Client for Windows CE for Handheld and Pocket PCs Administrator's Guide

Citrix Presentation Server™ Client for Windows CE® for Handheld and Pocket PCs,
Version 10.x

Last Updated: August 6, 2007 (AO)

Contents

Chapter 1 Before You Begin

Chapter 2 Introduction to the Client for Windows CE

Chapter 3 Installing and Configuring the Client for Windows CE

Before You Begin

Who Should Use this Guide?

This guide is for system administrators responsible for deploying, configuring, and maintaining the Client for Windows CE. This guide assumes knowledge of:

- The server to which your clients connect
- The Windows CE device
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports, and device adapters where applicable

The guide also describes administrative tasks that users can perform on the client device.

How to Use this Guide

To get the most out of this guide, review the table of contents to familiarize yourself with the topics discussed.

This guide contains the following chapters:

Chapter	Contents
Chapter 1, “Before You Begin”	Introduces the *Client for Windows CE for Handheld and Pocket PCs Administrator’s Guide* (this guide).
Chapter 2, “Introduction to the Client for Windows CE”	Provides a detailed list of features.
Chapter 3, “Installing and Configuring the Client for Windows CE”	Describes how to install and configure the Client for Windows CE.
Chapter 4, “Using Program Neighborhood Agent”	Describes how to configure and use Program Neighborhood Agent.

Accessing Product Documentation

The documentation for the Client for Windows CE includes online documentation and known issues information, 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 or 7).
- 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.
- 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.

Client for Windows CE Documentation

The documentation set for the Client for Windows CE comprises:

- *Client for Windows CE for Handheld and Pocket PCs Administrator’s Guide* (this guide)— introduces the Client for Windows CE and explains how to create, configure, and manage connections to computers running Citrix Presentation Server or to published applications
- *Client for Windows CE for Handheld and Pocket PCs OEM’s Reference Guide*—outlines how to customize the Client for Windows CE for use with OEM client devices

More information about Citrix documentation, and details about how to obtain further information and support, is available from the Citrix Web site, http://www.citrix.com/, and is included in *Getting Started with Citrix Presentation Server.*

Client Overview

The Client for Windows CE allows users to connect to computers running Citrix Presentation Server.

This guide uses the terms *click* and *double-click* instead of *tap* and *double-tap* to refer to the action of tapping on the Windows CE device screen with the stylus.

Introduction to the Client for Windows CE

Overview

This chapter contains information about new and existing client features.

What's New in this Release

The Client for Windows CE offers the following features and enhancements in this release:

- Client Lockdown and Client Selective Trust
- Program Neighborhood Agent backup URLs support
- Automatic proxy detection
- Keyboard shortcut pass-through
- Automatic port selection
- Improved panning support
- Support for 240 × 240 and 640 × 480 screens
- Support for logging on to computers running Presentation Server using smart cards

Client Lockdown and Client Selective Trust

If supported by the OEM, these features 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.

Client lockdown and selective trust consist of constraints that are placed on ICA configuration parameters, so that the client can only connect using a configuration that satisfies all the criteria specified in a lockdown profile.

Program Neighborhood Agent Backup URLs Support

Administrators can specify backup URLs for Program Neighborhood Agent in their Web Interface configuration. For information about creating backup addresses using the Web Interface, see the *Citrix Web Interface Administrator's Guide*.

Automatic Proxy Detection

This feature automatically detects a proxy server based on browser settings, so you do not have to configure the proxy server manually. For information about configuring proxy server detection, see "Configuring a Default Proxy Server" on page 39.

Keyboard Shortcut Pass-Through

You can choose whether keyboard shortcuts are interpreted on the client or server. This is needed where a keystroke or key combination has a local function that is different from the one on the application you are running.

To select shortcut behavior, see "Configuring Keyboard Shortcuts" on page 46.

Automatic Port Selection

This feature automatically tries to use alternative ports when the client fails to connect to the server on the configured port. For information about configuring ports, see "Enabling and Using Remote Access" on page 24.

Improved Panning Support

You can now pan using the arrow keys as well as the stylus.

Support for Logging On to Computers Running Presentation Server Using Smart Cards

You can now use smart cards to log on to servers. For information about logging on, see "Specifying Logon Information" on page 33.

Support for 240 × 240 and 640 × 480 Screens

Client sessions can now display correctly on 240 × 240 and 640 × 480 screens.

Existing Features

The following sections provide a brief overview of existing client features.

Important Some features are available only on certain client devices and when connecting to the most recent version of Citrix Presentation Server.

Connection Features

Session Reliability

Session reliability enables sessions to remain open and on the screen when network connectivity is interrupted, thus allowing users to view the application until the network connection is restored. This feature is especially useful for mobile users with wireless connections. If a user with a wireless link enters a tunnel and momentarily loses connectivity, the display on the client device freezes until connectivity resumes on the other side of the tunnel. Users continue to access the display during the interruption and can resume interaction with the application when the network connection is restored.

To enable session reliability, see “Session Reliability” on page 49.

Note Citrix recommends that you disable session reliability when you connect to the network using Windows Mobile Device Center or Microsoft ActiveSync.

Dynamic Session Reconfiguration

This feature creates a smoother experience for users who switch between client devices with varying display modes by reconfiguring window appearance appropriately between devices. Users don’t need to reconfigure the color depth or resolution for a session that they reconnect to on a client device with different display modes. The existing session’s display mode automatically adapts to the reconnecting client device’s display capabilities and mode preference.

Note When you move between client devices, and you try to reconnect to a disconnected session of a size and color depth greater than that specified on your current client device, the reconnection fails and a new session is created.

Auto Client Reconnect

ICA sessions can be dropped because of unreliable networks, highly variable network latency, or range limitations of wireless devices.

The auto client reconnect feature is triggered when the client detects a disconnected session and when the session reliability time-out period expires. When this feature is enabled on the server, users do not have to reconnect manually or reenter logon credentials to continue working. Automatic reconnection does not occur if users exit applications without logging off.

Roaming User Reconnect

Roaming user reconnect adds roaming capabilities to ICA sessions. Previously, ICA sessions were identified by the name of the client device from which they were initiated, and they were limited to that device. Starting with Feature Release 2 of MetaFrame XP, sessions are identified by user name. As a result, users can resume their ICA sessions from any ICA-enabled device. This allows users to start a session on one device and resume work on another.

Multiple Server Farm Support

You can now use Program Neighborhood Agent in Citrix Presentation Server deployments with more than one farm. When you configure the Web Interface to present users with applications from multiple farms, Program Neighborhood Agent automatically supports that configuration as well. For information about configuring the Web Interface, see the *Web Interface Administrator's Guide*.

Workspace Control

Workspace control enables users to switch between client devices and is especially useful to roaming or mobile users. It provides users with the ability to disconnect quickly from all running applications, reconnect to applications, or log off from all running applications. They can move between client devices and gain access to all of their applications when they 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 the computer running 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.

For more details about workspace control, see “Accessing Applications and Files Using Program Neighborhood Agent” on page 59.

Important Workspace control is available only to users connecting to published resources with Program Neighborhood Agent or through the Web Interface. However, workspace control connects or reconnects all previous active or disconnected sessions regardless of whether they were connected through Program Neighborhood Agent, Program Neighborhood, or the Web Interface.

User 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 there.

Remote Access

You may find it inconvenient to configure ICA connections locally on your client device. The Web-based approach allows you to do this “local” configuration from a remote computer, such as a PC or Macintosh, with a conventional screen and keyboard.

You can enable or disable remote access through a local Windows user interface on the client device. Remote access is disabled by default. If you enable remote access, you can specify a password that the user of the remote device has to supply. For more information about enabling remote access, see “Enabling and Using Remote Access” on page 24.

Program Neighborhood Agent

Using Program Neighborhood Agent, users connect to servers that run the Web Interface, which provides easy access to all the published applications and content that the user is authorized to use on the server farm. The client device must have a browser installed.

Program Neighborhood Agent:

- Allows you to control which settings users can modify on their own client devices. For example, you may or may not allow them to save passwords locally or modify window properties.
- Provides single sign-on to servers. With single sign-on, users supply their logon credentials only when they first connect to the server, not when they open each application.

For further information about configuring and enabling Program Neighborhood Agent, see “Using Program Neighborhood Agent” on page 53.

Automatic Network Connection

When you launch an ICA session without a network connection, the Client for Windows CE automatically establishes a network connection for your ICA session. It may request logon information if it is not already available.

Performance Features

Improved Compression Technology

New compression technology results in less data being sent over the network. This results in, for example, faster video rendering, file transfer, and printing, and provides a better overall user experience.

To reduce the amount of data transferred between the client and the server, see “Data Compression” on page 48.

Disk Caching

Commonly used graphical objects such as bitmaps are stored in a local cache on the client's file system. If the user's connection is bandwidth-limited, using disk caching improves performance.

For more information about disk caching, see “Disk Caching” on page 49.

SpeedScreen Browser Acceleration

This feature, which operates automatically, increases the speed at which images are downloaded and displayed. SpeedScreen Browser Acceleration requires Internet Explorer 5.0 or later to be installed on the server.

Improved Graphic Display Speed

Viewing graphic-intensive content over an ICA connection is now faster.

Low Bandwidth Requirements

The highly efficient ICA protocol uses very little bandwidth relative to the amount of information transferred.

Data Compression

Data compression can increase performance over low-speed asynchronous and WAN connections by reducing the amount of data sent over the communications link to the client device.

SpeedScreen Latency Reduction

SpeedScreen Latency Reduction is a collective term used to describe functionality that enhances the user’s experience on slower network connections. SpeedScreen Latency Reduction is not available when connecting to Presentation Server for UNIX. It is also not available on Japanese platforms.

SpeedScreen Latency Reduction functionality includes:

Local Text Echo

This option accelerates the display of the input text on the client device. This gives a usability improvement on high latency (not low bandwidth) connections, but it does not make applications run faster.

Mouse Click Feedback

On devices that display a mouse pointer, this option provides visual feedback for mouse clicks to show that the user’s input is being processed.

The Client for Windows CE supports high color depth and resolution for an ICA connection. Depending on the device you are using, you can configure the connection to use thousands of colors and dimensions of up to 1600 by 1200 pixels, as described in “Editing the Window Size and Colors” on page 34.

Application Features

Digital Dictation Support

Citrix Presentation Server now supports client-side microphone input. Using local microphones, users can record dictations from a device in one location and then retrieve them for review or transcription from another device or location.

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

To enable and configure digital dictation support for your client, see “Setting Sound Options” on page 35.

For information about configuring this feature, see the *Citrix Presentation Server Administrator's Guide*.

Default and Configurable Panning and Scaling

You can now set default panning and scaling settings for ICA sessions. You can specify them by individual connection or select default settings to be used for every connection.

Panning allows you to scroll an ICA session that has a higher resolution than that of your local client device. Initial panning positions for ICA sessions include **top left**, **bottom left**, **center**, and **custom**.

Scaling provides controls that enable you to shrink an ICA session to fit your screen. Scaling settings include 13 defined values between 1:1 to 32:1.

You can easily zoom in to or zoom out from the center of your screen using specific controls on the task bar. The previous method of doing this (double-clicking the original control) no longer has any effect.

Note The new controls are available only on Pocket PCs. To scale the screen on other types of device, you still double-click the original panning and scaling control.

On Pocket PCs, you can save default panning and scaling positions in the client so that a session can start up in the same position and using the same scale every time.

For more information about panning and scaling, see "Panning and Scaling" on page 50.

Input Method Editor (IME) Support

Input Method Editor (IME) is a program interface for inputting non-Latin characters. The interface can be present either on the server or on the client. It enables users to input, for example, Japanese or Korean characters. You can disable support for the client or server IME. Note that the client cannot enable the IME on either itself or the server; it can disable it only if it is already there. For more information about IME support, see "Setting IME Options" on page 36.

HTML User Interface

You can control and configure the client securely from any Web browser, locally or remotely, using the small Web server contained within the client. You create and edit connections and global settings through a set of Web pages.

Windows CE devices vary in screen size and shape; using a Web-based user interface allows existing Web browsers to fit the interface to the device's screen appropriately.

Depending on the type of device and browser you are using, you may find it necessary to double-click rather than click a link to open a Web page.

Basic File Type Association

Basic file type association is supported. You can associate files with a particular extension with a published application, so that whenever you open the file, it opens within that application.

Client Device Mapping

Client device mapping allows a remote application running on the server to access printers, drives, and devices attached to the client device.

Client Drive Mapping

Client drive mapping allows users to access floppy disk drives or CD drives attached to the client device during an ICA session. When both the server and client are configured to allow client drive mapping, users can access their locally stored files, work with them within ICA sessions, and then save them either locally or on a drive on the server.

Client Printer Mapping

Client printer mapping lets users access printers attached to the client device from applications running in an ICA session. When a computer running Citrix Presentation Server is configured to allow client printer mapping, applications running remotely on the server can print to local printers.

Client COM Port Mapping

Client COM port mapping allows users to access serial devices on the client device as if they were connected to the computer running Citrix Presentation Server. This feature is not available when connecting to servers running MetaFrame Server for UNIX Version 1.0 or 1.1.

Client Audio Mapping

Client audio mapping enables applications running on the server to play sounds through a sound device installed on the client device.

Client audio support includes configurable sound quality levels that allow you to customize sound quality based upon the amount of bandwidth available.

Web Browser Launching and Embedding

Users can access applications that are deployed on a Web site using Citrix Web Interface technology. You launch an application from a Web page by clicking a hyperlink that references an ICA file. You can then use this application as if it were installed and running on your local computer.

Note Embedding is not supported on devices running the Pocket Internet Explorer 3 browser.

Time Zone Support

This feature allows the user, when logging on to a server in a different time zone, to have the ICA session reflect the time zone of the client device.

For example: a user in London (Greenwich Mean Time) logs onto a server in New York City (Eastern time zone), and launches Microsoft Outlook as a published application. Microsoft Outlook stamps emails sent during this ICA session with the user's GMT time zone information.

Security Features

Windows NT Challenge/Response NTLM Support

Support is provided by default for networks using Windows NT Challenge/ Response for security and authentication.

Secure Proxy Support

As an alternative to SOCKS proxy, the Client for Windows CE also supports secure proxy (also known as Security Proxy, HTTPS proxy, and SSL-tunneling). Proxy authentication is also supported.

Transport Layer Security Encryption

As an alternative to Secure Sockets Layer (SSL) 3.0, the Client for Windows CE also supports Transport Layer Security (TLS) 1.0. TLS is the standardized form of SSL. Both are cryptographic security protocols designed to ensure the integrity and privacy of data transfers across public networks. SSL and TLS are functionally equivalent. Certain organizations have a security policy that requires TLS rather than SSL.

Installing and Configuring the Client for Windows CE

Overview

This chapter contains complete instructions for installing and configuring the Client for Windows CE. Topics in this chapter include:

- System Requirements
- Installing the Client for Windows CE
- Starting the Client for Windows CE
- Enabling and Using Remote Access
- Uninstalling the Client for Windows CE
- Creating a New Connection
- Connecting to a Server
- Editing a Connection
- Integrating the Client with Security Solutions
- Printing
- Configuring Keyboard Shortcuts
- Improving Performance
- Panning and Scaling

System Requirements

To run the Client for Windows CE, you require the following:

- Windows CE Core System Version 3.0 or later. The client supports Windows Mobile 5 or later.
- Pocket Internet Explorer. Note that Version 3.02 and earlier of Pocket Internet Explorer are not supported.
- A Windows CE-based device with a display that supports 16 or more colors or gray scales.
- A network interface card (NIC) connected to a local network using the TCP protocol or a modem.
- The appropriate version of the Client for Windows CE for your Windows CE device. Versions are available for the following processors: SH-3, SH-4, x86, MIPS, ARM, and ARMV4I.

Note Support for embedded applications on handheld and pocket PCs is limited. Ensure that you have the latest version of your browser installed.

Installing the Client for Windows CE

The Client for Windows CE can be installed using one of two methods:

- **Local installation**. The installation program is run on the Windows CE device from a previously downloaded setup file.
- **PC installation**. This method can be used only with Windows CE devices attached to a PC. The installation program is run on the PC that then downloads the necessary files to the Windows CE device.

Note If you are using a palm-sized device that does not have Windows File Explorer, you must install the Client for Windows CE using the PC installation method.

To install the Client for Windows CE using the local installation method

1. Copy the Client for Windows CE setup program (icasetup.*processor*.cab, where *processor* is the processor type for your Windows CE device) to the Windows CE device.

2. On the Windows CE device, launch the icasetup.*processor*.cab icon.
3. Specify the directory in which to install the client and click **OK**.
4. The license agreement appears. To accept the license agreement and continue installation, click **Accept**.

To install the Client for Windows CE using the PC installation method

1. Ensure that the Windows CE device is connected to, and synchronized with, your PC. You must have Windows Mobile Device Center or Microsoft ActiveSync installed on your PC for successful connection and synchronization.

   Note Citrix recommends that you disable session reliability when you connect to the network using Microsoft ActiveSync.

2. Double-click the *processor* icasetup.exe icon on your PC and follow the instructions that appear. The necessary files are downloaded to the Windows CE device.

   Caution Citrix Presentation Server now provides a ClientType Report that lists all client types, versions, build numbers, users, and number of connections currently open on the server or servers in your farm. See the *Citrix Presentation Server Administrator's Guide* for more details.

Starting the Client for Windows CE

To start the Client for Windows CE

Click **Start > Programs > ICA Client**.

The **Main** menu page appears listing the connections that you already created.

Note Right-click functionality is available during ICA sessions, but not in the local user interface. To simulate a right-click on a Pocket PC, you use a click and hold action. To simulate a right-click on handhelds, you tap while holding down the ALT key.

Enabling and Using Remote Access

Remote access is disabled by default for security reasons. However, if you want to configure the client from a remote device, or use a different set of user interface pages on a remote server, you need to enable remote access to the client device.

To enable remote access

1. Click **Start > Programs > ICA Client UI Settings.** The **Client Local UI** dialog box appears.
2. Select the **Enable Remote Access** check box.
3. Optionally, enter a password to be used for remote access.
4. Enter the port to use if this is different from 80. If port 80 is unavailable when the client tries to connect to the server, the client automatically tries other ports until it is successful.
5. Optionally, to access user interface pages on a remote server, enter the details of that server in the **Remote web host** and **Remote web directory** fields.
6. Click **Save**.

To use remote access from a host PC

1. Ensure that your client device is connected to the host PC.
2. Open a browser window on the host PC.
3. Enter your client's name or IP address (for example, 10.32.39.10) in the browser's **Address** field. The **Enter Network Password** dialog box appears.
4. Enter the remote access password for the client device. You do not have to type a user name.
5. The client user interface appears in the browser window. You can then configure the client just as you would on the client device.

Note You can access the Client for Windows CE on your client device directly from your PC after remote access is enabled, a password supplied, and your Windows CE device connected to your PC. Type http://*devicename*/*main.htm* in your browser and the **Main** page of the client opens. Make sure you enable remote access to your client device. See "Enabling and Using Remote Access" on page 24 for more details about how to do this.

To view your device name

1. Open your device’s **Control Panel** dialog box.
2. Select **Communications**.

   The **Communications Properties** dialog box opens. The name of your client device appears in the **Device name** box.

Uninstalling the Client for Windows CE

Before uninstalling the client, close any program that is running.

To uninstall the Client for Windows CE

1. Open your device’s **Remove Programs** dialog box.
2. Select **Citrix Systems ICA Client** and click **Remove**.
3. To complete uninstallation, click **OK**.

Creating a New Connection

You can create, configure, and run two types of ICA sessions: server connections and published applications:

- *Server connections* allow users to connect to a specific computer running Citrix Presentation Server. Users can run any applications available on the desktop, in any order.
- *Published applications* are specific applications set up by an administrator for remote users to run. When connected, users are presented with the application itself.

This chapter describes how to manually create and edit connections using the client’s local user interface.You can also use Program Neighborhood Agent to retrieve predefined ICA connection configurations from servers running the Web Interface. This avoids having to manually create and edit separate connections for each server or desktop application; users can connect to all published resources that they are authorized to use in a server farm through a single URL.

For details about configuring and using Program Neighborhood Agent, see "Using Program Neighborhood Agent" on page 53.

Note Citrix recommends that you quickly create a connection as outlined in the following procedure, and then configure the connection to best suit your needs. See "Editing a Connection" on page 27 for more details about configuring ICA connections.

To create a new connection

1. Make sure the client device is connected to the network through a network interface card (NIC), by a serial PPP connection to a Windows RAS server, or by a USB connection using Microsoft ActiveSync.

   Note Citrix recommends that you disable session reliability when you connect to the network using Microsoft ActiveSync.

2. On the **Main** menu page, click **Create New Connection**.
3. To display an up-to-date list of servers or applications, click **Refresh Servers** or **Refresh Published Applications** as appropriate.

   If the client device is not on the same network as the server you want to connect to, the server name does not appear in the list. To find it, click **Server Location**. For instructions about how to locate servers, see "To edit the server location options for a specific connection" on page 31.

4. Type the name of the server or application you want to connect to in **Server or Published Application**.

   If your connection is to an application, you can associate the application with a particular file type on the client. For details about how to do this, see "Associating a File Type with an Application" on page 32.

5. To create the connection, click **Save**. The client automatically uses the name of the server or application as the title for the new connection that appears on the **Main** menu page.

6. To change the connection settings, return to the **Main** menu page, select the name of the connection, click **Edit Settings**, and follow the instructions provided in “Editing a Connection” on page 27.

Important Do not use the following characters in your connection name: ` ! " % ^ & * ( ) { } \ @ ~ # | < > ? /

To edit the connection you just created, see “Editing a Connection” on page 27.

Connecting to a Server

To start a previously defined connection

On the **Main** menu page, select the name of the relevant connection from the list, then click **Connect**.

You are now connected to the server or published application of your choice.

If you specified a valid user name and password for the connection, you are logged on as that user. If no user name and password are present for the connection or the information is incorrect, the **Server Logon** dialog box appears. Enter a valid user name and password for the server and click **OK** to log on.

Note If the client device’s keyboard has predictive text enabled, you may want to disable this feature to prevent the prediction of logon credentials.

The client can automatically establish a network connection for your ICA session when you launch a session without a network connection. The client may request logon information if it is not already available.

To make a network connection automatically

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.
3. Select **Enable Auto-Connect to Network**.

Editing a Connection

This section describes how to edit the properties of an existing connection.

To edit the properties of a connection

1. On the **Main** menu page, select the connection you want to change, then click **Edit**. The **Edit Settings** page appears with the name of the connection displayed at the top of the page (for example, **Edit Server1 Settings**). You can choose any of the following:

    - The **Edit Server Settings** option, where you can set the server or published application name to which to connect. You can also display the **Server Location** dialog box to set server location options. See “Configuring Network Protocol and Server Location” on page 29.

    - The **Edit Application Settings** option, where you can specify an application to run after connecting to the server. See “Specifying an Application to Run after Connecting to a Server” on page 32.

    - The **Edit Login Information** option, where you can set the user name, password, and domain to use for automatic logon to the server. See “Specifying Logon Information” on page 33.

    - The **Window Settings** option, where you can set the session size and the color depth for the ICA session window. See “Editing the Window Size and Colors” on page 34. You also use this option to set initial panning and scaling positions for Pocket PCs. See “Setting Initial Panning and Scaling Positions” on page 51.

    - The **Edit Options** option, where you can control the connection between the server and the client device by setting configuration options for compression, session reliability, bidirectional sound, encryption, SpeedScreen support, IME support, and disk caching. For more information about these options see “Data Compression” on page 48, “Session Reliability” on page 49, “Setting Sound Options” on page 35, “Using Encryption” on page 41, “Setting IME Options” on page 36, and “Disk Caching” on page 49, respectively.

    - The **Edit Title** option, where you can change the name of the connection. You can also use this option to associate a file type with a published application. See “Associating a File Type with an Application” on page 32.

    - The **Edit Firewall Settings** option, where you can configure the client to use a SOCKS/secure proxy, alternate address remapping, and a Secure Gateway address. See “Integrating the Client with Security Solutions” on page 37 for more information about using the client with a firewall. See “Using Encryption” on page 41 for more information about using SSL/TLS.

2. Make the desired changes.

3. Click **Save**.

Note Workspace control is available only to users connecting to published resources with Program Neighborhood Agent or through the Web Interface. Workspace control connects or reconnects all previous active or disconnected sessions regardless of whether they were connected through Program Neighborhood Agent, Program Neighborhood, or the Web Interface.

Configuring Network Protocol and Server Location

This section outlines:

- Available network protocols
- Business recovery
- Server location (server browsing) options and how to change them

All of the above are configured from the **Server Location** page. You can configure the settings for a specific connection, as described on page 31, or you can configure default settings to be used for all new connections, as described on page 31. Note that these settings do not apply to Program Neighborhood Agent connections.

Network Protocol

The *network protocol* setting allows you to control the way the client locates servers. The network protocols are:

- TCP. The client uses the UDP protocol to locate servers. The client communicates with the server using ICA protocol over TCP. To keep the UDP protocol working, you must ensure that the relevant option on the server is switched on; for further details about this, see your Citrix Presentation Server documentation.
- TCP + HTTP. The client uses the HTTP protocol to locate servers. The client communicates with the server using ICA protocol over TCP. Select this option when using the client over the Internet or through a firewall or proxy server. This is the default protocol.
- SSL/TLS + HTTPS. The client uses the HTTPS protocol to locate servers. The client communicates with the server using ICA with SSL/TLS. SSL/TLS provides strong encryption of ICA traffic and server authentication. Select this option when using the client over the Internet or through a

firewall or proxy server. See "Using ICA Encryption with SSL/TLS" on page 42 for more information about configuring SSL/TLS.

Note When the TCP or TCP+HTTP protocols are selected, the ICA protocol can be encrypted using ICA encryption. See "Using ICA Encryption" on page 41 for more information.

Business Recovery

Business recovery provides consistent connections to published applications and servers in the event of server disruption. You can define up to three groups of servers to which you want to connect: a primary and two backups. Each group can contain from one to five servers. When you specify a primary server group for your client, the client attempts to contact all the servers within that group, the server or servers respond, and you connect to the server. If all the servers in the primary group fail, the client attempts to contact servers in the first backup group, and then the second backup group if necessary.

Server Location

*Server location (*also called *server browsing)* provides a method for a user at a network-connected client to view a list of all servers on the network that have ICA connections configured, and a list of all published applications. The way in which server location works depends on which network protocol is configured:

- TCP. The default setting for server location is **auto-locate**. The client attempts to contact any of the servers on the subnet by broadcasting on the UDP protocol. Alternatively, you can set specific addresses for computers running Citrix Presentation Server.

  Note TCP browsing fails on a Pocket PC device when the device has fixed IP information, has the server address set to auto-locate, and is connected to the PC using Microsoft ActiveSync. If the user manually removes the device from the network, resets it, reconnects to the network, and then browses again, a list of servers is successfully returned.

- TCP+HTTP and SSL/TLS+HTTPS. The default server address is **ica**. When using SSL, you must set fully qualified domain names (FQDN) for servers. The client uses either the HTTP or HTTPS protocol to contact the servers.

To edit the server location options for a specific connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Server Settings**.
3. On the **Server Settings** page, click **Server Location**.
4. Select the appropriate protocol.
5. Select the group that you want to configure, if this is different from the current group. You can configure your Primary, first backup (Backup 1), or second backup (Backup 2) group. You can create lists of specific servers in the server group you select.
6. Enter the name or IP address of a computer running Citrix Presentation Server.
7. Add or remove servers as necessary. Click **Save**.

To set default server location options for new connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Server Location**.
3. Select the appropriate protocol. For more information about available protocols, see "Network Protocol" on page 29.
4. Select the group that you want to configure, if this is different from the current group. You can configure your Primary, first backup (Backup 1), or second backup (Backup 2) group. You can create lists of specific servers in the server group you select.
5. Enter the name or address of a computer running Citrix Presentation Server.
6. Add or remove other servers as necessary.
7. If you need a time-out period for server browsing that is different from the default of 1000 milliseconds, enter the required number in the **Time-out** box.
8. Click **Save**.

Specifying an Application to Run after Connecting to a Server

Use the **Edit Application Settings** option to specify an application to run after connecting to a server. If you specify an application, users do not see the Windows desktop when they connect, and the connection is closed when they exit the application.

Note This option is not available for connections to published applications.

To specify an application to run after connecting to a server

1. On the **Main** menu page, select the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Application Settings**.
3. In the **Application** box, specify the path and file name of the application to be run after connecting to the server. For example, to launch Microsoft Notepad automatically after connecting to a server, type:

   ***C*:\Windows\Notepad.exe**

   where *C*: represents your server drive.
4. In the **Working Directory** box, specify the working directory to be used with the application. For example:

   C:\*YourProfile*\ My Documents
5. Click **Save**.

When users log on to the server, Microsoft Notepad runs; if they select **Open** from the **File** menu, the **C:\*YourProfile*\ My Documents** folder appears.

Associating a File Type with an Application

You can associate a published application with a particular file type on the client. This means that when a user opens a file, it is opened within that particular application.

Note that locally configured file type association is not available for applications that you run after connecting to a server, from a Web page, or for Program Neighborhood Agent applications.

To associate a file type with an application

1. On the **Main** menu page, click the name of the published application that you want to update, then click **Edit**.

2. On the **Edit Settings** page, click **Edit Title**.
3. On the **Title** page, in the **Associated Filetype** box, specify the file extension to associate with the published application.

   For example, to associate .txt files with your Microsoft Notepad published application type

   .txt.
4. Select **Create a Desktop shortcut** to place a shortcut to this application on your virtual desktop.

   Note This option is not available to users of Pocket PC devices.
5. Click **Save**.

Specifying Logon Information

You can include the settings needed to log on to the computer running Citrix Presentation Server as part of the connection. This saves time when connecting to the server but is less secure than prompting users for credentials each time they connect.

To specify logon information

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Logon Information**.
3. Enter a valid user name, password, and domain (where applicable). If you leave these boxes blank, users are prompted for a user name, domain, and password each time they connect to the server or published application. You can complete some boxes and leave others blank; for example you may want to enter the user name and domain, but leave the password blank for security purposes.

   Note If the client device's keyboard has predictive text enabled, you may want to disable this feature to prevent the prediction of logon credentials.
4. If you intend to log on using a smart card, select the **Allow Smart Card logon** check box. You can log on to servers using smart cards only from custom connections, and not connections established using the Web Interface or Program Neighborhood Agent.

5. Click **Save**.

Editing the Window Size and Colors

You can edit the window size and the number of colors used in ICA connection windows from the **Edit Window Settings** option. You can also set initial panning and scaling positions for Pocket PCs.

To specify the window colors and size for a connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Window Settings**.
3. In the **Window Colors** box, set the number of window colors to 16, 256, or High Color (16 bit).

Note The option to set High Color (16 bit) is available only if the client device is capable of high-color display. This option is shown only if the client software detects that the client device supports more than 256 colors.

4. You can either set the window size in pixels, or set it to the actual screen size of the Windows CE device by selecting **Change to Fit to Screen**. Remote session size can be configured depending on the maximum allowed by server video mode and any limitations imposed by the administrator.

   For details about setting initial scale factors and panning positions, see "Setting Initial Panning and Scaling Positions" on page 51. Note that these fields do not appear if you selected the **Change to Fit to Screen** option.

Note The options to set initial scale factors and panning positions are available only on Pocket PCs.

5. Click **Save**.

To edit Windows preferences for all connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.

The following settings are configured in the global **Preferences** option:

- **Default Window Width and Height.** Set the window size in pixels. You can configure a remote session size of up to 1600 by 1200 pixels.

  Note If the you rotate the screen, the ICA session might not cover the whole screen.

- **Default Window Colors. S**elect 16, 256, High Color, or True. When using a low-bandwidth connection, 16 color mode may provide better performance. The options to select High Color or True color are not available if your device is not capable of high color display.

The following options are available only on Pocket PCs:

- **Enable Palette Device**. If your device has a configurable hardware palette, select this check box to increase graphic presentation performance. If no hardware palette is present on the device, do not enable this feature or graphics will display incorrectly.
- **Enable Full Screen (No Local Task Bar)**. Select this check box to remove the local task bar from view. Citrix recommends this option for custom applications that require Fit to Screen mode and that do not require the Soft Input Panel (SIP) keyboard.

3. Click **Save**.

Setting Sound Options

To set sound options

1. On the **Main** menu page, click the name of the connection that you want to edit and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. To enable sound support, select one of the following quality levels from the **Sound Quality** list:

   - **Low**. This setting is recommended for low-bandwidth connections, including most modem connections. This setting causes any sound sent to the client to be compressed to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the **Medium** setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

- **Medium**. This setting is recommended for most LAN-based connections. This setting causes any sound sent to the client to be compressed to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device. The host CPU utilization decreases compared with the uncompressed version due to the reduction in the amount of data being sent across the wire.
- **High**. This setting is recommended only for connections where bandwidth is plentiful and sound quality is important. This setting allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.

4. From the **Microphone Input** list, select one of the following values:
   - **Disabled**. Selecting this option means that no sound can be recorded from a local microphone.
   - **Enabled**. Selecting this option means that users can record dictations with applications running on the server using local microphones. For example, a user away from the office can establish a client session to record notes. Later in the day, the user can retrieve the notes for review or transcription from the desktop device at the office.
   - **Ask before use**. Selecting this option means that a local user receives a message asking permission to record from the local microphone.

Note For information about configuring this feature on the server, see the *Citrix Presentation Server Administrator's Guide*.

Setting IME Options

To set IME connection options

1. On the **Main** menu page, click the name of the connection that you want to edit and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. To disable IME support on the client or server, select **Disable Client IME** or **Disable Server IME**. Note that the client cannot enable the IME on either itself or the server; it can disable it only if it is already there. The

settings to use depend on the version of Citrix Presentation Server your server is running:

- By default, client IME is enabled and server IME is disabled. Use this configuration for connecting to a server running Citrix MetaFrame XP Server for Windows, Feature Release 3 or later. Any character or symbol the user enters on the local keyboard or IME is sent to the server, which then attempts to pass it on to its applications.
- For servers running earlier versions of MetaFrame XP, Feature Release 3, disable the client IME but do not disable the server IME. Users must enter non-Latin characters through the server's IME. Any non-Latin character generated by the client's own keyboard or other input device is ignored.

To edit IME preferences for all connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.
   - **Disable Client IME**. Select this check box to disable client-side IME support for all connections.
   - **Disable Server IME**. Select this check box to disable server-side IME support for all connections.

Integrating the Client with Security Solutions

If your network is using a proxy server, for example to limit access to the computers running Citrix Presentation Server, you must configure the client to connect to the server through the proxy server.

The Client for Windows CE supports both SOCKS proxy and secure proxy protocols. Secure proxy is an alternative to SOCKS proxy and is also known as Security Proxy, HTTPS proxy, and SSL-tunneling.

Note The security solutions described in this section are not applicable to Program Neighborhood Agent connections. Security settings for Program Neighborhood Agent are specified on the server or using the Web Interface.

Configuring the Client to Use a SOCKS Proxy Server

If you want to connect to a computer running Citrix Presentation Server beyond a firewall and your network is using a SOCKS proxy server, you must configure the client to connect to servers through the SOCKS proxy server. You can configure a SOCKS proxy for a specific connection or a default SOCKS proxy for all connections.

To configure a SOCKS proxy for a specific connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Firewall Settings**.
3. Select **SOCKS** from the **Proxy** list. In the **Proxy Address** box, enter the SOCKS proxy server's IP address or DNS name. If you are unsure of this information, contact your security administrator.
4. In the **Port** box, enter the proxy server's port number (if different from 1080).
5. Click **Save**.

To configure a default SOCKS proxy server for all connections, see "Configuring a Default Proxy Server" on page 39.

Configuring the Client to Use a Secure Proxy Server

If you want to connect to a server beyond a firewall and your network is using a secure proxy server, you must configure the client to connect to servers through the secure proxy server. You can configure a default secure proxy for a specific connection or for all connections.

To configure a secure proxy server for a specific connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. Click **Edit Firewall Settings**.
3. Select **Secure (HTTPS)** from the **Proxy** list.
4. In the **Proxy Address** box, enter the secure proxy server's IP address or DNS name. If you are unsure of this information, contact your security administrator.

5. In the **Port** box, enter the secure proxy server's port number if different from 1080.
6. To enable SSL/TLS relay, enter the address in the **Secure Gateway Address** box. If you are unsure of this information, contact your security administrator.
7. Click **Save**.

Configuring a Default Proxy Server

Use Global ICA Client Settings to configure a default SOCKS or secure proxy server, and SSL/TLS relay settings for all new connections. You can alternatively configure the client to use the default proxy server specified in the Microsoft Internet Explorer settings.

To configure a default SOCKS proxy server

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Firewall Settings**.
3. Select **SOCKS** from the **Proxy** list.
4. In the **Proxy address** box, enter the SOCKS proxy server's IP address or DNS name. If you are unsure of this information, contact your security administrator.
5. In the **Port** box, enter the proxy server's port number (if different from 1080).
6. Click **Save**.

Now all connections are made through the default SOCKS proxy server you specified.

Note SOCKS does not work with UDP browsing.

To configure a default secure proxy server

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Firewall Settings**.
3. Select **Secure (HTTPS)** from the **Proxy** list.
4. In the **Proxy Address** box, enter the secure proxy server's IP address or DNS name. If you are unsure of this information, contact your security administrator.

5. In the **Port** box, enter the secure proxy server's port number if different from 1080.
6. To enable SSL/TLS relay, enter the address in the **Secure Gateway Address** box. If you are unsure of this information, contact your security administrator.
7. Click **Save**. A message appears, reminding you that you need to use SSL or 128-bit encryption to ensure a secure connection; for details about using encryption see "Using Encryption" on page 41. Click **Save** again to save your changes.

Important If you configure a default secure proxy, you must specify at least one server on the **Server Location** page for server and published application browsing to work. See "Server Location" on page 30.

Now all new connections are made through the default secure proxy server you specified.

To use Internet Explorer to set your default proxy server

Note The proxy server is identified in Internet Explorer's **LAN Settings** dialog box.

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Firewall Settings**.
3. Select **Use Web browser proxy settings**.

Connecting to a Server across a Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using ICA through a network firewall, use the information provided in this section to configure the firewall settings.

If the firewall uses address remapping, you must configure the client to use the alternate address returned by the data collector. This is necessary whether or not you are using a SOCKS/secure proxy server.

To use alternate address translation for a specific connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Firewall Settings**.

3. Click **Use alternate address through firewalls**.
4. Click **Save**.

To use alternate address translation for all connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Firewall Settings**.
3. Click **Use alternate address through firewalls**.
4. Click **Save**.

Using Encryption

Encryption increases the security of ICA connections. The Client for Windows CE supports two encryption protocols:

- *ICA encryption* provides strong encryption to increase the privacy of your ICA connections. It can be used in conjunction with the TCP and TCP+HTTP network protocols.
- *ICA with SSL/TLS* provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server to which you are connecting is a genuine server.

Using ICA Encryption

To change the encryption settings for an ICA connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. Select the level of encryption you want to use from the **Encryption Level** list. The default level is **Basic**. Select **128 bit - logon only** to use encryption during authentication.
4. Click **Save**.

Important The server must be configured to allow the selected encryption level and greater. For example, if the server is configured to allow RC5 56-bit connections, the client can connect with RC5 56- or 128-bit encryption.

Using ICA Encryption with SSL/TLS

To enable SSL/TLS you must:

- Ensure that your servers support SSL/TLS or have the SSL/TLS relay service installed. See your Citrix Presentation Server documentation for more information about configuring SSL/TLS on the server.
- Change the Server Location protocol to SSL/TLS+HTTPS. See "Server Location" on page 30 for a description of how to do this.
- If the SSL/TLS relay is not installed on a computer running Citrix Presentation Server, or is configured to use a port other than 443, specify the SSL/TLS relay's address and port.

To specify an address and port for the SSL/TLS relay for an ICA connection

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Firewall Settings**.
3. In the **Secure Gateway Address** box, enter the SSL/TLS relay's fully qualified domain name (FQDN).
4. In the **Port** box, enter the SSL/TLS relay's port number (if different than 443).
5. Click **Save**.

To use your own SSL/TLS certificates

Copy your root certificates into the Citrix folder on your client device.

If SSL/TLS is enabled, the client can connect to a server running the Web Interface only if the certificates are installed on the client device using the Microsoft AddRootCert Utility. You can download this utility from the Microsoft Web site (http://www.microsoft.com/).

Printing

Users can access printers attached to a client device from an ICA session. When a computer running Citrix Presentation Server is configured to allow client printer mapping, applications running remotely on the server can print to local printers.

Configuring Citrix Presentation Server for Client Printing

Before users can print from a client to a local or network printer, printing must be enabled on the computer running Citrix Presentation Server. This section describes how to enable printing on the server.

Mapping Client Printers on Citrix Presentation Server for Windows

Users can view mapped client printers and map new printers manually.

To view mapped client printers when connected to a server

1. While connected to a server, select **Start** > **My Computer** within the session.
2. Select **Control Panel**, and then **Printers**. The **Printers** dialog box appears.The **Printers** dialog box displays the mapped local printers along with any other printer available on the server. The name of the printer is *clientname#port*, where *clientname* is the name you assigned to your client and *port* is the printer port on your Windows CE device; for example, COM1 or LPT1.

To map a client printer manually on a server

1. Log on to the computer running Citrix Presentation Server.
2. Click **Start > Programs > Citrix Administration Tools > ICA Client Printer Configuration**.
3. On the **Printer** menu, click **New**.
4. Follow the steps in the wizard to map the client printer.

Mapping Client Printers on Citrix Presentation Server for UNIX

This section describes how to enable printing on a UNIX server. It describes how users can list available client printers and print files from the command line or from applications.

In a UNIX environment, the application performs the print rendering. The printer driver is specified inside the application or, in the case of a desktop utility, raw text is generated.

Note For further information about printing on Citrix Presentation Server for UNIX, see the *Citrix Presentation Server Client for UNIX Administrator's Guide*.

Setting up Printing

To check if client printing is currently enabled or disabled

1. Log on as an administrator.
2. At a command prompt, type:

   ctxcfg -p list

   A message stating whether or not client printing is enabled appears.

To enable or disable client printing

1. Log on as an administrator.
2. At a command prompt:

To	Type
Enable client printing	**ctxcfg -p enable**
Disable client printing	**ctxcfg -p disable**

To display mapped client printers

At a command prompt, type **ctxprinters**.

A list of printers configured on the client and mapped for use from the ICA session appears. **(default)** appears after the printer that is the default. The following information is shown for each printer:

- Printer name or printer port (for example, LPT1). This can be used in the **ctxlpr -P** command to specify a printer other than the default.
- Printer driver name. This is for information only.
- Printer connection description. This is for information only.

Printing from the Client

Procedures for printing from client devices vary according to the type of server.

Printing from the Client on Presentation Server for Windows

To print a file from a client session, users should first define a printer in the usual way. See your client device documentation for further information. Note that users must enter the complete path to correctly define a network printer. Printing to a network printer works by sending the print data to the network printer through the server.

Printing from the Client on Presentation Server for UNIX

To print a file from a client session

1. On the client device, open a command prompt and type **ctxprinters**.
2. From the results of ctxprinters, identify the printer or printer port that you want to use. To print to a printer other than the default, make a note of the printer name from the ctxprinters listing.
3. At a command prompt:

To	Type
Print the file named *filename* to the default printer.	**ctxlpr** ***filename***
Print a series of files to the default printer. Each file is treated as a separate print job.	**ctxlpr** ***filename1 filename2***
Print a file to a printer (or printer port) other than the default. This is the printer name or printer port shown in the first column of the output from ctxprinters.	**ctxlpr -P [Printername | Printerport]** ***filename***
Print a file in the background.	**ctxlpr -b** ***filename***
Print a file only if the printer is not in use. Use this option to stop an application from waiting while other printer jobs are handled. If the printer is in use, an error message appears.	**ctxlpr -n** ***filename***

To print from applications

The exact configuration of how to set up printing from UNIX applications depends on the behavior and user interface of the application.

If the user interface for an application allows you to specify the actual printer command to use when printing, you can configure client printing by replacing the **lpr** or **lp** command with the **ctxlpr** command.

Note If the application does not allow you to specify the actual printer command to use when printing, determine if the application (or window manager) uses a configuration file where you can replace the **lpr** command functionality with **ctxlpr**.

When a user connects to the server and prints from the application in a session, the server redirects the output to the mapped client printer.

Often, in this type of application, you can also specify the command-line modifiers on a different line. You can use the same switches for **ctxlpr** as when printing from the command line. For example, use **-P** with a printer name (or printer port) to print to a printer other than the default; use **-b** for background printing, and so on.

Configuring Keyboard Shortcuts

The Client for Windows CE provides users with keyboard shortcuts that can be used during ICA sessions to control various functions. Some keyboard shortcuts control the behavior of the client itself while others emulate standard Windows keyboard shortcuts.

When you want to use a Microsoft Windows key combination during a session, use the mapped keyboard shortcut instead. The following table lists the default client keyboard shortcuts.

Name	Default Value	Description
Status Dialog	CTRL+6	Displays client connection status.
Close Session	CTRL+2	Disconnects the client from the server and closes the client window on the local desktop. Using this keyboard shortcut leaves the ICA session running in a disconnected state on the server. If you do not want to leave your session running in a disconnected state, log off instead.
ESC	CTRL+3	Gives you the functionality of an ESC key on your device.
CTRL-ALT-DEL	CTRL+4	Displays the **Windows NT, Windows 2000, Windows.NET 2003 or Windows XP Security** dialog box on the server.
CTRL-ESC	CTRL+5	On servers, the Windows **Start** menu appears.

Name	Default Value	Description
ALT-ESC	CTRL+7	This keyboard shortcut cycles the focus through the minimized icons and open windows of applications running in your ICA session.
ALT-TAB	CTRL+8	This keyboard shortcut cycles through all applications in the ICA session. A pop-up window appears and displays the programs as you cycle through them. The selected application receives keyboard and mouse focus.
ALT-BACKTAB	CTRL+9	Like the ALT+TAB keyboard shortcuts, this key sequence cycles through applications that are open in the ICA session, but in the opposite direction. The chosen application receives keyboard and mouse focus.

Note The default keyboard shortcuts are mapped to suit Windows servers. These keyboard shortcuts can correspond to different actions in your respective UNIX Windows Manager.

If you have a palm-sized device, you can enter keyboard shortcuts using the virtual keyboard.

To edit the default keyboard shortcuts

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Keyboard Shortcuts**.
3. Use the lists of keys to change the default keyboard shortcut key sequences.
4. Click **Save**.

   Note You can disable one or more keyboard shortcuts by selecting **Disabled** in the appropriate lists.

If you use a Pocket PC device, you might encounter instances where a key has a local function, such as F8 rotating the screen, and also a remote function on the server. You can choose to have all shortcuts affect the remote application or the client, or choose to use the shortcuts locally only displaying the session full screen.

To choose to apply keyboard shortcuts to remote or local desktops

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.

3. Choose which desktop the shortcuts should affect from the **Apply Windows key combinations** list.
4. Click **Save**.

Improving Performance

Note The data compression and SpeedScreen Latency Reduction Features are not available for connections created using Program Neighborhood Agent.

Data Compression

Data compression reduces the amount of data transferred during the ICA session. This requires additional processor resources to compress and decompress the data, but can improve performance over bandwidth-limited connections.

To enable data compression

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. Select **Compress Data Stream** to reduce the amount of data transferred across the ICA session.

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.

Important SpeedScreen Latency Reduction works only if the SpeedScreen feature is enabled on the server to which you are connecting. If SpeedScreen is not enabled on the server, the client connects, but SpeedScreen functionality is not available. Also, this feature does not work if your screen is scaled to anything other than normal 1:1 size using the scaling feature.

To edit SpeedScreen Latency Reduction settings

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.

2. On the **Edit Settings** page, click **Edit Options**.
3. From the **SpeedScreen** list, select the setting you need:
   - If you are not certain of the connection speed, set the mode to **Auto** to turn SpeedScreen on or off depending on the latency of the connection
   - For slower connections (for example, if you are connecting over a WAN or a dial-in connection), set mode to **On** to decrease the delay between user input and screen display
   - For faster connections (for example, if you are connecting over a LAN), set mode to **Off**

Disk Caching

Disk caching stores commonly used graphical objects such as bitmaps in a local cache on the client. If the connection is bandwidth-limited, using disk caching increases performance. If the client is on a high-speed LAN, you do not need disk caching.

To enable disk caching

1. On the **Main** menu page, click the name of the connection that you want to change and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. Select **Use Disk Cache**.

Session Reliability

The session reliability feature enables you to continue to see a published application's window if the connection is interrupted.

Note Citrix recommends that you disable session reliability when you connect to the network using Microsoft ActiveSync.

To enable session reliability

1. On the **Main** menu page, click the name of the connection that you want to edit and click **Edit**.
2. On the **Edit Settings** page, click **Edit Options**.
3. Select **Session Reliability** and enter a port number. The default port number is 2598. Session reliability tides the application over for a default

three minutes, after which the Automatic Reconnect feature takes over. Any text that users enter is cached and displayed when the session is restored.

Note For session reliability to be successful, you need to enable session reliability on the server. You can also configure the port number and the time period that session reliability maintains the interrupted connection without moving to reconnect. For more details about how to do this, see the *Citrix Presentation Server Administrator's Guide*.

Panning and Scaling

Because remote sessions are often larger than the actual screen size of the Windows CE device, you need to pan (scroll) the screen to move around the remote desktop or scale (resize) the remote desktop so that you can see more of it on your screen.

Note that SpeedScreen Latency Reduction does not work if your screen is scaled to anything other than normal 1:1 size. For more information about SpeedScreen Latency Reduction see "SpeedScreen Latency Reduction" on page 48.

Panning and scaling work differently depending on whether you are using a handheld PC or Pocket PC.

Panning and Scaling on Handheld PCs

To pan (scroll) a remote desktop that is much larger than the viewable area on the client device, use either the arrow keys or the *virtual screen control*.

The virtual screen control is a small gray square at the far top right of the window. It is enabled automatically each time you launch a remote session with window dimensions configured to a size that is larger than the client desktop.

To move the virtual screen control around in the session, press the CTRL key and drag the control.

To use the virtual screen control to pan over the remote desktop, drag the dark gray bar within the virtual screen control up or down, and left or right.

Your ability to scale the remote desktop size depends on how you set the *display scale factor*. This allows you to select whether or not you can scale the remote desktop and, if so, how much flexibility you require.

To set the display scale factor

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.

3. Choose one of the **Default Display Scale Factor** settings:

   - To use the intermediate zoom factor, select **Intermediate**. This allows you to use the virtual screen control to resize the remote desktop to an intermediate size; that is, the average of the size of the remote desktop and the viewable area on the client device.

     If you select **Intermediate**, clicking once on the virtual screen control reduces the size of the remote desktop to fit the available client area. Clicking a second time resizes the remote session to the intermediate size. Clicking the virtual screen control a third time resizes the remote desktop to the default screen size.

     Note The intermediate zoom feature is available on handheld devices only. For Pocket PC devices, see “Panning and Scaling on Pocket PCs” on page 51.

   - If you want to be able to scale the remote desktop size to fit the available client area but you are not interested in the intermediate zoom factor, select **Normal**. This is the default.

     To scale the remote desktop size to fit the available client area, double-click the virtual screen control. To resize the remote desktop to the default screen size, double-click again.

   - If you do not need to scale the remote desktop at all, select **Disabled**. Clicking or double-clicking the virtual screen control then has no effect.

Panning and Scaling on Pocket PCs

To pan (scroll) a remote desktop that is much larger than the viewable area on the client device, use the *virtual screen control*. This control is described in “Panning and Scaling on Handheld PCs” on page 50. To hide or show the virtual screen control, click the icon on your taskbar (the *toggle* control) once.

To zoom in to the session, use the icon on your taskbar (the *zoom-in* control). By default you zoom into the default bottom left hand corner. To zoom in gradually, click repeatedly.

To zoom out from the session, use the icon on your taskbar (the *zoom-out* control). To zoom out gradually, click repeatedly.

Setting Initial Panning and Scaling Positions

You can save initial panning and scaling positions on Pocket PCs so that sessions start up in the same position and to the same scale every time.

To change the initial positions for a specific connection

1. On the **Main** menu page, click the name of the connection that you want to change, then click **Edit**.
2. On the **Edit Settings** page, click **Edit Window Settings**.
3. On the **Edit Window Settings** page:

   - To set the initial display scale factor, select the required scale from the **Initial Display Scale Factor** list. The higher the number, the greater the area of desktop or application appears on the device's screen.

     For example, when **Initial Display Scale Factor** is set to "2," each pixel on the client represents four (2 × 2) pixels in the session. When it is set to "1," the pixel size is the same as for the client screen.

   - To set the initial panning position, select the required position from the **Initial Panning Position** list.

   - To set custom x and y coordinates, type the required numbers in the **Custom X Position** and **Custom Y Position** fields. If the setting is larger than the session size, it is adjusted automatically to the furthest available position. For example, a setting of (999, 50) positions the screen all the way to the right of the session and 50 pixels down.
4. Click **Save**.

To change the default initial positions for new connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. On the **Edit Global Settings** page, click **Edit Preferences**.
3. To set the default display scale factor, select the required scale from the **Default Display Scale Factor** list.
4. To set the default panning position, select the required position from the **Default Panning Position** list.
5. To set custom x and y coordinates, type the required numbers in the **Custom X Position** and **Custom Y Position** fields. If the setting is larger than the session size, it is adjusted automatically to the furthest available position. For example, a setting of (999, 50) positions the screen all the way to the right of the session and 50 pixels down.
6. Click **Save**.

Using Program Neighborhood Agent

Overview

Program Neighborhood Agent allows users to connect without using a Web browser to a server running the Web Interface and access all published applications and content that they are authorized to use across multiple server farms. Users do not have to manually configure a connection to each application. Program Neighborhood Agent also provides single sign-on: when users log on at the start of a session, they do not have to supply their logon credentials again during that session, even if they connect to several different applications. You can update server URLs and configure ICA session settings using Program Neighborhood Agent, and you can also choose which, if any, of these settings your users can access and modify.

To use Program Neighborhood Agent:

- You must ensure that the configuration file on the server has suitable settings for your users. Use the Web Interface to check the default settings and edit them if necessary. For details about how to do this, see "Configuring Settings on the Server" on page 54.
- Users who want to connect using Program Neighborhood Agent then need to enable it on their client device and customize the settings if they want. For details about how to do this, see "Configuring Settings on the Client Device" on page 56.
- After users have the settings they require, they connect to the relevant server URL, and are presented with a list of the available published resources. Depending on the device they have, users can choose to display the resource names in a **Programs** submenu, in a desktop folder, or directly on the desktop. For details about how to make a connection and access published resources, see "Accessing Applications and Files Using Program Neighborhood Agent" on page 59.

Note that the options discussed in “Integrating the Client with Security Solutions” on page 37 do not apply to connections created using Program Neighborhood Agent.

Note Program Neighborhood Agent supports client-to-server content redirection. Content redirection allows you to enforce all underlying file type associations from the computer running Citrix Presentation Server, eliminating the need to configure extended parameter passing on individual client devices. If all users are running 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.

Configuring Settings on the Server

Program Neighborhood Agent configuration settings are stored on the server in a file called config.xml. This file's location differs depending on the version of the Web Interface you are running, so refer to the Web Interface Administrator's Guide for the location. You edit this file using the Web Interface, which provides an easy-to-use graphical interface to the file’s parameters. For more information about editing config.xml using the Web Interface, see the *Web Interface Administrator’s Guide*.

You can modify default settings for all users. You can allow or deny your users the ability to:

- Save their domain passwords.
- Log on as an anonymous user or receive a prompt to enter logon details.
- Place links to published resources in either of three locations (a **Programs** submenu, a desktop folder, or directly on the desktop), depending on the device.
- Customize how often their list of applications is refreshed.
- Connect to a different server URL or with a different security setting. See “Connecting to Applications” on page 60 for more details.
- Determine their own screen color depth and audio quality. See “To modify screen color depth and sound quality” on page 58 for more details.
- Set their own reconnection options. See “To enable automatic reconnection” on page 59 for more details.

When a user enables Program Neighborhood Agent on the client device and connects to the server URL, the client reads the configuration data from the server. The settings you configure using the Web Interface affect all users of this configuration file. The options and their settings appear on the client device's **PN Agent Properties** page.

Users need to click **Save** on the **PN Agent Properties** page before the client recognizes any change to the configuration file.

Caution The settings in the configuration file are global; the settings and any changes you make to them affect all users connecting to the file.

The Web Interface enables you to specify:

- Which options users see on their **PN Agent Properties** page.

  Users can enter the server URL to which they want to connect, how they want to connect (anonymously or with personal logon details); save their domain password; specify where they want their list of published resources displayed; how often they want the list of resources refreshed; and the window size, color depth, sound quality, and reconnection options for a session.

- Where users can place links to published resources on the client device.
- Server connections.
- Whether or not users can save their passwords.
- Whether or not users can modify their screen window size, color depth, and sound quality.

  The preferences users set for color depth and sound quality affect the amount of bandwidth the ICA session consumes. To limit bandwidth consumption, you can force the server default for some or all of the options on this tab. This removes all settings for the corresponding option, other than **Default**, from the interface.

- Whether or not users can change their reconnection settings.

  These settings determine if reconnection automatically takes place at logon or by clicking the **Reconnect** button. With both of these options, users can choose to reconnect to active sessions only or to both active and disconnected sessions. Active sessions are all sessions currently running on any client device connected to the server. When you reconnect to active sessions from another client device or devices, the sessions disappear from the original client devices.

Disconnected sessions are sessions to which you were previously connected and that are still running on the server. Sessions run on the server until you log off.

Note If the server specified in the URL is configured to use SSL/TLS for communications between clients and server, client devices need an SSL root certificate for the server. For information about installing certificates, see the documentation for your client device.

Configuring Settings on the Client Device

This section describes how to modify Program Neighborhood Agent settings on the client device. These tasks can be performed by the user. The administrator can choose not to make configuration settings available to users by changing the config.xml file as described in "Configuring Settings on the Server" on page 54; in this case the options appear on the **PN Agent Properties** page but are not configurable.

To enable Program Neighborhood Agent

1. On the **Main** menu page, click **PN Agent Properties**.

   Note To allow users to override the settings made on the server from the client, the administrator must configure the appropriate settings on the server running the Web Interface. If you disable user customization for a setting, the setting disappears from the client device. See the *Web Interface Administrator's Guide* for more information.

2. Type the name or the URL of the server to connect to, then click **Save**.

   Note The first time you enable Program Neighborhood Agent the **PN Agent Properties** page displays only the **Server URL** option. After you enable Program Neighborhood Agent for the first time, it displays all available parameters.

3. Enter your logon credentials.
4. Before continuing, click **Save** to ensure you see the latest updates made to the settings on the server. Whenever you click **Save** on the **PN Agent Properties** page, the page is updated not only with the changes you made

on the client device, but also with any changes that were made to the server settings since you last saved the page.

To save your domain password

If you select this option, the next time you log on to Program Neighborhood Agent the password you enter is saved. You are not prompted for a password again until you either change your password or disable, then reenable, Program Neighborhood Agent.

If you do not select this option, you are prompted for your password each time you connect to a URL or restart your device.

1. Enable Program Neighborhood Agent, as described in “To enable Program Neighborhood Agent” on page 56.
2. Select the **Save Password** check box.
3. Click **Save**.

The option to save your password is also available when you log on to Program Neighborhood Agent (see “Accessing Applications and Files Using Program Neighborhood Agent” on page 59).

To change logon mode

Depending how the server is configured, you can select to log on to the computer running Citrix Presentation Server anonymously or be prompted for your logon details each time.

1. Enable Program Neighborhood Agent, as described in “To enable Program Neighborhood Agent” on page 56.
2. From the **Logon Mode** drop-down list, select **Prompt user** or **Anonymous**.
3. Click **Save**.

To specify where to place links to published resources

You can choose to place links to published resources in a **Programs** submenu or on the desktop.

1. Enable Program Neighborhood Agent, as described in “To enable Program Neighborhood Agent” on page 56.
2. To place links in a **Programs** submenu, select the **Show this folder in Programs submenu** check box. By default, links are placed in a folder called **My PNAgent Folder**, which is created automatically during installation. Alternatively, you can type the name of another folder.

To place links in a desktop folder, select the **Show applications in desktop folder** check box. By default, links are placed in a folder called **My PNAgent Folder**, which is created automatically during installation. Alternatively, you can type the name of another folder. To place links directly on the desktop, leave the folder name blank.

3. Click **Save**.

To specify how often to refresh your list of published resources

You can choose to refresh your list of published resources whenever Program Neighborhood Agent starts, at hourly intervals, or whenever a remote application launches.

1. Enable Program Neighborhood Agent, as described in "To enable Program Neighborhood Agent" on page 56.
2. Select the appropriate check box. To refresh the list at hourly intervals, you must specify the interval; for example, 2 = every two hours.
3. Click **Save**.

To modify screen color depth and sound quality

1. Enable Program Neighborhood Agent as described in "To enable Program Neighborhood Agent" on page 56.
2. Make the desired configuration changes. Depending on how Program Neighborhood is configured on the server, you may be able to set preferences for the screen color depth and sound quality of ICA sessions.
3. Click **Save**.

To edit the server URL

Program Neighborhood Agent requires the URL to a configuration file on the server running the Web Interface. This file contains the information Program Neighborhood Agent needs for users to access remote applications and content on a local device.

1. Enable Program Neighborhood Agent as described in "To enable Program Neighborhood Agent" on page 56.
2. The **Server URL** box displays the currently selected URL. Delete this and type the new URL. Alternatively, you can just type the server name and if the client makes a successful connection it will complete the URL automatically.
3. Click **Save**.

To enable automatic reconnection

1. Enable Program Neighborhood Agent as described in “To enable Program Neighborhood Agent” on page 56.
2. Select reconnection options. You can:
   - **Enable automatic reconnection at logon**. Allows you to reconnect automatically when you log on to the server. You can select to reconnect only to disconnected sessions, or to both disconnected sessions on the server and active sessions on client devices.

     Active sessions are all sessions currently running on any client device connected to the server. *Disconnected* sessions are sessions to which you were previously connected and that are still running on the server. Sessions run on the server until you log off.
   - **Enable automatic reconnection from Reconnect button**. Allows you to use the **Reconnect** button to reconnect to the server. You can select to reconnect only to disconnected sessions, or to both disconnected sessions on the server and active sessions on client devices.
3. Click **OK** to confirm your settings.

Note Workspace control connects or reconnects all previous active or disconnected sessions regardless of whether they were connected through Program Neighborhood Agent, Program Neighborhood, or the Web Interface.

For more information about workspace control requirements and server configuration, see the *Citrix Presentation Server Administrator’s Guide* or the *Web Interface Administrator’s Guide*.

Accessing Applications and Files Using Program Neighborhood Agent

You can connect to, disconnect from, reconnect to, and log off from applications published on the computer running Citrix Presentation Server using Program Neighborhood Agent.

Connecting to Applications

To connect to applications

1. Enable Program Neighborhood Agent as described in "To enable Program Neighborhood Agent" on page 56.
2. In the **Server URL** box, type the URL you want to connect to, then click **Save**.

   Note You can use Program Neighborhood Agent in Citrix Presentation Server deployments with more than one farm. When you configure the Web Interface to present users with a combined list of published applications from multiple farms, Program Neighborhood Agent automatically supports that configuration as well. It's important to note that you cannot connect successfully to two applications with the same name when connecting to applications published from multiple server farms from the Client for Windows CE. For information about configuring the Web Interface, see the *Web Interface Administrator's Guide*.

3. Enter your domain logon credentials. Depending on how Program Neighborhood Agent is configured on the server, you may be given the option to save your password. If you select this option, you are not prompted for your password again until the next time you change it, or the next time you disable, then reenable, Program Neighborhood Agent. If you do not select this option, you are prompted for your password each time you connect or restart your device.

   The list of available resources appears in the specified place (a Programs submenu, a desktop folder, or directly on the desktop).

Disconnecting from Applications

Disconnecting from applications closes the connection between the client device and the server. The sessions remain active in the server and you can easily reconnect to them from the same or a different client device.

To disconnect from applications you accessed through Program Neighborhood Agent

1. On the **Main** menu page, click **PN Agent Properties**.
2. Click **Disconnect** and all connections between the client device and server are closed.

The sessions remain active on the server and you can reconnect from any client device. To close a session on the server, you must log off.

Note Use Citrix Presentation Server to determine a default time-out period for sessions active on the server. See the *Citrix Presentation Server Administrator's Guide* for more detail.

Reconnecting to Applications

To reconnect to applications you previously accessed through Program Neighborhood Agent and subsequently disconnected from

1. On the **Main** menu page, click **PN Agent Properties**.
2. Click **Reconnect** and all active and/or disconnected connections are reopened on your client device. See "To enable automatic reconnection" on page 59 to find out more about reconnection options.

Note When you reconnect to a disconnected session with a different screen resolution, the client dynamically reconfigures the session size for optimal performance.

However, when you move between client devices, and you try to reconnect to a disconnected session of a size and color depth greater than that specified on your current client device, the reconnection fails and a new session is created instead.

Logging off from Applications

Logging off from applications closes all sessions on the server and all connections between the client and the server.

To log off from all applications accessed through Program Neighborhood Agent

1. On the **Main** menu page, click **PN Agent Properties**.
2. Click **Log Off** and all connections are closed on both the client device and on the server.

Index