

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

MetaFrame Presentation Server Client for Windows CE
for Handheld and Pocket PCs, Version 8.x

Citrix® MetaFrame® Presentation Server 3.0
Citrix MetaFrame Access Suite

Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement. Note that copies of the End User License Agreement are included in the root directory of the MetaFrame Presentation Server CD and in the root directory of the MetaFrame Presentation Server Components CD.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

© 1994-2004 Citrix Systems, Inc. All rights reserved.

Citrix, NFuse, ICA (Independent Computing Architecture), Program Neighborhood, MetaFrame, and MetaFrame XP are registered trademarks, and Citrix Solutions Network and SpeedScreen are trademarks of Citrix Systems, Inc. in the United States and other countries.

RSA Encryption © 1996-1997 RSA Security Inc. All Rights Reserved.

Microsoft, MS, Windows, Windows NT, ActiveX, Active Directory, Windows 2000, Internet Explorer, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Apple, Mac, Macintosh, Mac OS X, and MRJ are trademarks of Apple Computer, Inc. registered in the United States and other countries.

Netscape, Netscape Navigator, and Netscape Communicator are trademarks of Netscape Communications Corporation in the United States and other countries.

Novell Directory Services, NDS, and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. Novell Client is a trademark of Novell, Inc.

Java, JavaSoft, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

All other trade names referred to are the Servicemark, Trademark, or Registered Trademark of the respective manufacturers.

Last Updated: July 21, 2004 (SOC)

Contents

Chapter 1	Before You Begin	
	Who Should Use this Guide?	7
	How to Use this Guide	7
	Client Overview	8
	Accessing Documentation	8
	Client for Windows CE Documentation	9
Chapter 2	Introduction to the Client for Windows CE	
	Overview	11
	Feature Summary	11
	Session Reliability	13
	Improved Compression Technology	13
	Improved Graphic Display Speed	13
	Digital Dictation Support	13
	Dynamic Session Reconfiguration	14
	Automatic Network Connection	14
	Zone Preference and Failover	14
	Workspace Control	14
	Multiple Server Farm Support	15
	Default and Configurable Panning and Scaling	15
	Input Method Editor (IME) Support	16
	HTML User Interface	16
	Remote Access	17
	Program Neighborhood Agent	17
	Disk Caching	17
	SpeedScreen Browser Acceleration	18
	Windows NT Challenge/Response (NTLM) Support	18
	Roaming User Reconnect	18
	Secure Proxy Support	18
	TLS Encryption	18
	Basic File Type Association	18

Client Device Mapping	19
Client Drive Mapping	19
Client Printer Mapping	19
Client COM Port Mapping	19
Audio Mapping	19
Web Browser Launching and Embedding	19
Time Zone Support	20
Client Auto Update	20
Low Bandwidth Requirements	20
Data Compression	21
SpeedScreen Latency Reduction	21
Local Text Echo	21
Mouse Click Feedback	21
Auto Client Reconnect	21

Chapter 3

Installing and Configuring the Client for Windows CE

Overview	23
System Requirements	24
Installing the Client for Windows CE	24
Starting the Client for Windows CE	26
Enabling and Using Remote Access	26
Updating Client Software	28
Preparing for Client Auto Update	28
Using Client Auto Update	29
The Client Update Process	30
Configuring the Client Update Database	31
Uninstalling the Client for Windows CE	37
Creating a New Connection	38
Connecting to a Server	40
Editing a Connection	40
Configuring Network Protocol and Server Location	41
Specifying an Application to Run after Connecting to a Server	45
Associating a File Type with an Application	46
Specifying Logon Information	46
Editing the Window Properties	47
Setting Performance Improvement, Sound, Encryption, and IME Options	49

Integrating the Client with Security Solutions	52
Configuring the Client to Use a SOCKS Proxy Server	52
Configuring the Client to Use a Secure Proxy Server	53
Connecting to a Server across a Firewall	54
Using Encryption	54
Printing	56
Configuring MetaFrame Presentation Server for Client Printing	56
Printing from the Client	58
Editing Global and Default Settings	59
Configuring Hotkeys	60
Configuring Global Preferences	62
Configuring Default Server Location Options	64
Configuring a Default Proxy Server	65
Using Alternate Address Translation	66
Improving Performance	66
Data Compression	66
SpeedScreen Latency Reduction	67
Disk Caching	67
Panning and Scaling	68
Panning and Scaling on Handheld PCs	68
Panning and Scaling on Pocket PCs	69

Chapter 4

Using the Program Neighborhood Agent

Overview	71
Configuring Settings on the Server	72
Configuring Settings on the Client Device	74
Accessing Applications and Files Using the Program Neighborhood Agent	79
Connecting to Applications	79
Disconnecting from Applications	80
Reconnecting to Applications	81
Logging Off from Applications	81

Index	83
-----------------	----

Before You Begin

Who Should Use this Guide?

This guide is for system administrators responsible for configuring, deploying, 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.

Important Most of the screen images shown in this guide are taken from a landscape-format handheld Windows CE device. Minor differences may be present on other handheld devices. Any other differences in functionality are noted in the text.

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 <i>Client for Windows CE for Handheld and Pocket PCs Administrator's Guide</i> (this guide).
Chapter 2, "Introduction to the Client for Windows CE"	Gives 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 the Program Neighborhood Agent"	Describes how to configure and use the Program Neighborhood Agent.

Client Overview

The Client for Windows CE allows users to connect to computers running MetaFrame 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.

Accessing Documentation

This guide is part of the MetaFrame Presentation Server documentation set. The documentation set includes guides that correspond to different features of MetaFrame Presentation Server. Documentation is provided as Adobe Portable Document Format (PDF) files, and the latest version of this guide is available from the **Downloads** section of Citrix Web site, <http://www.citrix.com/>.

Important information about known issues, and last-minute documentation updates and corrections are provided in the Readme. Be sure to read the Client for Windows CE for Handheld and Pocket PCs Readme.htm file, also available from the **Downloads** section of Citrix Web site, before you work with the client or during troubleshooting.

Important To view, search, and print the PDF documentation, you need to have the Adobe Acrobat Reader 5.0.5 or later with Search. You can download Adobe Acrobat Reader for free from Adobe Systems' Web site at <http://www.adobe.com/>.

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 MetaFrame Presentation Server or to published applications.
- *Client for Windows CE for Handheld and Pocket PCs OEM 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 MetaFrame Presentation Server*.

Introduction to the Client for Windows CE

Overview

This chapter begins by providing a list of the new and existing features of the Client for Windows CE. Each feature on the list is then described in more detail.

Feature Summary

The following features are new in this release:

- Session reliability
- Improved compression technology
- Improved graphic display speed
- Digital dictation support
- Dynamic session configuration
- Automatic network connection
- Zone preference and failover when using Program Neighborhood Agent
- Workspace control when using Program Neighborhood Agent
- Multiple server farm support when using Program Neighborhood Agent
- Default and configurable panning and scaling settings
- Support for the Input Method Editor (IME) program interface

Other major features are:

- HTML user interface
- Remote access
- Program Neighborhood Agent
- Reduced memory use when running multiple concurrent sessions
- Disk caching
- SpeedScreen browser acceleration
- Windows NT Challenge/Response (NTLM) proxy support
- Roaming user reconnect
- Secure proxy support
- Transport Layer Security (TLS) encryption
- Basic file type association
- Client device mapping
 - Client drive mapping
 - Client printer mapping
 - Client COM port mapping
 - Client audio mapping
- Web browser launching and embedding
- Time zone support
- Client auto update
- Low bandwidth requirements
- Data compression
- SpeedScreen latency reduction
- Auto-reconnect

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

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 “Setting Performance Improvement, Sound, Encryption, and IME Options” on page 49.

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

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 “Setting Performance Improvement, Sound, Encryption, and IME Options” on page 49.

Improved Graphic Display Speed

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

Digital Dictation Support

MetaFrame 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 back at the office.

To enable and configure digital dictation support for your client, see “Setting Performance Improvement, Sound, Encryption, and IME Options” on page 49.

Digital dictation support is available with MetaFrame Presentation Server Advanced and Enterprise Editions. For information about configuring this feature, see the *MetaFrame Presentation Server Administrator's Guide*.

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.

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.

Zone Preference and Failover

A new policy rule enables you to direct user connections to preferred zones and set transparent failover to backup zones when preferred servers are unavailable. When users open applications, the Zone Preference and Failover policy rule directs their connections to the server with the highest zone preference and smallest load. This feature is available for Program Neighborhood Agent connections only.

You set up and configure zone preference and failover on the computer running MetaFrame Presentation Server. For more information about the server-side setup, see the *MetaFrame Presentation Server 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 MetaFrame 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 the Program Neighborhood Agent” on page 79.

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 via Program Neighborhood Agent, Program Neighborhood or 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.

Multiple Server Farm Support

You can now use Program Neighborhood Agent in MetaFrame 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*.

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 syou 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 68.

Input Method Editor (IME) Support

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 Performance Improvement, Sound, Encryption, and IME Options” on page 49.

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.

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 machine, 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 26.

Program Neighborhood Agent

Using the 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 does not need to have a browser installed.

The 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 the Program Neighborhood Agent, see “Using the Program Neighborhood Agent” on page 71.

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 “Setting Performance Improvement, Sound, Encryption, and IME Options” 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.

Windows NT Challenge/Response (NTLM) Support

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

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.

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.

TLS Encryption

As an alternative to SSL 3.0, the Client for Windows CE also supports 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.

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 MetaFrame 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 MetaFrame Presentation Server. This feature is not available when connecting to servers running MetaFrame Server for UNIX Version 1.0 or 1.1.

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. There are two ways to run an application from a Web page — launching and embedding:

- Launching an application from a Web page involves clicking a hyperlink that references an ICA file. Clicking the hyperlink causes the application to start and appear full-screen. You can then use this application as if it were installed and running on your local computer.

- Embedding an application places the window in which the program runs within the Web browser window.

If you are cannot run a Web browser on your Windows CE device, you can use the Program Neighborhood Agent to access applications deployed through the Web Interface.

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.

Client Auto Update

The client auto update feature allows administrators to update client installations from a central location instead of having to manually install new client versions on each client device. New versions of clients are stored in a central client update database on the computer running MetaFrame Presentation Server. The latest versions of the client software are downloaded to client devices when users connect to the server. For more information about automatic updating, see "Updating Client Software" on page 28.

Important This feature requires write access to the Windows CE device. Check with your Windows CE device manufacturer for information about whether you can use this feature with your device.

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 servers running MetaFrame Server for UNIX 1.0 or 1.1. 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 Properties" on page 47.

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.

Installing and Configuring the Client for Windows CE

Overview

Topics in this section include:

- System requirements
- Installing the Client for Windows CE
- Starting the Client for Windows CE
- Enabling and using remote access
- Updating client software
- Uninstalling the Client for Windows CE
- Creating a new connection
- Connecting to a server
- Editing a connection
- Integrating the client with security solutions
- Printing
- Editing the global and default settings
- 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.
- 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

There are two ways in which you can install the Client for Windows CE:

- If you are installing the client on devices that do not already have the Client for Windows CE installed on them, you must install the client manually. This is the method described in this section.
- If you have a previous version of the Client for Windows CE, you can update it automatically to the latest version by adding the latest version of the client to the client update database. See “Updating Client Software” on page 28.

The Client for Windows CE can be installed manually 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 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.

Note MetaFrame 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 *MetaFrame Presentation Server Administrator's Guide* for more details.

Starting the Client for Windows CE

To start the Client for Windows CE

1. Click **Start>Programs>ICA Client**. The Main menu page appears:



*This is a screenshot of the **Main** dialog box.*

The screen lists the connections that you have 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.
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` into your browser and the **Main** page of the client opens. Make sure you have enabled remote access to your client device. See “Enabling and Using Remote Access” on page 26 for more details about how to do this.

To find out your device name, click **Start > Settings > Control Panel**. Select **Communications**, and the **Communications Properties** dialog box opens. The name of your client device appears in the **Device name** box.

Updating Client Software

You can set up the client software so that you can automatically update it from a computer running MetaFrame Presentation Server when a newer version is available. This means that you “push” a new version of the client software from a central database to the client device instead of installing the client software manually on each device.

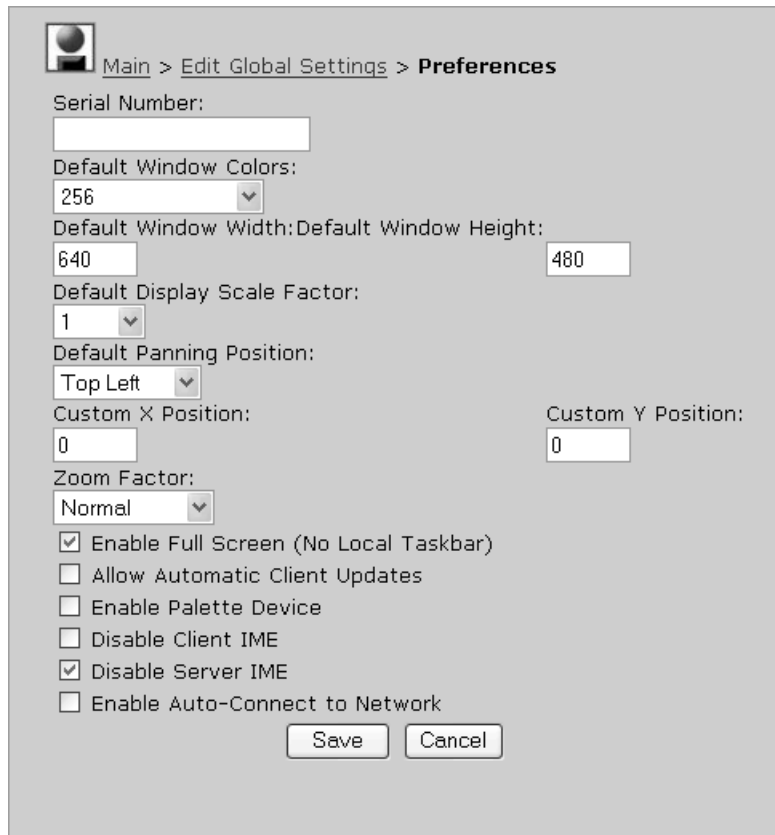
Preparing for Client Auto Update

You need to configure the client software on individual devices to allow automatic client software updates.

To enable the Client software for automatic update

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

2. On the **Edit Global Settings** page, click **Edit Preferences**:



The screenshot shows the Preferences dialog box with the following settings:

- Serial Number: [Empty text box]
- Default Window Colors: 256 (dropdown menu)
- Default Window Width: 640 (text box)
- Default Window Height: 480 (text box)
- Default Display Scale Factor: 1 (dropdown menu)
- Default Panning Position: Top Left (dropdown menu)
- Custom X Position: 0 (text box)
- Custom Y Position: 0 (text box)
- Zoom Factor: Normal (dropdown menu)
- Enable Full Screen (No Local Taskbar):
- Allow Automatic Client Updates:
- Enable Palette Device:
- Disable Client IME:
- Disable Server IME:
- Enable Auto-Connect to Network:

Buttons: Save, Cancel

*This is a screenshot of the **Preferences** dialog box.*

3. On the **Preferences** page, check **Allow Automatic Client Updates**.
4. Click **Save**.

Using Client Auto Update

Use the client auto update feature to store new versions of MetaFrame Presentation Server Clients. The client software is stored in a client update database and downloaded to client devices when users connect to a computer running MetaFrame Presentation Server. Although you would normally use client auto update to update client files to newer versions of the same product and model, you can replace the client files with an older version using the Version Checking feature. For further information about version checking, refer to “Configuring the Properties of the Client Update Database” on page 33, “Adding and Removing Clients from the Database” on page 35, and “Changing the Properties of a Client in the Database” on page 36.

Note The client auto update feature is not available on computers running MetaFrame Presentation Server for UNIX 1.0 or 1.1.

Client auto update:

- Automatically detects older client files
- Provides full administrative control of client update options for each client
- Updates clients from a single database on a network share point

The Client Update Process

The Client for Windows CE runs on several processor types. Each client has a product number, model number, and version number. The client product and model numbers uniquely identify the client. There is a client for each supported processor available:

Product/Model number	Processor Types
1F09/6	CE Client for x86
1F09/7	CE Client for SH-3
1F09/8	CE Client for SH-4
1F09/9	CE Client for MIPS
1F09/B	CE Client for ARM
1F09/C	CE Client for ARMV4I

The version number is the release number of the client. The process of updating clients with new versions is:

1. The server queries the client when the user logs on. If the server detects that the client is up-to-date, it continues the logon transparently.
2. If an update is needed, by default the server informs the user that a newer version of the client is available and asks to perform the update. You can specify that the update occurs without informing the user or without allowing the user to cancel the update.
3. By default, the user can choose to wait for the client files to finish downloading or to download the files in the background and continue working. You can force the client update to complete before allowing the user to continue.

4. During the client update, new client files are copied to the client device. The administrator can force the user to disconnect and complete the update before continuing the session. The user must log on to the server again to continue working.
5. After disconnecting from the server, the client completes the update. All client programs must be closed before the client can be updated.
6. If the user does not close all client programs before clicking **OK**, a message appears informing the user of the open program. When all programs are closed, the client can complete the update.
7. In case of a problem, the existing client files are saved to a folder called Backup in the **Client** directory on the client.

Configuring the Client Update Database

During setup of MetaFrame Presentation Server, a client update database is created on the server that contains a range of MetaFrame Presentation Server Clients.

You can configure a client update database on each server in a server farm, or a single client update database on a central network share. With a single database, you can configure updates once for all servers.

Use the Client Update Configuration utility to:

- Create a new client update database
- Set a default client update database
- Configure database properties
- Add and remove clients from the update database
- Configure client update options
- Change the properties of a client in the database

To start the Client Update Configuration utility

1. On a computer running MetaFrame Presentation Server, choose **Start > Programs > Citrix Administration Tools**.
2. Click **ICA Client Update Configuration**. The ICA Client Update Configuration window appears. The location of the current client update database is shown in the status bar. This is the database the server uses to update clients. The main window shows the clients currently configured in the database.

Creating a New Client Update Database

The default location of the client update database is %SystemRoot%\Ica\Clientdb. You can create a new database can be created on the local server hard drive or on a shared network drive.

To create a new client update database

1. Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31.
2. On the **Database** menu, click **New**. The **Path for the New Client Update Database** dialog box appears.
3. Enter a path for the new client update database and click **Save**. A new database is created in the specified folder and the new database is opened.

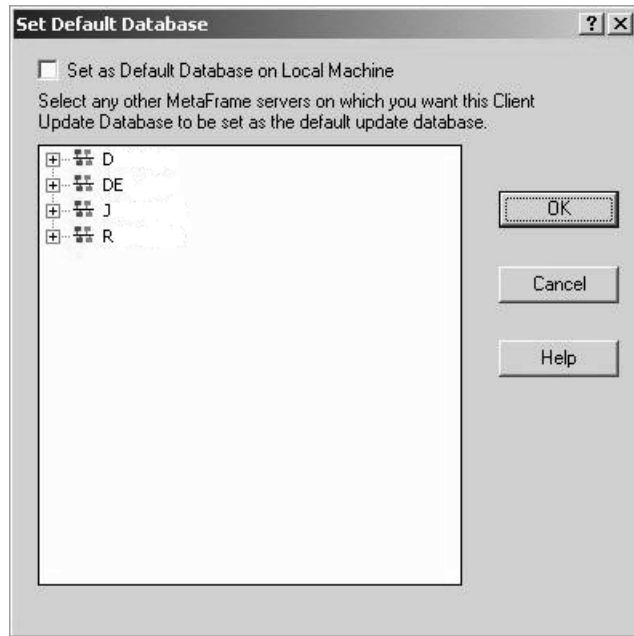
Setting a Default Database

An existing client update database can be used by multiple servers. If the client update database is on a shared network drive, use the Client Update Configuration utility to configure all computers running MetaFrame Presentation Server to use the shared database.

To specify a new default database for one or more servers

1. Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31.
2. On the **Database** menu, click **Open**. The **Open Existing Database** dialog box appears.
3. Specify the path to the database that will be used as the default and click **Open**.

4. On the **Database** menu, click **Set Default**. The **Set Default Database** dialog box appears.



*This is a screenshot of the **Set Default Database** dialog box.*

To make the currently open database the default database, select the **Set as Default Database on Local Machine** check box.

Tip You can set other computers running MetaFrame Presentation Server to use the currently open database as the default database. To view the servers in a domain, double-click the domain name. To set a server's default database to the currently open database, click that server. To select multiple servers, hold down the CTRL key.

Configuring the Properties of the Client Update Database

Use the **Database Properties** dialog box to configure the client update database.

To configure the properties of the client update database

Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31, then on the **Database** menu, click **Properties**. The **Database Properties** dialog box appears.

- To disable this client update database, clear the **Enabled** check box. Clients are not updated if the database is not enabled.

- The **Default update properties for clients** options specify the default behavior for clients added to the update database. If you change the properties of an individual client in the database, those properties will override the default properties.
 - In the **Client Download Mode** field:
 - To allow the user to choose to accept or postpone the client update, click **Ask user**.
 - To notify the user of the client update and require the update, click **Notify user**.
 - To update the user's client without notifying the user, click **Transparent**.
 - In the **Version Checking** field:
 - To update client versions that are older than the new client, click **Update older client versions only**.
 - To update all client versions to this version of the client, click **Update any client version with this client**. Use this option to force an older client to replace a newer client.
 - In the **Update Mode** field:
 - To require users to disconnect and complete the update, select the **Force Disconnection** check box. This check box is clear by default, allowing users to be given control over whether or not they disconnect and complete the client update after the new client files are downloaded.
 - To force users to wait for all client files to download before continuing, clear the **Allow background download** check box. By default, users can choose to download new client files in the background and continue working.
- To write an event in the event log when a client is updated, select the **Log Downloaded Clients** check box.
- By default, errors that occur during a client update are written to the event log. To turn off error logging, clear the **Log Errors During Download** check box.
- Specify the maximum number of simultaneous updates per computer running MetaFrame Presentation Server. While the specified number of client updates is occurring, new client connections are not updated. When the number of client updates drops below the specified maximum, new client connections are updated.

Adding and Removing Clients from the Database

Use the Client Update Configuration utility to add clients to and remove them from the database.

To add a new client to the client update database

1. Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31.

2. On the **Client** menu, click **New**. The **Description** dialog box appears.

Enter the path to the client installation file in **Client Installation File** or click **Browse**.

Download the client installation file, Update.ini, from the Citrix Web site. A client installation file is available for a variety of processor types. Unzip the client update package to access the .ini file.

When you specify the client installation file, the **Client Name**, **Product**, **Model**, **Version**, and icon of the selected client appear.

You can also modify any comment made in the **Comment** field for this client. After making any changes, click **Next** to continue.

3. The **Update Options** dialog box appears.

The **Update Options** dialog box controls how the client update occurs. These options for each client override the settings specified for the database as a whole in the **Database Properties** dialog box. For a description of the options, see “Configuring the Properties of the Client Update Database” on page 33.

Click **Next** to continue.

4. The **Event Logging** dialog box appears.

Auto client update uses the Windows event log to report status messages and update errors.

- To write an event in the event log when a client is updated, select the **Log Downloaded Clients** check box.
- By default, errors that occur during a client update are written to the event log. To turn off error logging, clear the **Log Errors During Download** check box.

Click **Next** to continue.

5. The **Enable Client** dialog box appears.
The client update database can contain multiple clients with the same product, model, and version information. However, only one client of each product, model, and version can be enabled. The enabled client is the one used for the auto client update.
To update clients to this client, select the **Enable** check box. All other clients of the same product, model, and version are disabled.
6. To copy the client installation files into the client update database, click **Finish**.

To remove a client from the database

1. Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31.
2. In the **ICA Client Update Configuration** dialog box, click the client you want to remove.
3. On the **Client** menu, click **Delete**. A dialog box displays the selected client information and asks for confirmation.
4. To remove the client, click **OK**. The client is removed from the database.

Changing the Properties of a Client in the Database

Use the **Properties** dialog box to configure a client in the client update database. The **Properties** dialog box contains four tabs: the **Description** tab, the **Update Options** tab, the **Event Log** tab, and the **Client Files** tab.

To modify the properties of a client in the database

1. Start the Client Update Configuration utility as described in “To start the Client Update Configuration utility” on page 31.
2. In the **ICA Client Update Configuration** dialog box, click the client you want to modify.
3. On the **Client** menu, click **Properties**. The **Properties** dialog box appears.

- The **Description** tab displays information about the selected client. The **Product**, **Model**, **Variant**, **Version**, and **Client Name** are display-only boxes.
To enter a new description of the client, type the description in **Comment**. This description is used within the utility itself as one of the client's properties.
To update clients to this client, select the **Enabled** check box. All other clients of the same product, model, and version are disabled.
The client update database can contain multiple clients with the same product, model, and version information. However, only one client of each product, model, and version can be enabled. The enabled client is the one used for the auto client update.
- The **Update Options** tab configures how the client is updated. For a description of the update options, see “Configuring the Properties of the Client Update Database” on page 33.
- The **Event Logging** tab configures the events to log for the client update. For a description of the options, see “Configuring the Properties of the Client Update Database” on page 33.
- The **Client Files** tab displays the individual files for the client. The client update database stores the **File Name**, **Group**, **Flags**, **File Size**, and **File CRC** (Cyclic Redundancy Check) for each file of a client.

Uninstalling the Client for Windows CE

To uninstall the Client for Windows CE

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

If you are using a palm-sized device:

1. Choose **Start > Settings > System > Remove Programs**.

— or —

If you are using a landscape-format handheld device:

1. Choose **Start > Settings > Control Panel**. The Control Panel appears. Double-click **Remove Programs**.

Continue with the following steps:

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 MetaFrame 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 the Program Neighborhood Agent to retrieve pre-defined ICA connection configurations from servers running the Web Interface. This saves 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 the Program Neighborhood Agent, see "Using the Program Neighborhood Agent" on page 71.

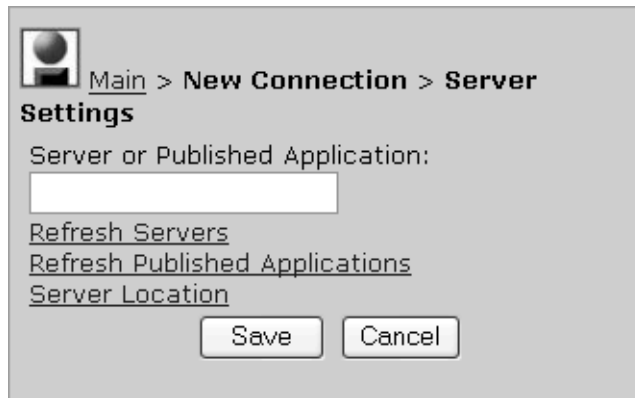
Note Citrix recommends that you quickly create a connection as outlined in the following procedure, and then configure the connection to best suit your needs. See "Editing a Connection" on page 40 for more details about configuring ICA connections.

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**. The **Server Settings** page appears:



*This is a screenshot of the **Server Settings** dialog box.*

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 on 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 43.

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 46.

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 is displayed 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 40.

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

To edit the connection you just created, see “Editing a Connection” on page 40.

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.

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 to edit 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 41.
 - 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 45.
 - 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 46.
 - The **Window Settings** option, where you can set the session size and the color depth for the ICA session window. See “Editing the Window Properties” on page 47. You also use this option to set initial panning and scaling positions for Pocket PCs. See “Setting Initial Panning and Scaling Positions” on page 69.

- 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. See “Setting Performance Improvement, Sound, Encryption, and IME Options” on page 49.
 - 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.
 - The **Edit Firewall Settings** option, where you can configure the client to use a SOCKS/secure proxy, alternate address remapping, and a Secure Gateway for MetaFrame address. See “Integrating the Client with Security Solutions” on page 52 for more information about using the client with a firewall. See “Using Encryption” on page 54 for more information about using SSL/TLS.
2. Make the desired changes.
 3. Click **Save** to save your changes.

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 via Program Neighborhood Agent, Program Neighborhood or Web Interface.

Note

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 43, or you can configure default settings to be used for all new connections, as described on page 64. 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 MetaFrame 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 55 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 55 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.

Note To configure server groups for a particular connection, see “Editing Server Location Options” on page 43. To configure server groups for all new connections, see “Configuring Default Server Location Options” on page 64.

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 MetaFrame 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.

Editing Server Location Options

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**. On the **Server Settings** page, click **Server Location**. The **Server Location** page appears:

Main > Edit Excel 2003 Settings > Server Settings > **Server Location**

Active Settings: TCP + HTTP, Primary:

Select Protocol: TCP / TCP + HTTP / SSL/TLS + HTTPS

Select Group: Primary: / Backup 1: / Backup 2:

Address List:

ica

Server Group Primary:

Server Group Backup 1:

Server Group Backup 2:

Save Cancel

*This is a screenshot of the **Server Location** dialog box.*

3. Select the appropriate protocol.
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 IP address of a computer running MetaFrame Presentation Server.
6. Add or remove servers as necessary. Click **Save** to save your changes.

Note To change the default server location for all new connections, see “Configuring Default Server Location Options” on page 64.

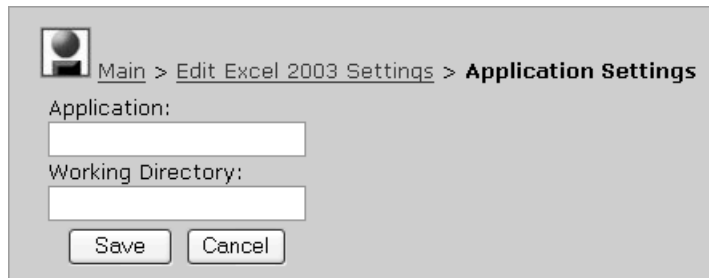
Specifying an Application to Run after Connecting to a Server

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 does not apply to connections to published applications. Any values entered are ignored.

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**. The **Application Settings** page appears:



*This is a screenshot of the **Application Settings** page.*

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** to save your changes.

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

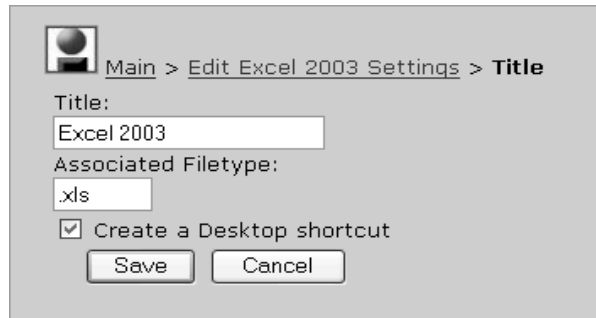
Associating a File Type with an Application

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 or 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**:



*This is a screenshot of the **Title** page.*

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. Click **Save** to save your changes.

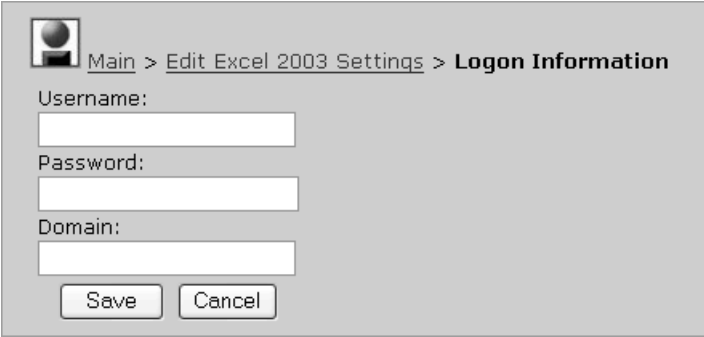
Note The option to **Create a Desktop shortcut** is available only on handheld and Pocket PCs.

Specifying Logon Information

You can include the settings needed to log on to the computer running MetaFrame 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**:



*This is a screenshot of the **Logon Information** page.*

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. Click **Save** to save your changes.

Editing the Window Properties

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**:



This is a screenshot of the **Window Settings** page.

Note If you have a Pocket PC, this screen contains additional panning and scaling parameters.

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. These options are 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.
5. For details how to set initial scale factors and panning positions, see “Setting Initial Panning and Scaling Positions” on page 69. 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.

6. Click **Save** to save your changes.

Setting Performance Improvement, Sound, Encryption, and IME Options

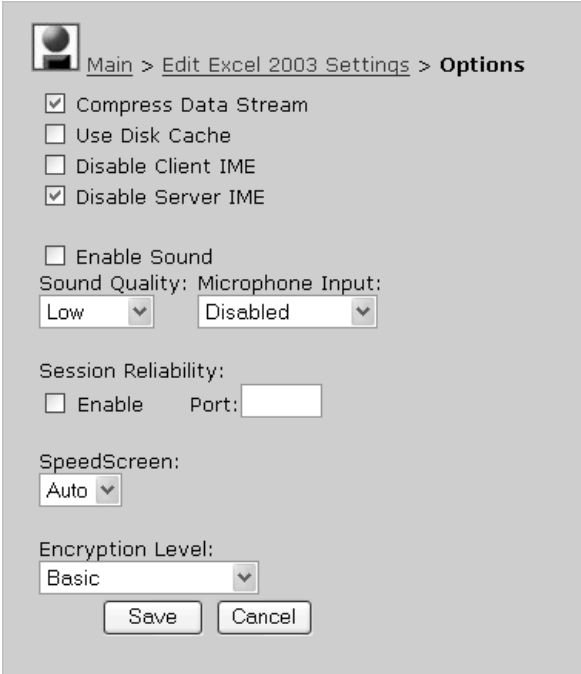
Use the **Edit Options** option to set the following options:

- Data compression
- Disk caching
- IME
- Sound support
- Microphone input
- Session reliability
- SpeedScreen latency reduction
- Encryption

To set connection options

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

On the **Edit Settings** page, click **Edit Options**:



The screenshot shows a dialog box titled "Main > Edit Excel 2003 Settings > Options". It contains several settings:

- Compress Data Stream
- Use Disk Cache
- Disable Client IME
- Disable Server IME
- Enable Sound
- Sound Quality: Microphone Input:
 - Low (dropdown)
 - Disabled (dropdown)
- Session Reliability:
 - Enable Port: [text box]
- SpeedScreen:
 - Auto (dropdown)
- Encryption Level:
 - Basic (dropdown)

At the bottom are "Save" and "Cancel" buttons.

*This is a screenshot of the **Options** page.*

2. To reduce the volume of data transferred between the client and the server, select the **Compress Data Stream** check box. If your connection is bandwidth-limited, enabling compression can increase performance. If your client device is on a high-speed LAN, you may not need compression. If you have sufficient bandwidth, leave compression off to conserve processing power on the server.
3. To use disk caching, select **Use Disk Cache**. For more information about this feature, see “Improving Performance” on page 66.
4. 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 MetaFrame 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, 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.
5. 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.

6. From the **Microphone Input** drop-down 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 back 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 Digital dictation support is available with MetaFrame Presentation Server Advanced and Enterprise Editions. For information about configuring this feature on the server, see the *MetaFrame Presentation Server Administrator's Guide*.

7. To enable users to continue to see a published application's window if the connection is interrupted, 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 once 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 *MetaFrame Presentation Server Administrator's Guide*.

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

8. To use SpeedScreen, select **Auto, On, or Off** from the **SpeedScreen** drop-down list. SpeedScreen enhances user experience on slow network connections. For more information about this feature, see “Improving Performance” on page 66.
9. To use ICA encryption, select the level of ICA encryption for the connection from the **Encryption Level** list. For more information about this feature, see “Using ICA Encryption” on page 55.

Important This encryption setting does not affect the encryption level used by SSL/TLS.

10. Click **Save** to save your changes.

Integrating the Client with Security Solutions

If your network is using a proxy server, for example to limit access to the computers running MetaFrame 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 Web Interface.

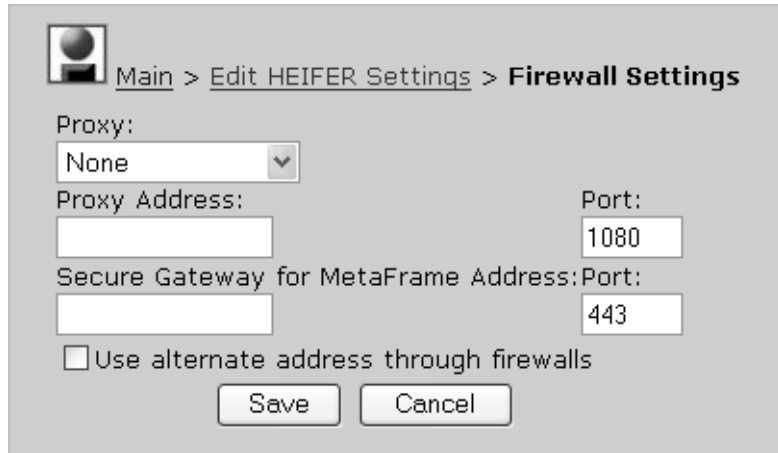
Configuring the Client to Use a SOCKS Proxy Server

If you want to connect to a computer running MetaFrame 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**.



*This is a screenshot of the **Firewall Settings** page.*

3. Select **SOCKS** from the **Proxy** drop-down 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** to save your changes.

Note To configure a default SOCKS proxy server for all connections, see “To configure a default SOCKS proxy server” on page 65.

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** drop-down menu.
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 for MetaFrame Address** box. If you are unsure of this information, contact your security administrator.
7. Click **Save**.

Note To configure a default secure proxy server for all connections, see “To configure a default secure proxy server” on page 65.

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 master ICA browser. 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 save your changes.

Note To configure alternate address translation for all connections, see “To use alternate address translation for all connections” on page 66.

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 MetaFrame Presentation Server documentation for more information about configuring SSL/TLS on the server.
- Change the Server Location protocol to SSL/TLS+HTTPS. See “Editing Server Location Options” on page 43 for a description of how to do this.
- If the SSL/TLS relay is not installed on a computer running MetaFrame 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 for MetaFrame 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 save your changes.

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 (www.microsoft.com).

Printing

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

Configuring MetaFrame 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 MetaFrame Presentation Server. This section describes how to enable printing on the server.

Mapping Client Printers on MetaFrame 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**.
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 MetaFrame Presentation Server.
2. Select **Start > Programs > Citrix Administration Tools > ICA Client Printer Configuration**.

3. On the **Printer** menu, click **New** to display the Add ICA Client Printer wizard. Follow the steps in the wizard to map the client printer.

Mapping Client Printers on MetaFrame 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 MetaFrame Presentation Server for UNIX, see the *MetaFrame 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
3. A message stating whether or not client printing is enabled appears.

To enable or disable client printing

Log on as an administrator. 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 is displayed. **(default)** is displayed 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 MetaFrame 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 MetaFrame Presentation Server for UNIX

To print a file from a client session

1. On the client device, open a command prompt, 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 <i>filename</i> to the default printer.	ctxlpr <i>filename</i>
Print a series of files to the default printer. Each file is treated as a separate print job.	ctxlpr <i>filename1 filename2</i>
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] <i>filename</i>
Print a file in the background.	ctxlpr -b <i>filename</i>
Print a file only if the printer is not in use. Use this option to stop an application waiting while other printer jobs are handled. If the printer is in use, an error message appears.	ctxlpr -n <i>filename</i>

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.

Editing Global and Default Settings

This section describes how to modify settings that apply for all ICA connections on the Windows CE device. It also describes how to change the default settings that are used when creating new ICA connections.

To edit the global settings

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

The **Global Settings** options are:

- The **Edit Hotkeys** option, where you can define custom key combinations for system hotkeys. See “Configuring Hotkeys” on page 60 for more information.
- The **Edit Preferences** option, where you can control a range of different settings used for new connections. See “Configuring Global Preferences” on page 62 for more information.
- The **Edit Server Location** option, where you can configure default network protocol and server location options for new connections. You can also set a time-out period for browsing for servers. See “Configuring Default Server Location Options” on page 64 for more information. You cannot configure options for Program Neighborhood connections using this option.

- The **Edit Firewall Settings** option, where you can configure default SOCKS/Secure proxy, alternate address remapping, and SSL/TLS relay settings for new connections. See “Integrating the Client with Security Solutions” on page 52 for more information about using the client with a firewall. See “Using ICA Encryption with SSL/TLS” on page 55 for more information about using SSL/TLS. You cannot configure options for Program Neighborhood connections using this option.
2. Click the required option and make the desired changes.
 3. Click **Save** to save your changes.

Configuring Hotkeys

The Client for Windows CE provides users with hotkeys that can be used during ICA sessions to control various functions. Some hotkeys control the behavior of the client itself while others emulate standard Windows hotkeys. When you want to use a Microsoft Windows key combination during a session, use the mapped hotkey instead. The following table lists the default client hotkeys.

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 hotkey 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 is displayed.

Name	Default Value	Description
ALT-ESC	CTRL+7	This hotkey cycles the focus through the minimized icons and open windows of applications running in your ICA session.
ALT-TAB	CTRL+8	This hotkey cycles through all applications in the ICA session. A popup box 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 hotkey, 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 hotkeys are mapped to suit Windows servers. These hotkeys can correspond to different actions in your respective UNIX Windows Manager.

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

To edit the default hotkeys

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Hotkeys**.
3. Use the lists of keys to change the default hotkey key sequences.
4. Click **Save** to save your changes.

Note You can disable one or more hotkeys by selecting **Disabled** in the appropriate drop-down lists.

Configuring Global Preferences

To edit global preferences

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

The screenshot shows the 'Preferences' tab of the 'Global Settings' dialog box. The breadcrumb path is 'Main > Edit Global Settings > Preferences'. The settings are as follows:

- Serial Number: [Empty text box]
- Default Window Colors: 256 (dropdown menu)
- Default Window Width: 640 (text box)
- Default Window Height: 480 (text box)
- Default Display Scale Factor: 1 (dropdown menu)
- Default Panning Position: Top Left (dropdown menu)
- Custom X Position: 0 (text box)
- Custom Y Position: 0 (text box)
- Zoom Factor: Normal (dropdown menu)
- Enable Full Screen (No Local Taskbar):
- Allow Automatic Client Updates:
- Enable Palette Device:
- Disable Client IME:
- Disable Server IME:
- Enable Auto-Connect to Network:

At the bottom, there are 'Save' and 'Cancel' buttons.

This is a screenshot of the **Preferences** tab of the **Global Settings** dialog box.

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

- **Serial Number.** This is the serial number of your Client for Windows CE software. This number is necessary only when you are using the client with a product such as *WINFRAME* Host/Terminal, which requires each client to have a Citrix PC Client Pack serial number. If a serial number is required, you must enter it exactly as it appears on the Serial Number card. The serial number is not used when connecting to computers running MetaFrame Presentation Server.
- **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.

- **Default Window Colors.** Select 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.
 - **Zoom factor.** You can disable the zoom factor completely, enable the intermediate zoom feature, or allow zooming but not intermediate zooming. For more information about this feature, see “Panning and Scaling on Handheld PCs” on page 68.
These options are available only on handheld PCs.
 - **Default initial scaling and panning settings.** For details about how to change these settings, see “Setting Initial Panning and Scaling Positions” on page 69.
These options are available only on Pocket PCs.
 - **Allow Automatic Client Updates.** Select this check box to allow the client software on this device to be updated automatically when a newer version is available. See “Preparing for Client Auto Update” on page 28 for more information.
 - **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.
 - **Disable Client IME.** Select this check box to disable client-side IME support. For more information about IME, see “Setting Performance Improvement, Sound, Encryption, and IME Options” on page 49.
 - **Disable Server IME.** Select this check box to disable server-side IME support.
 - **Enable Auto-Connect to Network.** Select this to 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.
 - **Enable Full Screen (Hide Local Task Bar).** Select this 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 SIP keyboard.
3. Make the desired changes.
 4. Click **Save** to save your changes.

Configuring Default Server Location Options

Use the Global Client Settings to configure default server location options and protocols for all ICA connections on the Windows CE device.

To edit the default server location options for new connections

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Server Location**:

Main > Edit Global Settings > Server Location

Active Settings: TCP + HTTP, Primary:

Select Protocol: TCP / TCP + HTTP / SSL/TLS + HTTPS
 Select Group: Primary: / Backup 1: / Backup 2:

Address List:

ica

Server Group Primary:

Server Group Backup 1:

Server Group Backup 2:

Time-out (milliseconds):
1000

Save Cancel

*This is a screenshot of the **Server Location** page.*

3. Select the appropriate protocol. For more information about available protocols, see “Network Protocol” on page 42.
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 MetaFrame 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 **Time-out**.
8. Click **Save** to save your changes.

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.

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** drop-down 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** to save your changes.

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** drop-down menu.
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 for MetaFrame 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 54. 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 “Editing Server Location Options” on page 43.

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

Using Alternate Address Translation

Use Global ICA Client Settings to configure alternate address mapping.

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** to save your changes.

Improving Performance

The features described in this section 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** drop-down list, select the setting (**Auto**, **On**, or **Off**) 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**.

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 67.

Panning and scaling work differently depending on whether you are using a handheld 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 the *virtual screen control*.

This control appears in the form of a small gray square at the far top right of the window. It is automatically enabled 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 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 *zoom 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 zoom factor

1. On the **Main** menu page, click **Edit Global Settings**.
2. Click **Edit Preferences**.
3. Choose one of the **Zoom 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 selected **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 69.

- 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 68. 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. See “Setting Initial Panning and Scaling Positions” on page 69 for more details about how to do this. 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.
 - 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 automatically adjusted 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. On the **Edit Preferences** page:
4. To set the default display scale factor, select the required scale from the **Default Display Scale Factor** drop-down list.
5. To set the default panning position, select the required position from the **Default Panning Position** drop-down list.
6. 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 automatically adjusted 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.
7. Click **Save**.

Using the Program Neighborhood Agent

Overview

The 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. The 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 the Program Neighborhood Agent, and you can also choose which, if any, of these settings your users can access and modify.

To use the Program Neighborhood Agent:

- You must ensure that the configuration file on the server has suitable settings for your users. Use the Program Neighborhood Agent Console 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 72.
- 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 74.
- Once 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 the Program Neighborhood Agent” on page 79.

Note that the options discussed in “Integrating the Client with Security Solutions” on page 52 do not apply to connections created using the Program Neighborhood Agent.

Note The Program Neighborhood Agent supports client to server content redirection. Content redirection allows you to enforce all underlying file type associations from the computer running MetaFrame Presentation Server, eliminating the need to configure extended parameter passing on individual client devices. If all users are running the Program Neighborhood Agent, and if you want to take advantage of the administrative ease of content redirection from client to server, see the *MetaFrame Presentation Server Administrator's Guide* for more information.

Configuring Settings on the Server

The Program Neighborhood Agent configuration settings are stored on the server in a file called Config.xml. You edit this file using the Program Neighborhood Agent Console, which provides an easy-to-use graphical interface to the file's parameters.

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 79 for more details.
- Determine their own screen color depth and audio quality. See “To modify screen color depth and sound quality” on page 78 for more details.
- Set their own reconnection options. See “To enable automatic reconnection” on page 78 for more details.

When a user enables the 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 Program Neighborhood Agent Console affect all users of this configuration file. The options and their settings are displayed 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.

To access the Program Neighborhood Agent Console, connect to `http://servername/Citrix/PNAgentAdmin/` on your server running the Web Interface.

The Program Neighborhood Agent Console 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.
- To hide or display options, use the **Client Tab Control** option in the Program Neighborhood Agent Console. To specify how often users' published resource lists are refreshed, use the **Application Refresh** options.
- Where users can place links to published resources on the client device.
To specify the locations in which users can place links (a **Programs** submenu, a desktop folder, or directly on the desktop), use the **Application Display** options.
- Server connections.
To specify the URL to which users can connect, use the **Server Settings** option in the Program Neighborhood Console.
- Whether or not users can save their passwords.
By default, users who are prompted for credentials can save their password. To disable this function, select the **Logon Methods** option and clear the **Allow user to save password** check box.
- Whether or not users can modify their screen window size, color depth and sound quality.
To define which settings are available to users, use the **Session Options** option in the Program Neighborhood Agent Console.
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 have been 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 72; in this case the options appear on the **PN Agent Properties** page but are not configurable.

To enable the Program Neighborhood Agent

1. On the **Main** menu page, click **PN Agent Properties**. The first time you enable Program Neighborhood Agent the following page opens. After you enable the Program Neighborhood Agent once however, the **PN Agent Properties** page displays all available parameters.



*This is a screenshot of the initial **PN Agent Properties** page.*

Note To allow users to override the settings made in their server from the client, the Server Settings page of the Program Neighborhood Agent Console must be configured. You configure the setting and select or deselect user customization. If you disable user customization for a setting, the setting appears as flat text on the client. Users can see the setting but cannot modify it in any way. See the *MetaFrame Presentation Server Administrator's Guide* for more information.

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

- The Program Neighborhood settings appear as follows, depending on which ones the administrator has made available to users:

Main > PN Agent Properties

Disable PN Agent

Server URL:
http://heifer/Citrix/PNAgent

Logon Mode:
Prompt user

Show this folder in Programs submenu:
My PN Agent Folder

Show applications in desktop folder:
My PN Agent Folder

Refresh application list when Program Neighborhood Agent starts

Refresh application list when remote application launches

Refresh application list on hourly interval: 6

Window Size:
Default

Color Depth:
Default

Sound Quality:
Default

Enable automatic reconnection at logon
Active and disconnected sessions

Enable automatic reconnection from Reconnect button
Active and disconnected sessions

Refresh Log Off Disconnect Reconnect

Save Cancel

*This is a screenshot of the **PN Agent Properties** page.*

- Before continuing, click **Save** to ensure you see the latest updates made to the settings on the server. Note that whenever you click **Save** on the **PN Agent Properties** page, the page is updated not only with the changes you have 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 the 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, the 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 the Program Neighborhood Agent, as described in “To enable the Program Neighborhood Agent” on page 74.
2. Select the **Save Password** check box.
3. Click **Save**.

The option to save your password is also available when you log on to the Program Neighborhood Agent (see “Accessing Applications and Files Using the Program Neighborhood Agent” on page 79).

To change logon mode

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

1. Enable the Program Neighborhood Agent, as described in “To enable the Program Neighborhood Agent” on page 74.
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 the Program Neighborhood Agent, as described in “To enable the Program Neighborhood Agent” on page 74.
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 the Program Neighborhood Agent starts, at hourly intervals, or whenever a remote application launches.

1. Enable the Program Neighborhood Agent, as described in “To enable the Program Neighborhood Agent” on page 74.
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 the Program Neighborhood Agent as described in “To enable the Program Neighborhood Agent” on page 74.
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

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

1. Enable the Program Neighborhood Agent as described in “To enable the Program Neighborhood Agent” on page 74.
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 the Program Neighborhood Agent as described in “To enable the Program Neighborhood Agent” on page 74.
2. Select reconnection options. You can select to:

- **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 via Program Neighborhood Agent, Program Neighborhood or Web Interface.

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

Accessing Applications and Files Using the Program Neighborhood Agent

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

Connecting to Applications

1. Enable the Program Neighborhood Agent as described in “To enable the Program Neighborhood Agent” on page 74.
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 MetaFrame 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 the 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, the 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 the 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 MetaFrame Presentation Server to determine a default time-out period for sessions active on the server. See the *MetaFrame Presentation Server Administrator's Guide* for more detail.

Reconnecting to Applications

To reconnect to applications you previously accessed through the 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 78 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 the 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

A

- adding clients to client update database 35
- alternate address translation, configuring 53
- applications
 - associating file types with 18, 45
 - hotkeys 61
 - on Web sites 19
 - printing from 56, 58
 - published 38, 44, 46, 66
 - specifying which to run after connecting 44–45
 - specifying working directory 45
 - Web Interface deployed 19
- audio
 - bidirectional 48
- audio input 13
- audio quality 19, 50
 - configuring using Program Neighborhood Agent 77
- auto client reconnect 21
- automatic update of client 28

B

- bandwidth
 - requirements 20
- bidirectional audio 48, 50
 - Options tab 41
- business recovery configuration 42

C

- Citrix documentation set
 - accessing 8
- client
 - installing from PC 25
 - installing locally 25
 - starting 26
 - uninstalling 37
 - updating automatically 28
- client audio mapping 19
- client auto update feature 20, 28
- client device mapping 18
 - overview 18
- client drive mapping 18

- Client for Windows CE
 - configuring 23, 71
 - configuring network protocol 41
 - controlling server location by 42
 - documentation 9
 - feature summary 11
 - overview 8, 11, 23, 71
- client printer mapping 19, 56
- client update database
 - adding clients 35
 - changing client properties 36
 - configuring 31
 - creating new 32
 - removing clients 35
 - setting default 32
- client, updating automatically 20, 28
- color depth
 - configuring 47
- COM port mapping 19
- compression 41, 48–50, 66
 - Options tab 41
- configuring default server location options 64
- configuring server-side for printing 56
- configuring the client update database 31
- connection
 - to a MetaFrame Presentation Server computer 40
 - using existing connections 40
- connections
 - changing properties of 51
 - changing server location options 43
 - configuring alternate address translation 53
 - configuring secure proxy server 53
 - configuring SOCKS proxy server 52
 - connecting using existing 40
 - creating new 38
 - editing properties of 40
 - enabling encryption level 51
 - enabling SpeedScreen 51
 - running applications 44
 - through Program Neighborhood Agent 78
 - to multiple server farms 79

- content redirection 72
- creating a new client update database 32
- creating a new connection
 - using connection manager 38
 - using Program Neighborhood Agent 78

D

- data compression 20, 41, 48, 50
 - enabling 66
- device mapping 18
- digital dictation support 11
 - overview 13
- disconnected sessions, reconnecting to 21
- disconnecting from applications
 - using Program Neighborhood Agent 79
- disk caching 49
 - overview 17
- displaying mapped client printers 57
- drive mapping 18
- dynamic session configuration 11
 - overview 14

E

- editing a connection 40
- encryption 12, 18, 42, 48, 51, 54
 - Options tab 41
 - setting level 51
 - using ICA encryption 54
 - using SSL/TLS 55

F

- feature summary list 11
- file type association 18, 45
- firewall proxy servers
 - secure proxy 18, 51, 53
 - SOCKS proxy 18, 51, 53, 60
- firewalls
 - alternate address translation 53
 - configuring client 51
 - connection settings 52
 - default settings 65

G

- global settings
 - edit 59
 - firewall settings 51
 - hotkeys 60
 - preferences 62
- guide 7
 - audience profile 7

H

- high latency connections 21, 67
- hotkeys 59
 - changing default 61
 - configuring 60
- HTML user interface
 - overview 16
- HTTPS proxy
 - see secure proxy

I

- ICA encryption 42, 46, 51, 54
- ICA session settings
 - modifying using Program Neighborhood Agent 77
- ICA sessions
 - auto client reconnect feature 21
 - different time zones 20
 - published applications 38
 - resuming on a different device 18
 - specifying logon information 46
- IME support
 - enabling 49
 - overview 16
- Input Method Editors
 - enabling 49
- installing the client 24
- intermediate zoom factor
 - setting 63

L

- local text echo 21
- logging off from ICA session
 - using Program Neighborhood Agent 80
- logon credentials
 - setting 40
- logon information 46

M

- mapping client devices
 - audio 18
 - COM port 18
 - drives 18
 - printers 18, 56
- MetaFrame Presentation Server for UNIX 19, 21, 56
 - mapping client printers 56
 - printing 56
- microphone input
 - ask before use 50
 - disabled 50
 - enabled 50
- mouse click feedback 21, 67
- multiple server farm support 11, 15, 79

N

- network connections
 - editing existing 40
 - improving slow 51
- network protocol 41
 - setting 41
 - SSL/TLS + HTTP 42, 44, 54, 64
 - SSL/TLS + HTTPS 42–44, 54–55, 64
 - TCP 41–42, 54
 - TCP + HTTP 42
- new connection, creating 38
- NTLM support
 - overview 17

O

- Options tab 48
 - bidirectional audio 41
 - compression 41
 - disk caching 41
 - encryption 41
 - session reliability 41
 - SpeedScreen support 41
- overview 7, 14–15

P

- palette device
 - enabling 63
- panning and scaling 40, 63, 68
 - overview 15
- passwords
 - specifying 46
- performance
 - data compression 66
 - disk caching 67
 - improving 66
 - SpeedScreen 67
- printer mapping 19
- printing
 - displaying mapped client printers 57
 - enabling 56
 - files from ICA sessions 58
 - from applications 58
 - from the client device 58
- Program Neighborhood Agent
 - accessing 78
 - configuring settings on the client device 74
 - configuring settings on the server 72
 - disconnecting from applications 79
 - enabling 78
 - logging off from ICA sessions 80
 - modifying session settings on the client device 74
 - overview 17
 - reconnecting to applications 80
- properties
 - connection 40
 - window 47
- published applications 38, 44, 46, 66

R

- Reconnect 18
- reconnecting to applications
 - using Program Neighborhood Agent 80
- remote access
 - enabling 27
- removing clients from client update database 35
- right-click functionality 18
- Roaming User Reconnect 18

S

- scaling 40, 63, 68
 - overview 15
- secure firewall proxy 53

- secure proxy
 - configuring 53
 - feature description 18
- security 51
 - configuring 51, 54
 - ICA encryption 54
 - SSL/TLS 55
- Security proxy
 - see secure proxy
- security proxy
 - see secure proxy
- serial number 62
- server connections
 - configuring using Program Neighborhood Agent 77
- server location 41
 - changing defaults 64
 - changing options 43
 - description 41
- server settings configuring 75
- session reliability 11, 48
 - enabling 51
 - Options tab 41
 - overview 13
- session settings
 - modifying using Program Neighborhood Agent 77
- sessions
 - reliability 48
 - roaming capabilities 18
- SOCKS firewall proxy
 - using with the Client for Windows CE 51
- sound quality 19, 50
 - configuring using Program Neighborhood Agent 77
- sound support 48
- specifying an application to run 44
- SpeedScreen
 - configuring 67
 - enabling 51
 - feature description 21
- SpeedScreen browser acceleration
 - overview 17
- SpeedScreen support
 - Options tab 41
- SSL 41–42, 44, 51, 53, 64–65
- SSL - Secure Sockets Layer 55, 60, 65
- SSL-tunneling
 - see secure proxy
- SSL/TLS + HTTP 42, 44, 54, 64
- SSL/TLS + HTTPS 42–44, 54–55, 64
- SSL/TLS + HTTPS browsing 42
- supported processors 24

- system requirements 24

T

- TCP 41, 54
- TCP server locations 41
- TCP+ HTTP browsing 42
- time zone support 20
- title, invalid characters 39
- TLS encryption 18
- Transport Layer Security (TLS) 12, 18, 55
 - support 18
 - TLS encryption 18

U

- UDP browsing 41
- uninstalling the client 37
- UNIX applications
 - printing from 58
- updating the client automatically 28
- updating the ICA client automatically 20
- user interface
 - overview 16
- user name, specifying 46

V

- virtual screen control 68

W

- Web Interface 19
- window properties 47, 77
 - configuring using Program Neighborhood Agent 77
- Windows NT Challenge/Response support
 - overview 17
- workspace control 11, 14
 - configuring 75

Z

- zone preference and failover 11
 - overview 14
- zoom factor
 - setting 63