

# Administrator's Guide

## **Citrix® ICA® Win32 Clients**

Version 7.0

Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement. A copy of the End User License Agreement is included in the root directory of the the root directory of the Components CD-ROM.

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.

Copyright ©1999-2003 Citrix Systems, Inc. All rights reserved.

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

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

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States of America and other countries.

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

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

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

This software is based in part on the work of the Independent JPEG Group.

All other trademarks and registered trademarks are the property of their respective owners.

Last Updated: April 30, 2003 4:23 pm (MP for LBL)

---

# Contents

## Chapter 1

### Before You Begin

How to Use this Guide . . . . .	7
Document Conventions . . . . .	8
Finding More Information . . . . .	9
Citrix on the World Wide Web . . . . .	10
Providing Feedback About this Guide. . . . .	11

## Chapter 2

### Introducing the Citrix ICA Win32 Clients

Overview . . . . .	13
Your Choices of ICA Win32 Clients . . . . .	14
Deciding Which ICA Win32 Client to Use . . . . .	15
Delivering Published Resources to Users . . . . .	15
New in this Release . . . . .	17
Features Included in Feature Release 2 . . . . .	20
Features Included In Feature Release 1 . . . . .	23
Features Included In MetaFrame XP For Windows . . . . .	25
Configuring the ICA Win32 Clients for Deployment. . . . .	29
Using Microsoft Systems Management Server or Active Directory Services . . . . .	29
Creating an ICA Client Download Web Site on a Web Server . . . . .	30
Deploying ICA Clients over a Network. . . . .	30
Creating ICA Client Installation Disks. . . . .	31
Using the Components CD. . . . .	32

**Chapter 3****Configuring and Installing the ICA Win32 Program Neighborhood Agent**

Overview of the ICA Win32 Program Neighborhood Agent . . . . .	34
ICA Win32 Program Neighborhood Agent Features . . . . .	34
System Requirements . . . . .	36
Installing the ICA Win32 Program Neighborhood Agent . . . . .	36
Installing the ICA Win32 Program Neighborhood Agent with the Windows Installer Package . . . . .	37
Installing the ICA Win32 Program Neighborhood Agent with the Self-Extracting Executable . . . . .	39
Configuring the ICA Win32 Program Neighborhood Agent Centrally . . . . .	42
The Program Neighborhood Agent Admin Tool . . . . .	42
Configuration Files . . . . .	43
Configuring Farm-Wide Settings . . . . .	44
The Properties Dialog Box . . . . .	44
Customizing the ICA Win32 Program Neighborhood Agent . . . . .	47
Configuring the Server URL . . . . .	47
Selecting a Logon Mode . . . . .	48

**Chapter 4****Installing and Configuring the ICA Win32 Web Client**

Overview of the ICA Win32 Web Clients . . . . .	49
Features of the ICA Win32 Web Clients . . . . .	50
System Requirements . . . . .	51
Configuring the ICA Win32 Web Client for Silent User Installation . . . . .	52
Installing the ICA Win32 Web Client . . . . .	53
Installing the ICA Win32 Web Client (Minimal Installation) . . . . .	54

**Chapter 5****Installing and Configuring the ICA Win32 Program Neighborhood Client**

Overview of the ICA Win32 Program Neighborhood Client . . . . .	57
ICA Win32 Program Neighborhood Client Features . . . . .	58
System Requirements . . . . .	59
Installing the ICA Win32 Program Neighborhood Client . . . . .	60
Installing the ICA Win32 Program Neighborhood Client with the Windows Installer Package . . . . .	60
Installing the ICA Win32 Program Neighborhood Client with the Self-Extracting Executable . . . . .	62
Starting the ICA Win32 Program Neighborhood Client . . . . .	66

Configuring the ICA Win32 Program Neighborhood Client . . . . .	67
Configuring Network Protocol and Server Location . . . . .	67
Specifying the Network Protocol for ICA Browsing . . . . .	68
Configuring Connections to MetaFrame Servers and Published Applications . . . . .	70
Using Application Sets and Custom ICA Connections . . . . .	73
Configuring General Settings . . . . .	82
Configuring Bitmap Caching . . . . .	83
Configuring Hotkeys . . . . .	84
Configuring Event Logging . . . . .	85
Improving ICA Performance Over Low-Bandwidth Connections . . . . .	86
Changing Your ICA Client Configuration . . . . .	87
Changing the Way You Use the Client . . . . .	87

## Chapter 6

### Configuring Features Common to the ICA Win32 Clients

Configuring New Features of Version 7.0 of the ICA Win32 Clients . . . . .	89
Dynamic Client Name Support . . . . .	89
SpeedScreen Browser Acceleration . . . . .	90
Windows NT Challenge/Response (NTLM) Support . . . . .	90
Certificate Revocation List Checking . . . . .	90
Configuring Existing Features Common to the ICA Win32 Clients . . . . .	91
User-to-User Shadowing . . . . .	91
Smart Card Support . . . . .	92
Auto Client Reconnect . . . . .	93
Novell Directory Services Support . . . . .	93
DNS Name Resolution . . . . .	96
Enabling Extended Parameter Passing . . . . .	97
Mapping Client Devices . . . . .	101
Turning off Client Device Mappings . . . . .	101
Configuring Multiple Monitors . . . . .	106
Using the ICA Win32 Program Neighborhood and Web Clients with Application Launching and Embedding . . . . .	107
Application Launching and Embedding . . . . .	107
Launched Applications . . . . .	108
Embedded Applications . . . . .	109

Using Applications Published on MetaFrame Servers for UNIX Operating Systems .....	111
Using the Window Manager .....	111
Cutting and Pasting Graphics Using ctxgrab and ctxcapture. ....	113

**Chapter 7****Implementing Security for the ICA Win32 Clients**

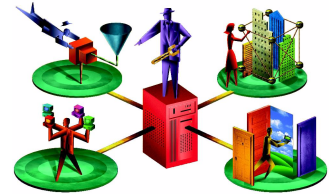
Integrating the ICA Win32 Clients with Your Security Solutions .....	117
Connecting to a Server Through a Proxy Server .....	118
Using the ICA Win32 Clients with the Secure Gateway for MetaFrame or SSL Relay .....	122
Connecting to a Server Through a Firewall .....	132

**Chapter 8****Updating the ICA Win32 Clients**

About the Client Auto Update Feature .....	135
The ICA Client Update Process .....	136
Configuring the Client Update Database .....	137
Using the Client Update Configuration Utility .....	137
Creating a New Client Update Database .....	138
Specifying a Default Client Update Database .....	139
Configuring Default Client Update Options .....	140
Adding ICA Clients to the Client Update Database .....	141
Working with the ICA Win32 Client Downloaded from the Citrix Web Site .....	142
Removing an ICA Client From the Client Update Database .....	143
Changing the Properties of the ICA Win32 Client .....	143

<b>Index .....</b>	<b>145</b>
--------------------	------------

# Before You Begin



This manual is for system administrators responsible for installing, configuring, deploying, and maintaining the Citrix ICA Win32 Clients (also called the Citrix ICA Clients for 32-bit Windows). This manual assumes knowledge of:

- The MetaFrame server to which your ICA Clients connect
- The operating system on the client device (Windows 9x, Windows Me, Windows NT, Windows 2000, or Windows XP)
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports, modems, and device adapters

## How to Use this Guide

To get the most out of the *Citrix ICA Win32 Clients Administrator's Guide*, review the table of contents to familiarize yourself with the topics discussed.

This guide contains the following sections:

Chapter	Contents
Chapter 1, "Before You Begin"	Gives an overview of this document.
Chapter 2, "Introducing the Citrix ICA Win32 Clients"	Highlights new and existing features of the ICA Win32 Clients; includes a discussion of which ICA Client(s) to use.
Chapter 3, "Configuring and Installing the ICA Win32 Program Neighborhood Agent"	Includes instructions for installing, configuring, and running the ICA Win32 Program Neighborhood Agent.
Chapter 4, "Installing and Configuring the ICA Win32 Web Client"	Includes instructions for installing, configuring, and running the ICA Win32 Web Client.
Chapter 5, "Installing and Configuring the ICA Win32 Program Neighborhood Client"	Includes instructions for installing, configuring, and running the ICA Win32 Program Neighborhood Client.

Chapter	Contents
Chapter 6, "Configuring Features Common to the ICA Win32 Clients"	Includes instructions for configuring new and existing features common to the ICA Win32 Clients.
Chapter 7, "Implementing Security for the ICA Win32 Clients"	Includes information about directing ICA traffic through proxy servers and firewalls, and configuring the ICA Clients to use the Secure Gateway for MetaFrame or SSL Relay.
Chapter 8, "Updating the ICA Win32 Clients"	Includes instructions for deploying ICA Win32 Client updates across your network using the Client Auto Update feature.

The MetaFrame XP product family allows you to publish a variety of resources for remote access by users. These resources include applications (executables), content files (non-executables, such as text or video files), and entire computer desktops. When referring to all types of resources you can publish with MetaFrame, this document generally uses the term *published resources*. When referring to published content files or published desktops, this document uses the term *published content*, or *published desktop*, respectively.

## Document Conventions

The following conventional terms, text formats, and symbols are used throughout the printed documentation:

Convention	Meaning
<b>Boldface</b>	Commands, names of interface items such as text boxes and option buttons, and user input.
<i>Italics</i>	Placeholders for information or parameters that you provide. For example, <i>filename</i> in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.
UPPERCASE	Keyboard keys, such as CTRL for the Control key and F2 for the function key that is labeled F2.
Monospace	Text displayed in a text file.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name specified when Windows is installed.
{ braces }	A series of items, one of which is required in command statements. For example, { <b>yes</b>   <b>no</b> } means you must type <b>yes</b> or <b>no</b> . Do not type the braces themselves.



Convention	Meaning
[ brackets ]	Optional items in command statements. For example, [ <b>ping</b> ] means that you can type <b>/ping</b> with the command. Do not type the brackets themselves.
(vertical bar)	A separator between items in braces or brackets in command statements. For example, { <b>/hold</b>   <b>/release</b>   <b>/delete</b> } means you type <b>/hold</b> or <b>/release</b> or <b>/delete</b> .
... (ellipsis)	You can repeat the previous item or items in command statements. For example, <b>/route:devicename[,...]</b> means you can type additional <i>devicenames</i> separated by commas.
▶	Step-by-step procedural instructions.

## Finding More Information

This manual contains conceptual information and installation and configuration steps for the ICA Win32 Clients. For additional information, consult the following:

- The online help for the ICA Client you deploy
- The *Citrix ICA Client Administrator's Guides* for the other ICA Clients you deploy
- The *Configuration Guide for the ICA Win32 Clients*, available from the Citrix Web site at <http://www.citrix.com/support>
- The documentation included in your MetaFrame server package for instructions about installing, configuring, and maintaining your MetaFrame servers

This book and other Citrix documentation are available in Adobe PDF format in the following locations:

- The documentation directory of your MetaFrame XP Components CD
- <http://www.citrix.com/download>; click the ICA Client platform for which you want information
- <http://www.citrix.com/support>; click Product Documentation and choose ICA Client

Using the Adobe Acrobat Reader, you can view and search the documentation electronically or print it for easy reference. You can download the Adobe Acrobat Reader for free from the Adobe Web site at <http://www.adobe.com/>.

---

**Important** Always consult the Readme files for your MetaFrame server and the Citrix ICA Client for any last-minute updates, installation instructions, and corrections to the documentation.

---

## Citrix on the World Wide Web

The Citrix Web site, at <http://www.citrix.com/>, offers a variety of information and services for Citrix customers and users. From the Citrix home page, you can access Citrix online Technical Support Services and other information designed to assist you, including the following:

- Downloadable Citrix ICA Clients (at <http://www.citrix.com/download>).
- Citrix Product Documentation Library, containing the latest documentation for all Citrix products (at <http://www.citrix.com/support>, select Product Documentation). You can download updated editions of the documentation that ships with Citrix products and supplemental documentation that may be available only from the Citrix Web site.
- Program information about Citrix Preferred Support Services options.
- An FTP server containing the latest service packs, hotfixes, and utilities.
- An online Solution Knowledge Base containing an extensive collection of application notes, technical articles, troubleshooting tips, and white papers.
- Interactive online Solution Forums for discussion of technical issues with other users.
- Notes containing Frequently Asked Questions with answers to common technical and troubleshooting questions are included in the Citrix Knowledge Base at <http://www.citrix.com/support/>. Click the link for Knowledge Base.
- Information about programs and courseware for Citrix training and certifications.
- Contact information for Citrix headquarters, including worldwide, European, Asia Pacific, and Japan headquarters.
- The Citrix Developer Network (CDN) at <http://www.citrix.com/cdn>. This open enrollment membership program provides access to developer tool kits, technical information, and test programs, for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate MetaFrame server-based computing solutions into their products.

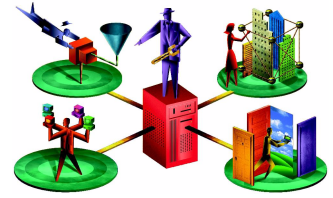
## Providing Feedback About this Guide

We strive to provide accurate, clear, complete, and usable documentation for Citrix products. If you have any comments, corrections, or suggestions for improving our documentation, we want to hear from you.

You can send email to the documentation authors at [documentation@citrix.com](mailto:documentation@citrix.com). Please include the product name, version number, and the title of the document in your message.



# Introducing the Citrix ICA Win32 Clients



This book introduces Version 7.0 of the Citrix ICA Win32 Clients for computers running 32-bit Windows operating systems. It is designed to help you decide which ICA Clients to use in your computing environment and how to deploy them.

---

**Note** For information about ICA Clients for other client devices and operating systems, see the documentation included on your MetaFrame XP Components CD, or visit our Web site at <http://www.citrix.com/>.

---

This chapter covers the following topics:

- Overview
- Deciding which ICA Win32 Client to use
- New in this release
- Improved in this release
- ICA Win32 Client features
- Preconfiguring and deploying the ICA Win32 Clients

## Overview

ICA Clients are the components of MetaFrame XP that users run on their computers to access applications running on MetaFrame XP servers. ICA Clients combine ease of deployment and use, and offer quick, secure access to applications, content, and entire computer desktops published on MetaFrame XP servers.

## Your Choices of ICA Win32 Clients

Different enterprises have different corporate needs, and your expectations and requirements for the way users access your published resources may shift as your corporate needs evolve and grow. This section summarizes the clients you can use. The clients are discussed in more detail in the next section.

MetaFrame offers you a choice of several ICA Win32 Clients for use on 32-bit Windows systems:

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

### ICA Win32 Program Neighborhood Agent

- Transparent integration of published resources with the user's desktop
- Native support for the full feature set of MetaFrame XP
- Requires Citrix NFuse Classic or the new Web Interface for MetaFrame XP

### ICA Win32 Web Client

- A smaller ICA Win32 Client for quick distribution
- Web browser-based access to published resources from links on your Web page for Netscape and Internet Explorer users
- Support for most of the features of MetaFrame XP
- Requires Citrix NFuse Classic, the new Web Interface for MetaFrame XP, or Application Launching and Embedding (ALE)
- Available in .Cab file format for Internet Explorer users for quick download and installation
- A minimal installation version is available that supports core ICA features, packaged in .Cab format

### ICA Win32 Program Neighborhood Client

- Program Neighborhood user interface
- Requires initial user configuration
- Does not require NFuse Classic or the new Web Interface for MetaFrame XP

## Deciding Which ICA Win32 Client to Use

Each ICA Win32 Client offers a robust and easy-to-manage solution for delivering your published resources to users. To decide which ICA Client or ICA Clients best fit your needs, consider the way you want users to access your published resources and the way you want to manage this access.

### Delivering Published Resources to Users

This section outlines the choices you have in delivering published resources to users, and which ICA Win32 Client to use with each delivery method. For in-depth information about each ICA Client, see the specific chapters for each client later in this book.

Based on your corporate technology needs, you can choose among three different methods for delivering published resources to users. Published resources can be delivered on the desktop, through a Web browser, or through a user interface.

### Access to Published Resources from Desktops

The ICA Win32 Program Neighborhood Agent allows your users to access published resources entirely from a familiar Windows desktop environment.

#### ICA Win32 Program Neighborhood Agent

**User Experience.** Users work with your published resources the same way they work with local applications and files. Published resources are represented throughout the client desktop, including the Start menu and the Windows system tray, by icons that behave just like local icons. Users can double click, move, and copy icons, and create shortcuts in their locations of choice. The Program Neighborhood Agent works in the background. Except for a shortcut menu available from the system tray, it does not have a user interface.

**Client Management and Administration.** All users running the Program Neighborhood Agent connect to a central configuration file. Once launched, this client periodically downloads its configuration data from a configuration file on your NFuse Classic server or server running the new Web Interface. You can modify the configuration data at any time as a means to manage and control your client population throughout your network from a single location and in real time. As a result, you can dynamically manage and control your client population network-wide from a single location and in real time.

The Program Neighborhood Agent requires NFuse Classic or the Web Interface and requires the presence on client devices of Microsoft Internet Explorer 5.0 or later, or of Netscape Navigator 4.78, 6.2, or later.

Because client-server data transfer occurs over standard HTTP or HTTPS protocols, you can use the Program Neighborhood Agent with firewalls using port 80 (for HTTP) or 443 (for HTTPS).

Depending on the deployment method you choose for this client, the size of its installation file ranges between approximately 1.9MB and 2.8MB.

For information about installing, configuring, and using the Program Neighborhood Agent, see “Installing the ICA Win32 Program Neighborhood Agent” on page 36 of this guide.

---

**Note** The configuration files stored on servers running the Web Interface for MetaFrame XP can be edited using the Program Neighborhood Agent Admin tool.

---

## Access to Published Resources from Web Browsers

If you want users to access your published resources from within their familiar Web browsers, use the ICA Win32 Web Client.

### ICA Win32 Web Client

**User Experience.** Users access published resources from within their Web browser by clicking links on a Web page you publish on your corporate intranet or the Internet. Clicking a link launches the published resource, either within the same browser window or in a new, separate browser window. The ICA Win32 Web Client does not require user configuration. It works in the background and does not have a user interface.

**Client Management and Administration.** You can use the ICA Win32 Web Client for access to resources enabled with NFuse Classic or the Web Interface, and for access to resources published with traditional Application Launching and Embedding (ALE). Publish links to your resources with NFuse Classic, the Web Interface, or by using an HTML wizard.

This ICA Client requires the presence on client devices of Microsoft Internet Explorer 5.0 or later, or of Netscape Navigator 4.78, 6.2, or later.

The ICA Web Client does not include a user interface or online Help files. Approximately 1.8MB in size, this ICA Client is quicker to download and install than the other ICA Win32 Clients.

The ICA Web Client is also packaged in .Cab file format for self-extraction and installation.

For information about installing, configuring, and using the ICA Web Client, see “Installing the ICA Win32 Web Client” on page 53.



### ICA Win32 Web Client (Minimal Installation)

A smaller version of the ICA Win32 Web Client, the minimal installation client is ideal for environments that do not require features such as COM port mapping, universal print driver, or client audio.

For information about installing, configuring, and using the ICA Web Client, see “Configuring the ICA Win32 Web Client for Silent User Installation” on page 52.

### Access to Published Resources from a User Interface

If you want users to access your published resources from within a distinctive user interface, use the ICA Win32 Program Neighborhood Client.

### ICA Win32 Program Neighborhood Client

**User Experience.** Using the ICA Program Neighborhood Client, users browse for application sets or create custom ICA connections to MetaFrame servers or to individual published resources. Icons representing application sets and custom ICA connections appear in the Program Neighborhood window.

**Client Management and Administration.** Choose this ICA Client if you do not want to publish your resources using NFuse Classic or the Web Interface. Although this client does not require either NFuse Classic or the Web Interface, you can use it to access resources published through NFuse Classic, the Web Interface, or Application Launching and Embedding (ALE).

Depending on how you choose to deploy this client, the installation file ranges in size between approximately 2.2MB and 3.2MB.

For information about installing, configuring, and using the Program Neighborhood Client, see “Installing the ICA Win32 Program Neighborhood Client” on page 60.

If you are planning to use NFuse Classic or the new Web Interface and have not yet deployed any ICA Clients, use the ICA Win32 Program Neighborhood Agent or the ICA Win32 Web Client.

## New in this Release

Version 7.0 of the ICA Win32 Clients ships with MetaFrame XP Server for Windows with Feature Release 3, and runs on Windows 9x, Windows NT, Windows 2000, and Windows XP operating systems. It introduces a wide range of new features and performance improvements, and is fully backward compatible with earlier versions of Windows and MetaFrame XP feature releases.

Highlights of Version 7.0 of the ICA Win32 Clients include:

- Support for rounded corners on seamless windows (Windows XP theme and custom application window design)
- Dynamic client name support
- SpeedScreen browser acceleration
- Program Neighborhood Agent administrative tool
- Windows NT Challenge/Response (NTLM) support
- Support for certificate revocation list checking

For information about enabling and configuring the new features on MetaFrame XP servers, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.

For detailed instructions about enabling and configuring the new features on client devices, see “Configuring Existing Features Common to the ICA Win32 Clients” on page 91 or the chapter about the specific ICA Win32 Client you plan to deploy.

In addition to offering a range of new features, Version 7.0 of the ICA Win32 Clients provides you with performance enhancements in the following areas:

- Universal Print Driver enhancements - Users can print in color and at a higher (600 dpi) resolution.
- Improved Auto Client Reconnect - If network problems cause a session to disconnect, users have more options for reconnecting to their disconnected session.
- Printer management enhancements - Client printer options are enhanced to include improved client printer mapping, automatic and on-demand replication of printer drivers, and printer resource assignment.

**Program Neighborhood Agent Admin Tool.** The Program Neighborhood Agent Admin tool is a Web browser-based tool designed to allow you to customize the settings and functionality of the Program Neighborhood Agent for your users. You can determine default settings for shortcuts, display size and colors, audio, logon method, authentication, and other functions. In addition, you can allow or deny users the ability to customize many of these options. The Admin tool resides on servers running the new Web Interface for MetaFrame XP. Changes to the configuration file, which resides on a server running the Web Interface, can be sent to connected clients when the configuration file is refreshed either at connection time or after a designated interval.

In previous releases of the Program Neighborhood Agent, the client configuration file had to be edited manually using a text editor. The Program Neighborhood Agent Admin tool allows you to edit the configuration file that resides on the server running the new Web Interface quickly and easily. This allows you to define client behavior and user options, as well as create, backup, and rename configuration files.

Features of the Program Neighborhood Agent Administrative tool include:

- Support for multiple configuration files
- Configuration file backup
- Concurrency control, allowing multiple administrators to view the same configuration file without overwriting each other's changes
- Restricted access to the tool (local machine administrators only)

For more information about the Program Neighborhood Agent Admin tool, see “Configuring Farm-Wide Settings” on page 44.

**Dynamic Client Name Support.** The ICA Win32 Clients now support dynamic client names. When selected during installation, the client name is set to the machine name when the client software is installed and is updated if the machine name changes.

For more information about dynamic client names, see “Dynamic Client Name Support” on page 89.

**SpeedScreen browser acceleration.** SpeedScreen browser acceleration introduces major performance improvements for users connecting to Internet Explorer published on a MetaFrame XP server. SpeedScreen browser acceleration is available only for Internet Explorer Version 5.5 or later running inside a MetaFrame session.

SpeedScreen browser acceleration requires less bandwidth and allows users running Internet Explorer as a published application to interact with the browser while graphically rich pages or large images are being downloaded. You can enable SpeedScreen browser acceleration for individual MetaFrame servers or for an entire MetaFrame XP server farm.

When the SpeedScreen browser acceleration feature is enabled, the user's browser experience is improved by the following functionality:

- **Background image delivery.** Users can now click Back and Stop while images are being downloaded from Web sites.
- **Progressive drawing.** JPEG images begin to appear in the browser before they are completely downloaded, allowing users to interact with them without having to wait until they are completely downloaded.
- **Responsive scrolling.** Users can now scroll Web pages before any image content is served. Images continue to be downloaded while users interact with the browser.

For more information about SpeedScreen browser acceleration, see the *MetaFrame XP Server Administrator's Guide*.

**Universal print driver.** Users printing with the Universal print driver can now print to color and high-resolution printers (600 dots per inch). Print drivers can be automatically installed for network printers and a driver compatibility check is enforced for all methods of printer creation.

**Windows NT Challenge/Response (NTLM) support.** Version 7.0 of the ICA Win32 Clients provides support for networks using Windows NT Challenge/Response (NTLM) for security and authentication.

---

**Note** On client devices running Windows 95, 98, and Me, you need to manually enable the **User Control Package** to use NTLM authentication. Go to **Control Panel > Network > Access Control**. On the Access Control screen, select **User-level access control**. If the User Control Package is not enabled, the client uses basic authentication, not NTLM authentication.

---

**Certificate Revocation List Checking Support.** When connected to a MetaFrame XP server, the ICA Win32 Clients can now check whether or not the server's certificate has been revoked. This feature improves the cryptographic authentication of the MetaFrame XP server and improves the overall security of the SSL/TLS connections between an ICA Win32 Client and a MetaFrame XP server.

## Features Included in Feature Release 2

**User-to-user shadowing.** Shadowing is the process of monitoring a user's session remotely and, optionally, participating in the session using your own keyboard and mouse. Previously reserved for MetaFrame administrators, this feature no longer requires administrative rights. You can now make shadowing available to users, adding powerful collaborative capabilities to a variety of applications, including:

- Help desks, where trained personnel troubleshoot applications
- Training organizations, where students observe instructors, and instructors monitor student performance
- Presentation sessions, where multiple remote users attend a presentation hosted by a single user

Shadowing does not require client configuration. This feature is governed by user policies set on the MetaFrame XP server. For information about enabling and configuring this feature, see the *MetaFrame XP Server Administrator's Guide* located in the \Docs directory of the MetaFrame CD.

**Smart Card support.** The ICA Win32 Clients offer support for a number of smart card readers. If smart card support is enabled on both the server and client sides, you can use smart cards for the following purposes:

- **Smart card logon authentication support.** Use smart cards to authenticate users to MetaFrame XP servers.
- **Smart card application support.** Allows users to digitally sign email within smart card-aware published applications. As of this writing, the following applications are smart card-aware:
  - Microsoft Outlook 2000; Microsoft Outlook XP
  - Microsoft Internet Explorer 5.5; Microsoft Internet Explorer 6.0

Smart card data is security-sensitive. MetaFrame XP offers a variety of security solutions to protect the transmission of your security-sensitive data. See Chapter 7 of this guide for more information.

Smart card devices and published applications must comply with the PC/SC industry standard.

Smart card support requires configuration on all ICA Win32 Clients.

**Content Redirection.** Using MetaFrame XP server-based file type association, you can redirect application launching from server to client or from client to server. As a result, the server controls whether a published or a local application is invoked when a user opens a particular file. MetaFrame XP supports the following types of content redirection:

- **From server-to-client:** Using server-to-client content redirection, you can leverage local applications to offload MetaFrame server resources. Server-to-client content redirection forces Web or multimedia links embedded in published applications to invoke the associated client-side application. For example, using a published application, you can view a text file that contains an embedded URL pointing to a multimedia file. When you click the URL, the multimedia file invokes the associated multimedia player on the client device rather than the player published on the MetaFrame server. If the associated multimedia player is not installed on the client device, the file invokes the published player.

This variation of content redirection does not require client configuration.

- **From client-to-server:** Double-clicking a client-side file invokes the associated published application. Opening a local text document, for example, invokes the associated published application.

For example, if you receive an email attachment and do not have an application installed on your local device that can open the attachment, you will not receive an error message. Instead, the associated published application is invoked on the MetaFrame server, allowing you to view the attachment.

*ICA Win32 Program  
Neighborhood Agent  
only*

Functionally equivalent to extended parameter passing, a feature introduced in Feature Release 1 of MetaFrame XP for Windows, client-to-server content redirection allows you to enforce all underlying file type associations from the MetaFrame server, eliminating the need to configure extended parameter passing on individual client devices.

This variation of content redirection does not require client configuration.

*ICA Win32 Program  
Neighborhood Agent  
or  
any ICA Win32 Client  
on a server running  
the Web Interface*

**Enhanced content publishing.** You no longer need to download published content to the client device and open it with a local application. Instead, you can associate and open published content with a published application on the MetaFrame server, allowing you to, for example, open published images using client devices that do not have applications other than a Web browser installed.

**Support for NFuse and the new Web Interface.** All ICA Win32 Clients provide support for NFuse Classic, the new Web Interface, and the new Web Interface Extension for MetaFrame XP.

**Support for TLS encryption of ICA traffic.** The ICA Win32 Clients support TLS 1.0, the successor to SSL 3.0, for environments that demand it. TLS (Transport Layer Security) is the standardized form of SSL (Secure Sockets Layer). 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.

**Support for the Secure Gateway for MetaFrame.** The ICA Win32 Clients provide full support for the Secure Gateway, which acts as a secure Internet gateway between SSL/TLS-enabled ICA Clients and MetaFrame XP servers. The Internet portion of ICA traffic between client devices and the server is SSL/TLS-encrypted. SSL/TLS is the Internet standard 128-bit encryption technology used for client/server authentication. It ensures the integrity and privacy of data transfers across public networks.

**Enhanced Internet proxy support.** As an alternative to SOCKS proxy, the ICA Win32 Clients also support secure proxy (also known as security proxy, HTTPS proxy, and SSL-tunneling). Proxy authentication is also supported.

The ICA Win32 Clients can automatically detect proxy servers by obtaining the details of proxy servers on the network from the Web browser.

**Roaming user reconnect.** This feature adds roaming capabilities to ICA sessions. Previously, ICA sessions were identified by the name of the client device from which they were initiated, and limited to that device. Feature Release 2 of MetaFrame XP makes ICA sessions portable, by allowing you to start a session on one client device and resume your work from any ICA-enabled device anywhere, anytime.

Roaming user reconnect does not require client configuration.

---

## Features Included In Feature Release 1

**Universal print driver support.** The Citrix universal print driver is a standard Windows 2000 or Windows NT print driver that encapsulates print jobs in PCL4 format. A client-based interpreter renders the print job using the client device's local print driver and printing services. The Universal Print Driver renders print jobs in black and white up to 300 dpi to high-resolution printers.

The universal print driver generates smaller print jobs, which can significantly improve performance when printing over WAN or dial-up connections.

---

**Note** If your MetaFrame server is running Feature Release 3, the universal print driver renders print jobs in color or black and white up to 600 dpi to high-resolution printers.

---

---

**Note** If the MetaFrame server is configured to automatically create both native driver and universal print driver printers on the client device, you must explicitly select a printer to process print jobs. If the print job requires color or advanced printing options such as duplex printing, select the standard printer, which uses the printer's native driver.

---

**Auto client reconnect.** ICA sessions can be dropped for a variety of reasons, including unreliable networks, highly variable network latency, or range limitations of wireless devices.

Auto client reconnect is triggered when the ICA Client detects a disconnected session. When this feature is enabled on a MetaFrame XP server, users can transparently reconnect to their session without having to reenter their logon credentials.

Automatic client reconnection does not occur if users exit applications without logging off.

**Windows Installer Packages for ICA Win32 Clients.** The ICA Win32 Program Neighborhood Agent and the ICA Win32 Program Neighborhood Client are available as Microsoft Windows Installer (.msi) packages. If your network is based on Windows 2000 or later, you can take advantage of Microsoft Systems Management Server or Active Directory Services to deploy updated versions of these clients using the Windows Installer packages.

If your network does not have Systems Management Server or Active Directory Services available, you can use client auto update to deploy to install ICA Client updates using the self-extracting executable (.exe) files.

The ICA Win32 Web Client is not currently available as a Windows Installer package. Use the self-extracting executable to install the ICA Web Client.

---

**Note** Use Microsoft Systems Management Server or Active Directory to update ICA Clients previously installed with Windows Installer packages, and use client auto update to update ICA Clients previously installed with the self-extracting executable. The two technologies are not interchangeable.

---

---

**Note** To install the ICA Client software using the Windows Installer package, the Windows Installer Service must be installed on the client device. This service is present by default on Windows 2000 systems. To install ICA Clients on client devices running earlier versions of the Windows operating system, you must use the self-extracting executable or install the Windows Installer 2.0 Redistributable for Windows, available at <http://www.microsoft.com/>.

---

**Published content support.** In addition to applications that are executable (.exe) files, you can also publish content files, which are non-executable. Content files include documents, Web pages, and audio/video files. You publish content on the MetaFrame server in the same manner as applications. The server then “pushes” the content to the client device.

Users open published content with the associated content viewer or player on the client device or the server, depending on published application settings.

**Novell Directory Services support.** When launching ICA Win32 Client software, users can log on and be authenticated using their NDS credentials. Supported NDS credentials are user name (or distinguished name), password, directory tree, and context.

**DNS name resolution.** You can configure ICA Win32 Clients that use the XML Service to connect to the MetaFrame farm to request a Domain Name System (DNS) name instead of a server's IP address.

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



---

## Features Included In MetaFrame XP For Windows

**Client auto update.** Client auto update allows you to update ICA Client installations using the self-extracting executable (.exe) files from a central location, rather than having to manually install new client versions on each client device. This feature does not require Microsoft Systems Management Server or Active Directory Services.

Client auto update stores self-extracting executables of new ICA Client versions in the client update database. It downloads the latest versions of the ICA Client software to client devices when users connect to the MetaFrame server. Citrix MetaFrame Server for UNIX Operating Systems does not support the client update database. To use the client update database, you must have a MetaFrame or MetaFrame XP for Windows server in your server farm.

ICA Client auto update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and serial).

ICA client auto update supports the following features:

- Automatically detects older client files
- Transparently copies new files over any ICA connection
- Provides full administrative control of client update options for each client
- Updates clients from a single database on a network share point
- Safely restores older client versions when needed

---

**Note** Use client auto update to update ICA Clients previously installed with the self-extracting executable. Use Microsoft Systems Management Server or Active Directory to update ICA Clients previously installed with Windows Installer packages. The two technologies are not interchangeable.

---

**Seamless windows.** Citrix ICA Win32 Clients support the seamless integration of local and remote applications on the local desktop. By selecting the Seamless windows option when configuring a connection, you can, in a single session, access multiple applications, have fully functional local keyboard controls (such as ALT+TAB), switch between local and remote applications on the local taskbar, and define remote application icons on the local desktop.

**Client device mapping.** ICA Win32 Clients support client device mapping. As a result, published resources running in an ICA session can access printers, disk drives, and COM port devices attached to the local client device.

- **Client drive mapping.** You can map server drives that are available to the client within an ICA session to the client drive. For example, you can map server drive H to drive C on the local device running the ICA Client. Applications, Windows Explorer, or File Manager use these mappings just like any other network mappings. Drive letters used for drive mapping are configurable and long file names are supported.
- **Client printer mapping.** Client printer mapping allows published resources to access local client printers. You browse for a client printer the same way as for network printers. You can transparently access your local printers from within the ICA session.
- **Client COM port mapping.** Just as with client printer mapping, the ICA Client COM port redirector allows published applications to access virtually any peripheral attached to the COM ports of the client device.

**Sound support.** ICA Client sound support allows a client device to execute sound files on the MetaFrame server and play them back on the sound system of the local client device if:

- The associated published application renders sound in waveform-audio format
- The client device is equipped with a sound card that supports the waveform-audio format

Waveform-audio is the standard sound format of Windows operating systems. ICA supports output in 8- and 16-bit mono and stereo at 8, 11.025, 22.05, and 44.1KHz. You can configure audio support to use one of three different sound compression schemes: high, medium, and low. Each scheme provides different sound quality and bandwidth usage.

This feature is not available on MetaFrame Server 1.0 and 1.1 for UNIX Operating Systems.

**Per-User time zone support.** This feature allows the ICA session to reflect the time zone of the client device, regardless of the time zone of the MetaFrame server hosting the session.

For example: A user in Los Angeles, which is in the Pacific time zone, logs on to a MetaFrame server in New York City, which is in the Eastern time zone, and launches Microsoft Outlook as a published application. Microsoft Outlook stamps emails sent during this ICA session with the user's Pacific time zone information.

**TAPI support.** ICA Win32 Clients provide TAPI modem support for dial-up connections to MetaFrame servers. TAPI support allows the Win32 Client to detect the presence of TAPI Version 1.4 or later modems on the client device. Users do not need to manage separate modem entries for their local communications programs.

When the ICA Client detects a TAPI modem, it uses the modem installation and configuration utilities built into Windows to manage the modem. If the client device is not TAPI-capable, the ICA Client uses its own modem installation and configuration utilities.

**Dialing prefixes.** ICA Clients support dialing prefixes. Dialing prefixes allow you to add special dialing codes, as required by different telephone systems, for dialing out and accessing a remote MetaFrame server.

The most common use of dialing prefixes is defining different dialing methods for different telephone systems. For example, a user with a laptop computer may need to dial 9 to get an outside line at the office, and may need to dial 1 plus the area code when working on the road or at home. In this case, the user can define a dialing prefix named Office for use when dialing out from the office, and a prefix called Remote for use when dialing in from the road or at home.

**Windows clipboard integration.** Users can copy, cut, and paste data between ICA sessions and local applications using the Windows clipboard.

**Low bandwidth requirements.** The Citrix ICA protocol typically uses 20K of bandwidth for each session.

**Disk caching and data compression.** These features increase performance over low speed asynchronous and WAN connections. Disk caching stores commonly used portions of your screen (such as icons and bitmaps) locally, increasing performance by avoiding retransmission of locally cached data. Data compression reduces 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 on MetaFrame Server 1.0 and 1.1 for UNIX Operating Systems.

The elements of SpeedScreen latency reduction are:

- **Local text echo.** This ICA Client and MetaFrame server option accelerates the display of text input on the client device.
- **Mouse-click feedback.** This ICA Client and MetaFrame server option provides visual feedback for mouse clicks to show that the user's input is being processed.

**Business recovery.** ICA Clients support multiple server sites (such as a primary and hot backup server) with different addresses for the same published resource name.

This feature provides uninterrupted connections to published resources in the event of a primary server disruption.

**TCP/IP+HTTP server location.** TCP/IP+HTTP server location allows you to retrieve MetaFrame server and published resource information across network configurations that restrict UDP broadcasts.

Configuring the ICA Win32 Clients to use the TCP/IP+HTTP network protocol has several advantages for most server farms:

- The protocol uses XML data encapsulated in HTTP packets, and uses TCP port 80 by default. Most firewalls are set to allow HTTP packets to pass on port 80.
- The protocol does not rely on UDP or broadcasts to locate servers in the server farm.
- The Citrix XML service works in a server farm that contains MetaFrame XP servers alone or in combination with NFuse Classic or the Web Interface, which allows users to connect to application portals with their Web browsers.

Routers pass TCP/IP packets between subnets, allowing client devices to locate servers that are not on the same subnet.

**Wheel mouse support.** If you run applications that offer wheel mouse support, the ICA Win32 Client transmits the wheel mouse movements in the same manner it transmits other mouse data. ICA Win32 Client wheel mouse support requires MetaFrame 1.8 Service Pack 1 or MetaFrame XP or later, and a local client device that supports wheel mouse functionality.

**Multiple-monitor support.** ICA Win32 Clients support multiple monitors connected to a single computer. Multiple-monitor support is available only when connecting to MetaFrame 1.8, Feature Release 1, and MetaFrame XP servers.

**Pass-through authentication.** Pass-through authentication provides the ability to pass the user's desktop password to the server, eliminating the need for multiple system and application authentications.

**Panning and scaling.** Panning allows you to scroll an ICA session image configured at a screen resolution that is higher than that of the client device. Scaling allows you to shrink an ICA session image to fit your screen.

---

**Note** You can shrink a Win32 Client session window to a minimum of 64 pixels in width. However, the Windows operating system may enforce a greater limit based on the prevailing desktop scheme, which overrides the ICA Client scaling limit.

---

## Configuring the ICA Win32 Clients for Deployment

You can deliver ICA Clients to your users and install the software using the following methods:

- Using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows 2000
- Creating an ICA Client download Web site on a Web server
- Copying the ICA Win32 files to a network share point
- Creating ICA Client installation disks
- Using the Components CD included in your MetaFrame XP media pack

For a detailed discussion of the latest deployment methods available, see the *MetaFrame XP Server Administrator's Guide*. If you are using MetaFrame XP in conjunction with the Web Interface, see the *Web Interface for MetaFrame XP Administrator's Guide* for information about deploying ICA Clients in that environment.

### Using Microsoft Systems Management Server or Active Directory Services

The ICA Win32 Program Neighborhood Client and the Program Neighborhood Agent are available as Windows Installer (.msi) packages for use with Microsoft Systems Management Server or Active Directory.

See your Windows 2000 or Systems Management Server documentation for more information.

The installer package files for all three ICA Win32 Clients are located in the following directories (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

Identical installer package files for the Program Neighborhood Agent are also located in the directory:

Icainst\language\ica32\pnagent

---

**Note** To install the ICA Client software using the Windows Installer package, the Windows Installer Service must be installed on the client device. This service is present by default on Windows 2000 systems. To install ICA Clients on client devices running earlier versions of the Windows operating system, you must use the self-extracting executable or install the Windows Installer 2.0 Redistributable for Windows, available at <http://www.microsoft.com/>.

---

## Creating an ICA Client Download Web Site on a Web Server

If you are not using NFuse Classic or the Web Interface, Citrix offers an installation method that uses a Web browser on the client device as the interface for downloading the ICA Client. You can create an ICA Client download Web site on a Web server. Users access a setup page that contains a link to ICA Win32 Client Setup.

You can download the elements required to create an ICA Client download Web site and the corresponding documentation from the Citrix Web site at <http://www.citrix.com/download>, or you can get the required files from the Components CD included in your MetaFrame XP media pack.

## Deploying ICA Clients over a Network

### ► To deploy ICA Win32 Client software from a network share point

1. Create a share point on a file server that is accessible to your users.
2. Copy the desired ICA Win32 Client executable from the Components CD to the share point. The executables are located in the following directory (substitute *language* with the language of your server software):

Icaweb\language\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)

- Es (Spanish)

Win32 Client	Executable	CAB file
Program Neighborhood Client	lca32.exe	N/A
Program Neighborhood Agent	lca32a.exe	N/A
Web Client	lca32t.exe	lca32.cab
Web Client (Minimal Installation)	N/A	lca32c.cab

3. Supply your users with the path to the executable.
4. Users double-click the executable to begin the installation process.

## Creating ICA Client Installation Disks

Use the ICA Client Creator to create client installation disks for the ICA Win32 Program Neighborhood Client. You will need three to four 3.5-inch, 1.44MB floppy disks to create the client installation disks.

- ▶ **To create Citrix ICA Client installation disks (on servers running Windows 2000)**
  1. From a MetaFrame XP server: Click **Start**> **Programs**> **Citrix**> **MetaFrame XP**> **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.
  2. In the Network Client or Service list, click the desired Citrix ICA Client. Select the **Format Disks** check box to format the disks when creating the installation media. Click **OK**.
  3. Follow the on-screen instructions.

- ▶ **To create Citrix ICA Client installation disks (on servers running Windows Server 2003)**

ICA Client Creator is not available on servers running Windows Server 2003. You must manually copy the files to preformatted floppies.

1. On a MetaFrame XP server: Navigate to the folder `\WINNT\system32\clients\lca\client\`
2. Copy the contents of each numbered folder onto corresponding preformatted floppy disks.

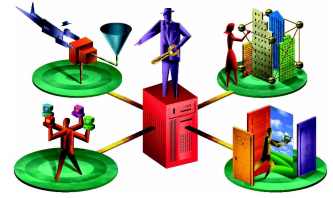
## Using the Components CD

The Components CD included in your MetaFrame XP media pack contains setup and installation files for all ICA Clients. You can use the Components CD to directly install ICA Client software on client devices that have CD-ROM drives or copy the CD image to a network share point on a file server.



---

# Configuring and Installing the ICA Win32 Program Neighborhood Agent



The Program Neighborhood Agent is a client designed for flexibility and ease of configuration. Shortcuts to resources published on MetaFrame servers can be integrated into users' desktops. For example, links to published applications can be displayed in users' Start menus or on their desktops with no need to open a Web browser or an additional application to launch the applications. You can determine what, if any, configuration options your users access and modify, such as audio, display, and logon settings.

Configure these options and settings on your server running the Web Interface using the Program Neighborhood Agent Admin tool. Each time users log on to the Program Neighborhood Agent, they see the most up to date Program Neighborhood Agent configuration. Changes made while users are connected will take effect when the client configuration is refreshed after a designated interval.

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

This chapter explains how to install and configure the ICA Win32 Program Neighborhood Agent and use the Program Neighborhood Agent Admin tool. The following topics are covered:

- Overview of the ICA Win32 Program Neighborhood Agent
- System Requirements
- Installing the ICA Win32 Program Neighborhood Agent
- Configuring the ICA Win32 Program Neighborhood Agent Centrally
- Configuring Farm-Wide Settings

- Customizing the ICA Win32 Program Neighborhood Agent

## Overview of the ICA Win32 Program Neighborhood Agent

Using the ICA Win32 Program Neighborhood Agent in conjunction with NFuse Classic or the Web Interface, you can integrate published resources with users' desktops. Users access remote applications, desktops, and content by clicking icons on their Windows desktop, in the Start menu, in the Windows system tray, or any combination thereof.

Among the functions the Program Neighborhood Agent handles are:

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

## ICA Win32 Program Neighborhood Agent Features

The ICA Win32 Program Neighborhood Agent offers the following features:

- Support for rounded corners (Windows XP theme and custom application window design)
- Dynamic client name support
- SpeedScreen browser acceleration
- Program Neighborhood Agent Admin tool (servers running the Web Interface only)
- NTLM support
- Support for certificate revocation list checking
- Universal print driver enhancements
- Improved auto client reconnect
- Printer mapping enhancements
- Windows desktop integration

- User-to-user shadowing
- Smart card support
- Content redirection
- Enhanced content publishing support
- Roaming user reconnect
- Support for SSL/TLS encryption of ICA session data
- Support for Citrix NFuse Classic, the new Web Interface, and the Web Interface Extension for MetaFrame XP
- Support for the Secure Gateway for MetaFrame
- Enhanced Internet proxy support
- Novell Directory Services support
- DNS name resolution support
- Seamless windows
- Client device mapping
- Sound support
- Windows installer packages
- Client auto update
- Windows clipboard integration
- Low bandwidth requirements
- SpeedScreen latency reduction
- Disk caching and data compression
- TCP/IP+HTTP server location
- Wheel mouse support
- Multiple monitor support
- Pass-through authentication
- Panning and scaling
- Per-user time zone support

## System Requirements

To run the ICA Win32 Program Neighborhood Agent, client devices must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system.
- Windows 95 (OSR2 or later), Windows 98, Windows Me, Windows 2000, Windows XP, or Windows NT 4 or later.
- 8MB RAM or greater for Windows 9x, 16MB RAM or greater for Windows NT 4.0, 32MB or greater for Windows Me and Windows 2000, and 128MB RAM for Windows XP.
- Internet Explorer Version 5.0 or later, or Netscape Navigator or Communicator Version 4.78, 6.2, or later.
- Microsoft mouse or 100% compatible mouse.
- VGA or SVGA video adapter with color monitor.
- High-density 3.5-inch disk drive (optional) and available hard disk space.
- Windows-compatible sound card for sound support (optional).
- For network connections to the MetaFrame server, a network interface card (NIC) and the appropriate network transport software are required. Supported connection methods and network transports are:
  - TCP/IP+HTTP
  - SSL/TLS+HTTPS

For information about configuring the ICA Win32 Clients to use SSL or TLS to secure communications, see “Configuring and Enabling ICA Clients for SSL and TLS” on page 126.

## Installing the ICA Win32 Program Neighborhood Agent

You can install the ICA Win32 Program Neighborhood Agent using one of the following packages:

- Ica32a.msi – a Windows Installer package for use with Windows 2000 Active Directory Services or Microsoft Systems Management Server, approximately 1.9MB in size
- Ica32a.exe – a self-extracting executable, approximately 2.75MB in size

---

**Note** For a discussion of methods for deploying ICA Win32 Client software to users, see the *MetaFrame XP Server Administrator's Guide*, included in your MetaFrame XP media pack.

---

## Installing the ICA Win32 Program Neighborhood Agent with the Windows Installer Package

You can distribute the Program Neighborhood Agent Windows Installer package (Ica32a.msi) with Microsoft Systems Management Server or Windows 2000 Active Directory Services.

This package is located in the following directories (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

Icainst\*language*\ica32\pnagent

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

---

**Note** To install the ICA Client software using the Windows Installer package, the Windows Installer Service must be installed on the client device. This service is present by default on Windows 2000 systems. To install ICA Clients on client devices running earlier versions of the Windows operating system, you must use the self-extracting executable or install the Windows Installer 2.0 Redistributable for Windows, available at <http://www.microsoft.com/>.

---

To uninstall an ICA Win32 Client that was installed with a Windows Installer package, run the **Add/Remove Programs** utility from the Control Panel, or run the installer package again and select the **Remove** option.

## Configuring the Windows Installer Package for Silent User Installation

You can configure the Program Neighborhood Agent Windows Installer package for “silent” user installation. Windows Installer informs the user when the client software is successfully installed. The user must clear the Windows Installer message box.

### ► To configure the Program Neighborhood Agent Windows Installer package for silent user installation

1. At a command prompt, type:

```
msiexec /I <MSI_Package> /qn+ [Key=Value]...
```

where <MSI\_Package> is the name of the installer package.

2. You can set the following keys:

**PROGRAM\_FOLDER\_NAME**=<Start Menu Program Folder Name>, where <Start Menu Program Folder Name> is the name of the Programs folder on the Start menu containing the shortcut to the Program Neighborhood Agent software. The default value is **Citrix Program Neighborhood Agent**. This function is not supported during client upgrades.

**ENABLE\_DYNAMIC\_CLIENT\_NAME**={**Yes** | **No**} To enable dynamic client name support during silent installation, the value of the property **ENABLE\_DYNAMIC\_CLIENT\_NAME** in your installer file must be **Yes**. To disable dynamic client name support, set this property to **No**.

**CLIENT\_ALLOW\_DOWNGRADE**={**Yes** | **No**} By default, this property is set to **No**. This prevents an installation of an earlier version of the client. Set to **Yes** to allow an installation of an earlier version of the client.

**ENABLE\_SSON**={**Yes** | **No**}. The default value is **No**. If you enable the **SSON** (Pass-through authentication) property, set the **ALLOW\_REBOOT** property to **No** to avoid automatic rebooting of the client system.

**ALLOW\_REBOOT**={**Yes** | **No**}. The default value is **Yes**.

**DEFAULT\_NDSCONTEXT**=<Context1 [,...]>. Include this parameter if you want to set a default context for NDS. If you are including more than one context, place the entire value in quotation marks and separate the contexts by a comma.

Examples of correct parameters:

```
DEFAULT_NDSCONTEXT=Context1
```

```
DEFAULT_NDSCONTEXT="Context1, Context2"
```

Example of an incorrect parameter:

```
DEFAULT_NDSCONTEXT=Context1, Context2
```

**SERVER\_LOCATION**=<Server\_URL>. The default value is **PNAgent**. Enter the URL of the NFuse Classic server, or the server running the Web Interface that hosts the configuration file. The format must be in the format `http://<servername>` or `https://<servername>`.

---

**Note** The Program Neighborhood Agent appends the default path and file name of the configuration file to the server URL. If you change the default location of the configuration file, you must enter the entire new path in the **SERVER\_LOCATION** key.

---

## Installing the ICA Win32 Program Neighborhood Agent with the Self-Extracting Executable

You can distribute the self-extracting executable (`Ica32a.exe`) to your users for direct installation on client devices.

This executable is located in the following directories (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

`Icaweb\language\ica32`

`Icainst\language\ica32\pnagent`

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

## Configuring the Self-Extracting Executable for Silent User Installation

You can limit user interaction with the self-extracting executable setup program by entering values in the `Install.ini` file before you deploy the Program Neighborhood Agent to your users.

---

**Important** You can use any standard compression utility to extract the client files from the packaged executable. However, you must use commercially available software to repackage the client files for distribution to your users.

---

► **To configure the self-extracting executable for silent user installation**

1. Extract the ICA Client files from Ica32a.exe using your preferred compression utility software, or by typing at a command line:

**Ica32a.exe -a -unpack:<Directory Location>**

where <Directory Location> is the path to the directory to which you want to extract the client files.

2. Locate and open the Install.ini file in a text editor.

You can set the following parameters. When you enter values for these parameters, setup dialog boxes do not appear on the user's screen.

**ServerURL**=URL for the server running the Web Interface or the NFuse Classic server. The default value is **PNAgent**. Enter the URL of the server running the Web Interface or the NFuse Classic server hosting the configuration file in the format **http://servername** or **https://servername** for SSL-secured communications.

**SetMachineNameClientName**=Enter **Yes** to accept the Windows machine name as the client device name.

**Location**=Enter the installation location. Use <PROGRAM\_FILES> if you want to install the files in a directory in the Program Files folder.

**StartMenu**=Enter the Start menu path. The path you enter here is appended to the Programs folder of the Start menu.

**InstallSingleSignOn**=Enter **Yes** to enable pass-through authentication.

**AcceptClientSideEULA**=Enter **Yes** to accept the end-user license agreement.

3. Save the file and exit the text editor.
4. Repackage the client files for distribution to your users.

► **To install the Program Neighborhood Agent with the self-extracting executable**

1. To install the client from the Components CD included in your MetaFrame XP media pack, run Ica32a.exe from the following directory (substitute *language* with the language of your server software):

Icaweb\language\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)



2. The **Welcome** screen appears. Read the information on this screen and click **Next**.
3. The **License Agreement** screen appears. Read the license agreement and click **Yes** if you agree to the terms of the agreement.  
Setup searches the client device for previously installed versions of the ICA Win32 Program Neighborhood Agent.
4. If Setup does not detect a previous installation of the ICA Win32 Program Neighborhood Agent, go to Step 6.  
If Setup detects a previous installation of the ICA Win32 Program Neighborhood Agent, the **Choose Installation Type** dialog box appears.  
The **Choose Installation Type** dialog box lets you choose to upgrade the existing client or to create a new installation of the Program Neighborhood Agent. The default value is **Upgrade the existing client**. Click **Next**.
5. The **Select Program Folder** dialog box appears.  
You can choose to use the default Citrix Program Neighborhood Agent folder, specify the name of a new program folder, or add the Program Neighborhood Agent icon to an existing folder. The program folder you specify is created if it does not already exist. Click **Next** to continue.
6. The **Server Address** dialog box appears.  
Enter the URL of the NFuse Classic server, or the server running the Web Interface to connect to in the format `http://servername` (for non-secure connections), or `https://servername` (for secure connections).  
Click **Next**.
7. The **Choose Installation Type** dialog box appears.  
Select **Yes** to enable the pass-through authentication logon mode. This feature allows the ICA Client to access a user's local Windows user name, password, and domain information, and pass it to the server. Users are not prompted to log on to the Program Neighborhood Agent separately.  
You must enable this logon mode in the configuration file on the NFuse Classic server or the server running the Web Interface to make it available to users. See "Configuring the ICA Win32 Program Neighborhood Agent Centrally" on page 42 for instructions. If you enabled this logon mode in the configuration file and you want the ICA Client to use this logon mode, select **Yes** on this screen then select **Pass-through authentication** as the logon mode in the client's **Properties** dialog box.

---

**Important** If you select **No** during the installation process, you must reinstall the Program Neighborhood Agent if you decide to use the pass-through authentication logon mode at a later time.

---

Click **Next**.

8. The **ICA Client Name** dialog box appears.

Specify a unique client name for your client device. MetaFrame servers use the client name to manage client printers and other system resources. If you do not assign a unique machine name to each client device, device mapping and application publishing may not operate correctly. You can use the client name displayed in the **Client Name** field or specify a new one.

When you are done, click **Next** to continue. A progress window appears, displaying the file names as they are copied to your hard drive.
9. You are informed that the Program Neighborhood Agent was successfully installed on the computer. Click **Finish**.

## Configuring the ICA Win32 Program Neighborhood Agent Centrally

Users' logon methods, shortcuts, and access to the user interface are determined by the options you set using the Program Neighborhood Agent Admin tool. You can allow or deny your users the ability to determine their own logon method, audio settings, shortcut placement, and display settings, depending on your company needs.

The custom options for all users running the Program Neighborhood Agent on your network are defined in a configuration file stored on your server running the new Web Interface. The client reads the configuration data from the server when a user launches the Program Neighborhood Agent, and updates at specified intervals. This allows the client to dynamically display the options you want your users to see based on the data received. The settings you configure using the Admin tool affect all users who read from this configuration file.

### The Program Neighborhood Agent Admin Tool

A default configuration file, Config.xml, is installed with default settings and is ready for use without modification in most network environments. However, you can edit the file or create multiple configuration files to suit your needs using the Program Neighborhood Agent Admin tool. This allows you to add or remove a particular option for users quickly and to easily manage and control your users' displays from a single location.

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

## Configuration Files

The default configuration file, `Config.xml`, is placed in the `\inetpub\wwwroot\Citrix\PNAgent` directory on the server running the Web Interface during the installation process. New and backup configuration files that you create using the Program Neighborhood Agent Admin tool are stored in the same folder as the default configuration file. The data configuration files serve two purposes:

- To point clients to the servers that run users' published resources
- To control the properties on users' local desktop, thereby defining what tabs and options users can customize

A configuration file controls the range of parameters that appear as options in the users's **Properties** dialog box. Users can choose from available options to set preferences for their ICA sessions, including logon mode, screen size, audio quality, and the locations of links to published resources.

You can create multiple configuration files to fill all of your organization's needs using the Program Neighborhood Agent Admin tool. After you create a configuration file and save it on the server running the new Web Interface, give your users a new server URL that points to the new file.

---

**Note** SSL/TLS-secured communications between the client and the server running the new Web Interface and smart card logon are not enabled by default. You must activate these features in the Server Settings section of the Program Neighborhood Agent Admin tool. In addition, you must enable SSL on the MetaFrame server. See "Securing the Program Neighborhood Agent with SSL/TLS" on page 130 for more information.

---

Before deploying the Program Neighborhood Agent throughout your network, you may want to test your configuration by installing a copy of the client on a single client device. You can then evaluate the default settings and determine whether or not you want to make adjustments to fit your particular network needs. Comparing between the configuration file and the client, you can monitor the effects of your changes on the client behavior.

---

---

**CAUTION** The settings in the configuration file are global; the settings affect all users connecting to that instance of the file. Changes you make to a configuration file affect all users served by it. The Program Neighborhood Agent Admin tool automatically creates a backup file (with the extension .bak) when a configuration file is loaded into the tool.

---

---

## Configuring Farm-Wide Settings

The Program Neighborhood Agent Admin tool is installed on the server running the new Web Interface. The tool allows you to define what is displayed to users running the Program Neighborhood Agent, and what they can and cannot change or customize. In addition to editing the default file (Config.xml) you can create, back up, copy, and load different configuration files.

The Program Neighborhood Agent Admin tool is divided into several sections, allowing you to control and define different aspects of the user experience. These sections are Client Tab Control, Server Settings, Logon Methods, Application Display, Application Refresh, and Session Options.

You can determine if users see any tabs in the **Properties** dialog box of the Program Neighborhood Agent, and also what options they can and cannot customize. Each tab and the settings you can customize are detailed below.

### The Properties Dialog Box

By default, users can access the **Program Neighborhood Agent Properties** dialog box from the Windows system tray. You can choose to hide or display tabs in the **Client Tab Control** section of the Program Neighborhood Agent Admin tool, including the **Server**, **Application Display**, **Application Refresh**, and **Session Options** tabs.

---

**Note** Changing these parameters directly affects the contents of the **Properties** dialog box for all users affected by the configuration file you are modifying. If you remove a tab from the client view, users cannot customize any options on that tab.

---

### Hiding and Showing Tabs of the Properties Dialog Box

The **Properties** dialog box can display up to four tabs: **Server**, **Application Display**, **Application Refresh**, and **Session Options**. Depending on your network needs, you may not want certain options to be available to users. You can modify or disable a particular option, or hide a tab altogether using the Program Neighborhood Agent Admin tool.

## Enabling and Disabling User-Customizable Options

This section contains an overview of the options you can enable and disable in the **Properties** dialog box. The instructions are presented in the order of the tabs on which each option appears.

### Server Tab Options

The **Server** tab options can be modified using the Program Neighborhood Agent Admin tool, on the options pages for **Server Settings** and **Logon Methods**.

**Server Settings.** This allows you to configure server connection and configuration refresh settings, such as redirection of users to a server running the new Web Interface using its Fully Qualified Domain Name (FQDN) or a user-provided server URL. In addition, you can define how often the client should refresh its configuration settings.

Other options allow you to define when users are redirected to a different server — at connection time or a scheduled client refresh. Enable SSL/TLS communication here as well, changing URLs to use the HTTPS protocol automatically.

**Logon Methods.** Providing a choice of multiple logon modes may be necessary in environments where multiple users use the same client device but different logon modes. This allows you to determine what logon methods are available to users, to force a default logon method, and to allow a user to save his password. The definable logon methods include Anonymous, Smart card, Smart card with pass-through authentication, user prompt, and pass through authentication.

If multiple logon methods are selected, users can choose their preferred logon method from a drop-down list. Novell Directory Services (NDS) credentials from the specified tree can be required from users who are prompted for a logon or who select pass-through authentication.

---

**Note** By default, users who are prompted for credentials can save their password. To disable this function, clear the **Allow user to save password** check box in the **Logon Methods** section of the Program Neighborhood Agent Admin tool.

---

If you do not want users to have access to any of these options, you can use the **Client Tab Control** section of the Program Neighborhood Agent Admin tool to hide the **Server** tab altogether. You can show or hide the tab at any time. For instructions about hiding and showing this tab, see “Hiding and Showing Tabs of the Properties Dialog Box” on page 44.

**Important** If you did not enable the pass-through authentication feature when you first installed the Program Neighborhood Agent, you must reinstall the client software before you can use the pass-through authentication logon mode.

---

## Application Display Tab Options

The options available on the **Application Display** tab let users place links to published resources in various locations of the client device, including the Windows desktop, the **Start** menu, the Windows system tray, and any combination thereof.

Using the **Application Display** options in the Program Neighborhood Agent Admin tool, you can define which settings users are allowed to customize. The client queries the configuration file at connection time to validate each user preference against its controlling element in the file.

If you do not want users to have access to any of these options, you can use the **Client Tab Control** section of the Program Neighborhood Agent Admin tool to hide the **Application Display** tab altogether. You can show or hide the tab at any time. For instructions about hiding and showing this tab, see “Hiding and Showing Tabs of the Properties Dialog Box” on page 44.

## Session Options Tab Options

The options available on the **Session Options** tab let users set preferences for the window size, color depth, and sound quality of ICA sessions. Using the **Session Options** section of the Program Neighborhood Agent Admin tool, you can define what settings are available to the user. Users can choose each available option from a list.

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.

Forcing the server default removes all settings for the corresponding option, other than **Default**, from the interface. The settings configured on the server running the new Web Interface apply.

If you do not want users to have access to any of these options, you can use the **Client Tab Control** section of the Program Neighborhood Agent Admin tool to hide the **Session Options** tab altogether. You can show or hide the tab at any time. For instructions about hiding and showing this tab, see “Hiding and Showing Tabs of the Properties Dialog Box” on page 44.

## Application Refresh Tab Options

The options available on the **Application Refresh** tab let users customize the rate at which the ICA Client queries the server running the new Web Interface to obtain an up-to-date list of their published resources.

The **Application Refresh** tab is hidden from the **Properties** dialog box by default. If you want to give users control over the refresh rate, you need to enable the tab first. For instructions about hiding and showing this tab, see “Hiding and Showing Tabs of the Properties Dialog Box” on page 44.

Enabling the **Application Refresh** tab makes all options on it user-customizable, unless you modify each option in the **Application Refresh** section of the Program Neighborhood Agent Admin tool.

# Customizing the ICA Win32 Program Neighborhood Agent

This section presents general information about customizing user preferences on the client device running the Program Neighborhood Agent.

## ► To customize user preferences for the Program Neighborhood Agent

1. In the Windows system tray, right-click the Program Neighborhood Agent icon and choose **Properties** from the menu that appears.
2. Select the **Session Options** tab.
3. Make the desired configuration changes.
4. Click **OK** to save your changes.

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

## Configuring the Server URL

The Program Neighborhood Agent requires the URL to a configuration file (Config.xml is the default configuration file) on the server running the new Web Interface or the NFuse Classic server. This configuration file contains the information the Program Neighborhood Agent needs so you can run remote content on your local computer.

Your system administrator may prompt you at times to change the server URL. Do not attempt to change the server URL unless you are directed to do so.

## ► To change the server URL

1. In the Windows system tray, right-click the Program Neighborhood Agent icon and choose **Properties** from the menu that appears.

2. The **Server** tab displays the currently configured URL. Click **Change** and enter the server URL as directed in the dialog box that appears. Enter the URL in the format `http://<servername>`, or `https://<servername>` to encrypt the configuration data using SSL.
3. Click **Update** to apply the change and return to the **Server** tab, or click **Cancel** to cancel the operation.
4. Click **OK** to close the **Properties** dialog box.

► **To delete memorized server URLs**

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

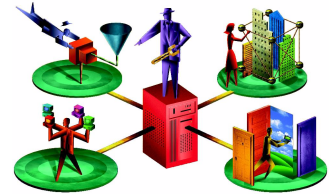
## Selecting a Logon Mode

Your installation of the Program Neighborhood Agent may offer multiple logon modes. Consult your system administrator to find out which logon mode to use.



---

# Installing and Configuring the ICA Win32 Web Client



This chapter explains how to install and configure the ICA Win32 Web Clients. The following topics are covered:

- Overview of the ICA Win32 Web Clients
- System Requirements
- Configuring the ICA Win32 Web Client for Silent User Installation
- Installing the ICA Win32 Web Client

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

## Overview of the ICA Win32 Web Clients

Use the ICA Win32 Web Client if you want users to access published resources from within their familiar Web browsers. This ICA Client requires the use of the new Web Interface for MetaFrame XP, NFuse Classic, or ALE (Application Launching and Embedding). For more information, see “Application Launching and Embedding” on page 107.

The full Web Client is available as a self-extracting executable and as a .cab file. At approximately 1.8MB in size, this package is significantly smaller than the other ICA Win32 Clients. The smaller size allows users to more quickly download and install the client software. You can configure the ICA Win32 Web Client for silent user installation.

The ICA Win32 Web Client (Minimal Installation) is a smaller version of the Web Client designed to support the core functions of MetaFrame XP for users running Internet Explorer. At approximately 1.01MB in size, this is the smallest Web Client available for use with MetaFrame XP products. Use this client when your environment requires a small download and minimal functionality, or use this client in a “locked down” environment where installing a traditional client may not be allowed by security settings.

## Features of the ICA Win32 Web Clients

The ICA Win32 Web Clients support the following features:

Feature	ICA Win32 Web Client	ICA Win32 Web Client (Minimal Installation)
User-to-user shadowing	X	
Smart card support	X	X
Content redirection	X	
Enhanced content publishing support	X	X
Roaming User Reconnect	X	
Support for SSL/TLS encryption of ICA session data	X	X
Support for the new Web Interface for MetaFrame XP, NFuse Classic, and the Web Interface Extension for MetaFrame XP	X	X
Support for the Secure Gateway for MetaFrame	X	X
Enhanced Internet proxy support	X	
Auto Client Reconnect	X	X
Novel Directory Services support	X	
Extended parameter passing	X	
Seamless windows	X	
Client device mapping	X	
Client drive mapping	X	X
Client printer mapping	X	X
Sound support	X	
TCP/IP+HTTP server location	X	X

Feature	ICA Win32 Web Client	ICA Win32 Web Client (Minimal Installation)
Wheel mouse support	X	
Multiple monitor support	X	
Panning and scaling	X	
Per-user time zone support	X	
Windows clipboard integration	X	
Low bandwidth requirements	X	X
SpeedScreen latency reduction	X	
Disk caching and data compression	X	

## System Requirements

To run the ICA Win32 Web Client, client devices must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system and Web browser.
- Windows 9x, Windows Me, Windows 2000, Windows XP, or Windows NT 3.51 or later.
- 8MB RAM or greater for Windows 9x, 16MB RAM or greater for Windows NT 3.51 or 4.0, 32MB or greater for Windows Me and Windows 2000, and 128MB RAM or greater for Windows XP.
- Internet Explorer Version 5.0 or later, or Netscape Navigator or Communicator Version 4.78, 6.2, or later.
- Microsoft mouse or 100% compatible pointing device.
- VGA or SVGA video adapter with color monitor.
- High-density 3.5-inch disk drive (optional) and available hard disk space.
- Windows-compatible sound card for sound support (optional).
- For network connections to the MetaFrame server, a network interface card (NIC) and the appropriate network transport software are required. The ICA Win32 Web Client supports the TCP/IP network transport only.

## Configuring the ICA Win32 Web Client for Silent User Installation

Installing the ICA Win32 Web Client requires minimal user interaction. A typical installation presents the user with the following:

1. An initial prompt informs the user that the Citrix ICA Win32 Web Client is about to be installed. The user clicks **Yes** to continue with Setup or **No** to stop Setup.
2. A Citrix License Agreement. The user clicks **Yes** to accept the agreement or **No** to reject the agreement. If the user clicks **No**, Setup stops.
3. An indication that Setup is copying files to the client device. By default, the ICA Win32 Web Client is installed in the Program Files\Citrix\Icaweb32 directory.
4. A message box informs the user that the Citrix ICA Web Client was installed successfully. The user must click **OK** to clear the message.
5. If the user is running Netscape Navigator, the user must restart the browser.

You can further limit user interaction with Setup by suppressing the appearance of the initial user prompt (Step 1 above) and of the Citrix License Agreement (Step 2 above). To do this, you need to extract the ICA Client files from Ica32t.exe, edit the Ctxsetup.ini file, and repackage the files for distribution. See the following section for instructions.

---

**Important** You can extract the client files from Ica32t.exe with any standard compression utility. However, you must use commercially available software to repackage the client files for distribution to your users.

---

### ► To configure the ICA Win32 Web Client for silent user installation

1. Extract the ICA Client files from Ica32t.exe using your preferred compression utility. This installer package is located in the following directory (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

2. Locate and open the Ctxsetup.ini file in any text editor.
3. To suppress the initial user prompt, locate the **InitialPrompt** parameter. Change the value of the setting from 1 to 0.
4. To suppress the Citrix License Agreement dialog box, locate the **DisplayLicenseDlg** parameter. Change the value of the setting from 1 to 0.
5. Save the file and exit the text editor.
6. Repackage the client files for distribution to your users.

## Installing the ICA Win32 Web Client

The ICA Win32 Web Client self-extracting executable, Ica32t.exe, is located in the following directory (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

If you are using the ICA Win32 Web Client with NFuse Classic, see the *NFuse Classic Administrator's Guide* for information about deploying this ICA Client with NFuse Classic.

If you are using the ICA Win32 Web Client with the new Web Interface for MetaFrame XP, see the *Web Interface for MetaFrame XP Administrator's Guide* for more information about deploying this ICA Client.

### ► To install the ICA Win32 Web Client

1. Run Ica32t.exe.
2. The initial prompt informs you that the Citrix ICA Win32 Web Client is about to be installed. Click **Yes** to continue with Setup or **No** to stop Setup.
3. The Citrix License Agreement appears. Click **Yes** to accept the agreement or **No** to reject the agreement. If you click **No**, Setup stops.
4. You are informed that Setup is copying files to the client device. The default file location for the ICA Win32 Web Client is Program Files\Citrix\icaweb32.

5. You are informed that the Citrix ICA Web Client was installed successfully. Click **OK** to clear the message.
6. If you are running Netscape Navigator, you must restart the browser.

## Installing the ICA Win32 Web Client (Minimal Installation)

The setup file for the minimal installation ICA Win32 Web client, `Wficac.cab`, is located in the following directory (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:

`Icaweb\language\ica32`

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

If you are using the ICA Win32 Web Client (Minimal Installation) with NFuse Classic, see the *NFuse Classic Administrator's Guide* for information about deploying this ICA Client with NFuse Classic.

If you are using the ICA Win32 Web Client (Minimal Installation) with the new Web Interface for MetaFrame XP, see the *Web Interface for MetaFrame XP Administrator's Guide* for more information about deploying this ICA Client.

---

► **Inserting the Win32 Web Client (Minimal Installation) in a Web page**

Add the following code to a Web page to prompt the download of the Wficac.cab file:

```
<OBJECT
    classid="clsid:238f6f83-b8b4-11cf-8771-00a024541ee3"
    data="np.ica"
    CODEBASE="http://web-server-root/some-directory/
wficac.cab"
    width='640'
    height='480'
    hspace='2'
    vspace='2'>
    <param name="Start" value="Auto">
    <param name="Border" value="On">
</OBJECT>
```

---

**Note** You will need to add the site or sites from which the .cab file is downloaded to the Trusted Sites zone.

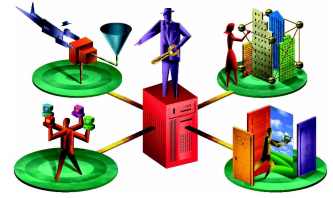
---





---

# Installing and Configuring the ICA Win32 Program Neighborhood Client



This chapter explains how to install and configure the ICA Win32 Program Neighborhood Client. The following topics are covered:

- Overview of the ICA Win32 Program Neighborhood Client
- System Requirements
- Installing the ICA Win32 Program Neighborhood Client
- Starting the ICA Win32 Program Neighborhood Client
- Configuring the ICA Win32 Program Neighborhood Client

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

## Overview of the ICA Win32 Program Neighborhood Client

Use the ICA Win32 Program Neighborhood Client if you are not using NFuse Classic or the new Web Interface for MetaFrame XP to deliver published resources. The Program Neighborhood Client has its own user interface — the Program Neighborhood window — from which users browse for application sets or create custom ICA connections to MetaFrame servers or published applications.

This ICA Client can be used with NFuse Classic, the Web Interface for MetaFrame XP, and ALE (Application Launching and Embedding); see “Application Launching and Embedding” on page 107. However, if you are planning to use NFuse Classic or the Web Interface for MetaFrame XP and have not yet deployed any ICA Clients, use the ICA Win32 Program Neighborhood Agent or the ICA Win32 Web Client.

## ICA Win32 Program Neighborhood Client Features

The ICA Win32 Program Neighborhood Client provides the following features:

- Program Neighborhood user interface
- User-to-user shadowing
- Smart card support
- Content redirection
- Roaming User Reconnect
- Support for SSL/TLS encryption of ICA session data
- Support for Citrix NFuse Classic, the new Web Interface for MetaFrame XP, and the Web Interface Extension for MetaFrame XP
- Support for the Secure Gateway for MetaFrame
- Enhanced Internet proxy support
- Auto Client Reconnect
- Published content support
- Novell Directory Services support
- DNS name resolution support
- Extended parameter passing
- TAPI support
- Seamless windows
- Client device mapping
- Sound support
- Dialing prefixes
- Windows Installer Packages
- Client Auto Update
- Windows clipboard integration

- Low bandwidth requirements
- SpeedScreen latency reduction
- Disk caching and data compression
- Business recovery
- TCP/IP+HTTP server location
- Wheel mouse support
- Multiple monitor support
- Pass-through authentication
- Panning and scaling
- Per-user time zone support

## System Requirements

To run the ICA Win32 Program Neighborhood Client, client devices must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system.
- Windows 9x, Windows Me, Windows 2000, Windows XP, or Windows NT 3.51 or later.
- 8MB RAM or greater for Windows 9x, 16MB RAM or greater for Windows NT 3.51 or 4.0, 32MB or greater for Windows Me and Windows 2000, and 128MB RAM or greater for Windows XP.
- To use the ICA Win32 Program Neighborhood Client with a Web browser, Internet Explorer Version 5.0 or later, or Netscape Navigator or Communicator Version 4.78, 6.2, or later.
- Microsoft mouse or 100% compatible pointing device.
- VGA or SVGA video adapter with color monitor.
- High-density 3.5-inch disk drive (optional) and available hard disk space.
- Windows-compatible sound card for sound support (optional).
- For serial (dial-up) connections to the MetaFrame server, an internal modem or serial port and external modem using a 16550 Universal Asynchronous Receiver/Transmitter (UART) is recommended.
- For network connections to the MetaFrame server, a network interface card (NIC) and the appropriate network transport software are required. Supported connection methods and network transports are:

- TCP/IP+HTTP
- SSL/TLS+HTTPS
- TCP/IP
- NetBIOS
- IPX
- SPX

For information about configuring the ICA Win32 Clients to use SSL or TLS to secure communications, see “Configuring and Enabling ICA Clients for SSL and TLS” on page 126.

## Installing the ICA Win32 Program Neighborhood Client

You can install the ICA Win32 Program Neighborhood Client using one of the following packages:

- Ica32.msi – a Windows Installer package for use with Windows 2000 Active Directory Services or Microsoft Systems Management Server, approximately 4.3MB in size
- Ica32.exe – a self-extracting executable, approximately 3.7MB in size

---

**Note** For a discussion of methods for deploying ICA Win32 Client software to users, see “Configuring the ICA Win32 Clients for Deployment” on page 29 of this guide, and the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.

---

## Installing the ICA Win32 Program Neighborhood Client with the Windows Installer Package

You can distribute the Program Neighborhood Client Windows Installer package (Ica32.msi) with Microsoft Systems Management Server or Windows 2000 Active Directory Services.

This package is located in the following directories (substitute *language* with the language of the ICA Client software) on the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

Icainst\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

---

**Note** To install the ICA Client software using the Windows Installer package, the Windows Installer Service must be installed on the client device. This service is present by default on Windows 2000 systems. To install ICA Clients on client devices running earlier versions of the Windows operating system, you must use the self-extracting executable or install the Windows Installer 2.0 Redistributable for Windows, available at <http://www.microsoft.com/>.

---

To uninstall an ICA Win32 Client that was installed with a Windows Installer package, run the **Add/Remove Programs** utility from the Control Panel, or run the installer package again and select the **Remove** option.

## Configuring the Windows Installer Package for Silent User Installation

You can configure the Program Neighborhood Client Windows Installer package for “silent” user installation. Windows Installer informs the user when the client software is successfully installed. The user must clear the Windows Installer message box.

► **To configure the Program Neighborhood Client Windows Installer package for silent user installation**

1. Enter the command line

```
msiexec /I <MSI_Package> /qn+ [Key=Value]...
```

where <MSI\_Package> is the name of the installer package.

2. You can set the following keys:

**INSTALLDIR**=<Installation\_Path>, where <Installation\_Path> is the path to the directory where the ICA Client software is installed. By default, the ICA Client software is installed in the Program Files\Citrix\ICA Client directory.

**CLIENT\_UPGRADE**={Yes | No}. The default value is **Yes**.

**PROGRAM\_FOLDER\_NAME**=<Start Menu Program Folder Name>, where <Start Menu Program Folder Name> is the name of the Programs folder on the Start menu containing the shortcut to the ICA Client software. The default value is **Citrix ICA Client**.

**ENABLE\_SSON**=**{Yes | No}**. The default value is **No**. If you enable the SSON property, set the **ALLOW\_REBOOT** property to **No** to avoid automatic rebooting of the client system.

**ALLOW\_REBOOT**=**{Yes | No}**. The default value is **Yes**.

**DEFAULT\_NDSCONTEXT**=**<Context1 [...]>**. Include this parameter if you want to set a default context for NDS. If you are including more than one context, place the entire value in quotation marks and separate the contexts by a comma.

Examples of correct parameters:

```
DEFAULT_NDSCONTEXT=Context1
```

```
DEFAULT_NDSCONTEXT="Context1, Context2"
```

Example of an incorrect parameter:

```
DEFAULT_NDSCONTEXT=Context1, Context2
```

**ENABLE\_DYNAMIC\_CLIENT\_NAME**=**{Yes | No}** To enable Dynamic Client Name support during silent installation, the value of the property **ENABLE\_DYNAMIC\_CLIENT\_NAME** in your installer file must be **Yes**. To disable dynamic client name support, set the property to **No**.

**CLIENT\_ALLOW\_DOWNGRADE**=**{Yes | No}** By default, this property is set to **No**. This prevents an installation of an earlier version of the client. Set to **Yes** to allow an installation of an earlier version of the client.

## Installing the ICA Win32 Program Neighborhood Client with the Self-Extracting Executable

You can distribute the self-extracting executable (*Ica32.exe*) to your users for direct installation on client devices.

This executable is located in the following directory (substitute *language* with the language of the ICA Client software) on the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

## Configuring the Self-Extracting Executable for Silent User Installation

You can configure numerous settings before you deploy the Program Neighborhood Client software to your users. This allows users to install the client and begin using it immediately, without having to configure settings.

You can customize many Program Neighborhood Client settings, including default application sets, server location, screen display resolution, and encryption level, among others. General instructions for preconfiguring the client are included below. For definitions of parameters in the client .ini files, see the *Configuration Guide for the ICA Win32 Clients* on the Citrix Web site at <http://www.citrix.com/support>; select **Product Documentation**.

---

**Important** When the ICA Win32 Program Neighborhood Client is installed on a client device, several of the .ini files you can modify are copied to the user's profile directory. If you modify settings for a new version of the ICA Win32 Program Neighborhood Client prior to updating with the Client Auto Update feature, your changes are not migrated to the .ini files under the user's profile directory.

---

### ► To configure the self-extracting executable for silent user installation

1. Obtain a copy of the ICA Client installer file (Ica32.exe). This file is located in the following directory (substitute *language* with the language of the ICA Client software) on the Components CD included in your MetaFrame XP media pack:

Icaweb\*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

2. Extract the contents of the installer file to a new folder, A.

---

**Note** You can use any standard compression utility to extract the contents of the installer file. However, you must use commercially available software to repackage the contents for distribution to users.

---

3. Install the ICA Client using the same installer file you used in Step 2.

4. Start the client and customize the client settings, as desired, from the client user interface.
5. When you are done, open the %User Profile%\Application Data\ICAClient folder and copy all files with an .ini extension to a new folder, B.
6. In folder B, replace all .ini file extensions with .src (source) extensions.
7. Copy the contents of folder B to folder A, overwriting the existing .src files in folder A with their modified equivalents from folder B. The contents of folder A now represent your custom installer set of .ini files.
8. Repackage the contents of folder A for distribution to users.

► **To install the Program Neighborhood Client with the self-extracting executable**

1. Make sure the client device is properly configured and cabled. Make sure any previous installations of the Citrix ICA Client (including the Program Neighborhood Connection Center, whose icon appears in the Windows system tray when active) are not running.
2. If you are installing from disks:

Insert ICA Win32 Client Setup disk number 1 in drive A (or other appropriate drive) of the client device. For Windows 9x, Windows Me, Windows 2000, and Windows NT 4.0 client devices, click **Start > Run a:\setup**. For Windows NT 3.5x client devices, on the **File** pull-down menu of Program Manager run **a:\setup**.

For information about creating ICA Client installation disks, see “Creating ICA Client Installation Disks” on page 31.

If you are installing from a MetaFrame server:

Run **Setup.exe**, located in the following directory on your MetaFrame server:

%SystemRoot%\System32\Clients\Ica\Ica32\Disks\Disk1



If you are installing the client from the Components CD included in your MetaFrame XP media pack:

Run **Ica32.exe**, located in the following directory (substitute *language* with the language of your ICA Client software):

Icaweb\*language*\ica32

where *language* is one of:

En (English)

Fr (French)

De (German)

Ja (Japanese)

Es (Spanish)

3. The **Welcome** screens appear. Read the information on these screens and click **Next**.
4. The Citrix License Agreement appears. Read the license agreement and click **Yes** if you agree to the terms of the agreement.  
Setup searches your client device for previously installed versions of the ICA Win32 Program Neighborhood Client.
5. If Setup does not detect a previous installation of the ICA Win32 Program Neighborhood Client, go to Step 6.  
If Setup detects a previous installation of the ICA Win32 Program Neighborhood Client, the **Choose Installation Type** dialog box appears. The **Choose Installation Type** dialog box lets you choose to upgrade the existing client or to create a new installation of the Program Neighborhood Client. The default value is **Upgrade the existing client**. Click **Next**.
6. The **Choose Destination Location** dialog box appears. You can change the displayed path if desired by clicking **Browse**. Click **Next** to accept the displayed path and continue installation.
7. The **Select Program Folder** dialog box appears. You can choose to use the default Citrix ICA Client folder, specify the name of a new program folder, or add the ICA Win32 Client icons to an existing folder. The program folder you specify is created if it does not already exist. Click **Next** to continue.
8. The **ICA Client Name** dialog box appears. By default, the machine name is used as the client name. You can specify a unique client name for your client device by unchecking the **Use machine name as client name** box. MetaFrame servers use the client name to manage client printers and other system resources. If you do not assign a unique machine name to each client device, device mapping and application publishing may not operate correctly.  
Click **Next** to continue.

9. The **Select Desired Features** screen appears. Select **Yes** if you want the Program Neighborhood Client to access your local Windows user name, password, and domain information. If you select **Yes**, you are not prompted to log on to the Program Neighborhood Client separately.  
When you are done, click **Next** to continue. A progress window appears, displaying the file names as they are copied to your hard drive.
10. If you are installing from a floppy disk, go to Step 11.  
If you are not installing from a floppy disk, a dialog box informs you that the Program Neighborhood Client was successfully installed on the computer. Click **Finish**.
11. If you are installing from a floppy disk, the **Setup Needs the Next Disk** dialog box appears. Remove the first ICA Win32 Client disk from drive A (or other appropriate drive) and insert the second disk. Click **OK**.
12. When the Citrix ICA Client finishes copying the program files, the **Information** dialog box appears. Click **OK** to exit this window.  
The Citrix ICA Client program group appears on the desktop.

## Starting the ICA Win32 Program Neighborhood Client

- ▶ **To start the Program Neighborhood Client**
  1. Double-click the Program Neighborhood Client icon on the desktop to open the **Program Neighborhood** window. If you specified a default application set for this user, this window contains all the resources the user can run. If no default is specified, a list of application sets appears.
  2. Double-click the application set to access. A logon dialog box appears.
  3. Enter a valid user name, domain, and password.

---

## Configuring the ICA Win32 Program Neighborhood Client

This section explains how to configure the Program Neighborhood Client using the Program Neighborhood user interface.

### Configuring Network Protocol and Server Location

With the Citrix ICA Win32 Program Neighborhood Client, users can connect to a MetaFrame server in the following ways:

- Establishing a custom ICA connection by dialing into a MetaFrame server using a modem installed on the client device. This method uses a serial connection to a MetaFrame server.
- Establishing a custom ICA connection over a direct serial cable. This method uses a serial connection to a MetaFrame server.
- Over the local or wide-area network connection between the client device and the MetaFrame server. This method uses one of the following network protocols:
  - TCP/IP+HTTP
  - SSL/TLS+HTTPS
  - TCP/IP
  - IPX
  - SPX
  - NetBIOS

---

**Note** Remote users can connect to MetaFrame XP servers running Windows Server 2003 over TCP/IP only. Terminal Services in Windows Server 2003 does not support remote connections over IPX/SPX, NetBIOS, and asynchronous transports.

---

You can also use Microsoft's Remote Access Service (RAS) or Dial-Up Networking (DUN) in combination with the Citrix ICA Client to connect to a MetaFrame server. For this type of connection, the client device must meet the following requirements in addition to those specified at the beginning of this chapter:

- The RAS or DUN client software must be installed on the client device
- The RAS server or third-party PPP server must be located on the same network as the MetaFrame server

## Specifying the Network Protocol for ICA Browsing

The network protocol setting allows you to control the way the ICA Client searches for MetaFrame servers and how it communicates with them.

This section discusses the TCP/IP+HTTP, SSL/TLS+HTTPS, and TCP/IP protocols and their implementation in a MetaFrame server farm. For additional information about configuring MetaFrame XP server farms for ICA browsing, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.

### Using TCP/IP+HTTP Network Protocol for ICA Browsing

If you select **TCP/IP+HTTP** as the network protocol from the Program Neighborhood Client's **Settings** dialog box, the ICA Client uses the HTTP protocol to search for MetaFrame servers. Select this protocol when using the ICA Client over the Internet or through a firewall or proxy server. Select **SSL/TLS+HTTPS** to use SSL/TLS-secured communications.

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

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

If you select **TCP/IP+HTTP** as the network protocol, specify servers to contact for ICA browsing by entering IP addresses or DNS names of MetaFrame servers in the **Address List** box in the Program Neighborhood Client.

If you select **TCP/IP+HTTP** as the network protocol and specify MetaFrame servers in the **Address List** box, the ICA Client communicates with the Citrix XML Service on a specified server for ICA browsing.

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

If you select **TCP/IP+HTTP** as the network protocol, auto-locate does not use a broadcast to determine the nearest farm server, but rather attempts to resolve the host name “ica” to a MetaFrame server. Therefore, if you want auto-locate functionality, the TCP/IP+HTTP protocol does not increase network traffic with ICA Client broadcasts.

---

**Tip** You can configure the ICA Clients’ DNS server to use round-robin DNS to map the name “ica” to a set of servers that can service the XML requests. Use this approach to avoid individually configuring server location addresses on ICA Clients.

---

To locate an XML Service, the ICA Client makes an HTTP connection to port 80 on the MetaFrame server. If the user is launching a published application, for example, the XML Service then sends to the client the address of a MetaFrame server that has the application published.

If you select **TCP/IP+HTTP** as the network protocol, communication between the client and XML Service consists of XML-formatted data in HTTP packets.

### **Communicating with the Citrix XML Service**

Citrix XML Service is installed by default on all MetaFrame XP servers. It is also installed with Feature Release 1 for MetaFrame 1.8.

If you select **TCP/IP+HTTP** as the network protocol, the XML Service communicates published application information to clients using HTTP protocol and XML data. The XML Service also communicates published application information to NFuse Classic servers and servers running the Web Interface for MetaFrame XP.

For example, when a user launches a published application from the Program Neighborhood Client, the client sends a request for the application. The XML Service responds with the address of a MetaFrame server on which the application is published.

With NFuse Classic or the Web Interface, for example, a user connects to a Web page using a Web browser. The XML Service provides a list of available applications to the NFuse Classic server or server running the Web Interface for MetaFrame XP. The server then displays the available applications on the user’s personalized application Web page.

## Using SSL/TLS+HTTPS Network Protocol for ICA Browsing

If you select **SSL/TLS+HTTPS** as the network protocol, the client uses the HTTPS protocol to search for a list of MetaFrame servers. The client communicates with the MetaFrame server using ICA with SSL/TLS. SSL/TLS+HTTPS provides strong encryption of ICA traffic and MetaFrame server authentication. Select this option when using the ICA Client over the Internet or through a firewall or proxy server.

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

---

**Note** The TCP/IP+HTTP and SSL/TLS+HTTPS protocols can be used only with compatible MetaFrame servers. See the *MetaFrame XP Server Administrator's Guide* for Windows or UNIX for information about configuring the MetaFrame server to use SSL/TLS.

---

## Using TCP/IP Network Protocol for ICA Browsing

If you select **TCP/IP** as the network protocol and **(Auto-Locate)** appears in the **Address List** box of the **Settings** dialog box, ICA Clients send UDP broadcasts to the ICA browser service on port 1604 to locate MetaFrame servers and published applications. Select this option if all of the MetaFrame servers and clients are located on the same network.

By default, MetaFrame XP server farms operating in native mode do not respond to ICA Clients that use UDP broadcasts for ICA browsing. Therefore, if clients are configured to use TCP/IP and to auto-locate servers, they will fail to locate MetaFrame XP servers or published applications in the server farm.

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

Because of broadcast limitations, you might prefer to enter one or more IP addresses or DNS names of MetaFrame servers in the **Address List** box in the Program Neighborhood Client. You must do this if the ICA Client is not on the same subnet as a data collector.

## Configuring Connections to MetaFrame Servers and Published Applications

This section describes how to configure connections to MetaFrame servers and published applications. The Program Neighborhood Client offers two connection methods:

- Connecting to MetaFrame servers and published applications using application sets
- Connecting to MetaFrame servers and published applications using custom ICA connections

## Configuring TCP/IP+HTTP Server Location

You can retrieve MetaFrame server and published application information across a firewall that does not allow UDP broadcasts by selecting **TCP/IP+HTTP** or **SSL/TLS+HTTPS** server location. The ICA Win32 Program Neighborhood Client uses TCP/IP+HTTP as the default network protocol.

### ► To configure TCP/IP+HTTP server location

1. From the **Network Protocol** drop-down list, select **TCP/IP+HTTP**.
2. Click **Add** to display the **Add Server Location Address** dialog box.
3. Enter the name or IP address of a MetaFrame server and a recognized port number (the default is port 80) and click **OK**.

---

**Note** If you do not enter an IP address, you must have a MetaFrame server on your network mapped to the default name of “ica.” TCP/IP+HTTP server location does not support the [**Auto-Locate**] function.

---

4. The specified server responds with a list of all servers and published resources in its server farm.

---

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

---

## Configuring SSL/TLS+HTTPS Server Location

If you configured your MetaFrame servers to accept SSL/TLS-secured connections, you can enable SSL/TLS on the Program Neighborhood Client.

### ► To configure SSL/TLS+HTTPS server location

1. From the **Network Protocol** drop-down list, select **SSL/TLS+HTTPS**.
2. Click **Add** to display the **Add Server Location Address** dialog box.

3. Enter the fully qualified domain name of the MetaFrame server with the digital server certificate and verify that port 443 is listed as the default port.
4. Click **OK**.

---

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

---

For more information about configuring connections, see “Configuring Connection Properties” on page 74. For more information about using SSL to secure client to server communication, see “Configuring and Enabling ICA Clients for SSL and TLS” on page 126.

## Configuring Server Location and Business Recovery

Server location (also called *server browsing*) provides a method for a user at a network-connected ICA Client to view a list of all MetaFrame servers on the network that have ICA connections configured for that network protocol, and a list of all published applications. You can specify a separate server location for each network protocol.

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

1. The ICA Client broadcasts a “Get Nearest MetaFrame server” packet. The first MetaFrame server to respond returns the address of the master ICA browser, which is used in the next step.
2. The ICA Client sends a request for the server and published application lists to the master ICA browser.
3. The master ICA browser responds with a list of all MetaFrame servers on the network and a list of all published applications.

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



*Business recovery* provides consistent connections to published applications in the event of a master ICA browser server disruption. You can define up to three groups of MetaFrame 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 server group for your client, the client attempts to contact all the servers within that group simultaneously and the first server to respond is the one to which you connect. The client broadcasts only if you select (**Auto-locate**) from the address list.

## Using Application Sets and Custom ICA Connections

An *application set* is a user's view of the resources published on a given server farm that the user is authorized to access. Applications published in an application set are preconfigured for such session properties as window size, number of colors, supported encryption levels, and audio compression rate. If these settings are not required to run the published application (such as, for example, the audio compression rate), you can change them on the client device at the application set level.

---

**Important** Application set functionality is not available for applications published on servers running MetaFrame Server for UNIX Operating Systems. To connect to an application published on these servers, you must use a custom ICA connection.

---

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

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

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

## Adding Application Sets and Custom ICA Connections

To locate additional application sets you can access, or to add a custom ICA connection, use the Find New Application Set or the Add New ICA Connection wizards, respectively.

▶ **To find a new application set**

1. Double-click the Find New Application Set icon in the Program Neighborhood window.
2. Follow the instructions in the Find New Application Set wizard.

▶ **To add a custom ICA connection**

1. Double-click the Custom ICA Connections icon. The **Custom ICA Connections** window opens.
2. Double-click the Add ICA Connection icon.
3. Follow the instructions in the Add New ICA Connection wizard.

For details about the settings in the Find New Application Set and Add New ICA Connection wizards, see the wizards' application help.

## Configuring Application Sets and Custom ICA Connections

The following procedures describe how to configure the properties and settings of application sets and custom ICA connections:

- Configuring connection properties
- Configuring default options
- Configuring a logon mode
- Configuring general settings
- Configuring bitmap caching
- Configuring hotkeys
- Configuring event logging

## Configuring Connection Properties

▶ **To configure connection properties**

1. Start the Program Neighborhood Client.
2. If you are configuring an application set:  
Select the application set and click **Settings** on the Program Neighborhood Client toolbar.

If you are configuring a custom ICA connection:

Select the custom ICA connection you want to configure and click the **Properties** button in the Program Neighborhood Client toolbar to display the **Properties** dialog box.

3. Click the **Connection** tab to display the **Connection** page.

From the **Connection** page, you can configure the following:

**Connection Type.** Choose a connection type. Select **Local Area Network** to connect to the MetaFrame server over a local network that covers a confined geographical area (such as an office building or complex). Select **Wide Area Network** to connect to the MetaFrame server over a network that covers a wide geographical area.

If you are configuring a custom ICA connection, you can select either **Server** or **Published Application**. When you select **Server**, this field specifies the MetaFrame server to run the published application.

For more information about the options on this tab, click **Help**.

## Configuring Default Options

### ► To configure default options

1. Start the Program Neighborhood Client.
2. If you are configuring an application set:  
Select the application set and click **Settings** in the Program Neighborhood Client toolbar.  
If you are configuring a custom ICA connection:  
Right-click in the custom ICA connection window and select **Custom Connections Settings**.
3. Click the **Default Options** tab to display the **Default Options** page. For custom ICA connections: Any options configured in this dialog box are applied to *all* custom ICA connections. To override these default options on an individual custom ICA connection, select the ICA connection and click **Properties** on the Program Neighborhood Client toolbar. Select the **Options** tab.
4. From the **Options** and **Default Options** pages, you can configure the following:  
**Use data compression.** Data compression reduces the amount of data that needs to be transferred but requires additional processor resources to compress and decompress the data. If your connection is bandwidth-limited, enabling data compression increases performance.  
**Use disk cache for bitmaps.** Bitmap caching to disk stores commonly-used graphical objects such as bitmaps in a local cache on the client's hard disk space. If your connection is bandwidth-limited, enabling disk caching increases performance. If your client is on a high-speed LAN, you do not need disk caching. Dial-in connections have disk caching enabled by default.

**Queue mouse movements and keystrokes.** Queuing causes the client to send mouse and keyboard updates less frequently to the MetaFrame server. Select this option to reduce the number of network packets sent from the ICA Client to the MetaFrame server. If you do not select this option, the session is more responsive to keyboard and mouse movements. Selecting this option improves performance if you dial in to RAS and then use a network to connect.

**Turn off desktop integration for this application set.** You can configure the Program Neighborhood Client to create desktop shortcuts and add items to the **Start** menu for published applications. If users do not want published applications sent directly to the desktop, they must select this check box.

**Enable sound.** Select this check box to enable sound support. The client device must have a compatible sound card installed. Published applications can then play sounds on the client.

Select one of the following values for **Quality**:

- **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.
- **Medium.** This setting is recommended for most LAN-based connections. This setting causes any sounds 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 will decrease compared with the uncompressed version due to the reduction in the amount of data being sent across the wire.
- **Low.** This setting is recommended for low-bandwidth connections, including most modem connections. This setting causes any sounds 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.

**Encryption Level.** Select the level of encryption for the ICA connection. The default level is **Basic**. Select **128-bit for Login Only** to use encryption during authentication.

The MetaFrame server must be configured to allow the selected encryption level or greater. To enable encryption levels higher than **Basic**, the MetaFrame server must support RC5 encryption. This support is included with SecureICA Services, MetaFrame 1.8 Feature Release 1, and MetaFrame XP.

---

**Note** Selecting an encryption level higher than **Basic** disables automatic logon to the MetaFrame server.

---

**SpeedScreen latency reduction.** SpeedScreen latency reduction is a collective term used to describe the functionality that helps enhance user experience on slower network connections. Latency reduction is available only if you are connecting to a server that is configured and licensed for latency reduction.

For slower connections (for example, if you are connecting over a WAN or a dial-up connection), select **On** to decrease the delay between user input and screen display. Choose either **Mouse Click Feedback** or **Local Text Echo**.

For faster connections (for example, if you are connecting over a LAN), select **Off**.

If you are not certain of the connection speed, set mode to **Auto** to turn latency reduction on or off depending on the speed of the connection. You can override Auto mode using the **Toggle Latency Reduction** hotkey.

**Window Properties.** Specify the number of colors displayed in the application's window in the **Windows Colors** field.

**Use Server Default** (for application sets). To use the server-configured default settings for the properties, make sure this check box is selected. To change the settings, clear this check box and choose new settings.

**Use Custom Default** (for custom ICA connections). To override the default options, clear this check box.

Specify the window size in which a published application runs in the **Window Size** field.

If you are connecting to a published application, you can select **Seamless Windows** to run the application on your local desktop in a separate, seamless window.

## Configuring a Logon Mode

### ► To configure a logon mode for application sets and custom ICA connections

1. Start the Program Neighborhood Client.
2. If you are configuring an application set:

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

If you are configuring a custom ICA connection:

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

3. On the **Logon Information** tab, select the logon mode you want to configure for this client:
  - **Local user** prompts users for authentication when they establish a connection.  
**Local user/pass-through authentication** enables pass-through authentication based on the user's Windows desktop credentials.
  - **Smart card** authenticates users based on a smart card and Personal Identification Number (PIN).  
**Smart card/pass-through authentication** enables pass-through authentication based on the smart card and the smart card PIN. This logon mode requires a smart card to be present or inserted in the smart card reader at logon time.
  - **User-specified credentials** authenticates users based on credentials (user name, password, and domain information) to be specified here.  
**User-specified credentials/save password.** This check box is selected by default. Clear the check box if you do not want users to save their passwords in clear text. For instructions about removing the check box from the interface altogether, see "Preventing Users from Saving Passwords" on page 80.

---

**Note** To connect to a MetaFrame server or published application that is configured to use Novell Netware Directory Services (NDS), enter the user's NDS distinguished name in the **User Name** field and the password in the **Password** field. Leave the **Domain** field blank.

---

4. Click **OK**.

## Reducing the Number of Required Logons

By default, users are required to enter their credentials each time they launch a published application or connect to a MetaFrame server desktop. You can configure the Program Neighborhood Client to reduce the number of times users have to enter credentials using one of the following methods:

- Enabling pass-through authentication
- Caching credentials with application set information

You can enable pass-through authentication to pass the user's local Windows desktop credentials to the MetaFrame server. This eliminates the need for multiple authentications.

If you enable pass-through authentication, all existing application sets are automatically configured to use pass-through authentication. However, existing custom ICA connections are automatically configured not to use pass-through authentication. You must, therefore, enable pass-through authentication for each custom ICA connection for which you want to use this logon mode.

## Enabling Pass-Through Authentication

To enable pass-through authentication, you must complete the following tasks:

- Enable the feature at the machine level
- Enable the feature at the user level

### ▶ To enable pass-through authentication at the machine level

1. Log on as an administrator.
2. Start the Program Neighborhood Client.
3. Go to **Tools > ICA Settings**.
4. Click the **General** tab and select the **Pass-Through Authentication** check box.
5. Click **OK**.

When this feature is turned on at the machine level, each user can enable it at the user level in the following manner.

### ▶ To enable pass-through authentication at the user level

1. Log on as a user.
2. Start the Program Neighborhood Client.
3. Go to **Tools > ICA Settings**.
4. Click the **General** tab and select the **Use local credentials to log on** check box.
5. Click **OK**.

Enabling pass-through authentication at the user level makes this the default configuration for all existing and new application sets. Follow the instructions below for enabling new and existing custom ICA connections to use this feature.

### ▶ To enable pass-through authentication for new custom ICA connections

When creating a new custom ICA connection, enable pass-through authentication by selecting **Use local User name and Password** in the Add ICA Connection wizard.

If you want to prevent users from caching their passwords in clear text, see “Preventing Users from Saving Passwords” on page 80.

- ▶ **To enable pass-through authentication for existing custom ICA connections**
  1. Start the Program Neighborhood Client.
  2. Select a custom ICA connection for which you want to enable pass-through authentication.
  3. On the Program Neighborhood Client toolbar, click the **Properties** button.
  4. Click the **Logon Information** tab.
  5. Select **Local user** to authenticate using the local Windows desktop credentials; select **Pass-through authentication** to enable pass-through authentication based on the same local Windows desktop credentials.

-Or-

Select **Smart card** to authenticate using a smart card and Personal Identification Number (PIN); select **Pass-through authentication** to enable pass-through authentication based on the smart card and the smart card PIN.

-Or-

Select **User-specified credentials** to authenticate using credentials other than local user or smart card credentials.

The **Save password** check box is selected by default. Clear the **Save password** check box if you do not want to save the password in clear text.

  6. Click **OK**.
  7. Repeat Steps 1 through 6 for each ICA connection for which you want to enable pass-through authentication.

## Preventing Users from Saving Passwords

You can remove the **Save Password** check box from an application set's logon screen and from the **Logon Information** tab of the **Settings** dialog box. Removing the check box prevents users from saving their passwords for application sets. You can prevent users from saving their passwords for all application sets or specific application sets.

Use the following table to determine which files you need to edit, then follow the instructions below.

To disable password saving for all application sets	To disable password saving for particular application sets
%User Profile%\Application Data\ICAClient\Appsrv.ini	%User Profile%\Application Data\ICAClient\Pn.ini



► **To prevent users from saving their passwords for *all* application sets**

1. Exit the Program Neighborhood Client if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section named **[WFClient]**.
4. Add the following line to the list of parameters and values in the **[WFClient]** section:  
**NoSavePwordOption=On**  
If the parameter already exists, make sure its value is set to **On**.
5. Save the file and exit the text editor.
6. Repeat Steps 1 through 5 for additional users.
7. Start the Program Neighborhood Client.

Adding this parameter and setting it to **On** prevents users from saving passwords for any application set. Any existing cached passwords are deleted.

► **To prevent users from saving their passwords for *particular* application sets**

1. Exit the Program Neighborhood Client if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Pn.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section name that corresponds to the application set for which you want to disable password saving; for example, [MyAppSet].
4. Add the following line to the list of parameters and values in that section:  
**NoSavePwordOption=On**  
If the parameter already exists, make sure its value is set to **On**.
5. Add the parameter and value to each application set section as desired.
6. Save the file and exit the text editor.
7. Repeat Steps 1 through 6 for additional users.
8. Start the Program Neighborhood Client.

Adding this parameter and setting it to **On** prevents users from saving passwords for the specified application set or sets. Any existing cached passwords are deleted.

## Configuring General Settings

### ► To configure the general settings

1. Start the Program Neighborhood Client.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **General** tab.

From the **General** page, you can configure the following settings:

- **Client Name.** This field allows you to change the name of the client device. The MetaFrame server uses the client name to uniquely identify resources (such as mapped printers and disk drives) associated with a given client device. The client name must be unique for each device running the Citrix ICA Client.
- **Serial Number.** This is the serial number of the ICA Client software. This field is necessary only when you are using the Citrix ICA Client with a Citrix Terminal product such as *WINFRAME* for Terminals and MetaFrame for Terminals, which require each client to have a Citrix *PC Client Pack* serial number to connect to the server. If a serial number is required, you must enter it exactly as it appears on the Serial Number card.
- **Keyboard Layout.** Allows you to specify the keyboard layout of your client device. The MetaFrame server uses the keyboard layout information to configure the user session for your keyboard layout. The default value of (**User Profile**) uses the keyboard layout specified in your user profile.
- **Keyboard Type.** Allows you to specify the keyboard type of your client device. The MetaFrame server uses the keyboard type information to configure your user session for your keyboard type. Use the default value of **Default** for most English and European keyboards. When used with a Japanese keyboard, **Default** auto-detects the keyboard type.
- **Display Connect To screen when making Dial-in Connections.** Select this check box to display the **Connect To** screen when you make a dial-in connection.
- **Display terminal window when making Dial-in Connections.** Select this check box if your dial-in configuration includes third-party products, such as security devices and X.25 PADs, that require an ASCII dialog before connecting to the MetaFrame server.

- **Allow automatic client updates.** Select this check box to allow the MetaFrame server to update your Citrix ICA Client software when newer versions become available. When the MetaFrame server detects an outdated client version, it notifies you that a newer version is available and replaces the ICA Client files.
- **Pass-Through Authentication.** If you are logged on as an administrator of the client device, select this option to enable pass-through authentication at the machine level. Each user must turn this feature on by selecting **Use local credentials to log on** described below. See “Enabling Pass-Through Authentication” on page 79 for more information.
- **Use local credentials to log on.** Select this check box to enable pass-through authentication at the user level. Pass-through authentication must also be enabled at the machine level. See “Enabling Pass-Through Authentication” on page 79 for more information.

## Configuring Bitmap Caching

### ► To configure bitmap caching

1. Start the Program Neighborhood Client.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Bitmap Cache** tab.

From the **Bitmap Cache** page, you can configure the following settings:

- **Bitmap Cache Size.** Specify the size of the bitmap cache in kilobytes.
- **Bitmap cache directory.** The default directory where the cached data is stored is displayed in this field.
- **Change Directory.** If you want to specify a new directory for cached data, click the **Change Directory** button.
- **Minimum size bitmap to be cached.** The size of the smallest bitmap to be cached to disk.
- **Clear cache Now.** Click this button to remove all cached data from the directory.

---

**Tip** Do not clear the cache if any ICA connections are open. Before clearing the cache, verify that all ICA connections are closed.

---

4. Click **OK** to close the dialog box.

## Configuring Hotkeys

► **To configure the hotkeys**

1. Start the Program Neighborhood Client.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Hotkeys** tab.
4. For each hotkey in the list, select a shift state and a key.
5. You can disable the hotkey by selecting **(none)** for the key.

Hotkeys are used to control the behavior of the Program Neighborhood Client, and as substitutes for the standard Windows hotkeys for a published application.

The fields on the **Hotkeys** page are:

- **Task List.** The Task List hotkey displays the local **Start** menu (**Windows Task List** on Windows NT 3.51.)
- **Close Remote Application.** The Close Remote Application hotkey disconnects the published application from the MetaFrame server and closes the Citrix ICA Client window. The behavior of this hotkey is the same as choosing **Close** from the system menu of the ICA Client window.  
Closing the published application in this manner either leaves the associated application in a disconnected state on the MetaFrame server or exits the application on the MetaFrame server, depending on how the server is configured.
- **Toggle Title Bar.** This hotkey causes the ICA Client window to alternately display and hide its title bar. When the title bar is displayed, the ICA Client window can be moved or closed.

---

**Note** This hotkey must be used to return to a seamless window after accessing the Windows NT Security dialog box using the **CTRL+ALT+DEL** hotkey.

---

- **CTRL-ALT-DEL.** This hotkey causes the CTRL-ALT-DEL key sequence to be sent to the server that is running the published resource. In Windows NT, the CTRL-ALT-DEL key sequence causes a Windows NT session to switch to the Windows NT Security desktop.
- **CTRL-ESC.** This hotkey causes the CTRL-ESC key sequence to be sent to the server that is running the published application. CTRL-ESC is a standard Windows hotkey. See your Windows documentation for more information about the CTRL-ESC hotkey.

- **ALT-ESC.** This hotkey causes the ALT-ESC key sequence to be sent to the server that is running the published application. ALT-ESC is a standard Windows hotkey. See your Windows documentation for more information about the ALT-ESC hotkey.
- **ALT-TAB.** This hotkey causes the ALT-TAB key sequence to be sent to the server that is running the published application. ALT-TAB is a standard Windows hotkey. See your Windows documentation for more information about the ALT-TAB hotkey.
- **ALT-BACKTAB.** This hotkey causes the ALT-SHIFT-TAB key sequence to be sent to the server that is running the published application. ALT-SHIFT-TAB is a standard Windows hotkey. See your Windows documentation for more information about the ALT-SHIFT-TAB hotkey.
- **CTRL-SHIFT-ESC.** This hotkey causes the CTRL-SHIFT-ESC key sequence to be sent to the server that is running the published application. CTRL-SHIFT-ESC is a standard Windows NT hotkey. See your Windows NT documentation for more information about the CTRL-SHIFT-ESC hotkey.
- **Toggle Latency Reduction.** This hotkey turns SpeedScreen Latency Reduction on or off. Latency reduction reduces the time between your keyboard or mouse input and a visible response on the screen. If a published resource on the MetaFrame XP server is configured to use latency reduction, the ICA Client also uses latency reduction by default. If the latency reduction feature causes problems when running the application, you can turn it off using this hotkey.

## Configuring Event Logging

Use the **Event Logging** page to instruct the Citrix ICA Client whether or not to keep a log of various events that occur while running published applications.

### ► To configure event logging

1. Start the Program Neighborhood Client.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Event Logging** tab.

From the **Event Logging** page, you can configure the following settings:

**Event Log File.** In the **Name** field, enter the name and directory path of the file in which to log Citrix ICA Client events.

- Select **Overwrite existing event log** to cause the event log file to be overwritten with new events when a published application is run.
- Select **Append to existing event log** to keep old events and add new ones to the end of the file.

**Log Events.** Select the event categories that you want to log from the types listed below. If no events are selected, no logging takes place.

- **Connections and Disconnections.** Logs an event whenever the Citrix ICA Client connects and disconnects from a MetaFrame server. This category is selected by default.
- **Errors.** Logs an event whenever an error is encountered by the Citrix ICA Client. This category is selected by default.
- **Data Transmitted.** Logs an event for each packet of information sent by the Citrix ICA Client to the MetaFrame server. This is intended primarily for technical support purposes.
- **Data Received.** Logs an event for each packet of information received by the Citrix ICA Client from the MetaFrame server. This category is intended primarily for technical support purposes.
- **Keyboard and Mouse Data.** Logs an event whenever you press a key on the keyboard or move the mouse. This category is intended for technical support purposes.

## Improving ICA Performance Over Low-Bandwidth Connections

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

- **Change your ICA Client configuration.** Changing your client configuration can reduce the bandwidth that ICA requires, and improve performance.
- **Change the way you use the client.** Changing the way you use the client can also reduce the bandwidth required for a high-performance connection.
- **Use the latest MetaFrame server and ICA Clients.** Citrix continually enhances and improves ICA performance with each release. Many performance features require the latest client and server software to function.

## Changing Your ICA Client Configuration

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

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

## Changing the Way You Use the Client

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

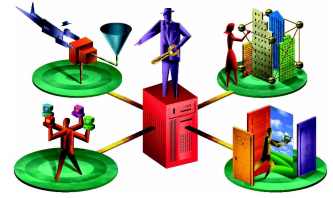
- **Accessing large files using client drive mapping.** When you access a large file with client drive mapping, the file is transferred over the ICA connection. On slow connections, this may take a long time.
- **Printing large documents on local client printers.** When you print a document on a local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





---

# Configuring Features Common to the ICA Win32 Clients



This chapter explains how to configure and use features common to the ICA Win32 Clients. The following topics are covered:

- Configuring New Features of Version 7.0 of the ICA Win32 Clients
- Configuring Existing Features Common to the ICA Win32 Clients
- Using Applications Published on MetaFrame Servers for UNIX Operating Systems

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

## Configuring New Features of Version 7.0 of the ICA Win32 Clients

Configure the following new features in the same manner for all of the ICA Win32 Clients.

### Dynamic Client Name Support

Dynamic client name support allows the client name to be the same as the machine name. When users change their machine name, the client name changes to match. This allows you to name machines to suit your naming scheme and find connections more easily when managing your MetaFrame XP server farm.

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

#### Configuring Dynamic Client Name Support During Installation

Enable dynamic client name support by selecting the check box **Enable Dynamic Client Name** during client installation. Doing so sets the client name the same as the machine name.

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

## SpeedScreen Browser Acceleration

This function, available to users running Internet Explorer 5.5 or later, enhances the speed at which images are downloaded and displayed. To enable SpeedScreen browser acceleration, set **SpeedBrowse** to **ON** or (**OFF** to disable it) in your .ica file.

If SpeedScreen browser acceleration is enabled on the client, but not the server, SpeedScreen browser acceleration is disabled.

## Windows NT Challenge/Response (NTLM) Support

Version 7.0 of the ICA Win32 Clients provides support for networks using Windows NT Challenge/Response (NTLM) for security and authentication. NTLM authentication is supported by default on machines running Windows NT, Windows 2000, and Windows XP.

On client devices running Windows 95, Windows 98, and Windows Me, manually enable the **User Control Package** to use NTLM authentication. Change this by going to **Control Panel > Network > Access Control**. On the **Access Control** screen, select **User-level access control**. If the User Control Package is not enabled, the client uses basic authentication, not NTLM authentication.

## Certificate Revocation List Checking

When certificate revocation list checking is enabled, the ICA Win32 Clients check whether or not the server's certificate has been revoked. This feature improves the cryptographic authentication of the MetaFrame XP server and improves the overall security of the SSL/TLS connections between an ICA Win32 Client and a MetaFrame XP server.

You can enable several levels of certificate revocation list checking. For example, you can configure the client to check only its local certificate list, or to check the local and network certificate lists. In addition, you can configure certificate checking to allow users to log on only if all Certificate Revocation Lists are verified.

► **To enable certificate revocation list checking**

In the `Template.ica` file, configure the `SSLCertificateRevocationCheckPolicy` setting to one of the following options:

- **NoCheck** - No certificate revocation list checking is performed
- **CheckWithNoNetworkAccess** - The local list is checked
- **FullAccessCheck** - The local list and any network lists are checked
- **FullAccessCheckAndCRLRequired** - The local list and any network lists are checked; users can log on if all lists are verified

## Configuring Existing Features Common to the ICA Win32 Clients

This section explains how to configure existing features that are common to the ICA Win32 Clients. For configuration instructions specific to each ICA Win32 Client, see the appropriate chapter about the client you plan to use.

The following topics are discussed in this section:

- User-to-User Shadowing
- Smart Card Support
- Auto Client Reconnect
- Novell Directory Services Support
- Disabling DNS Name Resolution
- Mapping Client Drives
- Mapping Client Printers
- Mapping Client COM Ports
- Mapping Client Sound Support
- Configuring Multiple Monitors

### User-to-User Shadowing

No client-side configuration is required to use this feature. You shadow a user from a client device using the published Shadow Taskbar.

For information about using the Shadow Taskbar, see the Shadow Taskbar help. For information about enabling and configuring this feature on the MetaFrame server, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.

## Smart Card Support

MetaFrame XP's smart card support is based on Microsoft's PC/SC standard specifications. MetaFrame XP supports smart cards and smart card devices only that are, themselves, supported by the underlying Windows operating system. A discussion of security issues related to PC/SC standards compliance is beyond the scope of this document.

► **To select smart card-based logon (Program Neighborhood Agent)**

1. In the Windows system tray, right-click the Program Neighborhood Agent icon and choose **Properties** from the menu that appears.
2. Select the **Server** tab.
3. From the **Logon mode** menu, select **Smart card logon** or **Smart card logon pass-through authentication**.

With **Smart card logon** selected, the ICA Client prompts the user for a smart card PIN (Personal Identification Number) when it starts up and every time the user requests a published resource.

With **Smart card logon pass-through authentication** selected, the ICA Client prompts the user for a smart card PIN when it starts up. Pass-through authentication then caches the PIN and passes it to the server every time the user requests a published resource. The user does not have to subsequently reenter a PIN to access published resources.

4. Click **OK** to close the **Properties** dialog box.

To set smart card based logon using the Program Neighborhood Agent Admin tool, see "Server Tab Options" on page 45.

---

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

---

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

## Auto Client Reconnect

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

When this feature is enabled on a MetaFrame server, users do not have to reconnect manually to continue working. The client attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. If **Require user authentication** is selected on **ICA Settings** in the Management Console for MetaFrame XP, a dialog box requesting credentials is displayed to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off. Users can reconnect only to disconnected sessions.

## Changing ICA Client Default Auto Reconnect Settings

Auto client reconnect is enabled on the ICA Win32 Clients by default. When the ICA Client detects that its connection to the server is broken, it waits 30 seconds before beginning the reconnection sequence. By default, the ICA Client attempts to reconnect three times and then stops.

If you want to change the default settings for a particular user, you must add the following lines to the **[WFClient]** section of the Appsrv.ini file located in the user's %User Profile%\Application Data\ICA Client directory:

**TransportReconnectEnabled=0** to disable auto client reconnect.

**TransportReconnectDelay=n** to configure the number of seconds to wait before attempting to reconnect.

**TransportReconnectRetries=n** to configure the number of reconnection attempts.

## Novell Directory Services Support

When launching ICA Win32 Client software, users can log on and be authenticated using their NDS credentials. Supported NDS credentials are user name (or distinguished name), password, directory tree, and context.

NDS support is integrated into the following:

- **Program Neighborhood Agent and Program Neighborhood Client.** If NDS is enabled in the MetaFrame XP farm, NDS users enter their credentials on an NDS tab on the ICA Client logon screen. If users have the Novell Client (Version 4.8) installed, they can browse the NDS tree to choose their context. See “Novell Directory Services Support” on page 93 for information about additional configuration necessary to enable NDS support for the Program Neighborhood Agent.
- **Pass-Through Authentication.** If users have the Novell Client (Version 4.8) installed, you can pass their credentials to the MetaFrame XP server, eliminating the need for multiple system and application authentications. To enable pass-through authentication, configure the following policy options in the User Package in ZENworks for Desktops:
  1. Enable the **Dynamic Local User** policy option.
  2. Set the **Use NetWare Credentials** value to **On**.
- **Custom ICA Connections.** When users run the Add New ICA Connection wizard, they must enter a distinguished name in the user name field and a password in the password field. Users must leave the domain field blank.
- **NFuse Classic or the new Web Interface for MetaFrame XP.** NDS users enter their credentials on an NDS logon screen provided by NFuse Classic or the Web Interface for MetaFrame XP. See the *NFuse Classic Administrator's Guide* or the *Web Interface for MetaFrame XP Administrator's Guide* for information about configuring your server for NDS.

---

**Note** To use NDS logon information with earlier versions of ICA Win32 Clients, enter the NDS tree name in the **Domain** field and a distinguished name in the **User** field on the ICA Win32 Client logon screen.

---

## Setting a Default Context for NDS

You can set a default context for NDS for the Program Neighborhood Client (Ica32.msi and Ica32.exe) and for the Program Neighborhood Agent (Ica32a.msi only). To set a default context for NDS, you must configure the particular installer file you are using to deploy the ICA Clients:

### Program Neighborhood Agent

**Windows Installer Package.** For instructions about setting a default context for NDS in the Windows Installer package of the Program Neighborhood Agent, see “Configuring the Windows Installer Package for Silent User Installation” on page 38.

## Program Neighborhood Client

**Windows Installer Package.** For instructions about setting a default context for NDS in the Windows Installer package of the Program Neighborhood Client, see “Configuring the Windows Installer Package for Silent User Installation” on page 61.

**Self-Extracting Executable.** For general information about configuring the self-extracting executable for the Program Neighborhood Client, see “Configuring the Self-Extracting Executable for Silent User Installation” on page 63.

### ► To set a default context for NDS in the self-extracting executable

1. Extract the client file set from Ica32.exe as outlined in “Configuring the Self-Extracting Executable for Silent User Installation” on page 63.
2. Locate and open Appsrv.src in a text editor.
3. Add the following parameter to the **[WFClient]** section:

**DefaultNDSContext**=<Context1 [,...]>.

If you are including more than one context, separate the contexts by a comma.

4. Save and close the file.

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

If the Program Neighborhood Client is configured to use pass-through authentication on a client device that has the Novell Client installed, the Program Neighborhood Client, by default, uses the NDS credentials to authenticate the user to the MetaFrame server. If you want the ICA Client to use the user’s Windows NT credentials with pass-through authentication instead, you must add a parameter to the ICA Client’s Appsrv.ini file. You can make the addition to the Windows Installer package before distributing it, or you can configure clients on individual client devices after installation is complete.

### Configuring the Windows Installer Package Prior to Installation

For information about configuring the Window Installer package for use of Windows NT credentials with pass-through authentication on client devices that have the Novell Client installed, see “Configuring the Windows Installer Package for Silent User Installation” on page 61.

### Configuring Individual Clients After Installation

1. Locate and open the user-level Appsrv.ini file in a text editor. By default, this file is located in the %User Profile%\Application Data\ICA Client directory.

2. Add the following parameter to the **[WFCLIENT]** section:  
**SSOnCredentialType=NT**
3. Save and close the Appsrv.ini file.

## DNS Name Resolution

You can configure ICA Win32 Clients that use the XML service to connect to the MetaFrame farm to request a Domain Name System (DNS) name instead of a server's IP address.

---

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

---

The ICA Win32 Program Neighborhood Client is configured to use TCP/IP+HTTP (the XML Service) browsing by default. ICA Clients connecting to published applications through NFuse Classic or the new Web Interface for MetaFrame XP also use the XML Service. For ICA Clients connecting through NFuse Classic or the Web Interface for MetaFrame XP, the Web server resolves the DNS name on behalf of the client.

DNS name resolution is disabled by default in the MetaFrame farm and enabled by default on the ICA Win32 Clients. When DNS name resolution is disabled in the farm, any client request for a DNS name will return an IP address. There is no need to disable DNS name resolution on the client.

## Disabling DNS Name Resolution

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

- ▶ **To disable DNS name resolution on the Win32 ICA Clients**
  1. Open the user-level Appsrv.ini file. By default, this file is located in the %User Profile%\Application Data\ICA Client directory.
  2. Change the line **xmlAddressResolutionType=DNS-Port** to **xmlAddressResolutionType=IPv4-Port**.
  3. Save and close the Appsrv.ini file.
  4. Repeat Steps 1 through 3 for each user of the client workstation.



## Enabling Extended Parameter Passing

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

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

---

**Note** Version 7.0 of the Program Neighborhood Agent supports content redirection, a feature introduced in Feature Release 2 of MetaFrame XP. Functionally equivalent to extended parameter passing, content redirection allows you to enforce all underlying file type association from the MetaFrame 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 XP Server Administrator's Guide* included in your MetaFrame XP media pack for more information.

---

Enabling extended parameter passing requires both server- and client-side configuration. On the server, add the %\* (percent and asterisk symbols) tokens to published applications. These tokens act as placeholders for client-passed parameters. For instructions about configuring the MetaFrame XP server to support parameter passing, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.

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

## Configuring Extended Parameter Passing

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

---

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

---

The command line you create must include the following elements:

- The file name of the ICA Win32 Client executable used to launch the published application
- The name of the published application to launch, in the correct syntax
- The parameter passing arguments

The next section explains how to determine which ICA Win32 Client executable to include in the command line.

### Determining the ICA Win32 Client Executable

Users can connect to published applications using the following methods:

- Finding and launching an application in an application set using the Program Neighborhood Client
- Creating and launching a custom ICA connection using the Program Neighborhood Client
- Launching an .Ica file (.Ica files are placed on the client device when the user connects using NFuse Classic or the new Web Interface for MetaFrame XP)

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

Connection method	ICA Client executable
Custom ICA connections (using Program Neighborhood Client)	Wfcrun32.exe
Applications identified in ICA files (including connecting using NFuse Classic or the new Web Interface for MetaFrame XP)	Wfica32.exe
Applications in application sets (using the Program Neighborhood Client)	Pn.exe

---

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

## Identifying Published Applications

Each ICA Win32 Client executable uses different command line syntax to specify configuration data when launching published applications. When creating your command line, you must use the executable's command line syntax to correctly identify the published application.

---

**Note** To view an executable's required command line syntax, from a command prompt, change directories to the ICA Win32 Client's installation directory and then type the executable's name followed by `/?` (forward slash question mark).

---

### Command Line Syntax for Wfcrun32.exe

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

```
C:\Program Files\Citrix\ICA Client\wfcrun32.exe "<application name>"
```

### Command Line Syntax for Wfica32.exe

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

```
C:\Program Files\Citrix\ICA Client\wfica32.exe <file_name>.ica
```

### Command Line Syntax for Pn.exe

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

```
C:\Program Files\Citrix\ICA Client\pn.exe /app:"<application name>"
```

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

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:"<application set name>" /app:"<application name>"
```

---

**Note** To use Pn.exe to launch an application in an application set, the application must exist in the Pn.exe application cache.

---

## Including Parameter Passing Arguments

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

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

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:"Production Farm" /app:"Notepad Text Editor" /param:"%1"
```

## Entering Parameter Passing in the Windows Registry

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

The following example command lines combine the required elements into a working ICA Win32 Client command line.

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

```
C:\Program Files\Citrix\ICA Client\pn.exe /app:“Notepad Text Editor” /  
param:“%1”
```

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

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:“Production Farm” /  
app:“Notepad Text Editor” /param:“%1”
```

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

```
C:\Program Files\Citrix\ICA Client\wfcrun32.exe “Notepad Text Editor” /  
param:“%1”
```

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

```
C:\Program Files\Citrix\ICA Client\wfica32.exe Notepad.ica /param:“%1”
```

---

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

---

## Mapping Client Devices

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

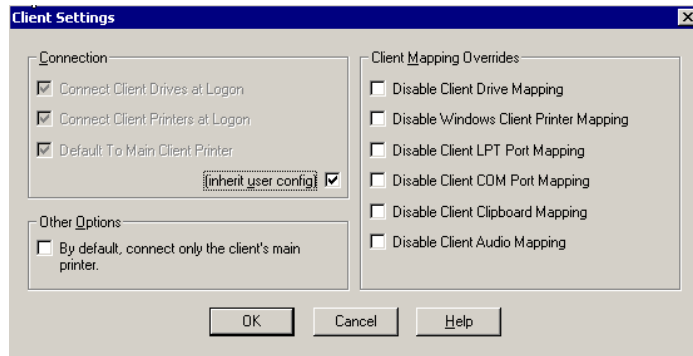
- Transparently access local drives, printers, and COM ports
- Cut and paste between the ICA session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the ICA session

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

You can use the **net use** and **change client** commands to map client devices not automatically mapped at logon. See your MetaFrame server documentation for information about the change client command.

## Turning off Client Device Mappings

On the MetaFrame server, specify client device mapping options in the **Client Settings** dialog box in Citrix Connection Configuration.



The **Connection** options control whether or not drives and printers are mapped to client drives and printers. If these options are cleared, the devices are still available but must be mapped to drive letters and port names manually.

Use the **Client Mapping Overrides** options to disable client device connections.

Option	Description
<b>Connect Client Drives at Logon</b>	If this option is selected, the client device's drives are automatically mapped at logon.
<b>Connect Client Printers at Logon</b>	If this option is selected, the client device's printers are automatically mapped at logon. This option applies only to Windows clients and maps only printers already configured in Print Manager on the client device.
<b>Default to Main Client Printer</b>	If this option is selected, the user's default client printer is configured as the default printer for the ICA session.
<b>(inherit user config)</b>	If this option is selected, the per-user settings in User Manager override these settings.

## Mapping Client Drives

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

Client drive mapping is transparently built into the standard Citrix device redirection facilities. These mappings can be used by the File Manager or Explorer and your applications just like any other network mappings.

---

**Important** Client drive mapping is not supported when connecting to MetaFrame Server 1.0 for UNIX Operating Systems.

---

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

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

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

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

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

When an ICA Client device connects to a MetaFrame server, client mappings are reestablished unless automatic client device mapping is disabled. Automatic client device mapping can be configured for ICA connections and users. In the **Client Settings** dialog box, you can enable or disable automatic client device mapping for an ICA connection. The **User Configuration** dialog box in User Manager for Domains allows you to enable or disable automatic client device mapping for a user.

## Mapping Client Printers

The Citrix ICA Win32 Client supports auto-created printers. With auto-created printers, users find their local printers mapped to their sessions and ready for use as soon as they connect.

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

---

**Important** For information about configuring ICA Client printing on servers running MetaFrame Server for UNIX Operating Systems, see the *MetaFrame for UNIX Operating Systems Administrator's Guide*.

---

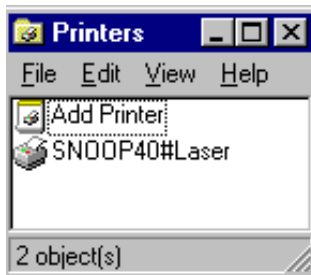
If the **Connect Client Printers at Logon** check box is selected in the terminal connection or user profile, the client printers are automatically connected when users log on and are deleted when they log off if the printers do not contain any print jobs. If print jobs are present, the printers (and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

If you do not want a user's automatically created printers to be deleted when the user logs off, modify or delete the **Auto Created Client Printer** entry in the **Comment** field of a client printer's **Properties** dialog box. If you modify or delete this description, the printer is not deleted when the user logs off. Each time the user logs on, the printer that is already defined is used. If users change the Windows printer settings, they will not automatically be set. If users have custom print settings, you may not want to delete the automatically created printers.

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

► **To view mapped client printers when connected to a MetaFrame server**

While connected to the MetaFrame server, go to the remote desktop's **Start** menu and choose **Settings > Printers**. The **Printers** window opens:



The **Printers** screen displays the local printers mapped to the ICA session. The name of the printer takes the form *clientname#printername*, where *clientname* is the unique name given to the client device during ICA Client Setup and *printername* is the Windows printer name. In this example ICA session, a client machine called "Snoop40" has access to its local printer named "Laser." This name cannot be changed and is used to locate the specific printer. Because the Windows printer name is used and not the port name (as with DOS Client printing), multiple printers can share a printer port without conflict.



## Mapping Client COM Ports

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

---

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

---

### ► To map a client COM port

1. Start the ICA Client and log on to the MetaFrame server.
2. At the command prompt, type

**net use comx: \\client\comz:**

where  $x$  is the number of the COM port on the server (ports 1 through 9 are available for mapping) and  $z$  is the number of the client COM port you want to map. Press **Enter**.

3. To confirm the operation, type

**net use**

at the command prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.

To use this COM port in a session on a MetaFrame server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the client device.

---

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

---

## Mapping Client Audio

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

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

You control the amount of bandwidth client audio mapping uses from the Citrix Connection Configuration tool, which is available from the ICA Administrator Toolbar on the MetaFrame server. The tool lets you choose among three different audio quality settings, and you can disable client audio mapping altogether. See the *MetaFrame XP Administrator's Guide* included in your MetaFrame XP media pack for more information about client audio mapping.

---

**Note** Client sound support mapping is not supported when connecting to MetaFrame Server 1.0 and 1.1 for UNIX Operating Systems..

---

## Configuring Multiple Monitors

If your client operating system with video hardware and drivers provides multiple monitor support with the Windows taskbar on the primary (left) monitor (Windows 98 and 2000 mode of multiple monitor support), there are restrictions in the level of support when using the client configured with “seamless” windows. Multiple monitors are fully supported when the client is configured in a non-seamless mode and set with the same color depth on all monitors in use.

---

**Note** Secondary windows sometimes appear in the primary monitor (uppermost, left).

---

## System Hardware Requirements

To enable multiple monitor support, the system must have the following:

- Multiple PCI video boards, compatible with the Citrix ICA Client on the appropriate Windows platform
- Or-
- A special multiple monitor video board, such as the Matrox G400, compatible with the Citrix ICA Client on the appropriate Windows platform

The following hardware configurations were tested with multiple monitor support.

---

**Important** Citrix highly recommends that you test these configurations on your own hardware to ensure that they function properly for your specific machine configuration.

---

- On Windows 98, Matrox G400 is fully supported as a Windows 98/2000-style multiple monitor
- On Windows 2000, Matrox G400 works in a Windows NT 4.0/Windows 95-style multiple monitor
- Both Windows 98 and Windows 2000 support Matrox G200 PCI (multiple cards installed) as a Windows 98/2000-style multiple monitor
- Windows 98 supports a wide variety of PCI video boards, including many models from ATI and Cirrus Logic

## Using the ICA Win32 Program Neighborhood and Web Clients with Application Launching and Embedding

If you are not planning to use NFuse Classic or the new Web Interface for MetaFrame XP but still want to deliver applications over the Web, you can use Application Launching and Embedding (ALE) in conjunction with the Web-based ICA Client Installation feature. The ICA Win32 Program Neighborhood and Web Clients can be used with launched and embedded applications.

The ICA Win32 Web Client replaces the ActiveX control and Netscape Plug-In Clients and is available as a self-extracting executable. At approximately 1.8MB in size, this package is significantly smaller than the other ICA Win32 Clients. The smaller size allows quicker downloads and installation. You can configure the ICA Win32 Web Client for silent user installation.

### Application Launching and Embedding

Using Application Launching and Embedding, you can provide access to full-function Windows-based applications from HTML pages over intranets or the Internet, without rewriting application code. The applications look and feel as if they are running locally, even though they are executing on the MetaFrame server.

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

- *Launching* an application from a Web page means you click a hyperlink that references an ICA file. Clicking the hyperlink causes the application to start and appear in a separate window on the local desktop. You can then use this application as if it is installed and running on your local computer.
- *Embedding* an application places the window in which the program runs within the Web browser window.

## Launched Applications

The Management Console for MetaFrame XP and the Published Application Manager (MetaFrame 1.8) include wizards that allow you to create ICA files and HTML pages. The HTML pages are saved on your Web server for users to visit and launch ICA sessions. HTML pages that launch ICA sessions contain a hyperlink to an ICA file that is located in a public HTML directory. When clicked, the hyperlink downloads the ICA file to the client device. The ICA Client software uses the parameters in the ICA file to launch the application on the user's desktop. If the ICA file does not detect ICA Client software installed on the client device, the client software is presented to the user to download and install.

### ► To set up a Web page so users can launch an application

1. Copy `Ica32t.exe` (for the ICA Win32 Web Client) or `Ica32.exe` (for the ICA Win32 Program Neighborhood Client) to your Web server. These files are located in the following directories (substitute *language* with the language of the ICA Client software) of the Components CD included in your MetaFrame XP media pack:  
`Icaweb\language\ica32`  
where *language* is one of:
  - En (English)
  - Fr (French)
  - De (German)
  - Ja (Japanese)
  - Es (Spanish)
2. Publish an application. See the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack for information about publishing applications.
3. Use the Create HTML File wizard (MetaFrame XP) or the Write HTML File wizard (MetaFrame 1.8) to create an HTML page on your server. You can also create an ICA file. For more information about creating HTML files that contain published applications, see your MetaFrame server documentation and the online Help for the Management Console for MetaFrame XP or the Published Application Manager (MetaFrame 1.8).
4. Open the HTML file in a text editor and edit the client type parameter to include the full path to the `Ica32.exe` or `Ica32t.exe` file, respectively. This parameter calls the ICA Win32 Client to run the published application.

## Embedded Applications

The Citrix ICA Win32 Program Neighborhood and Web Clients allow you to embed applications in Internet Explorer and Netscape Navigator.

Rather than creating separate Web pages for Microsoft Internet Explorer and Netscape Navigator users, you can create a single Web page that contains two types of HTML tags to embed applications for Internet Explorer and Netscape Navigator.

Complete the following steps to use one of the ICA Win32 Clients to embed applications in Internet Explorer or Netscape Navigator:

1. Create an ICA Client download Web site using the Web-based ICA Client Installation feature. The elements required for the download Web site are included in your MetaFrame XP media pack. You can also download them from the Download area of the Citrix Web site at <http://www.citrix.com/download>. Click the “Download Web-based ICA Clients Install Components” link.

For more information about constructing an ICA Client download Web site using your MetaFrame XP media pack, see the *MetaFrame XP Server Administrator’s Guide* included in your MetaFrame XP media pack.

For more information about constructing an ICA Client download Web site using the packages downloaded from the Citrix Web site, see the corresponding Readme.htm file located on the same Web page as the packages.

2. Create an HTML page using the appropriate wizard on your MetaFrame server.
3. Set the **cabLoc** parameter for Internet Explorer users.
4. Set the **Pluginspage** parameter for Netscape Navigator users.

Detailed instructions for Steps 2, 3, and 4 are below.

### ► To create an HTML page using MetaFrame server software

1. On MetaFrame XP, open the Create HTML File wizard from the Management Console.  
On MetaFrame 1.8, open the Write HTML File wizard from the Published Application Manager.
2. Create the HTML file and save it on your Web server. For detailed instructions, follow the online Help for the appropriate wizard.
3. Open the HTML file in a text editor.

► **To set the cabLoc parameter for Internet Explorer users**

1. In the HTML file you created in the preceding Step 2, locate the line that begins with: **var cabLoc =**.  
Replace the value after the equal sign (=) with the URL of the appropriate Win32 Client: "http://*Webserver/directory/Ica32.exe* or *Ica32t.exe*";  
Make sure you include the quotation marks and the semicolon.
2. Save the file and make sure it is stored on your Web server along with the ICA file for the embedded session. When users visit the HTML page, Internet Explorer automatically downloads and installs the ActiveX control.
3. Keep the HTML file open.

► **To set the Pluginspage parameter for Netscape Navigator users**

1. Locate the line that begins with: **var plugRefLoc =**.  
Replace the value after the equal sign (=) with the URL of the default Web page of the ICA Client download Web site you created with the Web-based ICA Client Installation feature.  
Example:  

```
var plugRefloc = "http://mywebserver/directory/  
setup.htm";
```

  
Make sure you include the quotation marks and the semicolon.
2. Save the file and make sure it is stored on your Web server along with the ICA file for the embedded session.
3. Publish a link to the HTML page. When users visit the HTML page, Netscape Navigator refers users who do not have the plug-in to the appropriate ICA Client download page.

# Using Applications Published on MetaFrame Servers for UNIX Operating Systems

For connections to applications published on a MetaFrame Server for UNIX Operating Systems, two additional utilities provide functionality for configuring session display and cutting and pasting objects between the ICA session and the client device. This section describes how to use these utilities.

## Using the Window Manager

If you are connecting to an application published on a MetaFrame Servers for UNIX Operating Systems, use the Citrix window manager to minimize, resize, position, and close windows, and access seamless “full screen” mode. This section describes how to use the window manager.

## About Seamless Windows

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

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

## Accessing Seamless “Full Screen” Mode

- ▶ **To switch between seamless and seamless “full screen” modes**






Press SHIFT+F2.

## Minimizing, Resizing, Positioning, and Closing Windows

When you connect to a published application on a MetaFrame server, buttons to minimize, resize, position, and close windows are provided by the ctwm window manager.

► **To minimize, resize, position, and close windows**

Use the left mouse button to click the following buttons:

To	Click	Note
Minimize published application windows on your desktop		Seamless windows are minimized as buttons on the desktop's taskbar. Non-seamless and seamless "full screen" windows are minimized as icons on the desktop.
Open a minimized window		Click its button on the taskbar or its icon on the desktop.
Adjust the size of published application windows		Click and hold down the mouse button, then move the pointer to the edge of the window and drag it in the direction you want to scale it. The window dimensions are displayed in the top left-hand corner. Release the mouse button to apply the resizing.  To resize the window proportionately, move the mouse pointer to a corner of the window and drag it.
Reposition published application windows		Click and hold down the mouse button, drag the window to the required position on the desktop, and release the mouse button.
Close and exit a published application		When you close the last application in a session, the session disconnects automatically after 20 seconds.

## Using the Citrix Window Manager Menus

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

► **To access the ctxwm menu system**

1. On a blank area of the remote desktop window, click and hold down the left mouse button. The ctxwm menu is displayed.
2. Drag the mouse pointer over **Shutdown** to display the shutdown options.



► **To choose an option from the ctxwm menu**

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

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

---

**Note** Your MetaFrame server may be configured to terminate any applications that are running if a session is disconnected.

---

## Cutting and Pasting Graphics Using ctxgrab and ctxcapture

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

### Using ctxgrab

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

► **To access the ctxgrab utility from the window manager**

1. In seamless mode, right click the **ctxgrab** button in the top, left-hand corner of the screen to display a menu and choose the **screengrab** option.  
In full screen mode, left click to display the ctxwm menu and choose the **screengrab** option.
2. When ctxgrab is started, a dialog box is displayed.

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

## Using ctxcapture

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

With ctxcapture you can:

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

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

- ▶ **To access the ctxcapture utility from the window manager**
  1. Left click to display the **ctxwm** menu and choose the **screengrab** option.
  2. When ctxcapture is started, a dialog box is displayed.
- ▶ **To copy from a local application to an application in an ICA Client window**
  1. From the **ctxcapture** dialog box, click **From screen**.
  2. **To select a window:** move the cursor over the window you want to copy and click the middle mouse button.
    - To select a region:** hold down the left mouse button and drag the cursor to select the area you want to copy.
    - To cancel the selection:** click the right mouse button. While dragging, cancel the selection by clicking the right mouse button before releasing the first button.

3. From the **ctxcapture** dialog box, click **To ICA**. The **xcapture** button changes color to indicate that it is processing the information.
4. When the transfer is complete, use the appropriate command in the application in the ICA Window to paste the information.

▶ **To copy from an application in an ICA Client window to a local application**

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

▶ **To copy from xv to an application in an ICA Client window or local application**

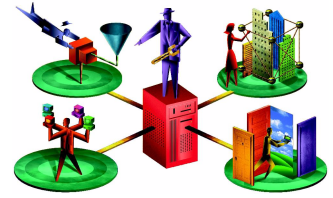
1. From xv, copy the graphic.
2. From the **ctxcapture** dialog box, click **From xv** and **To ICA**.
3. When the transfer is complete, use the appropriate command in the ICA Client window to paste the information.

▶ **To copy from an application in an ICA Client window to xv**

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



# Implementing Security for the ICA Win32 Clients



This chapter discusses measures you can take to secure the communication between your MetaFrame server farm and the ICA Win32 Clients. The following topics are covered:

- Connecting to a Server Through a Proxy Server
- Using the ICA Win32 Clients with the Secure Gateway for MetaFrame or SSL Relay
- Connecting to a Server Through a Firewall

---

**Note** NFuse Classic has been integrated as a feature in MetaFrame XP. It is now called the Web Interface for MetaFrame XP.

---

## Integrating the ICA Win32 Clients with Your Security Solutions

You can integrate the ICA Win32 Clients with a range of security technologies, including proxy servers, firewalls, and SSL/TLS based systems. This section describes:

- Connecting through a SOCKS proxy server or Secure proxy server (also known as *security proxy server*, HTTPS proxy server, or SSL tunneling proxy server)
- Integrating the ICA Win32 Clients with the Secure Gateway or SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- Connecting to a server through a firewall

## Connecting to a Server Through a Proxy Server

Proxy servers are used to limit access into and out of your network, and to handle connections between ICA Clients and MetaFrame servers. The ICA Win32 Clients support SOCKS and secure proxy protocols.

### ICA Win32 Program Neighborhood Agent and Web Client

In communicating with the MetaFrame server, the Win32 Program Neighborhood Agent and the ICA Win32 Web Client use proxy server settings that are configured remotely on the NFuse Classic server or the server running the new Web Interface for MetaFrame XP. See the *NFuse Classic Administrator's Guide*, or the *Web Interface for MetaFrame XP Administrator's Guide* for information about configuring proxy server settings for these ICA Clients.

In communicating with the Web server, the ICA Win32 Program Neighborhood Agent and the ICA Win32 Web Client use the proxy server settings that are configured through the Internet settings of the default Web browser on the client device. You must configure the Internet settings of the default Web browser on the client device accordingly.

### ICA Win32 Program Neighborhood Client

The Win32 Program Neighborhood Client uses proxy server settings you configure locally from the ICA Client's toolbar. You can configure proxy server settings in two ways:

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

### Enabling Auto-Client Proxy Detection

If you are deploying the ICA Win32 Client in an organization with many proxy servers, consider using auto-client proxy detection. Auto-client proxy detection communicates with the local Web browser to discover the details of the proxy server. It is also useful if you cannot determine which proxy server will be used when you configure the client. Auto-client proxy detection requires Internet Explorer 5.0 or later, or Netscape for Windows 4.78, 6.2, or later.

► **To enable auto-client proxy detection**

1. Start the Program Neighborhood Client.
2. If you are configuring an application set:  
Right-click the application set you want to configure and select **Application Set Settings**. The **Application Set** dialog box appears.  
If you are configuring an *existing* custom ICA connection:  
Right-click the custom ICA connection you want to configure and select **Properties**. The **Connection Properties** dialog box appears.  
If you are configuring *all future* custom ICA connections:  
Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
3. On the **Connection** tab, click **Firewalls**.
4. Select **Use Web browser proxy settings**.
5. Click **OK** twice.

### **Manually Specifying the Details of Your Proxy Server**

---

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

---

► **To manually specify the details of your proxy server**

1. Start the Program Neighborhood Client.
2. If you are configuring an application set:  
Right-click the application set you want to configure and select **Application Set Settings**. The **Application Set** dialog box appears.  
If you are configuring an *existing* custom ICA connection:  
Right-click the custom ICA connection you want to configure and select **Properties**. The **Connection Properties** dialog box appears.  
If you are configuring *all future* custom ICA connections:  
Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
3. On the **Connection** tab, click **Firewalls**.
4. Select the proxy protocol type (**SOCKS** or **Secure (HTTPS)**).

5. Enter the **Proxy address**.
6. Specify the port number of the proxy server (if other than 1080 for SOCKS or 8080 for secure proxy).
7. Click **OK** twice.

### **Configuring the User Name and Password**

Some proxy servers require authentication, prompting you for a user name and password when you enumerate resources or open an ICA connection. You can avoid these prompts by configuring the ICA Client to pass the credentials without user intervention. Do this by creating settings that:

- Apply to one or several existing custom ICA connections
- or-
- Act as the default for all future custom ICA connections to be created using the Add ICA Connection wizard

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

1. Exit the Program Neighborhood Client if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Appsrv.ini file (default directory: %UserProfile%\Application Data\ICAClient) in a text editor.
3. Locate the [***ServerLocation***] section, where *ServerLocation* is the name of the connection for which you want to create the default.



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

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

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

**ProxyUsername**=<*user name*>

**ProxyPassword**=<*password*>

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

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

Add the following lines to the [**WFClient**] section:

**ProxyUsername**=<*user name*>

**ProxyPassword**=<*password*>

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

5. Repeat Steps 3 and 4 for any additional connections if applicable.
6. Save your changes.

---

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

---

► **To create a default for all future custom ICA connections to be created using the Add ICA Connection wizard**

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

**ProxyUsername**=<*user name*>

**ProxyPassword**=<*password*>

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

5. Save your changes.

---

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

---

## Using the ICA Win32 Clients with the Secure Gateway for MetaFrame or SSL Relay

You can integrate the ICA Win32 Clients with the Secure Gateway or SSL Relay service. The clients support both SSL and TLS protocols

- SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.
- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the certificates you use for SSL in your MetaFrame installation will also work with TLS. Some organizations, including US government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS 140. FIPS 140 (Federal Information Processing Standard) is a standard for cryptography.

### The Secure Gateway

You can use the Secure Gateway for MetaFrame in either *Normal* mode or *Relay* mode. No ICA Client configuration is required if you are using the Secure Gateway in Normal mode.

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

- The fully qualified domain name (FQDN) of the Secure Gateway server
- The port number of the Secure Gateway server

---

**Note** Relay mode is not supported by the Secure Gateway for MetaFrame, version 2.0

---

## ICA Win32 Program Neighborhood Agent and Web Client

The Win32 Program Neighborhood Agent and the Win32 Web Client use settings that are configured remotely on the NFuse Classic server or the server running the new Web Interface for MetaFrame XP to connect to servers running the Secure Gateway. See the *NFuse Classic Administrator's Guide* or the *Web Interface for MetaFrame XP Administrator's Guide* for information about configuring proxy server settings for these ICA Clients.

## ICA Win32 Program Neighborhood Client

### ► To configure the details of your Secure Gateway server

1. Make sure the client device meets all system requirements outlined on pages 36, 59, and 124 of this guide.
2. Start the Program Neighborhood Client.
3. If you are configuring an application set:
  - Right-click the application set you want to configure and select **Application Set Settings**. The **Application Set** dialog box appears.
  - If you are configuring an *existing* custom ICA connection:
    - Right-click the custom ICA connection you want to configure and select **Properties**. The **Connection Properties** dialog box appears.
    - If you are configuring *all future* custom ICA connections:
      - Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
4. If you are configuring an application set or an *existing* custom ICA connection:
  - From the **Network Protocol** menu, select **SSL/TLS+HTTPS**.
  - If you are configuring *all future* custom ICA connections:
    - From the **Network Protocol** menu, select **HTTP/HTTPS**.
5. On the **Connection** tab, click **Firewalls**.

6. Enter the fully qualified domain name (FQDN) of the Secure Gateway server in the **Secure gateway address** box.

---

**Important** The fully qualified domain name (FQDN) must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

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

---

7. Enter the port number in the **Port** box.
8. Click **OK** twice.

## Citrix SSL Relay

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

You can use Citrix SSL Relay to secure communications:

- Between an SSL/TLS-enabled ICA Client and a MetaFrame server. Connections using SSL/TLS encryption are marked with a padlock icon in Citrix Connection Center.
- In an NFuse Classic deployment or a server running the new Web Interface for MetaFrame XP, between the MetaFrame server and the Web server.

For information about configuring and using SSL Relay to secure your MetaFrame installation, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack. For information about configuring the NFuse Classic server or server running the new Web Interface for MetaFrame XP to use SSL/TLS encryption, see the *NFuse Classic Administrator's Guide* or the *Web Interface for MetaFrame XP Administrator's Guide*.

## System Requirements

In addition to the system requirements listed for each ICA Win32 Client in its respective chapter, you also must ensure that:

- The client device supports 128-bit encryption

- The client device has a root certificate installed that can verify the signature of the Certificate Authority on the server certificate
- The ICA Client is aware of the TCP listening port number used by the SSL Relay service on the MetaFrame server.

### Verifying Cipher Strength/128-bit Encryption

If you have Internet Explorer installed on your system, you can determine the encryption level of your system as follows:

1. Start Internet Explorer.
2. From the **Help** menu, click **About Internet Explorer**.
3. Check the Cipher Strength value. If it is less than 128-bit, you need to obtain and install a high encryption upgrade from the Microsoft Web site. Go to <http://www.microsoft.com/> and search for “128-bit” or “strong encryption.”
4. Download and install the upgrade.

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

---

**Note** The ICA Win32 Clients support certificate key lengths of up to 4096 bits. Ensure that the bit lengths of your Certificate Authority root and intermediate certificates, and those of your server certificates, do not exceed the bit length your ICA Clients support, or connection may fail.

---

### About Root Certificates

See “Installing Root Certificates on the ICA Win32 Clients” on page 128 for information about root certificates.

---

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

---

### Using Citrix SSL Relay with Non-Standard TCP Ports

By default, Citrix SSL Relay uses TCP port 443 on the MetaFrame server for SSL/TLS-secured communication. If you configure SSL Relay to listen on a port other than 443, you must make the ICA Client aware of the non-standard listening port number as follows.

- ▶ **To apply a different listening port number for all connections:**
  1. Exit Program Neighborhood if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
  2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
  3. Locate the **[WFClient]** section.  
Set the value of the SSLProxyHost parameters as follows:  
SSLProxyHost=\*<SSL relay port number>,  
where <SSL relay port number> is the number of the listening port.
  4. Save and close the file.
  
- ▶ **To apply a different listening port number to particular connections only:**
  1. Exit Program Neighborhood if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
  2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
  3. Locate the particular **[Connection\_Section]**.  
Set the value of the SSLProxyHost parameters as follows:  
SSLProxyHost=\*<SSL relay port number>,  
where <SSL relay port number> is the number of the listening port.
  4. Repeat Step 3 for all connection sections for which you want to specify a different listening port number.
  5. Save and close the file.

## Configuring and Enabling ICA Clients for SSL and TLS

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

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

### Forcing TLS Connections for all ICA Win32 Clients

To force the ICA Win32 Clients (including the ICA Win32 Web Client) to connect with TLS, you must specify TLS on your the Secure Gateway server or SSL Relay service. See the *Secure Gateway Administrator's Guide* or SSL Relay service documentation for more information.

- ▶ **To configure the ICA Win32 Program Neighborhood Client to use SSL/TLS**
  1. Make sure the client device meets all system requirements outlined on pages 36, 59, and 124 of this guide.
  2. Open the Program Neighborhood Client.
  3. If you are configuring an application set to use SSL/TLS:
    - Right-click the application set you want to configure and select **Application Set Settings**. The **Application Set** dialog box appears.
    - If you are configuring an *existing* custom ICA connection to use SSL/TLS:
      - Right-click the custom ICA connection you want to configure and select **Properties**. The **Connection Properties** dialog box appears.
      - If you are configuring *all future* custom ICA connection to use SSL/TLS:
        - Right-click in a blank area of the **Custom ICA Connections** window and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
  4. If you are configuring an application set or an *existing* custom ICA connection:
    - From the **Network Protocol** menu, select **SSL/TLS+HTTPS**.
    - If you are configuring *all future* custom ICA connections:
      - From the **Network Protocol** menu, select **HTTP/HTTPS**.
  5. Add the fully qualified domain name of the SSL/TLS-enabled MetaFrame server(s) to the Address List.
  6. Click **OK**.
- ▶ **To configure the ICA Win32 Program Neighborhood Agent to use SSL/TLS**
  1. Make sure the client device meets all system requirements outlined on pages 36, 59, and 124 of this guide.
  2. To use SSL/TLS to encrypt application enumeration and launch data passed between the Program Neighborhood Agent and the NFuse Classic server or server running the Web Interface for MetaFrame XP, configure the appropriate settings in the configuration file on the Web server. The configuration file must also include the machine name of the MetaFrame server hosting the SSL certificate.
  3. To use secure HTTP (HTTPS) to encrypt the configuration information passed between the Program Neighborhood Agent and the NFuse Classic server or server running the Web Interface for MetaFrame XP, enter the URL of the NFuse Classic server hosting the configuration file in the format `https://<servername>` on the **Server** tab of the Program Neighborhood Agent **Properties** dialog box.

► **To configure the Appsrv.ini file to use TLS**

1. Exit the Program Neighborhood Agent if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section named **[WFClient]**.  
Set the values of these two parameters as follows:  
**SSLCIPHERS={GOV | All}**  
**SECURECHANNELPROTOCOL={TLS | Detect}**. Set the value to **TLS**, or **Detect** to enable TLS. If **Detect** is selected, the Program Neighborhood Agent tries to connect using TLS encryption. If a connection using TLS fails, the client tries to connect using SSL.
4. Save your changes.

### **Meeting FIPS 140 Security Requirements**

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

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

1. Exit the Program Neighborhood Agent if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Open the individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section named **[WFClient]**.
4. Set the values of these three parameters as follows:  
**SSELENABLE=On**  
**SSLCIPHER=GOV**  
**SECURECHANNELPROTOCOL=TLS**
5. Save your changes.

### **Installing Root Certificates on the ICA Win32 Clients**

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



The Citrix ICA Win32 Clients support the Certificate Authorities that are supported by the Windows operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

If you use your own Certificate Authority, you must obtain a root certificate from that Certificate Authority and install it on each client device. This root certificate is then used and trusted by both Microsoft Internet Explorer and the Citrix ICA Win32 Client.

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

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

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

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

---

**Note** The following steps assume that your organization has a procedure in place for users to check the root certificate as they install it. It is important to verify the authenticity of a root certificate before installing it.

---

► **To install a root certificate on the Win32 client device**

1. Double-click the root certificate file. The root certificate file has the extension .cer, .crt, or .der.
2. Verify that you are installing the correct root certificate.
3. Click **Install Certificate**.
4. The Certificate Import Wizard starts. Click **Next**.
5. Choose the **Place all certificates in the following store** option and then click **Browse**.
6. On the **Select Certificate Store** screen, select **Show physical stores**.
7. Expand the Trusted Root Certification Authorities store and then select **Local Computer**. Click **OK**.

8. Click **Next** and then click **Finish**. The root certificate is installed in the store you selected.

## Securing the Program Neighborhood Agent with SSL/TLS

Make sure the client device meets all system requirements outlined on pages 36, 59, and 124 of this guide.

To use SSL/TLS encryption for all communications between the Program Neighborhood Agent, the MetaFrame server, and the NFuse Classic server or server running the Web Interface for MetaFrame XP, the following configuration is necessary.

### What You Need to do on the NFuse Classic Server or the ServerRunning the New Web Interface for MetaFrame XP

- ▶ **To use SSL/TLS to secure the communications between the Program Neighborhood Agent and the Web server**
  1. In the Program Neighborhood Agent Admin tool, select **Server Settings** from the **Configuration settings** menu.
  2. Select **Use SSL/TLS for communications between clients and the Web server**.
  3. Save your changes.

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

### What You Need to do on the MetaFrame Server

- ▶ **To use SSL/TLS to secure the communications between the Program Neighborhood Agent and the MetaFrame server**

Make sure to select the **Enable SSL** option on the **ICA Client Options** tab of the **Application Properties** dialog box in the Management Console for every application you want to secure. For more information, see the *MetaFrame XP Server Administrator's Guide* included in your MetaFrame XP media pack.
- ▶ **To use the SSL Relay to secure communications between the MetaFrame server and the NFuse Classic server or the server running the Web Interface for MetaFrame XP**

You must specify the machine name of the server hosting the SSL certificate in your configuration file. See the *NFuse Classic Administrator's Guide* or the *Web Interface for MetaFrame XP Server Administrator's Guide* for more information about using SSL/TLS to secure communications between the MetaFrame server and the Web server.

## What You Need to do on the Client Device

This section assumes that a valid root certificate is installed on the client device. See “Installing Root Certificates on the ICA Win32 Clients” on page 128 for more information.

- ▶ **To use SSL/TLS to secure the communications between the Program Neighborhood Agent and the NFuse Classic server or the server running the Web Interface for MetaFrame XP**
  1. In the Windows system tray, right-click the Program Neighborhood Agent icon and choose **Properties** from the menu that appears.
  2. The **Server** tab displays the currently configured URL. Click **Change** and enter the server URL in the dialog box that appears. Enter the URL in the format `https://<servername>` to encrypt the configuration data using SSL/TLS.
  3. Click **Update** to apply the change and return to the **Server** tab, or click **Cancel** to cancel the operation.
  4. Click **OK** to close the **Properties** dialog box.
  5. Enable SSL/TLS in the client browser. For more information about enabling SSL/TLS in the client browser, see the client browser’s online Help.

## Enabling Smart Card Logon

This section assumes that smart card support is enabled on the MetaFrame server, and that the client device is properly set up and configured with third party smart card hardware and software. Refer to the documentation that came with your smart card equipment for instructions about deploying smart cards within your network.

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

- ▶ **To enable smart card logon with pass-through authentication**

This logon mode requires a smart card to be present or inserted in the smart card reader at logon time. With this logon mode selected, the Program Neighborhood Agent prompts the user for a smart card PIN (Personal Identification Number) when it starts up. Pass-through authentication then caches the PIN and passes it to the server every time the user requests a published resource. The user does not have to subsequently reenter a PIN to access published resources.

If authentication based on the cached PIN fails or if a published resource itself requires user authentication, the user continues to be prompted for a PIN.

1. From the Program Neighborhood Agent Admin tool, select **Logon Method** from the **Configuration settings** menu.
2. Click **Smart card pass-through authentication** to select the option.
3. Save your changes.

► **To enable smart card logon without pass-through authentication**

This logon mode requires a smart card to be present or inserted in the smart card reader when the user tries to log on. With this logon mode selected, the Program Neighborhood Agent prompts the user for a smart card PIN (Personal Identification Number) when it starts up and every time the user requests a published resource.

1. From the Program Neighborhood Agent Admin tool, select **Logon Method** from the **Configuration settings** menu.
2. Click **Smart card logon** to select the option.
3. Verify that **Pass-through authentication** is not selected.
4. Save your changes.

## Enabling NDS Logon Support

See “Novell Directory Services Support” on page 93 for additional information about enabling NDS support.

1. From the Program Neighborhood Agent Admin Tool, select **Logon Method** from the **Configuration settings** menu.
2. Click **Use NDS credentials for Prompt user and Pass-through authentication** to select the option.
3. Enter the default tree name.
4. Save your changes.

## Connecting to a Server Through a Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using the ICA Win32 Clients through a network firewall that maps the server's internal network IP address to an external Internet address, do the following:

1. Open the Program Neighborhood Client.

2. If you are configuring an application set:
  - Right-click the application set you want to configure and select **Application Set Settings**. The **Application Set** dialog box appears.
  - If you are configuring a custom ICA connection:
    - Right-click the custom ICA connection you want to configure and select **Custom Connection Settings**. The **Custom ICA Connections** dialog box appears.
3. Click **Add**. The **Add Server Location Address** window appears.
4. Enter the external Internet address of the MetaFrame server.
5. Click **OK**. The newly added external Internet address of the MetaFrame server appears in the Address List.
6. Click **Firewalls**.
7. Select **Use alternate address for firewall connection**.
8. Click **OK** twice.

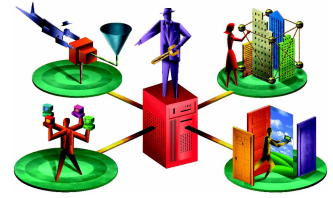
---

**Note** All MetaFrame servers in the farm must be configured with their alternate (external) address. See the *MetaFrame XP Server Administrator's Guide* for more information.

---



# Updating the ICA Win32 Clients



This chapter explains how to deploy ICA Client updates across your network. The following topics are covered:

- The ICA Client Update Process
- Using the Client Update Configuration Utility
- Specifying a Default Client Update Database
- Configuring Default Client Update Options
- Adding ICA Clients to the Client Update Database
- Working with the ICA Win32 Client Downloaded from the Citrix Web Site
- Removing an ICA Client From the Client Update Database
- Changing the Properties of the ICA Win32 Client

## About the Client Auto Update Feature

The ICA Win32 Program Neighborhood Agent and the ICA Win32 Program Neighborhood Client are available as Microsoft Windows Installer (.msi) packages. If your network is based on Windows 2000 or later, you can take advantage of Microsoft Systems Management Server or Active Directory to deploy updated versions of these clients using the Windows Installer packages.

To deploy updates to the ICA Win32 Web Client, or if your network does not have Systems Management Server or Active Directory Services available, you can use the Client Auto Update feature to deploy and install ICA Client updates using self-extracting executable (.exe) files.

The Client Auto Update feature is a convenient network management tool. It monitors client version numbers as users log on to a MetaFrame server and updates client installations network-wide as appropriate to a version you specify.

Typically, you use Client Auto Update to deploy the latest release of the ICA Win32 Clients on your network. You can also use this feature to revert to a previous version of a client. Visit the Citrix Web site at <http://www.citrix.com/download> frequently for the latest releases and documentation of the ICA Win32 Clients.

As new versions of ICA Clients become available, you add them to the client update database. When an ICA Client logs on to a MetaFrame server, the server queries the client to detect its version number. If the version matches the one in the client update database, the logon continues. Otherwise, the user is informed that an update to the client is available for download. The client is then updated according to the options you set in the database.

---

**Important** You cannot automatically update previous versions of the ICA Win32 Client installed with Windows Installer (.msi) packages. You must redeploy an ICA Win32 Client installer package when a new version of the ICA Client is released.

---

Client Auto Update works with all network protocols supported by ICA (TCP/IP, IPX, NetBIOS, and asynchronous). Client Auto Update:

- Automatically detects ICA Client versions
- Copies new files over any ICA connection without user intervention
- Provides administrative control of update options for each ICA Client
- Updates ICA Clients from a single database on a network share point
- Safely restores older ICA Client versions when needed

## The ICA Client Update Process

ICA Clients are identified by platform with a product and model number. The version number is assigned when new ICA Clients are released.

The process of updating ICA Clients with new versions uses the standard ICA protocol:

- By default, the MetaFrame server informs the user of newly available client updates and asks to perform the update. Optionally, you can specify that the update be performed without informing the user and without allowing the user to cancel the update.
- By default, users can choose between waiting for the download to complete and downloading the files in the background while they continue to work. Users connecting to the MetaFrame server with a modem get better performance waiting for the update process to complete. Optionally, you can force the client update to complete before allowing the user to continue.



- During the update, new ICA Client files are copied to the user's computer. Optionally, you can force the user to disconnect and complete the update before continuing the session. The user must log on to the MetaFrame server again to continue working.
- When the user disconnects from the server and closes all client programs, the ICA Client update process finishes.
- As a safeguard, the existing ICA Client files are saved to a folder named Backup in the Citrix\ICA Client subdirectory of the Program Files folder on the user's local disk.

## Configuring the Client Update Database

You can configure a client update database on each MetaFrame server in a server farm, or configure one database to update the ICA Clients for multiple MetaFrame servers.

The client update database contains several ICA Clients. As Citrix releases new versions of the ICA Clients, you add them to the client update database.

### Using the Client Update Configuration Utility

Use the Client Update Configuration utility to manage the client update database. From this utility, you can:

- Create a new update database
- Specify a default update database
- Configure the properties of the database
- Configure client update options
- Add new ICA Clients to the database
- Remove outdated or unnecessary ICA Clients
- Change the properties of an ICA Client in the database

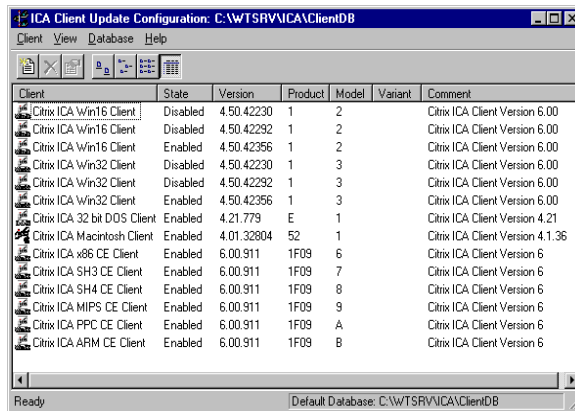
The following sections give an overview of the Client Update Configuration utility. For details, see the utility's online help.

► **To start the ICA Client Update Configuration utility**

1. From a MetaFrame XP server: From the **Start** menu, choose **Programs > Citrix > MetaFrame XP > ICA Client Update Configuration**.

From a MetaFrame 1.8 server: From the **Start** menu, choose **Programs > MetaFrame Tools > ICA Client Update Configuration**.

2. The **ICA Client Update Configuration** window appears. The status bar shows the location of the current update database, which the MetaFrame server uses to update ICA Clients. The window shows the ICA Clients in the database.



The screenshot shows the 'ICA Client Update Configuration' window with the following data:

Client	State	Version	Product	Model	Variant	Comment
Citrix ICA Win16 Client	Disabled	4.50.42230	1	2		Citrix ICA Client Version 6.00
Citrix ICA Win16 Client	Disabled	4.50.42292	1	2		Citrix ICA Client Version 6.00
Citrix ICA Win16 Client	Enabled	4.50.42356	1	2		Citrix ICA Client Version 6.00
Citrix ICA Win32 Client	Disabled	4.50.42230	1	3		Citrix ICA Client Version 6.00
Citrix ICA Win32 Client	Disabled	4.50.42292	1	3		Citrix ICA Client Version 6.00
Citrix ICA Win32 Client	Enabled	4.50.42356	1	3		Citrix ICA Client Version 6.00
Citrix ICA 32 bit DOS Client	Enabled	4.21.779	E	1		Citrix ICA Client Version 4.21
Citrix ICA Macintosh Client	Enabled	4.01.32804	52	1		Citrix ICA Client Version 4.1.36
Citrix ICA x86 CE Client	Enabled	6.00.911	1F09	6		Citrix ICA Client Version 6
Citrix ICA SH3 CE Client	Enabled	6.00.911	1F09	7		Citrix ICA Client Version 6
Citrix ICA SH4 CE Client	Enabled	6.00.911	1F09	8		Citrix ICA Client Version 6
Citrix ICA MIPS CE Client	Enabled	6.00.911	1F09	9		Citrix ICA Client Version 6
Citrix ICA PPC CE Client	Enabled	6.00.911	1F09	A		Citrix ICA Client Version 6
Citrix ICA ARM CE Client	Enabled	6.00.911	1F09	B		Citrix ICA Client Version 6

**Note** Citrix MetaFrame Server for UNIX Operating Systems does not use the Client Update Database. To use the client update database, you must have a MetaFrame or MetaFrame XP Server for Windows in your server farm.

## Creating a New Client Update Database

The ICA Client Distribution wizard creates the client update database in the location %SystemRoot%\Ica\ClientDB. You can create a new update database in any location on a server disk or on a network share point.

► **To create a new update database**

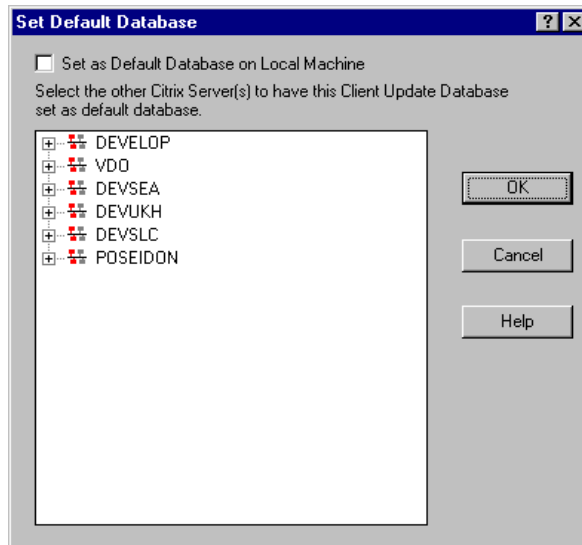
1. From the **Database** menu, choose **New**. The **Path for the new Client Update Database** dialog box appears.
2. Enter the path for the new update database and click **Save**. The utility creates a new update database in the specified location and opens the new database.

## Specifying a Default Client Update Database

You can configure one client update database to be used by multiple MetaFrame servers. If the client update database is on a shared network drive, use the ICA Client Update Configuration utility to configure your MetaFrame servers to use the same shared database.

► **To set the default database for MetaFrame servers**

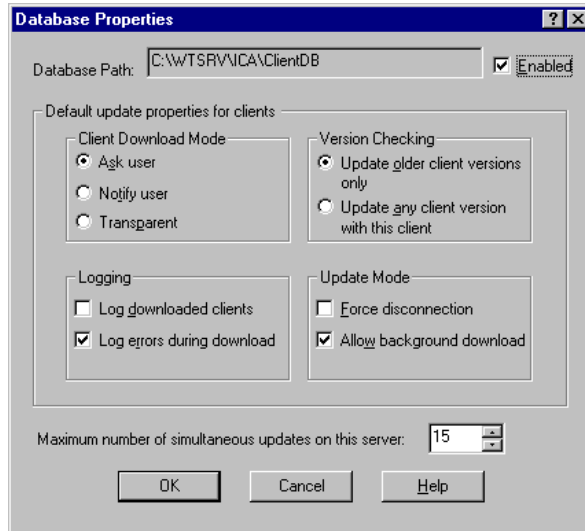
1. From the **Database** menu, choose **Open**.
2. Specify the path to the default database and click **Open**. The database opens.
3. On the **Database** menu, click **Set Default**. The **Set Default Database** dialog box opens:



4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other MetaFrame servers to use the currently open database as the default database.
5. Double-click a domain name to view the servers in that domain. Click a server to set its default database to the currently open database. Select multiple servers by holding down the CTRL key and clicking each server.
6. Click **OK**.

## Configuring Default Client Update Options

Use the **Database Properties** dialog box to configure overall database-wide settings for the current client update database. Choose **Properties** from the **Database** menu to display the dialog box.



- The **Database Path** box displays the path and file name of the database you are configuring.
- For this database to perform ICA Client updates, select **Enabled**.

---

**Tip** If the ICA Clients do not need to be updated, disable the database to shorten logon time.

---

- The options in the **Default update properties for clients** section specify the default behavior for the ICA Clients added to the database. You can also set properties for individual ICA Clients (as described later in this chapter). Individual ICA Client properties override the database properties.
- Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user's ICA Client software without notifying or asking the user.

- Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update both earlier and later versions of the client to this version; choose this option to force an older client to replace a newer client.
- Under **Logging**, select **Log downloaded clients** to write an event to the event log when a client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log errors during download** check box to turn this option off.
- Under **Update Mode**, select the **Force disconnection** option to require users to disconnect and complete the update process after downloading the new client. The **Allow background download** option is selected by default to allow users to download new client files in the background while they continue to work. Clear this check box to force users to wait for all client files to download before continuing.
- Specify the number of simultaneous updates on the server. When the specified number of updates is reached, new client connections are not updated. When the number of client updates is below the specified number, new client connections are updated.

Click **OK** when you finish configuring the database settings.

## Adding ICA Clients to the Client Update Database

To deploy a newer version of the ICA Win32 Client, add it to the client update database. You can download the latest ICA Clients from the Citrix Web site at <http://www.citrix.com/download>.

## Working with the ICA Win32 Client Downloaded from the Citrix Web Site

If you downloaded a new version of the ICA Win32 Program Neighborhood Client, you must first extract the files from the Ica32.exe file before you can add the client to the client update database.

► **To extract files from Ica32.exe**

1. Copy Ica32.exe to the root of your MetaFrame server's hard drive.
2. Create a directory to contain the extracted files.
3. At a command prompt, type:

```
Ica32.exe /a /extract /path c:\samplepath
```

where *samplepath* is the path to the directory you created in Step 2.

► **To add a Citrix ICA Client to the Client Update Database**

1. From the **Client** menu, click **New** to display the **Description** screen.
2. In the **Client Installation File** box, browse to or enter the path to the client installation file Update.ini. If you ran the ICA Client Distribution wizard, you can find the Update.ini file in System32\Clients\Ica. You can also find the Update.ini file on the MetaFrame XP Components CD.
3. The client name, product number, model number, and version number are displayed. The **Comment** text box displays a description of the new client. You can modify this comment.
4. Click **Next** to continue.
5. The **Update Options** dialog box appears. The options on this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients. The options available in this dialog box are discussed in the online Help for this dialog box.  
Click **Next** when you finish configuring the client update options.
6. The **Event Logging** dialog box appears. The database-wide logging options are displayed. You can specify different behavior for individual clients.
7. Select **Log Downloaded Clients** to write an event to the event log when this client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log Errors During Download** check box to turn this option off.
8. Click **Next**.

9. The **Enable Client** dialog box appears. The client update database can contain multiple versions of an ICA Client with the same product and model numbers. However, only one version of the client can be enabled. The enabled client is used for client updating. Click **Finish** to copy the ICA Client installation files to the client update database.

## Removing an ICA Client From the Client Update Database

It is important to delete ICA Clients that are not used from the client update database. A database with multiple versions of the same client unnecessarily slows the checking procedure that is carried out each time a user connects to the server.

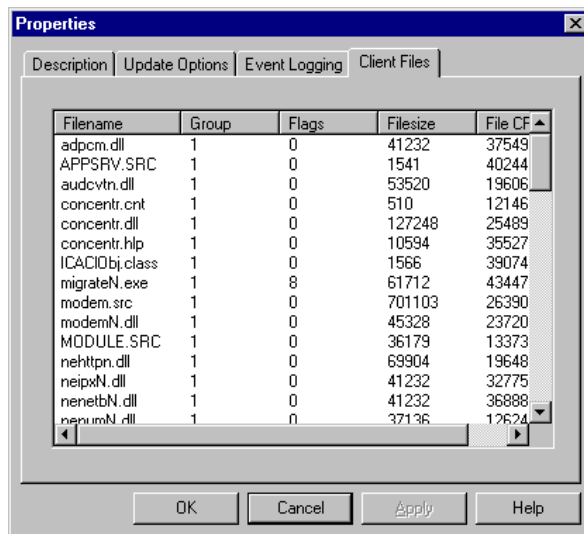
- ▶ **To remove the ICA Win32 Client from the database**
  1. Select the Win32 Client you want to remove from the database.
  2. From the **Client** menu, choose **Delete**. A message box asks you to confirm the deletion.
  3. Click **Yes** to remove the client.

## Changing the Properties of the ICA Win32 Client

Use the **Properties** dialog box to set properties for an individual ICA Client. Individual ICA Client properties override the database properties.

- ▶ **To change the properties of the ICA Win32 Client**
  1. Select the Win32 Client.
  2. On the **Client** menu, choose **Properties**. The **Properties** dialog box appears, containing tabs labeled **Description**, **Update Options**, **Event Logging**, and **Client Files**.
  3. The **Description** tab of the **Properties** dialog box lists the client name, product number, model number, and version number.  
Select **Enabled** to update the same platform ICA Client to this version.  
Optionally, enter a new comment in the **Comment** text box.
  4. Use the **Update Options** tab to configure update options for the client.
    - Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user's ICA Client software without notifying or asking the user.

- Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update all client versions to this version. Select this option to force an older client to replace a newer client.
  - Select the **Force Disconnection** option to require users to disconnect and complete the update process after downloading the new client.
  - Select the **Allow Background Download** option to allow users to download new client files in the background while they continue to work. Clear this check box to force users to wait for all client files to download before continuing.
  - Type a message to be displayed to users when they connect to the server.
5. Use the **Event Logging** tab to configure logging settings for this client.
    - Select the **Log Downloaded Clients** option to write an event to the event log when a client is updated.
    - Select the **Log Errors During Download** option to write errors that occur during a client update to the event log.
  6. Use the **Client Files** tab to view the list of files associated with this client.



The client update database stores the following information about each client file: file name, group, flags, file size, and file CRC.

7. Click **OK** when you finish configuring the settings for the client.



# Index

## A

- ALE 107
- Application Display tab 46
- application launching and embedding 107
- Application Refresh tab 47
- application sets 73
  - adding 73
- audio support 26, 46, 76, 105
- auto client proxy detection 118
- auto client reconnect 23, 93

## C

- certificate revocation list checking 20, 90
- certificates - built in 126
- Citrix SSL Relay 124
- Citrix Web site 10
  - product documentation 10
- Citrix XML Service 69
- Client Auto Update 25, 136
- client auto update 24, 135
- client device mapping 26
  - client COM port mapping 26
  - client drive mapping 26
  - client printer mapping 26
- client tab control 45
- Client Update Configuration Utility 137
- Client Update Database 137
  - adding clients 141
  - changing client properties 143
  - creating a new database 138
  - removing clients 143
  - specifying a default database 139
- configuration files 39, 42–47
- connection properties
  - configuring 74
- connections
  - configuring 70
- content redirection 21
- creating client installation disks 31
- custom ICA connections 73
  - adding 73

## D

- default options
  - configuring (Program Neighborhood Client) 75
- deploying the ICA Win32 Clients 29
  - creating an ICA Client download Web site 30
  - creating client installation disks 31
    - from a network share point 30
    - on servers running Windows Server 2003 31
- dialing prefix 27
- DNS name resolution 24
  - disabling 96
- dynamic client name 19

## E

- encryption 122
- enhanced content publishing 22, 92
- event logging
  - configuring 85
- extended parameter passing 25
  - enabling 92

## F

- finding more information 9
- FIPS 140 128
- firewalls 132
- FQDN 124
- full screen seamless mode 111
- fully qualified domain name 124

## G

- general settings
  - configuring (Program Neighborhood Client) 82

## I

- ICA Clients
  - downloading from the Citrix Web site 10
- ICA Win32 Clients
  - configuring common features 89
  - existing features 20
  - new features 17
- In 112

Installing 54

installing

- Program Neighborhood Agent 36
  - with the self-extracting executable 39
  - with the Windows Installer package 37
  - with Windows Installer package 37
- Program Neighborhood Client 60
  - with the Windows Installer package 60
- Web Client 53

Internet proxy support 22

## L

local text echo 77

logon methods 45

logon mode

- configuring (Program Neighborhood Client) 77

## M

mapping

- client audio 105
- client COM ports 105
- client devices 101
- client drives 102
- client printers 103

MetaFrame for UNIX 111

mouse click feedback 77

multiple monitors

- configuring 106

## N

NDS 93

- context (Program Neighborhood Agent) 38
- context (Program Neighborhood Client) 62, 95

new features 17

- certificate revocation list checking 20
- dynamic client name 19
- Program Neighborhood Agent Admin tool 18
- SpeedScreen Browser Acceleration 19
- Universal Print Driver 20
- Windows NT Challenge/Response (NTLM) support 20

Notes 10

Novell Directory Services 24, 93

NTLM 90

## O

Overview 57

## P

pass-through authentication

- enabling when installing Program Neighborhood Agent 41

Program Neighborhood Client 79

product documentation 10

Program Neighborhood Agent

- configuring 42
    - contents of the Properties dialog box 44
    - for silent user installation 38–39, 63
    - server URL 47
    - to use SSL/TLS 127
  - configuring with the Program Neighborhood Agent Admin tool 42
  - customizing using Program Neighborhood Agent Admin tool 44
  - installing with the self-extracting executable 39
  - installing with the Windows Installer package 37
- Program Neighborhood Agent Admin tool 18
- Program Neighborhood Client
- application sets and custom ICA connections 73
  - configuring
    - bitmap caching 83
    - connection properties 74
    - connections 70
    - default options 75
    - event logging 85
    - for silent user installation 61
    - general settings 82
    - hotkeys 84
    - logon mode 77

installing with the Windows Installer package 60, 62

starting 66

system requirements 59

proxy servers

- auto client proxy detection 119
- client configuration 118
- user name and password for 120

published content 24

## R

roaming user reconnect 23

root certificates

- installing on client devices 128

## S

Save password option

- Program Neighborhood Client 80

seamless windows 25, 111  
Secure Gateway 22, 122  
security measures 117  
Selecting 48  
self-extracting executable  
    configuring for silent user installation  
        Program Neighborhood Agent 39, 63  
        Web Client 52  
    installing the Program Neighborhood Agent with 39  
    installing the Program Neighborhood Client with 60  
    installing the Web Client with 53  
Server Settings 45  
Server tab 45  
Session Options tab 46  
smart card logon  
    (Program Neighborhood Agent, configuring client-side) 92  
    (Program Neighborhood Agent, configuring server-side) 131  
    (Program Neighborhood Client) 77  
smart card support 21  
sound 87  
sound support 26, 46, 76, 105  
SpeedScreen Browser Acceleration 19, 90  
SSL  
    installing root certificates on client devices 128  
    system requirements on client devices 124  
system requirements 36  
    Program Neighborhood Client 59  
    Web Client 51

## T

TAPI modems 27  
TCP/IP+HTTP server location 71  
time zone 26

TLS  
    definition 122  
    forcing 126  
    installing root certificates on client devices 128  
    system requirements on client devices 124  
TLS support 22

## U

Universal Print Driver 20  
UNIX applications 111  
user-to-user shadowing 20, 91  
Using 32

## W

Web Client  
    configuring for silent user installation 52  
    installing 53  
    system requirements 51  
Web Interface 22  
Windows 90  
Windows Installer packages  
    configuring for silent user installation  
        Program Neighborhood Agent 38  
        Program Neighborhood Client 61  
    installing the Program Neighborhood Agent with 37  
    installing the Program Neighborhood Client with 60, 62  
    installing the Web Client with 24  
Windows NT Challenge/Response (NTLM) support 20, 90

## X

XML Service 69

