

# Administrator's Guide

**Citrix® MetaFrame XP™**  
**Application Server for Windows**  
Version 1.0

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 © 2001 Citrix Systems, Inc. All rights reserved.

Citrix, ICA (Independent Computing Architecture), Independent Management Architecture (IMA), Program Neighborhood, MetaFrame, MetaFrame XP, and NFuse are registered trademarks or trademarks of Citrix Systems, Inc. in the U.S.A. and other countries.

RSA Encryption (c) 1996-1997 RSA Security Inc., All Rights Reserved.

Microsoft, MS, MS-DOS, Windows, Windows NT, and Windows 2000 Servers are registered trademarks or trademarks of Microsoft Corporation in the U.S.A and other countries.

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

Document Code mfxpw.ag.rcd.1f.20001215

---

# Contents

|                                                    |           |
|----------------------------------------------------|-----------|
| <b>Chapter 1 Welcome</b>                           | <b>9</b>  |
| MetaFrame XP Documentation                         | 10        |
| Using PDF Documentation                            | 10        |
| Documentation Conventions                          | 11        |
| Using Online Help                                  | 12        |
| Finding Information About Windows Servers          | 12        |
| Citrix on the World Wide Web                       | 13        |
| Reader Comments                                    | 13        |
| <b>Chapter 2 Introduction to MetaFrame XP</b>      | <b>15</b> |
| Overview of Server-Based Computing                 | 15        |
| MetaFrame XP Application Servers                   | 17        |
| Independent Computing Architecture and ICA Clients | 18        |
| Citrix ICA Clients                                 | 18        |
| ICA and Client Devices                             | 21        |
| Citrix Server Farms                                | 21        |
| Independent Management Architecture (IMA)          | 22        |
| Citrix Management Console                          | 23        |
| Citrix NFuse                                       | 23        |
| Citrix Management Products                         | 24        |
| Features of MetaFrame XP for Windows               | 26        |
| Application Server Features                        | 26        |
| Citrix ICA Client Features                         | 27        |
| New Features in MetaFrame XP                       | 28        |

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| <b>Chapter 3 Planning Your MetaFrame XP Deployment. . . . .</b> | <b>31</b> |
| System Requirements. . . . .                                    | 31        |
| System Software Requirements . . . . .                          | 32        |
| System Hardware Requirements . . . . .                          | 33        |
| Sizing Systems for MetaFrame XP . . . . .                       | 35        |
| Choosing a Database for the Data Store . . . . .                | 37        |
| System Sizing for the Data Store Database . . . . .             | 38        |
| Data Store Database Requirements . . . . .                      | 39        |
| Network Configuration and Account Authority Issues. . . . .     | 40        |
| General Configuration Issues . . . . .                          | 41        |
| Recommendations for Active Directory. . . . .                   | 41        |
| User Access to Applications and Printers . . . . .              | 43        |
| Active Directory Security Model and Restrictions . . . . .      | 44        |
| Configuring Citrix Administrator Accounts . . . . .             | 48        |
| Planning for Client and Server Communications . . . . .         | 49        |
| Linking ICA Clients and MetaFrame XP Servers . . . . .          | 50        |
| Configuring ICA Browsing . . . . .                              | 51        |
| Communicating with the Citrix XML Service. . . . .              | 54        |
| Configuring Network Firewalls . . . . .                         | 56        |
| Server Farm Configurations . . . . .                            | 56        |
| ICA Browsers and MetaFrame 1.8 Interoperability. . . . .        | 60        |
| Naming the Server Farm . . . . .                                | 62        |
| Changing Server Drive Letters . . . . .                         | 62        |
| Configuring Session Shadowing . . . . .                         | 64        |
| Interoperability with MetaFrame 1.8. . . . .                    | 65        |
| Configuring MetaFrame XP for Mixed Mode Operation . . . . .     | 65        |
| Pooling Licence Counts in Mixed Mode . . . . .                  | 67        |
| Using MetaFrame XP Tools in Mixed Mode. . . . .                 | 68        |

---

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b>Chapter 4 Installing MetaFrame XP</b>                    | <b>71</b> |
| Creating the Data Store with SQL Server or Oracle           | 71        |
| Authenticating to the Data Store during Setup               | 72        |
| Starting MetaFrame XP Installation                          | 74        |
| Choosing Options During Setup                               | 74        |
| Data Store Configuration                                    | 74        |
| Configuring Network ICA Connections                         | 80        |
| Configuring Asynchronous ICA Connections                    | 81        |
| Installing ICA Client Software                              | 82        |
| Entering Licenses and Product Codes                         | 83        |
| NFuse Web Server Extension                                  | 84        |
| Migrating Citrix Servers to MetaFrame XP                    | 84        |
| Supported Migration Paths                                   | 85        |
| Changing the Citrix XML Service Port                        | 86        |
| Setting Up Citrix SSL Relay                                 | 87        |
| Obtaining a Server Certificate                              | 88        |
| Changing the SSL Relay Port                                 | 88        |
| Installing a Server Certificate                             | 89        |
| Unattended Setup of MetaFrame XP Servers                    | 90        |
| Cloning a MetaFrame XP Server                               | 90        |
| Uninstalling MetaFrame XP                                   | 92        |
| Installing Citrix Management Console on Other Computers     | 92        |
| <b>Chapter 5 Configuring MetaFrame XP Servers and Farms</b> | <b>95</b> |
| Management Tools for MetaFrame XP                           | 95        |
| Overview of MetaFrame XP Management Tools                   | 96        |
| The ICA Administrator Toolbar                               | 97        |
| Citrix Management Console                                   | 99        |
| Using Citrix Management Console                             | 100       |
| Data Displayed in Citrix Management Console                 | 102       |
| Controlling Access to Citrix Management Console             | 104       |
| Configuring MetaFrame XP Properties                         | 106       |
| Properties of MetaFrame XP Server Farms                     | 106       |
| Using the Farm Properties Dialog Box                        | 107       |
| Configuring Zones and Data Collectors                       | 110       |
| MetaFrame XP Server Properties                              | 113       |
| Using the Server Properties Dialog Box                      | 114       |
| Configuring Latency Reduction for ICA Clients               | 116       |
| Deploying SpeedScreen Settings                              | 116       |

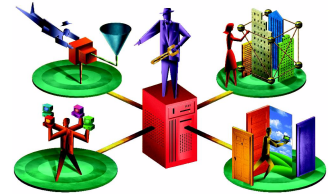
|                                                               |                |
|---------------------------------------------------------------|----------------|
| <b>Chapter 6 Licensing MetaFrame XP</b> .....                 | <b>119</b>     |
| Overview of Citrix Licensing. ....                            | 119            |
| Summary of the Licensing Process .....                        | 120            |
| Types of MetaFrame XP Licenses. ....                          | 122            |
| Product Licenses .....                                        | 122            |
| Connection Licenses .....                                     | 123            |
| Migrating Licenses from Other Citrix Products. ....           | 123            |
| Upgrading Licenses .....                                      | 124            |
| Understanding Citrix Licensing Codes .....                    | 124            |
| Product Codes .....                                           | 125            |
| Serial Numbers .....                                          | 127            |
| License Numbers .....                                         | 128            |
| License Activation Codes .....                                | 129            |
| Managing and Monitoring Licenses .....                        | 129            |
| Adding Licenses to Server Farms. ....                         | 130            |
| Activating Licenses. ....                                     | 131            |
| License Views .....                                           | 131            |
| Managing License Counts .....                                 | 134            |
| Pooling License Counts .....                                  | 135            |
| Assigning License Counts .....                                | 135            |
| Removing Licenses. ....                                       | 136            |
| Client Device Licensing .....                                 | 136            |
| <br><b>Chapter 7 Configuring ICA Client Connections</b> ..... | <br><b>137</b> |
| Configuring ICA Connections and Sessions .....                | 137            |
| Setting up ICA Connections .....                              | 138            |
| Adding ICA Connections .....                                  | 139            |
| Configuring Session Settings for ICA Clients. ....            | 142            |
| Precedence of Settings .....                                  | 143            |
| Configuring Connection Methods for Sessions .....             | 143            |
| Configuring Advanced ICA Connection Options .....             | 149            |
| Configuring ICA Session Shadowing .....                       | 150            |
| Configuring ICA Audio Settings .....                          | 152            |
| Configuring Client Device Mapping .....                       | 153            |
| Options for Client Device Mapping .....                       | 154            |

---

|                                                          |            |
|----------------------------------------------------------|------------|
| <b>Chapter 8 Deploying ICA Clients to Users</b>          | <b>159</b> |
| Choosing a Deployment Method                             | 159        |
| Delivering Applications to Users                         | 160        |
| Determining the Scope of ICA Client Deployment           | 162        |
| Using the ICA Client CD                                  | 163        |
| Pass-Through ICA Client                                  | 164        |
| ICA Client Object                                        | 164        |
| Deploying the ICA Clients                                | 165        |
| Web-Based Installation                                   | 165        |
| Deploying ICA Clients Over a Network                     | 168        |
| Deploying ICA Clients Using Diskettes                    | 169        |
| Updating the ICA Clients                                 | 169        |
| The ICA Client Update Process                            | 170        |
| Configuring the Client Update Database                   | 172        |
| Using the Client Update Configuration Utility            | 172        |
| Creating a New Client Update Database                    | 173        |
| Specifying a Default Client Update Database              | 173        |
| Configuring Default Client Update Options                | 174        |
| Adding ICA Clients to the Client Update Database         | 176        |
| Removing an ICA Client From the Client Update Database   | 180        |
| Changing the Properties of an ICA Client in the Database | 181        |
| ICA Client Deployment Practices                          | 184        |
| Manufacturing Enterprise                                 | 184        |
| Regional Bank                                            | 186        |
| Application Service Provider                             | 186        |
| Insurance Company                                        | 187        |
| <b>Chapter 9 Publishing Applications</b>                 | <b>189</b> |
| Introduction to Publishing Applications                  | 189        |
| User Access to Published Applications                    | 190        |
| Using Program Neighborhood                               | 190        |
| Administrative Control of Applications                   | 192        |
| Types of Applications You Can Publish                    | 193        |
| Using Published Applications                             | 194        |
| Configuring User Access to Applications                  | 195        |
| Publishing Applications                                  | 197        |
| Creating an ICA File                                     | 197        |
| Creating an HTML File                                    | 198        |
| Removing Published Applications                          | 198        |

|                                                     |            |
|-----------------------------------------------------|------------|
| <b>Chapter 10 Managing Users and ICA Sessions</b>   | <b>199</b> |
| Managing ICA Sessions                               | 199        |
| Controlling Logons by ICA Clients                   | 199        |
| Viewing Information About ICA Sessions              | 200        |
| Using Session Management Commands                   | 201        |
| Shadowing ICA Sessions                              | 204        |
| <b>Chapter 11 Managing Printers for ICA Clients</b> | <b>207</b> |
| Overview of Printing with MetaFrame XP              | 208        |
| Configuration of Printing Devices                   | 208        |
| Printing Configuration in Server Farms              | 209        |
| Printing Configuration Scenarios                    | 210        |
| Printer Management Features                         | 211        |
| Printer Management Views in the Console             | 212        |
| Setting Up Network Printers for ICA Client Users    | 216        |
| Installing and Replicating Printer Drivers          | 217        |
| Mapping Printer Drivers                             | 218        |
| Managing Drivers for Client Printers                | 219        |
| Autocreation of Client Printers for DOS and WinCE   | 220        |
| Limiting Printing Bandwidth in ICA Sessions         | 220        |
| ICA Client Settings for Printer Access              | 221        |
| <b>Appendix A MetaFrame XP Commands</b>             | <b>223</b> |
| ALTADDR                                             | 224        |
| APP                                                 | 226        |
| AUDITLOG                                            | 229        |
| CHANGE CLIENT                                       | 231        |
| CHFARM                                              | 235        |
| CLICENSE                                            | 236        |
| CLTPRINT                                            | 239        |
| CTXXMLSS                                            | 240        |
| DSMAINT                                             | 241        |
| ICAPORT                                             | 245        |
| QUERY                                               | 246        |
| TWCONFIG                                            | 254        |
| <b>Appendix B Glossary</b>                          | <b>257</b> |
| <b>Index</b>                                        | <b>265</b> |

# Welcome



Welcome to server-based computing with Citrix MetaFrame XP application server software.

MetaFrame XP is the server-based computing solution for organizations and large enterprises. MetaFrame XP provides integrated management capabilities for system administrators, along with ease of use and productivity enhancements for end-users who access applications on MetaFrame XP servers using Citrix ICA Clients.

This chapter describes the documentation provided with MetaFrame XP and additional resources for you to find more information about MetaFrame XP and related Citrix products.

This chapter includes the following topics:

- MetaFrame XP Documentation, page 10
- Finding Information About Windows Servers, page 12
- Citrix on the World Wide Web, page 13

---

**Important** Please be sure to read the **MetaFrame\_XP\_Readme.txt** file in the root directory of the MetaFrame XP CD-ROM. This file contains important information that includes last-minute documentation updates and corrections.

Citrix provides a variety of information resources online, including a complete product documentation library, documentation updates, and technical articles on the Citrix Web site at <http://www.citrix.com>.

---

## MetaFrame XP Documentation

The Citrix MetaFrame XP package includes electronic documentation and online application help.

The documentation included with MetaFrame XP is available in the DOC directory on the MetaFrame XP CD-ROM. Documentation for ICA Client software is available on the ICA Client CD-ROM.

On a MetaFrame XP server, documentation is installed in a Documentation folder. You can display the contents of this folder by choosing **Programs > Citrix > Documentation** from the **Start** menu.

The following documentation is included with MetaFrame XP in Adobe PDF format:

- This manual, the *MetaFrame XP Administrator's Guide*, provides conceptual information and procedures for system administrators who install, configure, and maintain MetaFrame XP for Windows. To get the most out of the guide, review the table of contents to familiarize yourself with the topics included in the book.
- The MetaFrame\_XP\_Readme.txt file contains last minute updates, corrections to the documentation, and a list of known problems. This file is in the root directory of the MetaFrame XP CD-ROM.
- The *Citrix NFuse Administrator's Guide* tells administrators how to install, configure, and customize NFuse.
- The *Citrix ICA Client Administrator's Guides* provide instructions for system administrators who deploy ICA Clients to end-users on various computing platforms.

This manual is available in the following locations:

- In the \Doc directory of your MetaFrame XP CD-ROM
- Installed into the Documentation folder of your MetaFrame XP server. From the **Start** menu, choose **Programs > Citrix > Documentation**.
- On the Citrix Web site at <http://www.citrix.com/support>, select the Product Documentation tab. You can check the Product Documentation area of the Web site at any time for the latest updates to Citrix technical manuals. Any updates to this manual published after the release of this product will be posted there.

## Using PDF Documentation

To use the MetaFrame XP and ICA Client documentation that is provided in PDF files, you need to have the Adobe Acrobat Reader program. The Reader program lets you view, search, and print the documentation files.

If you need to obtain the Reader program, you can download it for free from Adobe System's Web site (<http://www.adobe.com>). The self-extracting file includes installation instructions.

## Documentation Conventions

MetaFrame XP documentation uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

| 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 at a command prompt or 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.                     |
| [ 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                                                                                                                                                                            |

## Using Online Help

Online help is available for the Citrix Management Console and the other tools that are included with MetaFrame XP.

You can access online help from the Help menu of each program; the program must be running for you to view its online help. You can use shortcuts to launch MetaFrame XP utilities and the Citrix Management Console. Shortcut icons are located in the MetaFrame XP folder. To open this folder, click the **Start** menu and choose **Programs > Citrix > MetaFrame XP**.

Online help for the Citrix Management Console is in JavaHelp format and requires the Java Run-Time Environment (JRE), which MetaFrame XP installs by default on the server. Online help for server utilities and the Windows ICA Clients is in WinHelp format, which is available by default on all Windows systems. Online help for other ICA Clients uses standard help formats for their platforms.

Citrix ICA Client software for all platforms includes online help for using applications and configuration settings. Help is available from Help menus or Help buttons in the ICA Clients.

## Finding Information About Windows Servers

Most compatibility guidelines for Windows NT Server 4.0, Terminal Server Edition, and Windows 2000 Servers can be applied to Citrix MetaFrame XP because MetaFrame XP is designed to run with these products.

For example, MetaFrame XP supports the deployment of Win32, Win16, DOS, OS/2 1.x (text only), and POSIX applications. The ICA technology included in MetaFrame XP extends the capabilities of Windows servers and, in some cases, requires additional setup and configuration for best application performance.

- For Windows 2000, information on application compatibility and deployment issues is available at the Microsoft Web site at <http://www.microsoft.com/Windows2000>
- For Windows NT 4, Terminal Server Edition, information on application compatibility and deployment issues is available at <http://www.microsoft.com/ntserver>

For instructions on installing and using Windows servers, see the Microsoft documentation included in your Windows package and the Microsoft Web site (<http://www.microsoft.com>).

## 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 MetaFrame XP administrators, including the following:

- Citrix Product Documentation Library containing the latest documentation for all Citrix products (at <http://www.citrix.com/support>, select Product Documentation)
- Downloadable Citrix ICA Clients (at <http://www.citrix.com/download>)
- Program information on Citrix Preferred Support Services options
- An FTP server containing the latest service packs, hotfixes, utilities, and product literature for download
- An online Solution Knowledgebase 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
- Frequently Asked Questions pages with answers to common technical and troubleshooting questions
- 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 new, open enrollement 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 Citrix server-based computing solutions into their products.

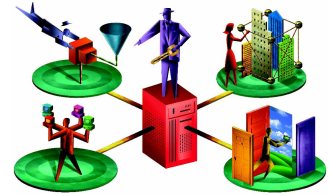
## Reader Comments

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



# Introduction to MetaFrame XP



This chapter introduces MetaFrame XP and Citrix server-based computing. The product information and concepts in this chapter can help you plan for deployment of Citrix server-based computing. The chapter includes the following topics:

- Overview of Server-Based Computing, page 15
- MetaFrame XP Application Servers, page 17
- Independent Computing Architecture and ICA Clients, page 18
- Citrix Server Farms, page 21
- Features of MetaFrame XP for Windows, page 26

## Overview of Server-Based Computing

Heterogeneous computing environments are a fact of life in the enterprise today. Computing infrastructures typically are built around incompatible parts, including an installed base of various client devices (PCs, terminals, network computers, portables), different operating systems, multiple network protocols, and various types of network connections.

Regardless of differences in computing environments, enterprises need to make applications available to all of their users. MetaFrame XP can bridge differences in computing environments. MetaFrame XP allows organizations to keep their desktops of choice and provide the best application fit for users and the enterprise.

Citrix MetaFrame XP application servers and Independent Computing Architecture (ICA) Client software are designed to meet the needs of all types of businesses, including large enterprises and application service providers (ASPs), whose customers require robust, easily managed, and cost-effective delivery of Windows applications to a variety of client devices.

Because the ICA protocol developed by Citrix supports all types of hardware, operating platforms, network connections, and network protocols, it lets organizations deliver a common set of applications to different types of client devices and to users in separate locations with better performance than alternative technologies.

Because MetaFrame XP centralizes application installation and management, it simplifies administration and unifies the enterprise computing environment. Citrix technologies and MetaFrame XP deliver solutions with a variety of benefits for application deployment throughout the enterprise:

**Seamless desktop integration.** MetaFrame XP provides a familiar user experience because it enables complete access to local system resources, such as 16-bit stereo audio, local drives, COM ports, local printers, and the Windows clipboard. Applications look, feel, and perform as though they are running locally, even though applications run remotely on the MetaFrame XP server. Users need no additional training because they continue working in their familiar personal computing environments.

Printer management features in Citrix Management Console simplify printer configuration, providing users with more flexibility and access to local printers. The business recovery feature in ICA Client software provides reliable backup connections to ensure users have consistent access to published applications.

**Any client device.** MetaFrame XP extends Windows applications to virtually any client device and platform, including all Windows platforms (Windows 3.1, Windows for Workgroups 3.11, Windows 95, Windows 98, Windows Me, Windows 2000, and Windows CE) as well as non-Windows client platforms including DOS, UNIX, Linux, OS/2 Warp, Macintosh, and Java.

**Any network connection.** Users can connect to networked MetaFrame XP servers through standard telephone lines, WAN links (T1, T3, 56Kb, X.25), broadband connections (ISDN, Frame Relay, ATM), wireless and CDPD connections, and the Internet. The unique bandwidth-conserving nature of Citrix's ICA protocol makes it an efficient solution for any network type, whether dial-up, LAN, WAN, Internet, Intranet, or wireless. ICA performance is fast and consistent, regardless of network infrastructure.

**Any network protocol.** MetaFrame XP supports ICA connections over TCP/IP, IPX/SPX, NetBIOS, SLIP/PPP, and asynchronous protocols. The Citrix ICA protocol is optimized for low-speed connections (28.8Kbps is the recommended minimum speed). Dial-in async support eliminates the need to configure a RAS server or RAS connection for client computers.

Server-based computing is a logical, efficient paradigm for today's networking environments. Server-based computing helps organizations simplify application deployment and administration, and thereby reduce the total cost of ownership of their application services.

The components and technologies that enable Citrix server-based computing include MetaFrame XP application servers, ICA Client software, the ICA protocol, and Independent Management Architecture (IMA), the foundation layer that unifies Citrix server-based computing solutions.

Citrix server-based computing is built on several key components:

**Multiusers operating system.** Server-based computing requires an operating system that allows multiple concurrent users to log on and run applications in separate, protected sessions on a single server. MetaFrame XP runs on Windows NT Server 4.0, Terminal Server Edition, and Windows 2000 Servers (Server, Advanced Server, or Datacenter Server). In these server operating systems, MultiWin technology licensed from Citrix provides the multiuser capabilities.

**MetaFrame XP server software.** MetaFrame XP is the application server component of Citrix's server-based computing solutions. The MetaFrame XP product incorporates Citrix's ICA protocol. The ICA protocol separates an application's logic from its user interface, so that only keystrokes, mouse clicks, and screen updates (with required data such as sound) are sent across the network.

**Citrix ICA Clients.** End users access applications running on MetaFrame XP servers using ICA Client software installed on their client devices. ICA lets virtually any type of client device access applications over any type of network connection, including LAN, WAN, dial-up, and direct asynchronous connections. Because ICA does not download applications to client devices (as in the Network Computing architecture), application performance is not limited by bandwidth or device performance.

## MetaFrame XP Application Servers

MetaFrame XP Application Server for Windows Version 1.0 is Citrix's advanced server-based computing solution for Microsoft Windows servers. The MetaFrame XP product incorporates Citrix's ICA protocol and provides high-performance, cost-effective, and secure ways to deploy, manage, and access applications throughout an enterprise, regardless of client device or network connection.

MetaFrame XP provides the following benefits:

- Brings server-based computing to heterogeneous computing environments, providing access to shrink-wrapped and custom 32-bit Windows applications, regardless of client hardware, operating platform, network connection, or protocol.
- Offers enterprise-class server and client management, which allows IS professionals to scale, deploy, and support applications from a single location.
- Provides seamless user experience at the desktop by delivering Windows-based applications with exceptional performance that is independent of bandwidth.

## Independent Computing Architecture and ICA Clients

MetaFrame XP provides server-based computing to local and remote users through the Independent Computing Architecture developed by Citrix.

ICA is the foundation of Citrix server-based computing with MetaFrame XP and ICA Client software. In simplified terms, the ICA protocol transports an application's screens from a MetaFrame XP server to ICA Client users, and returns the users' input to the application on the server.

As an application runs on a MetaFrame XP server, MetaFrame XP intercepts the application's display data and uses the ICA protocol to send this data (on standard network protocols) to the ICA Client software running on the user's client device. When the user types on the keyboard or moves and clicks the mouse, the ICA Client sends this data to the application on the MetaFrame XP server.

The Citrix ICA protocol provides advanced capabilities and enhanced performance with Windows terminal services. ICA delivers high performance on high- and low-bandwidth connections. It requires minimal client workstation capabilities, and includes error detection and recovery, encryption, and data compression.

### Citrix ICA Clients

Citrix ICA Client software lets users connect to Citrix servers (MetaFrame XP, MetaFrame, and *WINFRAME*) and access applications. The ICA Client extends the reach of Windows, Java and UNIX-based applications to virtually any client platform or device, including: 286, 386, 486 and Pentium-based PCs, Windows-based terminals, network computers, wireless devices, ICA-based information appliances, RISC-based systems, PowerPCs, UNIX based computers, and X-based devices.

ICA clients are available for Windows, Macintosh, UNIX, Linux, EPOC, Windows CE, DOS, and Java operating systems, as well as Web browsers that use the ActiveX control or Netscape plug-in.

For detailed instructions on installing and configuring Citrix ICA Clients, refer to the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

## ICA Client Platforms

Citrix continually updates its ICA Clients to support varied client computing platforms and operating system versions.

The MetaFrame XP product package includes a CD-ROM containing current versions of all ICA Clients at the time of this server release.

Please visit the Citrix Web site download area at <http://www.citrix.com/download> for information on new and updated ICA Clients.

The ICA Client supports the following computing platforms:

**Windows 32-bit.** The ICA Win32 Client supports client devices running Windows 9x, Windows NT 3.51, NT 4.0 (Workstation and Server), and Windows 2000.

In addition, Citrix provides versions of the ICA Win32 Client that are installable as browser plug-ins and support Application Launching and Embedding with compatible browsers. Application launching is available with any Windows-based Web browser that supports configurable MIME types. Microsoft Internet Explorer 4 and later versions, and Netscape Navigator 4 and later versions also support application embedding.

**Windows 16-bit.** The ICA Win 16 Client supports client devices running Windows 3.1 or greater (running in enhanced mode) and Windows for Workgroups 3.11 or greater. It also supports client devices running OS/2 2.1, OS/2 Warp Connect 3.0, and OS/2 Warp 4.0.

**Windows CE.** The ICA Windows CE Client works with client devices running Windows CE 2.0 or later, including HPC, HPC Pro, PocketPC, and Palm form-factor devices. OEMs also include a WinCE Client on Windows Based Terminals.

**EPOC.** The ICA EPOC Client works with client devices running EPOC release 5. The EPOC client is downloadable from <http://www.citrix.com/download>.

**Java.** The ICA Client for Java is a full client application that works on most computing platforms. It can be used as an applet that supports application embedding with Web browsers that fully implement Sun's Java Virtual Machine (JVM) Version 1.1 or later.

**Macintosh.** The ICA Client for Macintosh supports Apple Macintosh (and compatible) computers that contain 680040 or PowerPC microprocessors, with the following operating system versions: System 7.1 or later with installation of Apple's Thread Manager; System 7.5.3; Mac OS 8 or later.

**UNIX.** The ICA UNIX Client is available for client devices running the following versions of UNIX:

- Linux x86: RedHat 6.1, SuSE 6.4, Slackware 7.0, Debian 2.2, and Caldera 2.4
- Linux ARM: Netwinder Linux, kernel Version 2.2.14
- SCO UnixWare 7 (UnixWare 2.1 and OpenServer 5 with Binary Compatibility Modules from SCO)
- Hewlett Packard HP-UX 10.x and above
- Sun Solaris 2.5.1 and above (SPARC); Version 2.6 and above (x86)
- Sun SunOS 4.1.4
- Silicon Graphics IRIX 6.2 and above
- Digital UNIX 3.2 and above
- IBM AIX 4.1.4 and above

**DOS.** ICA Clients for DOS are available in 32-bit and 16-bit versions. The 32-bit version provides more features than the 16-bit version, while requiring less conventional memory. The ICA Clients for DOS require DOS 4.0 or later and an i386 or better processor.

## Application Launching and Embedding

When you publish applications with MetaFrame XP, two methods are available to make the applications available through Web browsers. These methods, referred to as *Application Launching* and *Embedding* (ALE), let users connect to MetaFrame XP servers and use applications by simply clicking links on a Web page.

**Launching.** Application Launching refers to running an application in an application window that is separate from the Web browser window. When a user launches an application from a Web page, the application runs in a separate window and the user can continue to access other Web pages in the browser.

**Embedding.** Application Embedding refers to running an application in a Web page that is displayed in a Web browser window. The Web page can include instructions or other information, as well as HTML formatting that integrates the application into the page.

**NFuse application portals.** With Citrix NFuse, users can connect to applications through corporate application portals that present customized application sets. NFuse runs on a Web server and communicates with MetaFrame XP servers through Citrix XML service. When users click an application link on an application portal Web page, NFuse automatically downloads the appropriate ICA Client (if necessary) and launches the application.

## ICA and Client Devices

ICA enhances the user experience because it supports file system redirection for client drive mapping, print redirection for client printer mapping, and COM port redirection.

**Drive mapping.** Drive mapping allows disks on the Citrix server to be remapped so that ICA Client users can access their local disks by their usual local drive letters.

**Printer mapping.** Printer mapping allows a printer device on the Citrix server to be redirected to a printer that is defined on the client computer.

**COM port redirection.** COM port redirection allows a COM port on the client computer to be treated as a COM port on the Citrix server.

Configuration of these mappings is built into the standard Windows device redirection facilities. The client mappings appear as another network that presents the client devices as sharepoints to which a drive letter or printer port can be attached.

ICA also provides clipboard cut-and-paste and audio support for ICA Clients on Windows. Audio support allows application sounds and Wav files to be played on client devices.

In addition, ICA provides enhanced performance through intelligent caching of bitmaps, persistent caching to disk, and use of advanced algorithms to discard redundant screen changes and optimize display operations.

## Citrix Server Farms

Citrix server farms provide you with a flexible and robust way of deploying applications to ICA Client users. A Citrix server farm is a group of Citrix servers managed as a single entity. Servers share some form of physical connection. In addition, the servers in the server farm share a single IMA-based data store.

---

**Note** Citrix servers running MetaFrame 1.8 and earlier versions can be grouped in server farms for application publishing and centralized administration. However, MetaFrame 1.8 and earlier versions do not use an IMA-based data store for a server farm. MetaFrame XP servers cannot join an existing non-IMA server farm. For information on interoperability of MetaFrame XP with MetaFrame 1.8 servers, see “Interoperability with MetaFrame 1.8” on page 65.

---

MetaFrame XP uses the data store to centralize configuration information for a server farm in one location. The data store maintains information about the servers, applications, and Citrix administrators in the server farm. Creation of a data store and connection to the data store by each server is a part of MetaFrame XP setup.

## Independent Management Architecture (IMA)

MetaFrame XP incorporates the advanced Citrix server communications and management foundation, the Independent Management Architecture (IMA). The integration of the MetaFrame XP application server software with IMA is central to the enhanced functionality of MetaFrame XP and the scalability of Citrix's server-based computing solutions.

IMA is a unified, enterprise-wide platform for installation, management, maintenance, support, and security for your organization's server-based computing and application hosting services. It is both an architectural model and a protocol for server-to-server communications. IMA is constructed on a collection of core subsystems that define and control execution of Citrix products.

IMA enables MetaFrame XP servers to be arbitrarily grouped into server farms that do not depend on the physical locations of the servers. IMA allows MetaFrame XP servers to be in a single server farm even if the servers are on different network subnets.

With MetaFrame XP for Windows servers and the extensible Citrix IMA foundation, organizations gain a wide range of enterprise management and scalability features and options:

- Central administration of MetaFrame XP and other Citrix servers
- Centralized data store for all Citrix configuration data
- Centralized license management and pooling without license gateways
- ICA Client discovery of published applications without UDP broadcasts
- Logging of shadowed sessions
- Simple Network Management Protocol (SNMP) support
- Auditing of administration activity

While IMA and MetaFrame XP provide significant enhancements that facilitate enterprise application hosting, both MetaFrame XP and IMA support the current functionality of all existing ICA Client software from Citrix and will operate with an installed base of ICA Clients.

In addition to the Citrix Management Console, several Windows-based management utilities are included with MetaFrame XP. These utilities provide management and configuration features that are independent of the IMA system.

As the size of an organization increases from dozens to hundreds to thousands of users, additional MetaFrame XP servers can be added to the server farm. With IMA, MetaFrame XP installations can scale to multi-site, enterprise-level server-based computing scenarios, while administrators maintain complete control from any location.

## Citrix Management Console

The management interface for MetaFrame XP servers and server farms is the *Citrix Management Console*, an extensible Java-based tool that operates in the framework of IMA. The console communicates with MetaFrame XP servers and other IMA-based Citrix servers using the IMA protocol over TCP/IP.

Citrix Management Console and IMA allow management of MetaFrame XP servers and server farms from any location. Authorized administrators can run the console on any connected Windows NT or Windows 2000 workstation, in addition to MetaFrame XP server consoles.

When you install Citrix Management Console, the Setup program also installs the files necessary for IMA protocol communication on any supported workstation or server. Installation of the console is optional (though recommended) with MetaFrame XP server installation.

---

**Note** Citrix Management Console incorporates functionality provided by several separate management utilities in MetaFrame 1.8 and earlier versions, including Citrix Licensing (plicense.exe), Citrix Server Administration (mfadmin.exe), and Published Application Manager (appcfg.exe).

---

## Citrix NFuse

NFuse is a highly customizable application delivery mechanism that integrates the capabilities of Citrix server software with Web application deployment. NFuse is included with MetaFrame XP; essential NFuse components are installed by default for a “turnkey” NFuse setup on MetaFrame XP servers (when the MetaFrame XP Setup program detects that Internet Information Server and the Microsoft JVM is also installed).

NFuse uses Java object technology executed on a Web server to dynamically create an HTML-based presentation of the Citrix server farm. Every user sees a Web page customized with the applications available in the server farm for that user.

NFuse is a developer’s tool and a Web master’s application. It includes an application programming interface and an easy-to-use wizard. The API lets you create customized Web server scripts for your environment, while the wizard creates scripts that you can use or modify according to the NFuse API.

NFuse provides complete control over application deployment. Using NFuse’s API, you can configure all ICA session options without entering any settings at users’ desktops.

## Citrix Management Products

Citrix IMA is an extensible architecture that supports current Citrix management products and services and will support future releases of management products that function with MetaFrame XP and the IMA framework.

Citrix products ship with software modules that plug in to the Citrix Management Console, so administrators can use the same interface to manage basic and extended features of MetaFrame XP and Citrix server farms.

The products referred to below ship with separate documentation. More information about each product is also available from Citrix resellers and the Product Information area of the Citrix Web site at <http://www.citrix.com/products>.

### Citrix Load Manager



With Citrix Load Manager, you can implement session-based load management among the MetaFrame XP servers in a server farm. You can access Load Manager from any workstation running the Citrix Management Console.

With Load Manager, you can monitor server loads and use pre-configured and custom “load evaluators,” which calculate server loads based on a variety of criteria. Load Manager routes the requests of ICA Client users to run applications to the servers that are less used, avoiding bottlenecks in server farm performance.

When connections are balanced in the server farm, your users can run the applications they need quickly and efficiently. You can increase productivity through monitoring of your servers and application loads to identify problem areas as soon as possible.

Load Manager lets you:

- Balance application loads across multiple MetaFrame XP servers in a server farm
- Monitor and manage server farm connection loads at the server or application level
- Schedule the days and times you want to make published applications available to users on load-managed MetaFrame XP servers
- Restrict ICA Client connections to published applications on specified subnets
- Evaluate server loads based on memory, CPU, and disk I/O statistics

You can use Load Manager XP to make load changes to each server or application as you view your environment. You can also make global changes by adjusting the thresholds of your load evaluators and applying them to all your MetaFrame XP servers and applications.

For more information, visit the Product Information area of the Citrix Web site at <http://www.citrix.com/products>.

## Citrix Installation Manager



Installation Manager provides administrators with tools to deploy applications to multiple Citrix servers quickly and eliminate the need for manual installation of applications on Citrix servers.

Installation Manager can automate the application installation process, enabling the replication of published applications to Citrix servers across an enterprise. Installation Manager lets organizations save time and reduce errors when they must install many applications or applications that are frequently updated.

Installation Manager allows you to schedule the deployment of applications to MetaFrame servers, and to uninstall applications according to a specified schedule. Installation Manager also supports deployment of MSI-enabled applications without requiring a packaging step. The status of installation tasks is displayed in Citrix Management Console.

For more information, visit the Product Information area of the Citrix Web site at <http://www.citrix.com/products>.

## Citrix Resource Manager



Citrix Resource Manager is an application- and systems-management product designed specifically for Citrix and Microsoft multiuser Windows environments.

Resource Manager provides full-featured management tools for analyzing and tuning MetaFrame and Windows NT Server 4.0, Terminal Server Edition or Windows 2000 server systems. Resource Manager provides audit trails, system monitoring, and billing reports.

The product works with the same Open Database Connectivity (ODBC)-compliant databases as MetaFrame XP to capture user connection information.

Resource Manager lets you view the percentage of time applications are used in contrast with the total time that applications are loaded. More than 30 real-time performance counters can be analyzed and displayed with green, yellow, or red condition indicators. Thresholds for each performance counter can be customized and alerts can be transmitted by SMS or e-mail message.

For billing reports, you can set fees per minute of connection time, or by RAM or processor utilization. You can assign users to cost centers and construct billing reports to show resource consumption, session start times, elapsed time, and applications executed.

For more information, visit the Product Information area of the Citrix Web site at <http://www.citrix.com/products>.

## Features of MetaFrame XP for Windows

Major features of the MetaFrame XP product, including IMA and the Citrix Management Console, are discussed earlier in this chapter. This section describes in more detail the features of MetaFrame XP, including new features in this release.

### Application Server Features

MetaFrame XP runs on two Microsoft Windows server platforms: Windows NT Server 4.0, Terminal Server Edition, and the Windows 2000 Server family (Windows 2000 Server, Advanced Server, and Datacenter Server).

The following are major features and benefits of MetaFrame XP:

**Application publishing.** Publishing an application on a MetaFrame XP server makes it available to ICA Client users (with proper authorization). You can publish applications across multiple servers in the server farm. With optional Citrix Load Manager, you can balance connections from ICA Client users to connect users to the least-loaded MetaFrame XP servers.

**Client Device Licensing.** A user can establish multiple sessions to multiple servers while consuming only a single pooled connection license count for each session.

**Automatic ICA Client update.** MetaFrame XP lets you automate distribution of updated versions of Citrix ICA Client software to client devices. After you install the latest ICA Client software on the server, you can schedule the download and installation of the software to client devices. For more information, see “Deploying ICA Clients to Users” on page 159.

**Security.** MetaFrame XP incorporates multilevel system security and 128-bit data encryption. Citrix administrator accounts can be configured with read-only or read-write access to Citrix Management Console for management of Citrix server farms. During MetaFrame XP installation, you can disable the ability to shadow ICA Client sessions, or you can allow shadowing but require logging of shadowing events to create an audit trail.

**TCP/IP port setting.** You can configure Citrix ICA packets to be compatible with many popular TCP/IP firewall products. For more information, see the ALTADDR command in “Command Reference,” Appendix A.

**SpeedScreen.** SpeedScreen reduces the transmission of frequently repainted screens to reduce bandwidth consumption. SpeedScreen latency reduction provides instant mouse-click feedback and local text echo. These features increase perceived performance of ICA sessions over high-latency connections. SpeedScreen latency reduction is not available in the Japanese version of MetaFrame XP.

**Application management.** MetaFrame XP enables you to manage and extend the reach of enterprise applications with tools such as Application Launching and Embedding and application publishing. With ALE, you can extend applications across the Web without programming. Application publishing lets ICA Client users access applications as simply as other resources on the network. You can deploy and manage multiple servers and applications from a single point.

## Citrix ICA Client Features

Citrix ICA Clients share many features for connecting to MetaFrame XP servers. Some features are available on particular ICA Clients. For detailed information on supported features, see the *ICA Client Administrator's Guide* for each client you use.

**Program Neighborhood.** Supported by ICA Clients for Win32 and Java, Program Neighborhood gives you complete application control by publishing server-based applications to the local desktops. With Program Neighborhood, server-based applications can be pushed to the client device, integrated into the local desktop, or pushed directly to the Start menu.

**TAPI support.** The ICA Client for Win32 provides TAPI support for dial-up connections. Citrix ICA Clients for DOS and Win16 can interpret Windows 9x and Windows 2000 modem configuration files into legacy Ini files to ensure optimum performance for dial-up users.

**International keyboard support for Web browsers.** Users worldwide can exploit the benefits of Citrix ICA Clients for Internet Explorer and Netscape Navigator, current versions of which support international keyboard layouts.

**Client device mapping.** Users can transparently access local printers and disk drives. Drive letters on the MetaFrame XP server are configurable so client devices can keep their drive letters, and long filenames are supported. Any printers detected when you connect to a Citrix server are automatically mapped for use with the applications users run on the server. Client printers can be browsed and connected to in the same way as network printers (Windows, WinCE, and DOS clients).

**COM port mapping.** The ICA Client COM port redirector lets ICA Client users (DOS, Win16, and Win32 platforms) use most peripherals that connect to serial ports as if they were connected to a COM port on the Citrix server.

**Windows clipboard integration.** Users can cut and paste data between ICA sessions and local applications using the Windows clipboard (Windows clients only).

**Remote audio.** MetaFrame XP provides remote audio support for the DOS, Win16, and Win32 ICA Clients. Compression can be used to maximize bandwidth utilization. Audio support requires a Sound Blaster Pro-compatible sound card in the ICA Client device.

**Disk caching and data compression.** These options increase performance over low-speed asynchronous and WAN connections. Disk caching stores frequently used application images (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.

**Seamless windows support.** Certain ICA Clients support the seamless integration of local and remote applications on the local desktop. Configuring an ICA connection for seamless windows lets end users switch among local and remote applications with keyboard controls or the local taskbar. Seamless windows connections also support remote application icons on the local desktop, and tiling and cascading between local and remote Windows applications.

**Business recovery.** ICA Clients support multiple site addresses (for primary and hot backup, for example) for the same published application name. This feature helps assure consistent connections to published applications in the event of server disruptions.

**Client print manager.** Users can define which client printers can be configured on their client devices. This feature provides a means to store printer properties on a per-client-device basis while simplifying printer configuration for non-Windows clients.

**Multi-monitor support.** The ICA Win32 Client supports the multi-monitor features of Microsoft Windows 98 and Windows 2000 clients. It also supports the virtual desktop feature provided by some graphics cards for Windows 95 and Windows NT 4.0.

**Panning and scaling.** If the ICA session is larger than the client computer's desktop, you can pan the ICA session window around the full session desktop. Scaling allows you to view more of the ICA session at one time without panning by shrinking the perceived size of the ICA session. See the *ICA Client Administrator's Guide* for instructions on using this feature on a particular ICA Client.

## New Features in MetaFrame XP

The following are new or significantly enhanced features in this release of MetaFrame XP:

**Enhanced scalability.** Large enterprise-wide server farms can be easily installed, managed, and expanded as business requirements demand. The IMA foundation supports complex network configurations, including multiple network segments and firewalls. The loss of any single server need not impact the functioning of a server farm.

**Integrated security.** MetaFrame XP server farms are resistant to security threats that could damage the farm or lead to theft of information and denial of service. SecureICA high encryption is integrated into the base product, so data on the network is protected with 128-bit encryption.

**NFuse integration.** Citrix's NFuse Web portal deployment solution is included with MetaFrame XP and installed by default on MetaFrame XP servers. NFuse provides Program Neighborhood functionality for Web browser clients to access MetaFrame XP servers.

**Licensing.** IMA provides enhancements that make MetaFrame XP license administration easier. Improvements include single-point license installation and activation, and enterprise-wide license pooling among IMA-based Citrix servers.

**SNMP support.** MetaFrame XP includes support for administrative event notification and basic management control of MetaFrame XP servers through third-party management products (Tivoli and OpenView) using Simple Network Management Protocol (SNMP).

**Printer management.** The Citrix Management Console and MetaFrame XP provide robust control over printer devices. Configurable options include client printer mapping, automatic and on-demand replication of printer drivers, and printer resource assignment.

**Application migration.** Applications that are published on MetaFrame 1.8 servers can be migrated transparently to MetaFrame XP servers with all configuration data, including user authorizations and connection settings, intact.

**Interoperability.** IMA server farms can co-exist with MetaFrame 1.8 servers and MetaFrame for UNIX Operating Systems 1.x servers. IMA and the Citrix Management Console operate independently of MetaFrame 1.8 and other non-IMA Citrix servers.

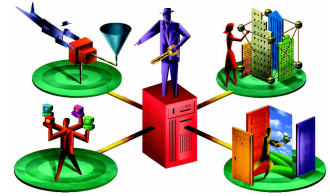
**Installation.** MetaFrame XP Setup supports attended and unattended installation. You can use Setup to install any or all of the components of the MetaFrame XP package, including IMA, MetaFrame XP application server, ICA Clients, and the Citrix Management Console.

**Shadowing options.** Administrators can enable shadowing notification or disable shadowing completely during MetaFrame XP installation. A shadowing indicator appears on the ICA Client desktop during shadowing and allows users to cancel shadowing easily with the mouse or a keyboard shortcut.

**Display options.** MetaFrame XP provides greater display capabilities while efficiently utilizing existing bandwidth. ICA Client users and administrators can select more colors and larger screen sizes than were supported by earlier Citrix servers.



# Planning Your MetaFrame XP Deployment



This chapter includes background information on decisions you need to make before you deploy MetaFrame XP. Be sure to read this chapter before you install MetaFrame XP on your servers.

This chapter includes the following topics:

- System Requirements, page 31
- Choosing a Database for the Data Store, page 37
- Network Configuration and Account Authority Issues, page 40
- Configuring Citrix Administrator Accounts, page 48
- Planning for Client and Server Communications, page 49
- Naming the Server Farm, page 62
- Changing Server Drive Letters, page 62
- Configuring Session Shadowing, page 64
- Interoperability with MetaFrame 1.8, page 65

## System Requirements

This section describes minimum configurations and recommendations for installation of MetaFrame XP servers, and other issues related to system sizing for MetaFrame XP installations. For information on system requirements of ICA Client devices, refer to the *ICA Client Administrator's Guide* for each client platform.

## System Software Requirements

You can install MetaFrame XP on servers with the following Microsoft operating systems:

- Windows NT Server 4.0, Terminal Server Edition with Service Pack 5 or later.
- Windows 2000 Server Family: Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server with Microsoft's Service Pack 1 or later. You must install the Terminal Services component before you install MetaFrame XP. Terminal Services is not installed in Windows 2000 by default; you can install it with Add/Remove Programs in Control Panel. Install Terminal Services in Application Server mode.
- To use the MetaFrame XP and ICA Client documentation that is provided in PDF files, you need to have the Adobe Acrobat Reader program. The Reader program lets you view, search, and print the documentation files.

If you need to obtain the Reader program, you can download it for free from Adobe System's Web site (<http://www.adobe.com>). The self-extracting file includes installation instructions.

---

---

**Warning** To use the NetWare Client with MetaFrame XP on Windows NT Server 4.0, Terminal Server Edition, you must install the NetWare Client before installing MetaFrame XP.

---

---

## Java Virtual Machine Requirements for NFuse

To install NFuse on the MetaFrame XP server, Microsoft Internet Information Server (IIS) Version 4.0 or higher and the Microsoft Java Virtual Machine (JVM) included with IIS must be installed before installing MetaFrame XP.

## Server Name Limitations

Multiple MetaFrame XP servers in the same farm (or in MetaFrame XP and MetaFrame 1.8 farms operating together in mixed mode) cannot have the same server name. You must change the name of the server before installing MetaFrame XP.

---

**Important** MetaFrame XP supports servers with extended characters in the server name only if your network's DNS server runs on Windows 2000. If your network's DNS server does not run on Windows 2000 and your server has extended characters in the server name, change the server name before installing MetaFrame XP.

---

## System Hardware Requirements

The following requirements are based on the requirements of the operating systems on which you run MetaFrame XP.

**Windows NT Server 4.0, Terminal Server Edition.** Microsoft recommends a Pentium or better microprocessor, 32MB of RAM, and a hard disk with at least 128MB of free space.

**Windows 2000 Server and Advanced Server.** Microsoft recommends a 133MHz or faster Pentium-compatible processor, 256MB of RAM, and a 2GB hard disk with at least 1GB of free space.

**Windows 2000 Datacenter Server.** Microsoft recommends an eight-way or greater array of Pentium III Xeon processors, 256MB of RAM, and a 2GB hard disk with at least 1GB of free space.

---

**Important** Microsoft recommends that you do not install Terminal Services on a Windows 2000 Server acting as a domain controller. By default, users are not able to log on to Terminal Services sessions on a domain controller. You can permit users to log on by setting the “log on locally” right; however, this is not recommended.

---

## Disk and Memory Requirements

In addition to the Windows operating system requirements for your server, the following are required for MetaFrame XP:

- 85MB disk space for standard MetaFrame XP installation, including Citrix Management Console, without ICA Client software
- 200MB disk space for installing all ICA Client software
- 20MB disk space for NFuse services on the MetaFrame XP server
- 64MB RAM for MetaFrame XP services, including IMA

## Modems and Multiport Adapters

In addition to ICA connections over network protocols (see “Configuring Network ICA Connections” on page 80), MetaFrame XP supports asynchronous ICA connections.

When you set up an asynchronous ICA connection on a MetaFrame XP server, client devices with modems can dial up the modem on a MetaFrame XP server. Once they connect, the ICA Client and MetaFrame XP server communicate directly, without the overhead of Windows Remote Access Service (RAS) and TCP/IP.

If you want to configure modems for ICA dial up connections and the modems are configured for Windows RAS, remove the modems from the RAS modem pool before you start MetaFrame XP installation.

---

**Important** You cannot configure a modem or serial port as both a RAS service port and an ICA asynchronous connection port.

---

For ICA asynchronous connections, Citrix recommends high-speed serial port hardware or intelligent multiport adapters on the server. These devices use the CPU efficiently, freeing CPU resources that can be devoted to running user sessions. If you have a multiport async adapter, install it before starting MetaFrame XP installation. You can choose to install modems connected to the multiport adapter before or during MetaFrame XP installation.

MetaFrame XP Setup recognizes TAPI-capable modems installed on the server. When a TAPI modem is detected, MetaFrame XP uses modem installation and configuration utilities in Windows to manage the modem. If no modems are installed on a server, MetaFrame XP Setup gives you the opportunity to install them.

## Citrix Management Console Requirements

Citrix Management Console is the centralized management utility you use to administer your MetaFrame XP server farm. It is installed on all MetaFrame XP servers by default. However, using the MetaFrame XP CD, you can install the Citrix Management Console on workstations that are not used as MetaFrame XP servers. Computers intended to run the console must meet the following requirements:

**Operating System.** You can install Citrix Management Console on any Windows NT 4.0 or Windows 2000 computer. You can install the console on your MetaFrame and MetaFrame XP servers, but the console does not require that MetaFrame XP is installed on the same computer.

**Sun Java Runtime Environment (JRE).** The console is a Java application and requires the Sun JRE Version 1.3. If your system does not have the correct JRE version, Setup installs it. Setup does not replace or affect any previously installed JRE.

**Disk space.** A minimum of 25MB of disk space is required for installation of Citrix Management Console and the Java Run-Time Environment.

**Memory.** A minimum of 64MB of RAM for running Citrix Management Console (in addition to RAM required for the operating system and other applications).

**Processor.** A Pentium-class or better processor is recommended.

## Sizing Systems for MetaFrame XP

MetaFrame XP supports multiple users on Windows NT 4.0 Server, Terminal Server Edition, and Windows 2000 Servers. A multiuser system requires more system resources than a single-user system. This section provides some system-sizing guidelines that can help you decide on a hardware configuration that will support your users with optimal performance.

Most companies find that their users can be categorized as typical users or power users.

**Typical user.** Generally uses one or two applications but normally only one at a time. Little actual program data is transferred between the client and server, and the users rarely use Object Linking and Embedding (OLE).

**Power user.** A more sophisticated user who uses three or more applications, often with several active at the same time. Data is often cut and pasted between local and remote applications, and OLE is used heavily.

Power users consume more resources than typical users. A good rule of thumb is that one power user is equivalent to two typical users in processor utilization and RAM requirements.

---

**Tip** The configuration examples in this section are based on numbers of typical users. Adjust the numbers for power users.

---

## Processor, Bus, and Memory

The processor and bus architecture are fundamental to MetaFrame XP server performance.

The ISA (AT bus) architecture is low-bandwidth and is not recommended for MetaFrame XP servers. Use a higher-performance bus, such as EISA or PCI, for best performance. These buses support the high sustained data transfer rates that are typical of a MetaFrame XP server.

The memory (RAM) requirement for MetaFrame XP is 16MB plus 4MB for each typical user or 8MB for each power user. In many cases, adding RAM has a larger effect on system performance than upgrading to a faster processor.

In general, processor and RAM requirements for MetaFrame XP scale linearly. You can roughly double the number of users supported on a multiprocessor-capable system by doubling the number of processors and doubling the amount of RAM. By purchasing multiprocessor-capable systems (even if you initially purchase only one processor), you provide for convenient system scaling as your requirements grow.

Note that not all multiprocessor systems scale the same way because of bus differences. The bus architecture in a multiprocessor system is crucial for multiprocessor performance with more than four processors, and vendor-specific drivers are usually required.

### **Win16 Application Requirements**

Windows NT and Windows 2000 are Win32 (32-bit) environments. Windows 3.x for DOS is a Win16 (16-bit) environment. Windows NT and Windows 2000 run Win16 applications through a process called WOW (Win16 on Win32), which translates 16-bit applications in enhanced mode. This process causes Win16 applications to consume additional system resources, reducing the number of users per processor by 20% and increasing the RAM required per user by 25%. For this reason, use Win32 applications whenever possible. If you intend to run Win16 applications, adjust your processor and RAM requirements accordingly.

### **Hard Disks**

The hard disk subsystem in a server is an important factor in system throughput. Small Computer System Interface (SCSI) disk drives and adapters, especially Fast Narrow SCSI (SCSI-2), Fast Wide SCSI, Wide Ultra SCSI, and Wide Ultra2 SCSI devices, have significantly better throughput than ST-506, Integrated Device Electronics (IDE), or Enhanced Small Device Interface (ESDI) disk drives and adapters.

For the highest disk performance, consider using a SCSI-based Redundant Array of Independent Disks (RAID) controller. RAID controllers automatically place data on multiple disk drives and can increase disk performance and improve data reliability.

Use NTFS for all disk partitions on your MetaFrame XP servers. NTFS allows security configuration, better performance, and more fault tolerance.

### **Network Interfaces**

The ICA protocol is highly compressed and causes negligible loading on a network, but because the MetaFrame XP server handles all network requests, a high-performance network interface card (NIC) is recommended.

If a multiport asynchronous communications adapter is installed for supporting serial ICA connections, be sure to use an intelligent (microprocessor-based) adapter to reduce interrupt overhead and increase throughput.

## Using Performance Monitoring Tools

Citrix recommends that you use performance monitoring tools to get accurate accounts of system performance and the effects of configuration changes on system throughput. The most important measurements for performance monitoring are the percentage of total processor time, memory pages per second, percentage of network utilization, and hard disk I/O rates.

A good way to estimate how many users a server can support is to measure system performance with two to five users on the system and then scale the results. This method has been found to yield reliable results.

## Choosing a Database for the Data Store

Before installing MetaFrame XP, you must decide which database to use for the data store for your server farm.

- Microsoft Access is a lightweight database that is included with Windows server operating systems. It is most appropriate for smaller server farms of up to 50 servers. However, mid-sized server farms of more than 50 servers often perform just as well with a Microsoft Access database as with SQL Server or Oracle.
- Microsoft SQL Server is a true client/server database that offers robust and scalable support for multiple-server data access. It is suited for use in farms of any size.
- Oracle is a true client/server database that offers robust and scalable support for multiple-server data access. It is suited for use in farms of any size.

It is important to note that other factors— in addition to the number of servers— affect data store and overall server farm performance. Other factors that affect performance are the number and type of published applications, the maximum number and the average number of concurrent client connections, and the hardware configuration of MetaFrame XP servers.

---

**Important** Microsoft SQL and Oracle servers require significant expertise to install and maintain. If you do not have expertise with these products, attempting to use them in a production environment is not recommended. See the documentation included with your database product for important details such as performance tuning and database backup procedures.

---

For information on supported database and ODBC driver versions, see “Data Store Database Requirements” on page 39.

When using Microsoft Access, the database is stored on the first MetaFrame XP server in the farm, and is created as part of the MetaFrame XP installation process.

When using Microsoft SQL Server or Oracle, the database is on a dedicated server running Microsoft SQL or Oracle that must be set up prior to creating the server farm.

---

**Important** Do not install MetaFrame XP on the Microsoft SQL or Oracle database server. Refer to the Microsoft SQL Server or Oracle documentation for specific hardware requirements for the database server.

---

After you decide which database to use for the data store, you need to decide whether MetaFrame XP servers will access it by direct connection or indirectly through another MetaFrame XP server.

To make a *direct connection* to the data store, a MetaFrame XP server must have the appropriate ODBC drivers installed and configured properly. The server then connects directly to the server on which the database is running.

For *indirect access*, a MetaFrame XP server connects to an intermediary MetaFrame XP server. The intermediary server connects to the data store directly. Using indirect connectivity with an SQL database eliminates the need to install and configure the ODBC drivers on every MetaFrame XP server. If you are using an SQL database for the data store, you can use a combination of direct and indirect access methods for the servers in the farm.

---

**Tip** Indirect access is not recommended for mission-critical server farms because the intermediary server is a single point of failure.

---

By default, indirect access uses TCP port 2512 for communication between the MetaFrame XP servers. If the MetaFrame XP servers are in different subnets, be sure this port is not blocked by any firewalls. If this port number is not convenient, it can be changed.

## System Sizing for the Data Store Database

Use the chart below as a guideline to determine which scenario most closely matches your environment. If your environment doesn't fit neatly into the categories listed, choose the category that has the most in common with your environment.

|                     | Small | Medium | Large  | Enterprise  |
|---------------------|-------|--------|--------|-------------|
| <b>Servers</b>      | 1-50  | 25-100 | 50-100 | 100 or more |
| <b>Named Users</b>  | < 150 | < 3000 | < 5000 | > 3000      |
| <b>Applications</b> | < 100 | < 100  | < 500  | < 2000      |

The following are general recommendations for the server farm's data store database:

- Microsoft Access is suitable for all small and many medium-sized environments.
- Microsoft SQL Server or Oracle are suitable for any environment and are recommended for all large and enterprise environments.

---

**Note** If you plan to use mixed mode to support MetaFrame 1.8 servers, do not include the MetaFrame 1.8 servers in your system sizing calculations.

---

## Data Store Database Requirements

You can choose to use Microsoft Access (included with Windows), Microsoft SQL Server, or Oracle for the data store. The following sections list the ODBC driver and database versions required by MetaFrame XP.

---

---

**Warning** Do not install MetaFrame XP on a server with Microsoft SQL or Oracle.

---

---

### Microsoft Access

The Microsoft Access database engine and ODBC drivers are a default component of Windows NT 4.0 Server, Terminal Server Edition and Windows 2000 Servers. To use this database, you do not have to install any drivers or perform any database configuration prior to MetaFrame XP installation.

### Microsoft SQL Server

MetaFrame XP is supported with Microsoft SQL Server 7 with SQL Service Pack 2 running on Windows NT 4.0 Server or the Windows 2000 Server Family. Microsoft SQL Server 2000 is also supported.

Version 3.70.08.20 or greater of the Microsoft SQL ODBC driver must be installed on each MetaFrame XP server that will directly access the SQL server. On Windows 2000 servers, the necessary drivers are installed with the operating system. On Windows NT 4.0 Server, Terminal Server Edition, install Microsoft Data Access Components (MDAC) Version 2.6, which can be downloaded for free from Microsoft's download site.

---

**Important** On TSE systems, before MDAC installation, stop the Terminal Services Licensing Service. After installing MDAC, clear the event log, then restart the server before installing MetaFrame XP.

---

## Oracle

MetaFrame XP supports the following Oracle databases for the server farm's data store:

- Oracle8i, Version 8.1.6
- Oracle 7, Version 7.3.4
- Oracle 8, Version 8.0.6

Install the Oracle Net8 client and ODBC drivers provided by Oracle on each MetaFrame XP server that will directly access the database server. The Citrix data store is stored as an object (schema) assigned to a user. You do not need a separate database for each data store.

Install the Oracle Net8 Client Version 8.01.06.00. During install, you can either run the Net8 Easy Config, or cancel the installation at that point and copy the tnsnames.ora and sqlnet.ora files from the Oracle server to %oracle home directory%\network\admin on each MetaFrame XP server.

---

**Important** Restart the system after you install the Oracle client and before you install MetaFrame XP.

---

## Network Configuration and Account Authority Issues

Before you implement your MetaFrame XP installation, you must consider issues related to network configuration and the management of user accounts. This section discusses recommended practices for:

- Windows NT domains and Active Directory
- Security models and user access to applications
- Configuration of accounts for Citrix administrators

## General Configuration Issues

Citrix recommends that you do not use Windows primary domain controllers or backup domain controllers as MetaFrame XP servers, because of these factors:

- Domain controllers handle user validation for network logons and access to network resources. These functions and the associated network communication can significantly affect the performance of an application server.
- The MetaFrame XP Setup program cannot create anonymous accounts on primary or backup domain controllers, so you cannot publish applications for anonymous access on MetaFrame XP servers that are domain controllers.

## Recommendations for Active Directory

If your network is configured to use Active Directory domains and groups, consider the following Citrix deployment recommendations:

**Use Windows 2000 Servers.** Install MetaFrame XP exclusively on Windows 2000 Servers. Native support for Active Directory is included in Windows 2000, so you do not need to install additional services.

If users of the server farm use User Principal Name (UPN) logons, you must use Windows 2000 servers exclusively, because UPN logons are not supported by Windows NT Server 4.0, Terminal Server Edition (TSE) servers, even with the Active Directory Services Interface installed. If the server farm contains both Windows 2000 and TSE servers, you must use the pre-Windows 2000 logon name in the format *domainname\username*.

**Use a single forest.** Install all servers in the server farm so they reside in one active directory forest. See “Using Active Directory Forests” on page 42.

**Install ADSI 2.5 or higher.** If you use TSE servers in the server farm, install Active Directory Services Interface (ADSI) 2.5 or higher on the TSE servers. ADSI significantly improves the speed of user enumeration in large domains. With ADSI, colored icons appear in directory lists to distinguish group types. Installing ADSI on all TSE servers and having Active Directory domains running in native mode lets you use domain local groups when publishing applications and allocating printers. In addition, ADSI lets TSE servers use LDAP queries rather than using legacy domain operations whenever possible.

If ADSI is not installed, TSE servers cannot enumerate domain local groups from Active Directory domains that are running in Active Directory native mode.

---

**Important** Even if a TSE server has ADSI installed, UPN logons aren't permitted for Program Neighborhood filtering or for administrators to log in to Citrix Management Console. For this reason, you must use only Windows 2000 servers if you want users to log on with UPN credentials.

---

## Recommended Domain Configurations

Citrix recommends the following for configuration of MetaFrame XP server farms with Active Directory:

- All servers reside in the same domain
- The server farm domain has no trust relationships with non-Active Directory domains
- The server farm is in a single Active Directory forest

These recommendations are not a requirement. However, multiple domains or trust relationships with non-Active Directory domains can affect all aspects of user authentication, which include:

- Authentication for Citrix administrators
- Access by users to published applications
- Assignment of users to network printers

## Using Active Directory Forests

If you use Windows Active Directory, Citrix recommends that all MetaFrame XP servers in a server farm belong to the same forest. If your server farm has MetaFrame XP servers in more than one forest, end users cannot use *user principal name* (UPN) logons in the farm.

UPN logons use the format *username@UPN identifier*. With Active Directory, UPN logons do not require a domain to be specified, because Active Directory can locate full UPN logons in the directory. However, if multiple forests exist in the server farm, problems can arise because the same UPN identifier can exist in two domains in separate forests.

---

**Important** Because there is no efficient way to perform account resolution, MetaFrame XP does not support UPN logons if a MetaFrame XP farm spans multiple Active Directory forests.

---

## User Access to Applications and Printers

To authorize user access to resources in a server farm, you select user and group accounts. For example, when you publish an application, you select the servers to host the application and Citrix Management Console lists the user accounts from the trust intersection of all the servers (accounts that are trusted by all the servers). You then select the users and groups that you want to allow to use the application.

After you select users, changing the list of host servers can change the trust intersection, which can make the application unavailable to users who are no longer in the servers' trust intersection. If the trust intersection changes, the console informs you and removes users from the authorized users list who are no longer eligible to use the resource.

A published application is available only to users who can access every server that hosts the application. When multiple servers host the same application, you can't predict which servers ICA Clients will connect to when they launch the application. Therefore, if a user is authorized to access only some servers, you cannot ensure that the user will always be able to use the application.

To prevent unpredictable access, MetaFrame XP removes users from the authorized users of a published application or printer if the accounts are not in the trust intersection for all the host servers.

## Trust-Based Routing

*Trust-based routing* allows servers to be members of a server farm even if the servers belong to domains that don't trust each other. In trust-based routing, a request to enumerate users or authenticate a user is routed to a server that has the required domain trust relationship if the originating server does not.

During a *trust query cycle*, a MetaFrame XP server registers its trusted domains with the server farm's data store. This operation occurs during every service startup and approximately every six hours while the service is executing. Therefore, the data store is a central repository of all trust data for the servers in the server farm.

When a server needs to perform an operation (as defined below) on a domain that it doesn't trust, the server determines from the data store which servers can perform the operation, and then routes the request to the most accessible server.

Trust-based routing applies to the following operations:

- Authenticating a Citrix administrator to Citrix Management Console
- Refreshing the display or launching an application in Program Neighborhood
- Enumerating users and groups in the console
- Resolving users and groups into distinguished accounts names when you add users or groups to a published application, add users to a printer auto-creation list, or define new Citrix administrators

## Active Directory Security Model and Restrictions

Active Directory introduces new types of security groups that network users can belong to. You can use these security groups when you select users for published applications and network printers.

This section describes the Active Directory security groups and gives recommendations for using Active Directory security groups in a MetaFrame XP server farm.

**Domain local groups.** In the Active Directory model, domain local groups can contain groups from other domains, but the domain local group can be assigned to resources only in the domain in which it exists.

**Universal groups.** Universal groups can contain groups from other domains. Universal groups are stored in the Active Directory global catalog. Universal groups can be used for assigning permissions to resources in any domain.

**Domain global groups.** Global groups contain groups within the same domain and can be assigned to resources in any domain. Citrix recommends that you use domain global groups for user access to published applications and network printers.

---

**Note** Domain global groups are equivalent to Windows NT 4.0 global groups.

---

Domain local groups and universal groups are available only in Active Directory domains that are operating in native mode.

If you plan to use universal groups or domain local groups, it's recommended that you follow the deployment guidelines in this section regarding domain configuration and use of groups to reduce administrative complexity.

For in-depth technical information on user access issues and configuration issues, see "User Permission Scenarios with Active Directory" on page 45.

If you change the servers that host a published application, the trust intersection with individual user accounts and with domain local groups can change.

For example, if all servers hosting an application or a printer reside in a common domain, D1, you can select domain local groups from D1 to grant access to the resource. If you then configure additional servers to host the resource and these servers do not reside in D1, Citrix Management Console detects the change and removes the D1 domain local group from the configured accounts for the resource.

For more information on domains, establishing trust relationship among domains, and configuring user accounts in domains or Active Directory, refer to your Windows documentation.

## **User Permission Scenarios with Active Directory**

With Active Directory, the following issues affect the choices you make when you configure a server farm and manage user permissions:

- If you use universal groups to give users permission to run published applications, all the servers that run an application (if you use Citrix Load Manager for load balancing) must reside in an Active Directory domain.
- If you use a domain local group to give users permission to run published applications, all servers that load-balance an application must belong to the same domain. Also, the domain local group you assign to an application must be in the common primary domain of all the load-balancing servers.
- If a user is a member of a domain local group, the group is in the user's security token only when the user logs on to a machine in the same domain as the domain local group. Trust-based routing does not guarantee that a user's logon request will be sent to a server in the same domain as the domain local group.

The table below describes how network configurations affect user permissions with Active Directory.

|                             | Program Neighborhood Filtering                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Authenticating to Published Applications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Authenticating to Citrix Management Console                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain Global Groups</b> | No adverse effects                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | No adverse effects                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | No adverse effects                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Domain Local Groups</b>  | <p><b>Recommendation:</b> All servers in the farm must be in the same domain for Program Neighborhood filtering to work properly.</p> <p><b>Rationale:</b> If a user is a member of a domain local group, the group is present in the user's security token only when logging onto a machine in the same domain as the domain local group. Trust-based routing (see page 43) does not guarantee that a logon request will be sent to a server in the same domain as the domain local group. It guarantees only that the request will be handled by a server in a domain that trusts the user's domain.</p> | <p><b>Recommendation:</b> All servers that load-balance an application must be in the same domain if a domain local group is authorized to use the application.</p> <p><b>Rationale:</b> Domain local groups assigned to an application must be from the common primary domain of all the load-balancing servers. When you publish applications, domain local groups appear in the accounts list if the first condition above is met and accounts from the common primary domain are displayed (a green domain icon denotes the servers' common primary domain).</p> <p>If a published application has users from any domain local groups and you add a server from a different domain, domain local groups are removed from the configured users list, because all servers must be able to validate any user with permission to run the application.</p> | <p><b>Recommendation:</b> If a user is a Citrix administrator only by membership in a domain local group, the user must connect the console to a server in the same domain as the domain local group.</p> <p><b>Rationale:</b> If the user connects the console to a server in a different domain than the domain local group, the user is denied access to the console because the domain local group is not in the user's security token.</p> |

|                         | Program Neighborhood Filtering                                                                                                                                                                                                                                                                                                                                                                                           | Authenticating to Published Applications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Authenticating to Citrix Management Console                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Universal Groups</b> | <p><b>Recommendation:</b> No Active Directory domains in the forest to which the servers belong have explicit trust relationships with pre-Windows 2000 domains.</p> <p><b>Rationale:</b> Pre-Windows 2000 domains have no knowledge of Universal groups and the domain controllers will exclude a universal group from a user's security token. As a result, applications might not appear in Program Neighborhood.</p> | <p><b>Recommendation:</b> If Universal groups are assigned permission to the application, all servers that manage the application must be in an Active Directory domain.</p> <p><b>Rationale:</b> A server in a Windows NT domain could authenticate the user to run the application. In this case, Universal groups are not in the user's security token, so the user is denied access to the application.</p> <p>It is possible for a server in a Windows NT domain to load balance an application with servers in an Active Directory domain if the domains have an explicit trust relationship.</p> | <p><b>Recommendation:</b> If a user is authenticating to the console and the user is a Citrix administrator only by membership in a universal group, the console must connect to a server that belongs to an Active Directory domain in the universal group's forest.</p> <p><b>Rationale:</b> Pre-Windows 2000 domain controllers and domains outside a universal group's forest have no information about the universal group.</p> |

## Using the BUILTIN Group

When you specify users and groups for access to published applications or network printers, or when you create Citrix Administrators, a special option, the BUILTIN group, is available from the menus that list network domains.

You can use the BUILTIN option:

- If your network environment is configured with Windows workgroups rather than with Windows network domains
- For compatibility with Novell's ZENworks product

## Using BUILTIN for Publishing Applications and Printer Management

If you use the BUILTIN group to specify users for applications and printer resources, do not use Program Neighborhood and NFuse for ICA Client connections to published applications. Use only custom ICA connections to launch applications.

## Compatibility with ZENworks Dynamic Local Users

In network environments that use Novell's ZENworks product for user management, use the BUILTIN group for compatibility. You select the BUILTIN group to specify dynamic local users managed by ZENworks when you publish applications and assign users to network printers.

With ZENworks, the software that handles user logons (called *GINA* for Graphical Identification and Authentication) on every machine that supports this feature is replaced with the GINA provided by Novell. Users log on by entering Novell Directory Service (NDS) credentials. An NDS server authenticates the user and determines permissions for the logon server. On this server, ZENworks dynamically creates a local user and gives group permissions according to the user policies. The only constant security ID between sessions is the security IDs of the BUILTIN groups to which the NDS user belongs.

## Changing Domain Trust Relationships

If you add a new domain trust relationship, you might not be able to select user accounts in the server farm based on the trust relationship right away.

You might see this situation when you publish an application, for example, after adding a new trust relationship. In the dialog box where you configure user accounts for the application, when you select a domain, the newly-trusted domain does not appear until the IMA service propagates the new trust relationship throughout the server farm.

The user management subsystem updates its domain trust information every six hours (and during service startup). Therefore, it might take as long as six hours for all servers in the server farm to recognize a new trust relationship.

You can avoid a delay in detection of network trust changes by restarting the IMA service on all servers affected by the change. For example, if you change a trust relationship to allow DomainX to trust DomainY, restart all servers that belong to DomainX. With Active Directory, if you add a new domain to an Active Directory forest, for example, restart the IMA service on all servers that belong to a domain in the forest that is affected by the change.

If you are unsure which servers are affected by a trust relationship change, you can restart the IMA service on all servers in the farm to ensure that the change is recognized. It is recommended that you restart the IMA service only during off-peak hours when the load on the servers is very low.

## Configuring Citrix Administrator Accounts

When you install the first MetaFrame XP server in a new server farm, you are asked to specify an initial farm administrator. By default, this is the user who logs on to the server to install MetaFrame XP. Setup configures this user account as a Citrix administrator with read-write permission in the console.

To give other user accounts access to Citrix Management Console, a Citrix administrator with read-write permission logs on to the console and adds other user accounts to Citrix Administrators.

To give administrators of your server farm access to Citrix Management Console, you add their network user accounts to Citrix Administrators in the console. The console uses standard Windows network logon and user account authentication mechanisms.

When you set up Citrix administrator accounts, Citrix recommends that you select your existing administrators group for the domain or network. This group is presumed to be well controlled and its users have administrative access to network resources, including print servers. When an administrator uses the console to configure a print server for the server farm, for example, he or she must enter user credentials that allow administration of the print server.

One Citrix administrator account that has read-write permission must always exist in the server farm. Therefore, you cannot delete the last remaining read-write Citrix administrator account from the console. However, if the account no longer exists in the network account authority, the console allows a local administrator to log on to the console to set up Citrix administrator accounts.

## Planning for Client and Server Communications

In a Citrix server farm, several types of data transmission and communication pathways link ICA Clients with MetaFrame XP servers and other components.

Consider the following communication issues for your deployment of MetaFrame XP, ICA Clients, and optionally, Citrix NFuse and related Citrix services:

- Configuring ICA browsing so ICA Clients can find published applications and MetaFrame XP servers in your server farm
- Configuring network firewalls to allow communication among ICA Clients, MetaFrame XP, and NFuse
- Configuring a MetaFrame XP server farm for interoperability with MetaFrame 1.8

The first part of this section focuses on MetaFrame XP. For information about communication issues with MetaFrame XP and MetaFrame 1.8, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 60.

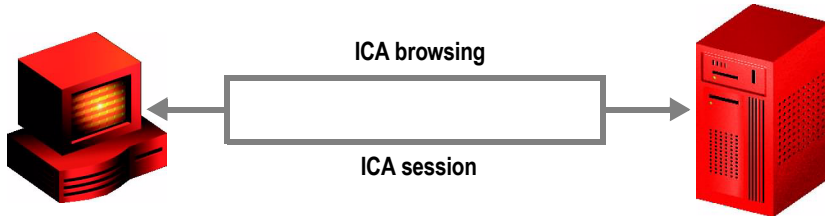
---

**Note** Features described in this section, including ICA browsing and published applications, are not available to all ICA Clients. This section focuses on the Version 6.0 ICA Win32 Client features and server farm configuration with this client. For information on server connections options in other clients, see the *Citrix ICA Client Administrator's Guide* for the clients you plan to deploy.

---

## Linking ICA Clients and MetaFrame XP Servers

In a server farm, the main communication processes between ICA Clients and MetaFrame XP servers are ICA browsing and ICA sessions.



*ICA Clients perform ICA browsing when requesting applications from MetaFrame servers. A client initiates an ICA session with the server to run an application.*

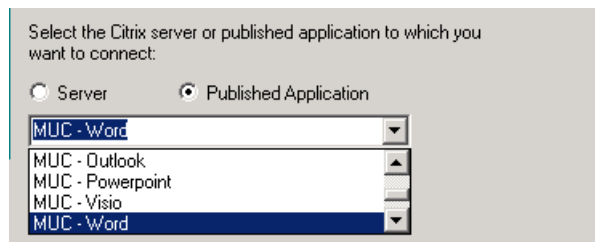
### ICA Browsing

*ICA browsing* is a process in which an ICA Client transmits data to locate MetaFrame servers on the network and get information about the server farm's published applications.

For ICA browsing, clients communicate with the Citrix XML Service or the ICA Browser, depending on the browsing protocol selected in the ICA Client. These options are described under "Configuring ICA Browsing" on page 51.

ICA browsing occurs when:

- Users launch published applications. The ICA Client sends a request to locate the application on a MetaFrame server. With the Citrix Load Manager option, the client gets the address of the server with the lightest load.
- Users display the **Application Set** list in the **Find New Application Set** wizard in Program Neighborhood.
- A user displays the **Server** or **Published Application** list in the **Add New ICA Connection** wizard to create a custom ICA connection.



*ICA browsing produces the Servers and Published Applications list for a custom ICA connection in the Win32 Client*

## ICA Sessions

An *ICA session* is the communication link between ICA Clients and MetaFrame servers that ICA Clients establish to run applications. In an ICA session, a MetaFrame server transmits an application's screen display to the client, and the ICA Client sends the user's keystrokes, mouse actions, and local data to the application running on the server.

The default port on MetaFrame servers for ICA sessions is 1494. This port must be open on firewalls for inbound communication if ICA Clients are outside the firewall. The port used on the client for the ICA session is configured dynamically when the session is established.

In addition to MetaFrame servers, other components, such as Citrix NFuse, Web servers, proxy servers, and Web browsers can be involved in establishing ICA sessions. In all cases, the basic communications link for an ICA session is between the ICA Client and MetaFrame server.

## Configuring ICA Browsing

Users connect to servers and applications from application sets or custom ICA connections in the ICA Client. As described above, ICA browsing is a process that locates MetaFrame servers and published applications in response to requests from an ICA Client.

- When a user launches an application from an application set, ICA browsing locates a server that hosts the published application so the ICA Client can connect to the server and run the application.
- When a user sets up a custom connection, ICA browsing produces a list of published applications or servers in the server farm. The user selects an application or server to define the custom connection.

## Server Location Settings

The method that ICA Clients use for ICA browsing depends on the specified Server Location settings, which you set in Program Neighborhood.

- For new application sets and custom connections, you configure server location settings from the **Server Location** button in the **Find New Application Set** wizard and **Add New ICA Connection** wizard in the ICA Client.
- For existing application sets and custom ICA connections, you can change Server Location settings on the **Connection** tabs in the **Settings** dialog boxes.

Server Location

Network Protocol:  
TCP/IP + HTTP

Server Group:  
Primary Rename Group

Address List:  
(ica.eng.citrix.com) Add  
Delete  
Firewalls...

☐ Use Custom Default

---

**Note** Some ICA Clients do not use ICA browsing and connect only to specified servers. The options described in this section are from the ICA Win32 Client. For information about other server location options, see the *Citrix ICA Client Administrator's Guide* for the clients you plan to deploy.

---

## Specifying the Network Protocol for ICA Browsing

The **Network Protocol** setting you specify for server location in the ICA Client affects the following deployment issues related to ICA browsing:

- The communications protocol the client uses to locate servers
- The Citrix component the client communicates with
- The port the client communicates with
- The default locations the client contacts

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

Citrix recommends you select **TCP/IP+HTTP** as the server location network protocol in the ICA Client. In addition, Citrix recommends that you specify servers to contact for ICA browsing by entering IP addresses or DNS names of MetaFrame XP servers in the **Address List** box.

When **TCP/IP+HTTP** is selected and you specify MetaFrame XP 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 **Server Address** list. This feature allows the DNS or WINS administrator to configure a host record that maps “ica” to a valid MetaFrame XP server IP address that can service XML requests from ICA Clients.

---

**Tip** You can configure the ICA Clients' DNS server to use round-robin DNS to map the name "ica" to a set of MetaFrame XP servers that can service the XML requests. This is a convenient method to use to avoid individual configuration of 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.

When you configure the ICA Client to use TCP/IP+HTTP, communication between the client and XML Service consists of XML-formatted data in HTTP packets.

Citrix recommends using TCP/IP+HTTP protocol for ICA browsing because it provides several 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

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

If **TCP/IP** is specified as the server location network protocol, and **(Auto-Locate)** appears in the **Address List** box, ICA Clients send UDP broadcasts to the ICA Browser service on port 1604 to locate MetaFrame servers and published applications.

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.

There are two configurations you can use for MetaFrame XP servers to respond to ICA Client broadcasts for ICA browsing:

- You can set the MetaFrame XP server farm to operate in mixed mode for interoperability with a MetaFrame 1.8 server farm as you migrate the farm to MetaFrame XP.
- You can set the MetaFrame XP server farm, or individual MetaFrame XP servers, to respond to ICA Client broadcasts for compatibility with deployed clients.

When a MetaFrame XP server farm operates in mixed mode, by default only MetaFrame XP servers that are master ICA Browsers respond to UDP broadcasts from ICA Clients. For more information on mixed mode operation, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 60. For information on data collectors, see “Configuring Zones and Data Collectors” on page 110. For information on configuring server response to broadcasts, see “Setting up Response to ICA Client Broadcasts” on page 109.

Because UDP broadcast packets do not traverse subnets, using broadcasts for ICA browsing works only if a server that responds to broadcasts is in the same subnet as the clients. After 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 XP servers in the **Address List** box. You must do this if the ICA Client is not on the same subnet as a data collector.

In summary, using the TCP/IP setting and auto-location for ICA browsing is less efficient than using TCP/IP+HTTP because it relies on UDP and UDP broadcasts.

## Effects of Server Location Settings on ICA Browsing

The following table summarizes ICA browsing methods that result from various **Network Protocol** and **Address List** settings.

| Network Protocol | Address List          | Data type     | Responder                      | Farm configuration                                                                                       |
|------------------|-----------------------|---------------|--------------------------------|----------------------------------------------------------------------------------------------------------|
| TCP/IP+HTTP      | Default (“ica”)       | XML / HTTP    | XML Service                    | Native mode or mixed mode.                                                                               |
| TCP/IP+HTTP      | Specified server(s)   | XML / HTTP    | XML Service                    | Native mode or mixed mode. In mixed mode, specify MetaFrame XP servers.                                  |
| TCP/IP           | Default (Auto-Locate) | UDP broadcast | ICA Browser on data collectors | Mixed mode. Native mode if servers are set to respond to broadcasts. Servers must be on clients' subnet. |
| TCP/IP           | Specified server(s)   | Directed UDP  | ICA Browser                    | Native or mixed mode.                                                                                    |

## Communicating with the Citrix XML Service

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

When ICA Clients are configured to use TCP/IP+HTTP for ICA browsing, 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-enabled Web servers.

For example, when a user launches a published application in Program Neighborhood, the ICA 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 Citrix NFuse, for example, a user connects to an application portal Web page with a Web browser. The XML Service provides a list of available applications to the NFuse-enabled Web server. The Web server displays the available applications on the user's personalized application Web page.

## Setting the Port for Citrix XML Service

The Citrix XML Service uses an IP port on the MetaFrame server for communication with ICA Clients and NFuse. You can set the port number during or after MetaFrame XP setup.

---

**Important** All MetaFrame servers in the server farm must use the same port for the XML service.

---

The XML Service default communication port is 80. Port 80 is open on most firewalls to allow inbound communication to Web servers. If your MetaFrame and Web servers are behind a firewall, this port is probably open, allowing ICA Clients to communicate with MetaFrame XP servers and allowing Web browsers to communicate with NFuse-enabled Web servers.

---

**Note** Port 80 is the default port for HTTP communication with Web servers. The Citrix XML Service includes an ISAPI extension that you can plug into Internet Information Server (IIS). The extension allows IIS and the XML Service to share port 80. This is necessary only if IIS is installed with NFuse on MetaFrame servers. The default MetaFrame XP installation does install NFuse if IIS is installed on the server. However, for best performance, Citrix recommends that IIS and NFuse be installed on separate dedicated Web servers.

---

For information on configuring the XML Service port number, see “Changing the Citrix XML Service Port” on page 86. For information on configuring the port that NFuse uses, see “Configuring Web Server Extension Properties” in the *NFuse Administrator's Guide*.

---

**Important** If you change the port used by the Citrix XML Service, you must set the correct port in the ICA Client. You can specify a port number when you add a server to the **Address List** under **Server Location** in the ICA Client. If you also use NFuse, be sure it uses the correct port for XML Service communication. For more information, refer to the NFuse documentation. See the *Citrix ICA Client Administrator's Guide* or the client's online help for instructions on configuring ICA Clients.

---

## Configuring Network Firewalls

Protecting servers that contain valuable data and are critical to your organization's mission requires that you consider security as an integral part of your MetaFrame XP deployment planning.

In addition to physically securing servers, most organizations will install network security measures including firewalls to isolate MetaFrame servers and Web browsers from the Internet and from publicly accessible networks.

To deploy MetaFrame XP servers behind network firewalls, configure access for ICA Client users by allowing packets to pass to specific communication ports that ICA Clients and other Citrix components use.

As described above, Citrix recommends that ICA Clients use TCP/IP+HTTP for ICA browsing. To use this protocol with clients outside a firewall, configure the firewall to pass inbound HTTP packets on port 80, the default port for the Citrix XML service on MetaFrame XP servers. This port is usually open on firewalls for inbound HTTP packets to Web servers.

In ICA sessions, ICA Clients communicate with port 1494 on MetaFrame servers. If the clients are outside the firewall, this port must be open for inbound communication to MetaFrame servers.

## Server Farm Configurations

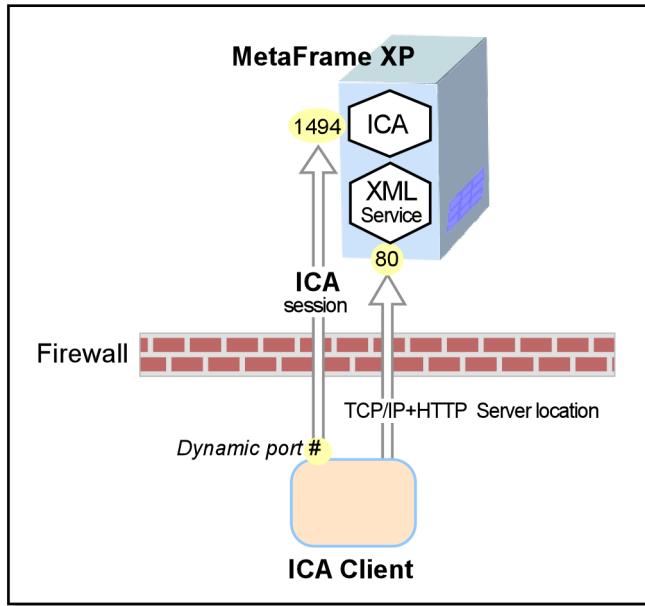
The diagrams below illustrate network configurations for Citrix server farms. The diagrams identify port numbers, components, and the recommended protocol for ICA browsing. See "Configuring ICA Browsing" on page 51 for more information.

In both diagrams, communication paths are bidirectional; arrows indicate the direction in which communication is initiated.

The first diagram shows the basic configuration for communication between ICA Client and MetaFrame XP server when a user launches a published application.

### Basic client-to-server communication

*With a firewall between ICA Clients and MetaFrame XP servers, port 80 is open for inbound HTTP to the XML service, and port 1494 is open for inbound ICA packets*



The process of running the application begins with ICA browsing (server location). TCP/IP+HTTP protocol and server addresses are specified for server location in the ICA Client.

1. The client sends a request to the Citrix XML Service on port 80 on a specified server using HTTP.
2. The XML service sends the address of a server that has the requested application.
3. The ICA Client establishes an ICA session with the MetaFrame XP server specified by the XML Service. ICA packets travel from the client to port 1494 on the server. ICA packets travel from the server to a dynamically assigned port number on the client.

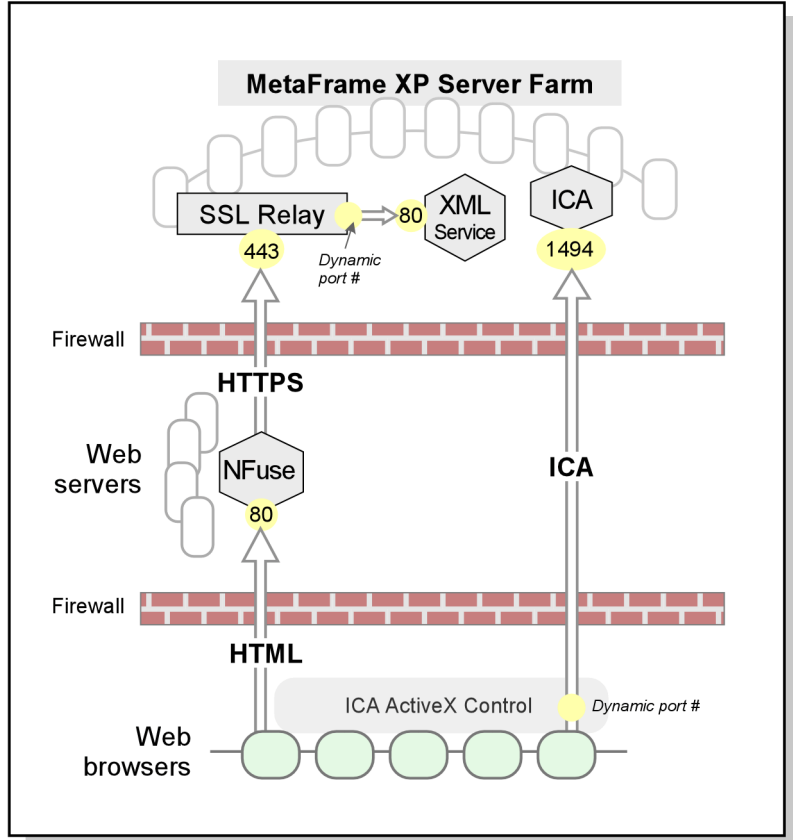
Organizations often place their Web servers in a demilitarized zone between firewalls. In this configuration, shown below, NFuse-enabled Web servers are between firewalls to isolate them from the MetaFrame server farm and ICA Clients.

### Communication with NFuse-enabled Web servers

*In a network configuration with Web servers in a demilitarized zone between firewalls, users' Web browsers send application requests to NFuse-enabled Web servers.*

*Web servers send secure (HTTPS) requests to the SSL Relay and XML Service in the server farm.*

*ICA Clients establish ICA sessions with MetaFrame XP servers on port 1494. The port used on the clients is configured dynamically.*



As with the basic configuration, Citrix recommends ICA Clients use TCP/IP+HTTP protocol to communicate through a firewall. When the user launches an application from a Web page, the ICA Client establishes an ICA session through the firewall to port 1494 on the MetaFrame server.

## Configuring IP Ports in Citrix Server Farms

The table below lists the IP ports that MetaFrame XP servers, ICA Clients, IMA, and other Citrix services use in a MetaFrame XP server farm. This information can help you configure firewalls and check to see if port conflicts exist with other software. The table includes information about setting port numbers for Citrix software when it is possible to change default settings.

| Port usage                                                     | Default port                 | Configuration                                                                                                                                                                                                    |
|----------------------------------------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICA sessions (ICA Clients to MetaFrame XP servers)             | 1494                         | See "ICAPORT" on page 245 for instructions on changing the port number. This port must be open on firewalls for inbound packets from ICA Clients to MetaFrame XP servers.                                        |
| Citrix XML Service                                             | 80                           | See "Changing the Citrix XML Service Port" on page 86 for configuration instructions. This port must be open on firewalls for inbound packets from ICA Clients (when clients use TCP+HTTP for server location).  |
| Citrix SSL Relay                                               | 443                          | See "Changing the SSL Relay Port" on page 88 for configuration instructions.                                                                                                                                     |
| MetaFrame XP server-to-server directed UDP communications      | 2512                         | See "To change the TCP port used for indirect access to the data store" on page 75 for configuration instructions.                                                                                               |
| MetaFrame XP communication with Microsoft SQL or Oracle server | 139, 1433, or 443 for MS-SQL | See the documentation for your database software.                                                                                                                                                                |
| Citrix Management Console-to-MetaFrame XP server communication | 2513                         | Not configurable.                                                                                                                                                                                                |
| ICA Clients to ICA Browser service                             | 1604 (UDP)                   | MetaFrame XP servers always respond to directed UDP requests. See "Setting up Response to ICA Client Broadcasts" on page 109 for instructions on enabling MetaFrame XP servers to respond to broadcast requests. |
| Server-to-Server directed UDP communication                    | 1604 (UDP)                   | Not configurable. This port is used only when the farm is operating in mixed mode with MetaFrame 1.8 servers.                                                                                                    |

## ICA Browsers and MetaFrame 1.8 Interoperability

This section describes issues related to ICA browsing when MetaFrame XP operates in mixed mode with a MetaFrame 1.8 server farm. For more information about selecting mixed mode and issues related to interoperability, see “Interoperability with MetaFrame 1.8” on page 65.

If you configure a MetaFrame XP to use mixed mode, two separate farms—one that contains only MetaFrame 1.8 servers and one that contains only MetaFrame XP servers—will act together so they appear to ICA Clients as one server farm.

When MetaFrame XP is in mixed mode, the two farms appear unified because ICA Browsers in each farm pool information and a MetaFrame XP server becomes the master browser of both farms. The *master browser* holds information about the published applications available on each server.

---

**Note** The ICA Browser is a system service on MetaFrame 1.8 servers. On MetaFrame XP servers, the ICA Browser is a subsystem of the IMA Service that can respond to ICA Client broadcasts. In this chapter, references to the ICA Browser apply to both the MetaFrame 1.8 browser service and the MetaFrame XP browser function.

---

In a MetaFrame 1.8 server farm, when a user launches a published application, the ICA Client asks the master ICA Browser for the address of a server that can run the application. The ICA Client also uses the master browser to find new application sets and to list servers and published applications for custom connections.

In mixed mode, ICA Clients can communicate with the single master browser for the interoperating server farms by connecting to MetaFrame servers in either farm. A client can contact the master browser through the ICA Browser using TCP/IP network protocol.

When you select mixed mode operation, you enable a MetaFrame XP farm to respond to broadcasts from ICA Clients that use TCP/IP and auto-location of servers. By default, only the master ICA Browser and RAS servers respond to broadcasts in mixed mode; the per-server option to respond to broadcasts is disabled.

For more information about ICA browsing methods that involve broadcasts, see “Configuring ICA Browsing” on page 51.

When ICA Clients use TCP/IP+HTTP for server location, they do not send broadcasts during ICA browsing and the Citrix XML Service, rather than the ICA Browser, responds to the clients, as mentioned above.

Citrix recommends you configure ICA Clients to use TCP/IP+HTTP and that you specify one or more servers in the Address List. The servers you specify must have the XML service to respond to ICA browsing. The XML Service is not available on MetaFrame 1.8 servers without Feature Release 1.

## Election of the Master ICA Browser

When a MetaFrame XP server farm operates in mixed mode, the ICA Browser runs on every server. A MetaFrame XP server takes over as the master ICA Browser for the MetaFrame 1.8 server farm and the MetaFrame XP server farm and stores information about both server farms.

The master ICA Browser is chosen by a master browser election. The ICA Browser system elects a master browser when:

- The master browser does not respond to another ICA Browser
- The master browser does not respond to an ICA Client
- A Citrix server is started
- Two master browsers are detected on the same network subnet

A set of election criteria is used to choose a master browser. An ICA Browser starts a browser election by broadcasting its election criteria. If another browser has a higher election criteria, it broadcasts its own election criteria. Otherwise, the last ICA Browser to respond to the election becomes the master browser.

The following criteria, in order, determine the master browser:

- Latest ICA Browser version
- Master browser designation by Citrix Server Administration or registry key
- Domain controller
- Longest ICA Browser up time
- Citrix server name in alphabetical order

For example, a Citrix server that has a later version of the ICA Browser Service wins election as master browser over a server that has a longer up time for the ICA Browser Service. Because the ICA Browser in MetaFrame XP is a later version than the MetaFrame 1.8 ICA Browser, a MetaFrame XP server in most cases becomes the master browser when server farms are in mixed mode.

---

**Note** If a MetaFrame XP server has “Do not attempt to become the master ICA Browser” selected, it does not participate in master browser elections.

---

You can use the **query server** command to discover the Citrix server acting as the master browser. The **query server** command displays all servers on each network transport (TCP/IP, IPX, and NetBIOS). An **M** next to the network address of a server indicates that it is the master browser for that network transport. A **B** indicates a backup browser. A **G** indicates a gateway between subnets in the MetaFrame 1.8 server farm.

## Naming the Server Farm

The name of the server farm can contain 32 or fewer characters. To operate in mixed mode (for interoperability with a MetaFrame 1.8 farm), the name must exactly match the name of the MetaFrame 1.8 server farm. Server farm names are case sensitive.

MetaFrame XP supports servers with extended characters in the server name only if your network's DNS server supports extended characters in server names.

## Changing Server Drive Letters

MetaFrame's *client drive mapping* gives ICA Client users access to their local drives when they use applications on MetaFrame servers. When users start ICA sessions, MetaFrame assigns drive letters to client drives.

- Client drives that use the same letters as the server's drives are assigned different drive letters, starting with V and going backwards through the alphabet.
- If client drive letters do not conflict with the server's drive letters, MetaFrame uses the original letters for client drives.
- Server floppy disk drives are not available to client users, so MetaFrame uses the drive letters for floppy disk drives specified on the ICA client devices. Non-Windows ICA Clients that support floppy drive mapping can be manually configured with specific drive letter mappings for each drive.

Default drive mappings for sessions are shown in the following table. Client drives C and D are renamed V and U, because the server drives use the letters C and D.

|               | Logical drive letter | Drive letter in ICA sessions |
|---------------|----------------------|------------------------------|
| Client drives | A (floppy drive)     | A                            |
|               | B (floppy drive)     | B                            |
|               | C                    | V                            |
|               | D                    | U                            |

|               | Logical drive letter | Drive letter in ICA sessions |
|---------------|----------------------|------------------------------|
| Server drives | C                    | C                            |
|               | D                    | D                            |
|               | E                    | E                            |

To make drive access more familiar for client users, you can change the server drives to use letters that are not likely to be used by client devices. Doing so ensures that client drives retain their original drive letters. The following table shows an example of drive letters used if you change the drive letters of a MetaFrame server.

|               | Logical drive letter | Drive letter in ICA sessions |
|---------------|----------------------|------------------------------|
| Client drives | A (floppy drive)     | A                            |
|               | B (floppy drive)     | B                            |
|               | C                    | C                            |
|               | D                    | D                            |
| Server drives | C                    | M                            |
|               | D                    | N                            |
|               | E                    | O                            |

---

**Warning** If you intend to change a server's drive letters, do it during MetaFrame XP installation. If you change server drive letters after MetaFrame XP installation, you must do it before installing any applications.

---

If you change the server's drive letters, MetaFrame XP searches the following registry keys and changes all drive references to reflect the new drive letters:

```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\*
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*
HKEY_LOCAL_MACHINE\SOFTWARE\Equinox\eqn\CurrentVersion\NetRules
HKEY_LOCAL_MACHINE\SYSTEM\*
HKEY_CLASSES_ROOT\*
HKEY_USERS\*

```

MetaFrame XP also updates the pagefile entry and the following shortcut files:

```
%SystemRoot%\Profiles\Default User\*.lnk  
%SystemRoot%\Profiles\Administrator\*.lnk  
%SystemRoot%\Profiles\All Users\*.lnk
```

The first time a user logs in to the MetaFrame server after you change the drive letters, references to the old drive letters in the user's profile are updated.

## Configuring Session Shadowing

You use MetaFrame's *session shadowing* to monitor and interact with users' ICA sessions. When you shadow an ICA session, you can view everything that appears on the session display. You can also use remote control features to control the mouse and enter keystrokes from a remote location.

Shadowing can be a useful tool for training, troubleshooting, and monitoring by supervisors, help desk personnel, and teachers.

During MetaFrame XP installation, you can limit or disable shadowing. You can disable shadowing of ICA sessions on all servers in your server farm if legal privacy requirements prohibit shadowing of users' sessions. Alternatively, you may want to disable shadowing on servers that host sensitive applications, such as personnel or payroll applications, to protect confidential data. MetaFrame XP Setup provides options on the Shadowing Setup page for you to limit or disable shadowing at installation time.

---

**Important** Shadowing restrictions are permanent. If you disable shadowing, or enable shadowing but disable certain shadowing features, the restrictions cannot be changed at a later time.

Do not disable shadowing as a substitute for instituting user- and group-specific permissions for ICA connections. Disabling shadowing for ICA sessions does not affect RDP sessions. Use Terminal Server Connection Configuration to disable shadowing of RDP sessions or remove the RDP connections completely.

---

**Allow shadowing of ICA sessions on this server.** This option enables shadowing of ICA sessions hosted by the server. When you enable shadowing, you have the option to select the following restrictions:

- **Prohibit remote control of ICA sessions.** By default, MetaFrame XP gives administrators the ability to input keystroke and mouse control during session shadowing. Select this option if you want administrators to be able to shadow without input. In some cases, shadowing without input hides administrator presence.
- **Prohibit shadow connections without notification.** By default, MetaFrame XP notifies users with a prompt when an administrator is attempting to shadow their sessions. Select this option to deny administrators the ability to shadow sessions without sending this notification.
- **Prohibit shadow connections without logging.** Events such as shadowing attempts, successes, and failures can be logged in the Windows event log and examined using Event Viewer. Select this option to enable logging.

**Do not allow shadowing of ICA sessions on this server.** This option permanently disables shadowing by anyone of all ICA sessions on the server.

## Interoperability with MetaFrame 1.8

A single MetaFrame XP server farm can interoperate with a single MetaFrame 1.8 server farm when the MetaFrame XP farm is set to *mixed mode*. This mode provides limited pooling of connection license counts between MetaFrame 1.8 and MetaFrame XP servers, and allows applications to be published across MetaFrame 1.8 and MetaFrame XP servers.

---

**Important** For interoperability in mixed mode, Citrix recommends that you install the latest service pack on MetaFrame 1.8 servers. You can download service packs from Citrix at <http://www.citrix.com/support/>.

---

## Configuring MetaFrame XP for Mixed Mode Operation

You can configure a MetaFrame XP server farm to operate in mixed mode when you install the first MetaFrame XP server in the farm. For information on configuring mixed mode during MetaFrame XP installation, see “Migrating Citrix Servers to MetaFrame XP” on page 84.

After you install MetaFrame XP, you can configure the farm to operate in mixed mode using Citrix Management Console. For more information, refer to the console’s online help.

When you switch a MetaFrame XP server farm from mixed mode to *native mode*, (the mode in which only IMA-based servers participate in the server farm), the MetaFrame 1.8 and MetaFrame XP server farms become completely separate.

Mixed mode is designed to facilitate migration to MetaFrame XP; it is not designed to be a permanent solution. Once all MetaFrame 1.8 servers in the MetaFrame 1.8 farm have been migrated to MetaFrame XP, be sure to set the MetaFrame XP server farm to operate in native mode using Citrix Management Console.

The following issues and limitations affect operation in mixed mode:

**ICA Browser election.** In mixed mode, a MetaFrame XP server becomes the master ICA Browser on the subnet. On each MetaFrame XP server in the farm, the ICA Browser and Program Neighborhood-related services shut down and restart. During this process, ICA Clients might be unable to refresh applications in Program Neighborhood or browse for published applications, although current ICA connections are not affected. Therefore, it's best to switch to mixed mode when the fewest users need to connect to published applications.

**ICA license gateways.** In mixed mode, license gateways in the MetaFrame 1.8 server farm do not function for license pooling. You must set up license pooling across subnets using Citrix Management Console. For more information, see "Pooling Licence Counts in Mixed Mode," below.

**Program Neighborhood service.** If you change the server farm from mixed mode to native mode before you migrate the entire MetaFrame 1.8 server farm to MetaFrame XP, you must stop and restart the Program Neighborhood service on all MetaFrame 1.8 servers that do not have MetaFrame 1.8 Service Pack 2 installed. If you do not restart the Program Neighborhood service, ICA Clients could have problems using published applications in the MetaFrame 1.8 server farm.

**Farm names.** The name you give to the MetaFrame XP server farm must be the same as the name of the MetaFrame 1.8 server farm. You enter the server farm name when you create the data store during MetaFrame XP installation on the first server in the farm.

**Subnet issues.** Do not use mixed mode if the server farm has no MetaFrame 1.8 servers operating in the same subnet as at least one MetaFrame XP server.

**Active Directory and user logons.** MetaFrame 1.8 servers do not support Active Directory. ICA Client users cannot enter user credentials in user principal name (UPN) format (user@domain) when a server farm operates in mixed mode. Entering UPN names can result in failure to display application sets and connect to published applications when clients connect to MetaFrame 1.8 servers.

## Pooling Licence Counts in Mixed Mode

Pooling MetaFrame 1.8 connection license counts across subnets is not supported when you use mixed mode. When operating in native mode, MetaFrame XP combines connection license counts into a common pool for the entire server farm.

When operating in mixed mode, there is one pool of connection license counts for each IP subnet. Within each subnet, the pooled MetaFrame XP license counts and any pooled MetaFrame 1.8 license counts are combined and available to both MetaFrame 1.8 and MetaFrame XP servers. You can configure the percentage of connection license counts to allocate to each subnet on the **Interoperability** tab in the farm **Properties** dialog box in Citrix Management Console after mixed mode is enabled.

If you use license gateways to pool licenses between subnets, the gateways do not function when the server farm is interoperating with a new MetaFrame XP server farm in mixed mode.

Here is an example of how license gateways are affected by mixed mode:

There are two subnets, with four MetaFrame 1.8 servers on Subnet A and two MetaFrame 1.8 servers on Subnet B. Each server contributes 15 pooled licenses through a license gateway. If you run the **Qlicense** command on a MF 1.8 server, it displays 90 pooled licenses.

If you install a MetaFrame XP server on each subnet and add a 10-count connection license, each MetaFrame XP server becomes the master ICA Browser on the respective subnets; the license gateway stops functioning. The MetaFrame XP servers allocate the MetaFrame XP connection license counts to each subnet spanned by the MetaFrame XP farm but the MetaFrame 1.8 licenses are no longer pooled. By default, the MetaFrame XP connection licenses are allocated to each subnet evenly.

The connection license allocation percentages can be modified as described above. Using the default license allocation (which in this example is 50% for Subnet A and 50% for Subnet B), when you run **Qlicense** on the MetaFrame 1.8 servers on Subnet A, it reports 65 pooled licenses (4 MetaFrame 1.8 Servers \* 15 licences each + (50% \* 10 MetaFrame XP license counts)).

When you run **Qlicense** on the MetaFrame 1.8 servers on Subnet B, it reports 35 pooled licenses (2 MetaFrame 1.8 servers \* 15 licences) + (50% \* 10 MetaFrame XP license counts). The result is that the servers on Subnet A allow 65 concurrent connections while the servers on Subnet B allow 35 concurrent connections.

## Pooling MetaFrame for UNIX Licenses

If your organization uses MetaFrame 1.8 for Windows and MetaFrame 1.0 or 1.1 for UNIX Operating Systems, you can pool connection licenses among the MetaFrame for Windows and MetaFrame for UNIX servers that are in the same subnet.

If you use IMA mixed mode to migrate the MetaFrame 1.8 for Windows servers to MetaFrame XP, connection license pooling continues between the MetaFrame 1.8 server farm and the MetaFrame for UNIX servers while the new MetaFrame XP server farm is in mixed mode for interoperability with MetaFrame 1.8.

When you complete the migration of MetaFrame 1.8 servers to MetaFrame XP and switch the new farm from mixed mode to native mode, the change causes license pooling with the MetaFrame for UNIX servers to stop. All licenses that were pooled in the MetaFrame 1.8 server farm move to the license pool of the new MetaFrame XP server farm.

Some organizations split licenses into two groups if their MetaFrame 1.8 for Windows and MetaFrame for UNIX servers are on different subnets. In this case, moving MetaFrame 1.8 servers to MetaFrame XP does not affect licensing because license pooling is not used with the MetaFrame for UNIX servers.

If you previously pooled license counts with MetaFrame for UNIX before migrating your MetaFrame 1.8 for Windows servers to MetaFrame XP, Citrix recommends that you configure your MetaFrame for UNIX servers in a separate subnet with sufficient connection license counts for the clients who connect to the servers. If you want to continue to pool license counts with MetaFrame for UNIX after migrating MetaFrame 1.8 servers to MetaFrame XP, contact your Citrix representative.

## Using MetaFrame XP Tools in Mixed Mode

During MetaFrame XP installation, the Setup program installs all of the tools that are included with MetaFrame 1.8. All of the utilities work with both MetaFrame 1.8 and MetaFrame XP servers, with the exceptions described below.

**Citrix Server Administration.** This utility allows you to configure various options on MetaFrame XP servers. However, the settings take effect only when the server farm is operating in mixed mode.

**Publishing Applications.** If you create or edit settings for published applications using the version of Published Application Manager included with MetaFrame XP, you cannot edit or delete the published applications using the version of Published Application Manager from MetaFrame 1.8. Use the version of the utility included with MetaFrame XP or installed with Service Pack 2 for MetaFrame 1.8.

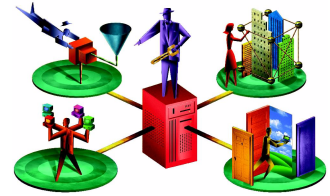
MetaFrame XP does not support publishing videos using Citrix VideoFrame 1.0. Videos can still be launched from an ICA session using a Cvi file.

**Shadowing.** In native mode, the Shadow Taskbar displays MetaFrame XP servers in a server farm. In mixed mode, the taskbar also displays MetaFrame 1.8 servers in the MetaFrame 1.8 server farm that is interoperating with the MetaFrame XP farm.

**Client printer configuration.** Use Citrix Management Console for all printer configuration and printer management for ICA Client users.



# Installing MetaFrame XP



This chapter describes how to install and set up MetaFrame XP on Windows servers. Be sure you have completely read “Planning Your MetaFrame XP Deployment” on page 31 before you begin to install MetaFrame XP.

This chapter includes the following topics:

- Creating the Data Store with SQL Server or Oracle, page 71
- Starting MetaFrame XP Installation, page 74
- Choosing Options During Setup, page 74
- Migrating Citrix Servers to MetaFrame XP, page 84
- Changing the Citrix XML Service Port , page 86
- Setting Up Citrix SSL Relay, page 87
- Unattended Setup of MetaFrame XP Servers, page 90
- Cloning a MetaFrame XP Server, page 90
- Uninstalling MetaFrame XP, page 92
- Installing Citrix Management Console on Other Computers, page 92

## Creating the Data Store with SQL Server or Oracle

To use Microsoft SQL Server or Oracle for a server farm’s data store, use your database management software to create a database. Then, during MetaFrame XP Setup, configure each server’s ODBC driver to connect to the database. The following procedures explain how to create databases using Microsoft SQL Server and Oracle.

If you are setting up your farm to use Microsoft Access, you do not need to read this section and can skip to “Starting MetaFrame XP Installation” on page 74. Using a Microsoft Access database involves creating a database locally during the installation of MetaFrame XP on the first server in the farm.

## Authenticating to the Data Store during Setup

During MetaFrame XP installation, the Setup program asks you to enter user credentials to access the server farm's data store database. There are several issues associated with user authentication to the data store when you use SQL Server.

SQL Server has two methods to verify user login IDs: with Windows NT authentication using the network login ID, or with SQL Server authentication using a login ID and password entered by the user.

- If you select the SQL Server authentication option, the MetaFrame XP Setup program can validate the credentials you enter and inform you if you enter incorrect or unauthorized credentials.
- If you control access through Windows NT authentication, the Setup program cannot validate the credentials you enter for database access unless the account you use to log on to the server has a privilege of “Act as part of the operating system.” This privilege is not usually set on user accounts.

If the account you use to log on to the server does not have the privilege “Act as part of the operating system,” the account must have access to the database, otherwise installation will fail, even if you enter the correct user name and password of a user that does have database access, because the Setup program cannot impersonate the user you specify.

---

**Important** If Setup cannot validate the credentials you enter, it cannot warn you if you enter the user name or password incorrectly or the credentials do not grant access to the database. When the Setup program attempts to access the database it will fail, and then initiate an uninstall of MetaFrame XP. To install MetaFrame XP, start the Setup program again and enter correct credentials for access to the database.

---

### ► To create a data store database with Microsoft SQL Server

Some dialog boxes might differ from the descriptions in this procedure, depending upon the version of Windows and SQL Server you use.

1. Run SQL Enterprise Manager on your Microsoft SQL server (**Start > Programs > Microsoft SQL Server 7.0 > Enterprise Manager**).
2. In the Enterprise Manager's left pane, expand the tree until you reach the folder level.

3. Right-click the Databases folder and choose **New Database**.
4. A dialog box appears. In the **Name** box, enter a name and click **OK**.
5. Expand the Security folder.
6. Right-click **Logins** and choose **New Login**.
7. A dialog box appears with the **General** tab displayed. In the **Name** box, enter a name. Make note of the name because you will need to enter it during MetaFrame XP installation.
8. In the **Authentication** section of the **General** tab, click **SQL Server authentication** and enter a password. Remember the password; you must enter it during MetaFrame XP installation.
9. In the **Defaults** area of the **General** tab, change the **Database** to the name you specified in Step 4.
10. Click the **Database Access** tab. In the **Database** list, select the database name specified in Step 4.
11. In the **Database Roles** list, select **DB\_Owner**. Leave other selected roles checked.
12. Click **OK**. You are prompted to confirm your password. Doing so completes database creation.

► **To create a data store database with Oracle**

1. If you do not already have Oracle installed, install it using the default database.
2. On the Oracle server, run SQL Plus. At the connection prompt, type **internal**.
3. Use the following commands as guidelines for creating a tablespace and user:

```
create tablespace MFXPIMA datafile 'D:\ORADATA\MFXPIMA.DBF'
size 5000k autoextend on next 5000k maxsize unlimited;
alter tablespace MFXPIMA default storage (pctincrease 0
maxextents unlimited);
create user MFXP identified by MFXP01 default tablespace
MFXPIMA temporary tablespace TEMP;
grant connect, resource to MFXP;
```

The tablespace is named MFXPIMA and saved in D:\ORADATA\MFXPIMA.DBF. The user is named MFXP and has the password MFXP01. Temp is the default temporary tablespace for Oracle8i. If you are using Oracle7, use TEMPORARY\_DATA instead of TEMP.

## Starting MetaFrame XP Installation

The following procedures explain how to install MetaFrame XP using the MetaFrame XP CD-ROM or a network sharepoint. For more information, including descriptions of Setup options, see “Choosing Options During Setup” on page 74.

---

**Important** If you want to install MetaFrame XP from a network share, do not attempt to install from a path that contains space characters, such as `N:\cdimages\MetaFrame XP`.

---

### ► To begin MetaFrame XP installation

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM into the CD drive.
  - If your CD drive supports Autorun, the MetaFrame XP splash screen appears.
  - If the splash screen does not appear or you are installing from a network sharepoint, from the **Start** menu, click **Run** and type `d:\autoroot.exe` where *d* is the path to your CD-ROM drive or network sharepoint.
3. Click MetaFrame XP **Setup**.

Once MetaFrame XP Setup begins, a series of information pages and dialog boxes ask you to select options and configure MetaFrame XP. Click **Next** to continue after you complete each entry. If you want to return to a previous page to make changes, click **Back**. If you click **Cancel**, the Setup program quits without finishing installation.

## Choosing Options During Setup

The following sections describe the various aspects of MetaFrame XP configuration that you perform in the MetaFrame XP Setup program.

### Data Store Configuration

This section explains how to configure MetaFrame XP servers to connect to the data store for a server farm. For background information on the data store, see “Choosing a Database for the Data Store” on page 37. For background information on IMA zones, see “Configuring Zones and Data Collectors” on page 110.

## Using Access for the Data Store

To use a Microsoft Access database for a server farm data store, you create the database when you install MetaFrame XP on the first server in the farm. Additional servers connect to the first server using TCP port 2512. If you want to use another port, see the procedure below for changing the port on the first server. You can specify the port number for the other servers during MetaFrame XP installation.

### ► To create a server farm using Access for the data store

1. On the first page of the Data Store Configuration wizard, select **Create a new farm** and click **Next**.
2. On the second page of the wizard, select **Use a local database as the data store** and click **Next**.
3. On the third page of the wizard, enter a name for the IMA zone.
4. On the fourth page of the wizard, enter a name for the server farm. Farm names can contain up to 32 characters and can contain spaces. Click **Next** to continue.
5. Continue with MetaFrame XP installation.

### ► To add more servers to the server farm

1. On the first page of the Data Store Configuration wizard, select **Join an existing farm**.
2. On the second page of the wizard, select **Connect to a data store set up locally on another server**.
3. On the third page of the wizard, enter a name for the IMA zone.
4. On the fourth page of the wizard, enter the name and TCP port of the server that contains the Access data store.
5. Continue with MetaFrame XP installation.

### ► To change the TCP port used for indirect access to the data store

1. On the MetaFrame XP server containing the data store, change the value of the registry key HKLM\Software\Citrix\IMA\ImaPort to the desired port number.
2. On all other MetaFrame XP servers in the farm, change the value of the registry key HKLM\Software\Citrix\IMA\PsserverPort to the desired port number.

## Using SQL or Oracle for the Data Store

The following procedure describes options that appear during MetaFrame XP Setup as part of the MetaFrame XP installation. The same procedures are used whether the data store is a Microsoft SQL database or an Oracle database.

Before starting MetaFrame XP Setup, you must create the data store database using your database management software; see the procedures “To create a data store database with Microsoft SQL Server” on page 72 or “To create a data store database with Oracle” on page 73.

► **To create a server farm with an SQL or Oracle data store**

Follow this procedure only on the first server in the farm on which you install MetaFrame XP. See the next procedure for configuring the remaining servers in the farm.

1. On the first page of the Data Store Configuration wizard, select **Create a new farm** and click **Next**.
2. On the next page, select **Use a third party database as the data store** and click **Next**.
3. On the third page of the wizard, enter a name for the IMA zone.
4. The next page displays a list of MetaFrame XP-supported ODBC drivers installed on the server. Select the driver for your database and click **Next**.

---

**Important** If your driver does not appear in the list, cancel MetaFrame XP Setup, install the driver, and then restart MetaFrame XP Setup.

---

5. Follow the procedure “To configure the ODBC driver for Microsoft SQL Server” on page 77 or “To configure the ODBC driver for Oracle” on page 80.
6. On the next page, enter the credentials to access the database. The credentials you enter must match those specified during database creation and ODBC driver setup. After verifying the credentials, click **Next**.
7. Enter a name for the farm in the **Server Farm** box. Farm names can contain up to 32 characters and can contain spaces.

This step completes data store configuration of the first server in the farm.

► **To add more servers to the server farm**

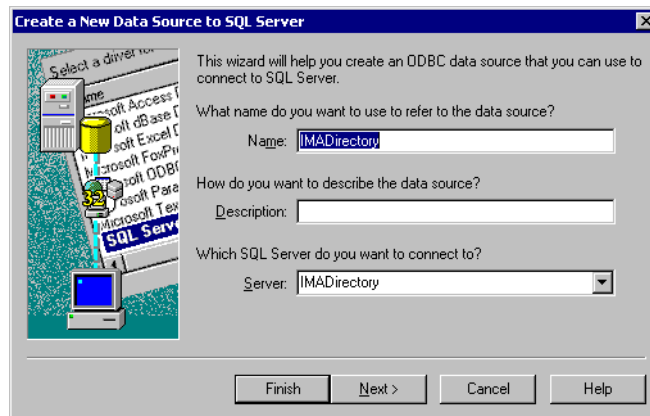
1. On the first page of the Data Store Configuration wizard, select **Join an existing farm** and click **Next**.
2. On the next page, select **Direct data store connection** and click **Next**.
3. Follow the instructions in the procedure “To create a server farm with an SQL or Oracle data store” beginning with Step 3.

## Configuring ODBC Drivers

This section provides step-by-step instructions on configuring ODBC drivers for Microsoft SQL Server and Oracle databases. Some of the dialog boxes shown are components of Microsoft's ODBC manager and may differ from those you see, depending upon the version of Windows and the ODBC driver you are using.

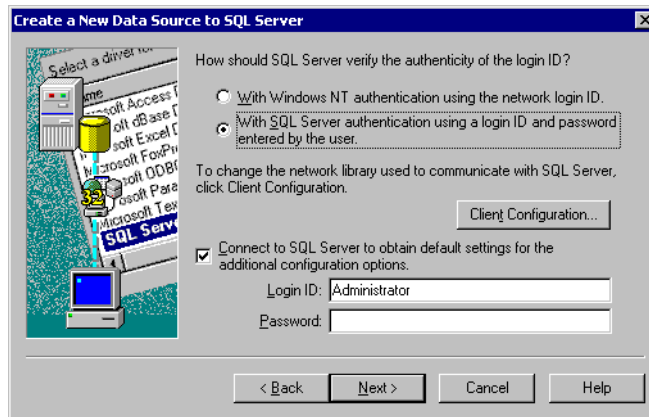
### ► To configure the ODBC driver for Microsoft SQL Server

1. After you select your SQL driver from the **Installed ODBC Driver** list in MetaFrame XP Setup, the following dialog box appears:



Leave the **Name** field as is. Click the pull-down list next to the **Server** field and select your SQL Server machine in the list. Click **Next**.

2. The following dialog box appears:

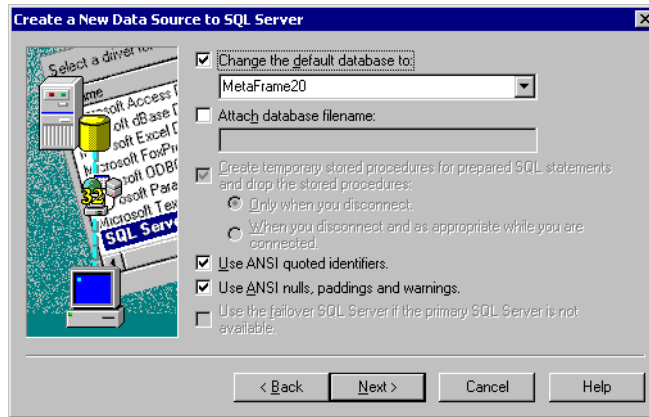


This dialog box lets you specify the method of authenticating the login ID that MetaFrame XP will present to the SQL Server when accessing the data store. To authenticate successfully, the SQL Server and MetaFrame XP must use the same authentication method. Make sure the database created for MetaFrame XP by the database administrator is using SQL Server authentication.

Choose **With SQL Server authentication**. In the **Login ID** field, specify the login created by the database administrator. In the **Password** field, specify the password for the login ID. Click **Next**.

If the ODBC manager is unable to authenticate to the database, it prompts you to re-enter the login ID and password.

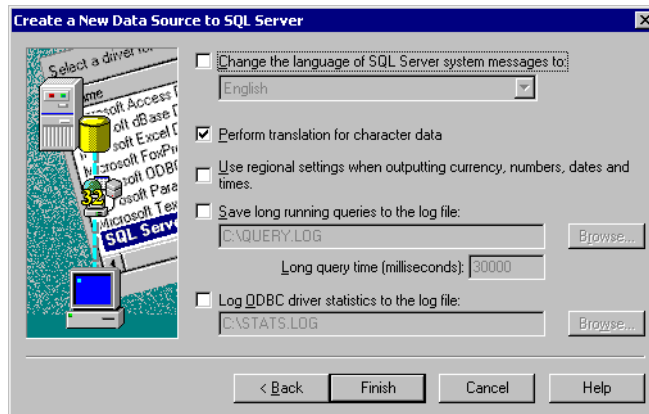
3. The following dialog box appears:



Click **Change the default database to** and select the name of the database you created for MetaFrame XP if it is not already selected.

**Note** SQL Server login IDs can be configured to log in to a database by default. If in your SQL Server administrative program the login ID has been set to log in to the data store database by default, you do not have to specify a default database in this dialog box.

4. Click **Next**. The following dialog box appears:

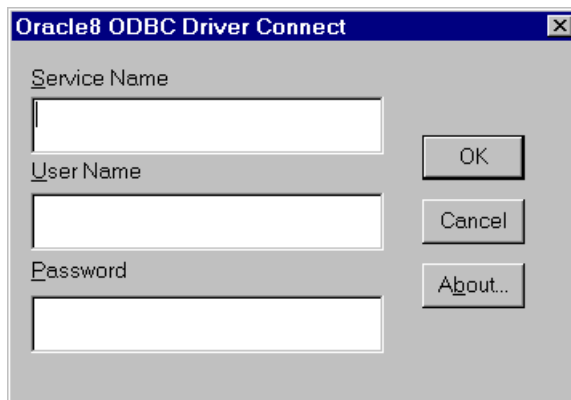


Click **Finish** to accept these values. A dialog box lets you test the new data source name. Click **Test Data Source**. If the test completes successfully, click **OK** and then click **OK** to complete data source name configuration.

5. Follow the steps in the procedure, “To create a server farm with an SQL or Oracle data store” on page 76, beginning with step 6.

► **To configure the ODBC driver for Oracle**

1. If you select an Oracle driver from the **Installed ODBC Driver** list in MetaFrame XP Setup, the following dialog box appears:



2. In the **Service Name** box, type the service name used when the Oracle client was installed. In the **User Name** and **Password** boxes, type the user name and password created on the Oracle server for the data store.
3. Click **OK**.

This completes the Oracle data store setup. You are now ready to install MetaFrame XP. Follow the steps in the procedure “To create a server farm with an SQL or Oracle data store” on page 76, beginning with step 6.

## Configuring Network ICA Connections

Citrix's ICA protocol works with the following network protocols: TCP/IP, IPX, SPX, and NetBIOS. Protocols installed under Windows networking are automatically selected during MetaFrame XP Setup. If a protocol appears grayed-out and unchecked, it was not configured under Windows networking.

By default, Setup enables ICA connections over all network protocols already installed on the server. Deselect protocols you do not want to support. The TCP/IP protocol cannot be deselected; you must install support for TCP/IP.

---

**Tip** If you want to enable ICA connections over a network protocol that is not available at the time of MetaFrame XP installation, you can do so after installation. After Setup completes, install the protocol under Windows networking and then use the Citrix Connection Configuration utility to enable ICA connections for the newly-installed protocol.

---

## Configuring Asynchronous ICA Connections

You can add modems and configure asynchronous ICA connections during MetaFrame XP installation. When the **TAPI Modem Setup** page appears, click **Add Modems** to install modems. The system modem installer appears to guide you through modem installation. If TAPI modems are installed on your server, the **Asynchronous ICA Connections** page is displayed for you to select modems for asynchronous ICA connections.

Select the devices to configure for asynchronous ICA connections. You can select multiple modems if desired. Click **Next** to accept the selected modems as valid asynchronous ports.

### ► To install a modem during MetaFrame XP installation

1. If no modems are already configured in your system, the **Install New Modem** dialog box appears. If you already have modems configured, proceed to Step 8.
  - If you want to auto-detect your modem, click **Next**.
  - If you want to manually select your modem, select the **Don't detect my modem** check box and click **Next**. Proceed to Step 4.
2. If you have a multiport async adapter, select a port on which to run auto-detection. MetaFrame XP Setup auto-detects the modem connected to the specified port. You can configure multiple ports with the same modem type in Step 5 below.
3. Windows searches for your modem. The detected modem is displayed. If this is the correct modem type, click **Next** and proceed to Step 5.
  - If you want to select another modem type, click **Change**.
  - If no modem is detected, click **Next**.
4. Select the manufacturer and model of your modem, or do one of the following, and click **Next**.
  - If you do not see your modem on the list, select a similar model from the same manufacturer or a generic modem type.
  - If your modem came with a driver on disk, click **Have Disk** and follow the manufacturer's instructions for installing the driver.

5. The port selection dialog box appears. Select the port(s) to which the modem is connected. Click **Next** when finished.
6. If this is the first modem installed, the **Location Information** dialog box appears. Specify the country you are in, the area or city code, the number that must be dialed to reach an outside line, and whether the modem should use tone or pulse dialing. These settings are used with all modems. When finished, click **Next**.
7. A dialog box appears informing you that the modem has been set up successfully. Click **Finish**.
8. The **Modems Properties** dialog box appears. To change the configuration of an existing modem, select the modem and click **Properties**. To add another modem, click **Add** and repeat Steps 1 through 5. When you are finished, click **Close** and then click **Next** in the **TAPI Modem Setup** dialog box.

Modem installation is complete.

## Installing ICA Client Software

During MetaFrame XP installation, the ICA Client Distribution wizard installs ICA Clients and ICA Client-related utilities from a Citrix ICA Client CD-ROM or network share point. For more information on deploying and configuring ICA Clients, see “Deploying ICA Clients to Users” on page 159.

---

**Note** You can skip ICA Client setup during MetaFrame XP installation. To cancel the ICA Client Distribution wizard, click **Cancel** when the wizard appears.

---

**Create or update ICA Client Images.** The ICA Client Creator is a Citrix server utility you use to create installation disks for Windows and DOS ICA Clients. The ICA Client Distribution wizard places copies of ICA Clients in the database from which this utility creates client disks.

**Create or update the ICA Client Update Database.** Client Auto Update is a feature that enables you to schedule the download and installation of the latest ICA Client software from MetaFrame XP servers to client devices. The ICA Client Distribution wizard places copies of ICA Clients in the database used by Client Auto Update.

**Install or upgrade the ICA pass-through Client on the server.** MetaFrame XP servers can include an installed copy of the ICA Win32 Client. You can publish its Program Neighborhood interface functionality to all clients. The ICA Client Distribution wizard installs the ICA Win32 Client on the MetaFrame XP server.

**Install ICA Client Administrator's Guides.** The wizard can copy the *ICA Client Administrator's Guides* in PDF format to the Program Files\Citrix\Documentation directory on the server.

When the wizard prompts you to specify the location of your ICA Client CD-ROM, insert your ICA Client CD in the server's CD-ROM drive and click **Next**. Alternatively, you can specify the location of a network-shared ICA Client CD-ROM or CD-ROM image. In the **ICA Client CD Image** field, specify the location of your installation media. The wizard requires you type in or browse to the location of the file ICASetup.ini. This file is located on the root of your ICA Client CD.

The wizard includes typical and custom installation paths. A typical installation does the following:

- Installs the Client Auto Update Database and copies each ICA Client into the database
- Installs the ICA Client Creator database and copies each ICA Client into the database
- Installs the ICA Win32 Client on the server
- Copies the *ICA Client Administrator's Guides* to the %SystemDrive%\Program Files\Citrix\Documentation\ICA Clients directory on the server

When performing a custom installation, a dialog box gives you options for installing ICA Clients and documentation.

If you select **Create/Update Citrix ICA Client Images** or **Create/Update Citrix ICA Client Update Database**, dialog boxes let you select ICA Clients to install. For example, if you choose to **Create/Update Citrix ICA Client Images**, a dialog box lets you select ICA Clients to add to the ICA Client Creator's database. Clear the check boxes for ICA Clients you do not want to add to the database.

## Entering Licenses and Product Codes

During MetaFrame XP installation, a dialog box lets you enter serial numbers for MetaFrame XP licenses. Another dialog box asks you to enter your *product code*, a string that specifies the product license to use on the MetaFrame XP server. License serial numbers and the product code are printed on a label in the MetaFrame XP product package.

You are not required to enter licenses or product codes during installation. However, you must enter licenses in the server farm and you must assign a product to a server for the server to accept ICA connections.

A MetaFrame XP server farm pools product licenses and connection licenses. You can enter one or more license serial numbers during MetaFrame XP installation. You can use Citrix Management Console to enter licenses after installation. You must also activate licenses that you enter in the server farm. Do not enter the same serial number more than once.

To enter a serial number during installation, type the number in the dialog box and click **Add**. Repeat this step to install additional licenses. Click **Next** when you finish.

If you entered a license serial number, Setup displays a recommended product code. Verify that the product code matches the product code printed in your MetaFrame XP product package. If you did not enter a license serial number, type the product code from your MetaFrame XP product package.

For more information on licenses and product codes, see “Licensing MetaFrame XP” on page 119.

## NFuse Web Server Extension

NFuse is the Citrix portal software that lets users access published applications with Web browsers. If Internet Information Server is installed on the server, MetaFrame XP Setup installs NFuse by default. The NFuse logon page allows users to run published applications from their Web browsers. By default, the Web page for the server is changed to the NFuse logon page. Setup gives you the option to not change the default Web page or not install NFuse. See the *NFuse Administrator's Guide* for more information on NFuse. The *NFuse Administrator's Guide* is available in PDF format on the NFuse CD. The NFuse CD also includes the Web Site wizard and example Web sites that you can use to create a custom-tailored NFuse front end to published applications.

To install NFuse, you must have IIS 4.0 and the Microsoft Java Virtual Machine installed. If they are not installed, NFuse is not installed during MetaFrame XP installation. If you choose not to install NFuse as part of the MetaFrame XP installation, you can install it later from the NFuse CD.

## Migrating Citrix Servers to MetaFrame XP

MetaFrame XP can run in mixed mode, with MetaFrame 1.8 servers and MetaFrame XP servers co-existing in a single farm. Citrix recommends you use this mixed mode only during pilot deployments or migrations, not as a permanent solution. See “Interoperability with MetaFrame 1.8” on page 65 for more information on the limitations of mixed mode.

## Supported Migration Paths

MetaFrame XP supports migration of Citrix servers that are running the following *WINFRAME* or MetaFrame versions:

MetaFrame 1.8 + FR 1

MetaFrame 1.8 + SP1

MetaFrame 1.8

MetaFrame 1.0

*WINFRAME* 1.8 + SP5C

*WINFRAME* 1.8

---

**Note** Servers running *WINFRAME* cannot be migrated directly to Windows 2000 Servers. They must be migrated to Windows NT 4.0 Server, Terminal Server Edition.

---

### ► Overview of migration process

1. Configure the SQL data store server if you are using Microsoft SQL or Oracle for the MetaFrame XP server farm's data store.
2. Install MetaFrame XP on a Citrix server other than the current master ICA Browser.
  - During MetaFrame XP installation, choose the option to create a new IMA-based server farm.
  - Name the new MetaFrame XP server farm exactly the same as the existing MetaFrame 1.8 server farm.
  - Enter the appropriate product code and serial numbers for your Citrix migration to MetaFrame XP license.

This server becomes the new master ICA Browser, so it must be a server capable of handling the increased load. You can use the **query server** command line utility to discover the Citrix server acting as the master browser. An **M** next to the network address of a server indicates that it is the master browser.

When the server restarts after MetaFrame XP installation, the browser election process causes published applications and server browsing to be temporarily unavailable. Therefore, it is best to do this initial migration outside of normal working hours.

3. Verify that you can connect to the MetaFrame XP server and check the migration log file to confirm that all applications were migrated successfully. The MetaFrame XP Setup program displays the name of the script file. The file is located in %SystemRoot%\System32.
4. Migrate additional MetaFrame 1.8 servers. During installation, choose to join an existing farm.

5. After all MetaFrame 1.8 servers have been migrated to MetaFrame XP, change the server farm to operate in native mode by selecting the farm node and choosing **Properties** in Citrix Management Console. Clear the check box under MetaFrame Interoperability on the **Interoperability** tab. When you make this change, license sharing with license gateways stops. For more information, see “Pooling Licence Counts in Mixed Mode” on page 67.

## Changing the Citrix XML Service Port

If you plan to change the port used by the Citrix XML Service on MetaFrame XP servers, make sure the port you plan to use is not used by any other application.

For a list of ports in use, type **netstat -a** at a command prompt. Make a note of the port number you specify. If you use a port other than the default port 80, you must configure your NFuse Web server and any ICA Clients using TCP/IP + HTTP server location to use the port you choose. See the *NFuse Administrator's Guide* for instructions on configuring NFuse to use a different port. See the *ICA Client Administrator's Guides* for instructions on configuring the ICA Clients to use a different port.

---

**Important** All of the MetaFrame servers in the server farm must use the same TCP port for the XML service. This requirement includes all MetaFrame 1.8 and MetaFrame XP servers when operating in mixed mode.

---

### ► To specify the XML Service port during installation

During MetaFrame XP installation, Setup prompts you for an available TCP/IP port on the server. Select to share port 80 with Internet Information Server (if installed) or enter a port number in the TCP/IP Port box and click **Next**. If the specified port is in use, Setup notifies you.

---

**Note** If you are migrating a Citrix server to MetaFrame XP, Setup does not display the dialog box for you to specify the XML Service port. Instead, the port remains the same as that used by the Citrix server before MetaFrame XP installation. You can change the port after installation as described below.

---

### ► To change the XML Service port after installation

---

**Important** Use this procedure only if you do not want to share the port used by Internet Information Server.

---

1. Use the Services icon in the Control Panel to stop the Citrix XML Service. On Windows 2000 servers, this icon is in the Administrative Tools folder in the Control Panel folder.

---

**Important** If your MetaFrame XP server is running Windows 2000, you must close the **Services** window after stopping the service.

---

2. At a command prompt, type **ctxxmlss /u** to unload the Citrix XML Service from memory.
3. Type **ctxxmlss /rnn**, where *nn* is the number of the port you want to use. For example, **ctxxmlss /r88** forces the Citrix XML Service to use TCP/IP port 88.
4. Restart the Citrix XML Service in the Control Panel.

► **To manually configure Citrix XML to share the TCP port with Internet Information Service**

1. Use the Services Control Panel to stop Citrix XML Service. On Windows 2000 servers, this icon is in the Administrative Tools folder in the Control Panel folder.

---

**Important** If your MetaFrame XP server is running Windows 2000, you must close the **Services** window after stopping the service.

---

2. At a command prompt, type **ctxxmlss /u** to unload the Citrix XML Service.
3. Copy Wpnbr.dll and Ctxxmlss.txt to the IIS scripts directory on your Web server. These files are installed to %SystemRoot%\System32\ during MetaFrame XP installation. The default scripts directory is: %RootDrive%\inetpub\scripts\
4. Use Internet Service Manager to give the files Read and Write access.
5. Stop and restart the Web server.

## Setting Up Citrix SSL Relay

The Citrix SSL Relay secures communications between an NFuse-enabled Web server and your MetaFrame server farm. The data sent from the NFuse-enabled Web server to the SSL Relay is decrypted and then redirected to the Citrix XML Service.

By default, the Citrix SSL Relay service listens on TCP port 443, the standard port for the SSL protocol. You can configure the SSL Relay to listen on any TCP port, but you must ensure that the port is open on any firewalls between the NFuse-enabled Web servers and the MetaFrame XP server running the SSL Relay.

► **To configure the SSL Relay**

1. Obtain a server certificate.
2. Change the SSL Relay port number, if necessary.
3. Install a server certificate.
4. Select the ciphersuites to allow. See the application help for the SSL Relay Configuration tool for instructions.
5. Change the target address or port, or add additional addresses for redundancy. See the application help for the SSL Relay Configuration tool for instructions.

## Obtaining a Server Certificate

Your organization's security expert should have a procedure for obtaining server certificates. A separate server certificate is needed for each MetaFrame XP server on which you install and run the Citrix SSL Relay. Instructions for generating server certificates using various Web server products are on the VeriSign Web site at <http://www.verisign.com>.

The SSL Relay requires certificates to be in Personal Electronic Mail (PEM) format. If your certificate is in Microsoft Internet Information Server Version 4 or 5 format, you can use the Citrix **keytopem** utility to convert it to PEM format.

Citrix NFuse Version 1.51 includes native support for the following certificate authorities:

- VeriSign, Inc., <http://www.verisign.com>
- Baltimore Technologies, <http://www.baltimore.com>

To use a different certificate authority, you must install a root certificate for the certificate authority on your NFuse server. See the NFuse documentation for instructions on installing the root certificate on your NFuse server.

## Changing the SSL Relay Port

The Citrix SSL Relay uses TCP port 443, the standard port for SSL connections. Most firewalls open this port by default. You can optionally configure the SSL Relay to use another port. Be sure that the port you choose is open on any firewalls between the NFuse-enabled Web servers and the MetaFrame XP server running the SSL Relay.

---

**Important** Microsoft Internet Information Server (IIS) Version 5.0 is installed by default on Windows 2000 Servers and allocates port 443 for SSL connections. To run MetaFrame XP on Windows 2000 Server, you must configure IIS to use a different port or configure the SSL Relay to use a different port.

---

► **To change the SSL port for Internet Information Server Version 5.0**

1. Run Internet Services Manager.
2. Click the plus sign next to the Web site in the left pane.
3. Right-click **Default Web Site** and then select **Properties**. The **Default Web Site Properties** dialog box appears.
4. Select the **Directory Security** tab and click **Server Certificate**. The Welcome to the Web Server Certificate wizard appears. Follow the instructions in the wizard to import your SSL certificate from a Key Manager backup file. Your certificate must be in Internet Information Server Key Manager format.
5. When your server certificate is installed, select the **Web Site** tab in the **Default Web Site Properties** dialog box.
6. Change the SSL Port number to something other than 443.
7. Click **OK** to close the **Default Web Site Properties** dialog box.

► **To change the SSL Relay port number**

1. Run the Citrix SSL Relay Configuration Tool.
2. Select the **Connection** tab and type the new port number in the **Relay Listening Port** box.
3. Click **OK**.

See the NFuse documentation to reconfigure NFuse-enabled Web servers with the new port number.

## Installing a Server Certificate

► **To convert a Microsoft Internet Information Server Key Storage File or personal information exchange (.pfx) protocol file to PEM format**

At the command prompt, type:

```
%SystemRoot%\sslrelay\keytopem input-file output-file
```

*input-file* is the server certificate file. *output-file* is the name for the new PEM-formatted certificate file. Citrix recommends you use .pem as the extension for the output file.

► **To install a PEM-formatted server certificate**

1. Copy the file to the \certs subdirectory of the keystore directory (%SystemRoot%\sslrelay\keystore, by default).
2. Choose **Start > Programs > Citrix > MetaFrame XP > Citrix SSL Relay Configuration Tool**.

3. On the **Relay Credentials** tab, select your server certificate in the **Server Certificate** list and enter the certificate password in the **Password** box.
4. Click **OK** to save changes and close the Citrix SSL Relay Configuration Tool.

## Unattended Setup of MetaFrame XP Servers

Use unattended setup to install MetaFrame XP without assistance from an administrator.

Unattended setup uses an *answer file* to provide answers to the questions asked during Setup. A sample answer file is located on the MetaFrame XP CD-ROM at MF\unattend.txt. Instructions are provided in the file for setup options. Copy the sample answer file to another location and modify it for your needs. At a minimum, you must include the product code and data store configuration information.

---

**Important** You cannot use unattended mode to install the first server in a server farm.

---

### ► To perform an unattended installation

1. Insert the MetaFrame XP CD-ROM in the CD-ROM drive of the server, or insert the MetaFrame XP CD-ROM in a CD-ROM drive accessible over the network. If your CD-ROM drive supports Autorun, the MetaFrame XP CD-ROM startup window appears. Close the window.
2. Choose **Run** from the **Start** menu. Type one of the following (replace *d* with the drive letter of the CD drive or sharepoint and *answer\_file* with the path and name of the answer file):
  - For Windows NT 4.0, Terminal Server Edition, type:  
***d:\tse\mf\setup /u:answer\_file***
  - For Windows 2000, type:  
***d:\w2k\mf\setup /u:answer\_file***
3. Follow the displayed instructions.

## Cloning a MetaFrame XP Server

If your organization uses system imaging utilities to clone standard server configurations, with a few adjustments you can also clone MetaFrame XP servers.

► **To prepare a MetaFrame XP server for imaging**

---

**Important** Do not attempt to image the first server in a farm using Microsoft Access for the data store. Do not attempt to image a server with an SSL certificate installed.

---

1. During MetaFrame XP installation, use the default IMA zone name and be sure to enter the appropriate product code.
2. After the installation is completed and the server reboots, use the Services icon in the Control Panel to stop the Independent Management Architecture service and set it to start manually. On Windows 2000 Server, the Services icon is in the Administrative Tools folder within the Control Panel folder.

---

**Important** If your MetaFrame XP server is running Windows 2000, you must close the **Services** window after stopping the service.

---

3. Delete the following values from the Windows registry:

```
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\HostId  
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\ImaPort  
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\MasterRanking  
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\PSRequired  
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\RassPort  
HKEY_LOCAL_MACHINE\Software\Citrix\IMA\Runtime\ZoneName
```

4. Image the server using the cloning software and then install the image on additional servers.
5. Change the Independent Management Architecture service to start automatically and start the service.

When you apply the image to new servers, the imaging tool must change the SID of the server to a unique value. You must also change the server name so that it is unique in the server farm.

► **To configure MetaFrame XP on a newly imaged server**

1. Add the registry key  
HKEY\_LOCAL\_MACHINE\Software\Citrix\IMA\ServerHost and set the value to the name of the server.
2. Edit the wfname.ini file on the root of the drive where you installed MetaFrame XP and replace the name with the name of the machine.
3. Using the Services icon in the Control Panel, set the Independent Management Architecture service to start automatically.

4. Reboot the machine.
5. If desired, obtain an SSL certificate for the server.

## Uninstalling MetaFrame XP

You must uninstall MetaFrame XP before you reinstall the software, rather than reinstalling over an existing installation. If you have a beta version of MetaFrame XP installed, you must uninstall the beta version before installing the retail version.

Before uninstalling MetaFrame XP, log off any ICA sessions and exit all programs running on the server.

Uninstalling MetaFrame XP removes the server from the server farm.

### ► To uninstall MetaFrame XP

1. Exit any applications running on the server.
2. Choose **Start > Settings > Control Panel > Add/Remove Programs**.
3. Do either:
  - On Terminal Server Edition, select **Citrix MetaFrame XP 1.0** and click **Add/Remove**.
  - On Windows 2000 Servers, click **Change or Remove Programs**, select **Citrix MetaFrame XP 1.0**, and click **Change/Remove**.
4. The MetaFrame XP Uninstall program appears. Follow the displayed instructions. When the uninstallation program finishes, it restarts the server.

## Installing Citrix Management Console on Other Computers

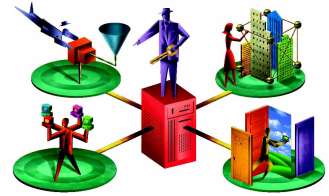
Citrix Management Console is the centralized management utility you use to administer your MetaFrame XP server farm. You can use the MetaFrame XP CD to install the Citrix Management Console on workstations where you do not install MetaFrame XP. For more information on console requirements, see “Citrix Management Console Requirements” on page 34. The console is installed with MetaFrame XP automatically.

► **To install the console on another computer**

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM into the CD drive.
  - If your CD drive supports Autorun, the MetaFrame XP splash screen appears.
  - If the splash screen does not appear or you are installing from a network sharepoint, from the **Start** menu, click **Run** and type **d:\autoroot.exe** where *d* is the letter of your CD drive or network sharepoint.
3. Click **MetaFrame XP Setup**.
4. Follow the instructions in the Setup wizard.



# Configuring MetaFrame XP Servers and Farms



This chapter describes options and settings for MetaFrame XP servers and server farms. It includes information about tools and utilities you use to manage servers and server farms.

This chapter contains the following topics:

- Management Tools for MetaFrame XP, page 95
- Citrix Management Console, page 99
- Configuring MetaFrame XP Properties, page 106
- Configuring Latency Reduction for ICA Clients, page 116

Some configuration options are part of the MetaFrame XP Setup program. For more information, see “Installing MetaFrame XP” on page 71.

## Management Tools for MetaFrame XP

Citrix provides a comprehensive suite of utilities for managing MetaFrame servers, ICA Clients, and Citrix server farms. MetaFrame XP includes the Citrix Management Console and additional tools, including utilities that let you manage MetaFrame 1.8 servers when your organization uses both MetaFrame 1.8 and MetaFrame XP.

This section provides an overview of the features and operations of MetaFrame XP tools. The MetaFrame XP Setup program installs the Citrix Management Console and other tools on the MetaFrame XP server by default when you install MetaFrame XP.

---

**Note** Citrix Management Console might not be installed on a MetaFrame XP server. You can install Citrix Management Console on a MetaFrame XP server or a workstation (Windows NT or Windows 2000) by selecting Citrix Management Console Setup on the startup screen of the MetaFrame XP CD-ROM.

---

## Overview of MetaFrame XP Management Tools

The following summaries of management tools for MetaFrame XP tell you where to find detailed information on the use of each tool.

**Citrix Connection Configuration.** Use this utility to configure the connections that ICA Clients use to link to MetaFrame servers. For information, refer to the online help in Citrix Connection Configuration, and see “Configuring ICA Client Connections” on page 137.

**Citrix Management Console.** Use this centralized administration tool to monitor and manage many aspects of MetaFrame XP operation from single servers to multiple server farms. For information, see “Citrix Management Console” on page 99.

**Citrix SSL Relay Configuration.** Use this utility to secure communication between an NFuse-enabled Web server and your MetaFrame server farm. For information, refer to the online help in Citrix SSL Relay Configuration.

**ICA Client Creator.** Use this utility to create diskettes or disk images for installing ICA Client software. For information, see “Deploying ICA Clients Using Diskettes” on page 169.

**ICA Client Update Configuration.** Use this tool to manage the Client Update Database on a MetaFrame XP server. The database contains current ICA Client software for each supported client platform and can be used to install ICA Clients when users log on to the server. For information, see “Deploying ICA Clients to Users” on page 159.

**Shadow Taskbar.** Shadowing allows administrators to view and control ICA Client sessions remotely. You can use the Shadow Taskbar to shadow sessions and to switch among multiple shadowed sessions. You can also use Citrix Management Console to shadow ICA sessions. For information on shadowing, see “Shadowing ICA Sessions” on page 204.

**SpeedScreen Latency Reduction Manager.** Use this tool to configure local text echo and other features that improve the user experience on slow networks. For information, see “Configuring Latency Reduction for ICA Clients” on page 116.

## Using MetaFrame XP Tools and Utilities

As with other Windows programs, you can use several methods to run the management tools installed with MetaFrame XP. The most common method is to choose a shortcut from the **Start** menu on the MetaFrame XP server console.

- Shortcuts to launch MetaFrame XP management tools are in the **Programs > Citrix > MetaFrame XP** submenu on the **Start** menu.
- Shortcuts for Citrix Management Console and Citrix documentation are in the **Programs > Citrix** submenu on the **Start** menu.
- The ICA Administrator Toolbar displays a series of buttons you can click to launch Citrix management tools and utilities. See “The ICA Administrator Toolbar” below.

## The ICA Administrator Toolbar

The ICA Administrator Toolbar is a configurable desktop toolbar. You can use the toolbar to launch MetaFrame XP management tools and other programs.

After you install MetaFrame XP and restart the system, the ICA Administrator Toolbar appears at the right edge of the screen. The default configuration of the toolbar provides a button to run each MetaFrame XP management utility.

To run a utility program from the toolbar, click the program’s button on the toolbar.



*ICA Administrator Toolbar (floating)*

You can reposition the ICA Administrator Toolbar by dragging it away from the right edge of the screen. If you drop the toolbar on the desktop, it becomes a floating toolbar. If you want the toolbar to snap to the edge of the screen, drag it close to the edge and then drop it (release the mouse button) when an outline of the toolbar appears along the edge of the screen.

---

**Note** A button for Citrix Management Console appears on the ICA Administrator Toolbar if you install the console at the same time you install MetaFrame XP on a server. If you install the console later, the button does not appear, but you can add it to the toolbar as described in this section.

---

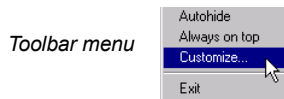
### ► To display the Administrator Toolbar

When the toolbar is not displayed, you can make it appear by choosing **Start > Programs > Citrix > MetaFrame XP > ICA Administrator Toolbar**.

## Configuring the ICA Administrator Toolbar

You can adjust the ICA Administrator Toolbar in the same ways you can adjust other toolbars in Windows. For example, you can drag the edge of the toolbar to make the toolbar larger or smaller.

You can right-click the toolbar to display a toolbar menu.



The menu contains commands that you can choose to change the behavior of the toolbar:

**Autohide.** Choose Autohide to make the toolbar hide itself except when you point to it (move the mouse pointer to the screen edge where the toolbar is attached). This option has no effect if the toolbar is floating on the desktop. To turn off the Autohide option so the toolbar is always visible, choose Autohide again.

**Always On Top.** This option makes the ICA Administrator Toolbar always appear in front of other windows and objects on the screen when it is displayed. When Always On Top is not selected, windows and other objects can appear in front of the toolbar when it is at the edge of the screen or floating.

**Customize.** Choose Customize if you want to add or remove buttons from the ICA Administrator Toolbar. See the next section for more information on using Customize.

**Exit.** Choose Exit to remove the toolbar from the screen. A dialog box asks if you want to display the toolbar again when you start MetaFrame XP. Click Yes if you want to display the toolbar when MetaFrame XP starts. Click No if you do not want to display the toolbar again.

## Customizing the ICA Administrator Toolbar

You can use the Customize command in the ICA Toolbar menu to change the buttons displayed on the toolbar.

► **To customize the toolbar**

1. Right-click the ICA Administrator Toolbar and choose **Customize** from the pop-up menu.
2. In the dialog box that appears, use the following options to customize the toolbar:
  - To hide a button on the toolbar, clear its check box in the list labeled **Show these files as buttons**.
  - To place a new button on the toolbar, click **Add Files**. Select the file you want to place on the toolbar and click **Add**. You can select any type of file, including executable files, help files, and text files.
  - To change the order of buttons, select a button name in the list. Then, click the arrow button above or below the word **Move**.
  - To remove an item from the list, select its name and click **Delete**. You can delete buttons and spaces that you add to the toolbar.
  - To change the name of a button, select it in the list and click **Rename**. Then type the new name in the dialog box and click **OK**.
  - To add space between buttons, select an item in the list and click **Add Space**. A space appears above the selected item in the list.
  - To restore the default button arrangement, click **Use Default**.
3. When you finish making changes, click **OK** to update the toolbar.

## Citrix Management Console

Citrix Management Console is the central console program that you use to monitor and manage MetaFrame XP servers and IMA-based Citrix server farms.

Citrix Management Console is a Java-based, extensible program that ships with MetaFrame XP and with other Citrix management products. Each Citrix product adds software modules to the console to provide controls and other features for those products.

For example, Load Manager is an optional component that works with MetaFrame XP. When Load Manager is enabled, it adds load evaluation options to Citrix Management Console.

Therefore, the features and capabilities of the console depend on the Citrix products and licenses that you have installed in a Citrix server farm. The commands, controls, and features that you see in the console can vary from the descriptions and illustrations in this manual, depending on the products that you have installed.

The MetaFrame XP setup program installs the console on each MetaFrame XP server by default. You can also use the MetaFrame XP CD-ROM to install the console on other workstations that you want to use to manage Citrix server farms.

In a Citrix server farm with MetaFrame XP servers, you can use Citrix Management Console to do the following:

- Configure servers and farm settings from any connected workstation
- View information about current sessions, users, and processes
- Set up and manage printers for ICA Client users
- Publish applications and monitor application usage
- Enter, activate, and assign MetaFrame XP licenses
- Monitor, reset, disconnect, and reconnect ICA Client sessions
- Send messages to ICA Client users and shadow their ICA sessions

---

**Note** Scrolling with the Microsoft wheel mouse is not supported in the Citrix Management Console.

---

## Using Citrix Management Console

To use Citrix Management Console, you must be an authorized user whose Windows user account is included in the Citrix Administrators group in the console. To run the console, you must enter your user name, password, and network domain.

To log in to a Citrix server farm with the console, you specify any Citrix server in the server farm. The console connects to the Citrix server and then displays information for the entire Citrix server farm and for the individual servers in the farm.

In the **Log On** dialog box for the console, the name of the last server that the console connected to appears in the **Citrix Server** box. The drop-down menu displays the names of other servers that the console has connected to recently.

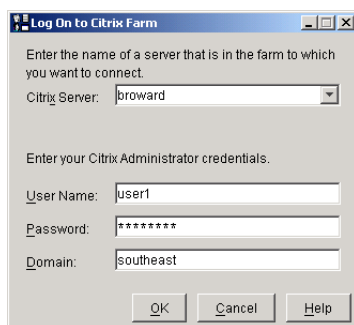
---

**Important** Citrix Management Console can monitor and manage MetaFrame XP servers and other IMA-based Citrix servers. It cannot be used to manage Citrix server products, including MetaFrame 1.8, that are not based on IMA. When MetaFrame XP servers are set to interoperate with MetaFrame 1.8 servers, the console displays information on MetaFrame XP and IMA-based servers only.

---

► **To use Citrix Management Console**

1. From the **Start** menu, choose **Programs > Citrix > Citrix Management Console**, or click the console button on the ICA Administrator Toolbar.
2. When the console starts, a dialog box asks you to log on to a MetaFrame XP server.
  - In the **Citrix Server** box, enter the name of a MetaFrame XP server in the server farm, or select a server from the drop-down menu. You can connect to any server in a farm to manage the entire farm.
  - Type your user name, domain, and password for your Windows user account. The account must be in the Citrix Administrators group in the console.



3. Click **OK**.



**Tip** You can click the Citrix Management Console button on the ICA Administrator's toolbar to launch the console.

## Switching Server Farms and Logging Off

When you are using the console and you want to log in to a different Citrix server farm, choose **Actions > Log Off from Citrix Farm**. The **Log On** dialog box appears and you can specify another Citrix server to log on to. You also use the **Log Off from Citrix Farm** command to exit the console if you do not want to keep the console running.

## Using Online Help in Citrix Management Console

For detailed information about using Citrix Management Console, refer to online help in the console.

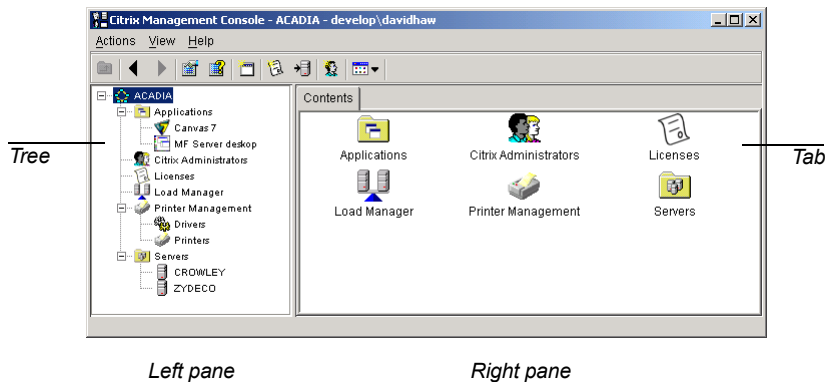
► **To view online help in Citrix Management Console**

When Citrix Management Console is running, choose **Help > Contents and Index**. The online help system provides detailed information about terms, concepts, and procedures related to management of Citrix server farms.

## Data Displayed in Citrix Management Console

When you are connected to a Citrix server farm, Citrix Management Console displays a window with two main parts, called *panes*.

- The left pane shows a hierarchical list of the components of a Citrix server farm.
- The right pane displays information about the object selected in the left pane.



Several common terms are used in this and other Citrix documentation to refer to the items you see in the Citrix Management Console window.

### The Tree View

The list of items in the left pane is referred to as a *tree*, because the pane displays the server farm as a hierarchy, with objects that branch off from a root object. The tree view is similar to the tree view in Windows Explorer and Microsoft Management Console.

The object at the top of the tree in Citrix Management Console represents a Citrix IMA-based server farm. The next level of objects under the server farm represent management features and components in the server farm. These objects are called *nodes*. In a MetaFrame XP environment, the nodes represent Applications, Printer Management, Licenses, and Servers.

Objects that appear under the nodes in the console tree view represent specific features and items in the server farm. For example, individual published applications appear under the Applications node and individual Citrix servers appear under the Servers node.

The function of the console tree is similar to the Windows Explorer tree.

- A plus symbol (+) indicates that a branch of the tree is compressed. Click the symbol or select the node and press the right-arrow key to expand the branch.
- A minus symbol (-) indicates that a branch is expanded. Click the minus symbol or select the node and press the left-arrow key to compress the branch and hide the objects under the node.

When an object is selected, the object appears highlighted in the tree. To select another object, you can click the object or use the arrow keys to move the highlight.

You cannot select multiple objects in the console tree. However, you can select multiple objects on the Contents tab in the right pane by pressing CTRL and clicking each object or pressing Shift and clicking to select a contiguous range of objects.

## Tab Views

The right pane of the console displays one or more screens, which are called *tabs* because each screen has a tab-shaped label at the top. The tab or tabs that are available in the right pane are based on the node or object that is selected in the tree.

The name of the tab appears at the top of each tab. One tab at a time is selected in the right pane, and the contents of one tab appear in the right pane. To use a different tab, click its name.

In most cases, a **Contents** tab appears in the right pane when you select a node in the tree. The Contents tab displays the objects that are under the selected node. You can double-click an object on the **Contents** tab to open the object; this action has the same effect as expanding a branch and selecting an individual object such as a published application or a Citrix server in the tree.

## Controlling Refresh of Data in the Console

To reduce network traffic and improve responsiveness, the Citrix Management Console does not refresh all data automatically. In general, the console receives notifications of events as they occur on Citrix servers and updates the displayed data in response to these events. However, some changes you make in the console and some events, such as a server coming online in the farm or an ICA session starting, does not cause the console to update the displayed data.

You can enable automatic data refresh so that the console automatically updates the display at a fixed rate. When you enable automatic refresh, you can specify the refresh rate. Whether automatic refresh is enabled or not, you can refresh the console's display manually at any time.

Refresh the console display when you view license usage data. Even if automatic refresh is enabled, the display of license usage data might not be current until you perform a manual refresh. When you view data about ICA sessions and servers, it is also useful to refresh the display manually to be sure that you view current information.

► **To refresh the data displayed in Citrix Management Console**

Choose **View > Refresh** or press F5. The Refresh command updates the information that appears on the current tab and tree view.

► **To enable automatic refresh of data in Citrix Management Console**

To enable all automatic refresh options in Citrix Management Console, you must enable automatic refresh for servers, server folders, applications, and licensing.

1. Choose **View > Auto Refresh Settings** from the **View** menu.
2. In the **Auto Refresh Interval** dialog box, you can select options to enable automatic data refresh for servers, server folders, and applications. After you enable an option, you can set the refresh interval. Enter the time in seconds to set the interval at which automatic refresh occurs.
3. Click **OK** to apply the refresh settings to the console.
4. Select the Licenses node in the tree and choose **Actions > License > Auto Refresh Settings**.
5. Select the option to enable licensing and enter the time in seconds to set the data refresh interval.
6. Click **OK** to apply the refresh settings to the console.

## **Controlling Access to Citrix Management Console**

You control the management of Citrix server farms by controlling access to the Citrix Management Console.

Citrix Management Console uses standard Windows logon and user account authentication to grant access to designated Citrix administrators.

During MetaFrame XP setup, the installation program asks you to enter credentials for a primary Citrix administrator. If you are installing the first MetaFrame XP server in a new server farm, the user account that you specify becomes the first Citrix administrator account for the new server farm. The setup program gives this Citrix administrator account read-write privileges. You must log on to the console with this account to add other users to the Citrix Administrators group.

To authorize administrators to use Citrix Management Console, a Citrix administrator with read-write privileges logs in to the console and sets up other administrator accounts. To add administrator accounts, right-click the Citrix Administrators node and choose **Add Citrix Administrator**. In the dialog box that appears, select the user and group accounts that you want to add to the Citrix Administrators group in the console.

---

**Tip** You can click the New Citrix Administrator button on the toolbar or choose **Actions > New > Citrix Administrator** to add accounts to the Citrix Administrators group.

---

When you add Citrix administrators, the dialog box displays the Windows user and group accounts from the domain you select. You also use the dialog box to specify the privileges to assign to a group of Citrix administrator accounts.

## Configuring Citrix Administrator Accounts

When you add a Citrix administrator, you can select individual user accounts and group accounts from Windows NT and Active Directory domains. For information about management of Windows domains and user accounts, refer to your Windows system documentation or online help.

---

**Tip** Use your standard network administrators group to add Citrix Administrator accounts to the console, so administrators have access to manage network resources, including print servers.

---

When you configure Citrix administrator accounts, you can grant read-write or read-only privileges. Citrix administrators who do not have read-write privileges cannot make changes to any Citrix administrator accounts, including their own. For example, an administrator with read-only permission cannot delete other Citrix administrators or change the privilege settings of administrator accounts.

In addition, Citrix administrator accounts that have read-only privileges cannot use commands that affect ICA sessions and processes in Citrix Management Console. The prohibited session commands are Connect, Disconnect, Shadow, and Reset. The Terminate command, which terminates an active ICA Client process on the server, also cannot be used by administrators with read-only privileges.

One Citrix administrator account that has read-write privileges must always exist in the server farm. Therefore, no administrator can delete the last read-write Citrix administrator account from the Citrix Administrators group in the console.

## Configuring MetaFrame XP Properties

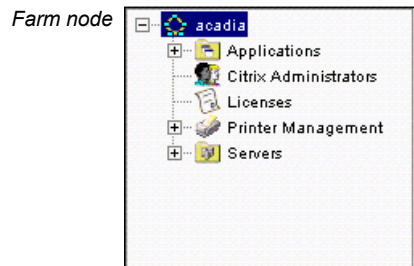
Configuring options and settings for MetaFrame XP servers and Citrix server farms takes place in two stages. First, you set options when you install MetaFrame XP on the first server in a server farm and on other servers that you add to the farm. Then, as the server farm is operating, you can adjust settings on individual servers and set options for the server farm using the Citrix Management Console.

**Setup options.** Some configuration options are available only during MetaFrame XP setup. For example, you choose the name of a server farm when you install MetaFrame XP on the first server in the farm. If you set restrictions on ICA shadowing during setup, the restrictions are permanent on the MetaFrame XP server. For details on setup options for MetaFrame XP servers and server farms, see “Installing MetaFrame XP” on page 71.

**Operating options.** After you create a MetaFrame XP server farm, you can use Citrix Management Console to change settings such as ICA display options and to manage ICA sessions on individual servers. You also use the console to configure options that affect performance, zone configuration, and interoperability with MetaFrame 1.8 servers for the entire server farm.

## Properties of MetaFrame XP Server Farms

After you log on to a server in the farm with Citrix Management Console, the console title bar displays the name of the server farm. In the left pane of the console, the farm name is the label of the main node at the top of the tree.



This section describes ways to manage farm configuration after you install MetaFrame XP. For options you can configure only during MetaFrame XP setup, see “Installing MetaFrame XP” on page 71.

MetaFrame XP also includes some commands that you can run from the command prompt to monitor and configure servers. For information on these commands, see “Command Reference,” Appendix A in this manual.

## Using the Farm Properties Dialog Box

To configure Citrix server farm properties, log on to the console and select the server farm node in the console tree. The server farm is represented by the first node, at the top of the tree in the left pane of the console. The label of the server farm node is the name of the server farm.

Most configuration options and settings for a Citrix server farm are available in the **Properties** dialog box for the farm in Citrix Management Console. When you configure farm settings, the settings apply to the entire farm, including servers that are temporarily offline.

To display the **Properties** dialog box for the server farm, select the farm node and choose **Properties**. The **Properties** command is available in the **Actions** menu, on the console toolbar, and from the menu that appears when you right-click on the farm node.

Configuration options for the server farm appear on tabs in the **Properties** dialog box. All of the settings in the dialog box apply to the entire farm. Some settings affect each MetaFrame XP server in the farm. Other settings apply to the farm’s data store, which all servers in the farm use to store and retrieve farm configuration information.

When you make changes in the **Properties** dialog box, the changes do not take effect until you click **OK**, which closes the dialog box and applies all the current settings. If you click **Cancel**, the dialog box closes and all changes you made in the dialog box are discarded.

For information about specific options, click the **Help** button in the **Properties** dialog box.

## ICA Display Options

Use the **ICA Display** tab to configure the transmission of display information and application graphics to clients.

You can optimize the display for ICA Clients by adjusting the amount of memory used for graphics and selecting other options that conserve bandwidth for ICA display transmission.

ICA uses highly optimized protocols to send the screen display of applications to ICA Client users. On standard (non-dialup) networks, the default settings are designed for optimum performance. You do not need to reconfigure ICA Display settings under most circumstances. However, you can adjust these settings for better performance when many users dial in to your server farm, or users' network access includes slow WAN links.

In the Resource Limits area, you can set a maximum amount of memory to be used on the MetaFrame XP servers for ICA display.

---

**Note** You can use the **ICA Display** tab and the TWCONFIG utility (see "MetaFrame XP Command Reference," Appendix A) to set the maximum amount of memory used for an ICA session on the MetaFrame XP server.

---

You might want to set a memory limit that accommodates typical sessions but prevents excessive memory usage by sessions that specify extremely large display sizes, such as 32,000 by 32,000 pixels at 24 bits per pixel, for example. If a session exceeds the memory limit that you set, the server scales down the session to a lower resolution to accommodate the memory limit.

When the memory limit forces the server to degrade the session, the option you choose on the **ICA Display** tab specifies whether the server reduces the session display size (resolution) or color depth.

### Effects of Memory Limits on Seamless ICA Sessions

When an ICA Client initiates a session in seamless mode, the size of the session is equivalent to a full-screen session. For example, a seamless session initiated by a client with a desktop size of 1,600 by 1,200 pixels, at 24 bits per pixel color depth, requires 5,760,000 bytes (5.5MB) of memory.

When a client device running Windows 98 or Windows 2000 has multiple monitors, the total desktop size is the total of both monitors, and the memory required for a seamless session is based on the total display size of both monitors.

If you set a memory limit that is less than required for the display size and color depth, the server scales down the session. If the option to reduce the resolution of the session is selected on the **ICA Display** tab in the console, the application launches in a remote desktop rather than a seamless mode window. If the option to reduce color depth is selected, the server might be able to accommodate a seamless mode session at a lower color depth.

## General MetaFrame XP Options

Use the **MetaFrame Settings** tab to control communication and other aspects of IMA, the Citrix protocol for communication among servers in your server farm. You also use this tab to change the way MetaFrame XP servers respond to broadcasts from ICA Client users.

### Setting up Response to ICA Client Broadcasts

With the options in the Broadcast Response area on the **MetaFrame Settings** tab, you can control whether the data collectors and RAS servers in your server farm respond to UDP broadcasts from ICA Clients.

You might want servers to respond to broadcasts if you have legacy ICA Clients that require this, or if all your ICA Clients use TCP/IP (rather than TCP/IP + HTTP) to auto-locate MetaFrame servers.

Select the option **Data Collectors respond to ICA Client broadcast (UDP) messages** if your ICA Clients do not have a specific server address specified for locating applications in the server farm and use TCP/IP protocol to auto-locate MetaFrame servers.

To use the UDP response option, you must also configure the server farm of MetaFrame XP servers to interoperate with a server farm of MetaFrame 1.8 servers. To do this, select **Work with MetaFrame 1.8 Servers** on the **Interoperability** tab in the **Properties** dialog box for the MetaFrame XP server farm. If you do not select this option, and MetaFrame XP detects MetaFrame 1.8 ICA Browsers on the same network subnet, it disables the broadcast response.

If you have ICA Client users who dial in to MetaFrame XP servers using RAS, select **RAS servers respond to ICA Client broadcast messages**. Because a dial-in client communicates only with the RAS server and cannot contact ICA Browsers or data collectors to locate the server farm's published applications, this option lets the dial-in clients locate applications in the server farm.

---

**Important** If two server farms of MetaFrame XP servers are on the same subnet and both farms respond to ICA Client broadcasts, the ICA Clients will have problems browsing for published applications in the server farms.

---

### ICA Client Time Zones

If you have users that connect to the server farm from different time zones, you can configure the farm to support the local time zones of client devices. Not all ICA Clients support this feature; refer to the *ICA Client Administrator's Guides* for more information.

Local time zone support provides correct local date and time stamps on files created by clients.

To enable local time zone support, select the option in the Client Time Zones area. For ICA Clients that do not report their local time zone to MetaFrame XP servers, the local time is estimated. You can disable local time estimation if this option causes incorrect local time display in ICA Clients.

### SNMP License Notification

If you use an SNMP-based network management product, the MetaFrame XP SNMP Agent can send traps if the usage of Citrix licenses in the server farm exceeds thresholds that you specify.

You can select options to enable SNMP traps on a farm-wide basis on the **Properties** tab for the server farm, and on the **Properties** tab for individual servers.

To enable SNMP notification messages, select **Enable SNMP Agent** on the **SNMP** tab in the **Properties** dialog box.

In the **Set** box, enter the percentage of available pooled licenses below which the SNMP Agent alerts the management product. The alert status remains in effect until the percentage of available pooled licenses exceeds the value in the **Reset** box.

SNMP notification is available when you install the MetaFrame XP SNMP Agent for Tivoli NetView or HP OpenView.

## Configuring Zones and Data Collectors

In an IMA-based Citrix server farm, a *zone* is a grouping of Citrix servers that you configure. By default, all servers in a farm that are on the same network subnet belong to the same zone. You can use the **Zones** tab in the **Properties** dialog box to create and configure additional zones.

Zones are designed to enhance the performance of a Citrix server farm by allowing geographically related servers to be grouped together, whether they are connected to the same network subnet or not.

- If all the servers in a farm are in one location, you can configure the farm with a single zone without causing slower performance or making the farm more difficult to manage.
- If you manage an enterprise server farm with servers in different geographic regions, you can place servers into zones based on the location of the servers. This can improve performance and make management of the farm more efficient.

On the **Zones** tab in Citrix Management Console, you can view the servers that belong to each zone in the farm. You can create, delete, and rename zones. To change the membership of a server from one zone to another, select the server from the list of servers in the zone and then move the server to another zone.

## Data Collectors

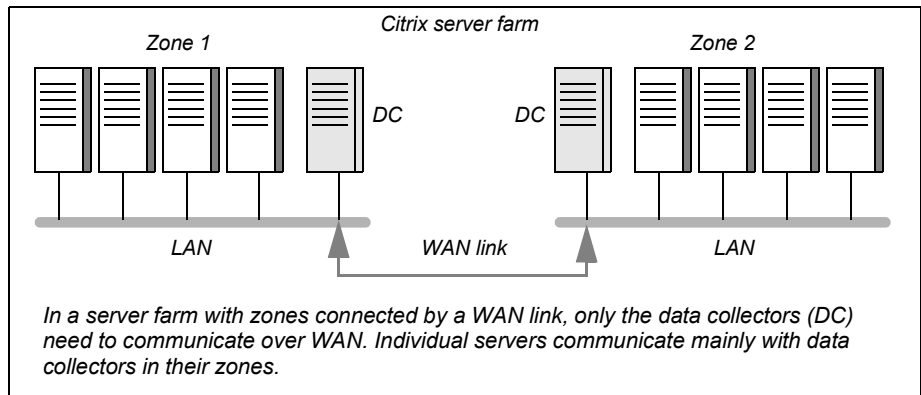
Each zone in a server farm contains one Citrix server that is designated as the *data collector* for the zone. A zone's data collector receives information from each MetaFrame XP server in the zone.

Data collectors store information about the servers and published applications in the server farm. The data collector knows the addresses of each server and the applications that are available on each server in the zone.

---

**Note** Data collectors in IMA-based server farms are similar in function to ICA Browsers in MetaFrame 1.8 server farms. However, data collectors use TCP/IP for server-to-server communication. ICA Browsers use UDP for server-to-server communication.

---



Data collectors are communication gateways between zones in server farms that have more than one zone. Each data collector communicates with the other data collectors in other zones in the server farm.

Because data collectors serve as communication gateways among zones, every server in the farm does not need to communicate with every other server. Servers that are separated by long distance and slow communication links do not add communication traffic to the server farm. Only data collectors send messages between zones.

---

**Tip** Because of the way data collectors concentrate communication among the servers in a farm, use zones if you have a geographically diverse farm.

---

## Election of Data Collectors

A zone in a Citrix server farm *elects*, or selects, a data collector for the zone if a new server joins the zone or the current data collector becomes unavailable. A data collector becomes unavailable if the server goes down or is disconnected from the network, or if you move the server to another zone.

When a zone elects a new data collector, it uses a preference ranking of the servers in the zone. You can set the preference ranking for the servers in a zone on the **Zones** tab in the server farm's **Properties** dialog box.

Each zone has four levels of preference for election of data collectors. The preference levels, in order from highest to lowest preference, are:

1. Most Preferred
2. Preferred
3. Default Preference
4. Not Preferred

All servers in a zone are assigned to one of the four election preference levels. When the zone elects a new data collector, it tries to select a server from the first preference level. If no servers at this level are available, the zone selects a server from the second level, and so on.

When you create a farm, the election preference for all servers is Default Preference, except for the first server added to the zone, which is set to Most Preferred and is the zone's initial data collector.

On the **Zones** tab in the console, a colored symbol appears next to each server name to indicate the election preference setting.

You can change the default election preference to designate a specific server as the data collector. To do this, set the election preference for the server to Most Preferred. If you do not want some servers to be data collectors, set the election preference for those servers to Not Preferred.

Assign servers that you do not want to become data collectors (except as a last resort) to the Not Preferred level.

---

**Tip** In large server farms and enterprise networks with high client traffic, you can reduce the possibility of data collector performance issues by using dedicated data collectors. You can do this by setting up data collectors on MetaFrame XP servers that do not host applications for client sessions.

---

### Setting the Election Preference for Data Collectors

To change a server's data collector election preference, select the server in the list on the **Zones** tab and click **Set Preference**. In the dialog box, select the election preference level to assign to the server.

To designate a specific server to be a zone's data collector when the next election occurs, make sure that the server has the highest election preference. You can do this by making the server the only one set to Most Preferred level, for example. The zone will elect the server to be the data collector when the next election occurs.

If you create a new zone, the first server that you move to the new zone becomes the zone's data collector, and its preference level is set to Most Preferred.

Zones do not maintain backup data collectors. Instead, the data store for the entire Citrix server farm maintains information that is used by each data collector.

## MetaFrame XP Server Properties

In addition to settings for an entire farm, you can configure settings for individual MetaFrame XP servers in the farm through Citrix Management Console. You can access most server configuration options from the **Properties** dialog box for each server.

When you change settings for a server's properties, the console applies the settings immediately if the server is available. If the server is offline or busy, the console applies the settings as soon as the server becomes available.

This section describes ways to manage server configuration after you install MetaFrame XP. For options you can configure only during MetaFrame XP setup, see "Installing MetaFrame XP" on page 71. MetaFrame XP also includes some commands you run from the command prompt to monitor and configure servers. For information on these commands, see "Command Reference," Appendix A.

## Using the Server Properties Dialog Box

To configure the settings of an individual server, select the server under the Servers node in the console tree. Then choose the Properties command from the **Actions** menu, the console toolbar, or by right-clicking. The Properties command displays the **Properties** dialog box for the selected server. This dialog box contains several tabs with options and settings that apply to a MetaFrame XP server. The settings that you configure in the **Properties** dialog box apply to the selected server only.

For example, you can configure SNMP traps on the **SNMP** tab in a server's **Properties** dialog box. These SNMP settings apply to a single server. If you select the farm node and use the **Properties** dialog box, you can set SNMP settings that apply to all servers in the server farm.

---

**Note** The Servers node in the console tree does not include a **Properties** dialog box. When you want to apply settings to multiple servers, you use the Farm node or another node in the console tree.

---

Use the **Properties** dialog box for servers to view and configure the following:

**Published application information.** On the **Published Applications** tab, view the names, status, connection type, and other information about the applications that are published on a selected server.

**SNMP traps.** On the **SNMP** tab, you can enable the Citrix SNMP Agent and select the events that trigger SNMP messages on the selected server. For more information, see “SNMP License Notification” on page 110.

**Server and network information.** The **Information** tab displays software, network, and licensing information for the selected server. This tab shows the versions of Windows and Citrix software that are installed and the installation date. The tab also displays the product code that is assigned to the server, which specifies the type of product license that the server uses. You can also verify that logons by ICA Client users are enabled and check the network address on this tab.

**Product code.** The **Information** tab displays the product code that is set on the selected server. The product code specifies the type of product license the server uses from the server farm's license pool. You cannot change the product code on this tab. However, you can change the product code if necessary for the server to use the correct license from the license pool. You might want to change the product code if you purchase a product upgrade or a full retail license for a server that uses an evaluation license. For more information about product codes and licensing, see “Product Codes” on page 125.

**Installed hotfixes.** On the **Hotfixes** tab, you can view a list of Citrix hotfixes that are installed on the selected server. The tab displays the name and installation date of each hotfix that is installed.

**ICA Display options.** The options on the **ICA Display** tab affect graphics and video display on ICA Clients. These settings apply to the applications that run on the selected server. The options let you conserve bandwidth used to transmit graphics to ICA Clients and to specify the size of the memory buffer to use for graphics display. You can configure these settings for all servers in the farm by using the **ICA Display** tab in the **Properties** dialog box for the farm.

**ICA Browser and logon settings.** The **MetaFrame Settings** tab displays various configuration settings for the selected server. The tab contains options that affect the selected server's response to UDP broadcasts from ICA Clients. UDP broadcasts allow ICA Clients to browse for published applications in a server farm that includes ICA Browser-based MetaFrame servers. Other options let you control the logging of shadowing events on the server.

**Citrix XML Service.** The **MetaFrame Settings** tab displays the port used by the Citrix XML service for TCP/IP+HTTP browsing by ICA Clients. This setting cannot be edited here, but you can change the port for a server with a command. To change the port setting, at the system command prompt, type **ctxmlss /rxxxxx**, with the actual port number following **/r**. This configures the service to auto start on port **xxxxx**. To activate the new settings, you have to stop and start the service.

**Controlling printer bandwidth.** If you want to limit the bandwidth that MetaFrame XP uses for printing by clients, you can enter a value on the **Printer Bandwidth** tab. To remove a bandwidth limit, select the **Unlimited** option. This setting applies to the selected server. You can view the current setting for each server on the **Bandwidth** tab when you select **Printer Management** in the console tree.

For more information about client printing and bandwidth, see "Bandwidth Tab" on page 213.

## Selecting Other Settings to Configure

To change some settings for individual servers, you use the Licenses, Printer Management, and Applications nodes in the Citrix Management Console tree.

You can:

- Assign licenses to servers and monitor license usage from the Licenses node
- Publish applications on servers and monitor application usage through the Applications node
- View and replicate printer drivers installed on servers from the Printer Management node

Select individual MetaFrame XP servers to configure settings that are not associated with application publishing, printer management, or licensing.

## Configuring Latency Reduction for ICA Clients

Delays between entry and echo of mouse movements and keyboard input is one of the primary frustrations that client users can experience on a high-latency network connection. SpeedScreen features in MetaFrame XP and the ICA Client software enable almost immediate echo of mouse movements and keystrokes at the ICA Client.

Use the SpeedScreen Latency Reduction Manager to customize SpeedScreen settings for a MetaFrame XP server, individual published applications, and input controls within applications. You can save a SpeedScreen configuration file and then deploy the file across your server farm.

To launch SpeedScreen Latency Reduction Manager, from the **Start** menu, choose **Programs > Citrix > MetaFrame XP > SpeedScreen Latency Reduction Manager**.



**Tip** You can launch SpeedScreen Latency Reduction Manager by clicking its button on the ICA Administrator Toolbar.

---

By default, instant mouse click feedback is enabled and local text echo is disabled for all applications.

You can enable local text echo on an application-by-application basis only. If you use this feature, the programs to which you apply it must use only standard Windows APIs for displaying text, or the settings will not work correctly.

---

**Important** Test all aspects of an application with local text echo in a non-production environment before enabling text echo for your users.

---

With SpeedScreen Latency Reduction Manager, you can also configure local text echo settings for individual input fields within an application. See the application help for the SpeedScreen Latency Reduction Manager utility for more configuration information.

For general information about SpeedScreen options, see the online help in the SpeedScreen Latency Reduction Manager.

## Deploying SpeedScreen Settings

After you use Speed Screen Latency Reduction Manager to configure SpeedScreen settings for the server (and specific applications, if you want), the manager saves the settings for each application in the directory C:\WINNT\system32\ss3config. To deploy the configuration settings throughout a server farm, copy the entire directory and its contents to each MetaFrame server in the server farm.

---

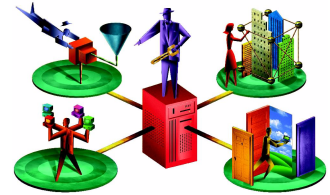
**Tip** If you plan to copy SpeedScreen configuration settings across a server farm, apply the settings to “all instances of an app” on the server when you configure individual application settings, because, path names might differ on various destination servers.

Be aware that applications developed using MFC generate application window names dynamically. This is not standard behavior. The SpeedScreen Latency Reduction Manager uses window names to identify exception entries, and could apply saved settings erroneously on a destination server if you applied SpeedScreen settings to a specific instance of the application.

---



# Licensing MetaFrame XP



This chapter describes Citrix licensing for MetaFrame XP and related products. It includes an overview of licensing requirements and describes various types of licenses.

This chapter includes the following topics:

- Overview of Citrix Licensing, page 119
- Types of MetaFrame XP Licenses, page 122
- Understanding Citrix Licensing Codes, page 124
- Managing and Monitoring Licenses, page 129
- Managing License Counts, page 134

To find step-by-step instructions for procedures mentioned in this chapter—including how to enter, activate, and assign licenses—use online help in Citrix Management Console.

For information on **Clicense**, a Citrix command-line utility that you use to view and change licensing data on Citrix servers, see Appendix A, “MetaFrame XP Command Reference.”

## Overview of Citrix Licensing

Using Citrix software requires that you follow the terms of Citrix license agreements. Usually, an organization must purchase a license that permits the software to be used on a specified number of servers and permits a specified number of ICA connections to the Citrix servers.

In addition to the legal agreement, the term *license* refers to codes and software that enable Citrix products to operate. Software mechanisms verify the presence of valid licenses for Citrix products in Citrix server farms. However, except for special enterprise licenses that require usage reporting, Citrix does not monitor or retrieve license usage data from Citrix server farms.

For details on licensing requirements and licensing terms for your Citrix product, be sure to refer to the End-User License Agreement that is provided with the software package in printed or electronic form.

---

**Important** If your organization participates in a Citrix enterprise licensing program or ASP licensing program, Citrix provides additional software and documentation for license metering and reporting. If your organization participates in an enterprise program, do not follow the licensing instructions in this chapter; instead, refer to your enterprise license documentation or ask your enterprise sales representative for the detailed enterprise licensing information.

---

## Summary of the Licensing Process

The steps below summarize the general process you use for MetaFrame XP licensing. Whether your server farm is small or large, the general steps you use to enter and activate licenses are the same.

For definitions of the licensing terms used in the following procedure, see “Understanding Citrix Licensing Codes” on page 124.

### ► To enter licenses for Citrix products

1. Get the product code and license serial number from your MetaFrame XP product packaging.
  - Make product codes and serial numbers available to administrators who install MetaFrame XP if you want to enter licenses during installation.
  - Make product codes and serial numbers available to administrators who manage licensing for the server farm.
  - Store the original product codes and serial numbers in a safe place.
2. When you install MetaFrame XP on a server, you assign a product code to the server.
  - If you enter a license serial number, the Setup program suggests a product code to assign to the server. Verify that the product code matches the product code in your product packaging. If you did not receive a product code in your product packaging, accept the suggested product code.
  - If you do not enter a serial number, enter the product code for your MetaFrame XP license included in the product package.
3. If you did not enter all your serial numbers during MetaFrame XP installation, use Citrix Management Console to enter the serial numbers for all your Citrix licenses. For each serial number you enter, a license description and license number appear on the **License Numbers** tab in the console.

4. When you enter a license in Citrix Management Console, the console asks if you want to activate the license. In a Web browser, go to the Citrix Activation System (CAS) Web page at <http://www.citrix.com/activate>. Paste the license number into the text box and then copy the activation code you receive for the license.
5. Enter the activation code in the **Activate License** dialog box and click OK to activate the license. Check the **License Numbers** tab to be sure you activate all licenses.
6. After you enter and activate licenses, MetaFrame XP pools all license counts in the server farm. Through IMA, license counts are allocated from the pool to MetaFrame XP servers in the server farm that require product and connection license counts. You can use Citrix Management Console to monitor license usage by the entire farm and by individual servers.
7. If you want to assign activated licenses to specific servers, use the New Assignment wizard to assign product and connection license counts to any MetaFrame XP server in the farm. License counts that you assign are taken out of the pool of unassigned licenses. You cannot assign licenses that are not activated. For more information on product and connection licenses, see “Product Licenses” on page 122 and “Connection Licenses” on page 123.

---

**Important** Citrix Management Console does not verify that license counts you assign to a server are the correct type specified by the server’s product code. If you assign a license count from a MetaFrame XP’s license, for example, and the server’s product code specifies MetaFrame XPe licensing, the server cannot use the assigned license count. The unused count is not returned to the license pool and therefore is not available for use in the server farm.

---

## Grace Periods for License Activation

After you enter a license serial number, you can use the software during a grace period before you must activate the license.

For MetaFrame XP licenses, refer to the Grace Days column on the **License Numbers** tab in Citrix Management Console. The numbers in this column tell you the number of days that remain in the grace period for each license. Before a grace period ends, you must activate the license.

Citrix recommends that you use the grace period to thoroughly test your hardware and software configuration. After you are sure your system is set up properly, you can permanently activate your licenses.

Demonstration licenses and evaluation licenses must be activated using the same procedure described above. However, these licenses are valid for a limited period even after activation.

## Types of MetaFrame XP Licenses

Two types of licenses appear in MetaFrame XP licensing: product licenses and connection licenses. When you manage licenses for MetaFrame XP, you work with both types of licenses. In some procedures, you need to specify one type of license.

A Citrix license can provide either a product or a connection license alone, or both types of licenses together. A serial number that provides product and connection licenses together can include no more than one license count for the product license. If you add more servers to a server farm, you can obtain a product license with the license count you need for the additional servers. For more information about license counts, see “Managing License Counts” on page 134.

### Product Licenses

A *product license* is a license to use one or more Citrix products on your servers. A server farm must have a product license with one license count to run Citrix server software on each server in the server farm.

The table below describes the product licenses that are available to enable MetaFrame XP and related Citrix products.

| Product license | Products enabled                                                                    |
|-----------------|-------------------------------------------------------------------------------------|
| MetaFrame XPs   | MetaFrame XP                                                                        |
| MetaFrame XPa   | MetaFrame XP with Load Manager                                                      |
| MetaFrame XPe   | MetaFrame XP, Load Manager, Resource Manager, Installation Manager, Network Manager |

As mentioned above, a Citrix serial number can include both product and connection licenses. For more information, see “Connection Licenses” on page 123.

When you add a Citrix license to your server farm, the product license provided by the license number appears on the **Product** tab in Citrix Management Console. Only one product license appears on the tab, even if the product license—such as a MetaFrame XPa product license—enables more than one Citrix product.

MetaFrame XP allocates product licenses from a pool of available licenses for a MetaFrame XP server farm. To monitor the product licenses in a farm, select **Licenses** in the tree pane and use the **Product** tab in Citrix Management Console.

A server does not consume a product license when it is not in operation—when the server is down or the IMA service is not running. When a server releases a product license, the license returns to the license pool and is available for use by another server.

With a MetaFrame XPa or MetaFrame XPe product license, which enables multiple products on your servers, you cannot divide the product license to enable one product on one server and other products on other servers.

## Connection Licenses

A *connection license* is a license for ICA Client connections to MetaFrame XP servers. A server farm must have a connection license with one license count for each concurrent ICA connection to the MetaFrame XP servers in the farm.

Each MetaFrame XP product license provides one grace license for the administrator to connect to the server console. The grace license prevents the server from reporting a licensing error if you install no connection licenses and log onto the server before putting it into service for ICA Clients.

License serial numbers that you receive with MetaFrame XP can provide connection licenses alone or in combination with a MetaFrame XP product license. If you add more users, you can get additional connection licenses with the license count you require.

## Migrating Licenses from Other Citrix Products

MetaFrame XP does not directly support licenses for MetaFrame 1.8, *WINFRAME* 1.8, and earlier versions of MetaFrame or *WINFRAME*. However, you can use licenses from other Citrix products if you purchase the appropriate product migration licenses.

You can enter MetaFrame and *WINFRAME* product licenses in your server farm's data store either automatically with the MetaFrame XP setup program or manually using Citrix Management Console.

If you install MetaFrame XP on an existing Citrix server, the Setup program migrates existing Citrix licenses into the new MetaFrame XP server farm.

---

**Important** If you cannot preserve your original licenses on a Citrix server because you cannot upgrade the operating system or you perform a clean install of the operating system or MetaFrame XP, you must enter the original license serial numbers in Citrix Management Console and then reactivate the licenses before they can be used with a migration license.

---

MetaFrame XP supports migration of licenses from the following products:

- MetaFrame 1.8 for Windows NT 4.0 Servers
- MetaFrame 1.8 for Windows 2000 servers
- MetaFrame 1.0
- *WINFRAME* 1.8
- *WINFRAME* 1.7

You can migrate earlier product licenses to MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe product licenses.

---

**Important** If you enter migration licenses in your server farm, you might need to change the product code. A server will not use a migration license if the server's product code is different from the product code of the migration license. For more information, see "Product Codes" on page 125.

---

When a server starts, it requests a product license from the server farm's license pool. If the server's product code allows it to take a migration license, it can use a migration license from the license pool if it can also get a corresponding original license for the migrated product.

For more information about products codes, see "Product Codes," below.

## Upgrading Licenses

You can upgrade your Citrix servers to enable more features by installing additional software and entering MetaFrame upgrade licenses into the server farm's license pool. For example, you can upgrade MetaFrame XPs to MetaFrame XPa or MetaFrame XPe by installing the Citrix software included with the upgrade licenses and entering the licenses into the server farm.

If you upgrade a server, you must change the server's product code to match the product code of the upgrade license. For example, if you upgrade a server from MetaFrame XPs to MetaFrame XPa, you must change the server's product code to the one included with the MetaFrame XPs-to-MetaFrame XPa upgrade license.

## Understanding Citrix Licensing Codes

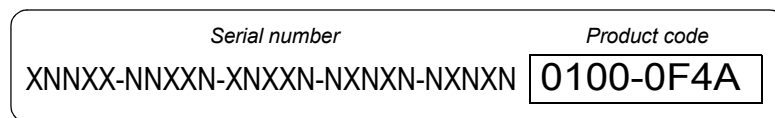
Licensing for MetaFrame XP and related Citrix products involves several *licensing codes*, which are strings of characters that you use during the licensing process. You get some licensing codes from your Citrix software package; Citrix software generates other strings that you use in connection with Citrix licensing.

## Product Codes

Each Citrix software package includes a *product code*. The product code is an alphanumeric string of nine characters that:

- Identifies the Citrix software product
- Distinguishes among retail, evaluation, and not-for-resale product versions
- Specifies the product license a server requests from the license pool to enable the installed Citrix software

The product code for MetaFrame XP appears on a label on the product package. The serial number for the product is also on the label.



## Allocating License Counts According to Product Codes

With MetaFrame XP, license counts are allocated to individual servers from a common license pool for the server farm. The automatic allocation of licenses means you do not have to manually assign licenses to servers.

A variety of MetaFrame XP licenses, including evaluation, migration, upgrade, and full retail licenses can exist in the license pool. The product code applied to a server specifies the kind of product license count the server takes from the license pool.

For example, you might have evaluation and full retail licenses in your server farm's license pool. You install evaluation applications on some servers and install production applications on other servers. In this scenario, you do not want evaluation servers to take retail licenses away from production servers. Therefore, you enter product codes to specify which servers require retail license counts and which servers can use evaluation license counts.

In addition to evaluation and retail licenses, product codes distinguish among MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe licenses. Without the correct product code on a server (and corresponding license counts available in the pool), the Citrix software will not function on a server.

For example, if you specify a MetaFrame XPs product code and no MetaFrame XPs license counts are available, the server will not take a MetaFrame XPa or MetaFrame XPe license count if these licenses are in the license pool.

If you install MetaFrame XP and Installation Manager on a server and enter the MetaFrame XPs license code, for example, the server will request a MetaFrame XPs license count from the license pool. Even if the license count is available, Installation Manager will not be enabled on the server because a MetaFrame XPs license enables only MetaFrame XP to run on the server.

## Entering a Server's Product Code During Setup

As the last step in MetaFrame installation, the Setup program asks if you want to enter Citrix licenses. You can skip this step if you have already entered your license serial number on the first server you set up or you want to enter licenses later using Citrix Management Console.

If you do enter a license, the Setup program displays the product code that corresponds with the license serial number. Verify that the recommended product code matches the product code included with your MetaFrame XP product package.

If you do not enter a license during installation, type the full product code (including the dash between the groups of alphanumeric characters) from your product package in the **Product Code** box when you are prompted to do so by the Setup program.

---

**Important** Because the product code specifies the product license for the server to use, be sure to enter the correct product code on each server. If the server cannot get a product license count for the installed software from the license pool, the Citrix software will not function.

---

## Changing a Server's Product Code

You can change a product code to change a server's product license specification. Adding a license to the server farm's license pool does not change the product code on any servers.

For example, you might want to change the product code to convert an evaluation server to use a full license. Another example is to change the product code when you upgrade a server that uses a MetaFrame XPs license to use a MetaFrame XPa license and enable Load Manager features.

### ► To change a server's product code

1. Select the server in Citrix Management Console.
2. Choose **Servers > Set MetaFrame Product Code** from the **Actions** menu.
3. Enter the product code and click **OK**.

---

**Tip** To select multiple servers so you can change their product codes at once, select the Servers node in the Citrix Management Console and then select the servers on the Contents tab.

---

When you change the product code, a status bar indicates the progress of the change. The process can last several minutes if you change the product code on many servers at once. The status bar indicates when the product code change is complete on all the selected servers.

## Serial Numbers

A *serial number* is the code that you enter in the first step of the licensing process, either in the MetaFrame XP Setup program or in Citrix Management Console.

The serial number represents the exact licenses you purchased. Citrix software uses the serial number to identify and validate your licenses.

The serial number is on a label in the MetaFrame XP software package. A MetaFrame XP serial number is a string of 25 letters, numbers, and symbols. The string has five groups of five characters each, with a hyphen between each group.

*serial number*

XNNXX-NNXXN-XNXXN-NXNXN-NXNXN 0100-04FA

---

**Tip** The licensing label in your product package might include more than one serial number, depending on the particular MetaFrame XP licenses that you purchase.

---

## Representation of Licenses by Serial Numbers

Serial numbers for MetaFrame XP can represent the following types of Citrix licenses:

**Product license.** MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe product licenses enable use of the MetaFrame XP and Citrix management products on servers. Each license enables particular Citrix products and features on servers (see the table on page 122 for more information).

The number of servers that a product license allows depends on the license count.

**Connection license.** This license enables concurrent connections by ICA Client users to MetaFrame XP servers. The number of concurrent connections allowed by the license depends on the license count.

### Types of Licenses Provided by a Serial Number

A Citrix license serial number can represent a single Citrix license or a combination of Citrix licenses. However, some license combinations cannot be represented by a single serial number. A single serial number can represent only the following:

- A product license (MetaFrame XPs, MetaFrame XPa, or MetaFrame XPe) that includes multiple license counts for multiple servers
- A connection license, which includes multiple license counts for concurrent ICA connections
- A product license with one license count plus a connection license with multiple license counts

For example, one serial number can represent a MetaFrame XPs product license with a single license count and a MetaFrame connection license with a 15-connection license count. Another serial number can represent a MetaFrame XPe product license with a 500-server license count.

To enable MetaFrame XP and Citrix management products for the number of servers and connections that you use in a server farm, you need to obtain a product license with a license count equal to (or greater than) the number of servers you have, and a MetaFrame connection license with a license count equal to (or greater than) the number of concurrent ICA connections your users require.

### Entering Serial Numbers

To add licenses to your server farm, you enter license serial numbers during installation of MetaFrame XP or with Citrix Management Console.

After you enter serial numbers, Citrix Management Console produces a license number from each serial number. You use the license number to receive an activation code from Citrix for the licenses.

All types of Citrix licenses require activation within a set period of time, which is called the *grace period* and typically lasts 90 days. Licenses that you do not activate during the grace period expire and are invalid. Evaluation licenses require activation but are valid for a limited period, typically 90 days, after activation.

### License Numbers

A *license number* is a code that you use in the licensing process for MetaFrame XP and Citrix management products. License numbers are strings of letters, numbers, and symbols.

For licensing of MetaFrame XP and other IMA-based Citrix products, you use a license number that is derived from each serial number you enter in a server farm. The Citrix Management Console displays each license number, which consists of the original serial number plus additional characters; these additional characters are referred to as the *machine code*.

You use license numbers to get activation codes, as described below, for each Citrix license.

## License Activation Codes

All types of Citrix licenses require activation. To activate a license, you enter the *activation code* for the license in Citrix Management Console. The activation code is a string of characters that you get from the Citrix Activation System (CAS) Web page. You can use the CAS system with any Web browser and Internet connection. For more information, see “Activating Licenses” on page 131.

Each activation code is a unique string that activates only one specific license number.

## Managing and Monitoring Licenses

In a MetaFrame XP server farm, the data store for the farm contains all data associated with licensing for the farm, including the types of licenses you enter, their license numbers, license counts, and license assignments to specific servers.

You use Citrix Management Console to monitor and manage licensing for MetaFrame XP servers and connections by ICA Client users. With the console, you can do the following:

- Add licenses to a server farm
- Activate licenses
- Monitor usage of product and connection license counts
- Assign license counts to specific servers
- Remove licenses from a server farm
- Copy license numbers for use in the CAS system

For information on the basics of using Citrix Management Console, see “To use Citrix Management Console” on page 101.

The Citrix Management Console communicates with the data store in a server farm to display information about licenses in the farm. When you make changes by adding or removing licenses, or changing license assignments, the console updates the licensing data in the farm’s data store through Citrix IMA.

**Important** When you view information about license usage, use the **Refresh** command to be sure the information is current. When ICA Clients connect or disconnect from the farm, the licensing data is not updated automatically. Using the **Refresh** command ensures that connection license data is current.

Similarly, MetaFrame XP does not refresh the data in the console when servers are brought online or go offline. Use the **Refresh** command to be sure that license usage data is current when you view product license information in Citrix Management Console.

---

► **To set automatic refresh of licensing data**

You can specify an interval for automatic refresh of licensing data displayed in Citrix Management Console. If you do not select the automatic refresh setting, licensing data is not refreshed unless you choose the **Refresh** command or a license change event, such as adding or removing a license from the server farm, occurs.

1. Select the License node in the console tree.
2. Choose **Auto Refresh Settings** from the **Actions** menu or the right-click menu.
3. In the dialog box, **Automatically refresh licensing data**, enter the refresh interval in seconds, and click OK.

## **Adding Licenses to Server Farms**

To add a license to a Citrix server farm, you enter a license serial number that you receive with a Citrix product.

Use Citrix Management Console to enter each serial number for licenses that you want to use in the farm. Choose **New > License** from the **Actions** menu or click the **Add License** button on the toolbar to begin entering a license.

Type Citrix serial numbers exactly as they are printed, including hyphens (dashes) between the groups of characters. The characters in a serial number can include numerals, letters, and symbols such as + (plus sign), ? (question mark), and \* (star).

After you enter a serial number, the license appears on the **License Numbers** tab. The license number that is shown on the tab is the serial number that you entered, followed by 12 additional characters that the licensing subsystem generates.

When you first enter a license, the license is not activated. The Status column on the **License Numbers** tab displays *Unactivated* and the Grace Days column shows the number of days remaining before the license will expire if you do not activate it.

When you enter an unactivated license, the console asks if you want to activate the license.

## Activating Licenses

You must activate each Citrix license to complete the licensing process for MetaFrame XP software and ensure continued operation. While a license is not activated, reminder messages appear on the MetaFrame XP server console.

If you do not activate a license, the license expires after a set grace period. When a license expires, the license is no longer valid. An invalid license prevents users from connecting to the MetaFrame XP server. In addition, you cannot assign unactivated licenses to servers.

To activate a license, you obtain an activation code and then enter the code in Citrix Management Console.

---

**Tip** You can right-click a license number on the **License Numbers** tab and choose **Activate** to start the activation process.

---

### ► To get an activation code for a license

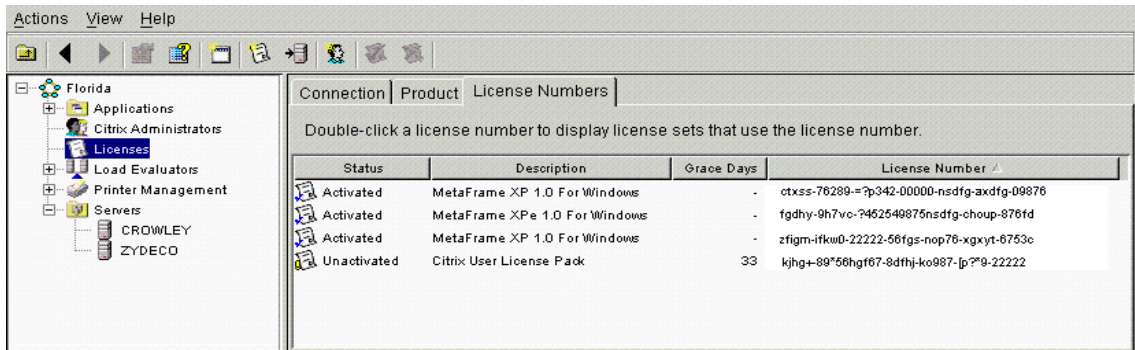
1. Select a license number on the **License Numbers** tab in Citrix Management Console and choose **Activate** from the Actions menu, the right-click menu or the toolbar.
2. In the **Activate License** dialog box, click **Copy to Clipboard** to copy the license number to the Clipboard for the next step.
3. On the CAS Web page (<http://www.citrix.com/activate>), enter the license number. The CAS page returns the activation code for the license number.
4. Copy the activation code, and enter the activation code in the **Activate License** dialog box and click OK to activate the license.

After you activate a license, the Status column displays *Activated* on the **License Numbers** tab. The license number remains the same because activation codes do not appear as part of the license number.

## License Views

To monitor and make changes to licensing in your server farm, you primarily use the Licenses node in Citrix Management Console.

When you select the Licenses node in the console's left pane, you can use the **Product**, **Connection**, and **License Numbers** tabs that appear in the right pane to monitor license usage and configuration.



## Displaying License Numbers

The **License Numbers** tab lists each license that you enter in the server farm. Each license that appears on the tab is based on a single license number, which you can view in the License Number column. The tab also shows which licenses are activated and unactivated, and the grace period for unactivated licenses.

This tab can display multiple licenses with the same description; the **License Numbers** tab does not consolidate licenses based on product or license type.

For example, if you enter three serial numbers that represent licenses for MetaFrame XP 1.0 for Windows, each license appears in the list on the **License Numbers** tab. Two licenses might contribute both product and connection licenses, while the third might add license counts for additional servers in the farm.

To see what licenses a license number contributes to the server farm, double-click the license in the list.

Use the **Copy to Clipboard** command to copy the license number of any license you select in the list. You can paste the data from the Clipboard into other applications for reporting and archiving.

## Monitoring Connection Licenses

The **Connection** tab lists MetaFrame XP connection licenses. The tab shows the license count, which is the number of concurrent ICA connections allowed by the license, and usage data for each connection license you enter.

More than one serial number can contribute to one type of connection license. Each type of connection license—such as MetaFrame Connection—appears only once on the tab.

For example, “MetaFrame Connection” appears once on the **Connection** tab, even if you enter multiple serial numbers that include connection licenses. Additional licenses increase the license count, which appears in the Count column.

*Connection license*

| Connection   Product   License Numbers                                            |                      |       |               |                  |          |          |
|-----------------------------------------------------------------------------------|----------------------|-------|---------------|------------------|----------|----------|
| Double-click a license for server assignment and usage information                |                      |       |               |                  |          |          |
| Status ▾                                                                          | Description          | Count | Pooled In Use | Pooled Available | Assigned | Assigned |
|  | MetaFrame Connection | 20    | 0             | 20               | 0        |          |

Use the **Properties** command (or double-click a license in the list) to display additional details about a connection license. You can monitor the use of the connection license by servers in the farm. You can also see the license number that includes the connection license, check the status of the license, and see how many grace days remain before you must activate a license that is not activated.

## Monitoring Product Licenses

The **Product** tab lists MetaFrame XP product licenses. The tab shows the license description, the license count (the number of servers allowed by the license), and usage data for each product license you enter.

If you enter multiple license serial numbers, each distinct Citrix product appears once on the **Product** tab. Additional licenses can increase the license count for a product without adding additional product licenses to the list.

*Product license*

| Connection   Product   License Numbers                                            |                                      |       |                 |                  |          |          |
|-----------------------------------------------------------------------------------|--------------------------------------|-------|-----------------|------------------|----------|----------|
| Double-click a license set for server assignment and usage information.           |                                      |       |                 |                  |          |          |
| Status                                                                            | Description                          | Count | Pooled In Use ▾ | Pooled Available | Assigned | Assigned |
|  | MetaFrame XP 1.0 English For Windows | 7     | 1               | 6                | 0        |          |

For example, “MetaFrame XP 1.0 English for Windows” is one distinct product license. If you enter more than one serial number for this license, the product description appears once. The Count column shows the total license count for the product license.

Use the **Properties** command or double-click a license description in the list to display additional details about a product license. In the **Properties** dialog box, you can monitor the use of the product license by servers in the farm. You can also see the license number that included the product license, check the status of the license, and see how many grace days remain before you must activate a license that is not activated.

## Monitoring Server Information

You can select individual servers in the console tree to view licensing information for each server.

When you select one server in the tree, the **Licenses** tab appears in the console's right pane. This tab shows any license counts that are in use by the server, as well as any license counts assigned to the server.

License counts that you assign to a server are removed from the license pool; an assigned license is available only to the server on which it is assigned. An assigned license is not available to other servers, even if the license is not in use because the server is down. For more information, see "Assigning License Counts" on page 135.

---

**Important** In a mixed server farm environment, Citrix Management Console monitors and manages licensing data for MetaFrame XP servers only. To change license data on MetaFrame 1.8 servers, use the licensing commands and utilities that shipped with that product; these utilities are also included on the MetaFrame XP CD-ROM for your convenience. The MetaFrame 1.8 licensing commands do not report or configure licensing data for MetaFrame XP or other IMA-based servers.

---

---

**Note** Licenses that are migrated into the server farm from older Citrix Products, such as Load Balancing Services and SecureICA Services, will appear in Citrix Management Console, even though the licenses are not used in the MetaFrame XP server farm.

---

## Managing License Counts

Product licenses and connection licenses each include a *license count*. The license count is the number of products or connections that the license authorizes.

For example, a MetaFrame XPa product license with a license count of 10 is a license to use MetaFrame XP and Citrix Load Manager on 10 servers. A connection license with a license count of 50 allows 50 concurrent ICA connections to the server farm.

License counts appear in the Count column on the **Product** and **Connection** tabs in Citrix Management Console. These tabs display similar licenses as single items in the list. These single items are called *license sets*. A license set includes the total license count from all licenses in the set.

For example, if you have two MetaFrame XPs licenses, one with a license count of 25 and one with a license count of 10. When you enter these licenses in your server farm, just one license set with a license count of 35 appears on the **Product** tab.

Citrix Management Console uses license count data wherever it displays license usage information. The numbers that are labeled “pooled” and “in use” refer to license counts that are pooled and in use.

## Pooling License Counts

To simplify management of licenses, MetaFrame XP always combines the license counts for each product license into a common pool for the server farm. It does the same with the license counts for connection licenses.

By default, all MetaFrame XP servers in the farm can take license counts from the license pools as needed for new connections and new servers.

For example, as more users connect to a MetaFrame XP server, the server takes connection license counts from the license pool. If you restart a farm server that was offline, the server takes a product license count from the license pool when it begins operating in the farm.

---

**Important** The product license count that a server takes from the license pool depends on the product code assigned to a server. A server does not take product license counts from licenses other than the license specified by its product code. For example, if a server’s product code specifies MetaFrame XPe, the server does not take a MetaFrame XPs or MetaFrame XPa license count from the license pool.

---

## Assigning License Counts

The only license counts that are not available to all servers are license counts that you explicitly assign to specific servers.

If you assign license counts to a server, you remove the specified count from the pool and dedicate the count to one server only. You can do this with most licenses, but you cannot assign some types of licenses, including unactivated, demonstration, and evaluation licenses.

You can assign licenses to servers based on the type of applications published in the farm and the number of servers that host mission-critical applications.

For example, if you assign connection license counts to certain servers and you set up certain ICA Clients to connect to those servers, you can be sure of the number of users who can connect to that group of servers. While the license pool for the server farm might run out of connection license counts at some times, the servers to which you assigned license counts will always have the number that you specified.

You use the New Assignment wizard in Citrix Management Console to assign product and connection license counts. Select a license set on the **Connection** or **Product** tab, and choose **License > New Assignment** from the **Actions** menu to begin the process.

The wizard guides you to select a specific server in the farm and then to specify the license count to assign to that server. Repeat the process if you want to assign more license counts to other servers in the farm.

## Changing License Assignments

To change a server's license count assignment, you select the server in Citrix Management Console and select the license set on the **Licenses** tab. Use the **Change Assignment** command to adjust the license count.

If you reduce the license count that is assigned to a server, you return the count to the license pool for use by all servers in the farm.

You can remove the assigned license counts from a server by selecting the license set and choosing the **Drop Assignment** command.

## Removing Licenses

Normally, you do not remove licenses from a server farm. However, you might want to remove a license if it has expired, or if you want to replace an evaluation license with a full product license.

To remove a license, select it on the **License Numbers** tab in Citrix Management Console and choose **License > Remove** from the **Actions** menu.

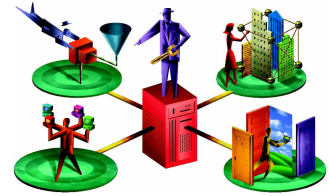
## Client Device Licensing

*Client device licensing* is a feature that allows users to start multiple sessions on the same or different servers while using only a single Citrix license count. The user must make all connections from a single client device.

When a user starts a second session on the same Citrix server, the new session does not consume a second connection license count. If the user starts a second session on a different server, the new session does not consume a second connection license count if the first session used a pooled license count.

Also, ICA Clients (Win16 or Win32) that shipped with MetaFrame 1.0 or earlier require that all sessions use the same network protocol (TCP/IP, IPX, or NetBIOS).

# Configuring ICA Client Connections



MetaFrame XP lets your users run server-based applications by enabling connections from varied computer platforms through ICA Client software. Managing the connections to your server farm involves management of network access and ICA connections to the farm.

You manage user access through standard Windows permissions and account configuration tools. MetaFrame XP provides the tools you use to configure ICA connections.

This chapter includes the following topics:

- Configuring ICA Connections and Sessions, page 137
- Configuring Session Settings for ICA Clients, page 142
- Configuring ICA Session Shadowing, page 150
- Configuring ICA Audio Settings, page 152
- Configuring Client Device Mapping, page 153

## Configuring ICA Connections and Sessions

Users are able to access applications on a MetaFrame XP server through ICA connections and ICA sessions.

*ICA connections* are logical input/output ports that are set up on a MetaFrame XP server. When an ICA Client links to a MetaFrame XP server through an ICA connection, it establishes an ICA session. The *ICA session* is an active link that runs on the MetaFrame XP server until the user logs off and ends the session.

This section explains how ICA connections and ICA sessions work together. It includes information on using Citrix Connection Configuration to configure ICA connections. Later sections in this chapter tell you how to set properties for ICA sessions.

---

**Note** In addition to ICA connections, Citrix Connection Configuration supports connections using Microsoft's RDP protocol for terminal services. ICA Client settings and other options, such as asynchronous connection options, are not available for RDP connections.

---

## Setting up ICA Connections

At least one ICA connection is required on a MetaFrame XP server for ICA Clients to use for establishing ICA sessions. Once an ICA connection is set up, it exists even if no ICA Clients are linked to the server with active ICA sessions. In contrast, an ICA session exists on a MetaFrame XP server only while an ICA Client is linked to the server and using resources. When an ICA Client user logs off the MetaFrame XP server, the ICA session ends.

Multiple ICA Clients can establish ICA sessions through the same ICA connection on a MetaFrame XP server. MetaFrame XP associates a user ID and ICA connection with each ICA session.

You can set up one ICA connection on a MetaFrame XP server for each network transport protocol and adapter that ICA Clients will use to link to the server.

MetaFrame XP supports the following ICA connection configurations:

**Network transport.** TCP/IP, IPX, SPX, NetBIOS, asynchronous (modem or direct cable connection)

**Network adapter.** Network interface cards (NIC), serial ports, modems

If your network uses TCP/IP and your MetaFrame XP server contains a NIC, the ICA Clients can launch sessions using an ICA connection configured for TCP and the NIC. To give dial-up access to remote users, you can also set up an ICA connection configured for a modem connected to a serial communication port on the MetaFrame XP server.

You do not need to set up all (or any) ICA connections yourself. During installation of MetaFrame XP, an ICA connection is automatically set up for each network transport that is configured on the server and for each configured modem on the server (unless you deselect one or more of these options during setup).

## Using Citrix Connection Configuration

Citrix Connection Configuration is an enhanced version of the Windows utilities Terminal Server Connection Configuration (NT 4.0, Terminal Server Edition) and Terminal Server Configuration (Windows 2000 Servers).

The Citrix Connection Configuration utility adds support for more connections and advanced configurations.

Use Citrix Connection Configuration to:

- Add network, asynchronous, and other types of connections
- Configure existing connections
- Set parameters for mapping client devices
- Set modem parameters
- Test modem configuration

You can use Citrix Connection Configuration to add ICA connections for transport protocols, network adapters, and asynchronous connections that were not created during MetaFrame XP installation.

► **To start Citrix Connection Configuration**

From the **Start** menu, choose **Programs > Citrix > MetaFrame XP > Citrix Connection Configuration**.

From the **Citrix Connection Configuration** window, you can view the existing ICA connections. You can use the **Connections** menu to add, edit, or delete ICA connections.

For more information on procedures for adding and modifying connections, choose **Contents** from the **Help** menu in Citrix Connection Configuration.

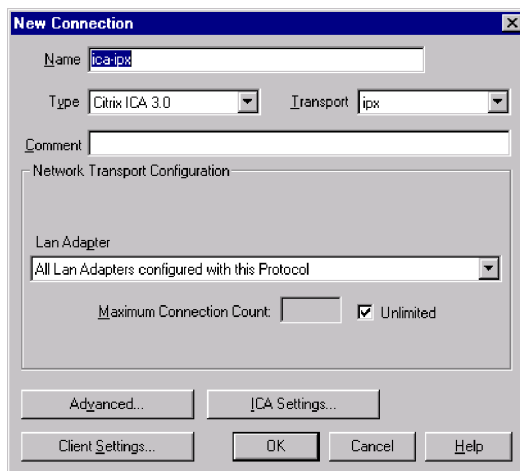
## **Adding ICA Connections**

If you install additional network protocols or modems, you can create ICA connections for ICA Clients to use to access the MetaFrame XP server.

► **To add a network ICA connection**

Use the following procedure to add an ICA connection for a network adapter. You might need to do this if, for example, you install an additional protocol such as IPX.

1. Run Citrix Connection Configuration (see “To start Citrix Connection Configuration” on page 139).
2. From the **Connection** menu, choose **New**. The **New Connection** dialog box appears:



3. Type a name for the connection in the **Name** box. You can enter an optional description in the **Comment** box.
4. From the **Type** list, select **Citrix ICA 3.0**.
5. From the **Transport** list, select the transport protocol.
6. Click **OK** to add the ICA connection. If a connection with these settings exists, a message tells you that a connection can't be created with the same settings.

## Adding Asynchronous ICA Connections

You can set up asynchronous ICA connections for access to MetaFrame XP servers. Asynchronous ICA connections can be dial-up connections through modems and direct cable (null modem) connections between the serial ports of a client device and MetaFrame XP server.

When you set up an asynchronous ICA connection in Citrix Connection Configuration, you avoid the overhead of Dial-Up Networking and TCP/IP on the server. MetaFrame XP supports modem configuration through the Windows Telephony Application Programming Interface (TAPI).

For the best performance over asynchronous connections, Citrix recommends using high-speed serial port hardware and processor-controlled multi-port adapters. Using hardware devices that place less demand on CPU resources allows more processor power to be devoted to running user sessions.

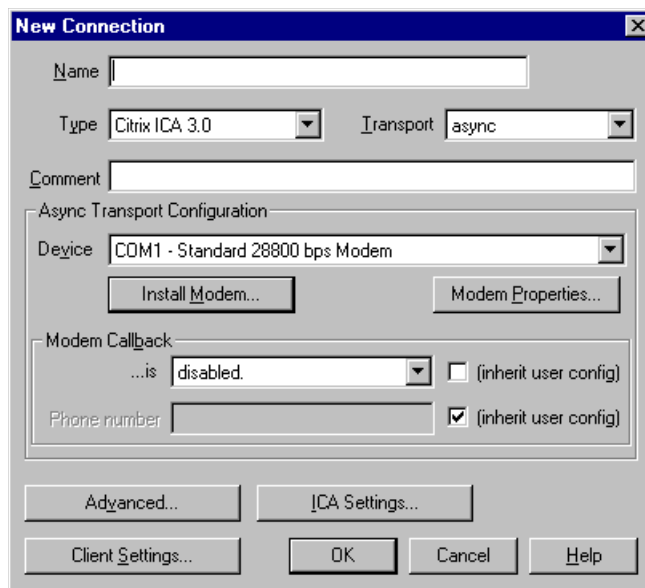
---

**Important** In a MetaFrame XP server, a modem or serial port cannot be configured as both a Dial-Up Networking port and an ICA asynchronous connection port. Also, you cannot configure an asynchronous direct cable connection using the **Serial Cable between 2 PCs** option in Windows Dial-Up Networking. Instead, you must configure the ICA asynchronous connection in Citrix Connection Configuration.

---

► **To add an asynchronous ICA connection**

1. Run the Citrix Connection Configuration utility (see “To start Citrix Connection Configuration” on page 139).
2. From the **Connection** menu, choose **New**. The **New Connection** dialog box appears.
3. Type a name for the new connection.
4. From the **Type** list, select **Citrix ICA 3.0**.
5. From the **Transport** list, select **async**. Options for asynchronous connections appear in the dialog box.
6. From the **Device** list, select the COM port for the connection. Standard COM ports appear in the list. If a TAPI modem is installed on a COM port, the modem type follows the COM port name in the list. If a modem is installed on a particular COM port, you cannot select that COM port for a direct cable (null modem).
  - To install a modem, click **Install Modem**. Then, follow the instructions in the Install New Modem wizard to install and configure the modem.
  - To configure an existing modem, click **Modem Properties**.
7. Click **OK** to add the connection. If a connection with these settings exists, a message tells you that a connection can't be created with the same settings.



## Configuring Session Settings for ICA Clients

Three types of settings control the behavior of an ICA session:

**Per-connection settings.** You can use Citrix Connection Configuration to configure settings for each ICA connection. These settings are referred to as *per-connection settings* because they affect all ICA sessions that users establish through the ICA connection.

You can click **Advanced**, **ICA Settings**, and **Client Settings** in the **New Connection** or **Edit Connection** dialog box to configure per-connection settings.

For example, for a particular ICA connection, you can set a timeout value in the **Advanced Connection Settings** dialog box. This timeout setting will affect the sessions of all users who link to the server through that ICA connection.

Procedures for configuring per-connection settings appear later in this chapter.

**Per-user settings.** User and group settings that you configure in Windows will apply to any ICA connection. These settings, which are based on individual user accounts, include user names and group memberships, permissions, and dialin settings for Windows NT or Windows 2000.

For more information on per-user settings, refer to your Windows documentation. See the online help for User Manager for Domains for Windows NT 4.0; for Windows 2000 Servers, see online help for Local Users and Groups, or Active Directory Users and Computers.

**Per-client settings.** You can configure an ICA Client to enable additional security and compression. These settings apply to any ICA session established by that ICA client, independent of the person using the client device or the ICA connection used for the session.

For information on configuring per-client settings, see the *Citrix ICA Client Administrator's Guide* for each client that you deploy.

## Precedence of Settings

A setting that you specify in Citrix Connection Configuration takes precedence over per-user and per-client settings. However, for some ICA connection settings, you can select an option to apply settings from user accounts or ICA Clients to the ICA connection.

- You can specify that an ICA connection use some settings from user accounts by selecting **Inherit User Config**.
- You can specify that an ICA connection use some settings from ICA Clients by selecting **Inherit Client Config**.

If you select one of these check boxes, the associated ICA connection settings are dimmed and cannot be edited. The setting specified by the Windows user account or ICA Client takes precedence over the ICA connection setting.

If you clear the check box for these options, the original ICA connection settings take effect.

## Configuring Connection Methods for Sessions

This section discusses ways to configure options for ICA connections associated with network interfaces, modems, and direct cable (null modem) connections.

You can configure new ICA connections in the **New Connection** dialog box as described earlier in this chapter. To modify the configuration of an existing ICA connection, double-click the connection in the Citrix Connection Configuration window.

For more information on configuration procedures, see the online help in Citrix Connection Configuration.

## Configuring Modem Callback

You can configure a modem ICA connection for modem callback. You can use this feature so that the call charges are incurred at the server end of the connection, or to provide a small measure of security.

To set modem callback options, use Citrix Connection Configuration.

When modem callback is active and a user dials in to the ICA connection on the MetaFrame XP server, the server modem answers, then hangs up, and dials a specified telephone number (the *callback number*) to reach the ICA Client modem and complete the connection.

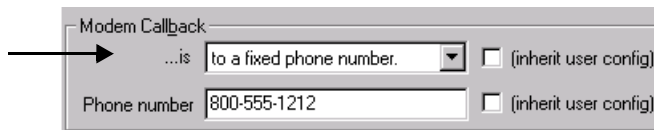
Modem callback to a fixed number can provide a small level of security based on telephone numbers. Using this feature verifies that authorized users are dialing in by calling back to specified numbers to complete dial-in ICA connections.

To configure modem callback for a new ICA connection, use the options in the **New Connection** dialog box when you create a modem ICA connection.

To change the settings for an existing ICA modem connection, double-click the ICA connection in Citrix Connection Configuration. Then, use the **Edit Connection** dialog box to configure modem callback.

### Enabling Modem Callback

You can enable or disable modem callback by using the first drop-down list and the adjacent check box in the Modem Callback area.



- Select the **Inherit User Config** check box to enable modem callback only for users who have modem callback enabled in their Windows user accounts. When this option is selected, the drop-down list is not available.
- From the drop-down list, choose **To a fixed phone number** or **To a roving phone number** to enable modem callback for all users.
- Choose **Disabled** from the drop-down list to disable modem callback for all users.

When you enable modem callback, you can specify one callback phone number for all users. You might do this if all users dial in from one phone number at a branch office, for example. Or, you can use callback numbers from each user's Windows account. Another option is to let users enter callback numbers when they make connections.

In Windows NT 4.0, a callback phone number can be entered in the **Dialin Information** dialog box, which is available from the **User Properties** dialog box for each user account. In Windows 2000, a phone number can be entered in the **Dial-in** tab of the **Properties** dialog box for each user account.

## Specifying a Callback Number

To enable callback to a specified phone number, select **To a fixed phone number** in the first list. Type the telephone number in the **Phone Number** box. The connection will call back the phone number in the **Phone Number** box to establish the connection for all users—unless the **Inherit User Config** option next to the **Phone Number** box is selected. When **Inherit User Config** is selected, the **Phone Number** box is not available.

You can select the **Inherit User Config** option to use the callback configuration from the user's Windows account configuration. If the user's account is set to a specified phone number, that number is used. Or, user accounts can allow callers to enter callback numbers each time they connect.

For example, if users' home phone numbers are specified in their user account configurations, you can choose **To a fixed phone number** and select the **Inherit User Config** option to ensure that users can dial in only from verified locations.

## Using a Roving Phone Number

To enable callback and allow all users to enter the callback number, select **To a roving phone number** in the first drop-down list in the Modem Callback area. This setting prompts users to enter a callback number when they start an ICA session by modem. If a phone number is entered in the **Phone Number** box, this is the default number for callback.

You might want to use callback to a roving number so that remote users who dial in from hotels and other locations do not have to be responsible for phone charges for lengthy connections.

You can select the **Inherit User Config** box next to the **Phone Number** box. When this is selected, the **Phone Number** box is not available. The modem will use the callback configuration from the user's Windows account. If the user's account is set to call back a specified phone number, that number is used for callback. If **Set by Caller** is selected in the user's account, the user can specify a callback number when making a connection.

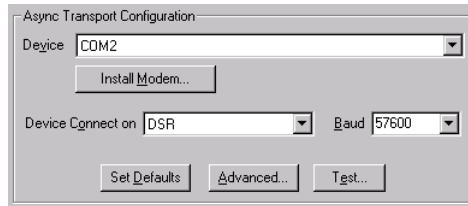
## Configuring Direct Cable Connections

You can use Citrix Connection Configuration to configure ICA connections for direct cable connections between serial (COM) ports on client devices and a MetaFrame XP server.

You can configure new connections in the **New Connection** dialog box when you create an asynchronous ICA connection.

To edit a connection, double-click the asynchronous ICA connection in Citrix Connection Configuration. Use the **Edit Connection** dialog box to configure the ICA connection.

Options for asynchronous cable (null-modem) ICA connections appear in the Async Transport Configuration area in the **New Connection** and **Edit Connection** dialog boxes.



With these options you can configure the following device and transmission properties for the ICA connection:

**Device.** Specifies the serial port (COM port) to use for the connection. The available COM ports on the MetaFrame XP server appear in the drop-down list.

**Device Connect On.** Specifies the signal type (CTS, DSR, RI, DCD, or First Character) for the server to use to determine when a connection is established and ready for user login. You can select **Always Connected** to bypass connection detection.

**Baud.** Sets the communication rate for the connection. You can select standard baud rates from the drop-down list.

**Set Defaults.** Resets the Device Connect On and Baud settings, and the settings in the **Advanced Async Configuration** dialog box, to default values.

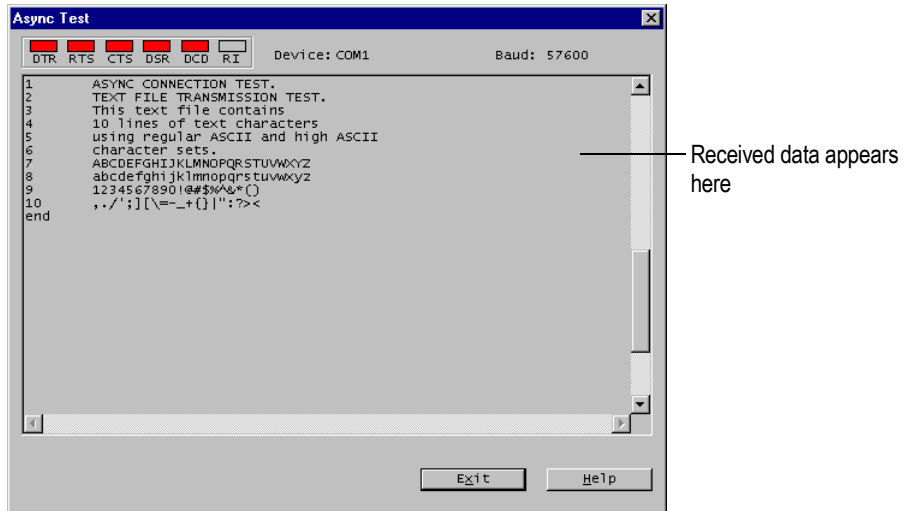
**Advanced.** Opens the **Advanced Async Configuration** dialog box for configuring additional serial port settings. These settings are described in the next section.

### Using the Async Test Dialog Box

You can test an asynchronous direct cable connection by using the **Test** button in the **New Connection** dialog box and the **Edit Connection** dialog box when you configure an async ICA connection.

The **Test** button appears in the Async Transport Configuration area when the Transport setting is Async and the selected Device is a COM port that does not have a modem installed on it.

The **Test** button opens the **Async Test** dialog box for testing communication through the specified serial port. In the dialog box, you can monitor control signals and transmit data to and receive data from a client device connected to the serial port.



The dialog box displays the name of the serial port and baud rate. A row of indicator “lights” shows the status of the DTR, RTS, CTS, DSR, DCD, and RI signals.

You can type text in the scrolling area to send ASCII data to a device that is connected to the specified serial port. The text you type does not appear in the dialog box unless a connected device echoes text that it receives.

If you transmit text from a terminal emulation program (such as HyperTerminal in Windows) that is running on a connected client device, the text appears in the **Async Test** dialog box if the connection is configured correctly.

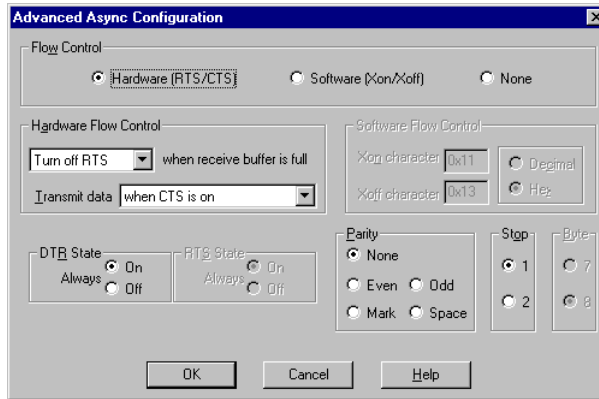
## Configuring Advanced Async Options

When you create or edit an async cable ICA connection, the **Advanced** button in the Async Transport Configuration area opens the **Advanced Async Configuration** dialog box. You can use this dialog box to configure flow control and other data transmission settings.

**Flow Control.** Select Hardware or Software flow control, or select None to configure the async connection with no flow control.

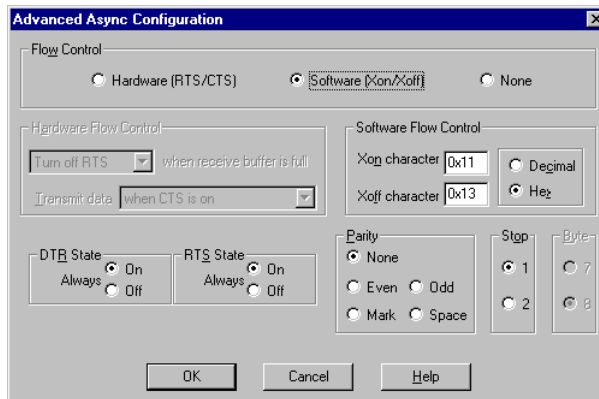
**Hardware Flow Control.** If you select Hardware in the Flow Control area, the options in the Hardware Flow Control area are available to specify signals used for flow control. Hardware flow control is the default configuration.

From the first drop-down menu, select the hardware signal action that indicates the receive buffer is full. From the second menu, select the hardware signal action that indicates data transmission can proceed. The default settings are “Turn off RTS when receive buffer is full” and “Transmit data when CTS is on.”



**Software Flow Control.** If you select Software in the Flow Control area, the options in the Software Flow Control area are available to specify the start and stop characters for data transmission.

Select Decimal or Hex to define character values, and then type decimal or hex values in the text boxes to set the Xon and Xoff characters for software flow control.



**DTR State.** The DTR State options are available with any flow control option unless Turn Off DTR is selected for Hardware Flow Control.

Select On to specify that the Data Terminal Ready (DTR) signal is always on. Select Off to specify that the signal is always off.

**RTS State.** These options are available with any flow control option unless Turn Off RTS is selected to hardware flow control.

Select On to specify that the Request To Send (RTS) signal is always on. Select Off to specify that the signal is always off.

**Parity.** Click an option to specify the parity type or click None to specify no parity setting.

**Stop.** Select 1 or 2 to specify the number of stop bits per character.

**Byte.** This setting for the configuration of transmitted data cannot be changed because ICA protocol requires 8 bits per byte.

## Configuring Advanced ICA Connection Options

The **Advanced Connection Settings** dialog box provides additional control over security and performance on ICA connections. To use the dialog box, click the **Advanced** button when you create or edit an ICA connection.

The Advanced Connection Settings options for Windows connections apply to Citrix ICA connections. For more information about advanced options, see the Citrix Connection Configuration online help.

**Advanced Connection Settings**

**Login**  
☐ Disabled ☒ Enabled

**Timeout settings (in minutes)**  
 Connection: 120 ☐ No Timeout  
☐ (inherit user config)  
 Disconnection: 10 ☐ No Timeout  
☐ (inherit user config)  
 Idle: 30 ☐ No Timeout  
☐ (inherit user config)

**Security**  
 Required encryption: Basic  
☐ Use default NT Authentication

**AutoLogin**  
 User Name: Vmarron  
 Domain: OAKLAND  
 Password:   
 Confirm Password:   
 Prompt for Password: ☐  
☐ (inherit client config)

**Initial Program**  
 Command Line:   
 Working Directory:   
☐ (inherit client/user config)  
☐ Only run Published Applications

**User Profile Overrides**  
☐ Disable Wallpaper

On a broken or timed-out connection, disconnect the session. ☐ (inherit user config)

Reconnect sessions disconnected from any client. ☐ (inherit user config)

Shadowing is enabled: input ON, notify ON. ☐ (inherit user config)

## Restricting Connections to Published Applications

For high-security environments, select the **Only run published applications** check box to restrict the connection to run only published applications defined by the administrator. This option is not available unless you select **Inherit Client/User Config** in the Initial Program area.

**Note** You cannot specify a published application as the initial program.

## Configuring ICA Encryption

In the Security area, you can configure encryption for the ICA connection. Select an option from the **Required Encryption** menu.

The default encryption level is Basic. You can select strong encryption that applies the RC5 encryption algorithm with 128-bit minimum session keys to login only or to all data transmission.

## Configuring ICA Session Shadowing

*Shadowing* an ICA session means viewing the session from another device. During shadowing, you can monitor the session activity as if you were watching the screen of the ICA Client that initiated the session. You can see the active program running in the session, with the user's keyboard input and mouse actions.

This section discusses settings for ICA connections related to shadowing. For information on how to shadow sessions, see "Shadowing ICA Sessions" on page 204.

While you are shadowing a session, if the MetaFrame XP server and ICA connection allow it, you can use your keyboard and mouse to remotely control the user's keyboard and mouse in the shadowed session.

The ability to shadow ICA sessions depends on shadowing being enabled, as described next.

### Enabling Shadowing on a Server

If you want to shadow ICA sessions, shadowing must be enabled on the MetaFrame XP server first and then for the ICA connections on the server.

You can enable shadowing on the MetaFrame XP server during installation of MetaFrame XP. To do this, you must select the default option, which allows shadowing on all ICA connections on the MetaFrame XP server. After you install MetaFrame XP, you can use Citrix Connection Configuration to limit or prohibit shadowing for specific ICA connections on the MetaFrame XP server.

If you select the option that allows shadowing, and also select options to restrict some aspects of shadowing, you cannot remove the restrictions using Citrix Connection Configuration. However, you can add shadowing restrictions for specific ICA connections on the server using Citrix Connection Configuration.

## Prohibiting Shadowing on a Server

If you select the option that prohibits shadowing during installation of MetaFrame XP, shadowing is not enabled for any ICA connections on the MetaFrame XP server. Any limits you set for shadowing during MetaFrame XP installation cannot be removed later in Citrix Connection Configuration.

## Configuring ICA Connections for Shadowing

When you configure an ICA connection, you can use the **Advanced Connection Settings** dialog box to configure shadowing for the ICA connection.

If you want individual user configurations to take precedence over the ICA connection settings for shadowing, select **Inherit User Config** next to the **Shadowing** menu in the **Advanced Connection Settings** dialog box. This makes the **Shadowing** menu not available. For more information on user configuration, see “Precedence of Settings” on page 143.

When the **Inherit User Config** option is not selected, you can use the **Shadowing** menu to configure shadowing for an ICA connection. The shadowing settings affect all ICA sessions that use the ICA connection.

The settings in the **Shadowing** menu are in the form of statements that include terms (described in the following table) for shadowing status and features.

| Term     | Meaning                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enabled  | Shadowing is possible for sessions on the ICA connection                                                                                                                                                                                                                                                                                                                      |
| Disabled | Sessions on the ICA connection cannot be shadowed                                                                                                                                                                                                                                                                                                                             |
| Input    | Refers to using the keyboard and mouse for remote control of the shadowed session.<br>“On” means that the input from the mouse and keyboard are accepted for remote control from the device shadowing the session. “Off” means that this input is not accepted.                                                                                                               |
| Notify   | Refers to a notification message that MetaFrame XP sends to an ICA Client user. The message asks the user to allow someone to shadow the session. Users can accept or deny shadowing requests.<br>“On” means the server notifies users of all attempts to shadow sessions. “Off” means the server does not notify users, so they cannot deny permission or prevent shadowing. |

For example, one option in the **Shadowing** menu states: “is enabled, input off, notify on.” This setting does the following: allows shadowing; prohibits remote control with the keyboard and mouse during shadowing; and requires the notification (and permission) of ICA Client users before anyone can shadow their sessions.

---

**Note** If you disable input for remote control or user notification when you install MetaFrame XP, options for these features are not available in the **Shadowing** menu in Citrix Connection Configuration. However, the options still appear in Microsoft's user properties dialog box, but choosing them does not override the settings you select during MetaFrame XP installation. In general, you can use individual client properties to disable shadowing features on a per-user basis, but not to enable shadowing features that you disable on a MetaFrame XP server.

---

## Configuring ICA Audio Settings

When you create or edit an ICA connection, you can use the **ICA Settings** button to configure audio for ICA Clients that connect to the MetaFrame XP server through that ICA connection.

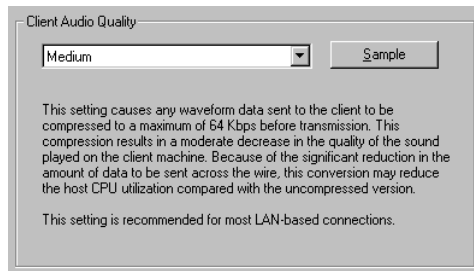
When you click the **ICA Settings** button, the **ICA Settings** dialog box appears. From the drop-down list in the Client Audio Quality area, you can specify the audio quality to use for the connection. High, Medium, and Low audio quality settings are available.

**High.** This setting is recommended for connections only 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 computer. The host CPU utilization can decrease compared with the non-compressed version due to the reduction in the amount of data to be 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 Moderate setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

**Sample.** You can click the **Sample** button to play a brief audio sample at the selected quality setting.



Audio mapping for ICA Clients can cause excessive load on the MetaFrame XP server and network. High quality increases bandwidth requirements by sending more audio data to ICA clients. High quality audio also increases server CPU utilization.

ICA Client users can also select an audio quality setting. If settings on the client and server are not the same, the lower quality setting is used for the session.

In the **Client Settings** dialog box, you can disable audio for an ICA connection.

---

**Note** Audio mapping requires that sound hardware and drivers be installed and configured correctly on the MetaFrame XP server. The **Sample** button in the **ICA Settings** dialog box is not available if audio hardware is not detected by Citrix Connection Configuration.

---

## Configuring Client Device Mapping

Citrix ICA Clients support mapping devices on client computers so they are available to the user from within a remote control ICA session. You do not need a network or RAS connection to use ICA Client device mapping. Client device mapping provides:

- Access to local drives, printers, and serial ports
- Cut-and-paste data transfer between an ICA session and the local Windows clipboard
- Audio (system sounds and Wav files) playback from the ICA session

During logon, the ICA Client informs the 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 ICA Client printers so they appear to be directly connected to the MetaFrame XP 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.

The MetaFrame XP server lists all client disk and printer devices under the Client Network icon in Network Neighborhood.

During a session, users can use ICA Printer Configuration to map client devices not automatically mapped at logon. For more information on using the ICA Printer Configuration utility, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

## Options for Client Device Mapping

Client device mapping options are specified in the **Client Settings** dialog box in Citrix Connection Configuration.

The Connection options control whether 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.

**Connect client drives at logon.** If this option is checked, the client computer's drives are automatically mapped at logon.

**Connect client printers at logon.** If this option is selected, MetaFrame XP maps printers that are configured on client computers with ICA Clients for Windows. With ICA Clients for DOS, users can manually map printers.

**Default to main client printer.** If this option is checked, the user's default client printer is configured as the default printer for the ICA session.

**Inherit user config.** If this option is selected, the per-user settings in User Manager are used.

To automatically connect to only the printer configured as the default printer when the user logs on, select the **By default, connect only the client's main printer** check box.

Default printers can be set on the ICA Client device. Users can override the default printer mapping with ICA Client Printer Configuration. For more information on ICA Client Printer Configuration, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Click **Client Mapping Overrides** to disable client device connections.

## Client Drive Mapping

Client drive mapping is built into the standard Citrix device redirection facilities. The client drives appear as a network type (Client Network) in Network Neighborhood. The client's disk drives are displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive.

### How MetaFrame XP Assigns Drive Letters to Mapped Client Drives

By default, the drives on the client system are automatically mapped to drive letters on the MetaFrame XP server during logon. The server tries to match the client drives to the client drive letters; for example, the client's first floppy disk drive to A, the second floppy disk drive to B, the first hard drive partition to C, etc. This allows the user access to client drive letters in the same way from local or remote sessions.

These drive letters are often used by the drives on the MetaFrame XP server. In this case, client drives are mapped to other drive letters. The MetaFrame XP server starts at V and searches in ascending order for free drive letters.

### Reassigning Server Drives

For an ICA session, a MetaFrame XP server tries to map disk drives on a client device to the typical drive letters for the client. If the drive letters are available, the server maps the client's first floppy disk drive to A, the second floppy drive to B, the first hard disk drive to C, and so on. However, a server can't map client device drives to letters that are assigned to the server's own disk drives.

During MetaFrame XP installation, the Setup program provides an option for you to change the drive letters of the MetaFrame XP server. By changing the server to use drive letters that are higher, such as M, N, O, the original lower drive letters become available for assignment to the drives on client devices. This can make the use of drives on client devices less confusing for end users, because they will see their drives identified by typical drive letters.

If you want to change server drive letters, you must do this during MetaFrame XP installation. Changing server drive letters after MetaFrame XP installation can cause unstable performance by the server, components of the operating system, and installed applications.

---

---

**Warning** With utilities provided in Windows NT 4.0 and Windows 2000, it is possible to change server drive letters after MetaFrame XP installation. Citrix advises against changing server drive letters after MetaFrame XP installation. Doing so can destroy data stored on disk drives and can leave MetaFrame XP and the operating system unable to operate.

---

---

## Controlling Drive Mapping Assignments When Using NetWare Login Scripts

Client drive mapping and NetWare login script execution occur in parallel. If the login script maps NetWare network drives, it is possible that a user could find drive V mapped to his client drive C during one session but mapped to a NetWare drive during another.

You can avoid this problem by adding two registry values in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\InitialNetwareDrive:

### REG\_SZ: InitialClientDrive

Defines the first drive letter to use for client drive mapping. The system searches backward through the alphabet to assign drive letters to client drives that could not be mapped to their “native” drive letters.

### REG\_SZ: InitialNetWareDrive

Defines the drive letter to use for the NetWare SYS:LOGIN directory that is mapped to the preferred server during the initial NetWare attachment. This setting is the equivalent of the DOS VLM Net.cfg setting “First Network Drive.” If this value is not set, the first available drive letter starting with C and working up to Z is used for this mapping.

## Client Printer Mapping

Client printer mapping allows a remote application running on a MetaFrame XP server to access client printers (printers that are attached locally to client computers). The client mappings appear as another network type, Client Network, to the Windows Print Manager.

MetaFrame XP maps client printers when a user logs on and deletes client printers when the user logs off, if the printers do not contain unfinished print jobs. If the print queue contains print jobs, MetaFrame XP retains the printer and the print jobs.

For more information about client printers and printer management in MetaFrame XP server farms, see “Managing Printers for ICA Clients” on page 207. For information about specific ICA Clients, refer to the *Citrix ICA Client Administrator's Guide* for each ICA Client you use.

## Client Serial Port Mapping

Client COM port mapping allows a remote application running on the Citrix server to access devices attached to COM ports on the client computer. Client COM ports are not automatically mapped to server ports at logon, but can be mapped manually using the **net use** or **change client** commands. See Appendix A, “MetaFrame XP Command Reference,” for more information on the **change client** command.

For more information on client COM port mapping, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

## Client Audio Mapping

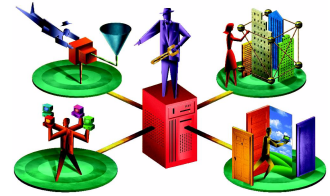
Client audio mapping allows applications running on the Citrix server to play sounds through sound device on the client computer. DOS and Win16 ICA Clients require Sound Blaster 16-compatible sound cards. ICA Win32 Clients require any Windows-compatible sound card; the ICA Win32 Client uses standard Windows API calls for audio.

The MetaFrame XP server can control the amount of bandwidth used by client audio mapping. Audio mapping is configured per-client and per-connection in the **ICA Settings** dialog box.

For more information on using client audio mapping, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.



# Deploying ICA Clients to Users



This chapter addresses issues to help you plan and implement your deployment of the ICA Clients.

This chapter includes the following topics:

- Choosing a Deployment Method, page 159
- Using the ICA Client CD, page 163
- Deploying the ICA Clients, page 165
- Updating the ICA Clients, page 169
- Configuring the Client Update Database, page 172
- ICA Client Deployment Practices, page 184

## Choosing a Deployment Method

To access applications on MetaFrame XP servers, your users run ICA Client software on their client devices. You can deliver the appropriate ICA Client to your users and install the software with the following methods:

- Using a Web browser
- Downloading from a network share point
- Using installation diskettes

---

**Tip** If you are updating the ICA Clients, use the Client Update Database to deploy the latest versions of the ICA Client software.

---

If you are a system administrator for a small company with users in one physical location, installing the ICA Client software from floppy disks or from a network file server presents few problems.

You can eliminate user involvement in the installation process by installing the ICA Client software on each user's machine using a set of floppy disks or the ICA Client CD. This method is useful if your users have limited computer experience.

If your users have a moderate level of computer expertise, you can direct them to a network share point containing the ICA Client files. You can send users an e-mail message that contains both a link to the installation files and instructions for installing the software. Installation by users can eliminate the need for you to manually install ICA Client software.

In a large enterprise or an application service provider (ASP) environment, with hundreds or thousands of users in multiple locations, manual installation methods are not efficient. In these situations, Web delivery of ICA Client software is the best choice.

The table below lists common computing environments and the appropriate deployment methods to use in each scenario.

| Organization                                                                                               | Deployment method      | Requirements                                                                                   |
|------------------------------------------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------|
| Enterprise, ASP supplying personalized content and published applications                                  | Citrix NFuse           | Users run a supported Web browser (see the <i>NFuse Administrator's Guide</i> for a full list) |
| Enterprise, ASP, small business                                                                            | Web-based installation | Users run a Web browser to access an ICA Client download Web site and install software         |
| Enterprise, small business                                                                                 | Network share point    | Users connect to a network share point and install software                                    |
| Small business (single site); organization with remote users who require ICA Client installation diskettes | Diskettes              | Client devices have floppy disk drives                                                         |

## Delivering Applications to Users

To choose the best method for deploying the ICA Clients, decide how your end users will access published applications.

If you want to deliver applications to your users by a Web page, use MetaFrame XP in conjunction with Citrix NFuse, or the Application Launching and Embedding (ALE) feature in MetaFrame XP. When you deliver applications using a Web-based method, users launch Web browsers to access applications published on MetaFrame XP servers.

If you do not want to deliver applications to your users by a Web page, publish the applications for direct access. To directly access applications published on MetaFrame XP servers, users launch ICA Client software. Using the ICA Client for Win32, users can launch Program Neighborhood to access the applications they are authorized to use on the MetaFrame XP servers. Using the ICA Client for Win16, users launch Remote Application Manager to establish connections to servers and published applications.

## **Developing Application Portals with Citrix NFuse**

If you have, or are planning to implement, a corporate Web-based portal, use Citrix NFuse in conjunction with MetaFrame XP to integrate personalized application sets and information into a single Web site on your company's Intranet or another Web location. With NFuse, users launch a Web browser to access published applications.

An NFuse system consists of three components: a Citrix server farm, a Web server, and client devices. NFuse includes an application programming interface (API) and an easy-to-use Web site wizard that allow you to configure all ICA session options on the Web server rather than at each user's desktop.

When a user logs on to an NFuse-enabled Web site the Web-based ICA Client Installation feature checks the user's computer for the presence of ICA Client software. If the ICA Client software is not detected, the Web-based ICA Client Installation feature identifies the user's platform and presents the appropriate ICA Client software for download and setup.

---

**Important** You can install NFuse as part of MetaFrame XP setup. If you choose to install NFuse, an optional NFuse Web site is installed on your MetaFrame XP server. This Web site contains logic that at runtime searches the MetaFrame XP server's document root directory for the presence of ICA Clients.

If the server's document root directory does not contain the ICA Clients, the NFuse Web site does not include the ICA Client installation option in the Web pages presented to the user.

To enable the Web-based ICA Client Installation feature for the Web site installed by MetaFrame setup, copy the Icaweb directory from the ICA Client CD to a directory named "Citrix" in the MetaFrame server's document root directory. For example:

```
c:\inetpub\wwwroot\citrix\
```

You must copy the Icaweb directory and all of its contents to this directory for Web-based ICA Client Installation to work with the NFuse Web site.

---

If you are planning to implement a Citrix NFuse system, see the *NFuse Administrator's Guide* for more information. If you are not planning to implement a Citrix NFuse system, but want to deploy ICA Client software using a Web-based method, see "Web-Based Installation" on page 165.

## Application Launching and Embedding

If you are not planning to implement a Citrix NFuse system, but want to deliver published applications to your users on a Web page, you can use Application Launching and Embedding. ALE allows users to run applications published on MetaFrame XP servers by clicking hyperlinks on a Web page.

For more information about Application Launching and Embedding, see the online help for the Citrix Management Console utility. For more information about using the Citrix ICA Win32 Client with Application Launching and Embedding, see the *Administrator's Guide* for the ICA Win32 Client.

## Determining the Scope of ICA Client Deployment

Take the following factors into consideration before you decide which deployment method to adopt:

**The ICA Clients you need to deploy.** To determine which ICA Clients you need to deploy, determine which client devices and operating systems you need to support.

A smaller organization with many similar client devices might need to deploy the ICA Client on only one or two platforms. In this scenario, using installation diskettes or copying the necessary files to a central network share point for download are the most efficient deployment methods.

Heterogeneous computing environments and geographic separation of large enterprises and ASPs can make it impossible to predetermine which client devices need to be supported. In these scenarios, Web-based installation is the most efficient deployment method.

**Centralized control and configuration requirements.** Determine what limits you need to impose on users' access to published applications. You can configure various settings before you initially deploy the ICA Clients.

For information on preconfiguring ICA Clients, see the *Administrator's Guide* for the required ICA Client, or the Support area of the Citrix Web site at <http://www.citrix.com>.

**Ease-of-use requirements for your end-users.** Providing a simple installation process that requires little interaction from end-users might be a key factor.

Enterprises and ASPs with hundreds or thousands of users with varied computing expertise require the most foolproof deployment process. You can “push” the ICA Client software to your users by various methods, including through the use of logon scripts or windows scripts, or through the use of a commercial software distribution package.

## Using the ICA Client CD

The ICA Client CD contains setup and installation files for all ICA Clients. You can use the ICA Client 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. For more information on installing ICA Client software see the *Administrator's Guide* for the required ICA Client.

You can copy the necessary files from the ICA Client CD to your server using the ICA Client Distribution wizard. You can then access the ICA Client files from your server.

The ICA Client Distribution wizard appears during MetaFrame XP setup. If you skipped this step during MetaFrame XP setup, you can run the wizard by choosing **Programs > Citrix > MetaFrame XP > ICA Client Distribution Wizard** from the **Start** menu.

Use the ICA Client Distribution wizard to:

- Create or update ICA Client images on your server
- Create or update the ICA Client Update Database

- Install or upgrade the pass-through ICA Win32 Client on the server
- Install the *Administrator's Guides* for all ICA Clients

For detailed instructions on running the ICA Client Distribution Wizard, see “Installing ICA Client Software” on page 82.

## Pass-Through ICA Client

The ICA Client Distribution Wizard installs the pass-through ICA Win32 Client on the server. You can give users running other ICA Clients access to the features of Program Neighborhood by publishing the server desktop, or publishing Program Neighborhood as an application.

Users running other ICA Clients can define a single connection to the Program Neighborhood published application. When users connect to the Program Neighborhood published application, they can launch all other applications published on the MetaFrame XP servers in your farm from a single interface.

## ICA Client Object

The ICA Client Object specification makes available a set of application programming interfaces (APIs) to the ICA Win32 Client. Any application that supports object embedding can interface with and pass instructions to this ICA Client.

The APIs give Citrix server administrators, Web developers, and advanced users of the ICA Client software the ability to programmatically control the appearance and behavior of the ICA Win32 Client. With these APIs you can:

- Use the ICA Client Object with commercial desktop applications that support object embedding, including standard Web browsers such as Internet Explorer and Netscape Navigator, as well as the Microsoft Office suite of business applications.
- Integrate ICA functionality into third-party applications.
- Use the ICA Client Object APIs within custom scripts (Visual Basic and HTML) to programmatically integrate and manipulate the appearance and behavior of the ICA Client.

For more information about the ICA Client Object, see the *Citrix ICA Client Object Programmer's Guide*, located on the ICA Client CD.

## Deploying the ICA Clients

The following section explains how to deploy the ICA Clients using Web-based installation, from a network share point, and with installation diskettes.

You can integrate components of the methods that follow with your existing electronic software distribution system, or create scripts that permit an unattended install of the ICA Client software on your users' devices.

### Web-Based Installation

More companies are turning to Web-driven technology to deliver information and applications to their employees. For large enterprises and ASPs, Web-based delivery can greatly automate repetitive tasks and centralize control of configuration options. Large organizations naturally want to minimize user involvement with software installation.

For companies that are not using Citrix NFuse, Citrix offers an installation method that uses a Web browser on the client device as the interface for downloading the ICA Client. Users access a setup page containing a link to the appropriate ICA Client setup program.

This section describes how to set up an ICA Client download Web site on a Windows-based Web server.

---

**Tip** If you are planning to implement a Citrix NFuse system, see the *NFuse Administrator's Guide* for information and instructions on deploying the ICA Clients with NFuse.

---

### Creating the ICA Client Download Web Site

You need the following components to set up an ICA Client download Web site:

**Installation Web pages.** These Web pages include hyperlinks to initiate the download of the ICA Client setup files. The pages are distributed on the NFuse CD in the \WebInst directory.

**ICA Clients.** The ICA Clients packaged for Web-based installation are distributed on the ICA Client CD in the \icaweb directory. If you ran the ICA Client Distribution wizard, these files are on your Citrix server.

---

**Important** You can also download the components and documentation for Web-based installation from the download area of the Citrix Web site at <http://www.citrix.com/download>.

Please be aware that the procedure to install the components downloaded from the Citrix Web site is different from the procedure to install the components located on the NFuse CD and ICA Client CD. Follow the instructions in this manual only if you are using the NFuse CD and ICA Client CD. If you are downloading the components from the Citrix Web site, follow the instructions posted with the packages in the Download area.

---

You can build an ICA Client download Web site with support for multiple languages. You must first set up a single-language ICA Client download Web site, as described next. After you set up a single-language download Web site, see “Adding Support for Additional Languages” on page 167 to add support for one or more additional languages.

► **To set up a single-language ICA Client download Web site**

1. Create a directory on your Web server for the ICA Client Web-based installation files. The directory `\ica60` is used throughout these instructions to represent the target directory on your Web server.
2. Copy the contents of the `\WebInst` directory on the NFuse CD to the target directory on your Web server. For example, type the following command at a command prompt (substitute `d:\` with the letter of your CD-ROM drive):

**xcopy d:\webinst \ica60 /s**

This creates the following directory structure in the `\ica60` folder:

```
\de
\en
\es
\fr
\images
\ja
```

If you inserted the English-language NFuse CD to set up an English-language download Web site, the `\en` subdirectory includes download and setup instructions in English for all supported ICA Clients.

3. Insert the ICA Client CD into your Web server's CD-ROM drive or locate the `\icaweb` directory on your Citrix server.

4. Copy the contents of the appropriate language directory in the \icaweb directory to the target directory on your Web server. For example, if you are setting up a download Web site in English, type the following command at a command prompt:

```
xcopy d:\icaweb\en \ica60 /s
```

5. Publish a link to Setup.htm.

The instructions on the Setup.htm page recommend a platform to the user, who can choose an alternate client platform and language. When the user selects an ICA Client platform, a page with installation instructions appears. The user clicks the **Download** button on this page to initiate the download process.

## Adding Support for Additional Languages

Each language edition of NFuse includes the necessary Web-based installation HTML pages and the ICA Clients for the target language. ICA Client software currently is available in five languages.

The following table lists the supported languages and the corresponding abbreviations that identify the subdirectories on the NFuse CD and the ICA Clients CD.

| Language | Directory abbreviation |
|----------|------------------------|
| English  | en                     |
| French   | fr                     |
| German   | de                     |
| Japanese | ja                     |
| Spanish  | es                     |

---

**Important** If you have the NFuse CD and the ICA Client CD in an additional language, follow the instructions in this manual. However, you can also download the necessary components in additional languages from the Download area of the Citrix Web site at <http://www.citrix.com/download>.

Please be aware that the procedure to install the components downloaded from the Citrix Web site is different from the procedure to install the components located on the NFuse CD and ICA Client CD. Follow the instructions posted on the Citrix Web site if you are downloading the components.

---

► **To add support for additional languages to the ICA Client download Web site**

After you set up a single language ICA Client download Web site as described previously, use this procedure to support additional languages.

1. Copy the HTML component in the desired language to the appropriate language subdirectory of the \ica60 directory on the Web server.

With the German-language NFuse CD, for example, use the following command at a command prompt to copy the files from the CD to the Web server (substitute *d:* with the letter of your CD-ROM drive):

```
xcopy d:\webinst\de \ica60\de /s
```

---

**Note** This action overwrites the setup.htm file that was placed in the \ica60\de subdirectory when you set up your single-language ICA Client download Web site. The new Setup.htm file in the \ica60\de subdirectory provides download and setup instructions in German for all supported ICA Clients.

---

2. Copy the corresponding language version of the ICA Client software to the appropriate subdirectory of the \ica60 directory.

If you are working with the German-language ICA Client CD, for example, insert the CD into your Web server's CD-ROM drive. Type the following command at a command prompt to copy the contents of the appropriate language subdirectory of the \icaweb directory to the target directory on your Web server (substitute *d:* with the letter of your CD-ROM drive):

```
xcopy d:\icaweb\de \ica60\de /s
```

3. Repeat the previous steps for each language you want to add to your ICA Client download Web site.

## Deploying ICA Clients Over a Network

► **To deploy ICA Client software from a network share point**

1. If you have not done so already, run the ICA Client Distribution wizard to copy the ICA Client files from the ICA Client CD to your MetaFrame XP server.
2. Copy the ICA Client files to a network share point. For example, if you are deploying the ICA Win32 Client, copy all files from \ICA32. The ICA Client Distribution wizard copies this folder to the location %SystemRoot%\System32\Clients\Ica on the server.
3. Supply your users with the path to the file Setup.exe. For example, the path to setup.exe for the ICA Win32 Client is *x:\ICA32\disks\disk1\setup.exe* (*x:* represents the share point).

4. To install the ICA Client software, double-click the Setup.exe file to begin the installation process. For more information on installing the ICA Clients from a network share point, see the *Administrator's Guide* for the required ICA Client.

## Deploying ICA Clients Using Diskettes

Use the ICA Client Creator to create installation disks for the ICA Client for DOS, the ICA Client for Windows 95/98/Me/NT, and the ICA Client for Windows 3.x. The procedure is described below. For more information on installing the ICA Clients from installation diskettes, see the *Administrator's Guide* for the required ICA Client.

Installation files for other ICA Clients are contained in the following folder: %SystemRoot%\System32\Clients\Ica. You can copy the files for the required ICA Client to create installation diskettes.

You can also distribute diskettes to remote users who require the ICA Client but do not have access to a common network share point.

### ► To use the ICA Client Creator to make installation diskettes

1. If you have not done so already, run the ICA Client Distribution wizard to copy the ICA Client files from the ICA Client CD to your Citrix server.
2. From the **Start** menu, choose **Programs > Citrix > MetaFrame XP > ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.
3. Select the desired ICA Client. The dialog box displays the number of disks you will need.
4. Select **Format Disks** to format the disks when creating the installation media.
5. Click **OK** and follow the directions to copy the ICA Client files to diskettes.

## Updating the ICA Clients

Use the Client Auto Update feature to update ICA Client installations with new versions of ICA Client software. As new versions of ICA Clients are released by Citrix, you add them to the Client Update Database. New versions of ICA Clients are released periodically and can be downloaded from the Citrix Web site at <http://www.citrix.com/download>.

When users log on to a Citrix server, the server queries the ICA Client to determine the version number. If the version matches the one in the Client Update Database, the logon continues. If the server detects an older version on the client device, the user is informed that a newer version of the ICA Client is available for download. The user can update the client according to the options you set in the database.

**Note** For users of NFuse Version 1.5: If you have populated the Client Update Database with the ICA Clients from the ICA Client CD included in the MetaFrame XP media, users may receive unnecessary update notifications.

When a user visits an NFuse 1.5 Web site (either a site produced by the NFuse 1.5 Web Site wizard or an example Web site), the client detection code in the site may incorrectly notify the user that the client device does not have the latest ICA Client installed and prompt the user to update the ICA Client. Select the **Do not show this window at login** checkbox in the update message box to prevent the message from appearing again.

The client detection process has been corrected in NFuse Version 1.51, which is included in the MetaFrame XP media.

---

Client auto update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and asynchronous). Client auto update supports the following features:

- Automatically detects older ICA Client files
  - 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
- 

**Important** Client auto update can update client files to newer versions of the same product and model. For example, it can update the ICA Win32 Client to a new version. It cannot upgrade the ICA Win16 Client to the ICA Win32 Client.

---

## 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.

| Product/model number | Platform                  |
|----------------------|---------------------------|
| 1/1                  | ICA Client for 16-bit DOS |
| 1/2                  | ICA Client for Win16      |
| 1/3                  | ICA Client for Win32      |
| E/1                  | ICA Client for 32-bit DOS |
| 52/1                 | ICA Client for Macintosh  |

---

| Product/model number | Platform                       |
|----------------------|--------------------------------|
| 1F09/6               | ICA Client for Windows CE x86  |
| 1F09/7               | ICA Client for Windows CE SH3  |
| 1F09/8               | ICA Client for Windows CE SH4  |
| 1F09/9               | ICA Client for Windows CE MIPS |
| 1F09/A               | ICA Client for Windows CE PPC  |
| 1F09/B               | ICA Client for Windows CE ARM  |
| 51/7                 | ICA Client for Linux           |

The process of updating ICA Clients with new versions uses the standard ICA protocol.

- If an update is needed, by default, the Citrix server informs the user that a new client is available and asks to perform the update. You can specify that the update occurs without informing the user and without allowing the user to cancel the update.
- By default, the user can choose to wait for the client files to finish downloading or to download the files in the background and continue working. Users connecting to the Citrix server with a modem get better performance waiting for the update process to complete. 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. You can force the user to disconnect and complete the update before continuing the session. The user must log on to the Citrix 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 directory on the user's local disk.

## Configuring the Client Update Database

You can configure a Client Update Database on each Citrix server in a server farm, or configure one database to update the ICA Clients for multiple Citrix servers.

Use the ICA Client Distribution wizard to create or update the ICA Client Update Database. The wizard appears during MetaFrame XP setup. If you skipped the wizard during MetaFrame XP setup, run the wizard by selecting **Start > Programs > Citrix > MetaFrame XP > ICA Client Distribution Wizard**. For more information about the ICA Client Distribution wizard, see page 82.

The Client Update Database contains the following ICA Clients: 32-bit Windows, 16-bit Windows, 32-bit DOS, Macintosh, and several WinCE Clients. As new versions of the ICA Clients are released by Citrix, 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 access the ICA Client Update Configuration utility

1. From the **Start** menu, choose **Programs > Citrix > MetaFrame XP > 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 Citrix server uses to update ICA Clients. The window shows the ICA Clients in the database.

| 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      |

## 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

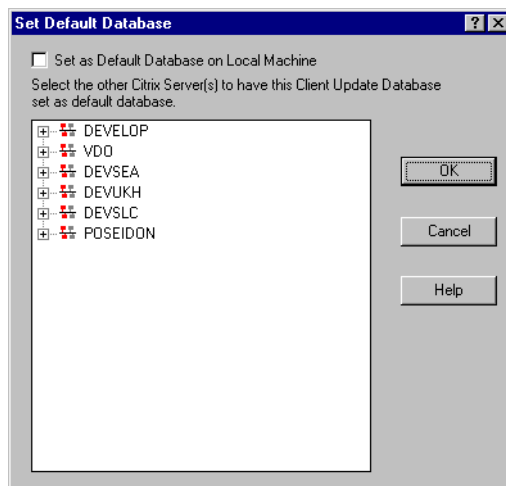
1. From the **Database** menu, choose **New**. The **Path for the new Client Update Database** dialog box appears.
2. Enter the path for the new update database and click **Save**. The utility creates a new update database in the specified location and opens the new database.

## Specifying a Default Client Update Database

You can configure one Client Update Database to be used by multiple Citrix servers. If the Client Update Database is on a shared network drive, use the ICA Client Update Configuration utility to configure your Citrix servers to use the same shared database.

### ► To set the default database for Citrix servers

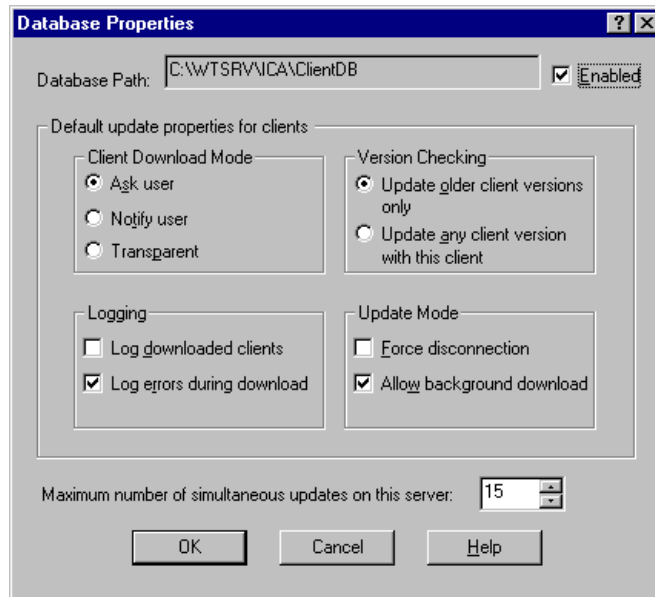
1. From the **Database** menu, choose **Open**.
2. Specify the path to the default database and click **Open**. The database opens.
3. On the **Database** menu, click **Set Default**. The **Set Default Database** dialog box opens:



4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other Citrix 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. You can 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.
- The **Enabled** check box must be selected for this database to perform ICA Client updates.

---

**Tip** If the ICA Clients do not need to be updated, disable the database to shorten your users' 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 all client versions 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 and continue working. 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.

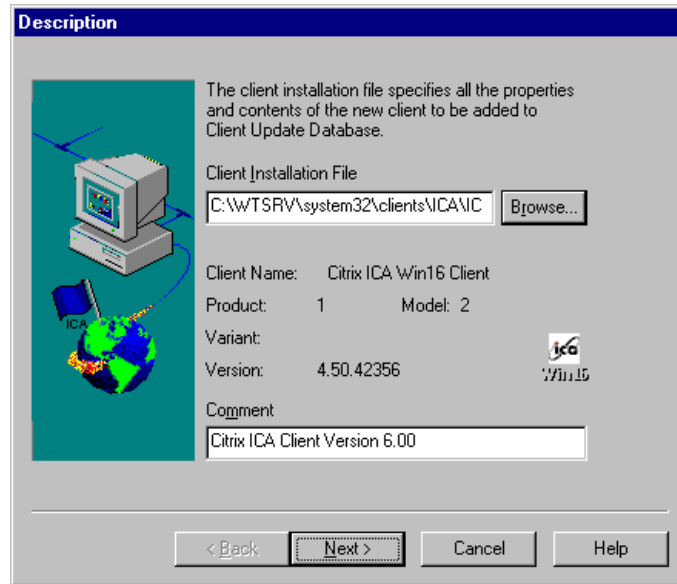
Click **OK** when you finish configuring the database settings.

## Adding ICA Clients to the Client Update Database

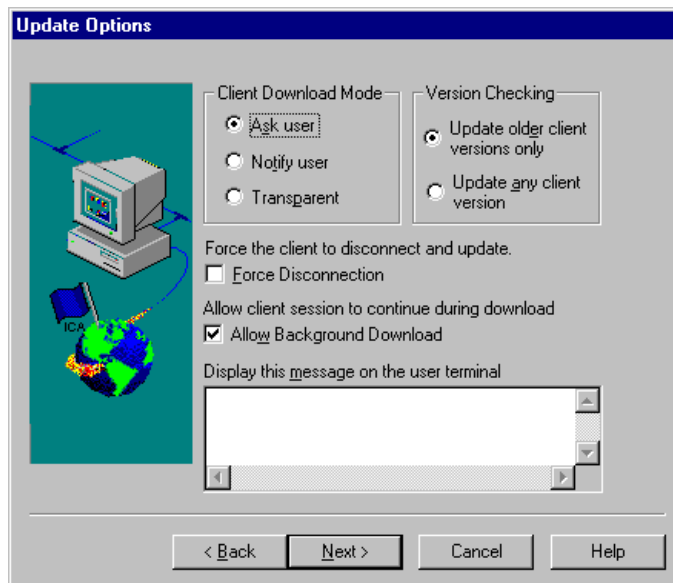
When you want to deploy a newer version of the ICA Client, add it to the Client Update Database. You can download the latest ICA Clients from the Download area of the Citrix Web site at <http://www.citrix.com/download>.

### ► 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 ICA Client CD.



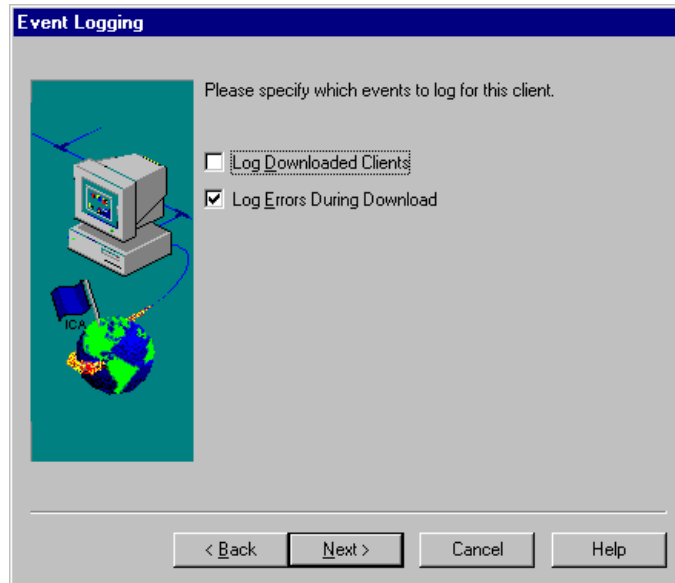
3. The client name, product number, model number and version number are displayed. The **Comment** text box displays a description of the new client. You can modify this comment. Click **Next** to continue.
4. The **Update Options** dialog box appears. The options on this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients.



For definitions of the options available in this dialog box, see “Configuring Default Client Update Options” on page 174, or see the online help for this dialog box.

Click **Next** when you finish configuring the client update options.

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



The database-wide logging options are displayed. You can specify different behavior for individual clients.

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.

Click **Next**.

6. 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. For example, when Citrix releases a new version of the ICA Win16 Client, you add it to the Client Update Database. 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 into 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 that contains multiple versions of the same client significantly slows the checking procedure that is carried out each time a user connects to the server.

### ► To remove an ICA Client from the database

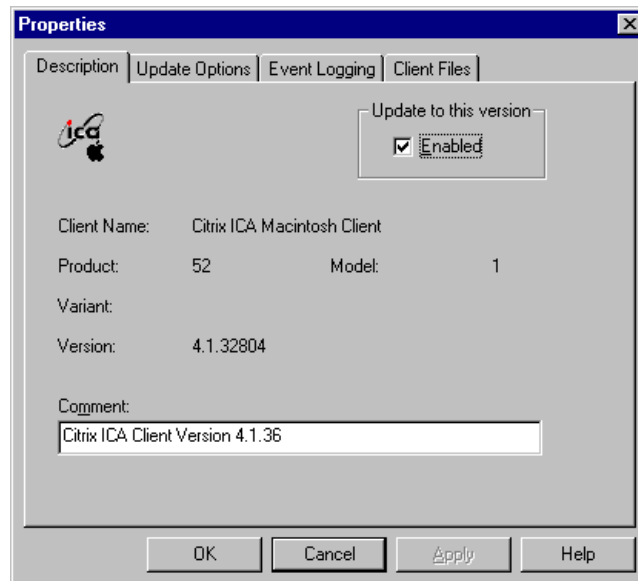
1. Select the ICA Client you want to remove from the database.
2. From the **Client** menu, choose **Delete**. A message box asks you to confirm the deletion.
3. Click **Yes** to remove the client.

## Changing the Properties of an ICA Client in the Database

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 an ICA Client in the Client Update Database**

1. Select the client you want to change.
2. On the **Client** menu, choose **Properties**. The **Properties** dialog box appears. This dialog box contains tabs labeled **Description**, **Update Options**, **Event Logging**, and **Client Files**.

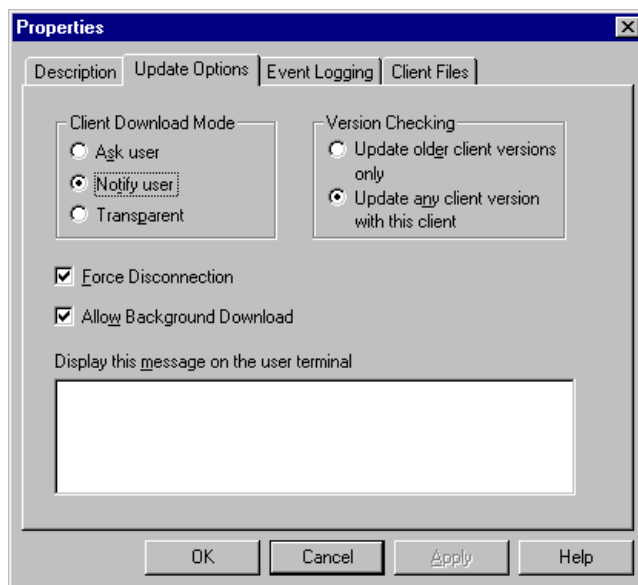


3. The **Description** tab of the **Properties** dialog box lists the client name, product number, model number, and version number.

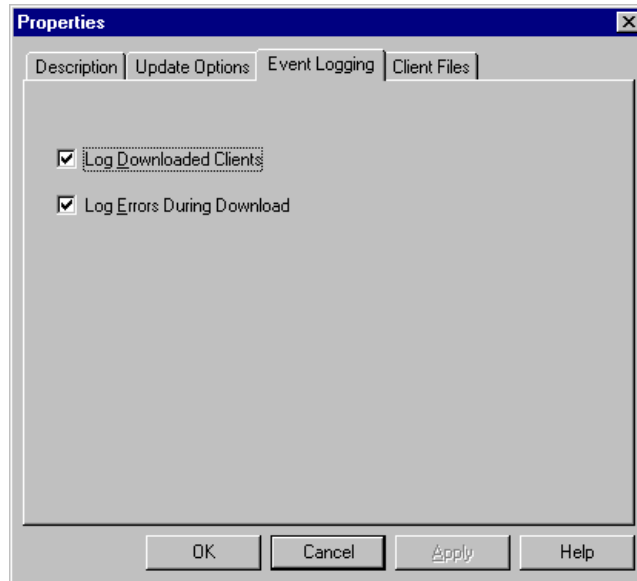
Select the **Enabled** check box to update the same platform ICA Client to this version.

Optionally, enter a new comment in the **Comment** text box.

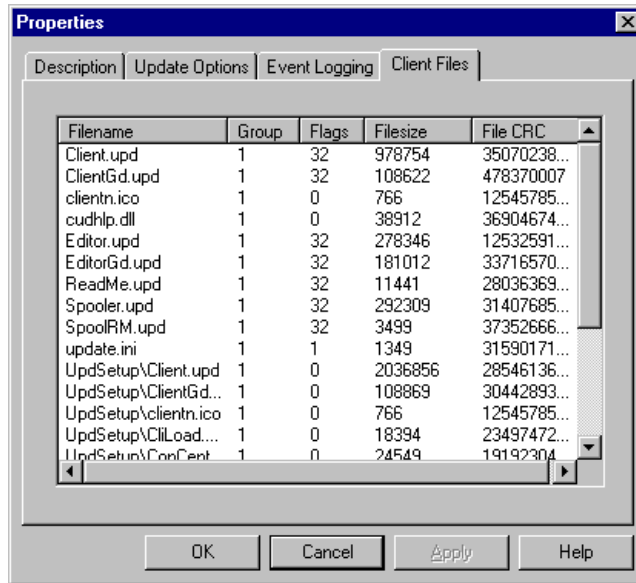
4. Use the **Update Options** tab to configure update options for the client.



- 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 and continue working. 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.

## ICA Client Deployment Practices

The following section provides examples of ICA Client deployment practices for a large manufacturing enterprise, a regional bank, an application service provider, and an insurance company.

### Manufacturing Enterprise

The Best Paper Company employs approximately 30,000 people, located in shop-floor sites and remote offices in several countries. The enterprise has many pockets of MetaFrame XP installations, each owned and managed by a different team. Published applications include PeopleSoft and Oracle Manufacturing and Financials.

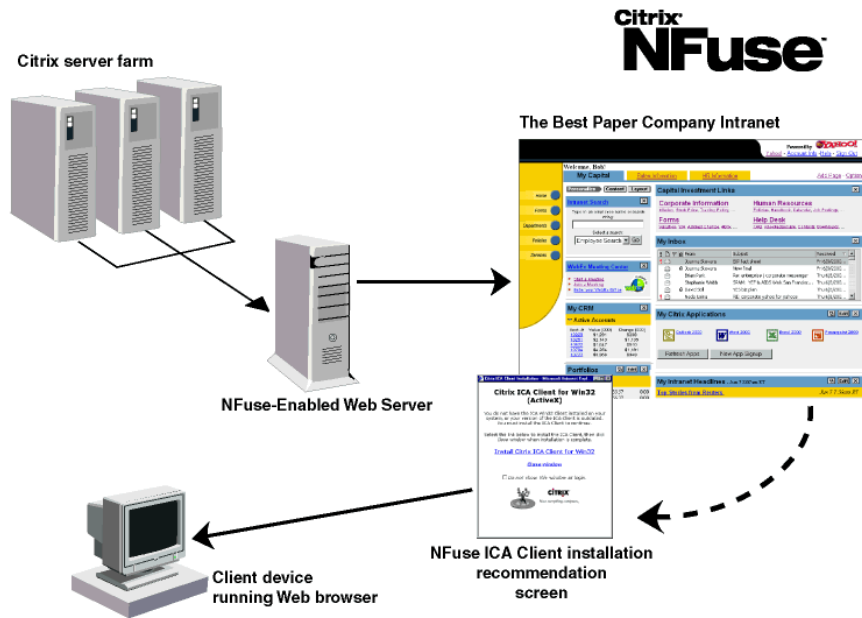
The networking environment includes the following:

- Ethernet LANs
- Frame Relay WAN
- Internet connections for remote users

- TCP/IP network protocol
- Thousands of 486 PCs running Windows 95, thousands of Pentium PCs running Windows 2000

The Best Paper Company is using Citrix NFuse to give users access to critical applications. The company's existing Citrix server farms function as an application serving back-end. The server farm supplies application set information and hosts published applications.

Application sets are delivered to groups or individual users, based on their role in the company. An employee launches a Web browser to access the NFuse portal site. When the employee is authenticated to the server farm the application set assigned to the employee is displayed within the browser. To start an application, the employee clicks a hyperlink on the NFuse portal site.



The company uses NFuse's built-in Web-based ICA Client Installation feature to deploy the ICA Client software. When a user launches an application, the user's computer is checked for the ICA Client software. If the client is not detected, the user's platform is identified and the appropriate ICA Client software is presented for download and setup.

The Web browser and ICA Client work together as viewer and engine. The browser displays the user's application sets and the ICA Client launches applications.

For more information about NFuse, see the *NFuse Administrator's Guide*.

## Regional Bank

Lenders Bank has 500 employees in its headquarters and 15 branch locations. The bank's staff connects to MetaFrame XP servers to run more than 60 applications, including Ceridien and Transcend-Banker financial applications, Microsoft Office 2000, Microsoft Outlook, and AS/400 applications.

The networking environment includes the following:

- Ethernet LANs
- Secured Fractional T1, 56K leased lines
- TCP/IP network protocol
- 200 486 PCs, Wyse Winterm Windows-based terminals

The bank's IT department used the Web-based ICA Client Installation package (without NFuse) to construct an ICA Client download Web site, integrated into the bank's Intranet, for ICA Client software deployment. The IT department posted user-friendly instructions that walk end-users through downloading and installing the ICA Client software.

For more information about constructing an ICA Client download Web site, see "Web-Based Installation" on page 165 of this guide. The elements required to construct an ICA Client download Web site can also be downloaded from the Citrix Web site at <http://www.citrix.com/download>.

## Application Service Provider

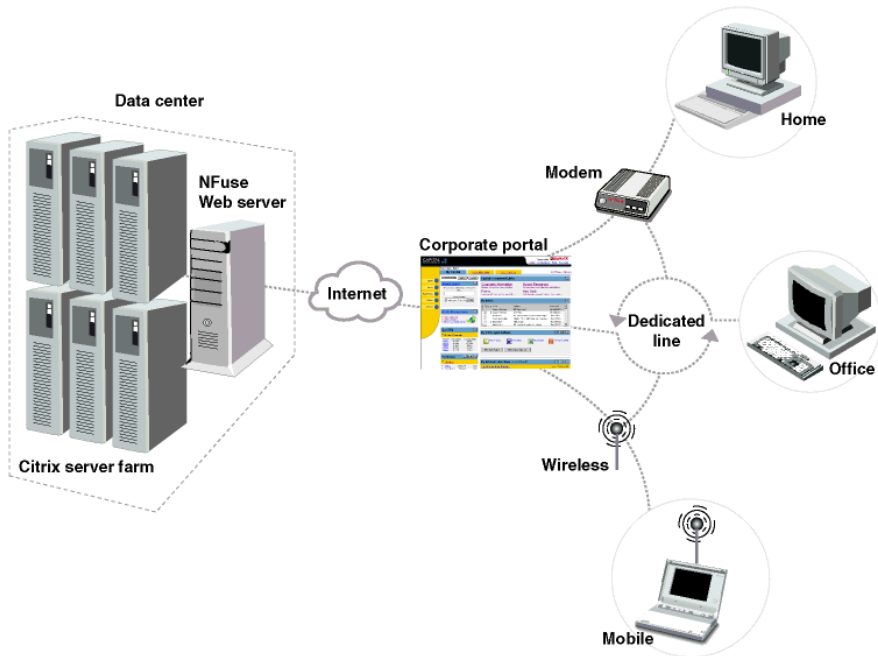
LinkToUs, a commercial ASP, has four data centers, located in the United States, Canada, and Ireland, serving over 100,000 end-users worldwide. LinkToUs offers its customers the following connection options:

- Internet
- Virtual Private Network (VPN)
- Frame Relay
- X.25 connections in more than 105 countries
- Private point-to-point lines

LinkToUs customers can choose from a variety of published application set packages, which can include applications from Microsoft, Onyx, Great Plains, Sales Logic, and Pivotal.

With the implementation of Citrix NFuse, LinkToUs is now also designing and hosting highly customized corporate entry portals providing application integration, personalized Web content, external Web content integration, and search and categorization features.

LinkToUs works closely with its customers to develop user groups that meet their needs, and then builds application sets based on these groups. The ASP can display published applications from several Citrix server farms, including MetaFrame XP for Windows and MetaFrame for UNIX servers, in a single Web page.



The Web developers at LinkToUs created a simple script that allows automatic download and install of the ICA Win32 Web Client. When end-users access the corporate portal hosted by LinkToUs for the first time, the ICA Client is automatically downloaded and installed on the user's computer.

For more information about NFuse, see the *NFuse Administrator's Guide*. For more information about automatic download and installation of the ICA Clients for the Web, see the Online Knowledge Base, accessible from the Support area of the Citrix Web site at <http://www.citrix.com>.

## Insurance Company

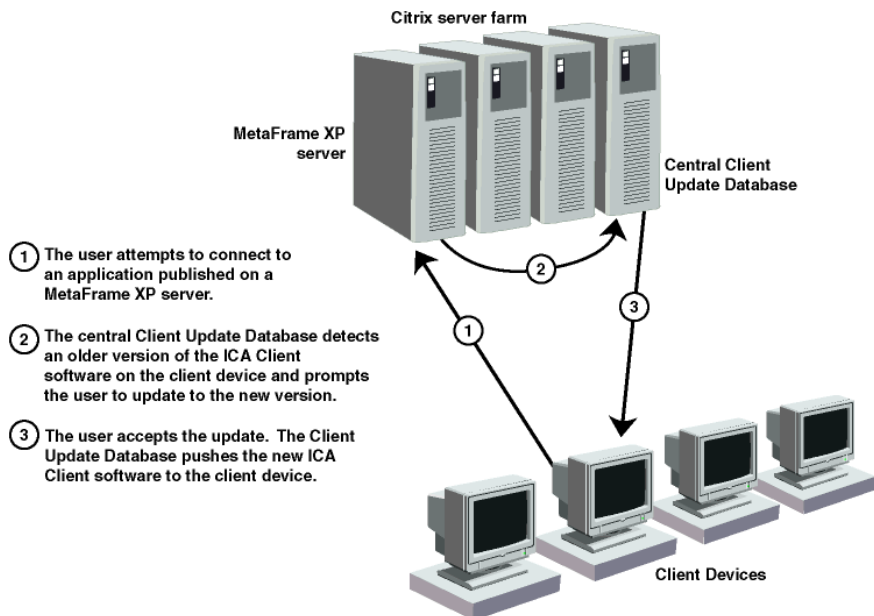
Protection Insurance is a mid-sized company with 800 employees. Published applications include PeopleSoft and customized applications for the insurance industry from JDI and Prelude. The networking environment includes:

- Ethernet LAN, Internet, and dial-up connections
- TCP/IP network protocol

- Pentium PCs running Microsoft Windows NT

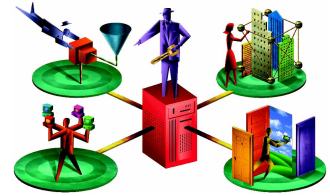
The purchasing department pre-configures users' systems to include the latest version of the ICA Win32 Client. When applications are published, a shortcut to each application is placed on the user's **Start** menu. Users can also launch Program Neighborhood to access other application sets they have permission to use.

When Citrix releases a new version of the ICA Client, Protection Insurance's IT staff adds the client to the Client Update Database. When users initiate their connections to a MetaFrame XP server, the new ICA Client is "pushed" to their client devices. The Citrix administrator sets the update options to force users to disconnect from their ICA sessions and accept the updates. This ensures that all staff members are using the most current version of the ICA Client.



For more information about client auto update, see "Updating the ICA Clients" on page 169 of this guide.

# Publishing Applications



This chapter describes concepts and procedures for making applications available to ICA Client users.

This chapter includes the following topics:

- Introduction to Publishing Applications, page 189
- Configuring User Access to Applications, page 195
- Publishing Applications, page 197

## Introduction to Publishing Applications

*Publishing applications* refers to a procedure you use to make applications that are installed on a MetaFrame XP server easily available to ICA Client users. With application publishing, you can:

- Increase your control over application deployment
- Shield users from the mechanics of the Windows server environment
- Push application icons and shortcuts to user desktops through Program Neighborhood

The Citrix Management Console simplifies application publishing. With the Citrix Management Console, you can publish applications on any server in the MetaFrame XP server farm, including servers that are temporarily out of operation.

## User Access to Published Applications

When you publish applications, user access to those applications is greatly simplified in several areas.

**Addressing.** Instead of connecting to a Citrix server by its IP address or server name, ICA Client users can connect to a specific application by whatever name you give it. Connecting to applications by name eliminates the need for users to remember which servers contain which applications.

**Navigation of the server desktop.** Instead of requiring client users to navigate the Windows interface on MetaFrame XP servers to find and start installed applications, published applications present most ICA Client users with only the desired application in an ICA session.

**User authentication.** Instead of logging on and logging off multiple Citrix servers to access applications, Program Neighborhood users can authenticate themselves a single time to all servers in a server farm and get immediate access to all applications configured for their user group or specific user names.

Publishing applications for the special Citrix Anonymous user group lets you completely eliminate the need for user authentication for those applications you want to provide to all users on your network. For more information, see “Anonymous Users” on page 195.

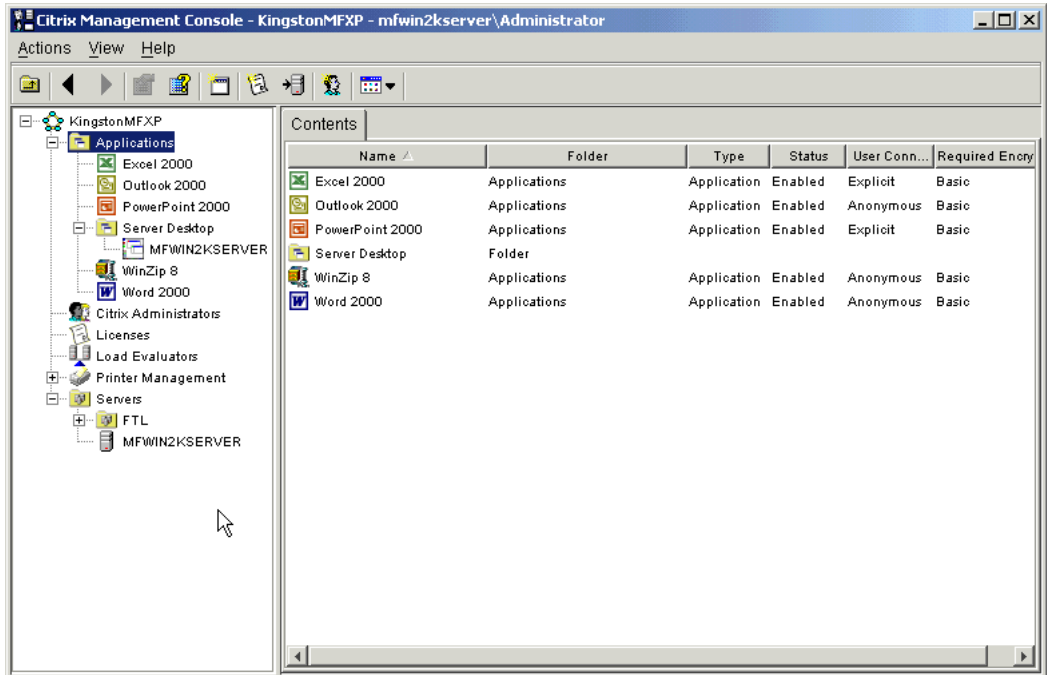
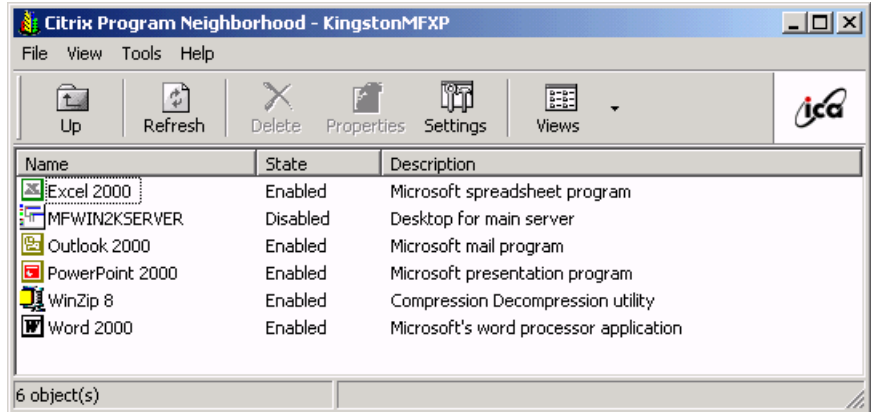
## Using Program Neighborhood

Program Neighborhood facilitates user access to published applications by eliminating the need for client-side configuration of connections.

Program Neighborhood presents *application sets* to client users. An application set is a user's view of published applications that user has authority to access. Each user performs a single authentication to all servers in a farm and is then presented with an application set containing each application configured for his or her specific user account or user group. Published applications appear as icons in the view of the farm and are configured for such connection properties as session window size and colors, supported level of encryption, audio compression, and video.

*Program Neighborhood displays application sets—the published applications that each user is authorized to run (right)*

*Citrix Management Console shows the server farm's published applications under the Applications node (below)*



**Note** Program Neighborhood is the program users run to connect to MetaFrame XP servers with the Citrix ICA Win32 Client, which runs on Windows 95, Windows 98, Windows Me, and Windows 2000 platforms, and the ICA Java Client.

Using Program Neighborhood simplifies the process of locating and connecting to applications. For example, to run a word processing application, users start Program Neighborhood, perform a single logon to authenticate to all published applications in an application set, and simply double-click the icon for the word processing program. To start additional applications, a user just double-clicks the application icons in Program Neighborhood.

Publishing applications in your server farm benefits users of other, non-Program Neighborhood ICA Clients (such as the UNIX, Macintosh, DOS, and Web Clients) as well. Although they do not support the complete (server and client-side) administrative configuration of the ICA connection provided by Program Neighborhood, these ICA Clients do support connections to published applications.

In the case of the ICA UNIX, Macintosh, and DOS Clients, client users benefit from application publishing's simplified addressing and desktop navigation when they configure connections to published applications using their connection configuration managers.

In the case of the ICA Clients that work with Web browsers (which are available as an Internet Explorer Active-X control, Netscape plug-in, or Java applet), you can create Web access that lets users of client devices running a Web browser and an ICA Web Client click a link in a Web page to start a published application.

## Setting up a Pass-Through ICA Client

To give a broader range of your users the benefits of Program Neighborhood, you can publish the ICA Win32 Client application on your Citrix servers.

Users of the ICA Client on other platforms can define in their connection managers a single connection to the Program Neighborhood application. After they connect to Program Neighborhood, they can use the interface to launch all other applications that are published on all the servers in the server farm.

To give other users the benefit of Program Neighborhood, use Citrix Management Console to publish the application, as described later in this chapter; the executable file to publish is `pn.exe`. This program file is located at `%systemroot%\System32\ICAPassThrough`.

## Administrative Control of Applications

When you publish applications, you get greater administrative control over application deployment with:

**Selected user access.** You publish applications for specific users and user groups. By definition, an application you publish for a specific user group is unavailable to other groups.

**Enabled and disabled applications.** You can temporarily restrict all access to an application by disabling it. You can enable the application later to return access to users. This capability is useful when you want to take an application offline for maintenance.

**Multiple-server application hosting.** Application publishing, when used in conjunction with Citrix Load Manager, lets you direct ICA Client connection requests to the least busy server in a farm of servers configured to run an application.

---

**Note** Citrix Load Manager is included in some Citrix MetaFrame product packages. Load Manager provides features for managing server loads in Citrix server farms. For information on Load Manager, refer to the *Getting Started* manual, which is available in PDF format in the DOC directory of the MetaFrame XP CD-ROM and in the Documentation directory on a MetaFrame XP server.

---

## Types of Applications You Can Publish

MetaFrame XP supports publishing of four types of applications.

### Standard Applications

You can publish any application that can run on the Windows console (32-bit Windows applications, 16-bit Windows applications, DOS applications, POSIX applications, and OS/2 applications).

### Citrix Installation Manager Applications

To publish Citrix Installation Manager applications, you must install Citrix Installation Manager on your network. Citrix Installation Manager performs remote unattended installation of applications on Citrix servers. Using Installation Manager, you can simultaneously install an out-of-the-box application on all Citrix servers on your network from a single point without manual intervention. You can install applications on servers regardless of their physical location, network connection type, or individual hardware setup.

Citrix Installation Manager can push application installations to Citrix servers and it can uninstall applications. Publishing a Citrix Installation Manager application causes each server that you specify to download and install the application. Deleting a published Installation Manager application uninstalls the application from each server that you specified to run the application.

## Load-Managed Applications

MetaFrame XP supports publishing of an application on multiple servers if Citrix Load Manager is enabled on those servers.

When an ICA Client user connects to an application that is published on more than one server in the server farm, Load Manager determines where to start the ICA session based on server load.

You can adjust server load calculations for individual servers with Load Manager. For instructions on configuring load evaluators, see the *Getting Started* Guide for Citrix Load Manager. The guide is available in the DOC folder on the MetaFrame XP CD-ROM, and is installed in the Documentation folder on MetaFrame XP servers.

## Videos

To publish videos, you must install Citrix VideoFrame on your network. Viewing a published video requires the same published application connection procedure used by standard published applications. When a user connects to a published video, the ICA Client connects to a MetaFrame XP server configured to run the video, determines the location of the video, and then launches the Windows Media Player, which plays the video from the VideoFrame server.

---

**Note** Playing videos requires that users have the Citrix ICA Client for Win32 (Program Neighborhood) and Microsoft Windows Media Player.

---

## Using Published Applications

When you publish an application, configuration information for the application is stored in the IMA data store for the server farm. The configuration information includes properties of the ICA connection, including its name, users who can connect to the application, and client-side session properties that include window size, number of colors, level of encryption, and audio setting

To the ICA Client user, a published application appears very similar to an application running locally on the client device. The way the user starts the application depends upon the ICA Client in use on the client device.

**ICA Win32 Client and ICA Java Client.** After starting Program Neighborhood, these users find a list of applications published for their user account or user group.

**ICA Client users on UNIX, Macintosh, and DOS.** Using connection managers, these ICA Client users can browse a list of all applications published on the network and select an application to run.

**Web access.** Users who have the ICA Win32 Client or the ICA Java Client can access applications that are embedded or launched by clicking a hyperlink on a Web page. For more information on ICA Client configurations that work with application launching and embedding, see “Deploying ICA Clients to Users” on page 159.

**NFuse portal users.** If your users access applications through an NFuse application portal, the applications they are authorized to access appear as icons on a customized Web page. NFuse connects the user’s client device to the application and downloads the appropriate ICA Client, if necessary, to the user’s device. For information on deploying and configuring application portals with NFuse, see the *NFuse Administrator’s Guide*.

## Configuring User Access to Applications

Before you publish applications, consider the network account authority that you use, and the ways that the configuration of your users’ accounts can affect user access to applications.

For general information on user account configuration, including use of Windows NT domains and Windows Active Directory, see “Network Configuration and Account Authority Issues” on page 40.

Publishing applications in Citrix server farms lets you set up two types of application access: explicit user account access and anonymous access.

---

**Note** The total number of users, whether anonymous or explicit, who are logged in to a Citrix server farm at the same time cannot exceed the total license count of all the MetaFrame XP connection licenses in the server farm.

---

### Anonymous Users

During MetaFrame XP installation, the Setup program creates a special user group named *Anonymous*. By default, this user group contains 15 user accounts with account names in the form Anonx, where *x* is a three-digit number from 000 to 014. By default, anonymous users have guest permissions.

---

**Note** MetaFrame XP cannot create anonymous user accounts on Windows primary or backup domain controllers. Therefore, you cannot publish applications for anonymous access on a MetaFrame XP server if it is a domain controller. Citrix does not recommend installing MetaFrame XP on Windows domain controllers.

---

If an application you publish on a MetaFrame XP server can be accessed by users with guest permissions, you can configure the application using the console to allow access by anonymous users.

When a user starts an application that is configured for anonymous users, the server does not require an explicit user name and password to log the user on to the server and run the application.

Anonymous users are granted minimal ICA session permissions, which include the following properties that differ from standard ICA session permissions for the default user:

- Ten-minute idle (no user activity) time-out
- Log off from broken or timed-out connections
- No password is required
- The user cannot change the password

When an anonymous user session ends, no user information is retained. The server does not maintain desktop settings, user-specific files, or other resources created or configured for the ICA Client.

For more information on configuration of ICA connections on MetaFrame XP servers, see “Configuring ICA Client Connections” on page 137.

### **Configuring Anonymous User Accounts**

The anonymous user accounts that MetaFrame XP creates during installation do not require additional configuration. If you want to modify their properties, you can do so with the standard Windows user account management tools.

### **Explicit Users**

An *explicit user* is any user who is not a member of the Anonymous group. Explicit users have Windows user accounts, which you create, configure, and maintain with standard user account management tools in Windows.

Explicit users who log in to MetaFrame XP server farms to run applications have a persistent existence: their desktop settings, security settings, and other information is retained between ICA sessions in a specific Windows profile.

---

**Important** Do not assign any explicit users to the Anonymous group.

---

# Publishing Applications

Making applications available to clients is an integral function of MetaFrame XP servers. Although applications do not have to be published for ICA Clients to access them, publishing provides management benefits and makes application access easier for end users.

You can use the Citrix Management Console to publish applications on any server in the farm you log into; you do not have to run the Citrix Management Console from the MetaFrame XP server where the applications are installed. The server or servers hosting a published application must be a member of the farm.

## ► To publish an application

1. Find the intended host server or servers under the Servers object before attempting to publish the application. If the server is listed, it is a member of the farm.
2. From the **Actions** menu, choose **New > Published Application**.
3. Follow the instructions in the Publish Application wizard. Detailed help on each step is available by clicking **Help**.

---

**Tip** If you want to publish an application on additional servers, you can drag the application in the console tree and drop it on MetaFrame XP servers to publish the application on the servers. The application must already be installed on the servers, and it inherits its settings from the first server where you published the application.

---

## Creating an ICA File

An ICA file contains published application information in Ini file format. When an ICA Client receives an ICA file, it initializes a session to run the specified application on the MetaFrame XP server. For more information, see “Deploying ICA Clients to Users” on page 159.

## ► To create an ICA file for an application

1. Select the published application in the Applications folder in the left pane of the Citrix Management Console. After you select an application, new menu options and toolbar buttons appear.
2. Click the **Create ICA File** button on the toolbar, or choose **Application > Create ICA File** from the **Actions** menu.
3. Follow the instructions in the Create ICA File wizard to create your ICA File.

## Creating an HTML File

You can easily create an HTML page that connects ICA Client users to a published application from a Web page. The connection is implemented through an ICA file. You can also create the ICA file when you generate the HTML file.

### ► To create an HTML file

1. Select the published application in the Applications folder in the left pane of the console.
2. Choose **Create HTML File** from the toolbar or the **Actions** menu.
3. Follow the instructions in the wizard to create your HTML file.

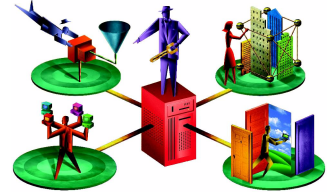
## Removing Published Applications

As you publish updated applications on your servers, you can remove the older or less-used applications. Removing a published application does not uninstall the application from the MetaFrame XP server, or make it completely unavailable to ICA Clients. It simply stops advertising the application's availability in Program Neighborhood.

### ► To remove a published application

1. Locate the application under **Applications** in the left pane of the Citrix Administration Tool.
2. Select the published application you want to remove.
3. From the **Actions** menu, choose **Delete Published Application**.
4. When prompted, confirm the deletion by clicking **OK**.

# Managing Users and ICA Sessions



This chapter describes how to manage users and their ICA sessions in a Citrix server farm. It includes information about using Citrix Management Console to monitor users' connections and the status of ICA sessions.

This chapter contains the following topics:

- Managing ICA Sessions, page 199
- Shadowing ICA Sessions, page 204

## Managing ICA Sessions

Citrix Management Console provides centralized monitoring and management of your user's ICA sessions. You can use the console to:

- Monitor ICA sessions according to the published applications and MetaFrame XP servers to which they are connected
- Send messages to users in active ICA sessions
- Reset or disconnect sessions and log off users
- Use shadowing to monitor and remotely control selected sessions

## Controlling Logons by ICA Clients

You can control the ability of ICA Client users to establish sessions on the MetaFrame XP servers in a server farm by enabling or disabling logons. By default, logons are enabled when you install MetaFrame XP. You might want to disable logons to servers when you install software or perform other maintenance or configuration tasks.

► **To enable or disable logons**

An option to enable and disable logons is available on the **MetaFrame Settings** tab in each server's **Properties** dialog box.

1. Right-click a server in the tree in Citrix Management Console and choose **Properties** to display the **Properties** dialog box.
2. To disable logons by ICA Client users, clear the checkbox labeled **Enable logons to this server** on the **MetaFrame Settings** tab.
3. To restore the ability of ICA Clients to connect to the server, select **Enable logons to this server**.

**Viewing Information About ICA Sessions**

Several tabs in Citrix Management Console display information about ICA sessions in table format. Each row in the table lists details for one ICA session. You can use different views in the console to monitor user sessions based on the published applications that users are connected to, or the servers where the ICA sessions are established.

Active sessions appear on several tabs when a MetaFrame XP server has active ICA Client sessions:

- When you select a published application in the tree, sessions that are running the application appear on the **Users** tab
- When you select a server, sessions that are running on the server, including console sessions, appear on the **Users** and **Sessions** tabs
- When you select the Servers node in the tree, the **Users** tab displays sessions running all servers; console sessions do not appear on this tab

KingstonMFXP

Applications

MFWIN2KSERVER

Word 2000 pubs

Citrix Administrators

Licenses

Load Evaluators

Printer Management

Servers

MFWIN2KSERVER

UsersSessionsProcessesLicensesLoad Manager MonitorPrintersPrinter Drivers

| Session   | User       | Session ID | State  | Type | Client Name | Logon Time               | Application       |
|-----------|------------|------------|--------|------|-------------|--------------------------|-------------------|
| Console   | michellefo | 0          | Active |      |             | Nov 16, 2000 12:58:58 PM |                   |
| ICA-top#3 | Anon002    | 3          | Active | ICA  | ZYDECO      | Nov 16, 2000 3:46:19 PM  | Word 2000 pubs    |
| ICA-top#2 | Anon001    | 2          | Active | ICA  | MF_wes      | Nov 16, 2000 3:43:24 PM  | Word 2000 pubs    |
| ICA-top#1 | Anon000    | 1          | Active | ICA  | MF_wes      | Nov 16, 2000 3:40:52 PM  | MFWIN2KSERVER1AB0 |
| RDP-Top   |            | 65,537     | Listen | RDP  |             |                          |                   |
| ICA-top   |            | 65,536     | Listen | ICA  |             |                          |                   |
|           |            | 4          | Idle   |      |             |                          |                   |
|           |            | 5          | Idle   |      |             |                          |                   |

Auto Refresh: off

For example, if you select a published application, the **Users** tab in the right pane displays the sessions in which the selected application is running. The information appears in columns, which display the user name, client device name, session ID number, the state of the session, and the time of logon.

## Session Information Displayed in the Console

On the tabs that display ICA session information, each row represents one ICA session. You can click the column headings to sort the information. When you click the active sort heading, you reverse the sort order. You can rearrange the information in the table by dragging a column heading to a new position.

The session information that appears in the console includes details that help you identify the various types of sessions and the users associated with the sessions. The following column labels appear on tabs that display session information.

**Session.** The Session column identifies a session with a name that includes the protocol that the session uses, usually ICA or RDP (for Microsoft's Remote Display Protocol). The name also includes the network protocol for the session, and a number that distinguishes the session from other sessions that are running on the server.

**User.** The name of the user account that initiates a session appears in the User column for each session. In the case of anonymous connections, the user name is a string with the letters "Anon" followed by a session number.

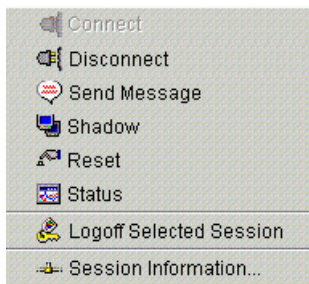
**Client name.** This column displays the name of the client device that is running the session.

**Session ID.** The Session ID is a unique number that begins with 0 for the first connection to the console. Listener sessions are numbered from 65,537 and numbered backward in sequence.

**State.** A session's state is listed as Active, Listen, Idle, Disconnected, or Down. The meaning of session state labels is explained in the following section, which describes commands you use for managing sessions on MetaFrame XP servers.

## Using Session Management Commands

In Citrix Management Console, you can select ICA sessions and choose commands to manage the sessions. You can use the **Actions** menu and the toolbar buttons in the console to choose session management commands. You can also right-click on a session in the console and choose session management commands from the context menu that appears.



## Disconnecting ICA Sessions

To disconnect an ICA session, choose **Disconnect**. When you disconnect a session, you close the connection between the ICA Client and the MetaFrame XP server. However, this does not log off the user, and programs that were running in the session still run on the server. If the ICA Client user then connects to the server (by selecting a published application or custom connection to the server), the disconnected session is reconnected to the client.

## Connecting to Disconnected Sessions

When an ICA session is disconnected, the word “Disconnected” appears in the State column on the tabs in Citrix Management Console where session information appears.

You can connect to a user’s disconnected session by choosing **Connect**. Your session must be capable of supporting the video resolution of the disconnected session. From the system console, you can connect only to sessions that were disconnected from the console.

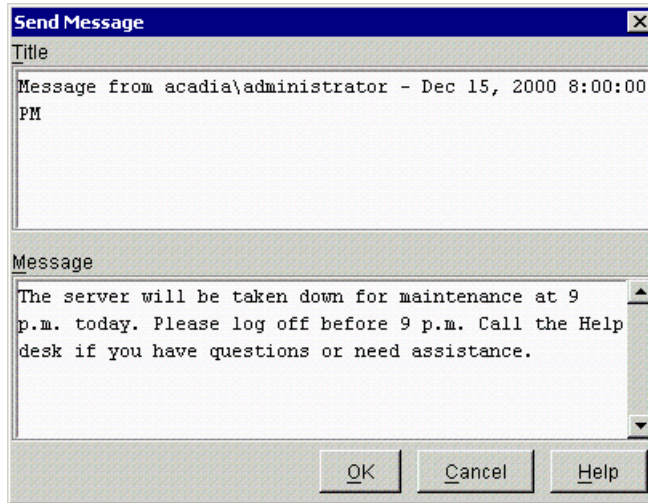
## Sending Messages to Users

You can send a message to a user by selecting the user’s sessions and choosing **Send Message**. You can select multiple sessions to send a message to multiple users at the same time. For information on viewing sessions, see “Viewing Information About ICA Sessions” on page 200.

To broadcast a message to all users, you can select all active user sessions in the right pane in the console.

In the **Send Message** dialog box, you can type a message title; the user name of the Citrix administrator who is logged in to the console and the current time appear in the **Title** box by default. Type the message text in the **Message** box. The text you type automatically wraps to the next line if you type past the right margin.

When you finish typing the message, click **OK** to send the message to the selected sessions.



## Resetting ICA Sessions

Resetting a session with the **Reset** command terminates all processes that are running in that session. You can use the **Reset** command to remove remaining processes in the case of a session error. However, resetting a session can cause applications to close without saving data.

If you reset a disconnected session, the word *Down* appears in the State column for the session. When you refresh the console display or when the next automatic refresh occurs, the session no longer appears in the list of sessions.

## Resetting All Sessions

Special sessions that listen for requests to connect to the server are identified by the word *Listen* in the State column. If you reset a listener session, the server resets all sessions that use the protocol associated with the listener. For example, if you reset the ICA listener session, you reset the ICA sessions of all users who are connected to the server.

## Viewing ICA Session Status

You can use the **Status** command to display user and I/O information about a session. The **Session Status** dialog box displays connection statistics, including the count of incoming and outgoing data that has been transmitted in the session and the number of errors and the compression ratio used in the session. The dialog box also shows the user name and session name.

By default, the Session Status data is updated every second. You can choose the command buttons in the dialog box to reset the counters and refresh the data.

- Click **Reset Counters** in the dialog box to return all counters to zero.
- Click **Refresh Now** to immediately refresh the displayed data.

## Logging Off ICA Sessions

Choose **Logoff Selected Session** to force a user's session to end. If you select multiple sessions, choosing the commands ends each selected session.

---

**Important** Ending users' sessions with the **Logoff Selected Session** command can result in loss of data if users do not close their applications first. You can send a message to warn users to exit all applications if you need to log off their sessions.

---

## Viewing Session Details

You can select a session in Citrix Management Console and choose **Session Information** to view detailed information about the processes, settings, ICA Client software, and client cache associated with the selected ICA session.

## Viewing and Terminating Processes

If you need to terminate a process started by an ICA session, select an ICA Client session and select the **Processes** tab in the right pane of the console. You can right-click on a process and choose the **Terminate** command to terminate the process.

# Shadowing ICA Sessions

You can monitor the actions of users in ICA sessions by shadowing the sessions. A shadowed session is displayed in the session of the *shadower*, the administrator who establishes shadowing.

Shadowing an ICA session provides a powerful tool for you to assist and monitor users. Shadowing is a useful option for your Help desk staff, who can use it to aid users who have trouble using an application. Help desk personnel can view a user's actions to troubleshoot problems and can demonstrate correct procedures. You can also use shadowing for remote diagnosis and as a teaching tool.

A shadower can remotely control a shadowed session through the shadower's mouse and keyboard, if this action has not been prohibited by options selected when MetaFrame XP was installed on the server.

---

**Tip** If shadowing restrictions were selected during MetaFrame XP installation, the restrictions cannot be changed later. For more information, see “Configuring Session Shadowing” on page 64.

---

By default, the user who will be shadowed is asked to accept or deny the request to shadow the ICA session.

You can shadow multiple sessions using Citrix Management Console or the Shadow Taskbar.

## Shadowing From the Console

When you use Citrix Management Console for shadowing, you must start shadowing each session individually; if you select multiple sessions, the **Shadow** command and button are not available. If you want to initiate shadowing sessions with multiple users at once, you can use the Shadow Taskbar.

To begin shadowing an ICA session, right-click on the session in the list that you want to shadow, and then choose **Shadow** from the context menu that appears. Or select a session and click the **Shadow** button on the console toolbar.

## Using the Shadow Taskbar

To launch the Shadow Taskbar, choose **Start > Programs > Citrix > MetaFrame XP > Shadow Taskbar**. The Shadow Taskbar appears as a toolbar at the top of the console display.



**Tip** You can click the **Shadow Taskbar** button on the ICA Administrator toolbar to launch the Shadow Taskbar.

---

When the Shadow Taskbar is running and no sessions are being shadowed, the **Shadow** button appears alone on the Taskbar. Click the **Shadow** button and the **Shadow Session** dialog box appears.

Use the **Shadow Session** dialog box to select the sessions you want to shadow. You can select sessions based on the server, the application, or the users who are associated with the sessions. You can select multiple sessions in the dialog box to begin shadowing several sessions at once. Click **OK** to begin shadowing the selected sessions.

For more information on shadowing with the Shadow Taskbar, press F1 to view online help when the Shadow Taskbar is running.



# Managing Printers for ICA Clients



Users can print documents easily when they run applications on MetaFrame XP servers. For most users, printing when they use applications in ICA sessions is no different than printing from applications that run on their own computers.

This chapter describes MetaFrame XP features for making printers available to ICA Clients and managing printers in MetaFrame XP server farms.

This chapter includes the following topics:

- Overview of Printing with MetaFrame XP, page 208
- Printing Configuration in Server Farms, page 209
- Printer Management Features, page 211
- Setting Up Network Printers for ICA Client Users, page 216
- Managing Drivers for Client Printers, page 219
- Limiting Printing Bandwidth in ICA Sessions, page 220
- ICA Client Settings for Printer Access, page 221

To find step-by-step instructions for using the features that are described in this chapter, use the online help feature in Citrix Management Console.

- To launch online help in the console, choose **Help > Contents and Index**.
- For information on Citrix Management Console, see “To use Citrix Management Console” on page 101.

For more information on printing configuration and options for ICA Clients, refer to the *Client Administrator's Guide* for the ICA Clients you plan to deploy.

## Overview of Printing with MetaFrame XP

When ICA Client users run applications that are published on MetaFrame XP servers, they can print to the following types of printers:

- Printers that are connected to ports on the users' client devices on Windows, WinCE, DOS, and Mac OS platforms
- Virtual printers created for tasks such as printing from a PostScript driver to a file on a Windows client device
- Shared printers that are connected to print servers on a Windows network
- Printers that are connected directly to MetaFrame XP servers

## Configuration of Printing Devices

The printers that ICA Clients can use can be categorized by connection types. You can set up three general types of printer connections in a MetaFrame XP server farm: client connections, network connections, and local connections. Therefore, this chapter refers to printers in a server farm as client printers, network printers, and local printers, depending on the type of connection they have in the farm.

**Client printers.** The definition of a *client printer* depends on the ICA Client platform.

- On DOS-based and WinCE client devices, a client printer is a printer that is physically connected by a cable to a port on the client device. A PC or Postscript printer connected to a serial port on a Mac OS system is also considered a client printer.
- On 32-bit Windows platforms (Windows 9x, Windows NT, and Windows 2000), any printer that is set up in Windows (these printers appear in the Printers folder on the client device) is a client printer. Locally connected printers, printers that are connected on a network, and virtual printers are all client printers.

---

**Note** Some virtual printers, such as a fax-modem device that is set up in the Printers folder, might not be available as a client printer in ICA sessions.

---

When a user shares a client printer through Windows printer sharing, the printer appears as a network printer to other users.

**Network printers.** Printers that are connected to print servers and shared on a Windows network are referred to as *network printers*. In Windows network environments, users can set up a network printer on their computers if they have permission to connect to the print server. When a network printer is set up for use on an individual Windows computer, the printer is a client printer for the ICA Client user of that computer.

**Local printers.** Printers that are connected directly to MetaFrame XP servers are *local printers* within a particular server farm. This definition includes a printer that is connected to the MetaFrame XP server that hosts a user's ICA session, as well as printers that are connected to other MetaFrame XP servers in the same server farm.

If a printer is connected to a MetaFrame XP server outside of a server farm (either the server is not a member of a server farm or is a member of a different server farm), the server farm considers the printer a network printer, not a local printer.

## Client Printing in ICA Sessions

The following list summarizes the types of printers that can be available for an ICA Client, based on the printer definitions above. Depending on the user's platform and the printers that exist in the farm, a user who connects to a MetaFrame XP server and runs a published application or desktop in an ICA session can print to the following:

- The user's own client printers
- Network printers that are set up for the farm
- Local printers on the MetaFrame XP server that hosts the user's ICA session
- Local printers on other MetaFrame XP servers that are set up for use in the farm

It's important to note that printer availability can vary with the client device. For specific information about printing capabilities, see the *Client Administrator's Guide* for each ICA Client you plan to deploy.

## Printing Configuration in Server Farms

The previous section describes printers that can be used by ICA Clients. Some printers can be used without being set up specifically for use in a MetaFrame XP server farm. For example, you can make client printers available for ICA Client users on Windows devices without configuring printers on each client device.

This section describes when and how you need to set up and configure printers for ICA Clients. It gives an overview of the configuration features available in MetaFrame XP through Citrix Management Console.

## Printing Configuration Scenarios

The steps required to set up printers for use by your ICA Client users depends on the configuration of the clients, the type of printers you use and their connections, and the configuration of your application servers.

For example, two scenarios for printing appear below. For more information about the printer management setup mentioned in these scenarios, see the feature descriptions later in this chapter.

### Scenario 1: Printers Installed on Windows Clients

ICA Client users run Windows NT Workstation on their computers. Printers are already set up for all users on their client computers (so they can print from applications that they run locally). Some users have PC printers connected directly to their computers, while others print to shared network printers.

In this type of environment, you can set up printers in the server farm by simply installing printer drivers on a MetaFrame XP server and using the replication feature in Citrix Management Console to distribute the drivers to all the servers in the farm.

- The printers that users normally print to are available automatically when they connect to MetaFrame XP servers, because MetaFrame XP creates each user's client printers for use during ICA sessions.
- Because printer drivers installed on Windows NT workstation computers are the same drivers you install on NT 4.0 Terminal Server and Windows 2000 MetaFrame XP servers, you do not need to set up printer driver mapping. Mapping is necessary when the printer drivers you install for Windows 9x client computers and Windows servers have different names.
- When users print from applications running on MetaFrame XP servers, the installed client printers appear in Windows in the following form: *#clientname/printername*. The *clientname* is the name of the client device and *printername* is the name for the installed client printer.

### Scenario 2: Network Printers in a Mixed Environment

In a typical mixed computing environment, users run ICA Clients on a variety of operating systems. Some, but not all users, might have printers connected to their client computers. Shared printers on network print servers might be available to all users, but they might not be set up because users are untrained or because administrators do not want to set up individual clients in a new network deployment or an application service provider environment.

In these situations, you can make printers available easily through MetaFrame XP. MetaFrame XP can autcreate client printers for the workstations that have printers installed. For the entire user base, you can set up network printers to be used by ICA Client users on all client platforms.

- You make printers that are already installed on client computers available in ICA sessions by installing printer drivers on a MetaFrame XP server and using the replication feature in Citrix Management Console to distribute the drivers to all servers in the farm. MetaFrame XP autcreates these client printers when users connect to servers in the farm.
- When some users have Windows 9x client workstations, you map client printer drivers to the drivers you install on MetaFrame XP servers. This is necessary when driver names (for the same printer) are different on Windows 9x and Windows servers. Driver mapping is not necessary for Windows NT Workstation or Windows 2000 clients, which use the same printer drivers as Windows servers.
- You import network print servers into the MetaFrame XP server farm to make the shared printers available to all users when they connect to servers in the farm.
- If some client printer drivers are not compatible with the MetaFrame XP server platforms in the farm, use the Driver Compatibility feature to prevent incompatible printer drivers from causing server errors.
- When users print from applications running on MetaFrame XP servers, the installed client printers appear in Windows in the following form: *#clientname/printername*. The *clientname* is the name of the client machine and *printername* is the name for the installed client printing device.
- When users print to the network printers in the server farm, they see the original assigned network printer names in Windows dialog boxes.

## Printer Management Features

Citrix Management Console provides access to all MetaFrame XP printer management features. You use Citrix Management Console to monitor and configure printers for ICA Client users in a server farm.

To make changes to printer configurations, you need to log in to the console with read-write privileges. If you log in as a user with read-only privilege, you can view printer configuration information but you cannot make changes to existing settings.

For information on using Citrix Management Console, see “To use Citrix Management Console” on page 101.

## Printer Management Views in the Console

You can use MetaFrame XP printer management features from several views in the Citrix Management Console. The first parts of this section describe the console views you can use for managing printers for ICA Client users, and the information you can monitor from the tabs in the console's right pane.

After you launch the console and log on to a Citrix server in the server farm, the left pane in the console displays the tree view of the server farm management nodes. When you select an item in the tree, the right pane displays one or more tabs.

Select the Printer Management node or the Servers node, or the objects under these nodes, to use the primary printer management features in the console.



### Using the Printer Management Node

When you select Printer Management in the console tree, the right pane displays tabs labeled **Contents**, **Bandwidth**, and **Network Print Servers** (the default tab).

When you expand the Printer Management node, the left pane displays objects labeled Printers and Drivers in the tree.

#### Contents Tab

When you select Printer Management, the **Contents** tab displays objects labeled Drivers and Printers. The same objects appear in the tree under Printer Management when you expand the node.

Double-clicking an object on the **Contents** tab is the same as selecting the object in the tree. Either action changes the right pane to display information about the object you select, and puts commands related to the object in the **Actions > Printer Management** submenu and on the console toolbar.

#### Network Print Servers Tab

Use the **Network Print Servers** tab to view the names of network print servers whose printers can be configured in the server farm. When you create a new MetaFrame XP server farm, the tab lists nothing until you import one or more network print servers.

After you import print servers, the **Network Print Servers** tab displays the name of each print server and the date and time when the console last updated the print server information. The tab uses the time zone of the console machine for the date and time display.

**Importing Print Servers.** Use the **Network Print Servers** tab when you want to import a network print server to make its printers available to the users of the server farm. When you select the tab, you can choose **Import Network Print Server** from the toolbar or the **Actions** menu. The command and toolbar button are not available when other tabs are selected.

---

**Tip** Importing a network print server lets users in the server farm use a printer that is not connected to their client device. Client printers are automatically made available to users in their ICA sessions.

---

**Updating Server Information.** If you add printers to or remove them from a network print server, update the print server information to be sure that the console displays the available printers on the **Printers** tab. To do this, select a print server and use the **Update Network Print Server** command from the right-click menu, the toolbar, or the **Actions** menu. You must take this action because updating of print server information does not take place automatically.

**Removing Print Servers.** Removing a print server removes all of its printers from the farm. This is the opposite of importing a network print server. If you remove printers, ICA Client users cannot print to them. If you want to do this, select the print server to remove, and then choose **Discard Network Print Server** from the right-click menu, the console toolbar, or the **Actions** menu. After you confirm the command, the printer server no longer appears on the **Network Print Server** tab and its printers do not appear on the **Printers** tab.

## Bandwidth Tab

When you select Printer Management in the console tree, the **Bandwidth** tab displays the print stream bandwidth setting for each server in the farm. Use this tab to set or remove print stream bandwidth limits on MetaFrame XP servers and copy settings from one server to others. Limiting printing bandwidth can improve application performance for clients when printing and application data must compete for limited bandwidth.

When you select a server in the list on the **Bandwidth** tab, you use the **Edit** command to change its bandwidth setting, or use the **Copy** command to copy its bandwidth setting to one or more servers in the farm. You can use these commands from the right-click menu, the console toolbar, or the **Actions** menu.

When you select the Servers node in the tree, the **Printer Bandwidth** tab provides the same display and features as the **Bandwidth** tab when you select Printer Management.

The **Properties** dialog box for each server in the farm contains a **Printer Bandwidth** tab that you can use to edit the server's print stream bandwidth setting.

For more information about limiting the bandwidth of print data streams, see "Limiting Printing Bandwidth in ICA Sessions" on page 220.

## Drivers Tab

When you select Drivers in the tree, the **Drivers** tab in the right pane displays information about printer drivers installed on MetaFrame XP servers. Use this tab to make sure printer drivers are installed and available as necessary on servers in the farm, and to copy them to other servers.

The tab lists any driver installed on a MetaFrame XP server in the farm. The tab does not list drivers that are installed on network print servers (non-MetaFrame XP servers). You must manually install drivers for all printers that ICA Client users need for printing from ICA sessions, including client printers and network printers.

The driver information includes each driver's name and operating system platform. You select a specific server from the **Server** drop-down menu to display the drivers installed on one server, or select **(Any)** to display all drivers on all servers in the farm.

Use the **Drivers** tab to copy printer drivers to other servers in a server farm. If printer drivers are not already installed, copy the drivers to each server where ICA Client users log on and need access to the driver for printing to client printers or network printers.

To copy a driver, select the driver and then use the **Replicate Drivers** command from the console toolbar, the right-click menu, or the **Actions** menu.

---

**Note** Two tabs in Citrix Management Console show printer driver information. To display the drivers installed on a MetaFrame XP server, you can select the server from the **Server** menu on the **Drivers** tab, or select the server in the console tree and look at the **Printer Drivers** tab. You can use either tab to copy printer drivers to other servers in a farm.

---

## Printers Tab

When you select Printers in the Citrix Management Console tree, the **Printers** tab in the right pane lists all printers that you can configure in the server farm. The list includes the following printers:

- Local shared printers that you install and connect directly to MetaFrame XP servers in the farm
- Network printers that are installed and connected to network print servers when you import the print servers into the farm

The printer list shows the printer name, print server name, driver name, and MetaFrame XP operating system platform for each local printer. For network printers, the list shows only the printer name and print server name.

You can select a local printer on the **Printers** tab and use the console to copy the drivers and settings for the printer to other servers. You cannot copy a driver of a network printer from this tab. (Use the **Drivers** tab to copy drivers from a MetaFrame XP server to other servers.)

Select a printer and use the **Auto-Creation** command to assign users to the printer. Auto-creation makes a printer available in ICA sessions for the users you specify. If you want to allocate other printers to the same users, select a printer and copy its autocreation settings from this tab.

## Using the Servers Node

When you select Servers in the Citrix Management Console tree, multiple tabs appear in the right pane. The tab that relates to printer management is the **Printer Bandwidth** tab. This tab displays the same information as the **Bandwidth** tab that appears when you select Printer Management in the console tree. See “Bandwidth Tab,” above.

## Printers Tab

When you select a MetaFrame XP server in the console tree under the Servers node or on the **Contents** tab, the **Printers** tab displays information about a server’s local printers. The tab displays information about the printers that are connected directly to the server, if you select the Shared option when you install the printers. Printers that you do not share do not appear on the tab.

This tab is similar to the **Printers** tab that appears when you select Printers in the console tree. However, when you select one server, the **Printers** tab displays only the server’s local printer information, not information about network printers in the farm.

You can select a local printer on the **Printers** tab and use the console to replicate the drivers and settings for the printer to other servers. You can also assign users to the printer to make it available as an autocreated printer in the users' ICA sessions. If you want to assign the same users to another printer, select the printer and copy its autocreation settings from this tab.

### Printer Drivers Tab

When you select a MetaFrame XP server in the console tree (under the Servers node), the **Printer Drivers** tab lists printer drivers that are installed on the server. Select a driver name in the list to display the names of all the servers that have the driver installed. Use the **Replicate Drivers** command to copy the driver to other servers in the farm. You need to copy printer drivers to each server where ICA Client users log on and need access to the driver for printing to client printers or network printers.

The **Printer Drivers** tab displays the same information as the **Drivers** tab displays when you select Drivers in the console tree.

## Setting Up Network Printers for ICA Client Users

To make network printers available to ICA Client users, you import network print servers into the MetaFrame XP server farm. Doing this makes all printers that are connected to the print server available to the ICA Client users that you specify. After you install required printer drivers, ICA Client users can print to these printers in their ICA sessions. You use Citrix Management Console to perform these procedures.

### ► To make network printers available to ICA users

The following steps outline the procedure for setting up network printers for ICA Client users. For detailed instructions, use the **Help** menu or click **Help** on the toolbar and dialog boxes in Citrix Management Console.

1. Import network printers from a network print server into the farm. Select **Printer Management** in Citrix Management Console, select the **Network Print Servers** tab, and choose **Import Network Print Server**. Specify the network print server to import.

When the operation finishes, the print server appears on the **Network Print Servers** tab in the console.

2. Install the printer drivers for your network printers on a MetaFrame XP server in the server farm. Use the **Replicate Drivers** command to distribute the drivers to all the MetaFrame XP servers in the farm.

3. Allocate network printers to users. Select a printer on the **Printers** tab and choose **Auto-Creation**. Specify a domain and select the groups and users who need to use the printer.

When a specified user logs on to a MetaFrame XP server in the farm, the printer becomes available in the user's ICA session as if the printer were installed on the user's client device.

4. To set up additional printers for ICA Client users, select the printer you have allocated to users. Choose **Copy Auto Creation Settings** to copy the printer's user list to other printers in the farm.

---

**Tip** Because you set up printers for autocreation by user account, the users can log on to applications from different client devices and use the same network printers. (Because client printers are connected directly, they are available only from the client devices where they are installed).

---

5. If necessary, map client printer drivers to server drivers if the driver names are different on each platform. For details, see "Mapping Printer Drivers" on page 218.

## Installing and Replicating Printer Drivers

To install printer drivers on a MetaFrame XP server, you use the standard Windows printer installation methods. The Add Printer wizard asks for information about a printer and copies the necessary driver files. You might need to insert a Windows installation CD-ROM or media from the printer manufacturer so the wizard can copy the files.

When you use the wizard to install drivers on a MetaFrame XP server, the actual printer is not attached to the server. Select the **Local** option and select any local printer port that does not have an actual printing device connected; you can add multiple printers to one port.

---

**Tip** In server farms where it's practical to do so, install all driver files on one server. If you use MetaFrame XP on both Terminal Server and Windows 2000 servers in the farm, install driver files on a MetaFrame XP server for each platform.

---

Once you install drivers, you can use the driver replication feature in Citrix Management Console to copy the driver files and registry settings to other servers in the server farm. Use the replication feature to save time when you install printer drivers, and to ensure that all drivers are available on all servers where ICA Clients need them, so that the ICA Client users can print to the client and network printers in the farm.

---

**Important** Because printer drivers are platform-specific (designed for either Terminal Server or Windows 2000), do not replicate drivers from a MetaFrame XP server to servers on a different platform. When the **Drivers** tab in the console lists drivers from both platforms and you choose **Replicate Drivers**, the console warns you about this because you can select drivers on either platform to replicate.

---

## Setting Up Automatic Replication of Printer Drivers

You can set up automatic printer driver replication so MetaFrame XP performs replication when you add a server to the farm, or when you restart a server in the farm.

MetaFrame XP maintains one auto-replication list for each platform in the server farm. When you select a printer driver for replication, MetaFrame XP adds the driver to the appropriate auto-replication list. You can add or remove drivers from the auto-replication lists by choosing **Auto-Replication** from the **Drivers** tab in the console.

When you edit the auto-replication list, you can use one server or any server as the source for a particular printer driver. If you specify any server, MetaFrame XP will copy the driver from any server that is available in the farm at the time of auto-replication to a new or restarted server. This setting avoids the possibility that a specific source server for a printer driver might be unavailable when new or restarted servers need to receive a printer driver.

MetaFrame XP cannot replicate drivers from network printers (printers installed on network print servers) because MetaFrame XP does not have guaranteed access to the driver files.

If driver replication fails because of communication errors, the console displays an error message and records the error in the server Event Log for each server where the operation failed.

## Mapping Printer Drivers

Mapping of printer drivers refers to identifying printer drivers for the same printer that have different names on different Windows platforms. You need to use mapping if drivers you install on MetaFrame XP servers have different names than the drivers used by Windows 9x computers for their client printers.

Printer mappings are listed in a Citrix file, WTSPRNT.INF. Select **Drivers** in Citrix Management Console and choose **Mapping** from the **Actions** menu to manage printer driver mapping for a server farm.

In the **Driver Mapping** dialog box, you choose a server platform (because drivers differ on Terminal Server and Windows 2000 servers) and add the names of client printer drivers that correspond to the drivers you install on MetaFrame XP servers in the farm.

---

**Note** When you designate a printer driver to be incompatible for client printers in the farm (see “Managing Drivers for Client Printers” on page 219), you cannot create a printer driver mapping with the same driver.

---

## Managing Drivers for Client Printers

Some printer drivers can cause server problems when users print to client printers in the server farm. Because printing with a badly behaved driver to a client printer can crash a server, you might need to prevent autocreation of client printers that use certain printer drivers.

If a bad driver is replicated throughout a server farm, it is difficult and time consuming to remove it from every server to prevent its use with client printers. However, you can accomplish the same result with Citrix Management Console. Use the printer driver compatibility feature to designate drivers that you want to allow or prohibit for use with client printers.

The driver compatibility feature allows or prevents drivers you select from being used with client printers, but does not affect the use of drivers for printing to network printers. This is because drivers usually cause problems only with printing to client printers.

### Maintaining Driver Compatibility Lists

MetaFrame XP has a driver compatibility list for each server platform (Terminal Server and Windows 2000). To add or remove drivers, or edit the driver names in the compatibility list, select Drivers in the console tree and choose **Compatibility** from the **Actions** menu or the console toolbar.

Use the **Driver Compatibility** dialog box to manage the printer driver compatibility list for each server platform. You can list the printer drivers you allow or the drivers you do not allow to be used in the farm. To add drivers to the list, choose from the menu of all drivers that are installed on servers in the farm.

MetaFrame XP normally sets up (autocreates) client printers for all users who have them installed on their client devices. When users log on, MetaFrame XP checks the client printer driver compatibility list before it sets up the client printers. If a printer driver is on the list of drivers that are not allowed, MetaFrame XP does not set up the printer. When the compatibility list prevents setup of a client printer, MetaFrame XP sends messages to client users and writes a message in the server's event log.

## Autocreation of Client Printers for DOS and WinCE

MetaFrame XP provides autocreation of client printers (printers that are locally connected to client devices) for DOS and WinCE Clients. Autocreation makes these printers available for the client user for printing from the applications they run in ICA sessions.

Autocreated client printers appear in the form *clientname#LPTx*. The machine name of the client device replaces *clientname* and the printer port number replaces *x*.

Choose **Client Printers** from the **Printers** tab in Citrix Management Console to monitor and configure printer autocreation for DOS and WinCE Clients.

MetaFrame XP can make the client printers available if you set up autocreation for these ICA Clients from the console. MetaFrame 1.8 can enable autocreation of client printers only if users run the Client Printer utility in an ICA session on the client computer.

MetaFrame XP servers send data to the client device to make the client printer available in ICA sessions. You can view the status of DOS and WinCE Client printers in the **Client Printers** dialog box from the console. In the dialog box, the word <downloaded> appears in the list when information for client printer setup has been sent from the server to the client device.

Use the **Client Printers** dialog box to add, remove, reset, edit, and delete the configuration for DOS and WinCE client printers.

These client printers are available to the individual client users only. A client printer appears in applications running on the server only during the client user's ICA session.

## Limiting Printing Bandwidth in ICA Sessions

When users access MetaFrame XP servers through slower networks or dial-up connections, data sent during printing can affect video updates and application performance. To achieve the best performance for some ICA Client users, you can limit the bandwidth used by print data streams in ICA sessions.

By limiting the data transmission rate for printing, you make more bandwidth available in the ICA data stream for transmission of video, keystrokes, and mouse data. More available bandwidth can help prevent degradation of the user experience during printing.

Use Citrix Management Console to limit printing bandwidth in the server farm. You can set limits on individual servers and copy the bandwidth setting from one server to one or more other servers.

You can monitor the current bandwidth setting when you select the Printer Management node or the Servers node in the console tree. For more information on views for bandwidth management, see “Using the Printer Management Node” on page 212 and “Bandwidth Tab” on page 213.

## ICA Client Settings for Printer Access

Settings that affect the autocreation of client printers appear in Citrix Connection Configuration; for more information, see the online help in that program. An overview of these settings is included here. For specific information on ICA Client capabilities and settings, refer to the *Citrix ICA Client Administrator's Guide* for each ICA Client platform.

If the “Connect Client Printers at Logon” option is selected in the connection or user profile, client printers are automatically created when users log on to ICA sessions. MetaFrame XP deletes the printers when users log off if the printers do not contain unfinished print jobs. If print jobs are present, MetaFrame XP retains the printer and its associated jobs.

If you do not want autocreated printers deleted when users log off, view the **Properties** dialog box for the client printer from the server's Printers folder in an ICA session.

The **Properties** dialog box displays a Comment field that contains the text Auto Created Client Printer for automatically created client printers. If you modify or delete this description, MetaFrame XP does not delete the printer when a user logs off from the server. Subsequent logons by the same user employ the printer already defined and do not modify it.

If users change their Windows printer settings, the settings are not automatically maintained in this case. You can preserve printers to maintain custom print settings.

If a user's connection profiles do not specify **Connect Client Printers at Logon**, the user can connect to a client printer through Windows printer setup. MetaFrame XP does not automatically delete printers that are set up this way when users log off.



# MetaFrame XP Commands



This appendix describes MetaFrame XP commands. These commands must be run from the command prompt on a MetaFrame XP server. They provide additional methods for maintaining and configuring MetaFrame XP servers and server farms.

| Command              | Description                                                                      |
|----------------------|----------------------------------------------------------------------------------|
| <b>altaddr</b>       | Specify server alternate IP address                                              |
| <b>app</b>           | Run application execution shell                                                  |
| <b>auditlog</b>      | Generate server logon/logoff reports                                             |
| <b>change client</b> | Change ICA Client device mapping                                                 |
| <b>chfarm</b>        | Change the server farm membership of the server                                  |
| <b>clicense</b>      | Maintain Citrix licenses                                                         |
| <b>cltprint</b>      | Set the number of ICA Client printer pipes                                       |
| <b>ctxxmiss</b>      | Change the XML service port number                                               |
| <b>dsmaint</b>       | Configure the IMA data store                                                     |
| <b>icaport</b>       | Configure TCP/IP port number                                                     |
| <b>query</b>         | View information about server farms, processes, servers, ICA sessions, and users |
| <b>twconfig</b>      | Configure ICA display settings                                                   |

## ALTADDR

Use **altaddr** to query and set the alternate (external) IP address for a MetaFrame XP server. The alternate address is returned to ICA Clients that request it and is used to access a MetaFrame XP server that is behind a firewall.

### Syntax

**altaddr** [/server:*servername*] [/set *alternateaddress* ] [/v]

**altaddr** [/server:*servername*] [/set *adapteraddress alternateaddress*] [/v]

**altaddr** [/server:*servername*] [/delete] [/v]

**altaddr** [/server:*servername*] [/delete *adapteraddress*] [/v]

**altaddr** [/?]

### Parameters

#### *servername*

The name of a MetaFrame XP server.

#### *alternateaddress*

The alternate IP address for a MetaFrame XP server.

#### *adapteraddress*

The local IP address to which an alternate address is assigned.

### Options

#### **/server:*servername***

Specifies the Citrix server on which to set an alternate address. Defaults to the current Citrix server.

#### **/set**

Sets alternate TCP/IP addresses. If an *adapteraddress* is specified, *alternateaddress* is assigned only to the network adapter with that IP address.

#### **/delete**

Deletes the default alternate address on the specified server. If an adapter address is specified, the alternate address for that adapter is deleted.

#### **/v (verbose)**

Displays information about the actions being performed.

#### **/?**

Displays the syntax for the utility and information about these options.

## Remarks

The MetaFrame server subsystem reads the **altaddr** settings for server external IP addresses at startup only. If you use **altaddr** to change the IP address setting, you must restart the IMA service for the new setting to take effect. However, if you restart the IMA service when the MetaFrame server has active ICA sessions, you will disconnect the ICA sessions.

If **altaddr** is run without any parameters, it will display the information for alternate addresses configured on the current server.

## Examples

Set the server's alternate address to 1.1.1.1:

```
altaddr /set 1.1.1.1
```

Set the server's alternate address to 1.1.1.1 on the network interface card whose adapter address is 2.2.2.2:

```
altaddr /set 2.2.2.2 1.1.1.1
```

## Security Restrictions

None.

# APP

**App** is a script interpreter for secure application execution. Use **App** to read execution scripts that copy standardized .Ini files to user directories before starting an application, or to perform application-related cleanup after an application has terminated. The script commands are described below.

## Syntax

**app** *scriptfilename*

## Parameters

### **directory**

A directory or directory path.

### **executablepath**

The fully qualified name of the executable to be run.

### **filespec**

Specifies the files to copy and can include wildcards (\*,?).

### **scriptfilename**

The name of a script file containing app commands (see script commands below).

### **sourcedirectory**

The directory and path from which files are to be copied.

### **targetdirectory**

The directory and path to which files are to be copied.

## Remarks

If no *scriptfilename* is specified, **app** displays an error message.

The Application Execution Shell reads commands from the script file and processes them in sequential order. The script file must reside in the %SystemRoot%\Scripts directory.

## Script Commands

The script commands are:

### **copy** *sourcedirectory\filespec targetdirectory*

Copies files from *sourcedirectory* to *targetdirectory*. *Filespec* specifies the files to copy and can include wild cards (\*,?).

**delete *directory\filespec***

Deletes files owned by a user in the *directory* specified. *Filespec* specifies the files to delete and can include wild cards (\*,?). See the Examples section for more information.

**deleteall *directory\filespec***

Deletes all files in the *directory* specified.

**execute**

Executes the program specified by the path command using the working directory specified by the **workdir** command.

**path *executablepath***

*Executablepath* is the fully qualified name of the executable to be run.

**workdir *directory***

Sets the default working directory to the path specified by *directory*.

## Examples

The following script file runs the program Sol.exe:

```
PATH C:\Wtsrv\System32\Sol.exe
WORKDIR C:\Temp
EXECUTE
```

The following script file runs the program notepad.exe. When the program terminates, the script deletes files in the Myapps\Data directory created for the user who launched the application:

```
PATH C:\Myapps\notepad.exe
WORKDIR C:\Myapps\Data
EXECUTE
DELETE C:\Myapps\Data\*.*
```

The following script file copies all the Wri files from the directory C:\Write\Files, executes Write.exe in directory C:\Temp.wri, and then removes all files from that directory when the program terminates:

```
PATH C:\Wtsrv\System32\Write.exe
WORKDIR C:\Temp.wri
COPY C:\Write\Files\*.* C:\Temp.wri
EXECUTE
DELETEALL C:\Temp.wri\*.*
```

The following example demonstrates using the script file to implement a front-end registration utility before executing the application Coolapp.exe. You can use this method to run several applications in succession:

```
PATH C:\Regutil\Reg.exe
WORKDIR C:\Regutil
EXECUTE
PATH C:\Coolstuff\Coolapp.exe
WORKDIR C:\Temp
EXECUTE
DELETEALL C:\Temp
```

## Security Restrictions

None.

# AUDITLOG

**Auditlog** generates reports of logon/logoff activity for a MetaFrame server based on the Windows NT Server security event log. To use **auditlog**, you must first enable logon/logoff accounting. You can direct the auditlog output to a file.

## Syntax

**auditlog** [*username* | *session*] [/eventlog:*filename*] [/before:*mm/dd/yy*]  
[/after:*mm/dd/yy*] [/write:*filename*] | [/detail | /time] [/all]

**auditlog** [*username* | *session*] [/eventlog:*filename*] [/before:*mm/dd/yy*]  
[/after:*mm/dd/yy*] [/write:*filename*] | [/detail] | [/fail] | [/all]

**auditlog** [/clear:*filename*]

**auditlog** [/?]

## Parameters

### *filename*

The name of the eventlog output file.

### *session*

Specifies the session ID for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular session.

### *mm/dd/yy*

The month, day, and year (in two-digit format) to limit logging.

### *username*

Specifies a username for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular user.

## Options

### /eventlog:*filename*

Specifies the name of a backup event log to use as input to **auditlog**. You can back up the current log from the Event Log Viewer by using **auditlog /clear:*filename***.

### /before:*mm/dd/yy*

Reports on logon/logoff activity only before *mm/dd/yy*.

### /after:*mm/dd/yy*

Reports on logon/logoff activity only after *mm/dd/yy*.

### /write:*filename*

Specifies the name of an output file. Creates a comma-delimited file that can be imported into an application, such as a spreadsheet, to produce custom

reports or statistics. It generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on.

If *filename* exists, the data is appended to the file.

**/time**

Generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on. Useful for gathering usage statistics by user.

**/fail**

Generates a report of all failed logon attempts.

**/all**

Generates a report of all logon/logoff activity.

**/detail**

Generates a detailed report of logon/logoff activity.

**/clear:*filename***

Saves the current event log in *filename* and clears the event log. This command does not work if *filename* already exists.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Remarks

**Auditlog** provides logs you can use to verify system security and correct usage. The information can be extracted as reports or as comma-delimited files that can be used as input to other programs.

You must enable logon/logoff accounting on the local server to collect the information used by **auditlog**. To enable logon/logoff accounting, log on as a local administrator and enable logon/logoff accounting with User Manager for Domains (Windows NT) or with Audit Policy in Microsoft Management Console (Windows 2000).

## Security Restrictions

None.

# CHANGE CLIENT

**Change client** changes the current disk drive, COM port and LPT port mapping settings for an ICA Client device.

## Syntax

**change client** [/view | /flush | /current]

**change client** [{/default | [/default\_drives] | [/default\_printers]} [/ascending]]  
[/noremap] [/persistent] [/force\_prt\_todef]

**change client** [/delete *host\_device*] [*host\_device client\_device*] [/?]

## Parameters

### *host\_device*

The name of a device on the host server to be mapped to a client device.

### *client\_device*

The name of a device on the client to be mapped to *host\_device*.

## Options

### **/view**

Displays a list of all available client devices.

### **/flush**

Flushes the client drive mapping cache. This action forces the server and the client to resynchronize all disk data. See Remarks for more information.

### **/current**

Displays the current ICA Client device mappings.

### **/default**

Resets host drive and printer mappings to defaults.

### **/default\_drives**

Resets host drive mappings to defaults.

### **/default\_printers**

Resets host printer mappings to defaults.

### **/ascending**

Uses ascending, instead of descending, search order for available drives and printers to map. This option can be used only with **/default**, **/default\_drives**, or **/default\_printer**.

**/noremap**

If **/noremap** is specified, client drives that conflict with MetaFrame drives are not mapped.

**/persistent**

Saves the current client drive mappings in the client device user's profile.

**/force\_prt\_todef**

Sets the default printer for the client session to the default printer on the client's Windows desktop.

**/delete *host\_device***

Deletes the client device mapping to *host\_device*.

**/? (help)**

Displays the syntax for the utility and information about the utility's options.

## Remarks

Typing **change client** with no parameters displays the current ICA Client device mappings; it is equivalent to typing **change client /current**.

Use **change client *host\_device client\_device*** to create a client drive mapping. This maps the *client\_device* drive letter to the letter specified by *host\_device*; for example, **change client v: c:** maps client drive C to drive V on the MetaFrame server.

The **/view** option displays the share name, the share type, and a comment describing the mapped device. Sample output for **change client /view** follows:

```
C:>change client /view
```

```
Available Shares on client connection ICA-tcp#7
```

| Sharename      | Type    | Comment          |
|----------------|---------|------------------|
| \\Client\A:    | Disk    | Floppy           |
| \\Client\C:    | Disk    | FixedDrive       |
| \\Client\D:    | Disk    | CdRom            |
| \\Client\LPT1: | Printer | Parallel Printer |
| \\Client\COM1: | Printer | Serial Printer   |

The **/flush** option flushes the client drive cache. This cache is used to speed up access to client disk drives by retaining a local copy of the data on the MetaFrame server. The timeout for hard drive cache entries is ten minutes and the timeout for diskette data is five seconds. If the client device is using a multitasking operating system and files are created or modified, the MetaFrame server does not know about the changes.

Flushing the cache forces the data on the MetaFrame server to be synchronized with the client data. The cache timeout for diskettes is set to five seconds because diskette data is usually more volatile; that is, the diskette can be removed and another diskette inserted.

The **/default** option maps the drives and printers on the client device to mapped drives and printers on the MetaFrame server. The A and B drives are always mapped to A and B on the MetaFrame server. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the MetaFrame server. If the corresponding drive letter is in use on the MetaFrame server, the default action is to map the drive to the highest unused drive letter. For example, if both machines have C and D drives, the client C and D drives are mapped to V and U respectively. These default mappings can be modified by the **/ascending** and **/noremap** options.

The **/default\_printers** option resets printer mappings to defaults. **/default\_printers** attempts a one-to-one mapping of all client printers; for example, the client's LPT1 and LPT2 ports are mapped to the server's LPT1 and LPT2 ports. If the **/ascending** option is specified, the mapping is done in ascending order.

The **/default\_drives** option resets host drive mappings to defaults. **/default\_drives** attempts a one-to-one mapping of all client drives; for example, client A and B drives are mapped to server drives A and B. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the MetaFrame server. If the corresponding drive letter is in use on the MetaFrame server, the default action is to map the drive to the highest unused drive letter. For example, if both machines have C and D drives, the client C and D drives are mapped to V and U respectively. If the **/ascending** option is specified, the mapping is done in ascending order.

The **/ascending** option causes the mapping to occur in ascending drive letter order. For example, if the first two available drive letters on the MetaFrame server are I and J, the C and D drives in the preceding example are mapped to I and J respectively.

The **/noremap** option causes the mapping to skip drive letters occupied on the MetaFrame server. For example, if the MetaFrame server has a C drive but no D drive, the client's C drive is mapped to D on the server, but the client's D drive is not mapped.

The **/persistent** option causes the current device mappings to be saved in the user's profile. Drive conflicts can occur if the **/persistent** option is in use, and the user logs on from a client device that has a different disk drive configuration, or logs on to a MetaFrame server that has a different disk drive configuration.

The **/force\_prt\_todef** option sets the default printer for the ICA session to the default printer on the client's Windows desktop.

## Security Restrictions

None.

# CHFARM

**Chfarm** is used to change the farm membership of a MetaFrame XP server.

## Syntax

**Chfarm**

## Remarks

You can use **chfarm** when you want to move a MetaFrame XP server from its current server farm. You can move the server to an existing IMA-based server farm, or create a new server farm at the same time that you move the server.

The **chfarm** utility is available on the MetaFrame XP CD-ROM. This utility must be run from the CD-ROM, as it accesses IMA installation information.

When you run **chfarm**, it stops the IMA service on the server. The data store configuration part of the MetaFrame XP Setup wizard appears. On the first page, you can select an option to join an existing IMA-based server farm or create a new server farm and then click **Next**.

The wizard continues and you specify an existing data store (to join an existing server farm) or set up a new data store (if you create a new server farm). For information on data store setup and server farm configuration, see “Data Store Configuration” on page 74.

After the farm membership is changed or a new farm is created, reboot the MetaFrame XP server.

When you create a new farm using **chfarm**, no Citrix administrator accounts are set up in the Citrix Management Console. To set up a Citrix administrator account for the new farm, you must use Citrix Management Console to log on to the server farm as a local administrator of the MetaFrame XP server.

Do not remove a server that hosts a server farm’s data store from the server farm. Doing so render the farm unstable.

# CLICENSE

You can use **clicense** to add, remove, query, and maintain license information for MetaFrame XP servers within a Citrix server farm. For more information about Citrix licensing, see “Licensing MetaFrame XP” on page 119.

## Syntax

**clicense** [**add** *serial\_number*]  
**clicense** [**remove** *license\_string*]  
**clicense** [**force\_remove** *license\_string*]  
**clicense** [**activate** *license\_string* *activation\_code*]  
**clicense** [**assign** *license\_set\_id* *server\_name* *number\_to\_assign*]  
**clicense** [**strings**]  
**clicense** [**products**]  
**clicense** [**connections**]  
**clicense** [**servers\_using** *license\_set\_id*]  
**clicense** [**in\_use\_by** *server\_name*]  
**clicense** [**in\_set** *license\_set\_id*]  
**clicense** [**sets\_in** *license\_string*]  
**clicense** [**assigned\_to** *server\_name*]  
**clicense** [**servers\_assigned** *license\_set\_id*]  
**clicense** [**available\_for\_assignment** *license\_set\_id*]  
**clicense** [**read\_db** [*file\_name*]]  
**clicense** [**refresh**]  
**clicense** [**help** *option*]

## Parameters

### *activation\_code*

The license activation code. This is obtained from the Citrix Product Activation System (<http://www.citrix.com/activate>).

### *file\_name*

The name of the licensing data base file.

### *option*

The name of a **clicense** option.

***license\_string***

The license number. A license number consists of seven groups of five characters each: *xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*. Each license number has an associated serial number which consists of five groups of five characters each: *xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*.

***license\_set\_id***

The license set ID number.

***number\_to\_assign***

The number of license counts to assign to a specified server.

***serial\_number***

The license serial number. This number can be found on the software packaging. See *license\_string*.

***server\_name***

The name or IP address of a Citrix server. Use a period (.) to specify the local server.

## Options

***add serial\_number***

Use to add serial numbers to the license store. This returns the added license string.

***remove license\_string***

Use to remove a license string from the license store, provided it does not have active assignments.

***force\_remove license\_string***

Use to force the removal of a license string from the license store. Active assignments are dropped.

***activate license\_string activation\_code***

Activates a license string in the license store.

***assign license\_set\_id server\_name number\_to\_assign***

Assigns licenses from the specified license set to the specified MetaFrame XP server. To specify the local server, enter a period (.).

***strings***

Retrieves a list of all installed license strings.

***products***

Retrieves a list of all the installed product licenses.

***connections***

Retrieves a list of all installed connection licenses.

**servers\_using *license\_set\_id***

Retrieves a list of all servers that are using a license from the specified license set.

**in\_use\_by *server\_name***

Queries and returns the license sets currently in use by the specified server.

**in\_set *license\_set\_id***

Returns a list of all strings that contribute licenses to a set.

**sets\_in *license\_string***

Returns a list of all license sets to which a string contributes.

**assigned\_to *server\_name***

Returns the license sets that are assigned to the specified server.

**servers\_assigned *license\_set\_id***

Returns the servers to which the specified license set is assigned.

**available\_for\_assignment *license\_set\_id***

Returns the number of activated licenses in a license set that have not yet and can be assigned.

**read\_db [*file\_name*]**

Reads license database configuration files into the license store. If a file name is specified, only files whose names begin with the specified file name are read into the license store.

**refresh**

Refreshes all licensing data.

**help *option***

Provides additional information about the specified option.

## Remarks

Citrix Management Console provides a graphical user interface with the same functionality as the **clicense** command for managing Citrix licenses.

## Security Restrictions

The commands **add**, **remove**, **force\_remove**, **activate**, **assign**, and **read\_db** can be executed only by a member of the Citrix Administrators group on the local machine.

# CLTPRINT

Use **cltprint** to set the number of printer pipes for the client print spooler.

## Syntax

**cltprint** [/q] [/pipes:*nn*] [/?]

## Options

**/q**

Displays the current number of printer pipes.

**/pipes:*nn***

Sets the specified number of printer pipes. This number must be from 10 to 63.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Remarks

Printer pipes are used to send data from applications to client print spoolers. The number of pipes specifies the number of print jobs that can be sent to the spooler simultaneously.

The default number of printer pipes is ten.

The Spooler service must be stopped and restarted after changing the number of pipes. Print jobs already spooled continue printing.

Print jobs sent to the spooler trigger an error message while the service is stopped. Make sure no users start printing during the time the spooler service is stopped.

## Security Restrictions

None.

# CTXMLSS

Use **ctxmlss** to change the Citrix XML Service port number.

## Syntax

**ctxmlss** [/r*nnn*] [/u] [/k*nnn*] [/?]

## Options

/r*nnn*

Changes the port number for the Citrix XML Service to *nnn*.

/u

Unloads Citrix XML Service from memory.

/k*nnn*

Keeps the connection alive for *nnn* seconds. The default is nine seconds.

/?

Displays the syntax for the utility and information about the utility's options.

## Remarks

For more information, see “Changing the Citrix XML Service Port” on page 86.

## Security Restrictions

None.

# DSMAINT

Use **dsmaint** to configure the IMA data store for a Citrix server farm.

## Syntax

**dsmaint config** [/user:username] [/pwd:password] [/dsn:filename]

**dsmaint backup** *destination\_path*

**dsmaint failover** *indirect\_server*

**dsmaint compactdb** [/ds] [/lhc]

**dsmaint migrate** [{ /srcdsn:*dsn1* /srcuser:*user1* /srcpwd:*pwd1* }] [{ /dstdsn:*dsn2* /dstuser:*user2* /dstpwd:*pwd2* }]

**dsmaint publishsqlids** {/user:*username* /pwd:*password*}

**dsmaint /recover**

**dsmaint** [/?]

## Parameters

*destination\_path*

Path to the backup data store.

*dsn1*

The name of the source data store.

*dsn2*

The name of the destination data store

*filename*

Name of the data store.

*indirect\_server*

Name of the new indirect server for IMA data store operations.

*password*

Password to connect to the data store.

*pwd1*

The source data store password.

*pwd2*

The destination data store password.

*user1*

The source data store user login.

***user2***

The destination data store user login.

***username***

Name of the user to use when connecting to the data store.

## Options

**config**

Changes configuration parameters used by IMA to connect to the data store.

***/user:username***

Username to connect to a data store.

***/pwd:password***

Password to connect to a data store.

***/dsn:filename***

Filename of an IMA data store.

**backup**

Creates a backup copy of the Access database that is the farm's data store. Run this command on the server that hosts the data store. Requires a path or sharepoint to which the database file will be copied. The **backup** command cannot be used to create backups for Oracle or SQL data stores.

**failover**

Switches the server to use a new direct server for IMA data store operations.

**compactdb**

Compacts the Access database file.

***/ds***

Specifies the database is to be compacted immediately. If the IMA service is running, this can be executed from the direct server or an indirect server. If the IMA service is not running, this can be executed only on the direct server.

***/lhc***

Specifies the local host cache is to be compacted immediately.

**migrate**

Migrate data from one data store to another. Use this command to move a data store to another server, rename a data store in the event of a server name change, or migrate the data store to an Oracle or SQL server.

***/srcdsn:dsn1***

The name of the data store from which to migrate data.

***/srcuser:user1***

The username to use to connect to the data store from which the data is migrating.

**/srcpwd:***pwd1*

The password to use to connect to the data store from which the data is migrating.

**/dstdsn:***dsn2*

The name of the data store to migrate the data to.

**/dstuser:***user2*

The username to use to connect to the data store the data is migrating to.

**/dstpwd:***pwd2*

The password to use to connect to the data store the data is migrating to.

### **publishsqlids**

Publishes a MetaFrame data store to allow replication.

### **recover**

Restores an Access data store to its last known good state. This must be executed on the direct server while the IMA service is not running.

**/?**

Displays the syntax for the utility and information about the utility's options.

## **Remarks**

### **compactdb**

During database compaction, the database is temporarily unavailable for both reading and writing. The compaction time can vary from a few seconds to a few minutes, depending on the size of the database and the usage.

### **config**

For Access databases, this command resets the password used to protect the database, setting the matched security context to allow IMA access to this database.

You must stop the IMA service before using **config** with the **/pwd** option.

---

---

**Warning** You must specify a **/dsn** for **dsmaint config** or you will change the security context for access to the SQL or Oracle database.

---

---

### **migrate**

Databases can be migrated from Access to SQL or Oracle and between SQL and Oracle.

---

**Important** By default, the Access database does not have a user name or password. When migrating a database from Access, leave the **/srcuser:** and **/srcpwd:** parameters blank.

---

The connection to a local Access database is based on the host server's name. If the name of the server changes, use **migrate** to change the name of the database.

**publishsqllds**

Execute **publishsqllds** only from the server that created the farm. The publication will be named **MFXPDS**.

**Security Restrictions**

The **dsmaint config** and **dsmaint migrate** commands can be executed only by a user with the correct username and password for the database.

# ICAPORT

Use **icaport** to query or change the TCP/IP port number used by the ICA protocol on the MetaFrame XP server.

## Syntax

**icaport** {/query | /port:*nnn* | /reset} [/?]

## Options

### /query

Queries the current setting.

### /port:*nnn*

Changes the TCP/IP port number to *nnn*.

### /reset

Resets the TCP/IP port number to 1494, which is the default.

### /?

Displays the syntax for the utility and information about the utility's options.

## Remarks

The default port number is 1494. The port number must be in the range of 0–65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the MetaFrame XP server, you must also change it on every ICA Client that will connect to that server. For instructions about changing the port number on ICA Clients, see the *Citrix ICA Client Administrator's Guides* for the ICA Clients that you plan to deploy.

## Examples

To set the TCP/IP port number to 5000:

```
icaport /port:5000
```

To reset the port number to 1494:

```
icaport /reset
```

## Security Restrictions

Only Citrix administrators can run **icaport**.

# QUERY

Use **query** to display information about server farms, processes, servers, sessions, terminal servers, and users within the network.

## Query Farm

### Syntax

```
query farm      [server [/addr | /app | /app appname | /load]]
query farm      [/tcp | [ /ipx | [ /netbios | [ /continue ]
query farm      [ /app | /app appname | /disc | /load | /process]
query farm      [/?]
```

### Parameters

#### *appname*

The name of a published application.

#### *server*

The name of a server within the farm.

### Options

#### **farm**

Displays information about servers within an IMA based server farm.

#### *server* **/addr**

Displays address data for the specified server.

#### **/app**

Displays application names and server load information for all servers within the farm, or for a specific server.

#### **/app** *appname*

Displays information for the specified application and server load information for all servers within the farm, or for a specific server.

#### **/continue**

Don't pause after each page of output.

#### **/disc**

Displays disconnected session data for the farm.

#### **/ipx**

Displays IPX data for the farm.

#### **/load**

Displays server load information for all servers within the farm, or for a specific server.

**/netbios**

Displays NetBIOS data for the farm.

**/process**

Displays active processes for the farm.

**/tcp**

Displays TCP/IP data for the farm.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Remarks

**Query farm** returns information for IMA-based servers within a MetaFrame XP server farm.

## Security Restrictions

None.

# Query Process

## Syntax

**query process**     [ \* | *processid* | *username* | *sessionname* | **/id:nn**  
                         | *programname* ][ **/server:servername** ] [ **/system** ]

**query process**     [/?]

## Parameters

**process**

Displays information about processes running on the current server.

**process \***

Displays all visible processes on the current server.

**process *processid***

Displays processes for the specified *processid*.

**process *username***

Displays processes belonging to the specified user.

**process *sessionname***

Displays processes running under the specified session name.

**process /id:nn**

Displays information about processes running on the current server by the specified ID number.

**process** *programname*

Displays process information associated with the specified program name.

**process** */server:servername*

Displays information about processes running on the specified server. If no server is specified, the information returned is for the current server.

**process** */system*

Displays information about system processes running on the current server.

*/?*

Displays the syntax for the utility and information about the utility's options.

**Options**

*\**

Displays all visible processes.

***processid***

The three- or four-digit ID number of a process running within the farm.

***programname***

The name of a program within a farm.

***servername***

The name of a server within the farm.

***sessionname***

The name of a session, such as **ica-tcp#7**.

***username***

The name of a user connected to the farm.

**Security Restrictions**

None.

**Query Server**

**Syntax**

|              |                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------|
| query server | [ <i>server</i> [/ping [/count: <i>n</i> ] [/size: <i>n</i> ]   /stats   /reset   /load<br>  /addr]] |
| query server | [/tcp] [/ipx] [/netbios] [/tcpserver: <i>x</i> ] [/ipxserver: <i>x</i> ]                             |
| query server | [/netbiosserver: <i>x</i> ]                                                                          |

**query server**      [/license | /app | /gateway | /serial | /disc | /serverfarm | /video]  
**query server**      [/continue] [/ignore] [/?]

## Parameters

### **server** *server*

Displays transport information for the specified server.

#### **/addr**

Displays address information for the specified server.

#### **/app**

Displays application names and server load for the specified server.

#### **/continue**

Don't pause after each page of output.

#### **/count:***n*

Number of times to ping the specified server.

#### **/disc**

Displays disconnected session data on the current server.

#### **/gateway**

Displays configured gateway addresses for the current server.

#### **/ignore**

Ignore warning message about interoperability mode.

#### **/ipx**

Displays IPX data for the current server.

#### **/ipxserver:***x*

Defines the IPX default server address.

#### **/license**

Displays user licenses for the current server.

#### **/load**

Displays local data on the specified server.

#### **/netbios**

Displays NetBIOS data for the current server.

#### **/netbiosserver:***x*

Defines the NetBIOS default server address.

#### **/ping**

Pings selected server. The default is five times.

#### **/reset**

Resets the browser statistics on the specified server.

#### **/serial**

Displays license serial numbers for the current server.

**/serverfarm**

Displays server farm names and server load.

**/size:*n***

Size of ping buffers. The default is 256 bytes.

**/stats**

Displays the browser statistics on the specified server.

**/tcp**

Displays the TCP/IP data for the current server.

**/tcpserver:*x***

Defines the TCP/IP default server address.

**/video**

Displays VideoFrame data for the current server.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Options

***n***

The number of times to ping a server (the default is five times), or the size of ping buffers (the default is 256 bytes).

***server***

The name of a server within the farm.

***x***

The default TCP, IPX, or NetBIOS server address.

## Remarks

**Query server** displays data about the Citrix servers present on a network within a server farm running in interoperability mode. It shows all ICA Browser-based and IMA-based servers within the farm, even if the server is not currently connected to the farm.

## Security Restrictions

None.

## Query Session

### Syntax

**query session** [*sessionname* | *username* | *sessionid*]

**query session**     [/server:*servername*] [/mode] [/flow] [/connect] [/counter]  
**query session**     [/?]

## Parameters

**session** *sessionname*

Identifies the specified session.

**session** *username*

Identifies the session associated with the user name.

**session** *sessionid*

Identifies the session associated with the session ID number.

**session** /server:*servername*

Identifies the sessions on the specified server.

**session** /mode

Displays the current line settings.

**session** /flow

Displays the current flow control settings.

**session** /connect

Displays the current connection settings.

**session** /counter

Displays the current Terminal Services counter information.

/?

Displays the syntax for the utility and information about the utility's options.

## Options

*servername*

The name of a server within the farm.

*sessionname*

The name of a session, such as **ica-tcp#7**.

*sessionid*

The two-digit ID number of a session.

*username*

The name of a user connected to the farm.

## Security Restrictions

None.

## Query Termserver

### Syntax

**query termserver** [*servername*] [/domain:*domain*] [/address] [/continue]

**query termserver** [/?]

### Parameters

**termserver** *servername*

Identifies a Terminal Server.

**/address**

Displays network and node addresses.

**/continue**

Don't pause after each page of output.

**/domain:***domain*

Displays information for the specified domain. Defaults to the current domain if no domain is specified.

**/?**

Displays the syntax for the utility and information about the utility's options.

### Options

*servername*

The name of a server within the farm.

*domain*

The name of a domain to query.

### Remarks

If no parameters are specified, **query termserver** lists all terminal servers within the current domain.

### Security Restrictions

None.

## Query User

### Syntax

**query user** [ *username* | *sessionname* | *sessionid* ] [ **/server:***servername* ]

**query user [/?]**

## Parameters

**user** *username*

Displays connection information for the specified user name.

**user** *sessionname*

Displays connection information for the specified session name.

**user** *sessionid*

Displays connection information for the specified session ID.

**user** **/server:***servername*

Defines the server to be queried. The current server is queried by default.

**/continue**

Do not pause after each page of output.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Options

*servername*

The name of a server within the farm.

*sessionname*

The name of a session, such as **ica-tcp#7**.

*sessionid*

The two-digit ID number of a session.

*username*

The name of a user connected to the farm.

## Remarks

If no parameters are specified, **query user** displays all user sessions on the current server.

## Security Restrictions

None.

## TWCONFIG

Use **twconfig** to configure ICA display settings that affect graphics performance for ICA Clients.

### Syntax

**twconfig** [/query | /q]

**twconfig** [/inherit:on|off]

**twconfig** [/discard:on|off]

**twconfig** [/supercache:on | off]

**twconfig** [/maxmem:*nnn*]

**twconfig** [/degrade:res|color]

**twconfig** [/notify:on|off]

**twconfig** /?

### Options

**/query, /q**

Query current settings.

**/inherit:on|off**

Set to **on** to use the ICA display properties defined for the farm. Set to **off** to use the settings specified for this server. By default, this is set to **on**.

**/discard:on|off**

Discard redundant graphics operations.

**/supercache:on|off**

Use alternate bitmap caching method.

**/maxmem:*nnn***

Maximum memory (in bytes) to use for each session's graphics (153,600 minimum, 7,680,000 maximum).

**/degrade:res|color**

When the **maxmem** limit is reached, degrade resolution first or degrade color depth first.

**/notify:on|off**

If **on**, users are alerted when **maxmem** limit is reached.

**/?**

Displays the syntax for the utility and information about the utility's options.

## Remarks

A MetaFrame XP server can be set to inherit its ICA display settings from the server farm ICA display settings. Use **/query** to display the current **inherit** settings. If **/inherit** is on, the settings displayed with **/query** are the server farm settings. When **/inherit** is off, the settings shown are for the current server only.

**Twconfig** can only be used to change the settings on this server, for this server. To change the settings for another server or for the server farm, use Citrix Management Console.

Within the **maxmem** limit, various combinations of session size and color depth are available. The session size and color depth values are determined using the following formula:  $height \times width \times depth \leq maxmem$ , where the *height* and *width* are measured in pixels and *depth* is the color depth in bytes according to the following table:

| Color depth         | Bytes |
|---------------------|-------|
| True Color (24-bit) | 3     |
| High Color (16-bit) | 2     |
| 256 Colors          | 1     |
| 16 Colors           | .5    |

The following is a list of the maximum session sizes with a 4:3 aspect ratio for each color depth at the default **maxmem** value (height by width by color depth):

- 1600 by 1200 by 24-bit color
- 1920 by 1440 by 16-bit color
- 2752 by 2064 by 256 colors
- 3904 by 2928 by 16 colors

## Security Restrictions

None.



# Glossary



**account authority** The platform-specific source of information on user accounts used by a Citrix server; for example, a Windows NT domain, Active Directory domain, or NetWare Directory Services.

**activation code** An alphanumeric string displayed on the Citrix Activation System Web page after you enter a Citrix license number. To activate a license, select the license number in Citrix Management Console and enter the activation code.

**anonymous application** An application published exclusively for the use of anonymous users.

**anonymous session** An ICA session started by an anonymous user.

**anonymous user** An unidentified user granted minimal access to a Citrix server, or server farm, and its published applications.

**anonymous user account** A user account defined on a Citrix server for access by anonymous users.

**application name** A text string used to uniquely identify a published application within a farm. The application name is used by the Citrix server farm and ICA Clients to recognize individual applications that may have the same display name. The text string is automatically generated based on the display name entered when the application was initially published.

**Application Launching and Embedding (ALE)** A feature of Citrix servers and ICA Clients that enables full-function, Windows-based applications to be launched from or embedded into HTML pages without rewriting any application code.

**Application Publisher** The wizard you use to publish applications on Citrix server farms.

**application set** A user's view of the applications published on a server farm that the user is authorized to access.

**automatic client update** The Citrix server feature that enables you to install the latest versions of ICA Clients on your servers, then schedule the download and installation of that software to your users' client devices.

**browser election** The process ICA Browsers go through to choose (elect) a master browser from among the Citrix servers on a given network. Browser elections occur when a new Citrix server is started, when the current master browser does not respond, or when two master browsers are detected by another server or an ICA Client.

**business recovery** The ICA Client feature that enables users or administrators to specify multiple server addresses (such as a primary and hot backup) for the same published application name. This feature provides consistent connections to published applications in the event of a primary server failure.

**ciphersuite** An encryption/decryption algorithm. When establishing an SSL connection, the client and server determine a common set of supported ciphersuites and then use the most secure one to encrypt the communications. Ciphersuites have different advantages in terms of speed, encryption strength, exportability, etc.

**Citrix Management Console** Citrix's extensible, platform-independent tool for administering Citrix servers and management products.

**Citrix administrators** System administrators responsible for installing, configuring, and maintaining Citrix servers. In a UNIX environment, it is the user group assigned to these administrators, which has the default name `ctxadm`.

**Citrix server** Any MetaFrame, *WINFRAME*, or VideoFrame server on which you publish applications or videos.

**Citrix SSL Relay** A Windows NT service that runs on a MetaFrame server to support an SSL-secured connection between an NFuse-enabled Web server and the MetaFrame server.

**Citrix XML Service** A Windows NT service that provides an HTTP interface to the ICA Browser. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80.

**client COM port mapping** The feature that enables applications running on a Citrix server to access peripherals attached to COM ports on the client device.

**client device** Any hardware device capable of running one of the ICA Clients.

**client device mapping** The feature that enables remote applications running on the Citrix server to access storage and peripherals attached to the local client device. Client device mapping consists of several distinct features: client drive mapping, client printer mapping, and client COM port mapping.

**client drive mapping** The feature that enables applications running on the Citrix server to access physical and logical drives configured on the client device.

**client printer mapping** The feature that enables applications running on the Citrix server to send output to printers configured on the client device.

**client update database** The database Citrix servers use to automatically update ICA Clients. It contains copies of the clients themselves and configuration information about how to perform the updates.

- Connection Center** The Win32 ICA Client task bar utility that displays all ICA connections established from the user's client device.
- connection license** A license that enables ICA connections between a client device and a Citrix server farm. Connection license counts can be assigned to specific servers or pooled among all servers in the farm.
- custom ICA connection** A user-created shortcut to a published application or Citrix server.
- data collector** A MetaFrame XP server that stores dynamic data for one zone in a MetaFrame XP server farm.
- data store** An ODBC-compliant database used by a MetaFrame XP server farm. The data store centralizes configuration information about published applications, users, printers, and servers. Each IMA-based Citrix server farm has a single data store.
- disconnected session** An ICA session in which the ICA Client is no longer connected to the Citrix server, but the user's applications are still running. A user can reconnect to a disconnected session. If the user does not do so within a specified time-out period, the Citrix server automatically terminates the session.
- display name** A name you specify when you publish an application. The display name appears in the newer Program Neighborhood client and in Application folders in Citrix Management Console. The display name is also available for use by Web Portals generated with Citrix NFuse technology.
- dynamic store** A data store that contains frequently updated configuration data such as application load and license usage information. A server farm replicates dynamic store information across multiple servers.
- ICA** Independent Computing Architecture. The architecture that Citrix uses to separate an application's logic from its user interface. With ICA, only the keystrokes, mouse clicks, and screen updates pass between the client and server on the network, while 100% of the application's logic executes on the server.
- ICA asynchronous connections** Asynchronous connection types allow direct dial-in to a Citrix server without the overhead of RAS and TCP/IP.
- ICA Browser** See "master ICA Browser or master browser."
- ICA Client** Citrix software that enables users to connect to Citrix servers from a variety of client devices.
- ICA Client Creator** The Citrix server utility you use to create disks from which you can install ICA Clients and the ICA File Editor on a wide range of client devices.
- ICA Client Printer Configuration** The utility you use to create and connect to client printers for ICA DOS and WinCE Clients. You must run this utility in an ICA session from the client whose printer you want to configure.
- ICA Client Update Configuration** The utility you use to configure the client update database.

- ICA connection** 1. The logical port used by an ICA Client to connect to, and start a session on, a Citrix server. An ICA connection is associated with a network connection (such as TCP/IP, IPX, SPX, or NetBIOS) or a serial connection (modems or direct cables). 2. The active link established between an ICA Client and a Citrix server.
- ICA file** A text file (with the extension ica) containing information about a published application. ICA files are written in Windows .ini file format and organize published application information in a standard way that ICA Clients can interpret. When an ICA Client receives an ICA file, it initializes a session running the specified application on the Citrix server specified in the file.
- ICA Printer Management** The ability to manage all local and network printers accessed by a Citrix server farm. Printer management is available through the Citrix Management Console.
- ICA protocol** The protocol that ICA Clients use to format user input (keystrokes, mouse clicks, and so forth) and address it to Citrix servers for processing. Citrix servers use it to format application output (display, audio, and so forth) and return it to the client device.
- ICA session** A lasting connection between an ICA Client and a Citrix server, identified by a specific user ID and ICA connection. It consists of the status of the connection, the server resources allocated to the user for the duration of the session, and any applications executing during the session. An ICA session normally terminates when the ICA Client user logs off the Citrix server.
- Independent Management Architecture (IMA)** Citrix's server-to-server infrastructure that provides robust, secure, and scalable tools for managing any size server farm. Among other features, IMA enables centralized platform-independent management, an ODBC-compliant data store, and a suite of management products that plug in to the Citrix Management Console.
- interoperability** The MetaFrame XP ability to work in *mixed mode* with MetaFrame 1.8 servers in the same server farm. Not all MetaFrame XP features are available in mixed mode.
- key store** The directory on the MetaFrame server running the SSL relay that contains the server certificate. The default directory is %SystemRoot%\SSLRelay\keystore\certs.
- license count** The number of Citrix products or ICA connections that a Citrix license authorizes.
- license number** An alphanumeric string displayed by Citrix Management Console when you enter a license serial number. You enter the resulting license number on the Citrix Activation System Web page to receive an activation code for the license.
- license pooling** A feature of Citrix servers that enables you to combine license counts of product and connection licenses into a common license pool for a server farm. All license counts are pooled by default. Assigning a license count to a server removes it from the pool.

- load management** A feature of Citrix Load Manager that enables management of application loads. When a user launches a published application that is configured for load management, that user's ICA session is established on the most lightly loaded server in the farm, based on criteria you can configure.
- local text echo** A feature that accelerates the display of text input on a client device to effectively shield users from experiencing latency on the network.
- master ICA Browser or master browser** The ICA Browser on one Citrix server in a network that gathers information about licenses, published applications, performance, and server load from the other member browsers within the network, and maintains that information.
- member ICA Browser or member browser** The ICA Browsers on the Citrix servers in a network that forward information about licenses, published applications, performance, and server load to the master browser.
- mixed mode** The mode in which MetaFrame XP servers operate when a server farm contains both MetaFrame XP servers and MetaFrame 1.8 servers.
- mouse-click feedback** A feature that enables visual feedback for mouse clicks. When a user clicks the mouse, the ICA Client software immediately changes the mouse pointer to an hourglass to show that the user's input is being processed.
- native mode** The mode in which MetaFrame XP servers operate when only IMA-based Citrix servers exist in the network and the option to work with MetaFrame 1.8 servers in the network is not selected.
- neighborhood folder** A group of logically related applications within a user's application set. You can assign an application to a specific neighborhood folder when you publish it.
- network printer** A printer that is connected to a network print server.
- panning and scaling** ICA Client features users can use to view a remote session that is larger than the client desktop. For example, if the client desktop is 1024 x 768 and the ICA session is 1600 x 1200 pixels, the session image does not fit in the session view window. Panning provides scroll bars. Scaling provides controls in the System menu to shrink the session window.
- pass-through client** An ICA Client installed on a MetaFrame server so that users of every ICA Client platform can access published applications by connecting to them through Program Neighborhood as a published application.
- product code** A nine-character string that identifies a Citrix server product. A server farm can contain Citrix servers with different versions of the same core product; for example, full retail, evaluation, and not-for-resale versions of MetaFrame XP. The product code allows a Citrix server to locate its product license among the product licenses stored for the entire server farm.
- product license** A software license that enables a Citrix product.

**Program Neighborhood** The user interface for the ICA Win32 and ICA Java Clients, which lets users view the published applications they are authorized to use in the server farm. Program Neighborhood contains application sets and custom ICA connections.

**published application** An application installed on a Citrix server or server farm that is configured for multiuser access from ICA Clients. With Load Manager, you can manage the load for published applications among servers in the server farm. With Program Neighborhood and NFuse, you can push a published application to your users' client desktops.

**relay listening port** The TCP port on the MetaFrame XP server that the Citrix SSL Relay monitors for data from a Web server.

**remote node** A client device that can connect to a LAN or WAN with a modem and additional software, such as Microsoft's Dial-Up Networking. When connected, the device has access to the same network resources as any other node in the network, but is still subject to bandwidth limitations and modem performance.

**seamless window** One of the settings you can specify for the Window Size property of a published application. If a published application runs in a seamless window, the user can take advantage of all the client platform's window management features, such as resizing, minimizing, and so forth.

**Secure Sockets Layer (SSL)** A standards-based architecture for encryption, authentication, and message integrity. It is used to secure the communications between two computers across a public network, authenticate the two computers to each other based on a separate trusted authority, and ensure that the communications were not tampered with. SSL supports a wide range of ciphersuites.

**serial number** An alphanumeric string that you enter in Citrix Management Console to receive a license number for the software installed on a server.

**server farm** A group of Citrix servers managed as a single entity, with some form of physical connection between servers and an IMA-based data store.

**server-based computing** Citrix's model for computing where applications are published on centralized servers, or server farms, and users access and run those applications from remote client devices. Server-based computing differs from traditional client-server computing in that all the application logic executes on the host, consuming less network bandwidth and requiring far fewer client resources.

**session ID** A unique identifier for a specific ICA session on a specific Citrix server.

**Shadow Taskbar** The taskbar on a Citrix server desktop that you can use to shadow multiple users and to quickly switch between shadowed sessions.

**shadowing** A feature of Citrix servers that enables an authorized user to remotely join or take control of another user's ICA session for diagnosis, training, or technical support.

- SOCKS** SOCKS is a protocol for secured TCP communications through a proxy server.
- SpeedScreen Latency Reduction** A combination of technologies implemented in ICA that decreases bandwidth consumption and total packets transmitted, resulting in reduced latency and consistent performance regardless of network connection.
- Web-based ICA Client installation** A Web-based method for deploying ICA Client software to users. You construct an ICA Client download Web site that users access to download the ICA Client for their client devices.
- Windows-Based Terminal (WBT)** A fixed-function thin-client device that can run applications only by connecting to a Citrix application server. WBTs cannot run applications locally.
- zone** A logical grouping of MetaFrame XP servers, typically related to the underlying network subnets. All MetaFrame XP servers in a zone communicate with the MetaFrame XP server designated as the data collector for the zone.



# Index

## A

- account authority 257
- Acrobat Reader program 10
- activation codes 129
  - defined 257
- Active Directory 40
- Active Directory Services Interface (ADSI) 40
- administration tools
  - see* management tools 95
- administrator accounts
  - see* Citrix administrators
- Altaddr command 224
- anonymous application 195
  - defined 257
- anonymous users 195
- App command 226
- Application Launching and Embedding (ALE) 195
  - defined 257
- application sets 191
- applications, data about 200
- applications, publishing
  - see* publishing applications
- assigning licenses to servers 134
- asynchronous ICA connections 33, 140
- audio mapping 157
- Auditlog command 229
- Auto Refresh Settings command 104
- automatic client update 169

## B

- Bandwidth tab 213
- broadcasts
  - MetaFrame server response to 53
- broadcasts, UDP 53, 109
- BUILTIN group 47

## C

- Change Client command 231
- Chfarm utility 235
- Citrix administrators 104
  - configuring accounts 105
  - privileges 105

- Citrix Connection Configuration 137, 143
- Citrix Documentation Library 13
- Citrix ICA Client Administrator's Guides 10
- Citrix Installation Manager 25
- Citrix licensing
  - see* licensing
- Citrix Load Manager 194
- Citrix Management Console 23, 99–106
  - controlling access to 104
  - installing separately 92
  - logging off 101
  - online help 12
  - refreshing data 104
  - switching server farms 101
- Citrix NFuse 10, 49, 161, 185–186
- Citrix Server Administration 68
- Citrix SSL Relay 87
- Citrix Web site 13
- Citrix XML Service 86
- Citrx XML Service 54
- Clicense command 236
- Client Administrator's Guides 10
- client device mapping 154
- client printers 208
- Client Update Configuration Utility 172
- Client Update Database 172, 188
  - adding clients 176
  - changing client properties 181
  - configuring update options 174
  - creating a new database 173
  - defined 258
  - removing clients 180
  - specifying a default database 173
- cloning MetaFrame XP servers 90
- Cltpri command 239
- COM port mapping 156
- command line utilities 223–255
- configuring
  - Citrix administrators 105
  - ICA Client connections 137
  - latency reduction 116
  - MetaFrame XP servers and farms 95
  - ODBC drivers 77
  - zones and data collectors 110

- Connect command 106
- Connection Center 259
- connection licenses 123, 128
  - defined 259
- controlling
  - access to Citrix Management Console 104
  - client logons 199
- conventions, documentation 11
- Ctxmlss command 240
- custom ICA connection 259

## D

- data collectors 110–111
  - defined 259
  - election preference 112
  - response to UDP broadcasts 109
- data store
  - see* IMA data store 71
- data, refreshing 104
- deploying ICA Clients
  - choosing a deployment method 159
  - determining the scope of deployment 162
  - from a network share point 168
  - practices 184
  - with NFuse 161, 185
  - with Web-Based Installation 165, 186
- Dialin Information dialog box 144
- Dial-in tab 144
- Disconnect command 106
- disconnected session 259
- disconnecting ICA sessions 202
- documentation 10
  - Citrix NFuse Administrator's Guide 10
  - conventions 11
  - ICA Clients 12
- DOS-based printers 208
- drive mapping 155
- Drivers tab 214
- Dsmaint command 241
- dynamic store 259

## E

- Edit Connection dialog box 144–145
- election of data collectors 112
- encryption, configuring 150
- explicit users 196
- external IP addresses 224

## F

- firewalls 49
- firewalls, configuring 56
- Frequently Asked Questions 13

## G

- Global groups 44
- grace period of licenses 128

## H

- hardware requirements 33
- HTML files 198

## I

- ICA (Independent Computing Architecture) 18
- ICA Browser 60–61
- ICA Browsing 50–51
- ICA browsing
  - Network Protocol setting 52
- ICA Client Administrator's Guides 10
- ICA Client CD 163
- ICA Client Creator 169, 259
- ICA Client Distribution wizard 82, 163
- ICA Client download Web site 165
- ICA Client Object 164
- ICA Client Printer Configuration 259
- ICA Client Update Configuration 259

## ICA Clients 18

- choosing a deployment method 159
- client printers 208
- Client Update Database 172
- client update process 170
- controlling logons to servers 199
- creating a download Web site 165
- creating installation diskettes 169
- defined 259
- deploying from a network share point 168
- deploying with diskettes 169
- deploying with NFuse 186
- deployment methods compared 160
- deployment practices 184
- download Web site 166
- downloading 13
- EPOC 19
- ICA Client Distribution wizard 82, 163
- installing the pass-through client 164
- Java Client 19
- logging activity 229
- Macintosh 19
- platforms supported 19
- printer mapping 156
- response to UDP broadcasts 109
- server response to broadcasts 53
- time zone support 109
- UNIX 20
- updating 169
- using connection licenses 128
- using the ICA Client CD 163
- Web-Based Installation 165
- WinCE 19
- Windows (16- and 32-bit) 19

## ICA connections

- adding 139
- asynchronous 33, 140, 259
- configuring asynchronous connections 81
- configuring client device mapping 153
  - audio mapping 157
  - COM port mapping 156
  - printer mapping 156
- configuring ICA encryption 150
- configuring Network connections 80
- defined 260
- drive mapping 155
- Edit Connection dialog box 144
- modem callback options 143
- restricting connections to published applications 149
- turning off client device mapping 154
- using null modem cables 143

## ICA Display Options 107

### ICA file 260

### ICA files 197

### ICA protocol 260

### ICA Sessions 51

### ICA sessions 194, 199

- controlling logons 199
- defined 260
- disconnecting sessions 202
- monitoring session status 200
- published application data 200
- resetting sessions 203
- sending messages to users 202
- session commands 106
- Session ID 201
- shadowing 96, 204
- states 201
- terminating processes 204

### Icaport command 245

### IMA

- data collectors 110–111
- defined 260
- zones 110

### IMA data store

- choosing a database 37
- configuring ODBC drivers 77
- defined 259
- Microsoft Access 39
- Microsoft SQL requirements 39
- Oracle requirements 40
- using SQL Server or Oracle 71

### Independent Computing Architecture

*see* ICA

Independent Management Architecture

*see* IMA

information sources 10

installation 31

configuring ODBC drivers 77

installing MetaFrame 71

shadowing restrictions 64

starting MetaFrame XP installation 74

unattended setup 90

uninstalling MetaFrame XP 90

Installation Manager 25, 193

installing MetaFrame 71

interoperability 65

migrating MetaFrame 1.8 to MetaFrame XP 84

mixed mode 53

interoperability with MetaFrame 1.8 60

IP addresses

alternate 224

IP ports 59

## J

Java ICA Client 19

Java Run-Time Environment (JRE) 12

Java Virtual Machine, requirement for NFuse 84

Jet database

*see* Microsoft Access

## L

latency reduction 116

licensing 119–136

activating licenses 129

assigning licenses 134

connection licenses 123

grace period 121, 128

installation 83

license activation 128

license counts 134–135

license numbers 128

machine codes 129

managing license counts 134

MetaFrame for UNIX connection licenses 68

migrating from other Citrix products 123

overview of 119

pooling licence counts in mixed mode 67

pooling license counts 135

product codes 121, 125

product licenses 122

serial numbers 127

upgrading licenses 124

Load Manager 194

local printers 209

local text echo 261

logons

controlling 199

reporting 229

## M

machine codes 129

Macintosh ICA Client 19

management tools 68

managing printer drivers 214

managing printers 207

Master ICA Browser 61

master ICA Browser 60

messages, sending to users 202

MetaFrame 1.8 95

interoperability 65

migrating to MetaFrame XP 84

MetaFrame commands 223–255

MetaFrame documentation 10

MetaFrame for UNIX 68

MetaFrame management tools 95

MetaFrame product licenses 127

Microsoft Access 39

migrating licenses 123

migrating MetaFrame 1.8 to MetaFrame XP 84

mixed mode 53, 60, 65

defined 261

modems 33

callback options 143

ICA connections with 143

mouse-click feedback 261

## N

native mode 65

defined 261

native mode, Active Directory 41, 44

native mode, MetaFrame XP 53–54, 66–69

NetWare drive mapping assignments 156

network firewalls 49

network printers 209–210

New Connection dialog box 143

NFuse 84

Novell ZENworks 47

null modem cables, ICA connections with 143

## O

- ODBC drivers, configuring 77
- online documentation 10
- Oracle
  - creating an IMA data store 71
  - requirements 40

## P

- pass-through client 164
- pass-through ICA Client 192
- ports used by Citrix software 59
- print servers
  - importing 213
- printer drivers 217
- printer management 207–221
  - client printer mapping 156
  - Drivers tab 214
  - features 211
  - importing print servers 213
  - installed printers 215
  - managing printer drivers 217
  - replicating printer drivers 218
  - setting up network printers 216
  - user permissions 45
- printers
  - client 208
  - installed on Windows clients 210
  - limiting bandwidth 213
  - local 209
  - network 209
  - network printers 210
  - shared 208
- Printers tab 215
- processes, terminating 204
- product codes 121, 125, 261
- product license 261
- product licenses 127
- Program Neighborhood 190, 262
- Properties (user account) dialog box 144
- proxy servers 51
- Published Application Manager 68

- publishing applications 189–198
  - application sets 191
  - data on running applications 200
  - Installation Manager applications 193
  - license usage 135
  - pass-through ICA Client 192
  - procedures 197
  - Program Neighborhood 190
  - publishing Program Neighborhood 192
  - standard applications 193
  - user authentication 190
  - user permissions 45
  - videos 194

## Q

- Query command 246

## R

- Readme.txt file 9
- read-only privileges for Citrix administrators 105
- Refresh command 104
- refreshing data 104
- relay listening port 262
- remote control of ICA sessions *see* shadowing 96
- replicating printer drivers 218
- requirements
  - data store database 39
  - disk and memory 33
  - hardware 33
  - Microsoft Access 39
  - Oracle 40
  - software 32
  - SQL Server 39
  - system sizing 35
- Reset command 106
- resetting ICA sessions 203
- restricting connections to published applications 149

## S

- Seamless Window 262
- Secure Sockets Layer (SSL) 262
- sending messages to users 202
- serial numbers 127
  - defined 262
- serial port mapping 156
- server certificate, SSL
  - installing 89
  - obtaining 88

- server farms
  - defined 262
- server-based computing 15
- Session ID 201
- session ID 262
- sessions
  - see* ICA sessions
- setting up
  - Citrix SSL Relay 87
  - MetaFrame unattended 90
  - network printers 216
  - printer drivers 217
- setup
  - see* installation
- Shadow command 106
- Shadow Taskbar 96, 205, 262
- shadowing 64, 106
  - defined 262
  - with Shadow Taskbar 96
- shadowing ICA sessions 204
- shared printers 208
- sizing
  - sizing systems for MetaFrame XP 35
- SNMP network management 110
- SOCKS 263
- Solution Knowledgebase 13
- SpeedScreen Latency Reduction Manager 116
- SQL Server
  - creating an IMA data store 71
  - requirements 39
- SSL Relay 87
- states of ICA sessions 201
- system sizing
  - MetaFrame XP 35

## T

- TCP ports
  - SSL relay (443) 87
  - XML Service (80) 86
- TCP/IP Network Protocol 53
- TCP/IP+HTTP Network Protocol 52
- terminating processes 204
- tools and utilities 68, 97
- tools, management 95
- Twconfig command 254

## U

- UDP (User Datagram Protocol) 53
- UDP broadcasts 109
- unattended setup 90
- uninstalling MetaFrame XP 90
- Universal groups 44
- UNIX ICA Clients 20
- updating the ICA Clients 169, 188
- upgrading MetaFrame 1.8 to MetaFrame XP 84
- user authentication 190
- user groups 195
- user permissions 45
- User Properties dialog box 144

## V

- videos, publishing 194
- virtual printers 208

## W

- Web server extension, NFuse 84
- Web-Based ICA Client Installation 186
- Web-based ICA Client Installation 165, 263
- WinCE
  - ICA Client 19
  - printers 208
- Windows 2000 12
- Windows Media Player 194
- Windows NT 4 12

## X

- XML data 53
- XML Service 54, 86

## Z

- ZENworks Dynamic Local Users 47
- zones 110, 263