port of the 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 SSL Relay. Ensure all the servers running the SSL Relay are configured to listen on the same port.

   Note: If you are using SSL Relay or HTTPS, ensure the server names you specify match exactly (including the case) the names on the certificate for the server running XenApp or XenDesktop.

8. To configure ticketing, click Ticketing Settings.

9. Enter the lifetime of tickets for Citrix clients for online resources in the ICA ticket lifetime boxes.

10. Enter the lifetime of tickets for the Citrix offline plug-in in the Streaming ticket lifetime boxes.

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.

To enable 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 and is enabled by default. Socket pooling should not be used when the Web Interface is configured to use one or more servers running XenApp for UNIX.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Advanced.
5. In the Socket Pooling area, select the Enable socket pooling check box.

To enable content redirection

You can use the Server Farms task in the Citrix Web Interface Management console to enable and disable content redirection from plug-in to server for individual XenApp Services sites. This setting overrides any content redirection settings configured for XenApp.

When you enable content redirection from plug-in to server, users running the Citrix online plug-in open online content and local files with applications delivered from servers. For example, a Citrix online plug-in user who receives an email attachment in a locally running email program opens the attachment in an online application. When you disable content redirection, users open online content and local files with locally installed applications.

By default, content redirection is enabled from plug-in to server for XenApp Services sites.

You configure content redirection from plug-in to server by associating applications with file types. For more information about file type association, see XenApp Administration.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Advanced.
5. In the Content Redirection area, select the Enable content redirection check box.

To configure Citrix XML Service communication

By default, contact with the Citrix XML Service times out after one minute and the service is considered failed after two unsuccessful attempts are made to communicate with it. You can change these default settings using the Server Farms task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Server Farms.
4. Click Advanced.
5. To configure the Citrix XML Service time-out duration, enter appropriate values in the Socket timeout boxes.
6. 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 Server Settings task in the Citrix Web Interface Management console to configure how the Citrix online plug-in communicates with a site and whether or not users are redirected to alternative sites in the event of failure.

To configure server communication settings

Use the server communication settings to:

- **Enable SSL/TLS for communication.** Smart card logon and SSL/TLS-secured communications between the plug-in 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 XenDesktop.

- **Allow users to customize the server URL.** The server URL directs the Citrix online plug-in to the correct configuration file. The default path is determined based on the server address entered during installation. You can allow users to change the URL, which enables the Server URL box on the Server Options page of the Citrix online plug-in Options dialog box.

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

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.

3. In the Action pane, click Server Settings.

4. To use secure communication between the Citrix online plug-in and a site, select Use SSL/TLS for communication between plug-ins and the site.

5. To allow users to change the URL that directs the Citrix online plug-in to the configuration file, select Allow users to customize server URL.

6. To configure how often the Citrix online plug-in refreshes its configuration settings, select Schedule an automatic refresh every and enter the refresh period in hours, days, weeks, or years.

To specify Citrix online plug-in backup URLs

You can specify backup servers for the Citrix online plug-in to contact if the primary Web Interface server is not available. Use the Server Settings task in the Citrix Web Interface Management console 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, the Citrix online plug-in attempts to contact the next server on the list.

Important: All backup URLs must point to sites that are hosted on the same type of Web server as the primary site. For example, if the primary site is a Web Interface for Microsoft Internet Information Services site, any backup sites must also be Web Interface for Microsoft Internet Information Services sites.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.

3. In the Action pane, click Server Settings.

4. Click Backup.

5. Click Add.

6. 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.

7. Click OK.

8. 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.

To configure 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 using the Server Settings task in the Citrix Web Interface Management console. Users are redirected to the new site immediately or the next time they launch the Citrix online plug-in.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.

3. In the Action pane, click Server Settings.

4. Click Redirection.

5. 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 when the Citrix online plug-in configuration is refreshed
   - If you want to redirect users to an alternative site next time the plug-in launches, select Redirect the next time the Citrix online plug-in starts up
6. Enter the URL of the alternative site in the Redirect URL box.

Configuring Authentication for the Web Interface

Authentication Methods

Authentication takes place when a user accesses 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 XenApp 6.0, XenApp 5.0 for Windows Server 2008, or XenDesktop. However, XenApp 6.0 is compatible with Novell Domain Services for Windows.

- **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 integrated Windows authentication to connect to server farms. 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 XenApp Administration.

- **Pass-through with smart card.** Users can authenticate by inserting a smart card in a smart card reader attached to the user device. If users have installed the Citrix online plug-in, they are prompted for their smart card PIN when they log on to the user device. After logging on, users can access their resources 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 integrated Windows authentication to connect to the Web Interface, with smart cards used for authentication to the server farm. 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 XenApp Administration.

  Note: Because of the security enhancements introduced in Windows Vista, smart card users running Windows Vista or Windows 7 are required to provide their PINs when they access 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.

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

  Important: 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.

  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 smart cards and you want to enable pass-through authentication, select the option to use Kerberos authentication
- 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

  Note: Users who log on to Windows using explicit credentials and then subsequently access a site configured for pass-through with smart card authentication are presented with a Welcome to Windows dialog box when accessing resources. To cancel this dialog box, users must press right-ALT (ALT GR) + DELETE. Citrix recommends creating separate sites for users logging on with smart cards and users logging on with explicit credentials.

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 Authentication Methods task in the Citrix Web Interface Management console to configure the ways in which users can authenticate to XenApp, XenDesktop, and the Citrix online plug-in.

To configure domain restriction settings

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Authentication Methods and ensure that anonymous authentication is not the only authentication method enabled for users.
4. Click Properties and select Domain Restriction.
5. 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 domain
   - If you want to restrict access to users from selected domains, select Restrict to the following domains
6. Click Add.
7. 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 and UPN Restriction lists. For more information, see To use domain-based authentication.

To configure automatic logon settings

Use the Authentication Methods task in the Citrix Web Interface Management console to configure automatic logon settings for users accessing their 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.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Authentication Methods and select one or more of the Pass-through, Pass-through with smart card, and Smart card checkboxes.

4. Click Properties and select Automatic Logon.

5. 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.

To use domain-based authentication

If you are using explicit or prompt authentication, use the Authentication Methods task in the Citrix Web Interface Management console to configure whether users authenticate using Windows or Novell Directory Services (NDS).

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit, Prompt, and/or Pass-through check boxes, as required.
4. Click Properties and select Authentication Type.
5. Select Windows or NIS (UNIX).
6. 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
7. Click Settings.
8. 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, select Pre-populated in the Domain list box and add UNIX as the domain name.
   - Specify the domains you want to appear in the Domain box on the Logon screen
9. 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 and UPN Restriction lists. For more information, see Configuring Authentication.

To use Novell Directory Services authentication

If you are using explicit or prompt authentication, use the Authentication Methods task in the Citrix Web Interface Management console to configure whether users authenticate using Windows or Novell Directory Services (NDS).

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit, Prompt, and/or Pass-through check boxes, as required.
4. Click Properties and select Authentication Type.
5. Select NDS.
6. Enter a name in the Default tree name box.
7. Click Settings and configure context restriction or contextless authentication, as appropriate.

   Note: By default, eDirectory does not give anonymous connection access to the cn attribute, which is required for contextless logon. For information about how to reconfigure eDirectory, visit http://developer.novell.com/wiki/index.php/Developer_Home.
8. For XenApp Services sites, select Use Windows credentials if you want Citrix online plug-in users with the Novell client installed to use their Windows credentials for pass-through authentication.

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. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Authentication Methods and select the Explicit check box.

4. Click Properties to configure further settings for explicit authentication.

To configure password settings for explicit authentication

Use the Authentication Methods task in the Citrix Web Interface Management console 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.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit check box.
4. Click Properties and select Password Settings.
5. If you want users to be able to change their password within a Web Interface session, select the Allow users to change passwords check box.
6. To specify when users can change their password, choose one of the following options:
   - To allow users to change their passwords when they expire, select Only when they expire. When you choose 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 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 choose 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.
7. 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 customized reminder setting. Specify the number of days, weeks, or years in the Remind users before expiry boxes.

To enable two-factor authentication

Use the Authentication Methods task in the Citrix Web Interface Management console to enable two-factor authentication for users, if required.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit check box.
4. Click Properties and select Two-Factor Authentication.
5. Select the type of two-factor authentication you want to use from the Two-factor setting list and configure any additional settings as appropriate.

For more information about configuring Aladdin SafeWord, RSA SecurID, and RADIUS authentication, see Configuring Two-Factor Authentication.

Configuring Account Self-Service

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

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 user account management functions for internal use only, you must ensure the site is not accessible outside of your internal network.

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 users access the Web Interface using an HTTP connection, account self-service is unavailable. Account self-service is not available for Access Gateway integrated sites.

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.

To configure account self-service

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Authentication Methods and select the Explicit check box.

4. Click Properties and select Account Self-Service.

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

6. 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. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Prompt check box.
4. Click Properties to configure further settings for prompt authentication.

To configure password settings for prompt authentication

Use the Authentication Methods task in the Citrix Web Interface Management console to specify whether or not users can save their passwords and to configure password change options for users.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Prompt check box.
4. Click Properties and select Password Settings.
5. To allow users to save their passwords, select the Allow users to save passwords option.
6. 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.
7. Specify the path through which the change password request is routed by choosing one of the following options:
   - If you want Citrix online plug-in 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 Citrix online plug-in to the domain controller, bypassing the Web Interface and XenApp/XenDesktop.
   - If you would prefer Citrix online plug-in users to change their passwords by connecting directly to the domain controller, but want to enable connections through the Web Interface and XenApp/XenDesktop if the preferred connection method fails, select Domain controller directly, with fallback to server farm.
   - If you want Citrix online plug-in users to change their passwords by connecting to the domain controller through the Web Interface and XenApp/XenDesktop, select Server farm. This option ensures that when users change their passwords, Web Interface plus XenApp and/or XenDesktop 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.

Pass-Through Requirements

To use the pass-through authentication feature, the Web Interface must be running on IIS and users must be running supported versions of Internet Explorer. For XenApp Web sites, users must add the site to the Windows Trusted sites or Local intranet zones using Internet Explorer.

If you are using Internet Explorer Version 7 or later:

1. Add the site to the Windows Trusted sites, click Internet Options and navigate to the Security tab.

2. Highlight the Trusted Sites zone and click Custom level.

3. Navigate to the end of the Security Settings window to User Authentication, click Logon, and then set it to automatic logon with the current user name and password.

For IIS 7.*x* 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 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 authentication cannot be used. To use pass-through with ICA encryption, your users must install the latest Citrix clients. 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 Citrix client (using the Web browser as an intermediary in some cases). The file can contain a setting that instructs the client to send the user’s workstation credentials to the server. By default, the client does not honor this setting; however, there is a risk that if the pass-through feature is enabled on the Citrix online plug-in, 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 Plug-in for Pass-Through Authentication

You must install the Citrix online plug-in or Citrix Desktop Viewer on your users' devices using an administrator account. Pass-through authentication is available only with these plug-ins, which are included on the XenApp and XenDesktop installation media. For security reasons, the Citrix online plug-in – web does not include this feature. This means that you cannot use Web-based client installation to deploy Citrix plug-ins containing this feature to your users.

After installation, you must enable pass-through authentication for all Citrix clients using group policy. For more information, see http://support.citrix.com/article/CTX122676 and the *Receiver and Plug-ins* > *Online Plug-in for Windows* documentation in Citrix eDocs.

Step 2: Enabling Pass-Through for the Plugins

Enabling pass-through authentication for the clients is a two-step process. First, you add the client template to the Group Policy Object Editor. Once added, you use this template to enable pass-through authentication for all clients.

To add the client template to the Group Policy Object Editor for pass-through authentication

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 client template file, icaclient.adm. This file is installed in the \Configuration folder for the clients, typically C:\Program Files (x86)\Citrix\ClientName\Configuration.
5. Click Open to add the template and then click Close.

To enable pass-through authentication for all clients

1. Open the MMC Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. In the left pane, expand the Administrative Templates node.
4. Select Classic Administrative Templates (ADM) > Citrix Components. Expand the node for the client you installed and select User authentication.
5. In the results pane, select Local user name and password.
6. On the Action menu, click Edit.
7. Click Enabled and verify that the Enable pass-through authentication check box is selected.
8. Ensure that all the above steps are completed for both the user and the computer in the Group Policy Object Editor.
9. Log off and then log on again to allow your policy changes to take effect.

Step 3: Enabling Pass-Through Using the Console

Use the Citrix Web Interface 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.

To enable pass-through authentication

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Pass-through check box.
4. Click Properties and select Kerberos Authentication.
5. If you want to enable Kerberos authentication, select the Use Kerberos authentication to connect to servers check box (for XenApp Web sites) or the Use Kerberos only check box (for XenApp Services sites).

Enabling Smart Card Authentication

To use smart card authentication, the Web Interface must be running on IIS and users must be running supported versions of Internet Explorer or Firefox. For pass-through with smart card authentication, users must be running supported versions of Internet Explorer; Firefox is not supported for pass-through with smart card authentication.

If you plan to enable pass-through with smart card authentication for a XenApp Web site, users must add the site to the Windows Trusted sites or Local intranet zones using Internet Explorer.

For IIS 7.*x* 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. If you plan to enable pass-through with smart card authentication, ensure that the Web Server > Security > Windows Authentication role service is also enabled.

Smart card authentication is not supported by Web Interface for Java Application Servers.

Secure Sockets Layer (SSL) must be enabled on the Web server because SSL is used to secure communication between the Web browser and server. For more information, see the documentation for your Web server.

To enable smart card authentication (with or without other authentication methods), you must configure the Logon screen so that it is accessible using HTTPS connections only. If simple HTTP is used or HTTPS is misconfigured, users receive an error message and cannot log on. To avoid this problem, provide the full HTTPS URL to all users; for example, https://www.*MyCompany.com*:443/Citrix/XenApp.

For more information about user device requirements and server requirements for smart card authentication, see Online Plug-in for Windows and XenApp Administration.

Step 1: Installing the Plugin for Smart Card Authentication

To use smart card authentication, users need to install the Citrix online plug-in or Citrix Desktop Viewer. Alternatively, they can use Web-based client installation to download and install the Citrix online plug-in – web from a suitably configured XenApp Web site. However, to use pass-through with smart card authentication, you must install the Citrix online plug-in or Citrix Desktop Viewer on your users' devices using an administrator account. Pass-through authentication is available only with these plug-ins, which are included on the XenApp and XenDesktop installation media. For security reasons, the Citrix online plug-in – web does not include this feature.

If you plan to enable pass-through with smart card authentication, you must first enable pass-through authentication for all Citrix clients using group policy after you have installed the plug-in. Enabling pass-through authentication for the clients is a two-step process. First, you add the client template to the Group Policy Object Editor. Once added, you use this template to enable pass-through authentication for all clients.

To add the client template to the Group Policy Object Editor for pass-through authentication

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 client template file, icaclient.adm. This file is installed in the \Configuration folder for the clients, typically C:\Program Files (x86)\Citrix\ClientName\Configuration.

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

To enable pass-through with smart card authentication for all clients

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

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

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

4. Select Classic Administrative Templates (ADM) > Citrix Components. Expand the node for the client you installed and select User authentication.

5. In the results pane, select Smart card authentication.

6. On the Action menu, click Edit.

7. Click Enabled and select the Allow smart card authentication and Use pass-through authentication for PIN check boxes.

Step 2: Enabling the Windows Directory Service Mapper

To enable smart card authentication, 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. Smart cards, however, contain certificates. 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 Microsoft Internet Information Services 7.x

1. On the Web Interface server, 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.

3. Select your Web server in the left pane and, in the Features View, double-click Authentication.

4. On the Authentication page, enable the Active Directory Client Certificate Authentication method.

To enable the Windows Directory Service Mapper on Microsoft 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, in the Action pane, click Properties.

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

Step 3: 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 obtain their resource sets) and authentication to the server (so that users can access resources in a session using the Web Interface).

To enable smart card authentication for XenApp Web sites

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Smart card or Pass-through with smart card check box, as appropriate.
4. Click Properties to configure further settings for smart card authentication.

To enable smart card authentication for XenApp Services sites

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Services Sites and select your site in the results pane.

3. In the Action pane, click Authentication Methods and select the Smart card or Pass-through with smart card check box, as appropriate.

4. Click Properties and 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

6. If you enabled pass-through with smart card authentication and you want to use Kerberos authentication between the plug-in and the XenApp Services site, click Kerberos Authentication and select the Use Kerberos to authenticate to the XenApp Services site check box.

Example: Enabling Smart Card Authentication for Users

You want to enable pass-through with smart card authentication for a user. The user's computer is running Windows XP. A smart card reader is attached to the computer and smart card support is configured on the server farm. Currently, the Web Interface is configured for explicit/prompt authentication only (user name and password).

To enable pass-through with smart card authentication

1. Use the appropriate installation media to install the Citrix online plug-in or Citrix Desktop Viewer on the user’s computer. The installation of the plug-in is performed using an administrator account. For XenApp Web sites, add the site to the Windows Trusted sites or Local intranet zones using Internet Explorer on the user's computer.

2. Enable pass-through authentication for all Citrix clients using group policy. For more information, see Step 1: Installing the Plugin for Smart Card Authentication. You must also ensure that pass-through authentication is enabled on the farm. For more information, see the documentation for your Citrix server.

3. Ensure that the Windows Directory Service Mapper is enabled. For more information, see Step 2: Enabling the Windows Directory Service Mapper.

4. Use the Authentication Methods task in the Citrix Web Interface Management console to enable pass-through with smart card authentication. For more information, see Step 3: Enabling Smart Card Authentication on the Web Interface Users log on to their physical Windows desktops using their smart cards. When users access their resources, they are logged on automatically. When smart card authentication is enabled without pass-through, users have to reenter their PINs when accessing their resources.

Configuring Two-Factor Authentication

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

- **Aladdin 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 resources on the server. When creating users on the RSA 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 two-factor authentication option available.

Enabling SafeWord Authentication on Microsoft Internet Information Services

This section describes how to enable RSA SecurID 6.0 support.

SafeWord Requirements

To use SafeWord authentication with the Web Interface for Microsoft Internet Information Services:

- Obtain the latest version of the SafeWord Agent from Aladdin Knowledge Systems. If support for UPN authentication is required, ensure you apply the latest auto-updates to the SafeWord Agent for the Web Interface and to 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.aladdin.com/safeword/default.aspx.

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 Authentication Methods task in the Citrix Web Interface Management console.

Enabling RSA SecurID Authentication on Microsoft Internet Information Services

This section describes how to enable RSA SecurID 7.0 support.

SecurID Requirements

To use SecurID authentication with the Web Interface for Microsoft Internet Information Services:

- The RSA ACE/Agent for Windows 7.0 or later must be installed on the Web server.
- The Web Interface must be installed after installing the RSA ACE/Agent.
- The Web Interface must be hosted on Microsoft Internet Information Services 6.0.

Adding the Web Interface Server as an Agent Host

You must create an Agent Host for the Web server in the RSA ACE/Server database so that the RSA ACE/Server recognizes and accepts authentication requests from the Web server. When creating the Agent Host, configure the Web Interface as a NetOS Agent. This setting is used by the RSA ACE/Server to determine how communication with the Web Interface occurs.

Copying the sdconf.rec File

Locate (or if necessary, create) the sdconf.rec file on the RSA ACE/Server and copy it to the \System32 folder on the Web Interface server, which is typically located at C:\Windows\System32. This file provides the Web Interface 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 Authentication Methods task in the Citrix Web Interface Management console.

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 of the form *DOMAIN\username* (as opposed to user name only) and use the Authentication Methods task in the Citrix Web Interface Management console to configure the Web Interface to send the domain and user name to the RSA ACE/Server.

Enabling RSA SecurID Windows Password Integration

The Web Interface supports the Windows password integration feature of RSA SecurID. With this feature enabled, users of the Web Interface can log on and access 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 Windows password integration with the Web Interface for Microsoft Internet Information Services:

- The RSA ACE/Agent Local Authentication Client for Windows must be installed on the Web server (administrators must log on to the Web Interface using local server administrator credentials)
- The Web Interface must be installed after installing the RSA ACE/Agent
- The RSA Authentication Agent Offline Local service must be running on the Web server
- The Agent Host for the Web server in the RSA ACE/Server 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

To reset the node secret registry key on the Web server

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

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

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

If the node secret on the Web Interface server and the RSA ACE/Server do not match, 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.

1. In the system registry, navigate to:
    - HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT on 32-bit servers
    - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SDTI\ACECLIENT on 64-bit servers
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 ACE/Server, the node secret can be reused.

Enabling RADIUS Authentication

This section describes how to install and configure Aladdin 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.
- The client type must be set to RADIUS standard.
- For added security, the Request must contain the Message Authenticator attribute option must be selected.

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. The location for this file is given by the RADIUS_SECRET_PATH configuration value in the web.config file (for sites hosted on IIS) or web.xml file (for sites hosted on Java application servers). The location given is relative to the \conf folder for sites hosted on IIS and relative to the /WEB_INF directory for sites hosted on Java application servers.

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.

Specifying a Network Access Server Identifier for RADIUS

The RADIUS protocol requires that access requests to RADIUS servers include the IP address or other identifier for the RADIUS client (that is, the Web Interface). In order to enable RADIUS authentication, you must either provide the IP address of the Web server or specify a value for the RADIUS network access server (NAS) identifier attribute. The value of the NAS identifier attribute can be any string containing three characters or more. Although this attribute does not need to be unique for each RADIUS client, setting a unique identifier for each client may help with diagnosing RADIUS communication problems.

To provide the IP address of the RADIUS client, enter the IP address of the Web server as the value for the RADIUS_IP_ADDRESS configuration parameter in the web.config file (for sites hosted on IIS) or web.xml file (for sites hosted on Java application servers). To set the RADIUS NAS identifier, specify a value for RADIUS_NAS_IDENTIFIER in web.config or web.xml.

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 Authentication Methods task in the Citrix Web Interface Management console. 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.

Important: When you enable RADIUS authentication, you must also either provide the IP address of the RADIUS client or specify a value for the RADIUS network access server identifier attribute in the web.config file (IIS) or web.xml file (Java application servers) for the site.

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 Enabling RADIUS Authentication.
- The client type must be set to RADIUS standard.
- For added security, the Request must contain the Message Authenticator attribute option must be selected.

Enabling RADIUS with RSA SecurID

RADIUS is enabled on the RSA Authentication Manager using the SecurID Configuration Management Tool. For more information about this tool, see the RSA Authentication Manager documentation.

Adding the Web Interface and RADIUS Servers as Authentication Agents

Assuming the RSA Authentication Manager that authenticates users also acts as the RADIUS server, you must create an Authentication Agent record for the local RADIUS server in the RSA Authentication Manager database. When creating the Authentication Agent record, set the name and IP address to that of the local server and configure this server as a NetOS Authentication Agent. The local server must be assigned as the acting server.

In addition, you must create an Authentication Agent record for each Web Interface server in the RSA Authentication Manager database so that the RSA Authentication Manager recognizes and accepts authentication requests from the Web Interface through the RADIUS server. When creating an Authentication Agent record, configure the Web Interface as a Communication Server and set the encryption key to the value of the secret that is shared with the Web Interface.

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 Microsoft Internet Information Services, 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 documentation for the SecurID software. To display the same messages to users accessing sites on IIS and Java application servers, the following challenges must be updated:

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

Managing Clients

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

Clients for Online Resources

The following Citrix clients can be used to access online resources:

- **Native client.** Administrators install the appropriate native client on users' devices. Alternatively, users without a native client can download and deploy the Citrix online plug-in – web using the client detection and deployment process. Seamless windows are supported; resources are presented in desktop windows that can be resized. If users are accessing resources through PDA devices, you must enable the native client.

- **Client for Java.** Users run the Client for Java when the resource is accessed. This client is typically used in situations where users do not have a native client installed and are unable to download and deploy the Citrix online plug-in – web or are prevented from doing so by the configuration of their devices or the XenApp Web site. The Client for Java supports seamless windows; resources are presented in desktop windows that can be resized.

- **Embedded Remote Desktop Connection (RDP) software.** Users can use the Remote Desktop Connection (RDP) software that is already installed as part of their Windows operating system if you have made this option available. The client detection and deployment process does not make the Remote Desktop Connection (RDP) software available to users who do not have it installed. Seamless windows are not supported; resources are presented embedded in browser windows.

  Note: The Client for Java and embedded Remote Desktop Connection (RDP) software are not supported on devices running Windows CE or Windows Mobile. The Client for Java and embedded Remote Desktop Connection (RDP) software are not supported for use with AD FS integrated sites.

Configuring the Citrix Online Plug-in

The Citrix online plug-in enables users to access applications, content, and virtual desktops directly from physical Windows desktops without using a Web browser. You can remotely configure the placement of links to resources on the Start menu, on the Windows desktop, or in the Windows notification area. The user interface of the Citrix online plug-in can also be “locked down” to prevent user misconfiguration. You can use the Citrix Web Interface Management console or the config.xml file to configure the Citrix online plug-in.

Using the Citrix Web Interface Management Console for Configuration

The Citrix online plug-in is configured with default presentation options, authentication methods, and server connection options. The Citrix Web Interface Management console enables you to change the default settings to prevent users from changing specific options.

Using the Configuration Files

You can also configure the Citrix online plug-in 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 Plug-in Configuration Files

The Citrix online plug-in options configured with the console are stored in a configuration file on the Web Interface server. The configuration file controls the range of parameters that appear as options in the user’s Citrix online plug-in 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 resources.

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

Copying Client Installation Files to the Web Interface

To use Web-based client installation, the client installation files must be available on the Web Interface server.

During Web Interface installation, Setup prompts you to access the XenApp or XenDesktop installation media. On IIS, Setup copies the contents of the \Citrix Receiver and Plug-ins folder on the installation media to a folder called \Clients in the root directory; for example, C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients. On Java application servers, Setup copies the Citrix clients from the installation media and packages them in the .war file.

If you did not copy the client installation files to the Web server during Web Interface installation, make sure you copy these files to the Web server before using Web-based client installation; for example, copy the files from Citrix Receiver and Plug-ins/Windows folder. If the XenApp or XenDesktop installation media is not available, you must manually recreate the required directory structure and then download the clients that you need from the Citrix Web site.

By default, the Web Interface assumes that the file names of the client installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download clients from the Citrix Web site or if you plan to deploy older clients, check that the appropriate client installation file names are specified in the configuration files for your XenApp Web sites.

To copy the client files to the Web Interface on Microsoft Internet Information Services

1. Locate the \Clients folder in the Web Interface installation; 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. Navigate to the \Citrix Receiver and Plug-ins folder on the installation media. Copy the contents of the folder on the installation media to the \Clients folder on the Web Interface server. Make sure you copy only the *contents* of the folder and not the \Citrix Receiver and Plug-ins folder itself.

   If the XenApp or XenDesktop installation media is not available, you must manually recreate the directory structure below and then download the clients that you need from the Citrix Web site.

   C:\Program Files (x86)\Citrix\Web Interface*Version*\Clients

   - \de
     - \Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with German language support in this folder.
   - \en
     - \Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with English language support in this folder.
   - \es
     - \Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with Spanish language support in this folder.
   - \fr
     - \Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with French language support in this folder.
   - \ja
     - \Unix

    Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with Japanese language support in this folder.

- \Java

  Place the Client for Java files in this folder.

- \Linux

  Place the Citrix Receiver for Linux installation file (linuxx86-*Version*.tar.gz) in this folder.

- \Mac

  - \Web Online Plug-in

    Place the Citrix online web plug-in for Macintosh installation file {Citrix online plug-in (web).dmg} in this folder.

- \Windows

  - \Offline Plug-in

    Place the Citrix offline plug-in installation file (CitrixOfflinePlugin.exe) in this folder.

  - \Online Plug-in

    Place the Citrix online plug-in – web installation file (CitrixOnlinePluginWeb.exe) in this folder.

By default, the Web Interface assumes that the file names of the client installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download clients from the Citrix Web site or if you plan to deploy older clients, check that the appropriate client installation file names are specified for the ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, and ClientStreamingWin32 parameters in the configuration files for your XenApp Web sites.

Once you have copied the client installation files into the directory structure above, any XenApp Web sites that are configured for Web-based client installation will automatically offer the clients to users who require one.

To copy the client files to the Web Interface 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 /Citrix Receiver and Plug-ins directory on the installation media. Copy the contents of the directory on the installation media to the /Clients directory on the Web Interface server. Make sure you copy only the *contents* of the directory and not the /Citrix Receiver and Plug-ins directory itself.

   If the XenApp or XenDesktop installation media is not available, you must manually recreate the directory structure below and then download the clients that you need from the Citrix Web site.

   XenAppWebSiteRoot/Clients

   - /de
     - /Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with German language support in this directory.
   - /en
     - /Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with English language support in this directory.
   - /es
     - /Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with Spanish language support in this directory.
   - /fr
     - /Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with French language support in this directory.
   - /ja
     - /Unix

       Place the Clients for UNIX installation files (solaris.tar.Z, sol86.tar.Z) with Japanese language support in this directory.
   - /Java

Place the Client for Java files in this directory.

- /Linux

  Place the Citrix Receiver for Linux installation file (linuxx86-*Version*.tar.gz) in this directory.

- /Mac

  - /Web Online Plug-in

    Place the Citrix online web plug-in for Macintosh installation file {Citrix online plug-in (web).dmg} in this directory.

- /Windows

  - /Offline Plug-in

    Place the Citrix offline plug-in installation file (CitrixOfflinePlugin.exe) in this directory.

  - /Online Plug-in

    Place the Citrix online plug-in – web installation file (CitrixOnlinePluginWeb.exe) in this directory.

By default, the Web Interface assumes that the file names of the client installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download clients from the Citrix Web site or if you plan to deploy older clients, check that the appropriate client installation file names are specified for the ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32, and ClientStreamingWin32 parameters in the configuration files for your XenApp Web sites.

4. Once you have copied the client installation files into the directory structure above, restart the Web server. If you have configured the XenApp Web site for Web-based client installation, the clients will be offered to users who require one.

Configuring Client Deployment and Installation Captions

The Web Interface provides a client detection and deployment process that detects which Citrix clients 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 client detection and deployment process in up to three ways:

- You can configure the client detection and deployment process to run automatically when users access a XenApp Web site. The client detection and deployment process starts automatically, helping users to identify and deploy the appropriate Citrix client to access their resources. For some environments, the client detection and deployment process can also detect the presence or absence of an installed client and prompt the user only when necessary.
- You can allow users to specify their preferred client for accessing online resources. This adds the Run Client Detection button to the Settings screen, enabling users to start the client 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 client detection and deployment process.

When a user accesses a XenApp Web site, the Web-based client detection and deployment process attempts to determine whether or not the preferred Citrix client is installed on the user's computer. Before the user logs on to a XenApp Web site configured for automatic client detection and deployment, the process starts automatically and guides the user through the procedure for identifying and deploying a suitable Citrix client to access their resources, including, where appropriate, reconfiguring their Web browser.

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

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

You can use the Client Deployment task in the Citrix Web Interface Management console to specify the circumstances under which users can access the client detection and deployment process.

To configure client deployment and installation captions

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.

3. In the Action pane, click Client Deployment. For sites that offer only online applications, select the Native client checkbox and click Properties.

4. Click Client Detection.

5. If you want the client detection and deployment process to start automatically when users without a suitable Citrix client access a XenApp Web site, select the Perform client detection at logon check box.

6. To prompt users to upgrade their clients when the client detection and deployment process detects that newer versions are available for download from the XenApp Web site, select the Offer upgrades for clients check box.

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

    - To notify the user if an appropriate client cannot be detected or if a more suitable client is available, select Whenever a client is needed. This is the default setting.

    - To notify the user only if an appropriate client cannot be detected, select Only if resources cannot be accessed.

    - If you do not want installation captions to appear under any circumstances, select Never.

Configuring ICA File Signing

The Web Interface can digitally sign generated ICA files with a chosen certificate, to allow compatible Citrix clients and plug-ins to validate that the file originates from your organization.

To use ICA File Signing, the following components are required:

- Web Interface version 5.4 or later
- Merchandising Server version 1.2 or later (for non-managed client security policy deployment)
- Group Policy Objects for managed client security policy deployment
- Administrative Template file format for Windows Server 2003 or later

Citrix recommends, in order of priority:

- You buy a code signing certificate or SSL signing certificate from a public Certificate Authority (such as Verisign.)
- If the enterprise already has a private Certificate Authority, create a code signing certificate or SSL signing certificate using the private Certificate Authority.
- Use an existing SSL certificate, such as the Web Interface or Dazzle server certificate.
- Create a new root Certificate Authority and distribute it to clients using Group Policy Objects.

The certificate must meet the following requirements:

- The certificate must include the private key.
- The certificate cannot be expired.
- One of the following must be true:
    - The certificate has no key usage or enhanced key usage field.
    - The key usage field allows the key to be used for digital signatures.
    - The enhanced key usage field is set to Code Signing or Server Authentication.

The Web Interface signs ICA files using either the SHA-1 or SHA-256 hash algorithm. The SHA-256 hash algorithm is newer and more secure, however it is only supported on servers running Windows 2008 or later and clients running Windows Vista or later. The SHA-1 hash algorithm can be used on all supported server and client operating systems.

ICA File Signing cannot be used with the Client for Java, RDP client, Citrix Streaming client, and for published documents downloaded from network shares.

To enable ICA File Signing, the site must be configured to use the native client, configured to display online applications, and EnableLegacyIcaClientSupport must be set to Off in the Webinterface.conf file.

For more information about enabling ICA File Signing for the Citrix Online Plug-in, see the Citrix Merchandising Server documentation.

To enable ICA File Signing in the Web Interface Management Console

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Client Deployment.
4. Click ICA File Signing.
5. Select Enable ICA File Signing and select a certificate from the drop-down menu. If the required certificate is not present in the list, click Import to import a certificate into the personal certificate store.
6. If you are running Windows 2008 or later, you can select the type of hash algorithm used. Otherwise, SHA-1 will be used. After configuring ICA File Signing on Windows 2003, you will need to restart the computer.

Configuring Streaming Session Monitoring

You can use the Client Deployment task in the Citrix Web Interface Management console 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 offline plug-in. 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 Delivery Services Console to view session information. You can view information for all user sessions in multiple farms, specific applications, sessions connecting to a specific server, or a specific user's sessions and applications.

To configure streaming session monitoring

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Client Deployment.
4. Click Citrix Offline Plug-in.
5. Select how the Web Interface communicates with the Citrix offline plug-in. Choose from the following:
    - To automatically detect the session URL used to communicate with the plug-in, select Automatically detect session URL
    - To set the session URL manually, select Specify session URL and enter the URL details

Deploying Remote Desktop Connection Software

Remote Desktop Connection (RDP) functionality is available on 32-bit Windows systems running Internet Explorer. Users who have installed version 6.0 (included with Windows XP with Service Pack 3) or later of the Microsoft Remote Desktop Connection (RDP) software can use it to access their resources. If users are unable to use any other clients, the client detection and deployment process checks whether the Remote Desktop Connection (RDP) software is available and helps users to enable the Terminal Services ActiveX Control, if necessary. The option to use Remote Desktop Connection (RDP) software is only available for sites that offer solely online applications.

Note: If Internet Explorer does not place the XenApp Web site in the Local intranet or Trusted sites zone, it displays an error message. The Web Interface client detection and deployment process provides users with instructions on how to add the site to the relevant Windows security zone.

Deploying the Client for Java

If you are deploying Citrix clients over a low bandwidth network or you are not sure what platform your users are running, 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.

Because the Client for Java offers the broadest range of support in terms of user environments, devices, operating systems, and Web browsers, it can be used as a fallback option for scenarios where a native client cannot be used. You can configure the client detection and deployment process to offer the Client for Java to users who do not have a native client or are unable to download and deploy a client from the XenApp Web site.

You must ensure that the Client for Java is available in the \Clients directory for the XenApp Web site in order to be able to deploy it to your users.

To configure fallback to the Client for Java

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Client Deployment. For sites that offer only online applications, select the Native client checkbox and click Properties.

   Note: You do not need to make the Client for Java available to users in order to provide the fallback functionality.
4. Click Fallback Behavior.
5. Specify the circumstances under which users without a native client are offered the Client for Java by choosing one of the following options:
   - If you want users without a native client to download and deploy an appropriate Citrix client, select Deploy a native client. This is the default setting.
   - If you want users without a native client to be offered the Client for Java and only be prompted to download and deploy a native client if they cannot use the Client for Java, select Deploy a native client and allow user to choose between this and the Client for Java.
   - If you want users without a native client to be prompted to download and deploy an appropriate client in addition to being offered the Client for Java, select Automatically fall back to the Client for Java.

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 is determined by the packages you include. The fewer packages selected, the smaller the size (it can be as small as 540 KB). If you want to limit the size of the Client for Java for users on low bandwidth connections, you can deploy only a minimum set of components. Alternatively, you can allow users to select which components they require. For more information about the Client for Java and its components, see the Client for Java documentation.

Note: Some components that you make available in the Client for Java may require further configuration on users' devices or on the server.

The following table explains the options available:

Package	Description
Audio	Enables resources running on the server to play sounds through sound devices installed on users' computers. You can control the amount of bandwidth used by the client audio mapping on the server. For more information, see XenApp Administration.
Clipboard	Enables users to copy text and graphics between online resources and applications running locally on their devices.
Local text echo	Accelerates the display of the input text on users' devices.
SSL/TLS	Secures communication using Secure Sockets Layer (SSL) and TLS (Transport Layer Security). SSL/TLS provides server authentication, encryption of the data stream, and message integrity checks.
Encryption	Provides strong encryption to increase the privacy of Citrix client connections.
Client drive mapping	Enables 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. For more information, see the Client for Java documentation.

Printer mapping	Enables users to print to their local or network printers from within a session.
Configuration UI	Enables the Client for Java Settings dialog box. This dialog box is utilized by users to configure the Client for Java.

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

If you configured Secure Gateway or the 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 user's device. For more information, see the Client for Java documentation.

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 Citrix clients. However, if you are using the Access Gateway, Secure Gateway, or a firewall in your deployment, you can use the Secure Access task in the Citrix Web Interface Management console 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 the Access Gateway.

This section explains how to use the Secure Access task to specify access settings, edit address translations, and configure gateway settings.

To configure direct access routes

If you want the actual address of the Citrix server to be given to a particular set of Citrix clients, you can specify user device addresses and masks using the Secure Access task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.

3. In the Action pane, click Secure Access.

4. 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.

5. From the Access method list, select Direct.

6. Enter the network address and subnet mask that identify the client network.

7. Use the Move Up and Move Down buttons to place the access routes in order of priority in the User device addresses table.

To configure alternate address settings

If you want the alternate address of the Citrix server to be given to a particular set of Citrix clients, you can specify user device addresses and masks using the Secure Access task in the Citrix Web Interface Management console. 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.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Secure Access.
4. 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.
5. From the Access method list, select Alternate.
6. Enter the network address and subnet mask that identify the client network.
7. Use the Move Up and Move Down buttons to place the access routes in order of priority in the User device addresses table.

To configure internal firewall address translation

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 Citrix client. To do this, use the Secure Access task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Secure Access.
4. 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.
5. From the Access method list, select Translated.
6. Enter the network address and subnet mask that identify the client network. Use the Move Up and Move Down buttons to place the access routes in order of priority in the User device addresses table and click Next.
7. 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.
8. In the Access Type area, select one of the following options:
    - If you want the Citrix client to use the translated address to connect to the Citrix server, select User device route translation
    - If you already configured a gateway translated route in the User device addresses table and want both the client and the gateway server to use the translated address to connect to the Citrix server, select User device and gateway route translation
9. Enter the internal and external (translated) ports and addresses for the Citrix server. Clients 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.

To configure gateway settings

If you are using the Access Gateway or Secure Gateway in your deployment, you must configure the Web Interface for gateway support. To do this, use the Secure Access task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.

3. In the Action pane, click Secure Access.

4. 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.

5. 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, select Gateway direct.

   - If you want the alternate address of the XenApp server to be given to the gateway, 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 to be determined by the address translation mappings set in the Web Interface, select Gateway translated.

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

7. If you are not using gateway address translation, continue to Step 10. 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.

8. In the Access Type area, select one of the following options:

   - If you want the gateway to use the translated address to connect to the Citrix server, select Gateway route translation

   - If you already configured a client translated route in the User device addresses table and want both the Citrix client and the gateway to use the translated address to connect to the Citrix server, select User device and gateway route translation

9. Enter the internal and external (translated) ports and addresses for the Citrix server and click OK. When the gateway connects to the Citrix server, it uses the external port number and address. Ensure that the mappings you create match the type of addressing being used by the server farm. Click Next.

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

11. If you want the Citrix server to keep disconnected sessions open while the client attempts to reconnect automatically, select the Enable session reliability check box.

12. If you enabled session reliability and want to use simultaneous ticketing from two Secure Ticket Authorities (STAs), select the Request tickets from two STAs, where available check box. When this option is enabled, the Web Interface obtains tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If for any reason the Web Interface is unable to contact two STAs, it falls back to using a single STA. Click Next.

    Note: You must deploy the Access Gateway in order to use this feature. Secure Gateway does not currently support multiple redundant STAs.

13. On the Specify Secure Ticket Authority Settings page, click Add to specify the URL of an 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[s]://*servername.domain.com*/scripts/ctxsta.dll. You can specify more than one STA for fault tolerance; however, Citrix recommends that you do not use an external load balancer for this purpose. Use the Move Up and Move Down buttons to place the STAs in order of priority.

14. 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.

15. 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.

To configure default access settings

The order in which the entries appear in the User device addresses table is the order in which the rules are applied. If the user device 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 Secure Access task in the Citrix Web Interface Management console.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Secure Access.
4. On the Specify Access Methods page, select the entry labeled Default from the list and click Edit.
5. 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 Citrix client, select Direct.
   - If you want the alternate address of the XenApp server to be given to the client, 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 client to be determined by the address translation mappings in the Web Interface, select Translated.
   - If you want the actual address of the Citrix server to be given to the gateway, select Gateway direct.
   - If you want the alternate address of the XenApp server to be given to the gateway, 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 to be determined by the address translation mappings set in the Web Interface, select Gateway translated.
6. Enter the network address and subnet mask that identify the client network. Use the Move Up and Move Down buttons to place the access routes in order of priority in the User device addresses table.

7. If you are using address translation or a gateway in your deployment, click Next and specify the appropriate additional settings for your default configuration. For more information, To configure internal firewall address translation and To configure gateway settings.

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 Citrix clients must communicate with the server running XenApp or XenDesktop through the proxy server. You use the Client-Side Proxy task in the Citrix Web Interface Management console 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 Citrix Web Interface Management console, you can set default proxy rules for Citrix clients. However, you can also configure exceptions to this behavior for individual users’ 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 is controlled by the client. For example, to use the Secure Proxy feature in XenApp and XenDesktop, configure the Web Interface to use the proxy settings specified on the client and configure the client for Secure Proxy. For more information about using Citrix clients to control proxy behavior, see the documentation for the client in question.

To configure default proxy settings

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, click Client-Side Proxy.
4. Click Add to create a new mapping or select an entry from the list and click Edit to edit an existing mapping.
5. Enter the external address of the proxy and the user device subnet mask in the IP address and Subnet mask boxes, respectively.
6. From the Proxy list, choose one of the following options:
   - If you want the Citrix client to detect the Web proxy automatically based on the user's browser configuration, select User's browser setting.
   - If you want the client 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 client 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.
7. 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 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 Web Site Appearance task in the Citrix Web Interface Management console 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 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’ 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 resources should be grouped on users’ Applications screens. You can either configure separate tabs for applications, content, and desktops or you can collect all 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.
- **Content.** Define custom messages and screen text, and specify localized versions of this text for the languages that your users may use when they access the site. You can specify page titles and messages for users’ Logon and Applications screens, and common footer text to appear on all screens. In addition, you can configure a pre-logon disclaimer that users must accept before they can log on.

Managing Shortcuts to Resources

You can use the Shortcuts task in the Citrix Web Interface Management console to specify how the Citrix online plug-in displays shortcuts for resources.

You can create the following types of shortcuts:

- **Start menu.** You can use the settings specified in the Shortcuts task, the settings defined when resources are published on XenApp and XenDesktop, 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 Shortcuts task, the settings defined when resources are published on XenApp and XenDesktop, 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 and/or allow users to select a name.
- **Notification area.** You can display resources in the notification area and/or allow users to specify how resources appear.

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

Using Resource Refresh Options

Use the Resource Refresh task in the Citrix Web Interface Management console to specify when users' lists of resources are refreshed and whether or not they can customize these settings. You can enable refreshes when the Citrix online plug-in starts up or when resources are accessed, and you can specify how often the list is refreshed.

Managing Session Preferences

Use the Session Settings task in the Citrix Web Interface Management console 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 user device name in the case of clients for online resources.

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 Settings 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.
- **Persistent URLs.** Specify whether or not users can use browser bookmarks to access the site.
- **Connection performance.** Specify preset default settings or allow users 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 online sessions and allow the Web Interface to use ClearType font smoothing, providing the corresponding settings are configured for users' Windows operating systems, users' Citrix client software, and the server farm.
- **Local resources.** Configure settings for Windows key combinations, PDA synchronization, and Special Folder Redirection.
- **User device names.** Specify whether or not the Web Interface should override user device names in the case of online resources.

  Important: You must enable the Override user device names setting if you want to use workspace control with Versions 8.*x* and 9.*x* of the Clients for Windows.

For XenApp Services sites providing online resources, you can use the Session Options task in the Citrix Web Interface Management console 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, the Citrix online plug-in, 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 online resources, their actions are redirected to the folders on their local computers. For more information, see Special Folder Redirection.

- **Workspace control.** Configure reconnection and logoff behavior. For more information, see Configuring Workspace Control.

Bandwidth Control

Bandwidth control enables users to select session settings based on their connection bandwidth. These options appear on the Settings screen, before or after logon. Bandwidth control enables adjustment of color depth, audio quality, and printer mapping. Additionally, you can use the Web Interface Management Console to specify default or custom settings for users. Use the Manage Session Settings task to customize bandwidth settings using the Connection Performance options. Select Custom from the Connection speed drop-down list to activate the Color quality, Sound, and Enable printer mapping options.

If the Client for Java is used, bandwidth control determines whether or not audio and printer mapping packages are available. 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 used, 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 settings specified for the resource on the server are used.

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 introduced in Windows XP. Font smoothing is enabled by default in Windows 7 and Windows Vista, but not in Windows XP.

The Web Interface and the Citrix online plug-in support ClearType font smoothing during ICA sessions. When a user running Windows XP or later connects to the server, the plug-in 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 online plug-in, the Web Interface site, and the server farm. Use the Session Settings task in the Citrix Web Interface Management console to enable font smoothing for XenApp Web sites and the Session Options task for XenApp Services sites.

Font smoothing applies to online resources only. This feature is not available for offline applications.

Special Folder Redirection

The Special Folder Redirection feature enables users to map Windows special folders for the server to those on their local computer so that they are easier to use with online resources. The term *special folders* refers specifically to standard Windows folders, such as \Documents and \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’ online 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 online resources only. This feature is not available for offline applications.

Enabling Special Folder Redirection

Special Folder Redirection support is disabled by default for both XenApp Web and XenApp Services sites. If you enable Special Folder Redirection for a site, you must ensure that none of the existing policy rules in your server farm prevent users from accessing or saving to their local drives.

Use the Session Settings task in the Citrix Web Interface Management console to enable Special Folder Redirection for XenApp Web sites and the Session Options task for XenApp Services sites. You can also allow users to choose whether or not to enable this feature on the Settings screen.

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

Configuring Workspace Control

Use workspace control to allow users to disconnect quickly from all resources (applications, content, and desktops), reconnect to disconnected resources, and log off from all resources. This allows users to move between devices and gain access to all of their resources (disconnected only or disconnected and active) either when they log on or manually at any time. For example, clinicians in hospitals may need to move between workstations and access the same set of resources each time they log on.

Workspace Control 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, you must enable the Override user device names setting in the Session Preferences task in the Citrix Web Interface Management console.
- If the Web Interface detects that it is being accessed from within a Citrix session, the workspace control feature is disabled.
- Depending on the security settings, Internet Explorer can block the download of files that do not appear to be directly initiated by the user, so attempts to reconnect to resources using a native client 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 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 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 for XenApp Web Sites.
- If credential pass-through is not enabled for XenApp Services sites, smart card users are prompted for their PINs for each Citrix session being reconnected. This is not an issue with pass-through or pass-through with smart card authentication on XenApp Services sites because credential pass-through is enabled with these options.

Workspace Control Limitations

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

- Workspace control is not available for sites configured to deliver offline applications. If you configure a site for dual mode delivery, workspace control operates with the online resources only.
- 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 Presentation Server 4.5 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 for XenApp Web Sites

The following section is applicable to XenApp Web sites only. 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 server running the Citrix XML Service that the Web Interface contacts. The Citrix XML Service passes information about resources between the Web Interface and servers running XenApp and XenDesktop. Without the trust relationship, the Disconnect, Reconnect, and Log Off buttons are inoperative for those users logging on using 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

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 Server Farms task in the Citrix Web Interface Management console.
- Configure the 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.

1. Log on to a server in the farm and click Start > All Programs > Citrix > Management Consoles > Citrix Delivery Services Console.
2. In the left pane of the console, navigate to Citrix Resources > XenApp, expand the node for your farm, and click Policies.
3. In the details pane of the console, select the Computer tab and click New.
4. Enter a name and, optionally, a description for your new policy and click Next.

5. In the Categories list, click XML Service and, under Settings, select Trust XML requests and click Add.

6. Select Enabled and click OK. Click Next.

7. If required, apply filters to your policy to determine the circumstances under which it is applied and click Next.

8. Ensure that the Enable this policy checkbox is selected and click Save.

To enable automatic reconnection when users log on

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.

3. In the Action pane, select the appropriate task for your site type:

   - For XenApp Web sites, click Workspace Control

   - For XenApp Services sites, click Session Options and select Workspace Control
4. Select the Automatically reconnect to sessions when users log on option.

5. 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
6. Select the Allow users to customize check box to allow users to configure this setting for themselves. Users can change this setting on the Settings screen of XenApp Web sites or in the Citrix online plug-in Options dialog box.

To enable the Reconnect button

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites or XenApp Services Sites, as appropriate, and select your site in the results pane.
3. In the Action pane, select the appropriate task for your site type:
   - For XenApp Web sites, click Workspace Control
   - For XenApp Services sites, click Session Options and select Workspace Control
4. Select the Enable the Reconnect button option.
5. 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
6. Select the Allow users to customize check box to allow users to configure this setting for themselves. Users can change this setting on the Settings screen of XenApp Web sites or in the Citrix online plug-in Options dialog box for XenApp Services sites.

To configure logoff behavior

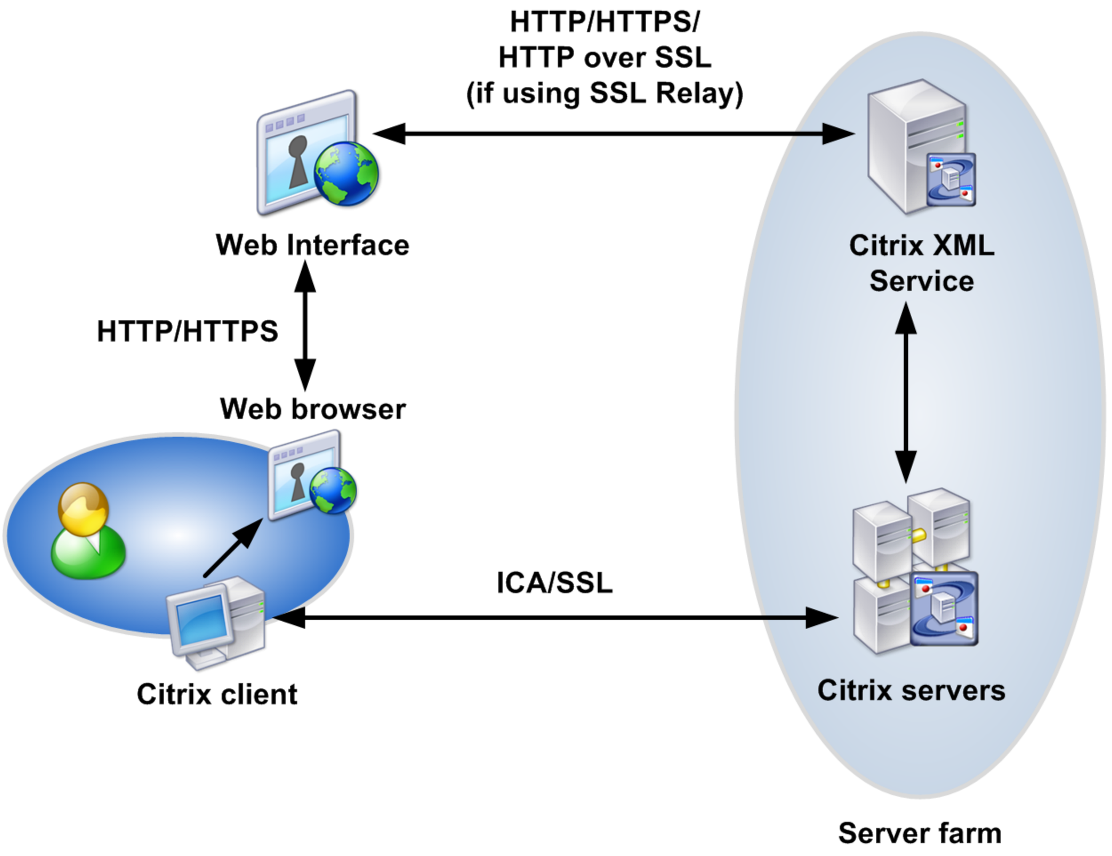
1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Workspace Control.
4. Select the Log off active sessions when users log off from the site 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.
5. Select the Allow users to customize check box to enable users to configure this setting for themselves on the Settings screen of the site.

Configuring Web Interface Security

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

- User device/Web Interface communication. Discusses issues associated with passing Web Interface data between Web browsers and servers and suggests strategies for protecting data in transit and data written on users' devices.
- Web Interface/Citrix server communication. Describes how to secure the authentication and resource information that passes between the Web Interface server and the server farm.
- User session/server communication. Considers issues associated with passing session information between Citrix clients and servers. Discusses implementations of the Web Interface and XenApp/XenDesktop security features that protect such data.

The figure shows how users' devices interact with the server running XenApp or XenDesktop and the Web Interface server.



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, visit the Microsoft Web site at http://support.microsoft.com/.

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. For more information about SSL, cryptography, and certificates, see XenApp Administration, Secure Gateway, and SSL Relay for UNIX Administration.

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 all supported versions of XenApp for Windows and XenDesktop. 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 with 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.

SSL Relay

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

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

After this authentication, the Web server and the SSL Relay negotiate an encryption method for the session. The Web server then sends all information requests in encrypted form to the SSL Relay. The SSL Relay decrypts the requests and passes them to the Citrix XML Service. When returning the information to the Web server, the Citrix XML Service sends all information through the server running the 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 SSL Relay, see XenApp Administration or SSL Relay for UNIX Administration.

ICA Encryption

Using ICA encryption, you can encrypt the information sent between a server and a Citrix client. 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.

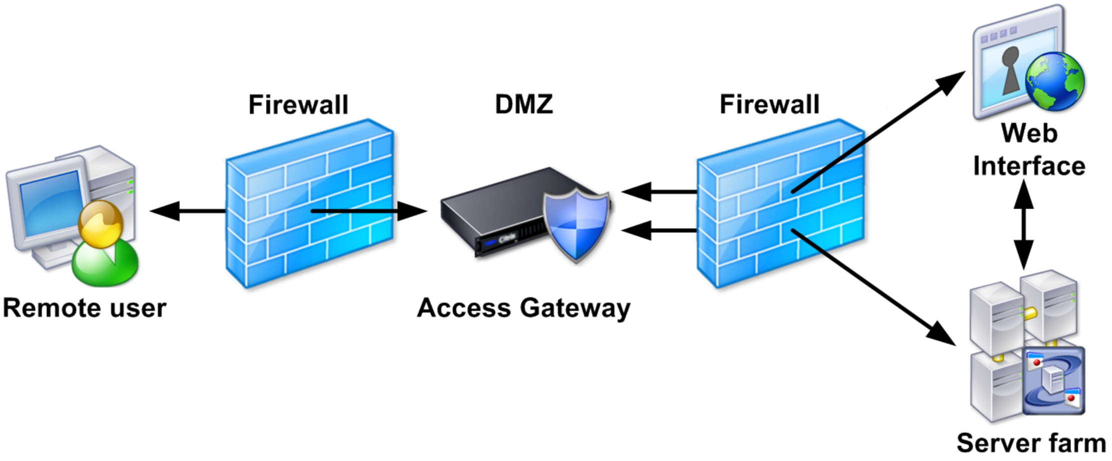
Access Gateway

You can use the Access Gateway with the Web Interface and the Secure Ticket Authority (STA) to provide authentication, authorization, and redirection to resources (applications, content, and desktops) delivered from a server running XenApp or XenDesktop.

The 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. The Access Gateway encrypts and supports all resources and protocols.

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

The figure shows how the Access Gateway secures communication between SSL/TLS-enabled Citrix clients and servers.



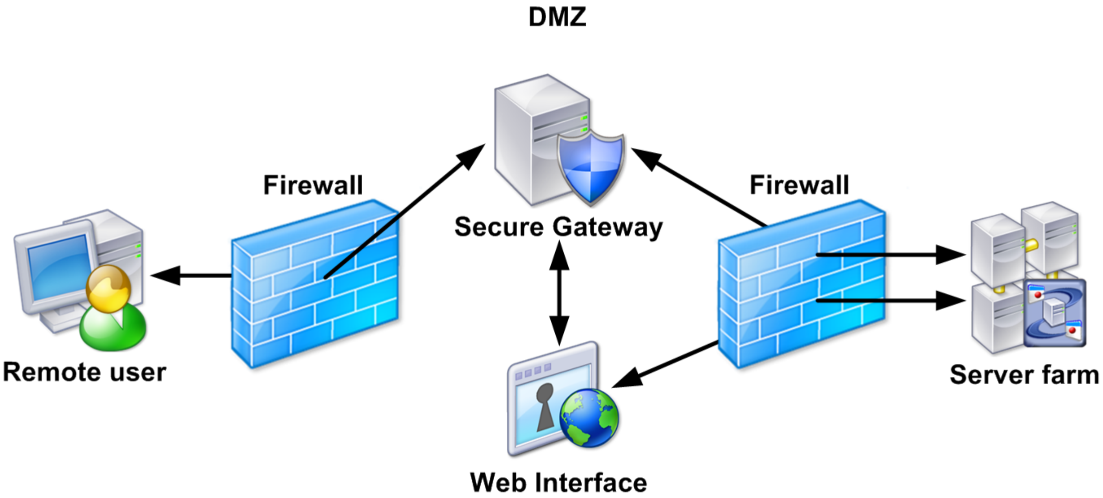
For more information about the Access Gateway, see the Access Gateway documentation. For more information about how to configure the Web Interface for Access Gateway support using the Citrix Web Interface Management console, see To configure gateway settings.

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 Citrix clients and servers, encrypting ICA traffic. The Internet portion of traffic between users' 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 Citrix clients and servers.



For more information about Secure Gateway, see Secure Gateway. For more information about how to configure the Web Interface for Secure Gateway support using the Citrix Web Interface Management console, see To configure gateway settings.

Securing Web Interface Communication

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

- Instruct users to connect to Web Interface pages using HTTPS (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 SSL Relay for encryption between the Web Interface server and the servers running XenApp and XenDesktop. Alternatively, if IIS is installed on the server running XenApp or XenDesktop, use HTTPS to secure the connection.

Securing the Citrix Online Plug-in with SSL

To use SSL to secure the communications between the Citrix online plug-in and the Web Interface server using the Citrix Web Interface Management console, click XenApp Services Sites in the left pane, select the site in the results pane, click Server Settings in the Action pane, and select the Use SSL/TLS for communication between plug-ins and the site check box.

Ensure that, for each application, the Enable SSL and TLS protocols check box is selected on the Client options page of the Application Properties dialog box in the Delivery Services Console.

User Device/Web Interface Communication

Communication between Citrix clients and the Web Interface server consists of passing several different types of data. As users identify themselves, browse their 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 user names and credentials in clear text.
- **HTML pages and session cookies.** After users enter their credentials on 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 resources available to the user.
- **ICA files.** When a user selects a resource, the Web server sends an .ica file for that resource to the Citrix client (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.

  In some cases, when a client is launched, the .ica file is saved as a plain text file on the user's hard disk. However, this does not prevent the client from launching successfully.

  The ICA File Signing feature allows users to verify that they are launching applications or desktops from a trusted Web server. For more information, see Configuring ICA File Signing

Security Issues with User Device/Web Interface Communication

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

- Attackers can intercept logon data, the session cookie, and HTML pages in transit between the Web server and 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 user's browser can retrieve the cookie and possibly use credential information.

- Although the .ica file does not contain any user credentials, it contains a onetime-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 Citrix client, 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 client captures users' credentials when they log on to their devices and forwards them to any server if the appropriate setting is contained in the .ica file.

Recommendations for Securing User Device/Web Interface Communication

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

Implement SSL/TLS-Capable Web Servers and Browsers

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

In a typical Web server to 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 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 screen. Data sent from the Web server, including credentials, session cookies, .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 more information about configuring the Web server to support SSL/TLS, see the documentation for your Web server.

Important: Many SSL/TLS-capable Web servers use TCP/IP port 443 for HTTP communications. By default, the SSL Relay uses this port as well. If your Web server is also running the SSL Relay, make sure you configure either the Web server or the 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 secure installations. Use this feature only in small, trusted environments.

Web Interface/Citrix Server Communication

Communication between the Web Interface and the server running XenApp or XenDesktop involves 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 with Web Interface/Citrix Server Communication

The Web Interface XML protocol uses 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.

Recommendations for Securing Web Interface/Citrix Server Communication

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

- Use the SSL Relay as a security intermediary between the Web Interface server and the server farm. The SSL Relay performs host authentication and data encryption.
- In deployments that do not support the SSL Relay, install the Web Interface on the server running XenApp or XenDesktop.
- 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 XenDesktop.

Use the SSL Relay

The 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 SSL Relay and verify the server's configuration. For more information about installing a server certificate and configuring the SSL Relay on servers, see XenApp Administration. You can also consult the application Help in the SSL Relay Configuration Tool. For XenApp for UNIX servers, see SSL Relay for UNIX Administration.

When configuring the SSL Relay, make sure the server running the SSL Relay permits passing SSL traffic to the servers you are using as the Citrix XML Service contacts. By default, the SSL Relay forwards traffic only to the server on which it is installed. You can, however, configure the SSL Relay to forward traffic to other servers. If the 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 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 SSL Relay using the Citrix Web Interface Management console or the WebInterface.conf file. For more information about using the console to configure the Web Interface to use the SSL Relay, see Configuring Settings for All Servers in a Farm.

To configure the Web Interface to use 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 SSL Relay on the server.

3. Change the value of the Transport setting in the **Farm<*n*>** parameter to SSL.

To add a new root certificate 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.

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 more information about certificates, see XenApp Administration. For XenApp for UNIX servers, see SSL Relay for UNIX Administration.

Enable the Web Interface on the Server Running XenApp or XenDesktop

For those deployments that do not support the 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 on the local host, thereby eliminating transmission of 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.

As a first step, you can place both the Web server and the server running XenApp or XenDesktop behind a firewall so that the communication between the two is not exposed to open Internet conditions. In this scenario, users' devices must be able to communicate through the firewall to both the Web server and the server running XenApp or XenDesktop. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for user device to Web server communication. For client-to-server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598. For more information about using ICA with network firewalls, see the documentation for your Web server. For more information about using the Web Interface with network address translation, see the Web Interface SDK.

Note: On systems running XenApp, Setup enables you to force the Citrix XML Service to share Internet Information Services' TCP/IP port instead of using a dedicated port. With XenDesktop, 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.

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 XenDesktop. HTTPS uses SSL/TLS to provide strong data encryption.

The Web server makes an HTTPS connection to IIS on the server running XenApp or XenDesktop. This requires IIS port sharing on the server running XenApp or XenDesktop, and for IIS 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 more information about how to configure the Web Interface to use the HTTPS protocol using the Citrix Web Interface Management console, see Managing Secure Access.

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.

User Session/Server Communication

Web Interface communication between users' 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 Citrix client 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 Citrix client and server through a number of virtual channels; for example, mouse input (from client to server) and graphical updates (from server to client).

Security Issues with User Session/Server Communication

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

- Intercept initialization request information sent from the Citrix client, including user credentials

- Intercept session information, including text and mouse clicks entered by users and screen updates sent from the server

Recommendations for Securing User Session/Server Communication

Citrix recommends securing the data sent between users' devices and servers either by encrypting the traffic or by deploying the Access Gateway.

Use SSL/TLS or ICA Encryption

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

Support for SSL is included in all supported versions of XenApp and XenDesktop. Support for SSL/TLS and ICA encryption is included in all supported versions of XenApp for Windows and XenDesktop. For a list of Citrix clients that support each method, see the documentation for the clients or the Citrix download site. For more information about ICA encryption, see XenApp Administration.

Use the Access Gateway

You can use the Access Gateway to secure the traffic between your Citrix clients and servers over the Internet. The Access Gateway is a universal SSL VPN appliance that provides a single, secure point of access to all resources. For more information about the Access Gateway, see the Access Gateway documentation. For more information about how to configure the Web Interface for Access Gateway support using the Citrix Web Interface Management console, see To configure gateway settings.

Controlling Diagnostic Logging

Use the Diagnostic Logging task under Site Maintenance in the Citrix Web Interface Management console 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 errors.

Configuring Sites Using the Configuration File

Site Configuration Files

Web Interface 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 settings for a site. For example, you can specify the settings that users can change and you can configure authentication to the Web Interface.

If you enter an invalid value for a setting when you edit a configuration file and then subsequently use the Citrix Web Interface Management console, the console replaces the invalid value with the default value when the file is saved.

If the Citrix Web Interface Management console is running when you edit a site configuration file manually, any subsequent changes you make using the console will cause all your configuration file edits to be overwritten. Citrix recommends that you close the Citrix Web Interface Management console before editing the site configuration files. If this is not possible, refresh the console to commit your manual configuration file edits before making any further changes using the console.

The WebInterface.conf file is available 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 configuration 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 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.

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.

AccountSelfServiceUrl

- Description: Specifies the URL for the Password Manager Service.
- Value: Valid URL using HTTPS
- Site type: XenApp Web

AdditionalExplicitAuthentication

- Description: Specifies the explicit two-factor authentication that must be carried out, in addition to SAM, ADS, or NDS.
- Value: None | SecurID | SafeWord | RADIUS
- Site type: XenApp Web

AddressResolutionType

- Description: Specifies the type of address to use in the .ica launch file.
- Value: dns-port | dns | ipv4-port | ipv4
- Site type: XenApp Web and XenApp Services

AGAuthenticationMethod

- Description: Specifies the permitted authentication methods for Access Gateway integrated sites. This parameter must be set to Explicit if users log on to the Access Gateway with a user name and password. If users log on to the Access Gateway with a smart card, setting this parameter to SmartCard indicates that users are required to enter a PIN each time they access a resource. The SmartCardKerberos option enables users logging on to the Access Gateway with a smart card to access their resources without providing a PIN.
- Value: Explicit | SmartCard | SmartCard Kerberos
- Site type: XenApp Web

AGEPromptPassword

- Description: Specifies whether or not users are prompted to reenter their passwords when logging on from the Access Gateway logon page.
- Value: Off | On

- Site type: XenApp Web

AGEWebServiceURL

- Description: Specifies the URL for the Access Gateway authentication service.
- Value: Valid URL
- Site type: XenApp Web

AllowBandwidthSelection

- Description: Specifies whether or not users can indicate the speed of their network connection so that ICA settings can be optimized.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeAudio

- Description: Specifies whether or not users are permitted to adjust the audio quality for ICA sessions.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeAutoLogin

- Description: Specifies whether or not users are permitted to enable and disable automatic logon.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizeClientPrinterMapping

- Description: Specifies whether or not users are permitted to enable and disable client printer mapping.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeJavaClientPackages

- Description: Specifies whether or not users are permitted to choose which Client for Java packages they want to use.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeLayout

- Description: Specifies whether or not users are permitted to choose whether to use the low graphics or full graphics user interface.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeLogoff

- Description: Specifies whether or not users are permitted to override the behavior of the workspace control feature when they log off from the server.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizePersistFolderLocation

- Description: Specifies whether or not users are permitted to enable and disable the feature that returns them to the last folder they visited on the Applications screen when they log on again.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeReconnectAtLogin

- Description: Specifies whether or not users are permitted to override the behavior of the workspace control feature at logon.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizeReconnectButton

- Description: Specifies whether or not users are permitted to override the behavior of the workspace control feature when the Reconnect button is clicked.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizeSettings

- Description: 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.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizeShowHints

- Description: Specifies whether or not users are permitted to show and hide hints on the Applications screen.
- Value: On | Off
- Site type: XenApp Web

AllowCustomizeShowSearch

- Description: Specifies whether or not users are permitted to enable and disable searching on the Applications screen.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeSpecialFolderRedirection

- Description: Specifies whether or not users are permitted to enable and disable the Special Folder Redirection feature.
- Value Off | On
- Site types XenApp Web

AllowCustomizeTransparentKeyPassthrough

- Description: Specifies whether or not users are permitted to select the key combination pass-through behavior.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeVirtualCOMPortEmulation

- Description: Specifies whether or not users are permitted to enable and disable PDA synchronization.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeWinColor

- Description: Specifies whether or not users are permitted to change the color depth for ICA sessions.
- Value: Off | On
- Site type: XenApp Web

AllowCustomizeWinSize

- Description: Specifies whether or not users are permitted to change the window size for ICA sessions.

- Value: On | Off
- Site type: XenApp Web

AllowDisplayInFrames

- Description: Specifies whether or not XenApp Web sites are permitted to be displayed within frames embedded in third-party Web pages.
- Value: On | Off
- Site type: XenApp Web

AllowFontSmoothing

- Description: Specifies whether or not font smoothing is permitted for ICA sessions.
- Value: On | Off
- Site type: XenApp Web and XenApp Services

AllowUserAccountUnlock

- Description: Specifies whether or not users are permitted to unlock their accounts using account self-service.
- Value: Off | On
- Site type: XenApp Web

AllowUserPasswordChange

- Description: Specifies the conditions under which users can change their passwords.
- Value: Never | Expired-Only | Always (XenApp Web sites only)
- Site type: XenApp Web and XenApp Services

AllowUserPasswordReset

- Description: Specifies whether or not users are permitted to reset their passwords using account self-service.
- Value: Off | On
- Site type: XenApp Web

AlternateAddress

- Description: Specifies whether or not to return the alternate server address in the .ica file.
- Value: Off | Mapped | On
- Site type: XenApp Web and XenApp Services

ApplicanceEmbeddedSmartCardSSO

- Description: Specifies whether or not smart card authentication uses the embedded ActiveX control for single sign-on.
- Value: Off | On
- Site type: Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- Description: The number of seconds that the embedded smart card authentication PIN entry screen waits before returning to the login screen when inactive.
- Value: 20
- Site type: Desktop Appliance Connector

ApplianceMultiDesktop

- Description: Specifies whether or not the list of desktops is displayed if users have multiple desktops assigned to them.
- Value: Off | On
- Site type: Desktop Appliance Connector

ApplicationAccessMethods

- Description: Specifies whether users can access applications using a client for online resources, the Citrix offline plug-in, or both.
- Value: Remote, Streaming
- Site type: XenApp Web and XenApp Services

AppSysMessage_<*Language Code*>

- Description: Specifies localized text to appear at the bottom of the main content area of the Applications screen. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.
- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks
- Site type: XenApp Web

AppTab<*n*>

- Description: 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 resources available to the user can be defined using the AllResources value.
- Value: Applications | Desktops | Content | AllResources
- Site type: XenApp Web

AppWelcome Message_<*Language Code*>

- Description: Specifies localized text to appear at the top of the main content area of the Applications screen. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.

- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks

- Site type: XenApp Web

AuthenticationPoint

- Description: Specifies where user authentication takes place.

- Value: WebInterface | ADFS | AccessGateway | 3rdParty | WebServer

- Site type: XenApp Web

AutoLaunchDesktop

- Description: Specifies whether or not automatic access to desktops is enabled. When this parameter is set to On, the Web Interface will automatically start the user's desktop if it is the only resource available to them from all farms.

- Value: Off | On

- Site type: XenApp Web

AutoLoginDefault

- Description: Specifies whether or not automatic logons are enabled by default for users accessing their resources using pass-through, pass-through with smart card, and smart card authentication.

- Value: On | Off

- Site type: XenApp Web

BrandingColor

- Description: Specifies the color for the header and footer areas.

- Value: Hex color number or color name

- Site type: XenApp Web

BrandingImage

- Description: Specifies the URL for the branding gradient image for the header and footer areas.

- Value: Valid URL

- Site type: XenApp Web

BypassFailedRadiusServerDuration

- Description: Specifies the time before a failed RADIUS server is considered for reuse.
- Value: Time in minutes (60)
- Site type: XenApp Web

BypassFailedSTADuration

- Description: Specifies the time before a failed server running the Secure Ticket Authority for a gateway device is considered for reuse.
- Value: Time in minutes (60)
- Site type: XenApp Web

ClientAddressMap

- Description: Specifies client 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 client address or subnet indicates the default for all otherwise unspecified Citrix clients.
- Value: <*Subnet Address*>/ <*SubnetMask*> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …
- Site type: XenApp Web

ClientDefaultURL

- Description: Specifies the URL to which the client detection and deployment process redirects users when the appropriate client is not available for download.
- Value: http://www. citrix.com/ download. Valid URL.
- Site type: XenApp Web

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- Description: Configures the client detection and deployment process for the specified platform. If the appropriate parameter has not been configured, users are redirected to the Web page specified by the ClientDefaultURL parameter. By default, these parameters are configured for the native clients supplied on the XenApp 6.0 installation media.

The first two fields specify the location and file name of the client installer. If the file is not found, users are redirected to the Web page specified by the ClientDefaultURL parameter.

The Mui field specifies whether or not the client specified by the Directory and Filename fields supports multiple languages. If this is set to No, the client detection and deployment process checks the <*LanguageCode*>\<*FolderName*> folder for the specified file.

The Version field gives the comma-separated version number of the client specified by the Directory and Filename fields. If no version number is specified, the client detection and deployment process attempts to determine the version from the specified file.

The ShowEULA field specifies whether or not users need to accept the Citrix license agreement in order to install the specified client.

The ClassID field specifies the class ID for clients for Windows and is a required setting for these clients.

The Url field specifies the Web page that users are redirected to when they click the Download button and a client file has not been specified using the Directory and Filename fields. This setting should only be used when a client file is not available.

The Description field specifies a custom message to be displayed above the Download button. Note that this text is not localized.

- Value: Directory: <*FolderName*>, Filename: <*FileName*>, [Mui:Yes | No,] [Version: <*Version Number*>,] [ShowEULA: Yes | No,] [ClassID: <*Value*>,] [Url: <*ValidURL*>,] [Description: <*Caption*>]
- Site type: XenApp Web

ClientProxy

- Description: Specifies client subnet addresses and masks and associated proxy settings for a client-side firewall. The client 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 Citrix clients. 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 (-).
- Value: <*Subnet Address*>/ <*SubnetMask*> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <*Proxy Address*> | <*ProxyAddress*>: <*ProxyPort*>, …
- Site type: XenApp Web and XenApp Services

CompactHeaderImage

- Description: Specifies the URL for the header image for the low graphics version of the user interface.
- Value: Valid URL

- Site type: XenApp Web

CompactViewStyles

- Description: Specifies the view styles available to users on the Applications screen of the low graphics user interface.
- Value: Icons, List
- Site type: XenApp Web

CredentialFormat

- Description: Specifies the credential formats accepted for explicit Windows and NIS logons.
- Value: All | UPN | DomainUsername
- Site type: XenApp Web and XenApp Services

CSG_EnableSessionReliability

- Description: Specifies whether or not to use session reliability with the Access Gateway or Secure Gateway.
- Value: On | Off
- Site type: XenApp Web and XenApp Services

CSG_Server

- Description: Specifies the address of the Access Gateway appliance or the Secure Gateway server.
- Value: None. Server address as an FQDN
- Site type: XenApp Web and XenApp Services

CSG_ServerPort

- Description: Specifies the port for the Access Gateway appliance or the Secure Gateway server.
- Value: None. Server port
- Site type: XenApp Web and XenApp Services

CSG_STA_URL<*n*>

- Description: Specifies the URL of the server running the Secure Ticket Authority for a gateway device.
- Value: None. URL of an STA
- Site type: XenApp Web and XenApp Services

CSG_UseTwoTickets

- Description: Specifies whether or not the Web Interface requests tickets from two separate Secure Ticket Authorities when a resource is accessed through the Access Gateway.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

DefaultAudioQuality

- Description: Specifies the default audio quality to use with ICA connections.
- Value: NoPreference | High | Medium | Low | Off
- Site type: XenApp Web

DefaultBandwidthProfile

- Description: Specifies the default bandwidth profile (that is, collection of bandwidth-related settings such as audio quality and color depth) to use with ICA connections.
- Value: Custom | High | Medium High | Medium | low
- Site type: XenApp Web

DefaultColorDepth

- Description: Specifies the default color depth to use with ICA connections.
- Value: NoPreference | TrueColor | HighNoPreferenceColor
- Site type: XenApp Web

DefaultCompactViewStyle

- Description: Specifies the default view style on the Applications screen of the low graphics user interface.
- Value: List | Icons
- Site type: XenApp Web

DefaultCustomTextLocale

- Description: Specifies the default locale to use for customized text. The same locale must be specified in any customized text parameters (*_<*LanguageCode*>) that are defined.
- Value: None. en | de | es | fr | ja | any other supported language identifier
- Site type: XenApp Web

DefaultPrinterMapping

- Description: Specifies whether or not printer mapping is enabled by default for ICA connections.
- Value: On | Off
- Site type: XenApp Web

DefaultViewStyle

- Description: Specifies the default view style on the Applications screen of the full graphics user interface.
- Value: Icons | Details | Groups | List | Tree
- Site type: XenApp Web

DefaultWindowSize

- Description: Specifies the default window mode to use for ICA sessions. This can be specified as a percentage of the total screen area using the format X% or fixed size custom dimensions using the format XxY
- Value: FullScreen | Seamless | X% | XxY
- Site type: XenApp Web

DisplayBrandingImage

- Description: Specifies whether or not to display the branding gradient image for the header and footer areas.
- Value: On | Off
- Site type: XenApp Web

DomainSelection

- Description: Specifies the domain names listed on the Logon screen for explicit authentication.
- Value: List of NetBIOS domain names
- Site type: XenApp Web and XenApp Services

DuplicateLogInterval

- Description: Specifies the time period over which DuplicateLogLimit log entries are monitored.
- Value: Time in seconds (60)
- Site type: XenApp Web and XenApp Services

DuplicateLogLimit

- Description: Specifies the number of duplicate log entries permitted in the time period given by DuplicateLogInterval.
- Value: Integer greater than 0 (10)
- Site type: XenApp Web and XenApp Services

EnableFileTypeAssociation

- Description: 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.
- Value: On | Off
- Site type: XenApp Web and XenApp Services

EnableKerberosToMPS

- Description: Specifies whether or not Kerberos authentication is enabled.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

EnableLegacyICAClientSupport

- Description: Specifies whether or not older Citrix clients 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.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

EnableLogoffApplications

- Description: Specifies whether or not the workspace control feature logs off active resources when users log off from the server.
- Value: On | Off
- Site type: XenApp Web

EnablePassthroughURLs

- Description: Specifies whether or not users are permitted to create persistent links to resources accessed using the Web Interface.
- Value: Off | On
- Site type: XenApp Web

EnableRadiusServerLoadBalancing

- Description: Specifies whether or not sessions are load balanced among the configured RADIUS servers. Failover between the servers still occurs regardless of the setting for this parameter.

- Value: Off | On
- Site type: XenApp Web

EnableSTALoadBalancing

- Description: Specifies whether or not requests are load balanced among the configured Secure Ticket Authority servers for a gateway device.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

EnableVirtualCOMPortEmulation

- Description: Specifies whether or not to enable PDA synchronization through tethered USB connections.
- Value: Off | On
- Site type: XenApp Web

EnableWizardAutoMode

- Description: Specifies whether or not the client detection and deployment process runs in auto mode.
- Value: On | Off
- Site type: XenApp Web

EnableWorkspaceControl

- Description: Specifies whether or not the workspace control feature is available to users.
- Value: On | Off
- Site type: XenApp Web

ErrorCallbackURL

- Description: Specifies a URL for the Web Interface to redirect to when an error occurs. The Web page that the URL refers to must accept and process four query string parameters:

  CTX_MessageType

  CTX_MessageKey

  CTX_MessageArgs

  CTX_LogEventID

- Value: Valid URL
- Site type: XenApp Web

Farm<*n*>

- Description: Specifies all the information for a farm. A maximum of 512 farms can be configured.
- Value: Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Name*>] [,XMLPort: <*Port*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Port*>] [,Bypass Duration: <*TimeInMinutes* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*TimeInSeconds* (200)>] [,RADETicket TimeToLive: <*TimeInSeconds* (200)>]
- Site type: XenApp Web and XenApp Services

Farm<*n*>Groups

- Description: Specifies the Active Directory groups that are permitted to enumerate resources from server farms. Including a setting for this parameter activates the user roaming feature. A maximum of 512 user groups can be specified for each farm defined with the Farm<*n*> parameter.
- Value: None. *Domain*\ *UserGroup*[,...]
- Site type: XenApp Web, XenApp Services, and XenDesktop

FooterText _<*Language Code*>

- Description: Specifies localized footer text to appear in the footer area of all pages. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.
- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks
- Site type: XenApp Web

HeaderFontColor

- Description: Specifies the font color in the header area.
- Value: Hex color number or color name
- Site type: XenApp Web

HeadingHomePage

- Description: Specifies the URL for the image to appear as the heading of the home page.
- Value: Valid URL
- Site type: XenApp Web

HeadingImage

- Description: Specifies the URL for the image to appear as the heading of the Web Interface.
- Value: Valid URL
- Site type: XenApp Web

HideDomainField

- Description: Specifies whether or not the Domain field appears on the Logon screen.
- Value: Off | On
- Site type: XenApp Web

IcaFileSigningCertificateThumbprint

- Description: The thumbprint of the certificate to use for ICA File Signing.
- Value: None. Thumbprint that may or may or not contain spaces
- Site type: XenApp Web and Desktop Appliance Connector

IcaFileSigningEnabled

- Description: Enables and disables the ICA File Signing feature.
- Value: Off | On
- Site type: XenApp Web and Desktop Appliance Connector

IcaFileSigningHashAlgorithm

- Description: The hash algorithm to use for ICA file signing.
- Value: SHA1 | SHA256
- Site type: XenApp Web and Desktop Appliance Connector

IgnoreClientProvidedClientAddress

- Description: Specifies whether or not to ignore the address provided by the Citrix client.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

InternalServerAddressMap

- Description: Specifies normal/translated address pairings. The normal address identifies the server with which the gateway communicates and the translated address is returned to the Citrix client.
- Value: NormalAddress = Translated Address, …

- Site type: XenApp Web and XenApp Services

JavaClientPackages

- Description: Specifies the default set of Client for Java packages made available to users.
- Value: ClipBoard, ConfigUI, PrinterMapping, SecureICA, SSL, Audio, ClientDriveMapping, ZeroLatency
- Site type: XenApp Web

JavaFallbackMode

- Description: Specifies whether to fall back to the Client for Java when users do not have a native client installed. This parameter only applies when the Ica-Local value is included for the LaunchClients parameter. The Manual setting allows users to choose whether or not to attempt to use the Client for Java.
- Value: None | Manual | Auto
- Site type: XenApp Web

KioskMode

- Description: 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.
- Value: Off | On
- Site type: XenApp Web

LaunchClients

- Description: Specifies the Citrix clients from which users are permitted to select. This parameter is ignored for dual mode sites, for which the setting is always Ica-Local. Omitting the Ica-Java setting does not prevent users from being offered the Client for Java. To do this, you also need to set the JavaFallbackMode parameter to None.
- Value: Ica-Local, Ica-Java, Rdp-Embedded
- Site type: XenApp Web

LoginDomains

- Description: Specifies the domain names used for access restriction.
- Value: List of NetBIOS domain names
- Site type: XenApp Web and XenApp Services

LoginSys Message_<*Language Code* >

- Description: Specifies localized text to appear at the bottom of the main content area of the Logon screen. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.

- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks
- Site type: XenApp Web

LoginTitle_<*Language Code* >

- Description: Specifies localized text to appear above the welcome message on the Logon screen. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.
- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks
- Site type: XenApp Web

LoginType

- Description: Specifies the type of Logon screen that is presented to users. The Logon screen can be either domain-based or NDS-based.
- Value: Default | NDS
- Site type: XenApp Web and XenApp Services

LogoffFederationService

- Description: 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.
- Value: On | Off
- Site type: XenApp Web

MultiFarmAuthenticationMode

- Description: This mode has three options for specifying the permitted authentication method. The “All” option is the default setting in which all farms are authenticated to enumerate any application. The “Any” option allows enumeration of applications from any farm to the authenticated user; however, if the user incorrectly enters their credentials, the incorrect credentials are presented to each farm for authentication regardless of failure to authenticate in any one of the farms. This can also lock the account. The “Primary” option allows the user to authenticate against the primary farm (the first farm in the list of farms configured for Web Interface) before it falls back to the “Any” mode; this option helps prevent accounts from being locked.
- Value: All | Any | Primary
- Site type: XenApp Web

MultiLaunchTimeout

- Description: Specifies the time for which resource icons are inactive following the initial click by the user to start the resource.

- Value: Time in seconds (2)
- Site type: XenApp Web

NDSContextLookupLoadbalancing

- Description: Specifies whether or not NDS requests are load balanced among the configured LDAP servers. Failover between the servers still occurs regardless of the setting for this parameter.
- Value: Off | On
- Site type: XenApp Web

NDSContextLookupServers

- Description: 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.
- Value: None. ldap://[:] | ldaps://[:],
- Site type: XenApp Web

NDSTreeName

- Description: Specifies the NDS tree to use when using NDS authentication.
- Value: None. NDS tree name
- Site type: XenApp Web and XenApp Services

OverlayAutologonCredsWithTicket

- Description: 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.
- Value: On | Off
- Site type: XenApp Web

OverrideIcaClientname

- Description: Specifies whether or not a Web Interface-generated ID must be passed in the clientname entry of an .ica launch file.
- Value: Off | On
- Site type: XenApp Web

PasswordExpiryWarningPeriod

- Description: Specifies the number of days before password expiration when users are prompted to change their passwords.

- Value: Integer between 0 and 999 (14)

- Site type: XenApp Web

PersistFolderLocation

- Description: Specifies whether or not users are returned to the last folder they visited on the Applications screen when they log on again.

- Value: Off | On

- Site type: XenApp Web

PNAChangePasswordMethod

- Description: Specifies how the Citrix online plug-in deals with change password requests from users. If this parameter is set to Direct-Only, the plug-in changes the password by communicating directly with the domain controller. Direct-With-Fallback indicates that the plug-in initially tries to contact the domain controller, but uses the XenApp Services site if this fails. The Proxy option indicates that the plug-in changes passwords by contacting the XenApp Services site.

- Value: Direct-Only | Direct-With- Fallback | Proxy

- Site type: XenApp Services

PooledSockets

- Description: Specifies whether or not to use socket pooling.

- Value: On | Off

- Site type: XenApp Web and XenApp Services

PreLoginMessageButton_<*Language Code*>

- Description: Specifies a localized name for the pre-logon message confirmation button. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.

- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks

- Site type: XenApp Web

PreLoginMessageText_<*Language Code*>

- Description: Specifies localized text to appear on the pre-logon message page. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.

- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks

- Site type: XenApp Web

PreLoginMessageTitle_<*Language Code*>

- Description: Specifies a localized title for the pre-logon message page. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.
- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks
- Site type: XenApp Web

RADERequestValidation

- Description: Specifies whether or not to perform text validation against incoming requests from the Citrix offline plug-in.
- Value:
- Site type: XenApp Web and XenApp Services

RADESessionURL

- Description: Specifies the URL for the RADE session page. If this parameter is set to auto, the URL is generated automatically.
- Value: Auto. Valid URL
- Site type: XenApp Web and XenApp Services

RadiusRequestTimeout

- Description: Specifies the time-out value to use when waiting for a response from the session's RADIUS server.
- Value: Time in seconds (30)
- Site type: XenApp Web

RadiusServers

- Description: 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 servers can be configured.
- Value: *Server* [:*Port*] [,...]
- Site type: XenApp Web

ReconnectAtLogin

- Description: Specifies whether or not workspace control should reconnect to resources when users log on, and if so, whether to reconnect all resources or disconnected resources only.
- Value: Disconnected AndActive | Disconnected | None
- Site type: XenApp Web

ReconnectButton

- Description: Specifies whether or not workspace control should reconnect to applications when users click the Reconnect button, and if so, whether to reconnect to all resources or disconnected resources only.
- Value: Disconnected AndActive | Disconnected | None
- Site type: XenApp Web

RecoveryFarm<*n*>

- Description: Specifies all the information for a disaster recovery farm. A maximum of 512 farms can be configured.
- Value: Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Name*>] [,XMLPort: <*Port*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Port*>] [,Bypass Duration: <*TimeInMinutes* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*TimeInSeconds* (200)>] [,RADETicket TimeToLive: <*TimeInSeconds* (200)>]
- Site type: XenApp Web, XenApp Services, and XenDesktop

RequestedHighColorIcons

- Description: Specifies whether or not high color depth 32-bit icons are requested from the Citrix XML Service and, if so, lists the icon sizes in pixels. If this parameter is set to None, only the standard 4-bit 32 x 32 icons are requested. The default setting varies according to the site type and its configuration.
- Value: 16, 32, 48 | None

  For XenApp Services sites, the default setting is to request all icons. For XenApp Web sites, only the 16 x 16 and 32 x 32 sizes are requested by default.
- Site type: XenApp Web and XenApp Services

RequestICAClientSecureChannel

- Description: Specifies TLS settings.
- Value: Detect-Any Ciphers, TLS- GovCiphers, SSL-AnyCiphers
- Site type: XenApp Web and XenApp Services

RequireLaunchReference

- Description: Specifies whether or not the use of launch references is enforced. Launch references are required for pass-through authentication to XenApp VM hosted apps. If compatibility with XenApp 4.0, with Feature Pack 1, for UNIX is required, this parameter must be set to Off.
- Value: On | Off
- Site type: XenApp Web and XenApp Services

RestrictDomains

- Description: Specifies whether or not the LoginDomains parameter is used to restrict user access.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

SearchContextList

- Description: Specifies context names for use with NDS authentication.
- Value: None. Comma- separated list of context names
- Site type: XenApp Web and XenApp Services

ServerAddressMap

- Description: Specifies normal/translated address pairings for the server-side firewall configuration. The normal address identifies the server and the translated address is returned to the Citrix client.
- Value: NormalAddress, Translated Address, …
- Site type: XenApp Web and XenApp Services

ServerCommunicationAttempts

- Description: Specifies the number of times a request to the Citrix XML Service is attempted before the service is deemed to have failed.
- Value: Integer greater than 0 (2)
- Site type: XenApp Web and XenApp Services

ShowClientInstallCaption

- Description: Specifies how and when installation captions appear. Setting this parameter to Auto causes installation captions to be shown if users do not have a Citrix client installed or if a better client is available. If the parameter is set to Quiet, installation captions are shown only if users do not have a client. The behavior of the Logon screen is slightly different in that captions are shown only for clients for online resources and only if no client is detected. Hence, there is no difference between the Auto and Quiet settings for the Logon screen.
- Value: Auto | Quiet | Off
- Site type: XenApp Web

ShowDesktopViewer

- Description: Specifies whether or not the Citrix Desktop Viewer window and toolbar are enabled by default when users access their desktops.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

ShowHints

- Description: Specifies whether or not hints appear on the Applications screen.
- Value: On | Off
- Site type: XenApp Web

ShowPasswordExpiryWarning

- Description: Specifies the conditions in which a user is presented with a password expiration warning.
- Value: Never | WindowsPolicy | Custom
- Site type: XenApp Web

ShowRefresh

- Description: Specifies whether or not the Refresh button is available for users on the Applications screen.
- Value: Off | On
- Site type: XenApp Web

ShowSearch

- Description: Specifies whether or not the Search control is available for users on the Applications screen.
- Value: On | Off
- Site type: XenApp Web

SpecialFolderRedirection

- Description: Specifies whether or not the Special Folder Redirection feature is enabled. If this parameter is set to On, 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 applications will be those on the server.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

SuppressDuplicateResources

- Description: Specifies whether or not the existance of resources with identical names and folder locations published on different farms is hidden from users.
- Value: Off | On
- Site type: XenApp Web and XenApp Services

Timeout

- Description: Specifies the time-out value to use when communicating with the Citrix XML Service.
- Value: Time in seconds (60)
- Site type: XenApp Web and XenApp Services

TransparentKeyPassthrough

- Description: Specifies the mode of Windows key combinations pass-through.
- Value: FullScreen Only | Local | Remote
- Site type: XenApp Web and XenApp Services

TwoFactorPasswordIntegration

- Description: Specifies whether or not to enable password integration with RSA SecurID 6.0.
- Value: Off | On
- Site type: XenApp Web

TwoFactorUseFullyQualifiedUserNames

- Description: Specifies whether or not to pass fully qualified user names to the authentication server during two-factor authentication.
- Value: Off | On
- Site type: XenApp Web

UpgradeClientsAtLogin

- Description: Specifies whether or not the client detection and deployment process runs automatically when users log on if a more recent version of the appropriate native client or the Citrix offline plug-in is available. This parameter only applies when EnableWizardAutoMode is set to On.
- Value: Off | On
- Site type: XenApp Web

UPNSuffixes

- Description: Specifies suffixes to which UPN authentication is restricted for explicit authentication.
- Value: List of UPN suffixes
- Site type: XenApp Web and XenApp Services

UserInterfaceBranding

- Description: Specifies whether the site is focused towards users accessing applications or desktops. Setting the parameter to Desktops changes the functionality of the site to improve the experience for XenDesktop users. Citrix recommends using this setting for any deployment that includes XenDesktop.

- Value: Applications | Desktops

- Site type: XenApp Web

UserInterfaceLayout

- Description: Specifies whether or not to use the compact user interface.

- Value: Auto | Normal | Compact

- Site type: XenApp Web

UserInterfaceMode

- Description: 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.

- Value: Simple | Advanced

- Site type: XenApp Web

ViewStyles

- Description: Specifies the view styles available to users on the Applications screen of the full graphics user interface.

- Value: Details | Groups | Icons | List | Tree

- Site type: XenApp Web

WebSessionTimeout

- Description: Specifies the time-out value for idle Web browser sessions.

- Value: Time in minutes (20)

- Site type: XenApp Web

Welcome Message_*<Language Code>*

- Description: Specifies localized welcome message text to appear in the welcome area of the Logon screen. *LanguageCode* is en, de, es, fr, ja, or any other supported language identifier.

- Value: None. Plain text plus any number of new line HTML <br> tags and hyperlinks

- Site type: XenApp Web

WIAuthenticationMethods

- Description: Specifies the permitted authentication methods for sites not integrated with the Access Gateway. This is a comma separated list and may contain any of the specified values in any order.
- Value: Any combination of: Explicit, Anonymous, Certificate SingleSignOn, Certificate, SingleSignOn
- Site type: XenApp Web, XenApp Services, and Desktop Appliance Connector

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 resources: in the Start menu, on the physical Windows desktop, or in the notification area. There is an additional parameter to specify a particular folder in the Start menu. These parameters correspond to the controls on the Application Display page of the Citrix online plug-in 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 plug-in to use in the future. This facilitates moving users to a different Web Interface server.
- Request. Specifies from where the plug-in should request 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 the circumstances under which Citrix online plug-in 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 online plug-in user 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 the Citrix online plug-in.
- ICA_Options. Defines the display and sound options for plug-in connections. This corresponds to the settings on the Session Options page of the Citrix online plug-in Options dialog box.
- AppAccess. Specifies the types of resources available to users.

For more information about using the config.xml file, see Online Plug-in for Windows.

Citrix Online Plug-in Considerations

Specific WebInterface.conf parameter settings affect the validation of Citrix online plug-in requests. Citrix recommends that the settings in WebInterface.conf be consistent with the settings in the config.xml file for the Citrix online plug-in.

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 the Citrix online plug-in and their recommended settings.

Parameter	Recommended setting
LoginType	If set to NDS, then Novell authentication must also be enabled in config.xml.
NDSTreeName	DefaultTree in the Logon section of config.xml must contain the same setting.
PNAChangePasswordMethod	Method in the ChangePassword section of config.xml must contain the same setting.
WIAuthenticationMethods	Use the same authentication method configured in the WebInterface.conf file. Authentication fails if this method differs in config.xml.

To configure the Web Interface when using the Citrix online plug-in

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

For more information about WebInterface.conf file settings, see WebInterface.conf Parameters.

Settings in the bootstrap.conf File

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

Parameter	Description	Values	Site types
ConfigurationLocation	Specifies the file from which the Web Interface site should obtain its configuration. This can be a local file or, for sites hosted on IIS, a remote file that is shared over the network.	Absolute path to WebInterface .conf	XenApp Web XenApp Services
DefaultLocale	Specifies the default language to be used if a Web browser requests a non-supported language.	en | de | es | fr | ja | any other supported language identifier	XenApp Web XenApp Services
SiteName	Specifies the name of the site that appears in the Citrix Web Interface Management console. The default setting uses the URL of the site.	Valid string	XenApp Web XenApp Services

To configure 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,…
   ```

To configure SSL Relay communication

In this example, you want to secure communication between the Web server and the server running XenApp or XenDesktop using Secure Sockets Layer (SSL). The SSL Relay is installed on the server running XenApp or XenDesktop, which has a fully qualified domain name of “blues.mycompany.com.” The 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.

To configure Secure Gateway support

In this example, you want to specify a Secure Gateway server called “csg1.mycompany.com” on which Citrix clients use port 443, using the following two Secure Ticket Authority addresses:

- http://country.mycompany.com/scripts/ctxsta.dll
- http://western.mycompany.com/scripts/ctxsta.dll

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.

To configure support for XenApp 4.0, with Feature Pack 1, for UNIX

In this example, you want to configure a site for compatibility with XenApp 4.0, with Feature Pack 1, for UNIX. New Web Interface sites are not initially compatible with this product—an additional manual site configuration step is required.

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

   ```
   OverrideIcaClientname=Off
   
   RequireLaunchReference=On
   ```

2. Change the settings as shown below:

   ```
   OverrideIcaClientname=On
   
   RequireLaunchReference=Off
   ```

   Note: Setting the RequireLaunchReference parameter to Off disables pass-through authentication to XenApp VM hosted apps. Users of this site will be required to enter their credentials each time they access a VM hosted app.

To configure disaster recovery farms

In this example, you have set aside two server farms that will only be used when there is an issue that prevents users accessing the production farms, such as a power failure or network outage.

The names of the servers running the Citrix XML Service in the farms are “jazz” and “fusion.” You want to designate these farms for disaster recovery. To do this:

1. Using a text editor, open the WebInterface.conf file and add the following lines:

   ```
   RecoveryFarm1=jazz,Name:RecoveryFarm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuratio
   RecoveryFarm2=fusion,Name:RecoveryFarm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDurat
   ```

   configuring the settings for this parameter according to your environment.

   Note that the second farm is only used if the first disaster recovery farm is inaccessible. Resources are not aggregated across both disaster recovery farms as they are for production farms. Instead, the Web Interface attempts to contact each disaster recovery farm in order and enumerates resources from the first farm with which communications are established.

To configure user roaming

In this example, you want to associate user groups in your company’s U.S. office with specific server farms so that when they visit the Japan office, they can log on to a local Web Interface server and automatically receive English language resources from a farm in the U.S.

An existing farm with the Citrix XML Service running on the server “waltz” is already defined as Farm1 in the configuration file and is available for all users logging on to the U.S. Web Interface server. The user groups “SalesMgrs” and “SalesTeam” are in the domain “ussales.mycompany.com” and the “Accounts” user group are in the “finance.mycompany.com” domain. You want to associate users from these groups with farms where the names of the servers running the Citrix XML Service are “foxtrot” and “tango.” To do this:

1. Using a text editor, open the WebInterface.conf file on the U.S. Web Interface server and locate the following line:

   ```
   Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance
   ```

   Important: When user roaming is enabled, the first farm defined in the configuration file must be running either XenApp 6.0 or higher or XenDesktop 4.0 or higher. If the first farm listed is running an earlier version, no resources are displayed for any users.

2. Define the new farms by adding the following lines:

   ```
   Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalan
   Farm3=tango,Name:Farm3,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance
   ```

3. Assign user groups to the new farms by adding the following lines:

   ```
   Farm2Groups=ussales.mycompany.com\SalesMgrs,ussales.mycompany.com\SalesTeam,finance.mycompan
   Farm3Groups=ussales.mycompany.com\SalesMgrs
   ```

   Adding the **Farm<*n*>Groups** parameter for a farm that is defined using **Farm<*n*>** activates the user roaming feature. This means that you must assign user groups to all your farms, not just those that will be used by roaming users.
4. Ensure that users can continue to access the existing farm by adding the following line:

   ```
   Farm1Groups=mycompany.com\DomainUsers
   ```

   To enable roaming users to access their resources when they are in Japan, you need to replicate these settings in the configuration file for the Japanese Web Interface server.
5. Using a text editor, open the WebInterface.conf file on the Web Interface server in Japan and insert the lines shown in Steps 2 and 3. Ensure that you also assign user groups to any existing Japanese farms so that local users can continue to access them.

Logged Messages and Event IDs

The Web Interface logs event IDs for all site types and platforms. On Windows operating systems, the event IDs can be viewed using Event Viewer and can be used by Citrix EdgeSight or third-party monitoring and reporting tools. On Java application servers, the event ID is included as part of the log message written to the Web server log file.

The following table shows Web Interface event IDs and the associated log messages. Brief descriptions of the issues and suggestions for their resolution are included.

Event ID	Message	Severity	Description
10001	A configuration parsing error occurred: <*error description*>.	Error	There is a problem with the site configuration file. Check WebInterface.conf for errors.
10002	A configuration loading error occurred.	Error	The site configuration file is missing or inaccessible. Check that WebInterface.conf has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
10003	The Citrix online plug-in configuration could not be retrieved.	Error	The online plug-in configuration file is missing or inaccessible. Check that config.xml has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
10004	The configuration data was reloaded successfully.	Information	Recent changes to the site configuration file (WebInterface.conf) or online plug-in configuration file (config.xml) have been validated and accepted.
10005	The following key(s) are duplicated in the configuration file: <*key name*>.	Warning	There is a duplicate parameter in the site configuration file. Correct the error in WebInterface.conf.
10006	Unknown Authentication Point: <*authentication point*>.	Error	An incorrect value has been specified for the AuthenticationPoint parameter in the site configuration file. Correct the error in WebInterface.conf.

10007	Anonymous logons cannot be used when user roaming is enabled.	Error	XenDesktop does not support anonymous users. To use the user roaming feature with XenDesktop, disable anonymous authentication.
10008	The configuration is invalid: NDS authentication is not supported in this version of the Web Interface.	Error	Reconfigure the authentication method for the site and select either user principal name (UPN) or Microsoft domain-based authentication.
10009	The configuration is invalid: neither smart card nor pass-through authentication are supported in this version of the Web Interface.	Error	This error is displayed if you are using the UNIX/JSP version of Web Interface, and are using Web Interface authentication points with pass-through, smart card, or pass-through with smart card authentication, or Access Gateway authentication points with smart card or pass-through with smart card authentication.
10010	There is a problem with your two-factor authentication configuration.	Error	Check that the Aladdin SafeWord for Citrix, RSA SecurID, or RADIUS server authentication has been configured correctly.
10011	There are no authentication methods currently available.	Error	Check that the site is configured correctly and that one or more valid authentication methods have been specified.
10101	The Protocol Transition Service is incorrectly configured. Please ensure a tokenManager is defined in web.config, and that it defines one or more token services.	Error	Check that the XenApp Web site's web.config file specifies one or more token issuers with associated certificate references that can be used to secure the trust relationship with the pass-through with smart card from Access Gateway service.
10201	The configuration file is invalid: ICA file signing is not supported in this version of the Web Interface.	Error	You must be running Web Interface 5.4 or later to use the ICA file signing feature.
10202	ICA file signing cannot be used when legacy client support is enabled.	Error	To enable ICA file signing, the site must be configured to use the native client and EnableLegacyIcaClientSupport must be set to Off in the Webinterface.conf file.

10203	ICA file signing cannot be used with offline applications.	Error	Check that the site is configured to display online or dual mode applications.
10204	You must allow users to choose the native client in order to use ICA file signing.	Informat ion	To enable ICA file signing, the site must be configured to use the native client.
10205	An error occurred while trying to sign an ICA file: <*error message*>	Error	Refer to the information in the error message for further details regarding any action you may need to take.
10206	An error occurred while trying to sign an ICA file: <>. Restart the Web server to ensure that the ICA file signing service is enabled.	Error	Restart the Web server and use the Web Interface Management Console to ensure that ICA file signing has been enabled.
11001	Invalid redirect URL passed to the client detection and download process.	Error	The redirect URL specifies the Web page to which users are directed when they complete the client detection and deployment process. This error indicates that the redirect URL has been modified in the code for the site.
11002	The client detection and deployment process could not deploy any of the enabled clients. Check that the user's browser, operating system, and access method are compatible with the enabled clients and that these clients are available in the \Clients folder of the XenApp Web site.	Error	The user could not obtain a client from the site. Check that an appropriate client for the user's device, operating system, browser, and access method is both available on the Web server and enabled on the site.
11003	The client detection and deployment process is not supported by the operating system on the user's computer.	Error	The user could not obtain a client from the site because the client detection and deployment process could not identify the operating system on the user's device.
11004	The request from the browser running on the user device <*IP address*> cannot be processed because the User-Agent HTTP header, which provides platform information, is missing.	Error	The user could not access the site because the request sent by the browser did not include a User-Agent HTTP header, which identifies the user's browser and platform. Check your network environment to ensure that User-Agent headers are not being stripped from user requests.

12001	The Web Interface has suppressed <*number*> attempts to log messages with this unique log ID. The reporting rate has now decreased and the Web Interface will begin logging these messages again.	Information	Use the Diagnostic Logging task under Site Maintenance in the Citrix Web Interface Management console to suppress duplicate events from being logged repeatedly and configure how many duplicate events are logged and how often.
12002	Further attempts to log messages with this unique log ID will be suppressed until the reporting rate decreases.	Information	Use the Diagnostic Logging task under Site Maintenance in the Citrix Web Interface Management console to suppress duplicate events from being logged repeatedly and configure how many duplicate events are logged and how often.
12003	The event ID file could not be loaded. Check in the <*file name*> that the path to the event ID file is correct.	Warning	The event ID file is missing or inaccessible. Check that the path given in web.config (for sites hosted on IIS) or web.xml (for sites hosted on Java application servers) is correct. In addition, check that WebInterfaceEventIds.txt has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
12004	The message key <*key name*> does not correspond to a valid event ID. Check that the event ID file has a valid entry for <*key name*>. The event ID must be an integer between 1 and 65535.	Warning	The specified event ID cannot be found in the event ID file. Check that this event ID has not been removed from WebInterfaceEventIds.txt.
13001	An SSL connection could not be established with the Web service at <*server address*>:<*port*>. The message reported from the underlying platform was <*error description*>.	Error	An SSL error has occurred, specific details of which are given at the end of the error message. Check that the Web Interface is configured correctly to integrate with Access Gateway or Password Manager over SSL.

13002	Security identifiers could not be retrieved for at least one group. Check that the Citrix XML Service is accessible and supports user roaming, and that the groups in the configuration file are correct.	Error	There is a problem with one or more user groups configured for the user roaming feature. Check that all the servers in the farm are running a version of XenApp or XenDesktop that supports the user roaming feature. In addition, check that the specified group names are valid and that communication is possible with the Citrix servers.
14001	There was a problem with the RSA SecurID ACE/Agent. Check that the ACE/Agent is installed correctly and that the path to the file aceclnt.dll has been added to the PATH environment variable.	Error	To use SecurID authentication with the Web Interface for Microsoft Internet Information Services, the Web Interface must be installed after installing the RSA Authentication Agent for Web for Internet Information Services.
14002	There was a problem with the RSA SecurID ACE/Agent. Check that the correct version of the ACE/Agent is installed.	Error	Check that a supported version of the RSA Authentication Agent for Web for Internet Information Services is installed on the Web server.
14003	There was a problem with the Aladdin SafeWord Agent. Check that the Agent is installed correctly.	Error	Check that the SafeWord Agent for the Web Interface is installed on the Web server. The Web Interface must be installed before installing the SafeWord Agent.
14004	Unable to update the password cached by the RSA SecurID ACE/Agent. Check that the RSA SecurID ACE/Agent and ACE/Server versions are compatible and that both the ACE/Agent and the ACE/Server are configured to use Windows password integration.	Error	Check that the RSA Authentication Manager and RSA Authentication Agent for Web for Internet Information Services versions are compatible. In addition, check that the RSA Authentication Manager database system parameters are configured to enable Windows password integration at the system level.
14005	Unable to obtain the password cached by the RSA SecurID ACE/Agent. Check that the RSA SecurID ACE/Agent and ACE/Server versions are compatible and that both the ACE/Agent and the ACE/Server are configured to use Windows password integration.	Error	Check that the RSA Authentication Manager and RSA Authentication Agent for Web for Internet Information Services versions are compatible. In addition, check that the RSA Authentication Manager database system parameters are configured to enable Windows password integration at the system level.

14006	There was a problem with the SafeWord authenticator while authenticating the user.	Error	There is a problem with the SafeWord server. For more information, see the log files on the SafeWord server.
14007	There was a problem with the RSA SecurID ACE/Agent. Check that the Web Interface application pool is configured for 32-bit or 64-bit applications as appropriate for the installed ACE/Agent version.	Error	Check the application requirements for the ACE/Agent version you are running.
15001	There was a problem reading the client version from <*file path*>. Users will not be prompted to upgrade to newer versions of this client.	Error	Check that the appropriate permissions have been configured to allow the specified client installer file to be read.
15002	There was a problem reading the language pack file <*file name*>. Check that the file is accessible and uses the correct format.	Error	Check that the specified file has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
15003	The directory <*directory name*> could not be accessed. The clients within this directory cannot be made available to users. Ensure that the Network Service account has the appropriate permissions to access the directory and then restart the Web server.	Error	Check that the specified directory has not been deleted and that the appropriate permissions have been configured to allow this directory to be accessed.
15004	There was a problem reading the language pack file <*file name*>. The version declaration is missing in the file so the language pack cannot be used.	Error	There is no version number in the language pack file. Correct the error in the specified file.
15005	There was a problem reading the language pack file <*file name*>. The language pack version is <*version number*>, which is not compatible with the current version of the Web Interface.	Error	There is a mismatch between the versions of the Web Interface and the language pack file. Language packs are specific to the version of the Web Interface that they are supplied with and cannot be used with earlier or later versions. Upgrade or revert the specified file, as appropriate.
15006	A language pack could not be found for the default locale <*installation locale*>. The language pack <*file name*> was found and will be used as the default.	Warning	When the Web Interface cannot find a language pack for the locale that was chosen during installation, the Web Interface falls back to the first compatible language pack available.

16001	Unable to read the RADIUS secret file <*file path*>.	Error	The RADIUS secret file is missing or inaccessible. Check that the path given in web.config (for sites hosted on IIS) or web.xml (for sites hosted on Java application servers) is correct. In addition, check that the RADIUS secret file has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
16002	The RADIUS secret file <*file path*> is empty.	Error	The RADIUS protocol requires the use of a shared secret—data that is available only to the RADIUS client (the Web Interface) and the RADIUS server against which it authenticates. The RADIUS secret file can contain any string, but must not be empty.
16003	There was a problem with the RADIUS authenticator while authenticating the user.	Error	There is a problem with the RADIUS server. For more information, see the log files on the RADIUS server.
16004	The RADIUS_NAS_IDENTIFIER and/or the RADIUS_IP_ADDRESS values must be present in the site's Web configuration file. RADIUS_NAS_IDENTIFIER values must contain at least 3 characters. RADIUS_IP_ADDRESS must be a valid IP address.	Error	The RADIUS protocol requires that access requests to RADIUS servers include the IP address or other identifier for the RADIUS client (the Web Interface). Check that web.config (for sites hosted on IIS) or web.xml (for sites hosted on Java application servers) contains a valid RADIUS NAS identifier or IP address.
17001	Context look-up failure on server <*server address*>:<*exception*>. This server has been temporarily removed from the list of active servers.	Error	There is a problem with the specified NDS server. This server will be bypassed until the problem is resolved. For more information, see the log files on the NDS server.
17002	All NDS servers have failed so context look-up is not possible. Try logging on with a fully qualified user name; that is, *.username.mycompany.com*.	Error	None of the NDS servers could be contacted. Try entering credentials in the form *.username.mycompany.com*. For more information, see the log files on the NDS servers.

18001	A communication error occurred while attempting to contact the Advanced Access Control authentication service at <*URL*>. Check that the authentication service is running. The message reported by the underlying platform was <*error description*>.	Error	There is a problem contacting the Access Gateway authentication service, specific details of which are given at the end of the error message. For more information, see the log files on the Access Gateway appliance.
18002	A communication error occurred while attempting to close the session using the Access Gateway authentication service at <*URL*>. Check that the authentication service is running. The message reported by the underlying platform was <*error description*>.	Error	There is a problem contacting the Access Gateway authentication service, specific details of which are given at the end of the error message. For more information, see the log files on the Access Gateway appliance.
18003	The Access Gateway authentication service failed to authenticate the user. The message reported by the service was <*error description*> [status code: <*code number*>].	Error	There is a problem with the Access Gateway authentication service, specific details of which are given at the end of the error message. For more information, see the log files on the Access Gateway appliance.
18004	The Access Gatway authentication service failed to close the session. The message reported by the service was <*error description*> [status code: <*code number*>].	Error	There is a problem with the Access Gateway authentication service, specific details of which are given at the end of the error message. For more information, see the log files on the Access Gateway appliance.
18005	Invalid Access Gateway authentication service URL in the site configuration: <*URL*>.	Error	An invalid URL has been specified for the AGEWebServiceURL parameter in the site configuration file. Correct the error in WebInterface.conf.
18006	User<*user name*> could not log on to the site: <*site name*>. Restart the Web server to ensure that the pass-through with smart card from Access Gateway service is enabled.	Error	The smart card user could not log on to the Access Gateway integrated site. Restart the Web server to ensure that the pass-through with smart card from Access Gateway service is running.

18007	This version of Access Gateway does not support Web Interface change password requests. To enable users to change their passwords, you must upgrade to a version of Access Gateway that supports this feature.	Error	This error is displayed if the change password feature is enabled on your site and you are not using the Access Gateway version that supports this feature. Disable the change password feature or upgrade Access Gateway to a version that supports this feature.
19001	An error occurred while disconnecting a user's resources. Either workspace control is not enabled, the user is anonymous, or an error occurred while retrieving the user's credentials or client name.	Error	There is a problem with workspace control. Check that workspace control is enabled for the site and that the user has logged on using an authentication method other than anonymous authentication.
19002	An error occurred while reconnecting a user's resources. Either workspace control is not enabled, the user is anonymous, or an error occurred while retrieving the user's credentials or client name.	Error	There is a problem with workspace control. Check that workspace control is enabled for the site and that the user has logged on using an authentication method other than anonymous authentication.
20001	A communication error occurred while attempting to contact the Password Manager Service at <*URL*>. Check that the service is running. The message reported by the underlying platform was <*error description*>.	Error	There is a problem contacting the Password Manager Service, specific details of which are given at the end of the error message. For more information, see the log files on the Password Manager server.
20002	Invalid Password Manager Service URL in the site configuration: <*URL*>.	Error	An invalid URL has been specified for the AccountSelfServiceUrl parameter in the site configuration file. Correct the error in WebInterface.conf.
21001	A critical server error occurred.	Error	A Java exception occurred in one of the scripts running on the Web page. Try reloading the page. Alternatively, use the Repair Site task under Site Maintenance in the Citrix Web Interface Management console to reinstall the scripts for the site.

21002	Critical server error: <*.NET error description*>.	Error	A .NET exception occurred in one of the scripts running on the Web page. Try reloading the page. Alternatively, use the Repair Site task under Site Maintenance in the Citrix Web Interface Management console to reinstall the scripts for the site.
21003	Due to an error, the file watcher could not be created at the path <*site configuration directory*>.	Error	Check that the path to the site configuration folder is correct and that the appropriate permissions have been configured to allow this directory to be read. Alternatively, try restarting IIS to update the site with the latest configuration changes.
21004	A user is unable to access the site because the fully qualified domain name of the Web server contains underscores (_). Rename the Web server and/or the domain to remove the underscores. If this is not possible, configure an alternative address for the Web server that does not contain underscores or instruct users to access the site using the IP address of the Web server.	Error	Sites cannot be accessed if the site name contains unrecognized characters, such as underscores. Check that the Web server name does not contain underscores, and use the Web Interface Management Console if you need to change the server name.
21005	The Citrix online plug-in ActiveX control with class ID <*ID number*> could not be started. Check that the correct class ID is specified in the site configuration file.	Error	Check that the ActiveX class ID matches the ID number in the Webinterface.conf file.
21006	The Citrix online plug-in ActiveX control with class ID <*ID number*> could not be started. Check that the correct class ID is specified in the site configuration file.	Error	Check that the ActiveX class ID matches the ID number in the Webinterface.conf file.
22001	The Client for Java files could not be located on the server. Check that these files are available in the \Clients folder of the XenApp Web site.	Error	The Client for Java packages are missing or inaccessible. Check that the files have not been deleted and that the appropriate permissions have been configured to allow these files to be read.

23001	An ICA error occurred while trying to access the desktop for user <*user name*>.	Error	The Citrix online plug-in could not access the user's desktop. Check that the desktop is running and is accessible.
23002	Internet Explorer could not provide access to the desktop for user <*user name*>. Check that the Citrix Desktop Appliance Lock is installed on the user's device and that the Desktop Appliance Connector has been added to an appropriate Windows security zone in Internet Explorer.	Error	The desktop appliance user could not access a full-screen-only mode desktop. Check that the Citrix online plug-in has been correctly installed and configured on the user device.
23003	The user <*user name*> has been granted access to <*number*> desktops. Users accessing a full-screen-only mode desktop through a Desktop Appliance Connector should only ever be permitted to access a single desktop.	Warning	More than one desktop has been made available for the desktop appliance user. The user can access a desktop. However, because there is no way to select the required desktop, the user may not be connected to the same desktop the next time they log on. Configure the Desktop Appliance Connector so that the user is only permitted to access a single desktop.
23004	The specified authentication method is invalid. You must specify either "Explicit" or "Certificate", but not both.	Error	Both the Explicit and Certificate values have been specified for the WIAuthenticationMethods parameter in the site configuration file. You cannot enable both explicit and smart card authentication for the same Desktop Appliance Connector. Correct the error in WebInterface.conf.
23005	The embedded smart card SSO authentication configuration is invalid. The authentication method must include "Certificate".	Error	The Certificate value must be specified for the WIAuthenticationMethods parameter in the site configuration file for the Desktop Appliance Connector. Correct the error in WebInterface.conf.

23006	The specified authentication methods are invalid. The combination of authentication mtehods are not supported.	Error	The Desktop Appliance Connector authentication methods specified in the WIAuthenticationMethods parameter in the site configuration file cannot be used together. Correct the error in WebInterface.conf.
24001	A logon attempt was made by an unauthenticated user. Verify that shadow accounts have been created for all of the intended users of the system. If the problem persists, try repairing the site using the Web Interface Management Console.	Error	There is a problem with the AD FS integrated site. The user could not be authenticated. Check that a shadow account has been created for the user in the resource partner domain. Alternatively, use the Repair Site task under Site Maintenance in the Citrix Web Interface Management console to reinstall the site.
24002	A logon attempt was made by an unauthenticated user. If the problem persists, try reparing the site using the Web Interface Management Console.	Error	There is a problem with the XenApp Web or XenApp Services site. The user could not be authenticated. Check that a user account has been created for the user in the domain. Alternatively, use the Repair Site task under Site Maintenance in the Citrix Web Interface Management console to reinstall the site.
30001	An error occurred while attempting to read information from the Citrix servers: <*farm name*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30002	An error occurred while attempting to write information to the Citrix servers: <*farm name*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30003	An error occurred while attempting to connect to the server <*server address*> on port <*port*>. Verify that the Citrix XML Service is running and is using the correct port. If the XML Service is configured to share ports with Microsoft Internet Information Services (IIS), verify that IIS is running. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check whether the XML Service has been configured to share TCP/IP ports with IIS and, if so, check that IIS is running. For more information, see the log files on the Citrix server.
30004	The server name <*server address*> cannot be resolved. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30005	The Citrix servers sent incorrect HTTP syntax. Verify that the current Web Interface version is compatible with the servers being used. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the server farm is running XenDesktop or Presentation Server 4.5 or later. Citrix recommends that all servers in a farm run the same product and version. For more information, see the log files on the Citrix server.
30006	The Citrix servers sent an incorrect or unexpected response. Verify that the current Web Interface version is compatible with the servers being used. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the server farm is running XenDesktop or Presentation Server 4.5 or later. Citrix recommends that all servers in a farm run the same product and version. For more information, see the log files on the Citrix server.
30008	The Citrix servers unexpectedly closed the connection. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30009	The Citrix servers sent HTTP headers indicating that an error occurred: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30010	The Citrix servers cannot process the request at this time. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30011	An error occurred on the Citrix servers while attempting to complete the request: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30012	The Citrix servers encountered a version mismatch error. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30013	The Citrix servers received an incorrect request. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30014	An error occurred on the Citrix servers during parsing of the request. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30015	The Citrix XML Service at address <*file path*> is not able to process requests.	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30016	The Citrix XML Service object was not found: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30017	The Citrix XML Service method is not supported: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30018	The Citrix XML Service response is not acceptable: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30019	The Citrix XML Service request length is required: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30020	The Citrix XML Service request is too short: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30021	The Citrix XML Service request exceeds the maximum size: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30022	The Citrix XML Service or the Citrix servers may be unavailable or temporarily overloaded: <*details*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30023	The XML document sent by the Citrix servers could not be processed. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30024	The XML document sent by the Citrix servers could not be processed because it contains invalid XML. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30025	An error occurred while attempting to read information from the Citrix servers: <*farm name*>. This error may be the result of attempting to communicate with an alternative to the SSL Relay. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. To use SSL/TLS encryption on connections to the server farm, you must use the SSL Relay to configure support on each server. For more information, see the log files on the Citrix server.
30026	An error occurred while attempting to make a connection with the SSL Relay: <*server address*>:<*port*>. Verify that there is an SSL Relay running and that it is listening on a valid port. The name contained in the server certificate that the SSL Relay is configured to contact must match exactly the name of the server to which the connection was attempted. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the SSL Relay is running and listening on the appropriate port (typically port 443) and that the SSL Relay server certificate contains the fully qualified name of the server (with the correct case) to which the connection was attempted. For more information, see the log files on the Citrix server.
30027	Ticketing may not be supported by one or more Citrix servers. To use this feature, you must either upgrade the servers running the XML Service or disable ticketing. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that all the servers in the farm are running XenDesktop or MetaFrame XP 1.0 or later. Citrix recommends that all servers in a farm run the same product and version. For more information, see the log files on the Citrix server.
30028	The name of the SSL Relay <*server address*> cannot be resolved. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30029	An SSL connection could not be established: <*SSL error description*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30030	An SSL Relay connection could not be established: <*SSL error description*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30031	The Citrix XML Service at address <*file path*> does not support capability <*feature name*>.	Error	Check that all the servers in the farm are running a version of XenApp or XenDesktop that supports the specified feature. For more information, see Minimum Software Requirements.
30101	The change password attempt was corrupted.	Error	For security reasons, the user could not change the Windows password. For more information, see the log files on the Citrix servers and/or the domain controller.
30102	The Citrix servers reported an unspecified error from the XML Service at address <*file path*>.	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30103	The Citrix servers reported that the alternate address cannot be found. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30104	An error occurred when connecting to the Citrix server to access the resource. Verify that the server is running and that the network is functioning. This error was reported for an XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check the server farm and the network for issues. For more information, see the log files on the Citrix server.
30105	The Citrix servers do not trust the server. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	Check that a trust relationship exists between the Web Interface server and the Citrix XML Service. For more information, see Using Workspace Control with Integrated Authentication Methods for XenApp Web Sites.

30106	The Citrix servers are not licensed to support the requested operation. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the Citrix License Server is running and is accessible. Citrix recommends that you upgrade the license server to the most recent version to ensure compatibility with the latest products. For more information, see the log files on the Citrix server and/or the license server.
30107	The Citrix servers reported that they are too busy to provide access to the selected resource. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the server farm is not overloaded. For more information, see the log files on the Citrix server.
30108	The ticketing feature is disabled on the Citrix server. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that all the servers in the farm are using the same port to communicate with the XML Service. For more information, see the log files on the Citrix server.
30109	The Citrix XML Service at address <*file path*> reported a registration error. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30110	An error of type <*error type*> with an error ID of <*error ID*> was reported from the Citrix XML Service at address <*file path*>. Depending on the server running the XML Service, more information may be available in the server's event log. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30111	The Citrix servers do not support the specified address type. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.

30112	No available resource found for user <*user name*> when accessing desktop group <*group name*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the user has been assigned to the specified desktop group and that there are unused desktops available in the group. For more information, see the log files on the Citrix server.
30113	A request from the Citrix server to prepare for a connection was rejected while processing the initialization of desktop group <*group name*> for user <*user name*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30114	The Citrix servers were denied access to retrieve security identifiers for the user. Either grant the XML Service read permissions to the Token-Group s-Global-And-Universal attribute in Active Directory or disable security identifier enumeration in the XML Service. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. If the XML Service is configured to enumerate security identifiers for users, check that the appropriate permissions have been granted in Active Directory. For more information, see CTX117489 and the log files on the Citrix server.
30115	The Citrix servers could not retrieve security identifiers for the user. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see CTX117489 and the log files on the Citrix server.
30116	Unable to connect to a desktop in maintenance mode for user <*user name*> when initializing desktop group <*group name*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the user's desktop has not been put into maintenance mode. For more information, see the log files on the Citrix server.

30117	The Citrix servers do not support the desktop restart operation. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the server farm is running XenDesktop 3.0 or later. Citrix recommends that all servers in a farm run the same product and version. For more information, see the log files on the Citrix server.
30118	The Citrix servers timed out while waiting for a machine in desktop group <*group name*> to power off for user <*user name*>. This message was reported from the XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30119	Unable to power off a machine in maintenance mode in desktop group <*group name*> for user <*user name*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. Check that the user's desktop has not been put into maintenance mode. For more information, see the log files on the Citrix server.
30120	Unable to find user <*user name*>. This message was reported from the Citrix XML Service at address <*file path*>. <*error description*>	Error	There is a problem with the Citrix XML Service, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30201	Invalid Secure Ticket Authority address: <*URL*>. <*error description*>	Error	An invalid URL has been specified for the **CSG_STA_ URL<*n*>** parameter in the site configuration file. Correct the error in WebInterface.conf.
30202	The Secure Ticket Authority <*URL*> does not support version 4 requests. All Secure Ticket Authority communications will now fall back to version 1. New connections through the Secure Gateway will not use session reliability.	Error	The Secure Gateway version in use does not support the Secure Ticket Authority redundancy feature. As a result, this feature has been disabled.

30203	The Secure Ticket Authority <*URL*> returned a ticket with an unexpected authority or type - <*error type*>, <*error ID*>, <*SSL error description*>, <*details*>. <*error description*>	Error	There is a problem with the Secure Ticket Authority, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix server.
30204	The specified Secure Ticket Authority could not be contacted and has been temporarily removed from the list of active services.	Error	There is a problem with the Secure Ticket Authority. This service will be bypassed until the problem is resolved. For more information, see the log files on the Citrix server.
30205	All the configured Secure Ticket Authorities failed to respond to this XML transaction.	Error	None of the Secure Ticket Authorities could be contacted. Try restarting the Web server. For more information, see the log files on the Citrix servers.
30301	The HTTP response indicates the underlying connection was closed.	Error	Check that the server farm is running XenDesktop or Presentation Server 4.5 or later. Citrix recommends that all servers in a farm run the same product and version.
30401	A socket has been forcibly destroyed by the transaction layer.	Error	Check the farm data store for corrupt applications. For more information, see CTX114769.
31001	The specified Citrix XML Service could not be contacted and has been temporarily removed from the list of active services.	Error	There is a problem with the Citrix XML Service. This server will be bypassed until the problem is resolved. For more information, see the log files on the Citrix server.
31002	This XML Service transaction failed, but the XML Service has not been removed from the list of active services.	Error	Although the Citrix XML Service is accessible, the request or instruction could not be completed. For more information, see the log files on the Citrix server.
31003	All the Citrix XML Services configured for farm <*farm name*> failed to respond to this XML Service transaction.	Error	None of the Citrix XML Service hosts for the specified farm could be contacted. Try restarting the Web server. For more information, see the log files on the Citrix servers.
31004	The XML protocol error <*error ID*> could not be converted to an access status error.	Error	Check that the user has Active Directory logon rights to the Citrix servers.

31005	<*number*> of <*number*> resources were ignored because they are invalid.	Error	The Citrix XML Service could not enumerate all of the resources available. For more information, see the log files on the Citrix server.
31006	The logon of user <*user name*> was rejected because the user is not licensed.	Error	The user could not be logged on because there were no Citrix licenses or Microsoft Remote Desktop Services client access licenses available. Check that the Citrix License Server is running and is accessible. Citrix recommends that you upgrade the license server to the most recent version to ensure compatibility with the latest products. For more information, see the log files on the Citrix servers and/or the license server.
31007	The Citrix servers are not licensed to support workspace control. This message was reported from the XML Service at address <*file path*>.	Error	Check that the Citrix licenses enable a product edition that includes the workspace control feature. In addition, check that the Citrix License Server is running and is accessible. Citrix recommends that you upgrade the license server to the most recent version to ensure compatibility with the latest products. For more information, see the log files on the Citrix server and/or the license server.
31008	The Citrix servers are not licensed to launch the resource <*resource name*>. This message was reported from the XML Service at address <*file path*>.	Error	Check that the Citrix licenses enable a product edition that includes this type of resource. In addition, check that the Citrix License Server is running and is accessible. Citrix recommends that you upgrade the license server to the most recent version to ensure compatibility with the latest products. For more information, see the log files on the Citrix server and/or the license server.

31009	The account data for the following account(s) cannot be retrieved: <*list of account names*> Check that the name is spelt correctly. This message was reported from the Citrix XML Service at address <*file path*>.	Error	The Citrix XML Service cannot access the specified accounts. Check that the accounts have not been deleted and that the appropriate permissions have been configured to allow them to be read by the XML Service. In addition, check that the account names have been entered correctly. For more information, see the log files on the Citrix server.
31101	The user <*user name*> has a server session, <*session ID*>, but does not have access to <*resource name*>, the resource that created the session. As a result, the user cannot access this session.	Error	The user's access permissions were changed while the user's session was still active. Reset the session. Note that this will result in loss of data for the user. For more information, see the log files on the Citrix server.
31201	The farm <*farm name*> has been configured to use ticketing, but no ticket tag was received. Check that the farm supports ticketing.	Error	Check that all the servers in the specified farm are running XenDesktop or MetaFrame XP 1.0 or later. Citrix recommends that all servers in a farm run the same product and version. For more information, see the log files on the Citrix servers.
31202	A user attempted to launch the resource <*resource name*>, which is currently disabled.	Error	Check that the specified resource is enabled on the server on which it is hosted.
31203	The farm <*farm name*> has been configured to use launch references, but a launch reference was not received from the Citrix XML Service. Check that the farm supports launch references or disable launch reference requests.	Error	To use launch references, all the servers in the specified farm must run XenDesktop or Presentation Server 4.5 or later. Citrix recommends that all servers in a farm run the same product and version. If the farm is running XenApp 4.0, with Feature Pack 1, for UNIX or Presentation Server 4.0 and earlier, ensure that the RequireLaunchReference parameter is set to Off and that OverrideIcaClientname is set to On in the XenApp Web site configuration file, WebInterface.conf.
31301	The configuration of farm <*farm name*> is invalid.	Error	There is a problem with the specified server farm. For more information, see the log files on the Citrix servers.

32001	The configuration does not include details of any Citrix servers.	Error	No farms have been specified for the **Farm<*n*>** parameter in the XenApp Services site configuration file. Correct the error in WebInterface.conf.
32002	Unable to parse the provider chain configuration.	Error	There is a problem with the XenApp Services site. Check the site configuration files for errors.
32003	<*Error cause*> The following system error occurred: <*error description*>	Error	There is a problem with the XenApp Services site, specific details of which are given at the end of the error message. Check the site configuration files for errors.
33001	Citrix Streaming Service: The specified Citrix XML Service could not be contacted and has been temporarily removed from the list of active services.	Error	The Citrix offline plug-in encountered a problem with the Citrix XML Service. This service will be bypassed until the problem is resolved. For more information, see the log files on the Citrix server.
33002	Citrix Streaming Service: This Citrix XML Service transaction failed, but the XML Service has not been removed from the list of active services.	Error	Although the Citrix XML Service is accessible to the Citrix offline plug-in, the request or instruction could not be completed. For more information, see the log files on the Citrix server.
33003	Citrix Streaming Service: All the Citrix XML Services configured for farm <*farm name*> failed to respond to this XML Service transaction.	Error	None of the Citrix XML Service hosts for the specified farm could be contacted by the Citrix offline plug-in. Try restarting the Web server. For more information, see the log files on the Citrix servers.
33004	Citrix Streaming Service: The configuration of farm <*farm name*> is invalid.	Error	The Citrix offline plug-in encountered a problem with the specified server farm. For more information, see the log files on the Citrix servers.
33005	Citrix Streaming Service: The configuration does not include details of any Citrix servers.	Error	No farms have been specified for the **Farm<*n*>** parameter in the site configuration file. Correct the error in WebInterface.conf.

33006	The configuration file RadeValidationRules.conf could not be loaded. Check that the file is available in the site configuration folder.	Error	The configuration file RadeValidationRules.conf is missing or inaccessible. Check that the file has not been deleted and that the appropriate permissions have been configured to allow this file to be read.
33007	The configuration file RadeValidationRules.conf cannot be used because it contains invalid rules. Check that all of the rules use valid regular expression syntax.	Error	There is a problem with the configuration file RadeValidationRules.conf. All rules in this file should be given using regular expression syntax. Check the file for errors. Alternatively, use the Repair Site task under Site Maintenance in the Citrix Web Interface Management console to reinstall the site. Any changes you have made to the file will be discarded.
34001	The configuration does not include details of any Citrix servers.	Error	No farms have been specified for the **Farm<*n*>** parameter in the Desktop Appliance Connector or XenApp Web site configuration file. Correct the error in WebInterface.conf.
34002	Unable to parse the provider chain configuration.	Error	There is a problem with the Desktop Appliance Connector or XenApp Web site. Check WebInterface.conf for errors.
34003	<*Error cause*> The following system error occurred: <*error description*>	Error	There is a problem with the XenApp Services site, specific details of which are given at the end of the error message. Check WebInterface.conf for errors.
40001	An error occurred while enumerating a user's resources. An unrecognized XML message was received from a user device.	Error	The Citrix online plug-in encountered a problem when connecting to the Citrix servers. Check that the Citrix online plug-in is configured correctly on the user's device.
40002	An error occurred while enumerating a user's resources. An unrecognized XML message was received from a user device.	Error	The Citrix online plug-in encountered a problem when connecting to the Citrix servers. Check that the Citrix online plug-in is configured correctly on the user's device.

40003	An error occurred while reconnecting a user's resources. An unrecognized XML message was received from a user device.	Error	The Citrix online plug-in encountered a problem when reconnecting to the Citrix servers. Check that the Citrix online plug-in is configured correctly on the user's device.
40004	<*IP address*> requested Citrix online plug-in configuration <*file name*>, which does not exist.	Error	Check on the user's device that the configuration file URL has been entered correctly in the Options dialog box for the Citrix online plug-in.
40005	An error occurred while launching a user's resource: <*error description*>	Error	The Citrix online plug-in encountered a problem, specific details of which are given at the end of the error message. For more information, see the log files on the Citrix servers.
40006	An error occurred while performing a desktop control operation. An unrecognized XML message was received from a user device.	Error	The Citrix online plug-in encountered a problem when restarting the user's desktop. Check that the Citrix online plug-in is configured correctly on the user's device.

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:

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

to:

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

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

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

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

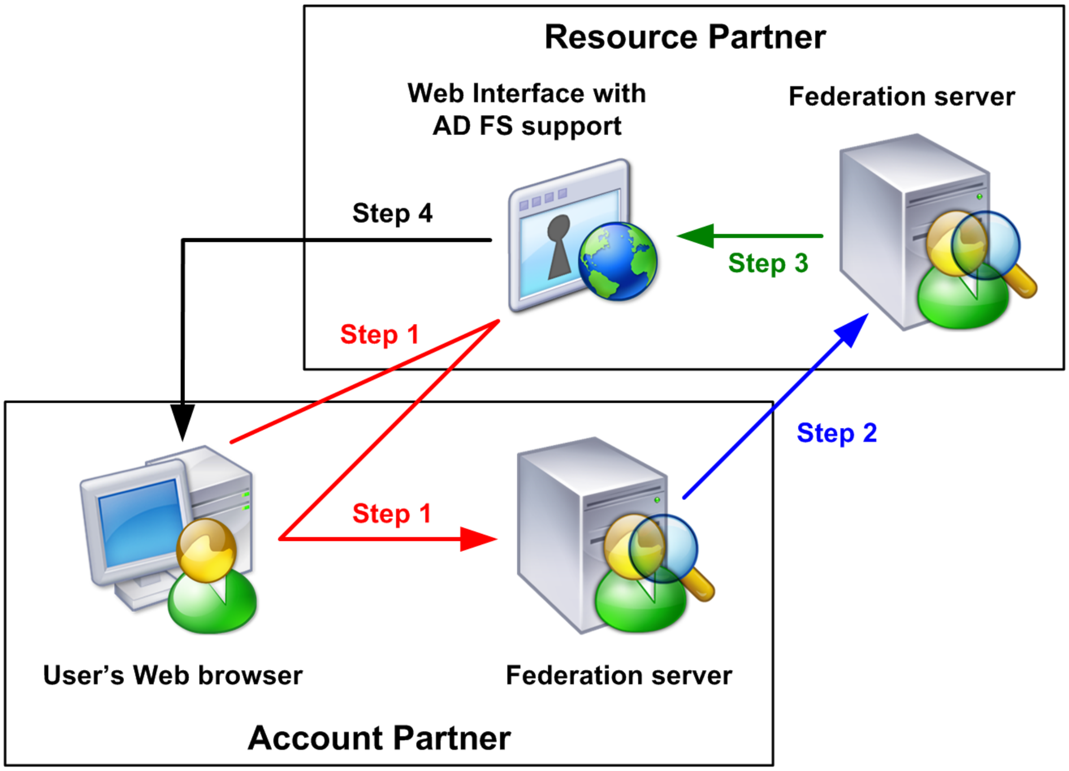
Configuring AD FS Support for the Web Interface

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

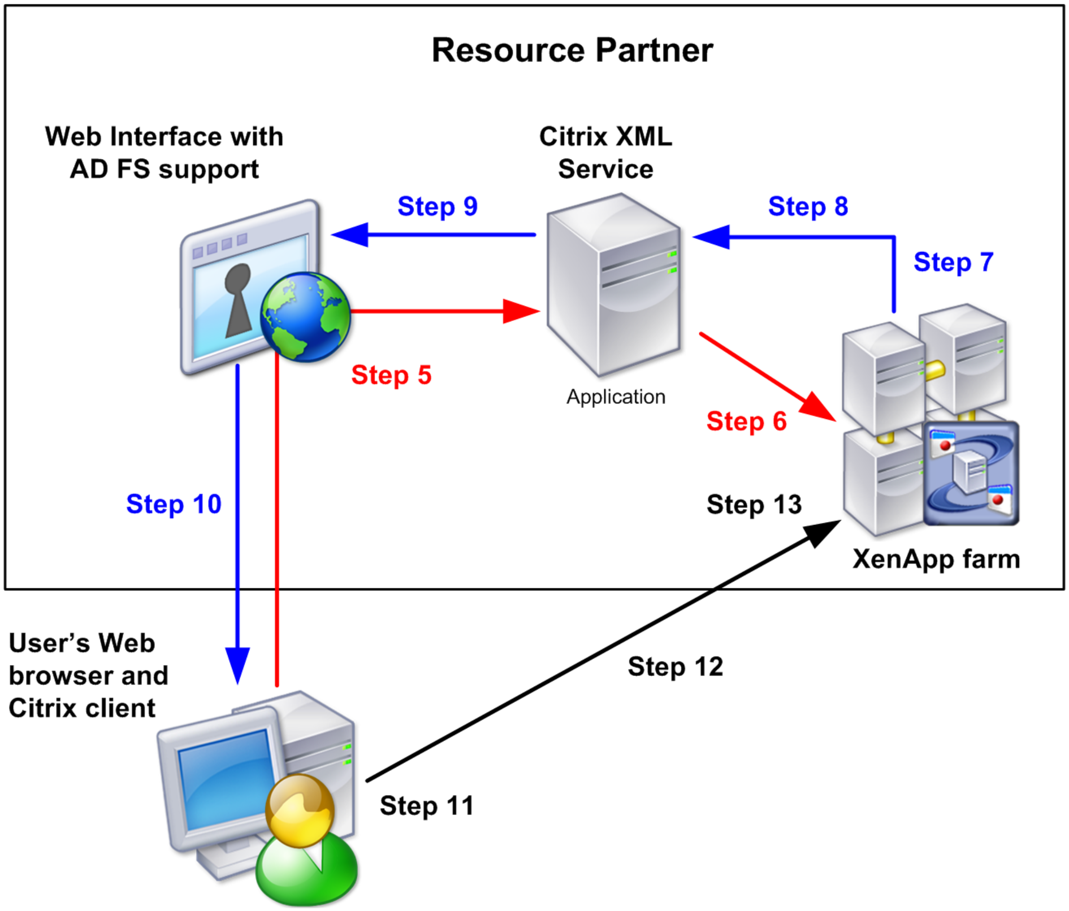
Important: AD FS requires secure communications between the Web browser, Web server, and federation servers. Web Interface users must use HTTPS/SSL to access the site.

How Active Directory Federation Services Integrated Sites Work

The following steps occur when a user on an account partner accesses an 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 accesses an application by clicking a hyperlink on the page. Web Interface contacts the Citrix XML Service to request access.
- **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 Web browser.
- **Step 11.** The user's device opens the .ica file and attempts an ICA connection to the server.
- **Step 12.** The Citrix client 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 access 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.

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.
- 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.
- Ensure all servers within your deployment are trusted for delegation. For more information, see Configuring Delegation for the Servers in Your Deployment.
- 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.
- 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 Using Workspace Control with Integrated Authentication Methods for XenApp Web Sites.

Important: This section 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.

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. In the case of the Web server, only the 32-bit versions of Windows Server 2008 and Windows Server 2003 R2 are supported.

- 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.

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
   - User devices

   The resource partner requires:

   - Domain controller
   - Federation server
   - Web server
   - One or more servers for a XenApp farm

   The federation servers must be hosted on computers running Windows Server 2008 or Windows Server 2003 R2 and have the Active Directory Federation Services server role installed.

   The Web server must be hosted on a computer running a 32-bit version of Windows Server 2008 or Windows Server 2003 R2. The Claims-aware Agent and Windows Token-based Agent role services must be installed, along with *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.
   - Install federation server certificates using the Microsoft Management Console (MMC) Certificates snap-in. For more information, see the *Step-by-Step Guide to the Microsoft Management Console* at http://technet.microsoft.com/.

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. In the Action pane, 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 Action 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 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, in the Action pane, click Properties.

3. If the domain is not at the highest possible functional level, select the domain name and, in the Action pane, 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. In the Action pane, 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. In the Action pane, 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. In the Action pane, 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 domain controllers 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.

Configuring a Time Limit for Access to Resources

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.

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 results pane, select Maximum lifetime for service ticket.
4. In the Action pane, click Properties.
5. Enter the required time limit (in minutes) in the Ticket expires in box.

If you do not want to configure a time limit for access to resources, select Use any authentication protocol when determining which resources are accessible from the XenApp server. If you select this option, any value specified for S4UTicketLifetime is ignored. For more information, visit the Microsoft Web site at http://support.microsoft.com/.

Setting up Shadow Accounts

To provide access to 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.

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. In the Action pane, 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.

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. In the Action pane, 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 Citrix Web interface 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. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click the Citrix Web Interface container.
3. In the Action pane, click Create Site.
4. Select XenApp Web and click Next.
5. On the Specify IIS Location page, specify the IIS location, the path, and a name for the site. Click Next.
6. 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.
7. Confirm the settings for the new site and click Next to create the site.

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.
3. In the Action pane, click New > Application.
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.

   Note: 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 user 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 online plug-in, do so now. For more information, see Online Plug-in for Windows.
4. Click an application to access it.

Logging off from Active Directory Federation Services Integrated Sites

Use the Authentication Methods task in the Citrix Web Interface 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 restart their applications. When they do this, the previous session unlocks and the new window closes.

To specify which services users log off from

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.

2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and, in the results pane, select your AD FS integrated site.

3. In the Action pane, click Authentication Methods.

4. 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.