Plug-in for Hosted Apps for Windows 11.0

Contents

Plug-in for Hosted Apps for Windows 11.0

Users run the plug-in on their devices to access applications published on XenApp servers. The plug-in combines ease of deployment and use, and offers quick, secure access to applications and content.

The plug-in for Windows documentation is for system administrators responsible for installing, configuring, deploying, and maintaining Citrix XenApp and the plug-in for user devices running 32-bit or 64-bit Windows operating systems.

Readme for Citrix XenApp Plugin for Hosted Apps 11.0 for Windows and Citrix XenApp Plugin for Streamed Apps 1.2 for Windows

Readme Version: 1.9

Notes:

- For the most up-to-date version of this readme file, click http://support.citrix.com/article/CTX116416.
- For the latest critical updates, visit the critical updates page for the 64-bit edition at http://support.citrix.com/product/xa/v5.0_2008/hotfix/x64/?onlyCritical=true or for the 32-bit edition at http://support.citrix.com/product/xa/v5.0_2008/hotfix/x86/?onlyCritical=true.
- For a list of issues resolved in this release, clickhttp://support.citrix.com/article/CTX116697.
- For information about new features and system requirements, see the product administration guides.

Finding Documentation

Use Read_Me_First.html on your installation media to access the complete set of documentation on the Web, or go to http://support.citrix.com/article/CTX113391).

For known issues related to other Citrix products, components, and features in the Citrix XenApp 5.0 release, see the following documents:

- Readme for XenApp 5.0 for Windows Server 2008 - http://support.citrix.com/article/CTX113393
- Readme for Web Interface 5.0.1 - http://support.citrix.com/article/CTX116591
- Readme for Password Manager 4.6 with Service Pack 1 - http://support.citrix.com/article/CTX117184
- Readme for XenApp 5.0 for Windows Server 2003 - http://support.citrix.com/article/CTX116620
- Readme for EasyCall Agent 1.2 - http://support.citrix.com/article/CTX117318

- Readme for EdgeSight for XenApp 5.0 - http://support.citrix.com/article/CTX117626
- Readme for Access Gateway 8.1 Enterprise Edition - http://support.citrix.com/article/CTX117170
- Readme for Access Gateway 4.5 Advanced Edition - http://support.citrix.com/article/CTX109105
- Readme for Access Gateway 4.5.6 Standard Edition - http://support.citrix.com/article/CTX115402

Licensing Documentation

For the latest licensing documentation, see 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 Website. The Support page includes links to downloads, the CitrixKnowledge Center, Citrix Consulting Services, and other usefulsupport pages.

Installation Issues

Important: Before you install this product, make sure you consult the Installation Checklist at http://support.citrix.com/article/CTX113392

- Citrix strongly recommends that you uninstall all previous clients and install the current versions of the Citrix XenApp Plugin for Hosted Apps (Program Neighborhood Agent and the Web Client), including the Citrix XenApp for Streamed Apps (the new name for the Streaming Client).

  In particular, XenApp server no longer supports clients that were installed using the Streaming Clients Package, which would appear in your list of removable programs as the Citrix Streaming Clients for Windows.

- If plugins are installed, runningXenAppHosted.msi only upgrades those plugins and does not installplugins that are not installed already.

  As a workaround, uninstall all of the CitrixXenApp Plugins for Hosted Apps before running XenAppHosted.msi.[#204703]

- Citrix XenApp or Program Neighborhood is not uninstalled properly when either is the only plugin selected in the Modify option of the Citrix XenApp Plugin for Hosted Apps installation package created using an administrative installation. As a workaround,

uninstall all of the Citrix XenApp Plugin and reinstall the desired client features. [#175591]

- To install XenApp components on a Windows 2000 Server, before you begin the installation, download the gdiplus.dll file from the Microsoft Website at http://www.microsoft.com/downloads/details.aspx?familyid=6A63AB9C-DF12-4D41-933C-BE590FEAA05A Run gdiplus_dnld.exe on the local server and copy gdiplus.dll in the winnt\system32 folder. Then start Autorun.[#190821]

Third-Party Issues for Citrix XenApp Plugin for Hosted Apps

- After installing Citrix XenApp Plugin for Hosted Apps successfully, SideBySide error messages might appear in the Event Viewer Application log after the launch of a published application from the plugin. These error messages do not impact plugin functionality. To eliminate the generation of these messages, install the Microsoft Visual C++ 2005 SP1 Redistributable Package from the Support\vcredist folder on the Citrix XenApp server installation media. [#187782 and #190365]

- Presentation Server Client icons might appear in the taskbar after upgrading to Citrix XenApp Plugin for Hosted Apps 11.0 for Windows. Windows stores the old icons in the icon cache and improperly updates them when you update the previous clients to the new plugins. See http://support.microsoft.com/kb/q132668 to resolve this issue. [#189031]

- When users log on for the first time to the XenApp 5.0 farm using the XenApp Plugin for Hosted Apps, the application icons download slowly to the Citrix XenApp list of published applications. The issue occurs when you publish applications using 32-bit color icons. For a workaround, see http://support.citrix.com/article/CTX118227. [#197417]

- Smart card pass-through authentication is unavailable if the Citrix XenApp Plugin is running on a Windows Server 2008 XenApp server and the user tries to access published applications from a second XenApp server. The user must provide a valid PIN to launch each application unless session sharing is configured. [#167561]

- Smart card pass-through authentication is unavailable if the Citrix XenApp Plugin is running on a Windows Vista client device. The user must provide a valid PIN to launch each application, unless session sharing is configured. [#168728]

- SpeedScreen Browser Acceleration is unavailable with Outlook 2007; Citrix supports SpeedScreen Browser Acceleration for Outlook 2003 only.

- Do not use SpeedScreen Flash Acceleration in 16-color mode. A third-party issue causes Microsoft Internet Explorer 7.0 to fail. [#164906]

- On Windows Server 2008, if you have two sessions running and you connect from one (session 1) to the other (session2) using TSCON, the first session (session 1) is disconnected and cannot be reconnected and there might be unexpected results in the connection to the second session (session 2). [#182790]

- Users of Philips SpeechMike USB devices cannot play backtheir recordings when accessing the SpeechMike applications as a publishedapplication or in a published desktop. If using the Philips SpeechMike Serial devices with thePhilips Foot Pedal for Playback USB device, users cannot play backtheir recordings when accessing the SpeechMike applications as a publishedapplication or in a published desktop. See Microsoft article http://support.microsoft.com/kb/961918 to resolve this issue. [#193435, #194558]

- Users of Philips SpeechMike USB devices cannot play backtheir recordings when accessing the SpeechMike Test Recorder application asa published application. Although the audio is recorded, users mustsave the audio files, end their current ICA session, and then playback the audio files in a separate ICA session. This limitationoccurs when the client computer is running Window XP or WindowsVista and the SpeechMike deviceis connected to the client computer through a USB port. Serial portPhilips SpeechMike devices do notexhibit this limitation. See Microsoft article http://support.microsoft.com/kb/961918 to resolve this issue.[#177437]

- Publishing Windows Media Player on Windows Server 2008 64-bit Edition, even if the audio quality is set at high, results in background static on client devices. This issue does not occur if you publish Media Player on a 32-bit operating system. [#197420]

- Because of a WinINET limitation, Internet Explorer 6 stops responding if reconnecting to more than two published Windows applications.

  Workaround:

  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.

  See Microsoft article http://support.microsoft.com/kb/183110 for instructions. [#192639 and #181830]

- Computers running Windows Server 2008, Windows Vista, or Windows Vista SP1 might experience a fatal exception, displaying a blue screen with stop code 0x000000D1.Microsoft has released a hotfix, available at http://support.microsoft.com/kb/955734 to address this issue. [#181457]

Other Known Issues for Citrix XenApp Plugin for Hosted Apps

- The Citrix Connection Center Terminate button does not terminate a published application that is in full-screen mode. As a workaround, use Shift-F2 to return the application to seamless mode, and then use the Terminate button. [#187727]

- When using Windows Vista with User Account Control (UAC) enabled, nonbuilt-in administrators cannot change the Program Neighborhood Enable Dynamic Client Name and Pass-through Authentication settings. As a workaround, right-click Program Files\Citrix\ICA Client\pn.exe, select Run as administrator, choose to continue, change the settings as needed, close pn.exe.

  Note: Use this workaround only to change the Enable Dynamic Client Name and Pass-through Authentication settings and not to launch connections from pn.exe. [#192317 and #193726]

- When the XenAppWeb.exe Repair option prompts for the location of the XenAppWeb.msi file, type the path to the XenAppWeb.msi file, Clients\ica32\XenAppWeb.msi, on the XenApp installation media. [#192366]

- Though it is still running in the background, the Citrix XenApp plugin icon disappears from the notification area after uninstalling the Citrix XenApp Plugin for Streamed Apps. To avoid this issue, stop Citrix XenApp (pnagent.exe) before uninstalling Citrix XenApp Plug for Streamed Apps. Note that users' sessions will be disconnected. [#193979]

- When Special Folder Redirection is enabled on the client and the XenApp Web site, the Desktop folders should be mapped to the client device. Only contents of the client desktop should be visible in an ICA session. However, when Special Folder Redirection is enabled, the contents of the server desktop and some contents of client desktop are merged together in published applications, such as Windows Explorer, Notepad, and Microsoft Word. [#189351]

- When Special Folder Redirection is enabled and users launch applications in a pass-through session (multihop), the applications open with various error messages, including insufficient memory and inability to locate the application. There is no workaround for this issue. Note that these launch error messages do not occur when Special Folder Redirection is disabled. [#197355]

- If a user is running a desktop or published application ICA session to a XenApp server that is set to Restrict users to one session only and disconnects the session, the user cannot log on to the server using a physical console until resetting or logging off the disconnected session. [#173506]

- Automatic logon fails when a user with a blank password launches a published application. As a workaround, users must use a password. [#169280]

- Configure XenApp Plugin for Hosted Apps using the Group Policy template icaclient.adm. Changes made directly to the registry keys used by the plugin might not be preserved during an upgrade. [#189360]

- When shadowing a published application or a published desktop session with a published desktop on a computer having lower desktop resolution than the client device being shadowed, do not maximize or resize the shadowed session. Doing so might cause unexpected mouse-click and desktop-graphic behavior. [#194642]

- When shadowing from a full-screen published desktop on a computer that is using multimonitors and has a higher desktop resolution than the client device being shadowed, the Windows taskbar moves off screen. As a workaround, on the session being shadowed, press Shift-F2 to change to seamless mode and then Shift-F2 again to change to full-screen mode. [#197192]

- After using the Shadow Taskbar to launch session shadowing, the shadowed session appears in the Windows Taskbar instead of the Shadow Taskbar. [#196063]

- When using the Citrix XPS Universal Printer driver to print a Microsoft Word document that contains both portrait and landscape pages, all pages print in portrait mode. This trims the landscape pages to fit portrait orientation. [#194634]

  Workarounds:

  - Ensure at least three to four printers are created in the session, which forces the dialog box to draw a scroll bar and lets users scroll to select the printers

  - Assign printers short names so that their names render with fewer than 60 characters in a session

  - Instruct users to right-click the Select Printer window and select another display type, such as Details, instead of the default List, and then they can select the printers
- On Windows XP client devices with Citrix Clients for Windows installed, such as Version 9.0 or earlier, printing failure might occur if users have not designated a default printer in Windows or if the application is unable to locate an existing default printer.

  Citrix recommends uninstalling previous clients and installing the Citrix XenApp Plugin provided in this release. Otherwise, to correct this issue, try these suggestions in the Windows printer setup [#195822]:

  - If a printer is not available in the Print dialog box, add a printer.

  - If the application cannot find an existing printer that is already installed, set the printer as the default printer

  - If a default printer is installed but the application is unable to use it, uninstall the printer driver, and then install the latest version of the printer driver.

  - If the printer is on a print server, make sure the printer is available, the network is functioning, the server is not stalled, the printer is not out of paper, or the printer is not suspended by the administrator.

- Pass-through authentication is not available when accessing a published application from within a published desktop on XenApp 5.0 for Windows 2008 servers. Instead, the user must provide valid credentials to launch a session within a desktop session even when pass-through authentication is enabled in the plugin. To resolve this issue, you must install a server-side hotfix for XenApp 5.0 for Windows 2008 that contains Fix #194894. [#194894]

- If you launch a desktop or a published application session to a XenApp server using a Program Neighborhood Custom Connection, so credentials are required on the server's logon UI (instead of being passed in from the client), and the session disconnects due to network issues, reconnecting the session requires you to enter the credentials on the server again. [#189338]

- If you embed the .ica file in an .html file, the .ica file does not launch when you access the .html file from a Web browser. To launch the embedded .ica file, add the .ica Multipurpose Internet Mail Extensions (MIME) type to the Internet Information Services (IIS) settings. [#195572]

  Workaround:

  1. Launch Internet Information Services (IIS) Manager and select **Default Web Site**.
  2. Under the **IIS** section, select **MIME Types**.
  3. In the **Action** section, select **Add.**
  4. In the **File** name extension field, type **.ica**.
  5. In the **MIME type** field, type **text/html**.
- Note that this issue does not occur on client devices with nonseamless desktops. Users with multiple client devices configured for mixed single and multimonitor environments and full-screen or custom desktops may experience unusual behavior when maximizing an application. This issue occurs when a user maximizes an application on a single-monitor client device, disconnects, and then reconnects to open the same application on a multimonitor device. When the user maximizes the application, it maximizes on all monitors. There is no workaround for this issue. [#196014]

- Client devices with multiple monitors that are configured in nonstandard monitor configuration or geometry might experience errors when streaming audio files from a Windows Media Player installed on Windows Server 2008. For example, this issue can occur when the monitors have different display resolutions or layouts. Note that this issue can occur whether or not you enable SpeedScreen Multimedia Acceleration. [#194652]

- When a client-side proxy is configured and the XenApp Plugin attempts to connect to a Secure Gateway host using IPV6, the plugin fails to communicate using IPV6 and attempts to connect using IPV4. However, if the XenApp plugin is able to resolve the

IPV6 address of the Secure Gateway host, the plugin bypasses the client-side proxy and connects directly to the Secure Gateway host using IPV6. [#196978]

Known Issues for the Citrix XenApp Plugin for Streamed Apps

- By default, you cannot install the XenApp Plugin for Streamed Apps and Streaming Profiler 1.2 for Windows on Microsoft Vista Home Edition and XP Home Edition operating systems. For supported platforms, refer to the Installation Checklist. For more information and a possible (unsupported) workaround, see http://support.citrix.com/article/CTX118086.

- When streaming applications using XenDesktop, the Citrix Streaming Service on client devices (endpoint devices and target devices) might use 100% of the CPU processing resources and the system freezes. To prevent this issue, when you create a virtual desktop image as part of a XenDesktop deployment, do not copy the following registry keys to the default user profile:

  HKEY_CURRENT_USER\Software\Citrix\Rade

  HKEY_CURRENT_USER\Software\Citrix\

  Additionally, using Standard Images for Citrix Provisioning Server with XenDesktop may cause significantly longer launch times of streamed applications every time after logon, sometimes taking as long as a first-time application launch. The CPU usage by the Streaming Service may also jump to 100% and remain at this level for several minutes because of first-time launch operations. To prevent this issue, use Private Images to preserve first-time launch changes. Consult the Citrix XenApp documentation library for information about related products and instructions for using their features. [#196274]

- To stream applications through Web Interface to users with a Firefox browser, follow these recommendations:

  1. Install the XenApp Plugin for Streamed Apps after they install the Firefox browser. If the plugin is installed before the browser, the browser might not detect the plugin and present a message that the plugin is not installed.

     Alternatively, if the XenApp Plugin for Streamed Apps is already installed before they install Firefox, they should rerun XenAppStreaming.exe after installing Firefox to repair the plugin's installation on the client device.

  2. Add the Web Interface site to the Trusted Sites list in Microsoft Internet Explorer. [#192295]
- When the following combination of conditions exist, applications configured for HTTP protocol fail to stream through an HTTP site: Anonymous access is disabled, the authentication method is set to Integrated Windows Authentication in IIS, and users are not logged in as a domain user. In this situation, the XenApp Plugin for Streamed Apps

does not prompt for credentials, and the application does not launch. As a workaround, ensure that users are members of the Domain Users group. [#189503]

- On Windows Vista, XP, Server 2003, and Server 2008 client devices, launched streamed applications are not included in the list of recently used applications on the Start menu. This is a third party issue and there is no workaround at this time. [#184061]

- If users must work with streamed versions of both Microsoft Office 2003 and 2007, they must configure Outlook 2003 before configuring 2007. This sequence is necessary for both address books to work correctly. [#175702]

- Users with Skype software installed locally and streamed Microsoft Outlook might experience Outlook failure if the Skype application attempts to interact with the Outlook contacts and calendar list. To prevent this, from the Skype View menu, clear the option to Show Outlook Contacts. [#180241]

- If you install both the XenApp Plugin for Streamed Apps and the Virtual Desktop Agent, and then you uninstall either one of them, you must repair or reinstall the other. This issue occurs because the two components share registry entries. [#193172]

- To run streamed applications offline, client devices must have the current plugins installed; that is, the XenApp Plugin for Streamed Apps 1.2 and XenApp Plugin for Hosted Apps 11.x, available with this release. In particular, previous releases of Program Neighborhood Agent, including 10.x, do not support offline access when used with Version 1.2 of the XenApp Plugin for Streamed Apps (formerly called the Streaming Client). [#196836 and #188888]

- When users clear the cache for Microsoft Outlook using the RadeCache /flushall command, this action clears the user root where Outlook stores the information about the .ost file. Thus reopening Outlook creates another .ost file. This issue occurs even when users uninstall and reinstall the XenApp Plugin for Streamed Apps.

  To prevent this problem, instead of using RadeCache to removed the streamed Outlook, users should manually delete the .ost file on the client device. This file is located in C:\Users\%user%\AppData\Local\Microsoft\Outlook\. [#193655]

- When streaming any Office application to a Microsoft Vista platform, users cannot delete a file using the Open File dialog box. Attempting to do causes an error message stating that the recycle bin is corrupted. If this occurs, users can disregard this message. The recycle bin is neither corrupted nor related to the Office application. [#172666]

Documentation Errata

Document Library (Online Help)

Some of the procedures documenting configuration changes using the Group Policy editor specify an incorrect path.

The correct path is:

Classic Administrative Templates (ADM) > Citrix Components > Citrix XenApp Plugin for Hosted Apps > *rest of path*. [#196596]

Citrix XenApp Plugin for Hosted Apps for Windows Administrator's Guide

The paragraphs describing how to enable or disable session reliability using Program Neighborhood in the section "Providing Session Reliability" on page 52 of the PDF version of the guide should be:

Users of Program Neighborhood can control session reliability in their application set or custom connection settings. To enable session reliability in Program Neighborhood, select **Enable session reliability** on the **Options** tab of the settings for a particular application set or custom connection (enabled by default). Session reliability does not work if it is disabled on either the Program Neighborhood plugin connection or the server.

Users of Citrix XenApp and Citrix XenApp Web Plugin cannot override the server settings for session reliability.

Deciding Which Plug-in to Use

Different enterprises have different corporate needs, and your expectations and requirements for the way users access your published resources can shift as your corporate needs evolve and grow.

The plug-ins are:

- Citrix XenApp (formerly named Program Neighborhood Agent)
- Program Neighborhood
- Citrix XenApp Web Plug-in (formerly named the Web Client)

Each of the plug-ins differs in terms of:

- Access method by which published resources are delivered to users. Resources can be delivered to users by three different methods—through a Web browser, through a user interface, or on the desktop.
- Extent of user involvement in configuring, administering, and managing the plug-in.
- Support for the XenApp feature set. For a complete list of Citrix XenApp features, refer to the Plug-in Feature Matrix available from the Plug-in Download page of the Citrix Web site (http://www.citrix.com/).

To decide which plug-in best fits your needs, consider the way you want users to access your published resources, the way you want to manage this access, and the feature set that your users will need.

Plug-in	Access method	User involvement	Plug-in features
Citrix XenApp	Transparent integration of published resources into user's desktop	Central administration of user settings	Supports the full feature sets of XenApp server.
Citrix XenApp Web Plug-in	Web browser-based access to published resources	Central administration of user settings	Supports the full feature sets of XenApp server.
Program Neighborhood	An interface users access from their desktops	Requires initial user configuration	Supports the full feature sets of XenApp server except for zone preference and failover.

Citrix XenApp Plug-in Overview

Citrix XenApp supports the full XenApp feature set. Using Citrix XenApp with the Web Interface, you can integrate published resources with users' desktops. Depending on the version of XenApp server you have installed, centrally administer and configure the plug-in in the Access Management Console or Delivery Services Console using a Citrix XenApp site created in association with a site for the server running the Web Interface.

Citrix XenApp is one of two plug-ins (the other being the Citrix XenApp Web Plug-in) that operates with the Citrix XenApp Streaming Plug-in, to provide application streaming to the user desktop. Install Citrix XenApp on client devices running the Citrix XenApp Streaming Plug-in to take advantage of the full set of application streaming features of the XenApp plug-in and Citrix XenApp. For more information about the streamed application feature, see the Application Streaming documentation at Citrix eDocs.

Important: Citrix XenApp requires the Citrix Web Interface.

How Published Resources are Accessed with Citrix XenApp

Citrix XenApp allows your users to access all of their published resources from a familiar Windows desktop environment. Users work with your published resources the same way they work with local applications and files. Published resources are represented throughout the client desktop, including the Start menu and the Windows notification area, by icons that behave just like local icons. Users can double-click, move, and copy icons, and create shortcuts in their locations of choice. Citrix XenApp works in the background. Except for a shortcut menu available from the notification area, it does not have a user interface.

Citrix XenApp Management and Administration

You configure Citrix XenApp at a site created in the consoles and associated with the site for the server running the Web Interface. By using the consoles in this way, you can manage and control your client population dynamically throughout your network from a single location and in real time.

Citrix XenApp Web Plug-in Overview

Citrix XenApp Web Plug-in is a smaller plug-in that can be installed from the XenAppWeb.msi or the XenAppWeb.exe file. Citrix XenApp Web Plug-in setup files are significantly smaller than those for the other plug-ins. The small size allows users to download and install the plug-in software quickly.

How Published Resources are Accessed with Citrix XenApp Web Plug-in

If you want users to access published resources from within a familiar browser environment, use Citrix XenApp Web Plug-in. Users access published resources by clicking links on a Web page you publish on your corporate intranet or the Internet. The published resource launches either in the same window or in a new, separate browser window. Citrix XenApp Web Plug-in does not require user configuration and does not have a user interface.

Citrix XenApp Web Plug-in Management and Administration

You can use Citrix XenApp Web Plug-in to access resources available from the Web Interface and for access to resources published with traditional Application Launching and Embedding (ALE). Publish links to your resources with the Web Interface or by using an HTML wizard.

This plug-in requires the presence on client devices of Microsoft Internet Explorer 6.0 or 7.0; or Mozilla Firefox 1.0 and later.

Program Neighborhood Overview

Program Neighborhood supports the full XenApp feature set and it requires user configuration and maintenance. Use Program Neighborhood if you are not using the Web Interface to deliver resources. Program Neighborhood cannot be configured from a centralized site, such as the Citrix XenApp site; thus, it does not require the Web Interface.

Program Neighborhood does not support zone preference and failover on XenApp.

How to Access Published Resources with Program Neighborhood

If you want users to access your published resources from within a distinctive user interface, use Program Neighborhood. Using Program Neighborhood's own user interface, the Program Neighborhood window, users can browse for groups of published resources (referred to as application sets) or create custom connections to individual published resources or to XenApp servers. Icons representing application sets and custom ICA connections appear in the Program Neighborhood window.

Program Neighborhood Management and Administration

You can set up scripted updates for Program Neighborhood using various .ini files and users can also configure options for Program Neighborhood using its interface. For this reason, users running Program Neighborhood must be able to navigate through the interface easily and be able to understand the implications of any changes to their options.

Choose Program Neighborhood if you do not want to publish your resources using the Web Interface. If you choose to implement the Web Interface at a later time, Program Neighborhood users can also access resources published through the Web Interface. However, if you are planning to use the Web Interface and did not deploy any plug-ins, use the Citrix XenApp or Citrix XenApp Web Plug-in.

Citrix Connection Center Overview

The Citrix Connection Center displays all connections established from the online plug-in.

The **Connections** window displays a list of active sessions. Each server entry in the list represents a session. For each seamless session, below each server entry, a list of the published resources you are running on that server appears.

The Connection Center offers various options to view statistics and control sessions and applications:

- Disconnect a session
- Logoff a session
- Switch to full screen mode
- Show connection status details like frames sent and received
- Terminate an application
- Security settings

Delivering the Plug-in Software to Your Users

The Citrix XenApp server installation media contains the installation files for Citrix XenApp Hosted Plug-in in the Clients directory.

These topics describe how to deliver and install your plug-in software. Topics include:

- Ensuring you meet the system requirements
- Packaging the plug-in software
- Configuring the installation package to limit user interaction in the installation process
- Delivering the installation package to users
- Installing the plug-in software; specifically, the options that the Setup wizard presents to your users
- Uninstalling the plug-in software

Before you upgrade the plug-ins, check if your users previously installed the Citrix Streaming Clients Package.msi, which included the client for streaming and the Citrix XenApp Hosted Plug-in (formerly named the Presentation Server Clients). Citrix no longer releases or supports the Streaming Clients package.

If your list of removable programs shows Citrix Streaming Clients for Windows, uninstall that package, and then individually install the current versions of the Citrix XenApp Hosted Plug-in using XenAppHosted.msi, and Citrix XenApp streaming plug-in, using XenAppStreaming.exe.

Packaging the Plug-in Software

You can install the plug-ins using a Microsoft Windows Installer package (MSI). You can allow users to choose their own options when installing or you can preconfigure an MSI package to select certain options in advance. If all options are preconfigured, the install is "silent," requiring no user interaction.

Each installation that includes the plug-ins also includes the Citrix Connection Center, allowing users to see information about their current ICA connections.

Note: If you installed a previous version of the plug-in software on client devices by using the Access Client package, you cannot upgrade the plug-in software using stand-alone plug-in installation software. To install this version of the plug-in software on client devices where the Access Client package is deployed, uninstall the Access Client package first. (Removing the Access Client package removes all previous plug-ins from the client device.)

Creating MSI Packages

The installation packages, XenAppHosted.msi (also called the Client Packager) and XenAppWeb.msi for the Citrix XenApp Web Plug-in, are provided on the installation media. Using the Client Packager, you can wrap all of the plug-ins into a single MSI package. You can customize the Client Packager to deploy and maintain any number and combination of plug-ins network-wide. Based on Windows Installer technology, using the Client Packager you can install, uninstall, modify, and repair plug-ins as well as perform controlled plug-in upgrades.

Important: To install the plug-in software using an MSI package, the Windows Installer Service must be installed on the client device. This service is present by default on systems running Windows XP, Windows Vista, Windows Server 2003, or Windows Server 2008. To install plug-ins on client devices running Windows 2000, you must install the Windows Installer 3.0 Redistributable for Windows, available at http://www.microsoft.com/.

Using an MSI Package to Configure Installation Files

If you choose to use MSI packages to deploy the plug-ins, you can preconfigure numerous settings for your users. You can remove some user interaction in the installation process or all of it; thus enforcing a “silent” installation.

You can configure MSI packages in three ways:

- With the Client Packager
- Using command-line parameters
- Using transforms

To configure an MSI package using the Client Packager

1. Copy the Client Packager (XenAppHosted.msi) from the installation media to a local directory.
2. Create a share point on a file server that is accessible to your users.
3. Type the following at a command prompt:

   msiexec.exe /a *path*/XenAppHosted.msi

   where *path*/ is the local path where you placed this file in Step 1. The Client Packager Setup wizard appears.
4. Enter the Uniform Naming Convention (UNC) path to the network share point where you want to store the customized package.
5. Select your compression option and click **Next**.
6. Select one or more plug-ins to be included in the install package. If you select Program Neighborhood or Citrix XenApp, the Setup wizard for each plug-in appears.
7. On the **Upgrade Settings** page, choose whether or not the install package can upgrade or downgrade existing plug-ins.
8. On the **Select User Dialog Boxes** page, specify the dialog boxes displayed to users when they run the install package.
9. Verify your selections on the summary page and click **Finish**. The install package you specified above is created in the specified UNC path.

To configure the plug-ins using command-line parameters

1. On the computer where you want to install the plug-in package, type the following at a command prompt:

   msiexec.exe /I *path*/XenAppHosted.msi [Options]

   where *path*/ is the location of the MSI package and [Options] can be any of the traditional MSI command-line parameters.

2. Set your options as needed. These are the recommended parameters. See the Microsoft documentation for a complete list of parameters.

   - **/qn** executes a completely silent installation.
   - **/qb** shows simple progress and error handling.
   - **/qb-!** shows simple progress and error handling without displaying a Cancel button to the user.
   - **/l*v** *logfile_path* creates a verbose install log where *logfile_path* is the path and filename for where to save the log. Use quotation marks for a path with spaces.
   - *PROPERTY*=*Value*

     Where PROPERTY is one of the following all-uppercase variables (keys) and Value is the value the user should specify.

     - **PROGRAM_FOLDER_NAME**=*Start Menu Program Folder Name*, where *Start Menu Program Folder Name* is the name of the Programs folder on the Start menu containing the shortcut to the Citrix XenApp software. The default value is **Citrix**. This function is not supported during plug-in upgrades.
     - **INSTALLDIR**=*Installation directory*, where *Installation directory* is the location where the plug-in software is installed. The default value is **C:\Program Files\Citrix\ICA Client**.
     - **CLIENT_NAME**=*ClientName*, where *ClientName* is the name used to identify the client device to the server farm. The default value is **%COMPUTERNAME%**.
     - **ENABLE_DYNAMIC_CLIENT_NAME={Yes | No}**. To enable dynamic client name support during silent installation, the value of the property ENABLE_DYNAMIC_CLIENT_NAME in your installer file must be **Yes**. To disable dynamic client name support, set this property to **No**.
     - **ADDLOCAL=***feature*[,...]. Install one or more of the specified features. When specifying multiple feature parameters, separate each parameter with a comma and without spaces. The names are case sensitive.

ICA_Client. Plug-in engine component (always installs)

PN. Installs Program Neighborhood (not installed by default)

PN_AGENT. Installs Citrix XenApp

WEB_CLIENT. Installs Citrix XenApp Web Plug-in

SSON. Installs the files for pass-through authentication

- **CLIENT_UPGRADE={Yes | No}**. By default, this property is set to **Yes**. This installs the plug-in if an earlier version of the plug-in is already installed.
- **ENABLE_SSON={Yes | No}**. The default value is **No**. If you enable the **SSON** (pass-through authentication) property, set the **ALLOW_REBOOT** property to **No** to avoid automatic restarting of the client system.

  Important: If you disable pass-through authentication, users must reinstall the plug-in if you decide to use pass-through authentication at a later time.
- **ALLOW_REBOOT={Yes | No}**. The default value is **Yes**.
- **DEFAULT_NDSCONTEXT**=Context1 [,…]. Include this parameter if you want to set a default context for Novell Directory Services (NDS). If you are including more than one context, place the entire value in quotation marks and separate the contexts by a comma. Examples of correct parameters:

  DEFAULT_NDSCONTEXT=Context1

  DEFAULT_NDSCONTEXT="Context1,Context2"

  Example of an incorrect parameter:

  DEFAULT_NDSCONTEXT=Context1,Context2
- **SERVER_LOCATION**=*Server_URL*. The default value is **Web Server**. Enter the URL of the server running the Web Interface. The URL must be in the format http://*servername* or https://*servername*.

  Citrix XenApp appends the default path and file name of the configuration file to the server URL. If you change the default location of the configuration file, you must enter the entire new path in the **SERVER_LOCATION** key.
- **CTX_PN_ENABLE_CUSTOMICA = {Yes | No}**. By default, this property is set to **Yes**. Defines whether or not you want to enable the Custom Connection icon in Program Neighborhood.
- **CTX_PN_ENABLE_QUICKLAUNCH = {Yes | No}**. By default, this property is set to **Yes**. Defines whether or not you want to enable the Quick Launch bar in Program Neighborhood.

Example of a Command-Line Installation

Using the above procedure, a command-line configuration of your MSI package could resemble:

```
msiexec.exe /I XenAppHosted.msi /qb-! /l*v “c:\my
logs\ica32_install.log” ADDLOCAL=ICA_Client,PN_AGENT,WEB_CLIENT
SERVER_LOCATION=http://mywebinterface
```

This example:

- Installs defined plug-ins with visible progress dialog boxes, but the Cancel button is disabled for the user
- Logs the installation messages to “c:\my logs\ica32_install.log”
- Installs the plug-in engine, Citrix XenApp, and Citrix XenApp Web plug-in
- Specifies the URL (http://mywebinterface) of the server running the Web Interface that Citrix XenApp will reference

To configure an MSI package using transforms

Important: Transforms manipulate the installation process by making changes to the installation database contained within a Windows Installer package. Do not attempt the following procedure if you are not familiar with transforms and their impact on these settings. For more information, see the *Citrix XenApp Administrator's Guide*.

1. Using your preferred tool for editing Windows Installer packages, open the Client Packager (XenAppHosted.msi).

2. In the Property table, enter new values for the properties you want to change.

3. Generate the transform file and save it with a .mst file extension.

4. To install the MSI package and use the transform you just created, follow the same steps as outlined in To configure the plug-ins using command-line parameters. Additionally, however, you must add the following **TRANSFORMS** = *path*\"*my.mst*" where *path* is the location of the transform and "*my.mst*" is its file name.

Delivering Plug-ins from a Network Share Point

In many environments, your users can access internal resources from network share points. You can centralize your plug-in delivery by deploying an MSI package from a single network share point. Use the Client Packager to configure your installation settings. During this procedure you can provide a UNC path to the network share point where you want to store the customized MSI package.

Note: You can also use Active Directory Group Policy to install the plug-in software or provide the network path to your users. See your Windows or Systems Management Server documentation for more information.

Delivering the XenApp Web Plug-in from a Web Page

The Citrix XenApp installation media also contains the XenAppWeb.exe installation package, which is functionally the same as the XenAppWeb.msi package. The only difference is that you can deploy the XenAppWeb.exe package from a Web page to ensure that users have the plug-in installed before they try to use the Web Interface. Create a home page and run an Internet Explorer script to download the XenAppWeb.exe package automatically from the Web server and install it for the user.

To install the plug-in software using XenAppWeb.exe, the Windows Installer Service must be installed on the client device. This service is present by default on systems running Windows XP, Windows Vista, Windows Server 2003, or Windows Server 2008. To install plug-ins on client devices running Windows 2000, you must install the Windows Installer 3.0 Redistributable for Windows, available at http://www.microsoft.com/.

Add the site(s) from which the XenAppWeb.exe file is downloaded to the Trusted Sites zone.

How Installation Outcomes Differ Based on the Operating System, User Type, and Installation Package

The outcome of XenAppHosted.msi or XenAppWeb.exe package plug-in installations differs based on the combination of the operating system on the client device, user type, whether User Account Control (UAC) is enabled or disabled on Windows Vista and Windows 2008 computers, and which installation package is used.

Operating system and user type	XenAppHosted.msi	XenAppWeb.exe
OS: Windows XP, and Windows Server 2003 **User:** Administrator	**Installation type:** per-computer **Features:** Citrix XenApp, Program Neighborhood, Citrix XenApp Web Plug-in, and pass-through authentication	**Installation type:** per-computer **Features:** Citrix XenApp Web Plug-in
OS: Windows XP, and Windows Server 2003 **User:** Non-administrator	**Installation type:** per-user **Features:** Citrix XenApp Web Plug-in	**Installation type:** per-user **Features:** Citrix XenApp Web Plug-in
OS: Windows Vista and Windows Server 2008 **User:** Built-in administrator with UAC disabled	**Installation type:** per-computer **Features:** Citrix XenApp, Program Neighborhood, Citrix XenApp Web Plug-in, and pass-through authentication	**Installation type:** per-computer **Features:** Citrix XenApp Web Plug-in
OS: Windows Vista and Windows Server 2008 **User:** Built-in administrator with UAC enabled	**Installation type:** per-computer **Features:** Citrix XenApp, Program Neighborhood, Citrix XenApp Web Plug-in, and pass-through authentication	**Installation type:** per-user **Features:** Citrix XenApp Web Plug-in
OS: Windows Vista and Windows Server 2008 **User:** Standard user	Not supported	**Installation type:** per-user **Features:** Citrix XenApp Web Plug-in

Installation Options Available When Using the Setup Wizard

For each MSI package, the Setup wizard guides you through the process of installing the plug-in software. When Setup begins, a series of information pages and dialog boxes prompts you to select options and configure the product. In each installation, you must accept the Citrix License Agreement before Setup continues.

Note: The Canadian keyboard layouts now are aligned with those supported by Microsoft. If users install the plug-ins without uninstalling the Presentation Server Clients Version 10.*x* first, they must manually edit the module.ini file (usually in C:\Program Files\Citrix\ICA Client) to upgrade the keyboard layout settings:

Replace:

Canadian English (Multilingual)=0x00001009

Canadian French=0x00000C0C

Canadian French (Multilingual)=0x00010C0C

With:

Canadian French=0x00001009

Canadian French (Legacy)=0x00000C0C

Canadian Multilingual Standard=0x00011009

Selecting a User Interface Language

The Windows Installer package includes a Multilingual User Interface, meaning it installs the plugins in all supported languages automatically.

During the installation, the user selects a language for the user interface: German (Deutsch), English, Spanish (Español), French (Français), Japanese, Russian, Simplified Chinese, or Traditional Chinese. After the plugin is installed, the user interface appears in the language stored in the ICA_UILocale registry value. If the value does not exist or has no data, the user interface language of the plugin is determined by the following factors, in order:

- The UILocale ICA parameter defined in the ICA file is checked if an ICA session is getting started
- If the language specified in the UILocale ICA parameter is not supported, the user's default language is checked
- If the user's default language is not supported, the system's default language is checked
- If the system's default language is not supported, the user interface defaults to English

Options Displayed When Installing the Citrix XenApp Plug-in

When users install Citrix XenApp, they are presented with the following options:

Upgrade existing plug-in software. Setup searches the client device for previously installed versions of Citrix XenApp. If Setup detects a previous installation of Citrix XenApp, the user can upgrade Citrix XenApp. The default value is Upgrade the existing plug-in. If you are upgrading with the MSI package, you are not presented with any further options.

Select Program Folder. Users can choose to use the default plug-in folder, specify the name of a new program folder, or add the Citrix XenApp icon to an existing folder.

Specify the Server Address. Users must enter the URL of the appropriate server running the Web Interface in the format http://*servername* (for non-secure connections) or https://*servername* (for secure connections). Citrix XenApp connects to the server at startup to get the latest configuration information including available published resources and permissions to change local settings.

Enable Pass-Through Authentication. Users must select whether or not to enable and use their local user credentials automatically for Citrix sessions from the plug-in being installed. Pass-through authentication allows the plug-in to access a user's local Windows user name, password, and domain information and pass it to the server. Users are not prompted to log on to Citrix XenApp separately. You must enable this logon mode using the Web Interface to make it available to users.

Important: If users do not enable pass-through authentication during the installation process, they must reinstall Citrix XenApp if they decide to use pass-through authentication at a later time.

Specify the Client Name. Servers use the client name to manage system resources. By default, the computer name is used as the client name. If you do not assign a unique computer name to each client device, device mapping and application publishing might not operate correctly.

Important: The client name cannot contain the following characters:\/:*?"<>|,.()[]. A blank client name (or a missing registry key) uses the client's computer name as the client name. The client name must be fewer than 20 bytes.

Specifying Backup Server Addresses

The Web Interface lets you specify backup servers to contact if Citrix XenApp cannot access the primary Web Interface server. If backup URLs are specified in the Web Interface configuration, those addresses take precedence and are specific to individual users. For more information, see the Web Interface administrator documentation in eDocs.

Installing Citrix XenApp Web Plug-in

Installing the Citrix XenApp Web Plug-in requires minimal user interaction. After a user accepts the Citrix License Agreement, Setup copies files to the client device. By default, the Citrix XenApp Web Plug-in is installed in the Program Files\Citrix\ICA Client directory.

Installing Program Neighborhood

When users install Program Neighborhood, they are presented with the following options:

Upgrade existing plug-in software. Setup searches the client device for previously installed versions of Program Neighborhood. If Setup detects a previous installation of Program Neighborhood, the user can upgrade the existing plug-in. The default value is **Upgrade the existing client**. If you are upgrading with the MSI package, you are not presented with any further options.

Choose Destination Location and Select Program Folder. Users can change the default installation path and the default Program folder.

Specify Client Name. XenApp servers use the client name to manage system resources. By default, the computer name is used as the client name. If you do not assign a unique computer name to each client device, device mapping and application publishing may not operate correctly.

Program Neighborhood Options. Users can enable the Program Neighborhood Quick Launch Bar and Custom ICA Connections. These provide additional methods to connect to the server. By default, both of these options are enabled.

Enable Pass-Through Authentication. Users must select whether or not to enable and use their local user credentials automatically for Citrix sessions from the plug-in being installed. Pass-through authentication allows the plug-in to access a user's local Windows user name, password, and domain information and pass it to the server. Users are not prompted to log on to Program Neighborhood separately.

Important: If users do not enable pass-through authentication during the installation process, they must reinstall Program Neighborhood if they decide to use pass-through authentication at a later time.

Uninstalling the Plug-in Software

To uninstall a plug-in, run the Add/Remove Programs utility from the Control Panel on Windows XP, Windows 2000, or Windows Server 2003. Run the Programs and Features utility from the Control Panel on Windows Vista and Windows Server 2008. Alternatively, if the plug-in was installed or upgraded using a Windows Installer package, you can run the installer package again and select the **Remove** option.

After uninstalling the plug-in software from a client device, manually delete any user-created Citrix XenApp and Program Neighborhood shortcut icons from the desktop, Start menu, and Quick Launch Bar.

Caution: Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

After uninstalling the plug-in software from a client device, the custom client-setting registry keys created by icaclient.adm remain in the Software\Policies\Citrix\ICA Client directory under HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER. If you reinstall the client, these policies might be enforced, possibly causing unexpected behavior. If you want to remove these customizations, delete them manually.

Configuring Plug-in Software

After plug-in software is deployed to your users and they install it, there are configuration steps that can be performed for Citrix XenApp and Program Neighborhood. The Citrix XenApp Web Plug-in does not require configuration.

Configuring Citrix XenApp Plug-in

Depending on the version of the XenApp server you have installed, configure the options and settings for Citrix XenApp using the associated Citrix XenApp site in the Access Management Console or Delivery Services Console. Each time users log on to Citrix XenApp, they see the most recent Citrix XenApp configuration. Changes made while users are connected take effect when the plug-in configuration is refreshed manually or automatically after a designated interval.

Important: Citrix XenApp requires the Citrix Web Interface.

Citrix XenApp handles the following functions:

- **User authentication.** The plug-in provides user credentials to the Web Interface when users try to connect and every time they launch published resources.
- **Application and content enumeration.** The plug-in presents users with their individual set of published resources.
- **Application launching.** The plug-in is the local engine used to launch published applications.
- **Desktop integration.** The plug-in integrates a user's set of published resources with the user's desktop.
- **User preferences.** The plug-in validates and implements local user preferences.

For a complete list of Citrix XenApp features, refer to the Plug-in Feature Matrix available from the Plug-in Download page of the Citrix Web site (*http://www.citrix.com/*).

Using the Group Policy Object Template to Customize Citrix XenApp

Citrix recommends using the Group Policy Object icaclient.adm template file to configure the Citrix XenApp options and settings.

You can use the icaclient.adm template file with domain policies and local computer policies. For domain policies, import the template file using the Group Policy Management Console. This is especially useful for applying plug-in settings to a number of different client devices throughout the enterprise. To affect a single client device, import the template file using the local Group Policy Editor on the device.

For details about Group Policy management, see the Microsoft Group Policy documentation.

To import the icaclient template using the Group Policy Management Console

To affect domain-based group policies, import the icaclient.adm file with the Group Policy Management Console.

1. As an administrator, open the Group Policy Management Console.
2. In the left pane, select a group policy and from the **Action** menu, choose **Edit**.
3. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
4. From the **Action** menu, choose **Add/Remove Templates**.
5. Choose **Add** and browse to the Configuration folder for the plug-ins (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
6. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

To import the icaclient template using the local Group Policy Editor

To affect the policies on a local computer, import the icaclient.adm file with the local Group Policy Editor.

1. As an administrator, open the Group Policy Editor by running gpedit.msc from the Start menu.
2. In the left pane, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the Configuration folder for the plug-ins (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

To customize user preferences for Citrix XenApp

Users can customize their preferences. For example, they can define window sizes for published applications, choose when to refresh the list of available published resources, and specify where the available published resources appear.

1. In the Windows notification area, right-click the **Citrix XenApp** icon and choose **Options** from the menu that appears.

2. On the **Options - Citrix XenApp** page, select a property and make the desired configuration changes.

If you configure seamless windows and set the task bar to Auto-hide, you cannot access the taskbar when you maximize published applications. To access the taskbar, resize the published application.

For more detailed information, see the online help for the Citrix XenApp.

To change the server URL in Citrix XenApp

Citrix XenApp requires that you specify the location of a configuration file (Config.xml is the default configuration file) on the server running the Web Interface. You can ask your users to change the server URL as you create new configuration files or delete old ones.

Note: To prevent users from accidentally changing their server URL, disable the option.

1. In the Windows notification area, right-click the **Citrix XenApp** icon and choose **Change Server**. The **Change Server** dialog box displays the currently configured URL.

2. Type or select the server URL in the format http://*servername* or, to encrypt the configuration data using SSL, https://*servername*.

Configuring Program Neighborhood

Unlike Citrix XenApp, Program Neighborhood cannot be administratively configured in the Access Management Console or Delivery Services Console. You must configure options for Program Neighborhood using its user interface. For this reason, users running Program Neighborhood must be able to navigate through the interface easily and be able to understand the implications of any changes to their options.

For step-by-step instructions about how to configure Program Neighborhood, see the Program Neighborhood online help.

Using Application Sets or Custom ICA Connections to Connect to Published Resources

With Program Neighborhood, users can connect to published resources and XenApp servers using:

- Application sets
- Custom ICA connections

Application Sets

An *application set* is a user's view of the resources published on a given server farm that the user is authorized to access. Resources published in an application set are preconfigured for such session properties as window size, number of colors, supported encryption levels, and audio compression rate.

Users can change nonessential settings of a published application (for example, the audio compression rate) at an application set level on the client device.

Application set functionality is not available for applications published on servers running UNIX. To connect to an application published on these servers, users must create a custom ICA connection.

Custom ICA Connections

A *custom ICA connection* is a user-defined shortcut to a published application or server desktop. While you can create custom ICA connections to connect to any server desktop or published application, you must use custom ICA connections to connect to:

- A XenApp server outside of a server farm scope of management
- An application published prior to the installation of a MetaFrame 1.8 server that cannot be migrated into a server farm
- An application published on a server running UNIX

Applications published in this way are not enabled for automatic configuration of Program Neighborhood sessions.

With Program Neighborhood, users can connect to a server in the server farm using the local or wide-area network connection between the client device and the server. This method uses one of the following network protocols:

- TCP/IP+HTTP
- SSL/TLS+HTTPS
- TCP/IP

Remote users can connect to servers running Windows Server 2003 over TCP/IP only.

Note: The supported width and height values when specifying the custom window size in a custom ICA connection **Properties > Option** dialog box are in the range of 64 to 16384.

ICA Browsing

ICA browsing is a process in which a plug-in transmits data to locate servers on the network and get information about the applications published in the server farm.

For ICA browsing, plug-ins communicate with the Citrix XML Service or the ICA browser, depending on the browsing protocol selected in the plug-in.

ICA browsing occurs when:

- Users launch published applications. The plug-in sends a request to locate the application on a server.
- Program Neighborhood users display the Application Set list in the Find New Application Set wizard.
- Program Neighborhood users display the Server or Published Application list in the Add New ICA Connection wizard to create a custom ICA connection.

For more information about the Citrix XML Service, see the Citrix XenApp Administrator's documentation in Citrix eDocs.

Specifying the Network Protocol for ICA Browsing

Changing the network protocol setting allows you to control the way the plug-in searches for XenApp servers and how it communicates with them.

You can choose from three network protocol options for ICA browsing: SSL/TLS+HTTPS, TCP/IP+HTTP, and TCP/IP. The network protocol you select depends on how your plug-ins connect to XenApp servers.

For step-by-step instructions about configuring the network protocol, see the Program Neighborhood online help.

Important: SSL/TLS+HTTPS or TCP/IP+HTTP retrieves information only on a per-server farm basis. To retrieve information from more than one server farm, you must configure server location settings for each application set. For custom ICA connections, you must configure server location settings for each ICA connection. Do not place addresses from separate farms in the same server location list.

Using TCP/IP+HTTP for ICA Browsing

Program Neighborhood uses TCP/IP+HTTP as the default network protocol. The plug-in uses the HTTP protocol to search for XenApp servers. Select this protocol when plug-ins connect over the Internet or through a firewall or proxy server.

Using the TCP/IP+HTTP protocol for ICA browsing provides the following advantages for most server farms:

- TCP/IP+HTTP uses XML data encapsulated in HTTP packets that the plug-in sends to port 80 by default. Most firewalls are configured so port 80 is open for HTTP communication.
- TCP/IP+HTTP does not use User Datagram Protocol (UDP) or broadcasts to locate servers in the server farm.
- Routers pass TCP/IP packets between subnets, which allows plug-ins to locate servers that are not on the same subnet.

By default, if no server is specified, the plug-in attempts to resolve the name **ica** to an IP address. This is indicated by the virtual server location **ica** in the Address List box. This feature allows the Domain Name Service (DNS) or Windows Internet Naming Service (WINS) administrator to configure a host record that maps **ica** to a valid server IP address that can service XML requests from plug-ins.

You must map a XenApp server to the default name of **ica** on your network or you must specify at least one IP address in Program Neighborhood.

You can configure the DNS server for the plug-ins to use round-robin DNS to map the name **ica** to a set of servers that can service the XML requests. Use this approach to avoid individually configuring server location addresses on your client devices.

You can specify servers to contact for ICA browsing by entering IP addresses or DNS names of XenApp servers in the Address List box in Program Neighborhood. You can define up to three groups of servers: a primary and two backups. Each group can contain from one to five servers. When you specify a server group for your plug-in, the plug-in attempts to contact all the servers within that group simultaneously and the first server to respond is the one to which you connect.

To locate the Citrix XML Service, the plug-in makes an HTTP connection to port 80 on the XenApp server. If the user is launching a published application, for example, Citrix XML Service sends to the plug-in the address of a XenApp server that has the published application.

Using SSL/TLS+HTTPS for ICA Browsing

With SSL/TLS+HTTPS as the network protocol, the plug-in uses the HTTPS protocol to search for a list of XenApp servers. The plug-in communicates with the server using ICA with SSL/TLS. SSL/TLS+HTTPS provides strong encryption of ICA traffic and server authentication. Select this option when using SSL or TLS communication over the Internet or through a firewall or proxy server.

Important: By default, Internet Information Services (IIS) and SSL/TLS for ICA connections are set to port 443. If your users are configured to use port 443 for IIS, you must specify another port number for SSL Relay after you install the certificate for SSL/TLS.

If you select SSL/TLS+HTTPS as the network protocol, you must enter the fully qualified domain name (FQDN) of the server hosting the digital certificate.

The TCP/IP+HTTP and SSL/TLS+HTTPS protocols can be used only with a compatible XenApp server. See the Citrix XenApp server administrator documentation at Citrix eDocsfor Windows or UNIX for information about configuring the server to use SSL/TLS.

Using TCP/IP+HTTP for ICA Browsing

Program Neighborhood uses TCP/IP+HTTP as the default network protocol. The plug-in uses the HTTP protocol to search for XenApp servers. Select this protocol when plug-ins connect over the Internet or through a firewall or proxy server.

Using the TCP/IP+HTTP protocol for ICA browsing provides the following advantages for most server farms:

- TCP/IP+HTTP uses XML data encapsulated in HTTP packets that the plug-in sends to port 80 by default. Most firewalls are configured so port 80 is open for HTTP communication.
- TCP/IP+HTTP does not use User Datagram Protocol (UDP) or broadcasts to locate servers in the server farm.
- Routers pass TCP/IP packets between subnets, which allows plug-ins to locate servers that are not on the same subnet.

By default, if no server is specified, the plug-in attempts to resolve the name **ica** to an IP address. This is indicated by the virtual server location **ica** in the Address List box. This feature allows the Domain Name Service (DNS) or Windows Internet Naming Service (WINS) administrator to configure a host record that maps **ica** to a valid server IP address that can service XML requests from plug-ins.

You must map a XenApp server to the default name of **ica** on your network or you must specify at least one IP address in Program Neighborhood.

You can configure the DNS server for the plug-ins to use round-robin DNS to map the name **ica** to a set of servers that can service the XML requests. Use this approach to avoid individually configuring server location addresses on your client devices.

You can specify servers to contact for ICA browsing by entering IP addresses or DNS names of XenApp servers in the Address List box in Program Neighborhood. You can define up to three groups of servers: a primary and two backups. Each group can contain from one to five servers. When you specify a server group for your plug-in, the plug-in attempts to contact all the servers within that group simultaneously and the first server to respond is the one to which you connect.

To locate the Citrix XML Service, the plug-in makes an HTTP connection to port 80 on the XenApp server. If the user is launching a published application, for example, Citrix XML Service sends to the plug-in the address of a XenApp server that has the published application.

To configure settings for multiple users and devices

In addition to the configuration options offered by the plug-in user interface, you can use the Group Policy Editor and the icaclient.adm template file to configure settings. Using the Group Policy Editor, you can:

- Extend the icaclient template to cover any plug-in setting by editing the icaclient.adm file. See the Microsoft Group Policy documentation for more information about editing .adm files and about applying settings to particular computer.
- Make changes that apply only to either specific users or all users of a client device.
- Configure settings for multiple client devices

Citrix recommends using Group Policy to configure client devices remotely; however you can use any method, including the Registry Editor, which updates the relevant registry entries.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.
3. From the **Action** menu, choose **Add/Remove Templates**.
4. Choose **Add** and browse to the Configuration folder for the plug-ins (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.
5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.
6. Under the **User Configuration** node or the **Computer Configuration** node, edit the relevant settings as required.

Optimizing the Plug-in Environment

The ways you can optimize the environment in which your Citrix XenApp Plug-in for Hosted Apps operates include:

- Securing your connections
- Improving performance
- Improving performance over low bandwidth
- Facilitating the connection of numerous types of client devices to published resources
- Improving the user experience
- Providing support for NDS users
- Using connections to Citrix XenApp for UNIX
- Supporting naming conventions
- Supporting DNS naming resolution

Securing Your Connections

To maximize the security of your environment, the connections between the clients and the resources you publish must be secured. You can configure various types of authentication for your plug-in software, including enabling certificate revocation list checking, enabling smart card support, and using Security Support Provider Interface/Kerberos Pass-Through Authentication.

Windows NT Challenge/Response (NTLM) Support for Improved Security

Support for networks using Windows NT Challenge/Response (NTLM) for security and authentication was introduced in Version 7.0 of the clients. NTLM authentication is supported by default on computers running Windows NT, Windows 2000, Windows XP, Window Vista, Windows Server 2003, and Windows Server 2008.

To enable certificate revocation list checking for improved security with the Web plug-in

When certificate revocation list (CRL) checking is enabled, the plug-ins check whether or not the server's certificate is revoked. By forcing plug-ins to check this, you can improve the cryptographic authentication of the XenApp server and the overall security of the SSL/TLS connections between a client device and a XenApp server.

You can enable several levels of CRL checking. For example, you can configure the plug-in to check only its local certificate list or to check the local and network certificate lists. In addition, you can configure certificate checking to allow users to log on only if all CRLs are verified.

Important: This option is available only with the Web plug-in.

If you are making this change on a local computer, exit the plug-in if it is running. Make sure all plug-in components, including the Connection Center, are closed.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the Configuration folder for the plug-ins (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **Network routing > TLS/SSL data encryption and server identification**.

7. From the **Action** menu, choose **Properties** and select **Enabled**.

8. From the **CRL verification** drop-down menu, select one of the options.

   - **Disabled.** No certificate revocation list checking is performed.

- **Only check locally stored CRLs.** CRLs that were installed or downloaded previously are used in certificate validation. Connection fails if the certificate is revoked.
- **Require CRLs for connection.** CRLs locally and from relevant certificate issuers on the network are checked. Connection fails if the certificate is revoked or not found.
- **Retrieve CRLs from network.** CRLs from the relevant certificate issuers are checked. Connection fails if the certificate is revoked.

If you do not set **CRL verification**, it defaults to **Only check locally stored CRLs** for Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

Smart Card Support for Improved Security

XenApp smart card support is based on Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. XenApp supports only smart cards and smart card devices that are, themselves, supported by the underlying Windows operating system. A discussion of security issues related to PC/SC standards compliance is beyond the scope of this document.

Enabling smart card support for Citrix XenApp is done through the Web Interface. For more information, see the Web Interface Administrator's documentation at Citrix eDocs. However, smart card-based logon for Program Neighborhood is configured locally on the client device.

Note: Microsoft strongly recommends that only smart card readers tested and approved by the Microsoft Windows Hardware Quality Lab (WHQL) be used on computers running qualifying Windows operating systems. See http://www.microsoft.com for additional information about hardware PC/SC compliance.

XenApp does not control smart card PIN management. PIN management is controlled by the cryptographic service provider for your cards.

To select smart card-based logon (Program Neighborhood)

1. For an application set, select the application set and click **Properties** on the Program Neighborhood toolbar. For a custom ICA connection, select the custom ICA connection and click **Settings** on the Program Neighborhood toolbar.

2. From the **Logon Information** tab, select **Smart Card**.

3. Select **Pass-through authentication** to cache the PIN and pass it to the server every time the user requests a published resource.

Using Security Support Provider Interface/Kerberos Pass-Through Authentication for Improved Security

Rather than sending user passwords over the network, Kerberos pass-through authentication leverages Kerberos authentication in combination with Security Support Provider Interface (SSPI) security exchange mechanisms. Kerberos is an industry-standard network authentication protocol built into Microsoft Windows operating systems.

Kerberos logon offers security-minded users or administrators the convenience of pass-through authentication combined with secret-key cryptography and data integrity provided by industry-standard network security solutions. With Kerberos logon, the plug-in does not need to handle the password and thus prevents Trojan horse-style attacks on the client device to gain access to users' passwords.

Users can log on to the client device with any authentication method; for example, a biometric authenticator such as a fingerprint reader, and still access published resources without further authentication.

System requirements. Kerberos logon requires Citrix Presentation Server 3.0, 4.0, or 4.5, Citrix XenApp 5.0, and Citrix Presentation Server Clients for Windows 8.*x*, 9.*x*, 10.*x* or XenApp Hosted Plug-in 11.*x*. Kerberos works only between clients and servers that belong to the same or to trusted Windows 2000, Windows Server 2003, or Windows Server 2008 domains. Servers must also be *trusted for delegation*, an option you configure through the Active Directory Users and Computers management tool.

Kerberos logon is not available in the following circumstances:

- Connections configured with any of the following options in Terminal Services Configuration:
  - **On the General tab**, the **Use standard Windows authentication** option
  - On the **Logon Settings** tab, the **Always use the following logon information** option or the **Always prompt for password** option
- Connections you route through the Secure Gateway for XenApp
- If the server requires smart card logon
- If the authenticated user account requires a smart card for interactive logon

Important: SSPI requires XML Service DNS address resolution to be enabled for the server farm, or reverse DNS resolution to be enabled for the Active Directory domain. For more information, see the Citrix XenApp administrator documentation in Citrix eDocs.

Configuring Kerberos Authentication

The plug-in, by default, is not configured to use Kerberos authentication when logging on to the server. You can set the plug-in configuration to use Kerberos with or without pass-through authentication. Using Kerberos without pass-through authentication is more secure than using Kerberos with pass-through authentication. The configuration you choose also depends on your deployment, because Kerberos without pass-through authentication is supported only for the Web Interface and Program Neighborhood.

To use Kerberos authentication for your connections, you can either create and install a custom plug-in installation package or configure the plug-in using the Group Policy Editor. See the Microsoft Group Policy documentation for more information about editing .adm files

To configure Kerberos without pass-through authentication

With this configuration, the user logs on using Kerberos authentication only. If Kerberos logon fails for any reason, the user is prompted for credentials. Kerberos can fail due to a missing operating system requirement, such as the requirement that the server be trusted for delegation.

Note: This configuration is supported only for the Web Interface and Program Neighborhood.

To deploy Kerberos without pass-through authentication, Citrix recommends that you create a "Kerberos only" plug-in package using the Client Packager. To create a plug-in package, you can execute Autorun.exe on the installation media and select the option to create a custom Windows plug-in installation package. During Setup, configure plug-ins to use the local name and password to log on and select the option **Use Kerberos only**.

Note: During the Client Packager Setup, you can select dialog boxes that you want to be displayed to users. Accept the default configuration - **Single Sign On** dialog box is **Hidden**. Otherwise, users can override your configuration and set their plug-in configuration to use pass-through authentication.

You can also configure Kerberos without pass-through authentication by using the Group Policy Editor. You must make the modification on each client device for which you want to use Kerberos without pass-through authentication. To do so more easily, use the Group Policy Management Console to apply the modification to the group of client devices.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **User authentication** > **Kerberos authentication**.

7. From the **Action** menu, choose **Properties** and select **Enabled**.

To configure Kerberos with pass-through authentication

You must use Kerberos with pass-through authentication if you want to use Kerberos with Citrix XenApp.

When plug-in configurations are set to use Kerberos with pass-through authentication, the plug-in attempts to use Kerberos authentication first and uses pass-through authentication if Kerberos fails.

Caution: This configuration is less secure than using Kerberos without pass-through authentication. The user cannot disable this plug-in configuration from the user interface.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates**, navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **User authentication**, double click **Kerberos authentication** and select **Enabled**.

7. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **User authentication** > **Local user name and password**.

8. From the **Action** menu, choose **Properties** and select **Enabled** > **Enable pass-through authentication**.

To apply the setting, close and restart Citrix XenApp on the client device.

Improving Plug-in Performance

You can improve the performance of your plug-in software by:

- Enabling SpeedScreen Browser Acceleration
- Enabling auto-plugin reconnections
- Providing session reliability
- Enabling the Program Neighborhood Quick Launch Bar

To increase image download speed by enabling SpeedScreen Browser Acceleration

For users running Internet Explorer 5.5 through 7.0, you can enhance the speed at which images are downloaded and displayed by using the SpeedScreen Browser Acceleration feature.

You must enable SpeedScreen Browser Acceleration on the server for it to be available on the client device. If SpeedScreen Browser Acceleration is enabled on the client device but not the server, SpeedScreen Browser Acceleration is effectively disabled.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plugin Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **User Experience** > **Client graphic settings**.

7. From the **Action** menu, choose **Properties**, select **Enabled**, and choose the desired SpeedScreen options.

Reconnecting Users Automatically

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the autoplug-in reconnection feature, the plug-in can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically.

When this feature is enabled on the server, users do not have to reconnect manually to continue working. The plug-in attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. If user authentication is required, a dialog box requesting credentials appears to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off. Users can reconnect only to disconnected sessions.

To disable autoplug-in reconnect for a particular user

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plug-in for Hosted Apps** > **Network Routing** > **Session reliability and automatic reconnection**.

7. From the **Action** menu, choose **Properties** and select **Disabled**.

Providing Session Reliability

With the session reliability feature, users continue to see a published application's window if the connection to the application experiences an interruption. For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

You can configure your system to display a warning dialog box to users when the connection is unavailable.

Users of Program Neighborhood can control session reliability in their application set or custom connection settings. To enable session reliability in Program Neighborhood, select **Enable session reliability** on the **Options** tab of the settings for a particular application set or custom connection (enabled by default). Session reliability does not work if it is disabled on either the Program Neighborhood plugin connection or the server.

Users of Citrix XenApp and Citrix XenApp Web Plugin cannot override the server settings for session reliability.

Important: If session reliability is enabled, the default port used for session communication switches from 1494 to 2598.

Enabling the Program Neighborhood Quick Launch Bar

The Program Neighborhood Quick Launch Bar can be used, for example, to allow administrators to quickly access server desktops for administrative purposes. This type of access can also be obtained through the Application Set wizard or by creating a new custom ICA connection, but the Quick Launch Bar enables administrators to establish a connection with a server by simply entering its name or IP address, then clicking Go.

This option is available by selecting **Enable Quick Launch Bar** in the Program Neighborhood Options screen of the installation wizard. The Quick Launch Bar is configured by selecting the **Options** button that appears next to the address bar in the Program Neighborhood user interface. For more information about configuring this feature, see the Program Neighborhood online help.

Improving Performance over Low-Bandwidth Connections

Citrix recommends that you use the latest version of XenApp on the server and its plug-ins. Citrix continually enhances and improves performance with each release. Many performance features require the latest plug-in and server software to function.

If you are using a low-bandwidth connection, you can make a number of changes to your plug-in configuration and the way you use the plug-in to improve performance.

Changing Your Plug-in Configuration

On devices with limited processing power or in circumstances where only limited bandwidth is available, there is a trade-off between performance and functionality. The plug-in provides both user and administrator with the ability to choose an acceptable mixture of rich functionality and interactive performance. Making one or more of these changes can reduce the bandwidth your connection requires and improve performance:

- **Enable data compression.** Compression reduces the size of the data that is transferred over the ICA connection. Enable compression and specify the maximum compression parameter.
- **Enable the bitmap cache.** Bitmap caching stores commonly used bitmaps (images) locally on your client device so that they do not have to be transferred over the ICA connection every time they are needed.
- **Queue mouse movements and keystrokes.** When queuing is enabled, the plug-in sends mouse and keyboard updates less frequently to the XenApp server. Enabling this option improves performance only if you are using a low-bandwidth connection.
- **Enable SpeedScreen Latency Reduction.** SpeedScreen Latency Reduction improves performance over high latency connections by providing instant feedback to the user in response to typed data or mouse clicks.
- **Reduce the window size.** Change the window size to the minimum size you can comfortably use.
- **Reduce the number of colors.** Reduce the number of colors to 256.
- **Reduce sound quality.** If plug-in audio mapping is enabled, reduce the sound quality to the minimum setting.

Changing Plug-in Use

ICA technology is highly optimized and typically does not have high CPU and bandwidth requirements. However, if you are using a very low-bandwidth connection, the following tasks can impact performance:

- **Accessing large files using client drive mapping.** When you access a large file with client drive mapping, the file is transferred over the ICA connection. On slow connections, this may take a long time.
- **Playing multimedia content.** Playing multimedia content uses a lot of bandwidth and can cause reduced performance.

Connecting Client Devices and Published Resources

You can facilitate sessions and optimize the connection of your client devices to resources published in the server farm by:

- Using the workspace control feature
- Synchronizing to tethered PDA devices
- Enabling TWAIN redirection support
- Mapping client devices
- Understanding how your client drives and devices are mapped

Configuring Workspace Control Settings to Provide Continuity for Roaming Users

The workspace control feature provides users with the ability to disconnect quickly from all running applications, reconnect to applications, or log off from all running applications. You can move among client devices and gain access to all of your applications when you log on. For example, health care workers in a hospital can move quickly among workstations and access the same set of applications each time they log on to XenApp. These users can disconnect from multiple applications at one client device and open all the same applications when they reconnect at a different client device.

Workspace control is available only to users connecting to published resources with Citrix XenApp or through the Web Interface.

Policies and client drive mappings change appropriately when you move to a new client device. Policies and mappings are applied according to the client device where you are currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session as soon as the user logs on to the client device in the X-ray laboratory.

Important: Workspace control can be used only with Version 8.*x* and later of the client/plug-in, and works only with sessions connected to computers running Citrix Presentation Server Version 3.0, 4.0, or 4.5 or Citrix XenApp 5.0.

If the workspace control configuration settings of the Web Interface are configured to allow users to override the server settings, users can configure workspace control in the **Account Settings** options of the Web Interface **Preference** menu or the **Reconnect Options** page of Citrix XenApp Options.The following options are available in Citrix XenApp Options on the **Reconnect Options** page:

- **Enable automatic reconnection at logon** allows users to reconnect to disconnected applications or both disconnected and active applications
- **Enable reconnection from the menu** allows users to reconnect to disconnected applications or both disconnected and active sessions

To configure workspace control settings

For users launching applications through the Web Interface, similar options are available from the **Settings** page:

- **Enable automatic reconnection at logon** allows users to reconnect to disconnected applications or both disconnected and active applications

- **Enable automatic reconnection from Reconnect menu** allows users to reconnect to disconnected applications or both disconnected and active sessions

- **Customize Log Off button** allows users to configure whether or not the log off command will include logging them off from applications that are running in the session

If users log on with smart cards or smart cards with pass-through authentication, you must set up a trust relationship between the server running the Web Interface and any other server in the farm that the Web Interface accesses for published applications. For more information about workspace control requirements, see the Citrix XenApp and Web Interface Administrator documentation in Citrix eDocs.

Synchronizing PDAs with Tethered USB Connections

XenApp supports synchronizing a USB PDA device to a client device. This includes USB-tethered and Microsoft Windows powered PDAs that use ActiveSync as a synchronization agent.

Support for this feature is controlled in Citrix XenApp Advanced Configuration or the Presentation Server Console (depending on the version of XenApp server you have installed) with the policy Client Devices > Resources > PDA Devices > Turn on automatic virtual COM port mapping, which should be set to **Enabled**. Users can configure other settings for this feature by clicking **PDA Security** in the Program Neighborhood Connection Center.

Making Scanning Transparent for Users

If you enable TWAIN redirection support, users can control client-attached TWAIN imaging devices transparently with applications that reside on the server farm. To use this feature, a TWAIN device must be attached to the client device and the associated 32-bit TWAIN driver must also be installed on the client device.

Administrators can enable or disable this feature from a Client Device policy rule in XenApp Advanced Configuration or the Presentation Server Console (depending on the version of XenApp server you have installed) - Client Devices > Resources > Other > Configure TWAIN redirection. Additionally, you can enable lossy (JPEG) compression in this policy along with choosing a high, medium, or low level of compression. Further policy rules that facilitate the administration of this feature are:

- Bandwidth > Session Limits > TWAIN Redirection
- Bandwidth > Session Limits (%) > TWAIN Redirection

These policies allow the specification of a maximum amount of bandwidth (in kilobits/second or as a percentage) that can be used for TWAIN redirection.

Mapping Client Devices

The plug-in supports mapping devices on client devices so they are available from within a session. Users can:

- Transparently access local drives, printers, and COM ports
- Cut and paste between the session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the session

During logon, the plug-in informs the XenApp server of the available client drives, COM ports, and LPT ports. By default, client drives are mapped to server drive letters and server print queues are created for client printers so they appear to be directly connected to the XenApp server. These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

You can use the net use and **CHGCDM** commands to map client devices not automatically mapped at logon.

Turning off Client Device Mappings

You can configure client device mapping including options for drives, printers, and ports, using the Terminal Services Configuration tool. For more information about the available options, see your Terminal Services documentation.

Mapping Client Drives to XenApp Server Drive Letters

Client drive mapping allows drive letters on the XenApp server to be redirected to drives that exist on the client device. For example, drive H in a Citrix user session can be mapped to drive C of the local device running the plug-in.

Client drive mapping is built into the standard Citrix device redirection facilities transparently. To File Manager, Windows Explorer, and your applications, these mappings appear like any other network mappings.

Note that Client drive mapping is not supported when connecting to MetaFrame Server 1.0 for UNIX operating systems.

The XenApp server can be configured during installation to map client drives automatically to a given set of drive letters. The default installation mapping maps drive letters assigned to client drives starting with V and works backward, assigning a drive letter to each fixed drive and CD-ROM drive. (Floppy drives are assigned their existing drive letters.) This method yields the following drive mappings in a session:

Client drive letter	Is accessed by the XenApp server as:
A	A
B	B
C	V
D	U

The XenApp server can be configured so that the server drive letters do not conflict with the client drive letters; in this case the server drive letters are changed to higher drive letters. For example, changing server drives C to M and D to N allows client devices to access their C and D drives directly. This method yields the following drive mappings in a session:

Client drive letter	Is accessed by the XenApp server as:
A	A
B	B
C	C
D	D

The drive letter used to replace the server drive C is defined during Setup. All other fixed drive and CD-ROM drive letters are replaced with sequential drive letters (for example; C > M, D > N, E > O). These drive letters must not conflict with any existing network drive mappings. If a network drive is mapped to the same drive letter as a server drive letter, the network drive mapping is not valid.

When a client device connects to a XenApp server, client mappings are reestablished unless automatic client device mapping is disabled. You can use the Terminal Services Configuration tool to configure automatic client device mapping for ICA connections and users. You can also use policies to give you more control over how client device mapping is applied. For more information about policies, see the Citrix XenApp Administrator's documentation at Citrix eDocs.

Mapping Client Printers for More Efficiency

The plug-ins support printing to network printers and printers that are attached locally to client devices. By default, unless you create policies to change this, XenApp lets users:

- Print to all printing devices accessible from the client device
- Add printers (but it does not retain settings configured for these printers or save them for the next session)

However, these settings might not be the optimum in all environments. For example, the default setting that allows users to print to all printers accessible from the client device is the easiest to administer initially, but might create slower logon times in some environments.

Likewise, your organization's security policies might require that you prevent users from mapping local printing ports. To do so, use XenApp Advanced Configuration or the Presentation Server Console (depending on the version of XenApp server you have installed) to set these policy rules to **Enabled**:

Client Devices > Resources > Ports > Turn off COM ports

To change default printing settings, see the "Managing Printers" topic in the Citrix XenApp Administrator's documentation at Citrix eDocs for guidance.

To view mapped client printers

While connected to the XenApp server, from the **Start** menu, choose **Control Panel > Printers**

The **Printers** window displays the local printers mapped to the ICA session. When connecting to servers running Citrix Presentation Server 4.0 or 4.5 or Citrix XenApp 5.0, by default the name of the printer takes the form:

printername **(from** *clientname***) in session** *x*

where *printername* is the name of the printer on the client device, *clientname* is the unique name given to the client device or the Web Interface, and *x* is the SessionID of the user's session on the server; for example, **printer01 (from computer01) in session 7.**

When connecting to servers running Presentation Server 3.0 or earlier, or when the Legacy client printers policy rule is enabled on the server, a different naming convention is used. The name of the printer takes the form:

Client/clientname#/printername

where *clientname* is the unique name given to the client device during client setup and *printername* is the Windows printer name. Because the Windows printer name is used and not the port name, multiple printers can share a printer port without conflict.

For more information about printing, and about managing printing using policies, see the Citrix XenApp Administrator's documentation at Citrix eDocs.

To map a client COM port to a server COM port

Client COM port mapping allows devices attached to the COM ports of the client device to be used during sessions on a XenApp server. These mappings can be used like any other network mappings.

Note: Client COM port mapping is not supported when connecting to MetaFrame Server 1.0 and 1.1 for UNIX Operating Systems.

You can map client COM ports at the command prompt. You can also control client COM port mapping from the Terminal Services Configuration tool or using policies. See the Citrix XenApp Administrator's documentation at Citrix eDocs for more information about policies.

1. Start the plug-in and log on to the XenApp server.

2. At a command prompt, type: **net use com*x*: \\client\com*z***: where *x* is the number of the COM port on the server (ports 1 through 9 are available for mapping) and *z* is the number of the client COM port you want to map.

3. To confirm the operation, type: **net use** at a command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports. To use this COM port in a session on a XenApp server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the client device.

   Note: COM port mapping is not TAPI-compatible. TAPI devices cannot be mapped to client COM ports.

Mapping Client Audio to Play Sound on the Client Device

Client audio mapping enables applications executing on the XenApp server to play sounds through a Windows-compatible sound device installed on the client device. You can set audio quality on a per-connection basis on the XenApp server and users can set it on the client device. If the client device and server audio quality settings are different, the lower setting is used.

Client audio mapping can cause excessive load on servers and the network. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process.

You control the amount of bandwidth client audio mapping uses from the Terminal Services Configuration tool. You can also configure client audio mapping using policies. See the Citrix XenApp Administrator's documentation at Citrix eDocs for more information about policies.

Note: Client sound support mapping is not supported when connecting to Citrix XenApp for UNIX.

Associating Client Device File Types with Published Applications

With extended parameter passing you can associate a file type on a client device with an application published on a server. When a user double-clicks a locally saved file, the file is opened by the application associated with it on the XenApp server.

For example, if you associate all text-type files on the client device with the application “Notepad” published on the server, opening a locally saved text-type file on the client device causes Notepad to open on the server.

Important: Citrix XenApp supports content redirection, a feature introduced in MetaFrame XP, Feature Release 2. Functionally equivalent to extended parameter passing, content redirection allows you to enforce all underlying file type associations from the server, eliminating the need to configure extended parameter passing on individual client devices. If all users are running Citrix XenApp and if you want to take advantage of the administrative ease of content redirection from client device to server, see the Citrix XenApp administrator’s documentation at Citrix eDocs for more information.

Enabling extended parameter passing requires both server-side and client-side configuration. On the server, add the “%*” (percent and asterisk symbols) tokens to published applications. These tokens act as placeholders for client-passed parameters. For more information about passing parameters to published applications, see the Citrix XenApp administrator’s documentation at Citrix eDocs.

On the client device, you must replace the **open** command for the file type with a command line that passes the file name and path to the XenApp server. You must enable extended parameter passing on each client device you want to use this feature.

Configuring Extended Parameter Passing

File type association data is stored in the Windows registry. To associate a file type on the client device with the published application, you need to replace the **open** command for the file type with a command line that passes the file name and path to the application published on the server.

XenApp supports the ISO8859-1 character code for western European languages, including English, and the ShiftJIS character code for Japanese. You must use one of these two character codes to establish file type associations.

The command line you create must include the following elements:

- The file name of the client-side executable used to launch the published application
- The name of the published application to launch, in the correct syntax

- The parameter passing arguments

Determining the Plug-in Executable

Users can connect to published applications using the following methods:

- Finding and launching an application in an application set using Program Neighborhood
- Creating and launching a custom ICA connection using Program Neighborhood
- Launching an .ica file (.ica files are placed on the client device when the user connects using the Web Interface)

Each of these methods launches the published application using a different executable on the client device. The following table lists which executable you must include in the parameter passing command line based on the user's connection method.

Connection method	Executable
Custom ICA connections (using Program Neighborhood)	Wfcrun32.exe
Applications identified in ICA files (including connecting using the Web Interface)	Wfica32.exe
Applications in application sets (using Program Neighborhood)	Pn.exe

Using the Correct Command Syntax to Identify Published Applications

Each plug-in executable uses different command-line syntax to specify configuration data when launching published applications. When creating your command line, you must use the command-line syntax to correctly identify the published application.

Note: To view the required command-line syntax for an executable from a command prompt, change directories to the installation directory of the plug-in and then type the name of the executable followed by /? (forward slash question mark).

To use Wfcrun32.exe to launch a custom ICA connection

To use Wfcrun32.exe to launch a custom ICA connection, specify:

"installdir"\wfcrun32.exe *"application name"*

where *installdir* is your plug-in installation directory; for example, C:\Program Files\Citrix\ICA Client.

To use Wfica32.exe to launch a published application described in an ICA file

To use Wfica32.exe to launch a published application described in an ICA file, specify:

"installdir"\wfica32.exe *file_name*.**ica**

To use Pn.exe to launch a custom ICA connection

To use Pn.exe to launch a custom ICA connection, specify:

*"installdir"***\pn.exe /app:***"application name"*

To use Pn.exe to launch an application published in an application set

To use Pn.exe to launch an application published in an application set, specify:

“*installdir*”**\pn.exe /pn:**“*application set name*” **/app:**“*application name*"

Including Parameter Passing Arguments in the Command Line

When you determine the launching executable and identify the application, you must include the parameter passing arguments **/param:“%1”**.

The sample command line below associates text-type files with the published application “Notepad Text Editor” in the application set “Production Farm.”

“<*installdir*>”**\pn.exe /pn:“Production Farm” /app:“Notepad Text Editor” /param:“%1”**

Entering Parameter Passing in the Windows Registry

When you assemble the required elements of the new command line, you must enter the new command in the Windows registry. You can access the **open** command for the file types you want to associate through the **Folder Options** dialog box in Control Panel. For instructions about editing the **open** command for a file type, see the online Help for the Windows operating system of the client device.

The following example command lines combine the required elements into a working plug-in command line.

To associate text files with a custom published application named “Notepad Text Editor” launched using Pn.exe, specify:

“*installdir*”**\pn.exe /app:“Notepad Text Editor” /param:“\\client\%1”**

To associate text files with an application named “Notepad Text Editor” that is published in an application set called “Production Farm,” specify:

“*installdir*”**\pn.exe /pn:“Production Farm” /app:“Notepad Text Editor” /param:“\\client\%1”**

To associate text files with a custom published application named “Notepad Text Editor” launched using Wfcrun32.exe, specify:

“*installdir*”**\wfcrun32.exe “Notepad Text Editor” /param:“\\client\%1”**

To associate text files with an application identified in an ICA file named Notepad.ica, using Wfica32.exe as the launching executable, specify:

“*installdir*”**\wfica32.exe Notepad.ica /param:“\\client\%1”**

Important: In the previous examples, it is assumed that the client devices are not connecting to servers that contain remapped server drives. If your server drives are remapped, remove the following text from the argument: **\\client\;** for example: **/param:“\\client\%1”**. However, remapping server drives is not supported in XenApp 5.0 for Windows Server 2008.

Improving the Plug-in User Experience

You can improve your users' experiences with the following supported features:

- ClearType font smoothing
- Client-side microphone input for digital dictation
- Multiple monitor support
- Printing performance enhancements
- Windows key combinations for remote sessions
- 32-bit color icons

ClearType Font Smoothing in Sessions

XenApp server supports ClearType font smoothing with Citrix XenApp and Citrix XenApp Web Plug-in for users on computers running Windows XP and Windows Vista.

If you enable ClearType font smoothing on XenApp, you are not forcing the client devices to use ClearType font smoothing. You are enabling the server to support ClearType font smoothing on client devices that have it enabled and are using Citrix XenApp or Citrix XenApp Web Plug-in.

The plug-in automatically detects the client devices's font smoothing setting and sends it to the server. The session connects using this setting. When the ICA session is disconnected or terminated, the server's setting reverts to its original setting.

An older client connects using the font smoothing setting configured in that user's profile on the server.

When ClearType font smoothing is enabled, three times more data is sent across the virtual channel, which might cause a decrease in performance.

To enable or disable ClearType font smoothing in Citrix XenApp

1. Depending on the version of the XenApp server you have installed, select **Citrix Resources** > **Configuration Tools** > **Web Interface** > *XenApp Services site name* > **config.xml** in the left pane of the Access Management Console or Delivery Services Console.

2. From the **Action** menu, choose **Change session options**.

3. In Change session options, choose **Display** and select the **Allow font smoothing** check box to enable ClearType font smoothing or clear the box to disable it. This setting takes effect for new connections. Current sessions retain the previous setting.

To enable or disable ClearType font smoothing in the Web Interface

1. Depending on the version of the XenApp server you have installed, select **Citrix Resources** > **Configuration Tools** > **Web Interface** > *XenApp Web site* in the left pane of the Access Management Console or Delivery Services Console.

2. From the **Action** menu, choose **Manage Session Preferences** > **Remote Connection**> **Display** and select the **Allow font smoothing** check box to enable ClearType font smoothing or clear the box to disable it. This setting takes effect for new connections. Current sessions retain the previous setting.

Client-Side Microphone Input for Digital Dictation

XenApp supports client-side microphone input. This allows you to publish dictation software for use in sessions. Using local microphones, including a number of Philips SpeechMike speech processing devices, users can record dictations with applications running on the server.

For example, a client user away from the office can establish a session to record notes using a laptop. Later in the day the user can retrieve the notes for review or transcription from the desktop device back at the office.

Digital dictation support is available with XenApp. For information about configuring this feature, see the Citrix XenApp Administrator's documentation at Citrix eDocs.

Users of Program Neighborhood and Citrix XenApp can disable their microphones by selecting **No** in the **Audio Security** dialog box available from the Citrix Connection Center, or from the plug-in's system menu (for non-seamless connections). Citrix XenApp Web Plug-in users are presented with the same dialog box automatically at the beginning of their sessions.

On the client device, users control audio input and output in a single step—by selecting an audio quality level from the **Settings** dialog box (for Program Neighborhood) or from the **Options** dialog box (for Citrix XenApp).

Important: When using the Winscribe software with a Philips foot pedal device, you do not need to configure the Winscribe software to use a foot pedal; it works automatically.

Configuring Multiple Monitors

Multiple monitors are fully supported when the plugin is configured to connect to seamless applications.

To enable multiple monitor support, ensure the following:

- The client device must have multiple video boards compatible with the plug-in on the appropriate Windows platform, or a single video board that can support connections to more than one monitor.

- The client device operating system must be able to detect each of the monitors. To verify that this detection occurs, on the client device, view the **Settings** tab in the **Display Properties** dialog box and confirm that each monitor appears separately.

- After your monitors are detected, depending on the version of the XenApp server you have installed, in the left pane of the Access Management Console or Delivery Services Console, select the farm and in the task pane, select **Modify Server Properties > Modify all properties > Server Default > ICA > Display.** Set the **Maximum memory to use for each session's graphics** setting to a large enough size (in kilobytes) to incorporate the entire virtual desktop. If this setting is not high enough, the seamless application is restricted to the subset of the monitors that fits within the size specified.

Enhancing Printing Performance

Printing performance can play a vital role in your users' experiences. The printing configuration you create affects these aspects of the user's experience:

- User ease and comfort level
- Logon times
- Ability to print to a nearby printer when traveling or when moving between client devices in a building

User Ease and Comfort Level

In environments with novice users, consider changing the following potentially confusing default printing behaviors:

- **Printer names change at the start of each session.** When, by default, client printers are auto-created, the printer name is appended with the name of the client device and session. For example, auto-created client printers appear in the Print dialog box with a name like **HP LaserJet 1018 (from *clientname*) in session 35**.

  To resolve this problem, you can either reduce the number of printers auto-created or provision printers using another method. To control printer auto-creation, use XenApp Advanced Configuration or the Presentation Server Console (depending on the version of XenApp server you have installed) to enable the Printing > Client Printers > Auto-creation policy rule and select one of the following in the **When connecting** list box:

  - **Do not auto-create client printers**
  - **Auto-create the client's default printer only**
  - **Auto-create local (non-network) client printers only**
- If many printers are installed by default on client devices, your users might be confused by the large number of available printers. You can limit the printers that appear to them in sessions.
- **Citrix Universal Printer uses a nonstandard printing dialog box.** If your users have trouble learning new features on their own, you might not want to use the Citrix Universal Printer as the default printer in a session. The user interface for this printer is slightly different from the standard Windows print dialog box.

Logon Times

The printing configuration you select can impact how long it takes users to start a session. When XenApp is configured to provision printers by creating them automatically at the beginning of each session, it increases the amount of time to build the session environment. In this case, XenApp has to rebuild every printer found on the client device. You can decrease logon time by specifying any of the following on the XenApp server:

- Auto-create only the Citrix Universal Printer. This is done automatically when you configure the Citrix Universal Printer.
- Auto-create only the default printer for the client device by using the Printing > Client Printers > Auto-creation policy rule.
- Do not auto-create any client printers through the **Auto-creation** policy rule and route print jobs to network printers by configuring the Session printers policy rule.

Configuring Printers for Mobile Workers

If you have users who move among workstations in the same building (for example, in a hospital setting) or move among different offices, you might want to configure Proximity Printing. The Proximity Printing solution ensures that the closest printer is presented to the users in their sessions, even when they change client devices during a session.

For more information about setting printing policies, see the Citrix XenApp Administrator's documentation at Citrix eDocs.

Windows Key Combinations Supported in Remote Sessions

Program Neighborhood and Citrix XenApp allow the pass-through of Windows keyboard shortcuts within a remote session. Users must select the target to which the key combinations apply. In the **ICA Settings** dialog box, the following options can be selected for **Apply Windows key combinations**:

- **In full screen desktops only.** The key combinations apply to the session only when it is in full-screen mode
- **On the remote desktop.** The key combinations apply to the session when its window has the keyboard focus
- **On the local desktop.** The key combinations always apply to the local desktop

Plug-in Support for 32-Bit Color Icons

The Windows plug-ins now support high color icons (32x32 bit) and automatically select the color depth for applications visible in the Citrix Connection Center dialog box and Windows notification area and task bar to provide for seamless applications.

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

To set a preferred depth, you can add a string registry key named TWIDesiredIconColor to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences and set it to the desired value. The possible color depths for icons are 4, 8, 16, 24, and 32 bits-per-pixel. The user can select a lower color depth for icons if the network connection is slow.

Providing Support for NDS Users

When launching plug-in software, users can log on and be authenticated using their Novell Directory Services (NDS) credentials. Supported NDS credentials are user name (or distinguished name), password, directory tree, and context.

NDS support is integrated into the following:

- **Citrix XenApp and Program Neighborhood.** If NDS is enabled in the server farm, NDS users enter their credentials on an NDS tab on the plug-in logon screen. If users have the Novell Client (Version 4.8) installed, they can browse the NDS tree to choose their context.

- **Pass-Through Authentication.** If users have the Novell Client (Version 4.8) installed, you can pass their credentials to the XenApp server, eliminating the need for multiple system and application authentications.

  To enable pass-through authentication, configure the following policy options in the User Package in ZENworks for Desktops:

  - Enable the **Dynamic Local User** policy option

  - Set the **Use NetWare Credentials** value to **On**
- **Custom ICA Connections.** When users run the Add New ICA Connection wizard, they must enter a distinguished name in the user name field and a password in the password field. Users must leave the domain field blank.

- **The Citrix Web Interface.** NDS users enter their credentials on an NDS logon screen provided by the Web Interface. See the Web Interface Administrator's documentation at Citrix eDocs for information about configuring your server for NDS.

  Note: To use NDS logon information with earlier versions of the clients, enter the NDS tree name in the **Domain** field and a distinguished name in the **User** field on the client logon screen.

Setting a Default Context for NDS

You can set a default context for NDS for Program Neighborhood and Citrix XenApp. To set a default context for NDS, you must configure the particular installer file you are using to deploy the plug-ins.

Using Windows NT Credentials with the Novell Client and Pass-Through Authentication

If Program Neighborhood is configured to use pass-through authentication on a client device that has the Novell Client installed, Program Neighborhood, by default, uses the NDS credentials to authenticate the user to the server.

If you want the plug-in to use the user's Windows NT credentials with pass-through authentication instead, use the Group Policy Editor to enable pass-through authentication. You can make the addition to the Windows Installer package before distributing it, or you can configure plug-ins on individual client devices after installation is complete.

To configure individual plug-ins after installation

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the **Administrative Templates** folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates**, navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plugin for Hosted Apps** > **User authentication**, double click **Local user name and password** and select **Enabled > Enable pass-through authentication**.

Using the Window Manager when Connecting to Citrix XenApp for UNIX

You can use the window manager to change the session display when connecting to published resources on XenApp servers for UNIX. With the window manager, users can minimize, resize, position, and close windows, as well as access full screen mode.

About Seamless Windows

In seamless window mode, published applications and desktops are not contained within a session window. Each published application and desktop appears in its own resizable window, as if it is physically installed on the client device. Users can switch between published applications and the local desktop.

You can also display seamless windows in “full screen” mode, which places the published application in a full screen-sized desktop. This mode lets you access the *ctxwm* menu system.

To switch between seamless and full screen modes

Press SHIFT+F2 to switch between seamless and full screen modes.

Minimizing, Resizing, Positioning, and Closing Windows

When users connect to published resources, window manager provides buttons to minimize, resize, position, and close windows. Windows are minimized as buttons on the taskbar.

When the user closes the last application in a session, the session is logged off automatically after twenty seconds.

Using the Citrix Window Manager Menus

In remote desktop and seamless full screen windows, you can use the ctxwm menu system to log off, disconnect, and exit from published applications and connection sessions.

To access the ctxwm menu system

1. On a blank area of the remote desktop window, click and hold down the left mouse button. The ctxwm menu appears.

2. Drag the mouse pointer over **Shutdown** to display the shutdown options.

To choose an option from the ctxwm menu

Drag the pointer over the required option to select it. Release the mouse button to select the option.

To	Choose
Terminate the connection and all running applications	Logoff
Disconnect the session but leave the application running	Disconnect
Disconnect the session and terminate the application	Exit

Note: The server can be configured to terminate any applications that are running if a session is disconnected.

Using ctxgrab and ctxcapture to Cut and Paste Graphics When Connected to XenApp for UNIX

If you are connected to an application published on a XenApp server for UNIX, use ctxgrab or ctxcapture to cut and paste graphics between the session and the local desktop. These utilities are configured and deployed from the server.

Important: You might need to deploy UNIX applications that are designed for use with a 3¤button mouse. Use ctx3bmouse on the XenApp for UNIX server to configure 3-button mouse emulation. For more information, see the XenApp for UNIX administration documentation.

- ctxgrab
- ctxcapture

Using the ctxgrab Utility to Cut and Paste Graphics

This topic does not apply to XenDesktop connections.

The ctxgrab utility is a simple tool you use to cut and paste graphics from published applications to applications running on the local user device. This utility is available from a command prompt or, if you are using a published application, from the ctxwm window manager.

Important: Use ctx3bmouse on the XenApp for UNIX server to configure 3-button mouse emulation. For more information, see the XenApp for UNIX administration documentation.

To access the ctxgrab utility from the window manager

- In seamless mode, right-click the **ctxgrab** button in the top, left-hand corner of the screen to display a menu and choose the **grab** option
- In full screen mode, left-click to display the **ctxwm** menu and choose the **grab** option

To copy from an application in a plug-in window to a local application

1. From the **ctxgrab** dialog box, click **From screen**.
2. To select a window, move the cursor over the window you want to copy and click the middle mouse button. To select a region, hold down the left mouse button and drag the cursor to select the area you want to copy. To cancel the selection, click the right mouse button. While dragging, click the right mouse button before releasing the left button.
3. Use the appropriate command in the local application to paste the object.

Using the ctxcapture Utility to Cut and Paste Graphics

This topic does not apply to XenDesktop connections.

The ctxcapture utility is a more fully-featured utility for cutting and pasting graphics between published applications and applications running on the local user device.

With ctxcapture you can:

- Grab dialog boxes or screen areas and copy them between an application in a plug-in window and an application running on the local user device, including non-ICCCM-compliant applications
- Copy graphics between the plug-in and the X graphics manipulation utility xvf

If you are connected to a published desktop, ctxcapture is available from a command prompt. If you are connected to a published application and the administrator makes it available, you can access ctxcapture through the ctxwm window manager.

Important: Use ctx3bmouse on the XenApp for UNIX server to configure 3-button mouse emulation. For more information, see the XenApp for UNIX administration documentation.

To access the ctxcapture utility from the window manager

Left-click to display the **ctxwm** menu and choose the **screengrab** option.

To copy from a local application to an application in a plug-in window

1. From the **ctxcapture** dialog box, click **From screen**.
2. To select a window, move the cursor over the window you want to copy and click the middle mouse button. To select a region, hold down the left mouse button and drag the cursor to select the area you want to copy. To cancel the selection: click the right mouse button. While dragging, click the right mouse button before releasing the left button.
3. From the **ctxcapture** dialog box, click **To ICA**. The **xcapture** button changes color to indicate that it is processing the information.
4. When the transfer is complete, use the appropriate command in the published application window to paste the information.

To copy from an application in a plug-in window to a local application

1. From the application in the plug-in window, copy the graphic.
2. From the **ctxcapture** dialog box, click **From ICA**.
3. When the transfer is complete, use the appropriate command in the local application to paste the information.

To copy from xv to an application in a plug-in window or local application

1. From xv, copy the graphic.
2. From the **ctxcapture** dialog box, click **From xv** and **To ICA**.
3. When the transfer is complete, use the appropriate command in the plug-in window to paste the information.

To copy from an application in a plug-in window to xv

1. From the application in the plug-in window, copy the graphic.
2. From the **ctxcapture** dialog box, click **From ICA** and **To xv**.
3. When the transfer is complete, use the paste command in xv.

Matching Client Names and Computer Names

The dynamic client name feature allows the client name to be the same as the computer name. When users change their computer name, the client name changes to match. This allows you to name computers to suit your naming scheme and find connections more easily when managing your server farm.

If the client name is not set to match the computer name during installation, the client name does not change when the computer name is changed.

Users enable dynamic client name support by selecting **Enable Dynamic Client Name** during plug-in installation.

To enable dynamic client name support during silent installation, the value of the property ENABLE_DYNAMIC_CLIENT_NAME in your installer file must be Yes. Set the property to No to disable dynamic client name support.

DNS Name Resolution

You can configure plug-ins that use the Citrix XML Service to request a Domain Name Service (DNS) name for a server instead of an IP address.

Important: Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS name resolution in the server farm.

Program Neighborhood is configured to use TCP/IP+HTTP (the Citrix XML Service) browsing by default. Plug-ins connecting to published applications through the Web Interface also use the Citrix XML Service. For plug-ins connecting through the Web Interface, the Web server resolves the DNS name on behalf of the plug-in.

DNS name resolution is disabled by default in the server farm and enabled by default on the plug-ins. When DNS name resolution is disabled in the farm, any plug-in request for a DNS name returns an IP address. There is no need to disable DNS name resolution on the plug-in.

To disable DNS name resolution for specific client devices

If you are using DNS name resolution in the server farm and are having problems with specific client devices, you can disable DNS name resolution for those devices.

Caution: Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

1. Add a string registry key xmlAddressResolutionType to HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing.
2. Set the value to IPv4-Port.
3. Repeat for each user of the client devices.

Securing Online Plug-in Communication

To secure the communication between your server farm and the online plug-in, you can integrate your plug-in connections to the server farm with a range of security technologies, including:

- A SOCKS proxy server or secure proxy server (also known as *security proxy server*, HTTPS proxy server, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between the online plug-in and servers. The online plug-in supports SOCKS and secure proxy protocols.
- Secure Gateway for Citrix XenApp or SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using the plug-ins through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.
- Trusted server configuration.

Note: For information about increasing security in application streaming for desktops, see the Citrix Knowledge Base article *Enhancing Security in Application Streaming for Desktops*.

The Citrix onlne plug-in is compatible with and functions in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates are used. These templates are supported on the Microsoft Windows XP, Windows Vista, and Windows 7 platforms. Refer to the Windows XP, Windows Vista, and Windows 7 security guides available at http://technet.microsoft.com for more information about the templates and related settings.

Support for Microsoft Security Templates

The Citrix XenApp plug-ins are compatible with and function in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security template is used. These templates are supported on the Microsoft Windows XP and Vista platforms. Refer to the Windows XP and Windows Vista security guides available at http://technet.microsoft.com for more information about the template and related settings.

Connecting Citrix XenApp and the XenApp Web Plug-in through a Proxy Server

Proxy servers are used to limit access to and from your network, and to handle connections between plug-ins and XenApp servers. The plug-ins support SOCKS and secure proxy protocols.

When communicating with the server farm, the Citrix XenApp and Citrix XenApp Web Plug-in use proxy server settings that are configured remotely on the server running the Web Interface. See the topics for *Web Interface* for information about configuring proxy server settings for these plug-ins.

In communicating with the Web server, the Citrix XenApp and XenApp Web Plug-in use the proxy server settings that are configured through the Internet settings of the default Web browser on the client device. You must configure the Internet settings of the default Web browser on the client device accordingly.

Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay

You can integrate the plug-ins with the Secure Gateway or Secure Sockets Layer (SSL) Relay service. The plug-ins support both SSL and TLS protocols.

- SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.

- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the certificates you use for SSL in your software installation will 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 FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

Connecting with the Secure Gateway

You can use the Secure Gateway in either *Normal* mode or *Relay* mode to provide a secure channel for communication between the plug-in and the server. No plug-in configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

Citrix XenApp and Citrix XenApp Web Plug-in use settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway. See the topics for the Web Interface for information about configuring proxy server settings for these plug-ins.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. See the topics for the Secure Gateway for more information about Relay mode.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure the plug-in to use:

- The fully qualified domain name (FQDN) of the Secure Gateway server.
- The port number of the Secure Gateway server. Note that Relay mode is not supported by Secure Gateway Version 2.0.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example: *my_computer.my_company.com* is an FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (my_company), and a top-level domain (com). The combination of intermediate and top-level domain (my_company.com) is generally referred to as the *domain name*.

Connecting with Citrix SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the XenApp server for SSL/TLS-secured communication. When the SSL Relay receives an SSL/TLS connection, it decrypts the data before redirecting it to the server, or, if the user selects SSL/TLS+HTTPS browsing, to the Citrix XML Service.

If you configure SSL Relay to listen on a port other than 443, you must specify the nonstandard listening port number to the plug-in.

You can use Citrix SSL Relay to secure communications:

- Between an SSL/TLS-enabled client and a server. Connections using SSL/TLS encryption are marked with a padlock icon in the Program Neighborhood Connection Center.
- With a server running the Web Interface, between the XenApp server and the Web server.

For information about configuring and using SSL Relay to secure your installation, see the Citrix XenApp administrator's documentation at Citrix eDocs. For information about configuring the server running the Web Interface to use SSL/TLS encryption, see the Web Interface administrator's documentation at Citrix eDocs.

Client Device Requirements

In addition to the system requirements listed, you also must ensure that:

- The client device supports 128-bit encryption
- The client device has a root certificate installed that can verify the signature of the Certificate Authority on the server certificate
- The client is aware of the TCP listening port number used by the SSL Relay service in the server farm
- Any service packs or upgrades that Microsoft recommends are applied

If you are using Internet Explorer and you are not certain about the encryption level of your system, visit the Microsoft Web site at http://www.microsoft.com to install a service pack that provides 128-bit encryption.

Note: The plug-ins support certificate key lengths of up to 4096 bits. Ensure that the bit lengths of your Certificate Authority root and intermediate certificates, and those of your server certificates, do not exceed the bit length your plug-ins support or connection might fail.

To apply a different listening port number for all connections

If you are changing this on a local computer, close all plug-in components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plugin Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Presentation Server Client** > **Network routing** > **TLS/SSL data encryption and server identification**.

7. From the **Action** menu, choose **Properties**, select **Enabled**, and type a new port number in the **Allowed SSL servers** text box in the following format: *server:SSL relay port number* where *SSL relay port number* is the number of the listening port. You can use a wildcard to specify multiple servers. For example, ***.Test.com:***SSL relay port number* matches all connections to **Test.com** through the specified port.

To apply a different listening port number to particular connections only

If you are changing this on a local computer, close all plug-in components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the **Start** menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already added the icaclient template to the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plugin Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Presentation Server Client** > **Network routing > TLS/SSL data encryption and server identification**.

7. From the **Action** menu, choose **Properties**, select **Enabled**, and type a comma-separated list of trusted servers and the new port number in the **Allowed SSL servers** text box in the following format: *servername:SSL relay port number*,*servername:SSL relay port number* where *SSL relay port number* is the number of the listening port. You can specify a comma-separated list of specific *trusted* SSL servers similar to this example:

   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444

   which translates into the following in an example appsrv.ini file: [Word] SSLProxyHost=csghq.Test.com:443

   [Excel]

   SSLProxyHost=csghq.Test.com:444

   [Notepad]

   SSLProxyHost=fred.Test.com:443

Configuring and Enabling Plug-ins for SSL and TLS

SSL and TLS are configured in the same way, use the same certificates, and are enabled simultaneously.

When SSL and TLS are enabled, each time you initiate a connection, the plug-in tries to use TLS first and then tries SSL. If it cannot connect with SSL, the connection fails and an error message appears.

To force the plug-ins (including XenApp Web Plug-in) to connect with TLS, you must specify TLS on the Secure Gateway server or SSL Relay service. See the topics for the Secure Gateway or your SSL Relay service documentation for more information.

In addition, make sure the client device meets all system requirements outlined in the XenApp *Installation Checklist*.

To use SSL/TLS encryption for all plug-in communications, configure the client device, XenApp, the XenApp plug-in, and the server running the Web Interface as described in this section.

Installing Root Certificates on the Client Devices

To use SSL/TLS to secure communications between SSL/TLS-enabled plug-ins and the server farm, you need a root certificate on the client device that can verify the signature of the Certificate Authority on the server certificate.

The plug-ins support the Certificate Authorities that are supported by the Windows operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

If you use your own Certificate Authority, you must obtain a root certificate from that Certificate Authority and install it on each client device. This root certificate is then used and trusted by both Microsoft Internet Explorer and the plug-in.

Depending on your organization's policies and procedures, you may want to install the root certificate on each client device instead of directing users to install it. If you are using Windows 2000 with Active Directory on all client devices, you can deploy and install root certificates using Windows 2000 Group Policy. See your Microsoft Windows 2000 documentation for more information.

Alternatively, you may be able to install the root certificate using other administration or deployment methods, such as:

- Using the Microsoft Internet Explorer Administration Kit (IEAK) Configuration Wizard and Profile Manager
- Using third-party deployment tools

Make sure that the certificates installed by your Windows operating system meet the security requirements for your organization or use the certificates issued by your organization's Certificate Authority.

To configure Citrix XenApp to use SSL/TLS

1. Make sure the client device meets all requirements outlined in Client Device Requirements and in the XenApp Installation Checklist.

2. To use SSL/TLS to encrypt application enumeration and launch data passed between Citrix XenApp and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the computer name of the XenApp server that is hosting the SSL certificate.

3. To use secure HTTP (HTTPS) to encrypt the configuration information passed between Citrix XenApp and the server running the Web Interface, enter the server URL in the format https://*servername* on the **Server Options** page of the Citrix XenApp **Options** dialog box.

To configure TLS support

If you are changing this on a local computer, close all plug-in components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by running gpedit.msc locally from the **Start** menu when applying this to a single computer or by using the Group Policy Management Console when using Active Directory.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Administrative Templates (ADM)** > **Citrix Components** > **Presentation Server Client** > **Network routing** > **TLS/SSL data encryption and server identification**.

7. From the **Action** menu, choose **Properties**, select **Enabled**, and from the drop-down menus, select the TLS settings.

   - Set SSL/TLS Version to **TLS** or **Detect all** to enable TLS. If **Detect all** is selected, the plug-in connects using TLS encryption. If a connection using TLS fails, the plug-in connects using SSL.
   - Set SSL ciphersuite to **Detect version** to have the plug-in negotiate a suitable ciphersuite from the Government and Commercial ciphersuits. You can restrict the ciphersuites to either Government or Commercial.
   - Set CRL verification to **Require CRLs for connection** requiring the plug-in to try to retrieve Certificate Revocation Lists (CRLs) from the relevant certificate issuers.

To use the Group Policy template to meet FIPS 140 security requirements

If you are changing this on a local computer, close all plug-in components, including the Connection Center.

To meet FIPS 140 security requirements, use the Group Policy template to configure the parameters or include the parameters in the Default.ica file on the server running the Web Interface. See the information about Web Interface for additional information about the Default.ica file.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 3 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Classic Adminstrative Templates (ADM)** > **Citrix Components** > **Citrix XenApp Plugin for Hosted Apps** > **Network routing** > **TLS/SSL data encryption and server identification**.

7. From the **Action** menu, choose **Properties**, select **Enabled**, and from the drop-down menus, select the correct settings.

   - Set SSL/TLS Version to **TLS** or **Detect all** to enable TLS. If **Detect all** is selected, the plug-in tries to connect using TLS encryption. If a connection using TLS fails, the plug-in tries to connect using SSL.
   - Set SSL ciphersuite to **Government**.
   - Set CRL verification to **Require CRLs for connection**.

To configure the Web Interface to use SSL/TLS when communicating with the plug-in

When using the Web Interface, specify the computer name of the server hosting the SSL certificate. See the information about Web Interface for more details about using SSL/TLS to secure communications between XenApp and the Web server.

1. From the **Configuration settings** menu, select **Server Settings**.
2. Select **Use SSL/TLS for communications between clients and the Web server**.
3. Save your changes.

Selecting SSL/TLS changes all URLs to use HTTPS protocol.

To configure Citrix XenApp to use SSL/TLS when communicating with the plug-in

You can configure the XenApp server to use SSL/TLS to secure the communications between the Citrix XenApp and the server.

1. Depending on the version of the XenApp server you have installed, in the Access Management Console or Delivery Services Console, open the **Properties** dialog box for the application you want to secure.

2. Select **Advanced > Client options** and ensure that you select **Enable SSL and TLS protocols**.

3. Repeat these steps for each application you want to secure.

For more information, see the XenApp administrator documentation.

When using the Web Interface, specify the computer name of the server hosting the SSL certificate. See the information about Web Interface for more details about using SSL/TLS to secure communications between XenApp and the Web server.

To configure Citrix XenApp to use SSL/TLS when communicating with the server running the Web Interface

You can configure the plug-in to use SSL/TLS to secure the communications between Citrix XenApp and the server running the Web Interface.

Note: This procedure assumes that a valid root certificate is installed on the client device. For more information, see the information about installing root certificates on client devices.

1. In the Windows notification area, right-click the Citrix XenApp icon and choose **Change Server**.

2. The **Change Server** screen displays the currently configured URL. Click **Change** and enter the server URL in the dialog box that appears. Enter the URL in the format https://*servername* to encrypt the configuration data using SSL/TLS.

3. Click **Update** to apply the change.

4. Enable SSL/TLS in the client device browser. For more information about enabling SSL/TLS in the browser, see the online Help for the browser.

Configuring Program Neighborhood

When connecting through a proxy server, Program Neighborhood uses proxy server settings you configure locally from the plug-in's toolbar. You can configure proxy server settings in three ways:

- Enable automatic plug-in proxy detection
- Enable automatic proxy detection
- Manually specify the details of your proxy server

When connecting with Citrix SSL Relay, by default, it uses TCP port 443 on the XenApp server for SSL/TLS-secured communication. If you configure SSL Relay to listen on a port other than 443, you must specify the nonstandard listening port number to the plug-in. In Program Neighborhood, users can change the port number in the Firewall Settings dialog box. For step-by-step instructions, see the Program Neighborhood online help.

When connecting with the Secure Gateway, Program Neighborhood users can manually specify the details of the Secure Gateway server for both application sets and custom ICA connections.

To enable automatic plug-in proxy detection

If you are deploying the plug-in in an organization with multiple proxy servers, consider using automatic plug-in proxy detection. Automatic plug-in proxy detection communicates with the local Web browser to discover the details of the proxy server. It is also useful if you cannot determine which proxy server will be used when you configure the plug-in. Automatic plug-in proxy detection requires Internet Explorer 5.0 through 7.0 or Mozilla Firefox 1.0.

1. Start Program Neighborhood.
    - If you are configuring an application set:

      Right-click the application set you want to configure and select **Application Set Settings**. A **Settings** dialog box for the application set appears.

    - If you are configuring an *existing* custom ICA connection:

      Right-click the custom ICA connection you want to configure and select **Properties**. The **Properties** dialog box for the custom connection appears.

    - If you are configuring all *future* custom ICA connections:

      Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
2. On the **Connection** tab, click **Firewalls**.
3. Select **Use Web browser proxy settings**.

To enable automatic proxy settings

This setting is provided to detect a proxy server automatically, so users do not have to configure the proxy server manually. In larger environments, this feature also means administrators do not have to spend time supporting incorrect or dynamic configurations.

You must configure either DNS or DHCP (Dynamic Host Configuration Protocol) to support automatic proxy detection.

1. Start Program Neighborhood.
    - If you are configuring an application set:

      Right-click the application set you want to configure and select **Application Set Settings**. A **Settings** dialog box for the application set appears.
    - If you are configuring a *new* custom ICA connection:

      Click **Server Location** when stepping through the Add ICA Connection wizard. The **Locate Server or Published Application** dialog box for the custom connection appears. Clear the check box for **Use Default**.
    - If you are configuring an *existing* custom ICA connection:

      Right-click the custom ICA connection you want to configure and select **Properties**. The **Properties** dialog box for the custom connection appears. Ensure the check box for **Use Custom Default** is cleared.
    - If you are configuring all *future* custom ICA connections:

      Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connections Settings**. The **Custom ICA Connections** dialog box appears.
2. Click **Firewalls**.
3. Select **Automatically detect proxy**.

To manually specify the details of your proxy server

Program Neighborhood allows users to configure their proxy settings manually, both for application sets and for custom ICA connections.

If you are configuring the proxy manually, confirm these details with your security administrator. ICA connections cannot be made if these details are incorrect.

1. Start Program Neighborhood.
    - If you are configuring an application set:

      Right-click the application set you want to configure and select **Application Set Settings**. A **Settings** dialog box for the application set appears.
    - If you are configuring an *existing* custom ICA connection:

      Right-click the custom ICA connection you want to configure and select **Properties**. The **Properties** dialog box for the custom connection appears.
    - If you are configuring all *future* custom ICA connections:

      Right-click in a blank area of the Custom ICA Connections window and select **Custom Connections Settings**. The **Custom ICA Connections** dialog box appears.
2. On the **Connection** tab, click **Firewalls**.
3. Select the proxy protocol type (**SOCKS** or **Secure (HTTPS)**).
4. Enter the proxy address and the port number for the proxy server.
    - The default port for SOCKS is 1080
    - The default port for secure proxy is 8080

To create a setting for one or several existing custom ICA connections

Use this procedure to create custom settings for Program Neighborhood only. Use the Group Policy template to create settings affecting the entire XenApp Plug-in for Hosted Apps.

Some proxy servers require authentication, prompting you for a user name and password when you enumerate resources or open an ICA connection. You can avoid these prompts by configuring the plug-in to pass the credentials without user intervention. You can create settings that apply to one or several existing custom ICA connections or act as the default for all future custom ICA connections to be created using the Add ICA Connection wizard.

1. Exit Program Neighborhood if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.

2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.

3. Locate the [*ServerLocation*] section, where *ServerLocation* is the name of the connection you want to configure.

4. Locate the **DoNotUseDefaultCSL** property of that [*ServerLocation*] section.

    - If the value of DoNotUseDefaultCSL is On, perform the following steps:

      Add the following lines to that [*ServerLocation*] section:

      ProxyUsername=*user name*

      ProxyPassword=*password*

      where *user name* is the user name recognized by the SOCKS server and *password* is the password associated with the user name recognized by the proxy server.

    - If the value of DoNotUseDefaultCSL is Off or if the parameter is not present, perform the following steps:

      Add the following lines to the [WFClient] section:

      ProxyUsername=*user name*

      ProxyPassword=*password*

      where *user name* is the user name recognized by the SOCKS server and *password* is the password associated with the user name recognized by the proxy server.

5. Repeat Steps 3 and 4 for any additional connections if applicable.

Note: Users can override the default setting from within a particular custom ICA connection's **Properties** dialog box.

To create a default for all future custom ICA connections

1. Exit Program Neighborhood if it is running and make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section named [WFClient].
4. Add the following lines to the list of parameters and values in the [WFClient] section:

   ProxyUsername=*user name*

   ProxyPassword=*password*

   where *user name* is the user name recognized by the SOCKS server and *password* is the password associated with the user name recognized by the proxy server.
5. Save your changes.

Note: Users can override the default setting from within a particular custom ICA connection's **Properties** dialog box.

To connect to a server through a firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using the plug-ins through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

1. Open Program Neighborhood.
    - If you are configuring an application set.

      Right-click the application set you want to configure and select **Application Set Settings**. A configuration dialog box for the application set appears.

    - If you are configuring a custom ICA connection:

      Right-click the custom ICA connection you want to configure and select **Custom Connections Settings**. The **Custom ICA Connections** dialog box appears.
2. Click **Add**. The **Add Server Location Address** dialog box appears.
3. Enter the external Internet address of the server.
4. Click **OK**. The external Internet address you added appears in the Address List.
5. Click **Firewalls**.
6. Select **Use alternate address for firewall connection**.

Important: All servers in the server farm must be configured with their alternate (external) address.

To configure Program Neighborhood for Secure Gateway

Program Neighborhood users can manually specify the details of the Secure Gateway server for both application sets and custom ICA connections.

1. Make sure the client device meets all system requirements outlined in the documentation.
2. Start Program Neighborhood.
   - If you are configuring an application set:

     Right-click the application set you want to configure and select **Application Set Settings**. A configuration dialog box for the application set appears.
   - If you are configuring an *existing* custom ICA connection:

     Right-click the custom ICA connection you want to configure and select **Properties**. The **Properties** dialog box for the custom connection appears.
   - If you are configuring all future custom ICA connections:

     Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connections Settings**. The **Custom ICA Connections** dialog box appears.
3. Select your connection:
   - If you are configuring an application set or an existing custom ICA connection:

     From the **Network Protocol** menu, select **SSL/TLS+HTTPS**.
   - If you are configuring *all future* custom ICA connections:

     From the **Network Protocol** menu, select **HTTP/HTTPS**.
4. On the **Connection** tab, click **Firewalls**.
5. Enter the FQDN of the Secure Gateway server in the **Secure gateway address** box.
6. Enter the port number in the **Port** box.

To configure Program Neighborhood to use SSL/TLS

1. Make sure the client device meets all requirements outlined in Client Device Requirements and the XenApp *Installation Checklist*.

2. Open Program Neighborhood.

   - If you are configuring an application set to use SSL/TLS:

     Right-click the application set you want to configure and select **Application Set Settings**. A **Settings** dialog box for the application set appears.

   - If you are configuring an *existing* custom ICA connection to use SSL/TLS:

     Right-click the custom ICA connection you want to configure and select **Properties**. The **Properties** dialog box for the custom connection appears.

   - If you are configuring all future custom ICA connections to use SSL/TLS:

     Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connections Settings**. The **Custom ICA Connections** dialog box appears.

3. Select an option:

   - If you are configuring an application set or an *existing* custom ICA connection:

     From the **Network Protocol** menu, select **SSL/TLS+HTTPS**.

   - If you are configuring *all future* custom ICA connections:

     From the **Network Protocol** menu, select **HTTP/HTTPS**.

4. Add the fully qualified domain name of the SSL/TLS-enabled servers to the Address List.

Enabling Smart Card Logon

Enabling smart card logon allows users to use smart cards instead of passwords to authenticate to XenApp servers. You can use smart card logon either with or without pass-through authentication.

You must enable smart card support on the server and set up and configure the client device properly with third-party smart card hardware and software. Refer to the documentation that came with your smart card equipment for instructions about deploying smart cards within your network.

The smart card removal policy set on XenApp determines what happens if you remove the smart card from the reader during an ICA session. The smart card removal policy is configured through and handled by the Windows operating system.

- Kerberos pass-through authentication requires a smart card inserted in the smart card reader at logon time only. With this logon mode selected, the plug-in prompts the user for a smart card PIN (Personal Identification Number) when it starts up. Kerberos pass-through authentication then caches the PIN and passes it to the server every time the user requests a published resource. The user does not have to subsequently reenter a PIN to access published resources or have the smart card continuously inserted. If authentication based on the cached PIN fails or if a published resource itself requires user authentication, the user continues to be prompted for a PIN.

- Disabling pass-through authentication requires a smart card to be present in the smart card reader whenever the user accesses a server. With pass-through disabled, the plug-in prompts the user for a smart card PIN when it starts up and every time the user requests a published resource.

Enforcing Trust Relations

Trusted server configuration is designed to identify and enforce trust relations involved in plug-in connections. This trust relationship increases the confidence of client administrators and users in the integrity of data on client devices and prevents the malicious use of plug-in connections.

When this feature is enabled, plug-ins can specify the requirements for trust and determine whether or not they trust a connection to the server. For example, a plug-in connecting to a certain address (such as https://*.citrix.com) with a specific connection type (such as SSL) is directed to a trusted zone on the server.

When trusted server configuration is enabled, XenApp servers or the Access Gateway must reside in a Windows Trusted Sites zone. (For step-by-step instructions about adding servers to the Windows Trusted Sites zone, see the Internet Explorer online help.)

If you connect using SSL, add the server name in the format https://CN, where CN is the Common Name shown on the SSL certificate. Otherwise, use the format that the plug-in uses to connect; for example if the plug-in connects using an IP address, add the server's IP address.

To enable trusted server configuration

If you are changing this on a local computer, close all plug-in components, including the Connection Center.

1. As an administrator, open the Group Policy Editor by either running gpedit.msc locally from the Start menu when applying policies to a single computer or by using the Group Policy Management Console when applying domain policies.

   Note: If you already imported the icaclient template into the Group Policy Editor, you can omit Steps 2 to 5.

2. In the left pane of the Group Policy Editor, select the Administrative Templates folder.

3. From the **Action** menu, choose **Add/Remove Templates**.

4. Choose **Add** and browse to the plug-in Configuration folder (usually C:\Program Files\Citrix\ICA Client\Configuration) and select icaclient.adm.

5. Select **Open** to add the template and then **Close** to return to the Group Policy Editor.

6. Expand the **Administrative Templates** folder under the **User Configuration** node.

7. From the Group Policy Editor, expand **Administrative Templates** and navigate through **Citrix Components** > **Presentation Server Client** > **Network Routing** > **Configure trusted server configuration**.

8. From the **Action** menu, choose **Properties** and select **Enabled**.