Clients for Windows Administrator’s Guide

Citrix® Presentation Server Clients 10.*x* for Windows®

Citrix Presentation Server™ 4.5

Copyright and Trademark Notice

Trademark Acknowledgements

Document Code: August 30, 2007 (JP)

Contents

Chapter 1 Introduction

Chapter 2 Deploying and Installing Client Software

Chapter 3 Configuring Client Software

Chapter 4 Optimizing the Client Environment

Introduction

This manual is for system administrators responsible for installing, configuring, deploying, and maintaining the Citrix Presentation Server Clients for Windows.

This manual assumes knowledge of:

- The server farm to which your clients connect
- The operating system on the client device (Windows NT, Windows 2000, Windows XP, Windows XP (x64 edition), Windows XP Embedded, Windows 2003, or Windows Fundamentals for Legacy PCs)

Overview

This chapter introduces Version 10.*x* of the clients for computers running 32-bit or 64-bit Windows operating systems. It is designed to help you decide which clients to use in your computing environment and also details the new features included in this release.

Note: For information about the Client for Windows CE devices, refer to the *Client for Windows CE for Handheld and Pocket PCs Administrator's Guide* available from the Downloads section of the Citrix Web site, http://www.citrix.com/.

Citrix Presentation Server Clients are the components of Citrix Presentation Server that users run on their client devices to access resources published on computers running Citrix Presentation Server. The clients combine ease of deployment and use, and offer quick, secure access to applications, content, and entire server desktops.

Deciding Which Client to Use

Different enterprises have different corporate needs, and your expectations and requirements for the way users access your published resources may shift as your corporate needs evolve and grow. This section summarizes the clients you can use and how to decide which one best suits your needs.

Citrix Presentation Server offers you a choice of the following clients for use on Windows systems:

- Program Neighborhood Agent
- Program Neighborhood
- Web Client

Note: For information about clients for other client devices and operating systems, see the documentation included on your Citrix Presentation Server Components CD or visit our Web site at http://www.citrix.com/.

Each of the clients for use with Windows differs in terms of:

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

To decide which client 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. The following sections and table summarize these considerations.

Program Neighborhood Agent

The Program Neighborhood Agent supports the full Citrix Presentation Server feature set. Using the Program Neighborhood Agent in conjunction with the Web Interface, you can integrate published resources with users’ desktops. It is centrally administered and configured in the Access Management Console using a Program Neighborhood Agent site created in association with a site for the server running the Web Interface.

The Program Neighborhood Agent is one of two clients that operate with the Citrix Streaming Client to provide application streaming to the user desktop. To take advantage of the full set of application streaming features of Presentation Server along with Program Neighborhood Agent features, install it on client devices along with the streaming client. For more information about the streamed application feature, see the *Citrix Application Streaming Guide*.

Important: The Program Neighborhood Agent requires the Citrix Web Interface.

Access method. The Program Neighborhood Agent 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. The Program Neighborhood Agent works in the background. Except for a shortcut menu available from the notification area, it does not have a user interface.

Client management and administration. You configure Program Neighborhood Agent at a site created in the Access Management Console and associated with the site for the server running the Web Interface. By using the Access Management Console in this way, you can dynamically manage and control your client population throughout your network from a single location and in real time.

Web Client

The Web Client is a smaller client that can be installed from a .cab file or from the main .msi file. The Web Client setup files are significantly smaller than the other clients. The small size allows users to quickly download and install the client software.

Access method. If you want users to access published resources from within a familiar browser environment, use the Web Client. 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. The Web Client does not require user configuration and does not have a user interface.

Client management and administration. You can use the Web Client 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 client requires the presence on client devices of Microsoft Internet Explorer 5.0 through 7.0; Netscape Navigator 4.78, and 6.2 through 7.1; or Mozilla Firefox 1.0 through 1.5.

Program Neighborhood

Program Neighborhood supports the full Citrix Presentation Server 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 Program Neighborhood Agent site; thus, it does not require the Web Interface.

Note: Program Neighborhood does not support zone preference and failover.

Access method. 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 computers running Citrix Presentation Server. Icons representing application sets and custom ICA connections appear in the Program Neighborhood window.

Client 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.

Important: 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 have not yet deployed any clients, use the Program Neighborhood Agent or the Web Client.

The following table compares the clients.

Client	Access Method	User Involvement	Client Features
Program Neighborhood Agent	Transparent integration of published resources into user's desktop	Central administration of user settings	Supports the full feature set of Citrix Presentation Server.
Web Client	Web browser-based access to published resources	Central administration of user settings	Supports the full feature set of Citrix Presentation Server.
Program Neighborhood	An interface users access from their desktops	Requires initial user configuration	Supports the full feature set of Citrix Presentation Server except for zone preference and failover.

New in this Release

Version 10.*x* of the clients ships with Citrix Presentation Server 4.5 for Windows and runs on Windows NT 4.0, Windows 2000, Windows 2003, Windows XP, and Windows Fundamentals for Legacy PCs operating systems. It introduces a wide range of new features and performance improvements and is fully backward compatible with earlier versions of Windows and MetaFrame XP feature releases.

Highlights of Version 10.*x* of the clients include the following:

Added support for new operating systems.

The Clients for Windows now support the following operating systems:

- Windows XP (x64 edition)
- Windows XP Embedded
- Windows Fundamentals for Legacy PCs

Application streaming. The Program Neighborhood Agent now operates with the Citrix Streaming Client to provide application streaming to the user desktop as well as access to offline applications. For more information about the streamed application feature, see the *Citrix Application Streaming Guide*.

Non-administrator client installation. This feature allows client users who do not have administrator privileges on a “locked down” computer, such as an Internet cafe or kiosk, to download the Ica32pkg.msi package and install a modified Web Client on a per-user basis. In this way, users can have secure, remote access to their applications. See “Enabling Non-Administrators to Install Clients” on page 17.

Trusted server configuration. This feature is designed to identify and enforce trust relations involved in client 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 client connections.

When this feature is enabled, clients can specify the requirements for trust and determine whether or not they trust a connection to the server. For example, a client connecting to a certain address (such as https://*.citrix.com) with a specific connection type (such as SSL) will be directed to a trusted zone on the server. When trusted server configuration is enabled, computers running Citrix Presentation Server must be added to a Windows Trusted Sites zone. For more information, see "Enforcing Trust Relations" on page 83.

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

During the installation, the user selects a language: German (Deutsch), English, Spanish (Español), French (Français), Japanese, Simplified Chinese, or Traditional Chinese. The user interface appears in the selected language. For more information, see "Selecting a User Interface Language" on page 23.

32-bit color icon support. This feature supports high color icons and automatically selects the color depth for applications visible in the Program Neighborhood Connection Center dialog box and Windows notification area and task bar to provide for seamless applications. See "32-Bit Color Icon Support" on page 60.

Program Neighborhood Agent backup URL support. Administrators can specify backup URLs for Program Neighborhood Agent in their Web Interface configuration. In addition, if the Program Neighborhood Agent cannot connect to the Web Interface, administrators can specify backup URLs in a new property for the .msi package. For information about creating the backup addresses in the .msi package, see "Specifying Backup Server Addresses" on page 25. For more information about creating backup addresses using the Web Interface, see the *Citrix Web Interface Administrator's Guide*.

SpeedScreen Multimedia Acceleration. This feature extends SpeedScreen Multimedia Acceleration on the server to support additional media types on the client.

Enhanced proxy detection support. This feature automatically detects a proxy server 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. For more information, see "Enabling Automatic Proxy Detection" on page 68.

Program Neighborhood Agent support through the Access Gateway. The Program Neighborhood Agent can now use pass-through authentication to connect through the Access Gateway to computers running Citrix Presentation Server. This means users do not have to reenter their credentials when they connect to the server.

Advanced Encryption Standard (AES) support. The Clients for Windows now support the AES cipher for connections using TLS.

Note: AES support is available only when connecting to servers running Citrix Presentation Server 4.5. The client device must be running Windows XP, Service Pack 2; Windows 2003, Service Pack 1 or later; or Windows Fundamentals for Legacy PCs.

Discontinued client functionality. The following functions are no longer supported:

- Beginning with Version 10.0 of the Clients for Windows, the option to use InstallShield client packages is no longer available. In addition, the Client Auto Update feature, which was used to update the InstallShield client packages, is also no longer available. To deploy updated clients, you can use the Citrix Web Interface, or third-party products or desktop management software that can distribute Microsoft Software Installer (MSI) packages, including Windows Active Directory.
- IPX, SPX, and NetBios network protocols are no longer supported for client connections to computers running Citrix Presentation Server. To reconfigure connections, use Properties. To create a new connection, use the Add ICA Connection wizard and select a supported connection protocol.
- ICA dial-in connections to computers running Citrix Presentation Server are no longer supported. To connect to modems, use Microsoft Remote Access Service (RAS).

Accessing Documentation

The documentation for Citrix Presentation Server includes online documentation, known issues information, and application Help, as follows:

Use Welcome to Citrix Presentation Server (Read_Me_First.html) to access the complete set of online guides on the Web. Alternatively, to access the documentation at any time, go to http://support.citrix.com/docs/.

- Online documentation is provided as Adobe Portable Document Format (PDF) files. To view, search, and print the PDF documentation, you need Adobe Reader (supported versions include 5.0.5 with Search, Version 6, 7, and 8).

- Known issues information is included in the product readme, also available on the Web. Use *Welcome to Citrix Presentation Server* (Read_Me_First.html) to access the product readme.
- In many places in the user interface, integrated on-screen assistance is available to help you complete tasks. For example, in the Access Management Console, you can position your mouse over a setting to display help text that explains how to use that control.
- Online Help is available for some tasks. You can access the online Help from the **Help** menu or **Help** button.
- For information about terminology related to Presentation Server, see the *Citrix Presentation Server Glossary*, available from the Knowledge Center at http://support.citrix.com/docs/.
- More information about Citrix documentation, and details about how to obtain further information and support, is included in *Getting Started with Citrix Presentation Server*, available from the Knowledge Center at http://support.citrix.com/docs/.

To provide feedback about the documentation, go to go to http://support.citrix.com/docs/. To access the feedback form, click the Submit Documentation Feedback link.

Deploying and Installing Client Software

The Components CD included in your Citrix Presentation Server media pack contains installation files for all the Citrix Presentation Server Clients for Windows in the Clients directory.

This chapter discusses the steps necessary for deploying and installing your client software, including:

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

System Requirements

To run Version 10.*x* of the clients, client devices must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system
- Windows NT 4.0 or later, Windows 2000, Windows XP, Windows 2003, or Windows Fundamentals for Legacy PCs
- Available memory as recommended for the operating system by Microsoft
- Internet Explorer Version 5.0 or later; Netscape Navigator or Communicator Version 4.78, 6.2, or later; Mozilla Firefox 1.0 or later

- Microsoft mouse or 100% compatible mouse
- VGA or SVGA video adapter with color monitor
- High-density 3.5-inch disk drive (optional) and available hard drive space
- Windows-compatible sound card for sound support (optional)
- For network connections to the server farm, a network interface card (NIC) and the appropriate network transport software are required

Supported connection methods and network transports are:

Protocol	**Program Neighborhood Agent**	**Web Client**	**Program Neighborhood**
TCP/IP+HTTP	X	X	X
SSL/TLS+HTTPS	X	X	X
TCP/IP		X	X

For information about configuring the clients to use SSL or TLS to secure communications, see “Configuring and Enabling Clients for SSL and TLS” on page 76.

For requirements concerning the use of the Citrix Streaming Client to provide streamed applications to the user desktop, see the *Citrix Application Streaming Guide*.

Packaging the Client Software

You can install the Citrix Presentation Server Clients for Windows using an MSI package or a cabinet file. 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 will be “silent,” requiring no user interaction.

Note: Each client installation that includes a Citrix Presentation Server Client includes the Program Neighborhood Connection Center, allowing users to see information about their current ICA connections.

Creating MSI Packages

An MSI package, Ica32pkg.msi, is provided on the Components CD. The file is approximately 5MB in size. Using the Client Packager for Citrix Presentation Server, you can wrap all of the clients into a single MSI package. You can customize the Client Packager to deploy and maintain any number and combination of clients network-wide. Based on Windows Installer technology, the Client Packager lets you install, uninstall, modify, and repair clients as well as perform controlled client upgrades.

Important: To install the client 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 or Windows Server 2003. To install clients on client devices running earlier versions of the Windows operating system, you must install the Windows Installer 2.0 Redistributable for Windows, available at http://www.microsoft.com/.

Enabling Non-Administrators to Install Clients

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

When the installer detects non-administrator credentials, a per-user version is installed in the user’s local AppData folder, which cannot be changed during installation.

Note: If the Windows Group Policy Editor setting for DisableUserInstalls is 1, non-administrator users are not allowed to install this client.

The installer package automatically upgrades a previously installed Web Client on the local machine. For information about using the client with the Web Interface, see the *Citrix Web Interface Administrator’s Guide*.

Cabinet File

Cabinet files provide the capability for users to install the Web Client automatically from a Web page. Icaweb.cab is a cabinet file for the Web Client and is approximately 3MB in size.

Configuring Your Installation Files

If you choose to use MSI packages to deploy the clients, 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. This section details how to configure these settings.

MSI packages can be configured in three ways—with the Client Packager, using command-line parameters, and through the use of transforms.

To configure an MSI package using the Client Packager

1. Copy the Client Packager (Ica32pkg.msi) from the Components CD 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*/ica32pkg.msi

   where *path*/ is the local path where you placed this file in Step 1. The Client Packager Setup wizard appears.
4. Enter the 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 clients to be included in the install package. If you select Program Neighborhood or Program Neighborhood Agent, the Setup wizard for each client appears.
7. On the **Upgrade Settings** page, choose whether or not the install package can upgrade or downgrade existing clients.
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 an MSI package using command-line parameters

1. On the machine where you want to install the client package, type the following at a command prompt:

   msiexec.exe /I *path*/ica32pkg.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. Examples of some parameters that are supported:

   - **/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** creates a verbose install log where *logfile* is the path and filename for where to save the log. Use quotes 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 Program Neighborhood Agent software. The default value is **Citrix\Citrix Access Clients**. This function is not supported during client upgrades.
     - **INSTALLDIR**=<Installation directory>, where <Installation directory> is the location where the client 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**. See “Matching Client Names and Machine Names” on page 65 for more information about this feature.
     - **CLIENT_UPGRADE={Yes | No}**. By default, this property is set to **Yes**. This installs the client if an earlier version of the client 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.

Note: If you disable pass-through authentication, users must reinstall the client 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*.

Note: The Program Neighborhood Agent 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.
- **CTX_ALLOW_CLIENT_DOWNGRADE={Yes | No}**. By default, this property is set to **No**. This prevents installation of the client over a more recent version. Set to **Yes** to allow the installation of the client to replace a more recent version. To

downgrade to a client version earlier than 9.*x*, you must also set the **REINSTALLMODE** property to **aums**.

- **REINSTALLMODE**=<mode>. The default for this property is oums. Set to aums to overwrite later versions of the client. See Microsoft Windows Installer documentation for details.

Example of a command-line installation

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

```
msiexec.exe /I ica32pkg.msi /qb-! /l*v “c:\my
logs\ica32_install.log” SERVER_LOCATION=http://
mywebinterface
```

This would:

- Install all clients with visible progress dialog boxes, but the Cancel button is disabled for the user
- Log the installation messages to “c:\my logs\ica32_install.log”
- Specify the URL (http://mywebinterface) of the server running the Web Interface that the Program Neighborhood Agent 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. The following procedure should be attempted only by those familiar with transforms and their impact upon these settings. For more information, see the *Citrix Presentation Server Administrator’s Guide*.

1. Using your preferred tool for editing Windows Installer packages, open the Client Packager (Ica32pkg.msi).
2. Enter new values for the properties you want to change in the Property table.
3. Generate the transform file and save it with an .mst file extension.
4. To install the MSI package and use the transform you just created, follow the same steps as outlined above in the procedure dealing with command-line installations. Additionally, however, you must add the following **PROPERTY=Value option**:
TRANSFORMS = *path*\“my.mst”
where *path* is the location of the transform and “*my.mst*” is its file name.

Deploying Your Installation Files

You can deliver client software to your users using several methods, depending on the size of your organization and the available resources. This section discusses some of the methods by which you can deploy your client installation files. If you are using Citrix Presentation Server in conjunction with the Web Interface, see the *Citrix Web Interface Administrator’s Guide* for information about deploying clients in that environment.

Important: MSI packages can be deployed with Windows Active Directory Services or Microsoft Systems Management Server. See your Windows or Systems Management Server documentation for more information.

Deploying Clients from a Network Share Point

In many environments, your users can access internal resources from network share points. You can centralize your client deployment by deploying an MSI package from a single network share point. Use the Client Packager to configure your installation settings, as detailed on page 16. During this procedure you can provide a UNC path to the network share point where you want to store the customized MSI package.

Note: Active Directory Group Policy can also be used to install the client software or provide the network path to your users. See your Windows or Systems Management Server documentation for more information.

Deploying the Web Client from a Web Page

You can provide a link on a Web page for users to install the Web Client.

For example, to insert the Web Client on a Web page, add the following code to a Web page to prompt the download of the Icaweb.cab file:

```
<OBJECT

classid="clsid:238f6f83-b8b4-11cf-8771-00a024541ee3"

data="np.ica"

CODEBASE="http://web-server-root/some-directory/icaweb.cab"

width='640'

height='480'

hspace='2'

vspace='2'>
```

```
<param name="Start" value="Auto">
<param name="Border" value="On">
</OBJECT>
```

Important: Add the site(s) from which the .cab file is downloaded to the Trusted Sites zone.

If you are using the Web Client with the Web Interface, see the *Citrix Web Interface Administrator's Guide* for more information about deploying this client.

Installation Options for the Clients

For each MSI package, the Setup wizard guides you through the process of installing the client 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 will continue.

The following section describes the various options you configure during Setup. Depending on the components you choose to install, you may not encounter all configuration options described in this section, or you may encounter them in different order.

Selecting a User Interface Language

The Windows Installer package includes a Multilingual User Interface, meaning it automatically installs the clients in all supported languages. Beginning with Version 10.0 of the Windows clients, language-specific installation packages are no longer available.

During the installation, the user selects a language for the user interface: German (Deutsch), English, Spanish (Español), French (Français), Japanese, Simplified Chinese, or Traditional Chinese. After the client 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 client 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.

For more information about the Multilingual User Interface and about updating the user interface language of the client, see the Advanced Concepts Guide.

Installing the Program Neighborhood Agent

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

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

Select Program Folder. Users can choose to use the default Citrix Presentation Server Client folder, specify the name of a new program folder, or add the Program Neighborhood Agent 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). Program Neighborhood Agent 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 automatically use their local user credentials for Citrix sessions from the client being installed. Pass-through authentication allows the client 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 the Program Neighborhood Agent 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 the Program Neighborhood Agent if they decide to use pass-through authentication at a later time.

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

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

Specifying Backup Server Addresses

The Web Interface lets you specify backup servers to contact if the Program Neighborhood Agent 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 *Citrix Web Interface Administrator's Guide*.

Optionally, you can specify backup URLs in the MSI package in case the Program Neighborhood Agent cannot connect to the Web Interface.

To add backup URLs to the Program Neighborhood Agent, add the following MSI property: PNA_WI_BACKUPLOCATIONS.

Then specify the backup addresses. Unlike those configured in the Web Interface, these backup addresses apply to all users.

Installing the Web Client

Installing the Web Client requires minimal user interaction. After a user accepts the Citrix License Agreement, Setup copies files to the client device. By default, the Web Client is installed in the Program Files\Citrix\Icaweb32 directory.

Installing Program Neighborhood

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

Upgrade existing client 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 client. The default value is **Upgrade the existing client**. If you are upgrading with the MSI package, you will not be 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. Computers running Citrix Presentation Server use the client name to manage system resources. By default, the machine name is used as the client name. If you do not assign a unique machine 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 Citrix Presentation Server. By default, both of these options are enabled.

Enable Pass-Through Authentication. Users must select whether or not to enable and automatically use their local user credentials for Citrix sessions from the client being installed. Pass-through authentication allows the client 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 Client Software

To uninstall a client, run the Add/Remove Programs utility from the Control Panel. Alternatively, if the client was installed or upgraded using a Windows Installer package, you can run the installer package again and select the **Remove** option.

CHAPTER 3

Configuring Client Software

After client software is deployed to your users and they install it, there are configuration steps that can be performed. This chapter discusses these steps for the Program Neighborhood Agent and Program Neighborhood—the Web Client does not require configuration. It also describes how administrators can configure settings that apply to all users of a client device, or to multiple client devices.

Configuring the Program Neighborhood Agent

This section provides an overview of the Program Neighborhood Agent and discusses how to customize user preferences and change the URL of the Web Interface server to which the client device points.

Overview of the Program Neighborhood Agent

Configure the options and settings for Program Neighborhood Agent using the associated Program Neighborhood Agent site in the Access Management Console. Each time users log on to the Program Neighborhood Agent, they see the most recent Program Neighborhood Agent configuration. Changes made while users are connected take effect when the client configuration is refreshed manually or automatically after a designated interval.

Important: The Program Neighborhood Agent requires the Citrix Web Interface.

The Program Neighborhood Agent handles the following functions:

- **User authentication.** The client provides user credentials to the Web Interface when users try to connect and every time they launch published resources.
- **Application and content enumeration.** The client presents users with their individual set of published resources.

- **Application launching.** The client is the local engine used to launch published applications.
- **Desktop integration.** The client integrates a user's set of published resources with the user's desktop.
- **User preferences.** The client validates and implements local user preferences.

For a complete list of Program Neighborhood Agent features, refer to the Client Feature Matrix available from the Client Download page of the Citrix Web site (http://www.citrix.com/).

Customizing User Preferences

This section presents information about customizing user preferences on the client device running the Program Neighborhood Agent. For example, users can define window sizes for published applications, choose when to refresh the list of available published resources, and specify where the available published resources are displayed.

To customize user preferences for the Program Neighborhood Agent

1. In the Windows notification area, right-click the **Citrix Program Neighborhood Agent** icon and choose Properties from the menu that appears.
2. On each tab, make the desired configuration changes.
3. Click **OK** to save your changes.

For more detailed information, see the online help for the Program Neighborhood Agent.

Changing the URL of the Web Interface Server

The Program Neighborhood Agent requires that you specify the location of a configuration file (Config.xml is the default configuration file) on the server running the Web Interface.

Note: To prevent users from accidentally changing their server URL, disable the option or hide the Server tab entirely.

You may ask your users to change the server URL as you create new configuration files or delete old ones.

To change the server URL in Program Neighborhood Agent

1. In the Windows notification area, right-click the **Citrix Program Neighborhood Agent** icon and choose Properties. The Server tab displays the currently configured URL.
2. Click Change URL and enter the server URL in the format http://*servername* or https://*servername* to encrypt the configuration data using SSL.
3. Click **Update** to apply the change and return to the Server tab.
4. Click **OK** to close the Properties dialog box.

To delete memorized server URLs

1. In the Windows notification area, right-click the **Citrix Program Neighborhood Agent** icon and choose Properties from the menu that appears.
2. Select the **Server** tab and click **Change URL**.
3. Click the down arrow to view the entire list of memorized server URLs.
4. Right-click the URL you want to delete and select **Delete**.
5. Click **Update**.
6. Click **OK**.

Configuring Program Neighborhood

This section explains how to configure Program Neighborhood and discusses connecting to published resources and improving performance over low-bandwidth connections.

Important: Unlike Program Neighborhood Agent, Program Neighborhood cannot be administratively configured in the Citrix Access Management 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.

Connecting to Published Resources

With Program Neighborhood, users can connect to published resources and servers running Citrix Presentation Server using:

- Application sets
- Custom ICA connections

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 non-essential settings that are not required to run the published application (such as, for example, the audio compression rate) at an application set level on the client device.

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

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 server running Citrix Presentation 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 Citrix Presentation Server for 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 running Citrix Presentation Server. This method uses one of the following network protocols:

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

- TCP/IP

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

With Microsoft Remote Access Service (RAS) or Dial-Up Networking (DUN) in combination with the client, users can connect to a server running Citrix Presentation Server. For this type of connection, the client device must meet the following requirements:

- The RAS or DUN client software must be installed on the client device
- The RAS server or third-party PPP server must be located on the same network as the computer running Citrix Presentation Server

ICA Browsing

ICA browsing is a process that locates servers and published applications in response to requests from a client.

For ICA browsing, clients communicate with the Citrix XML Service or the ICA browser, depending on the browsing protocol selected in the client.

ICA browsing occurs when:

- Users launch published applications. The client 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 Presentation Server Administrator’s Guide*.

Specifying the Network Protocol for ICA Browsing

As described previously, ICA browsing is a process in which a client transmits data to locate servers on the network and get information about the applications published in the server farm. Changing the network protocol setting allows you to control the way the client searches for computers running Citrix Presentation Server 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 clients connect to computers running Citrix Presentation Server, as described below.

For step-by-step instructions about configuring the network protocol, see the Program Neighborhood online help. For more information about using SSL to secure client-to-server communication, see “Configuring and Enabling Clients for SSL and TLS” on page 76.

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 client uses the HTTP protocol to search for computers running Citrix Presentation Server. Select this protocol when clients 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 client sends to port 80 by default. Most firewalls are configured so port 80 is open for HTTP communication.
- TCP/IP+HTTP does not use UDP (User Datagram Protocol) or broadcasts to locate servers in the server farm.
- Routers pass TCP/IP packets between subnets, which allows clients to locate servers that are not on the same subnet.

By default, if no server is specified, the client 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 clients.

You must map a computer running Citrix Presentation Server to the default name of “ica” on your network or you must specify at least one IP address in Program Neighborhood.

Note: You can configure the DNS server for the clients 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 configuring server location addresses on your client devices individually.

You can specify servers to contact for ICA browsing by entering IP addresses or DNS names of computers running Citrix Presentation Server 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 client, the client 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 client makes an HTTP connection to port 80 on the computer running Citrix Presentation Server. If the user is launching a published application, for example, Citrix XML Service sends to the client the address of a computer running Citrix Presentation Server that has the application published.

Using SSL/TLS+HTTPS for ICA Browsing

With SSL/TLS+HTTPS as the network protocol, the client uses the HTTPS protocol to search for a list of computers running Citrix Presentation Server. The client 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.

Note: The TCP/IP+HTTP and SSL/TLS+HTTPS protocols can be used only with compatible computers running Citrix Presentation Server. See the *Citrix Presentation Server Administrator’s Guide* for Windows or UNIX for information about configuring the computer running Citrix Presentation Server to use SSL/TLS.

Using TCP/IP for ICA Browsing

With TCP/IP as the network protocol, clients send UDP broadcasts to the ICA browser service on port 1604 to locate published applications and servers running Citrix Presentation Server. Select this option if all computers running Presentation Server and all clients are located on the same network.

Note: The term *master browser* refers to a browser located on a data collector.

With TCP/IP as the network protocol, the default setting for server location is (Auto-Locate). The auto-locate function works as follows:

- The client broadcasts a “Get Nearest Citrix server” packet. The first computer running Citrix Presentation Server to respond returns the address of the master browser, which is used in the next step.
- The client sends a request for the server and published application lists to the master browser.
- The master browser responds with a list of all computers on the network running Presentation Server and a list of all published applications.

To eliminate broadcasts on your network or if your network configuration uses routers or gateways, you can set a specific server address for the server that functions as the master browser.

Important: By default, server farms do not respond to clients that use UDP broadcasts for ICA browsing. Therefore, if clients are configured to use TCP/IP and to auto-locate servers, they will fail to locate servers or published applications in a server farm running MetaFrame XP or Citrix Presentation Server.

Because UDP broadcast packets do not traverse subnets, using broadcasts for ICA browsing works only if a server that responds to broadcasts is on the same subnet as the client. When the client locates a server, it communicates using directed (not broadcast) UDP to port 1604.

Because of broadcast limitations, you might prefer to enter one or more IP addresses or DNS names of computers running Presentation Server in the Address List box in Program Neighborhood. You must do this if the client is not on the same subnet as a data collector.

Improving Performance over Low-Bandwidth Connections

If you are using a low-bandwidth connection, such as a modem, you can make a number of changes to your client configuration and the way you use the client to

improve performance.

In addition, Citrix recommends that you use the latest version of Citrix Presentation Server and its clients. Citrix continually enhances and improves performance with each release. Many performance features require the latest client and server software to function.

Changing Your Client 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 client 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 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 client sends mouse and keyboard updates less frequently to the computer running Presentation 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 client audio mapping is enabled, reduce the sound quality to the minimum setting.

Changing Client 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.

Configuring Settings for Multiple Users and Devices

In addition to the configuration options offered by the client user interface, administrators can configure settings using the registry. You can make changes that apply only to specific users of a client device, or to all users of a client device. You can also configure settings for multiple client devices.

This section describes using Group Policy to remotely configure client devices, however you can use any method which updates the relevant registry entries.

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 making changes to it.

To configure settings for all users of a client device

1. Identify the setting you want to configure. Any setting from any of the client .ini files can be configured in this way.
2. Add this setting as a string registry key and value to:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences

To configure settings for the user currently logged on to a client device

1. Identify the setting you want to configure. Any setting from any of the client .ini files can be configured in this way.
2. Add this setting as a string registry key and value to:

   HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences

   Note: See your Microsoft documentation for information about updating the registry for users not currently logged on to the client device.

To configure settings across multiple client devices

Note: If you already added the icaclient template to the Group Policy Object Editor, you can omit Steps 2 to 4.

1. Open the Group Policy Object Editor.
2. Right-click the **Administrative Templates** folder and choose Add/Remove Templates.
3. Click **Add** and browse to the icaclient template on the Components CD.
4. Click **Open** to add the template, then click **Close** to return to the Group Policy Object Editor.
5. Edit the relevant settings under the **User Configuration** node or the **Computer Configuration** node as required.

   Note: You can extend the icaclient template to cover any client setting by editing the icaclient.adm file. See your Microsoft Group Policy documentation for more information about editing .adm files, and for information about applying settings to particular machines.

Optimizing the Client Environment

The following sections discuss ways you can optimize the environment in which your Citrix Presentation Server Clients will operate.

Ways in which this can be done include:

- Securing your client connections
- Improving client performance
- Facilitating the connection of numerous types of client devices to published resources
- Improving the user experience
- Utilizing connections to Citrix Presentation Server for UNIX
- Supporting naming conventions

Securing Your Client Connections

To maximize the security of your environment, the connections between Citrix Presentation Server Clients and the resources you have published must be secured. This section discusses how to configure various types of authentication for your client software.

Windows NT Challenge/Response (NTLM) Support

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 machines running Windows NT, Windows 2000, Windows XP, and Windows 2003.

Certificate Revocation List Checking

When certificate revocation list checking is enabled, the clients check whether or not the server’s certificate is revoked. By forcing clients to check this, you can improve the cryptographic authentication of the computer running Presentation Server and the overall security of the SSL/TLS connections between a client and a computer running Presentation Server.

You can enable several levels of certificate revocation list checking. For example, you can configure the client 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 certificate revocation lists are verified.

To enable certificate revocation list checking

1. On the server running the Web Interface, locate and open the Default.ica file.
2. Configure the **SSLCertificateRevocationCheckPolicy** setting to one of the following options:
   - **NoCheck.** No certificate revocation list checking is performed
   - **CheckWithNoNetworkAccess.** The local list is checked
   - **FullAccessCheck.** The local list and any network lists are checked
   - **FullAccessCheckAndCRLRequired.** The local list and any network lists are checked; users can log on if all lists are verified

   If you do not set **SSLCertificationRevocationCheckPolicy**, it defaults to **NoCheck** for Windows NT 4.0. For Windows XP and Windows Server 2003, the default setting is **CheckWithNoNetworkAccess**.

Smart Card Support

Citrix Presentation Server smart card support is based on Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. Presentation Server 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 Program Neighborhood Agent is done through the Web Interface. For more information, see the *Citrix Web Interface Administrator’s Guide*. 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. Visit http://www.microsoft.com/ for additional information about hardware PC/SC compliance.

Citrix Presentation Server 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.

SSPI/Kerberos Security for Pass-Through Authentication

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 client 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, and Citrix Presentation Server Clients for Windows 8.*x*, 9.*x*, or 10.*x*. Kerberos works only between clients and servers that belong to the same or to trusted Windows 2000 or Windows 2003 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 Citrix Presentation Server
- If the computer running Citrix Presentation 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 Presentation Server Administrator's Guide*.

Configuring Kerberos Authentication

The client, by default, is not configured to use Kerberos authentication when logging on to the server. You can set the client 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 may also depend on your deployment, because Kerberos without pass-through authentication is supported only for the Web Interface and Program Neighborhood. For the Program Neighborhood Agent, the user is prompted for credentials.

Configuring 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” client package using the Citrix Presentation Server Client Packager. To create a client package, you can execute Autorun.exe on the Components CD and select the option to create a custom Windows client installation package. During Setup, configure clients 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 that the **Single Sign On** dialog box is **Hidden**. Otherwise, users can override your configuration and set their client configuration to use pass-through authentication.

You can also configure Kerberos without pass-through authentication by modifying the settings of the Wfclient.ini file in the Citrix\ICA Client directory on a client device. For this method of configuration, you must modify Wfclient.ini on each client device for which you want to use Kerberos without pass-through authentication.

To configure the Wfclient.ini file on the client device for Kerberos logon

1. Ensure that the Wfclient.ini has the setting **SSPIEnabled=off**.
2. From Program Neighborhood, open **ICA Settings** from the Tools menu, clear **Pass-Through Authentication**, and click **OK**.
3. Log off from the client device and log back on.
4. With a text editor, open the Wfclient.ini from the Citrix\ICA Client directory and modify the following settings to:

   SSPIEnabled=on

   UseSSPIOnly=on
5. From Program Neighborhood, open **ICA Settings** from the **Tools** menu. **Pass-Through Authentication** is now selected.
6. Select **Use local credentials to log on**.

Configuring Kerberos with Pass-Through Authentication

You must use Kerberos with pass-through authentication if you want to use Kerberos with Program Neighborhood Agent.

When client configurations are set to use Kerberos with pass-through authentication, the client 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 client configuration from the user interface.

You can configure a client device to use Kerberos with pass-through authentication by modifying the settings of the Wfclient.ini file in the Citrix program files on a client device. **Change SSPIEnabled=off** to **SSPIEnabled=on** in the [WFClient] section of the Wfclient.ini file.

Program Neighborhood Agent must be closed and restarted on the client device for the settings to be applied.

Improving Client Performance

The following section discusses improving the performance of your client software by enabling SpeedScreen Browser Acceleration, auto-client reconnections, session reliability, and by utilizing the Program Neighborhood Quick Launch Bar.

Increasing Image Download Speed

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. To enable SpeedScreen Browser Acceleration, set **SpeedScreenBA** to **ON** (or **OFF** to disable it) in your .ica file.

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

Reconnecting Users Automatically

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

When this feature is enabled on a computer running Citrix Presentation Server, users do not have to reconnect manually to continue working. The client 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 is displayed 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.

Note: To disable auto-client reconnect for a particular user, add the following line to the [WFClient] section of the Appsrv.ini file located in the user's %User Profile%\Application Data\ICA Client directory:
TransportReconnectEnabled=Off

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 come out on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

To reduce the likelihood that users continue to click links or type text while the connection is being restored, mouse pointers become hourglass icons while the application is unresponsive.

Note: You can configure your system to display a warning dialog box to users when the connection is unavailable. For more information about this feature, see the *Advanced Concepts Guide for Citrix Presentation Server.*

Users of Program Neighborhood can control session reliability in their application or connection settings. Enabling or disabling **Enable session reliability** at the client overrides the session reliability settings for the server farm. Session reliability is enabled by default. Users of Program Neighborhood Agent and the Web Client cannot override the server settings for session reliability.

To enable session reliability in Program Neighborhood, select **Enable session reliability** on the **Options** tab of the settings for the application set.

Important: If session reliability is enabled, the default port used for ICA 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.

Connecting Client Devices and Published Resources

The following sections discuss how you can facilitate ICA sessions and optimize the connection of your client devices to resources published in the server farm. This can be achieved by utilizing the workspace control feature, understanding how your client drives and devices are mapped by Citrix Presentation Server, and enabling extended parameter passing. Your Citrix Presentation Server Client can also synchronize to tethered PDA devices and support local TWAIN devices for use with published applications.

Providing Continuity for Roaming Users

The workspace control feature provides users with the ability to quickly disconnect from all running applications, reconnect to applications, or log off from all running applications. You can move between 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 between workstations and access the same set of applications each time they log on to Citrix Presentation Server. 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.

Important: Workspace control is available only to users connecting to published resources with Program Neighborhood Agent 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, and works only with sessions connected to computers running Citrix Presentation Server Version 3.0, 4.0, or 4.5.

To configure workspace control settings

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 **Settings** options of the Web Interface or the **Reconnect Options** tab of Program Neighborhood Agent Properties.

The following options are available in Program Neighborhood Agent Properties on the **Reconnect Options** tab:

- **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.

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 Presentation Server Administrator’s Guide* or the *Citrix Web Interface Administrator's Guide*.

Synchronizing PDAs with Tethered USB Connections

Citrix Presentation Server supports synchronizing a USB PDA device to a Presentation Server 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 the Presentation Server Console 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 transparently control client-attached TWAIN imaging devices 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 the Citrix Presentation Server Console (**Client Devices** > **Resources** > **Other** > **Configure TWAIN redirection**). Additionally, lossy (JPEG) compression can be enabled in this policy along with choosing a high, medium, or low level of compression, if selected. A second policy rule that facilitates the administration of this feature is **Bandwidth > Session Limits > TWAIN Redirection**. This policy allows the specification of a maximum amount of bandwidth (in kilobits/ second) that may be used for TWAIN redirection.

Mapping Client Devices

The Citrix Presentation Server Client supports mapping devices on client devices so they are available from within an ICA session. Users can:

- Transparently access local drives, printers, and COM ports

- Cut and paste between the ICA session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the ICA session

During logon, the client informs the computer running Citrix Presentation 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 computer running Presentation 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 change client 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

Client drive mapping allows drive letters on the server running Citrix Presentation 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 client.

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

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

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

Client drive letter	Is accessed by the computer running Presentation Server as:
A	A
B	B
C	V
D	U

The computer running Presentation 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 client session:

Client drive letter	Is accessed by the computer running Presentation 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 disk 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 computer running Presentation 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 Presentation Server Administrator’s Guide*.

Mapping Client Printers

The Citrix Presentation Server Client supports auto-created printers. With auto-created printers, users find their local printers mapped to their sessions and ready for use as soon as they connect.

Published applications and ICA server connections configured to run a specified initial program offer users the same access to their local printers. When connected to published applications, users can print to local printers in the same way they would print to a local printer when using local applications

If a user changes a client printer setting from within an ICA session, this information is saved to the registry of either the client machine or the server. The Printer properties retention policy rule allows administrators to specify whether this information is stored client-side or server-side. By default, printer properties are always restored from the properties store if any data is stored there.

To pick up printer properties directly from the printer itself, rather than from the properties store, use the following procedure. This means that if a change is made to the printer inside the session, the client attempts to write the change back to the printer on the client machine when logging off.

To pick up printer properties directly from the printer

1. Open the client's appsrv.ini file, located in %UserProfile%\Application Data\ICAClient.
2. Add the following line to the [WFClient] section of the file:

   ```
   Win32FavorRetainedPrinterSettings=Off
   ```

   If the **Connect Client Printers at Logon** check box is selected in the Terminal Services Configuration tool or user profile, the client printers are automatically connected when users log on and are deleted when they log off if the printers do not contain any print jobs. If print jobs are present, the printers (and the associated print jobs) are retained.

   If your user profile and Terminal Services Configuration do not specify **Connect Client Printers at Logon**, you can use the **Add Printer** wizard to connect to a client printer. These printers are not deleted automatically when you log off.

   Important: For information about configuring client printing on computers running Citrix Presentation Server for UNIX, see the *Citrix Presentation Server for UNIX Administrator's Guide*.

To view mapped client printers

While connected to the computer running Citrix Presentation Server, from the **Start** menu, choose **Settings > Printers**. The Printers window opens.

The **Printers** screen displays the local printers mapped to the ICA session. When connecting to servers running Citrix Presentation Server 4.0 or later, by default the name of the printer takes the form *printername (from clientname) in session x*, for example, “printer01 (from machine01) in session 7”. *Printername* is the name of the printer on the client machine, *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.

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 (as with DOS Client printing), multiple printers can share a printer port without conflict.

Note: For more information about printing, and about managing printing using policies, see the *Citrix Presentation Server Administrator’s Guide*.

Mapping Client COM Ports

Client COM port mapping allows devices attached to the COM ports of the client device to be used during ICA sessions on a computer running Citrix Presentation 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 from the command prompt as described below. You can also control client COM port mapping from the Terminal Services Configuration tool, or using policies. See the *Citrix Presentation Server Administrator’s Guide* for more information about policies.

To map a client COM port

1. Start the client and log on to the computer running Citrix Presentation Server.
2. At a command prompt, enter

   ```
   net use comx: \\client\comz:
   ```

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, enter

```
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 computer running Presentation 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

Client audio mapping enables applications executing on the computer running Citrix Presentation 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 computer running Presentation Server and users can set it on the client device. If the client 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 Presentation Server Administrator’s Guide* for more information about policies.

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

Associating Client 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 computer running Citrix Presentation 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: The Program Neighborhood Agent 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 the Program Neighborhood Agent and if you want to take advantage of the administrative ease of content redirection from client to server, see the *Citrix Presentation Server Administrator’s Guide* for more information.

Enabling extended parameter passing requires both server- 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 Presentation Server Administrator’s Guide*.

On the client side, you must replace the **open** command for the file type with a command line that passes the file name and path to the computer running Citrix Presentation 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.

Important: Citrix Presentation Server 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 executable used to launch the published application
- The name of the published application to launch, in the correct syntax
- The parameter passing arguments

The next section explains how to determine which client executable to include in the command line.

Determining the Client 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	**Client executable**
Custom ICA connections (using Program Neighborhood Client)	Wfcrun32.exe
Applications identified in ICA files (including connecting using the Web Interface)	Wfica32.exe
Applications in application sets (using Program Neighborhood)	Pn.exe

The following section explains how to identify the published application with the correct syntax.

Identifying Published Applications

Each client 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 client 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 client 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

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 client 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:“%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:“%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:“%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:“%1”
```

Important: The above examples assume that the client devices are connecting to servers that contain remapped server drives. If your server drives are not remapped, you must add the following text to the argument: **\\client\;** for example: **/param:“\\client\%1”**.

Improving the User Experience

The following sections discuss the ways that you can improve your users’ experience, including improved support for client-side microphone input, multiple monitors, print performance, Windows key combinations, and 32-bit color icons.

Supporting Digital Dictation

Citrix Presentation Server supports client-side microphone input. This allows you to publish dictation software for use in client 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 user away from the office can establish a client 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 Presentation Server. For information about configuring this feature, see the *Citrix Presentation Server Administrator’s Guide*.

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

On the client, 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 **Properties** dialog box (for Program Neighborhood Agent).

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 client 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 client on the appropriate Windows platform, or a single video board that can support connections to more than one monitor.
- The client 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, right-click the farm in the Access Management Console and go to **Properties > Server Default > ICA >

Display and set the **Maximum memory to use for each session's graphics setting** to a large enough size (in kilobytes) to incorporate the client's 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.

Improving Print Performance

The Citrix Presentation Server Clients offer improved print performance. The following sections discuss how this is accomplished with an advanced universal print driver (UPD) and print provider and port monitor improvements.

Advanced Universal Print Driver

The Universal Print Driver (UPD) that supports Citrix Presentation Server Client print performance uses Windows' Enhanced Metafile Format (EMF) technology. EMF is a device-independent format for recording the graphical elements printed on each page of a print job. A client-side renderer uses EMF and provides a substantial reduction in the processing time of UPD print jobs on the client.

Users can choose to preview their print job in the EMF *Print Previewer* before sending the job to the client printer. This application provides a graphical representation of the pages that will be printed.

Print Provider and Port Monitor Improvements

Policies and properties settings for administering the naming of auto-created client printers and the ports to which they are bound can be accessed in the Citrix Presentation Server Console under the **Printing** node.

Note: For more information about printing, see the *Citrix Presentation Server Administrator's Guide*.

Client Session Support for Windows Key Combinations

Program Neighborhood and Program Neighborhood Agent allow the pass-through of Windows keyboard shortcuts within a remote client 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

32-Bit Color Icon Support

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

To set a preferred depth, you can add a string registry key named TWIDesiredIconColor to HKEY_LOCAL_MACHINE\SOFTWARE\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.

Supporting NDS Users

When launching client 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:

- **Program Neighborhood Agent and Program Neighborhood Client.** If NDS is enabled in the server farm, NDS users enter their credentials on an NDS tab on the client 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 computer running Citrix Presentation 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:

  A. Enable the **Dynamic Local User** policy option.

  B. 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 *Citrix Web Interface Administrator's Guide* for information about configuring your server for NDS.

Note: To use NDS logon information with earlier versions of 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 the Program Neighborhood Agent. To set a default context for NDS, you must configure the particular installer file you are using to deploy the clients.

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 client to use the user's Windows NT credentials with pass-through authentication instead, you must add a parameter to the Appsrv.ini file on the client device. You can make the addition to the Windows Installer package before distributing it, or you can configure clients on individual client devices after installation is complete.

To configure individual clients after installation

1. Locate and open the user-level Appsrv.ini file in a text editor. By default, this file is located in the %User Profile%\Application Data\ICA Client directory.
2. Add the following parameter to the [WFClient] section:

   ```
   SSOnCredentialType=NT
   ```
3. Save and close the Appsrv.ini file.

Connecting to Citrix Presentation Server for UNIX

This section describes how you can use the window manager to change the way ICA sessions are displayed when connecting to published resources on computers running Citrix Presentation Server for UNIX. It also describes utilities you can use to copy and paste graphics between local and remote applications when connecting to these servers.

Using the Window Manager

The window manager allows users to adjust the ICA session display for published resources on computers running Citrix Presentation Server 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 an ICA 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.

Switching 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.

Cutting and Pasting Graphics Using ctxgrab and ctxcapture

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

Using ctxgrab

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

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 client 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.

   Note: 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 ctxcapture

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

With ctxcapture you can:

- Grab dialog boxes or screen areas and copy them between an application in a client window and an application running on the local client device, including non-ICCCM-compliant applications
- Copy graphics between the client 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.

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 client 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.

Note: 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 client window to a local application

1. From the application in the client 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 client 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 client window to paste the information.

To copy from an application in a client window to xv

1. From the application in the client 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.

Supporting Naming Conventions for Your Network

Citrix Presentation Server Clients support the following network naming conventions: dynamic client name support and DNS name resolution.

Matching Client Names and Machine Names

The dynamic client name feature allows the client name to be the same as the machine name. When users change their machine name, the client name changes to match. This allows you to name machines 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 machine name during installation, the client name does not change when the machine name is changed.

Users enable dynamic client name support by selecting **Enable Dynamic Client Name** during client 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 clients 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. Clients connecting to published applications through the Web Interface also use the Citrix XML Service. For clients connecting through the Web Interface, the Web server resolves the DNS name on behalf of the client.

DNS name resolution is disabled by default in the server farm and enabled by default on the clients. When DNS name resolution is disabled in the farm, any client request for a DNS name will return an IP address. There is no need to disable DNS name resolution on the client.

Disabling DNS Name Resolution

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

To disable DNS name resolution on the Clients for Windows

1. Open the user-level Appsrv.ini file. By default, this file is located in the %User Profile%\Application Data\ICA Client directory.
2. Change the line **xmlAddressResolutionType=DNS-Port** to **xmlAddressResolutionType=IPv4-Port**.
3. Save and close the Appsrv.ini file.
4. Repeat Steps 1 through 3 for each user of the client workstation.

Securing Client Communication

This chapter discusses measures you can take to secure the communication between your server farm and the clients. You can integrate your client 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)
- Secure Gateway for Citrix Presentation Server or SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- A firewall
- Trusted server configuration

Connecting through a Proxy Server

Proxy servers are used to limit access to and from your network, and to handle connections between clients and computers running Citrix Presentation Server. The clients support SOCKS and secure proxy protocols.

Program Neighborhood Agent and the Web Client

When communicating with the server farm, the Program Neighborhood Agent and the Web Client use proxy server settings that are configured remotely on the server running the Web Interface. See the *Citrix Web Interface Administrator's Guide* for information about configuring proxy server settings for these clients.

In communicating with the Web server, the Program Neighborhood Agent and the Web Client 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.

Program Neighborhood

Program Neighborhood uses proxy server settings you configure locally from the client's toolbar. You can configure proxy server settings in three ways:

- Enable auto-client proxy detection
- Enable automatic proxy detection
- Manually specify the details of your proxy server

Enabling Auto-Client Proxy Detection

If you are deploying the client in an organization with multiple proxy servers, consider using auto-client proxy detection. Auto-client 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 client. Auto-client proxy detection requires Internet Explorer 5.0 through 7.0; Netscape for Windows 4.78, and 6.2 through 7.1; or Mozilla Firefox 1.0 through 1.5.

To enable auto-client 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 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**.
4. Click **OK** twice.

Enabling Automatic Proxy Detection

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.

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

To enable automatic proxy settings

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**.
4. Click **OK** twice.

Manually Specifying 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.

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

To manually specify the details of your proxy server

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

5. Click **OK** twice.

Configuring the User Name and Password

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 client 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

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

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.

6. Save your changes.

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.

Connecting with the Secure Gateway or Citrix SSL Relay

You can integrate the clients with the Secure Gateway or SSL Relay service. The clients support both SSL and TLS protocols.

- SSL (Secure Sockets Layer) 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 US 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 client and the server. No client configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

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 *Secure Gateway for Windows Administrator's Guide* 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 client 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.

Important: 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*.

Configuring Program Neighborhood Agent and Web Client for Secure Gateway

The Program Neighborhood Agent and the Web Client use settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway. See the *Citrix Web Interface Administrator's Guide* for information about configuring proxy server settings for these clients.

Configuring 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.

To configure the details of your Secure Gateway server

1. Make sure the client device meets all system requirements outlined in this guide.

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. Do one of the following:
    - 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.
7. Click **OK** twice.

Connecting with Citrix SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the computer running Citrix Presentation 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.

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 computer running Citrix Presentation Server and the Web server.

For information about configuring and using SSL Relay to secure your installation, see the *Citrix Presentation Server Administrator’s Guide*. For information about configuring the server running the Web Interface to use SSL/TLS encryption, see the *Citrix Web Interface Administrator’s Guide*.

System 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

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

Note: The clients 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 clients support or connection may fail.

About Root Certificates

See “Installing Root Certificates on the Clients” on page 79 for information about root certificates.

Important: All secure systems need to be maintained. Ensure that you apply any service packs or upgrades that Microsoft recommends.

Using Citrix SSL Relay with Non-Standard TCP Ports

By default, Citrix SSL Relay uses TCP port 443 on the computer running Citrix Presentation Server for SSL/TLS-secured communication. If you configure SSL Relay to listen on a port other than 443, you must make the client aware of the non-standard listening port number.

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.

To apply a different listening port number for all connections

1. Make sure all client 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 [WFClient] section.

   Set the value of the SSLProxyHost parameters as follows:

   SSLProxyHost=*:*SSL relay port number*

   where *SSL relay port number* is the number of the listening port.
4. Save and close the file.

To apply a different listening port number to particular connections only

1. Make sure all client 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 particular [Connection_Section].

   Set the value of the SSLProxyHost parameters as follows:

   SSLProxyHost=*:*SSL relay port number*

   where *SSL relay port number* is the number of the listening port.
4. Repeat Step 3 for all connection sections for which you want to specify a different listening port number.
5. Save and close the file.

Configuring and Enabling Clients 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 client tries to use TLS first, then tries SSL. If it cannot connect with SSL, the connection fails and an error message appears.

Forcing TLS Connections for all Clients

To force the clients (including the Web Client) to connect with TLS, you must specify TLS on the Secure Gateway server or SSL Relay service. See the *Secure Gateway for Windows Administrator's Guide* or SSL Relay service documentation for more information.

To configure Program Neighborhood to use SSL/TLS

1. Make sure the client device meets all system requirements outlined in this guide.
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. Do one of the following:
   - 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.
5. Click **OK**.

To configure the Program Neighborhood Agent to use SSL/TLS

1. Make sure the client device meets all system requirements outlined in this guide.
2. To use SSL/TLS to encrypt application enumeration and launch data passed between the Program Neighborhood Agent and the server running the Web Interface, configure the appropriate settings using the Web Interface. You must include the machine name of the computer running Citrix Presentation Server that is hosting the SSL certificate.
3. To use secure HTTP (HTTPS) to encrypt the configuration information passed between the Program Neighborhood Agent and the server running the Web Interface, enter the server URL in the format https://*servername* on the **Server** tab of the Program Neighborhood Agent **Properties** dialog box.

To configure the Appsrv.ini file to use TLS

1. Exit the client if it is running. Make sure all client 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. Set the values of these two parameters as follows:

   SSLCIPHERS={GOV | All}

   SECURECHANNELPROTOCOL={TLS | Detect}

   Set the value to **TLS** or **Detect** to enable TLS. If **Detect** is selected, the client tries to connect using TLS encryption. If a connection using TLS fails, the client tries to connect using SSL.
5. Save your changes.

Meeting FIPS 140 Security Requirements

To meet FIPS 140 security requirements, you must include the following parameters in the Default.ica file on the server running the Web Interface or in the user-level Appsrv.ini file of the local client device. See the *Citrix Web Interface Administrator’s Guide* for additional information about the Default.ica file.

To configure the Appsrv.ini file to meet FIPS 140 security requirements

1. Exit the client if it is running. Make sure all client 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. Set the values of these three parameters as follows:

   SSLENABLE=On

   SSLCIPHER=GOV

   SECURECHANNELPROTOCOL=TLS
5. Save your changes

Installing Root Certificates on the Clients

To use SSL/TLS to secure communications between SSL/TLS-enabled clients 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 clients 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 client.

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.

Securing the Program Neighborhood Agent with SSL/TLS

Make sure the client device meets all system requirements outlined in this guide.

To use SSL/TLS encryption for all client communications, configure the Program Neighborhood Agent, the computer running Citrix Presentation Server, and the server running the Web Interface as described in this section.

Configuring the Server Running the Web Interface

You can configure the server running the Web Interface to use SSL/TLS to secure the communications between the Program Neighborhood Agent and the Web server.

To configure the Web Interface to use SSL/TLS when communicating with the client

1. Select **Server Settings** from the **Configuration settings** menu.
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.

Configuring the Computer Running Citrix Presentation Server

You can configure the computer running Citrix Presentation Server to use SSL/TLS to secure the communications between the Program Neighborhood Agent and the server.

To configure Citrix Presentation Server to use SSL/TLS when communicating with the client

1. In the Citrix Access Management 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 *Citrix Presentation Server Administrator’s Guide*.

To use the SSL Relay to secure communications between Citrix Presentation Server and the server running the Web Interface

Using the Web Interface, you must specify the machine name of the server hosting the SSL certificate. See the *Citrix Web Interface Administrator's Guide* for more information about using SSL/TLS to secure communications between Citrix Presentation Server and the Web server.

Configuring the Client Device

You can configure the client to use SSL/TLS to secure the communications between the Program Neighborhood Agent and the server running the Web Interface.

To configure the Program Neighborhood Agent to use SSL/TLS when communicating with the server running the Web Interface

1. In the Windows notification area, right-click the Citrix Program Neighborhood Agent icon and choose **Properties** from the menu that appears.
2. The **Server** tab 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 and return to the **Server** tab, or click **Cancel** to cancel the operation.
4. Click **OK** to close the **Properties** dialog box.
5. Enable SSL/TLS in the client browser. For more information about enabling SSL/TLS in the client browser, see the online Help for the browser.

Note: This section assumes that a valid root certificate is installed on the client device. See "Installing Root Certificates on the Clients" on page 79 for more information.

Enabling Smart Card Logon

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

This section assumes that smart card support is enabled on the server, and that the client device is properly set up and configured 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 Citrix Presentation Server 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. For more information about enabling smart card support, see "Smart Card Support" on page 40.

Smart Card Logon with Kerberos Pass-Through Authentication

Kerberos pass-through authentication requires a smart card inserted in the smart card reader at logon time only. With this logon mode selected, the client 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.

For more information about Kerberos pass-through authentication, see "SSPI/ Kerberos Security for Pass-Through Authentication" on page 41.

Smart Card Logon without Pass-Through Authentication

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 client prompts the user for a smart card PIN when it starts up and every time the user requests a published resource.

Connecting through a Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using the clients 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), perform the following steps:

To connect to a server through a firewall

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**.
7. Click **OK** twice.

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

Enforcing Trust Relations

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

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

When trusted server configuration is enabled, computers running Citrix Presentation Server or the Access Gateway must reside in a Windows Trusted Sites zone.

To enable trusted server configuration

1. Open the Group Policy Object Editor.

   Note: If you already added the icaclient template to the Group Policy Object Editor, you can omit Steps 2 to 4.

2. Right-click the **Administrative Templates** folder and choose **Add/ Remove Templates**.
3. Click **Add** and browse to the icaclient template on the Components CD.

4. Click **Open** to add the template, then click **Close** to return to the Group Policy Object Editor.
5. Expand the **Administrative Templates** folder under the **User Configuration** node.
6. Select **Citrix Components > ICA Client > Network Routing**.
7. Double-click the **Configure trusted server configuration** setting. The **Configure trusted server configuration properties** dialog box appears.
8. Select **Enabled** and click **OK**.

To add a server to the Windows Trusted Sites zone

For step-by-step instructions about adding servers to the Windows Trusted Sites zone, see the Internet Explorer online help.

Note: 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 client uses to connect; for example if the client connects using an IP address, add the server’s IP address.

Index