

Administrator's Guide

Citrix® MetaFrame XP™

Application Server for Windows

Version 1.0, Feature Release 2

Citrix Systems, Inc.

Copyright and Trademark Notice

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 © 2002 Citrix Systems, Inc. All rights reserved.

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

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

Trademark Acknowledgements

Adobe, Acrobat, and PostScript are trademarks or registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Apple, LaserWriter, Mac, Macintosh, Mac OS, and Power Mac are registered trademarks or trademarks of Apple Computer Inc.

DB2 is a registered trademark and PowerPC is a trademark of International Business Machines Corp. in the U.S. and other countries.

Java, Sun, and SunOS are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Solaris is a registered trademark of Sun Microsystems, Inc. Sun Microsystems, Inc has not tested or approved this product.

Microsoft, MS-DOS, Windows, Windows NT, Win32, Outlook, ActiveX, and Active Directory are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corp. in the U.S. and other countries.

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

UNIX is a registered trademark of The Open Group.

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

Contents

Chapter 1

Welcome

MetaFrame XP Documentation	14
Using PDF Documentation.	15
Documentation Conventions	15
Using Online Help	16
Providing Feedback About this Guide	16
Finding Information About Windows Servers.	16
Citrix on the World Wide Web	17

Chapter 2

Introduction to MetaFrame XP

Overview of Server-Based Computing	19
Components of Citrix Server-Based Computing	20
Advantages of ICA and MetaFrame XP	20
Overview of MetaFrame Server Farms	21
Independent Management Architecture (IMA)	22
Independent Computing Architecture and ICA Clients.	23
Citrix ICA Clients	23
Overview of the MetaFrame XP Family	24
What's Included in MetaFrame XPs	24
What's Included in MetaFrame XPa	27
What's Included in MetaFrame XPe	28
Features of MetaFrame XP for Windows	31
Application Server Features	31
Citrix ICA Client Features	32
MetaFrame XP Feature Releases	33
Features Included in Feature Release 2	33
Features Included in Feature Release 1	38
New Features in MetaFrame XP	41

Chapter 3

Planning for MetaFrame XP Deployment

System Requirements.	43
System Software Requirements	43
System Hardware Requirements	45
Sizing Systems for MetaFrame XP	47

Choosing a Database for the Data Store	50
System Sizing for the Data Store Database	51
Connecting to the Data Store	52
Data Store Database Requirements	52
Microsoft Access	52
Microsoft SQL Server.	53
Oracle	56
IBM DB2.	58
Network Configuration and Account Authority Issues	60
General Configuration Issues	60
Recommendations for Active Directory.	60
User Access to Applications and Printers	62
Active Directory Security Model and Restrictions	63
Supporting Novell Directory Service Users	66
Setting up Support for NDS	67
Configuring Printer Auto creation in NDS.	70
Changing Domain Trust Relationships	71
Configuring Citrix Administrator Accounts	72
Planning for Client and Server Communications	73
Linking ICA Clients and MetaFrame XP Servers	74
Configuring ICA Browsing	75
Communicating with the Citrix XML Service.	79
Using DNS Address Resolution.	80
Configuring Network Firewalls	81
Server Farm Configurations	81
ICA Browsers and MetaFrame 1.8 Interoperability.	86
Changing Server Drive Letters	88
Using Smart Cards with MetaFrame XP	90
Software Requirements.	91
Configuring the Server	91
Configuring the Client	93
Interoperability with MetaFrame 1.8.	93
Configuring MetaFrame XP for Mixed Mode Operation	93
Pooling License Counts in Mixed Mode	95
Using MetaFrame XP Tools in Mixed Mode.	96

Chapter 4**Installing MetaFrame XP**

Creating the Data Store with SQL Server, Oracle, or DB2	99
Using the MetaFrame XP Windows Installer Package	101
Important Recommendations for Windows Installer	102
Common Windows Installer Commands	103
Creating a Log File	103
Unattended Setup of MetaFrame XP Servers	104
Applying Transforms	104
Creating an Answer File	105
Starting MetaFrame XP Setup	106
Choosing Options During Setup	107
Selecting the MetaFrame XP Family Level	107
Configuring the Data Store	108
Assigning Farm Administrator Credentials	115
Configuring Session Shadowing	115
Configuring Network ICA Connections	117
Installing Citrix NFuse Classic	117
Configuring the Citrix XML Service Port	117
Setting the Server's Default Web Page	119
Installing ICA Client Software	119
Migrating Citrix Servers to MetaFrame XP	121
Supported Migration Paths	121
Cloning a MetaFrame XP Server	123
Uninstalling MetaFrame XP	123
Installing Citrix Management Console on Other Computers	124

Chapter 5**Deploying Feature Release 2 and Service Pack 2**

Upgrading to Feature Release 2 or Service Pack 2	125
Choosing Installation Options	126
Updating Citrix Management Console	127
Backing Up Files Before Installation	128
Viewing Updated Documentation	128
Using Setup	128
Downloading and Installing a Service Pack	130
Updating ICA Client Software	130
Unattended Setup of MetaFrame XP, Feature Release 2	130
Creating an Answer File	131
Using the Command Line	131

Downgrading Feature Release 2 or Service Pack 2.	132
Setting the Feature Release Level	132

Chapter 6

Licensing MetaFrame XP

Overview of Citrix Licensing.	135
Summary of the Licensing Process	136
Types of MetaFrame XP Licenses.	138
Product Licenses	138
Connection Licenses	139
Migrating Licenses from Other Citrix Products.	139
Upgrading Licenses	140
Understanding Citrix Licensing Codes	140
Product Codes	140
Serial Numbers	142
License Numbers	144
License Activation Codes.	144
Managing and Monitoring Licenses	144
Adding Licenses to Server Farms.	145
Activating Licenses.	146
License Views.	147
Managing License Counts	150
Pooling License Counts	151
Assigning License Counts	151
Removing Licenses.	152
Client Device Licensing	152
Licensing Requirements for Feature Release 2	152
Activating Feature Release 2 Licenses.	154
Viewing Feature Release License Information	154

Chapter 7

Configuring MetaFrame XP Servers and Farms

Management Tools for MetaFrame XP	157
Overview of MetaFrame XP Management Tools	158
The ICA Administrator Toolbar	159
Citrix Management Console	161
Configuring Citrix Administrator Accounts	162
Using Citrix Management Console	166
Data Displayed in Citrix Management Console.	167

Citrix Web Console	170
Configuring MetaFrame XP Properties	171
Properties of MetaFrame XP Server Farms	172
Using the Farm Properties Dialog Box	172
Configuring MetaFrame XP Server Properties	176
Using the Server Properties Dialog Box	176
Configuring Zones and Data Collectors	179
Functions of Data Collectors	179
Setting Up Citrix SSL Relay	182
Obtaining and Installing Server Certificates	183
Changing the SSL Relay Port	187
Configuring Latency Reduction for ICA Clients	188
Deploying SpeedScreen Settings	189

Chapter 8

Configuring ICA Connections

Overview of ICA Connections and Sessions	191
Setting Up ICA Connections	192
Using Citrix Connection Configuration	192
Adding ICA Connections	193
Adding Asynchronous ICA Connections	194
Configuring Session Settings for ICA Clients	196
Precedence of Settings	197
Configuring ICA Connection Options	198
Configuring Modem Callback	198
Configuring Direct Cable Connections	200
Configuring Advanced ICA Connection Options	204
Restricting Connections to Published Applications	205
Configuring ICA Encryption	205
Using Shadowing to Monitor ICA Sessions	205
Enabling Shadowing on a Server	206
Configuring ICA Connections for Shadowing	206
Configuring ICA Audio Settings	208
Configuring Client Device Mapping	209
Options for Client Device Mapping	210
Client Drive Mapping	210
Client Printer Mapping	212
Client Serial Port Mapping	213
Client Audio Mapping	213

Chapter 9**Deploying ICA Clients to Users**

Choosing a Deployment Method	215
Delivering Applications to Users	217
Determining the Scope of ICA Client Deployment	218
Using the MetaFrame XP Components CD	219
Pass-Through ICA Client	220
ICA Client Object	220
Deploying the ICA Clients	220
Using Installer Packages for Client Deployment	221
Web-Based Installation	221
Deploying ICA Clients Over a Network	222
Deploying ICA Clients Using Diskettes	222
Updating the ICA Clients	223
The ICA Client Update Process	224
Configuring the Client Update Database	224
Using the Client Update Configuration Utility	225
Creating a New Client Update Database	226
Specifying a Default Client Update Database	226
Configuring Default Client Update Options	227
Adding ICA Clients to the Client Update Database	228
Removing an ICA Client From the Client Update Database	232
Changing the Properties of an ICA Client in the Database	233
ICA Client Deployment Practices	236
Manufacturing Enterprise	236
Regional Bank	237
Application Service Provider	238
Insurance Company	239

Chapter 10**Making Information Available to Users**

Deciding How Users Access Information	242
Managing Users' Access to Information with Content Publishing and Content Redirection	243
Publishing Applications and Content	244
User Access to Published Applications	245
Administrative Control of Applications	247
Using Published Applications	247
Configuring User Access to Applications	248

Procedures for Publishing Applications	250
Associating Published Applications with File Types	251
Passing Parameters to Published Applications.....	254
Creating Files for Application Launching and Embedding.....	254
Removing Published Applications.....	255
Configuring Content Redirection.....	256
Redirecting Content from Client to Server.....	256
Redirecting Content from Server to Client.....	257
Publishing Content.....	258
Publishing Content to be Opened with Applications Published on MetaFrame Servers.....	259
Publishing Content to be Opened with Applications on Local Client Devices	259
Publishing Content on MetaFrame XP Servers	261
Setting CPU Priority Levels for Applications	262
Assigning CPU Priority Levels to Applications	263

Chapter 11

Managing Users and ICA Sessions

Controlling Logons by ICA Clients.....	265
Controlling User Connections	266
Limiting Total Connections in a Server Farm	267
Limiting Application Instances.....	267
Configuring Connection Control Settings	268
Logging Connection Control Events	269
Monitoring and Managing ICA Sessions	270
Viewing Information About ICA Sessions	271
Using Session Management Commands	272
Reconnecting ICA Sessions Automatically.....	276
How Automatic Reconnection Works	276
Configuring Reconnection Settings	277
Setting Up ICA Connections for Auto Reconnect.....	278
Logging Reconnection Events	280
Creating and Applying User Policies.....	281
Prioritizing Policies.....	283
Shadowing ICA Sessions.....	284
Configuring User-to-User Shadowing	286
Monitoring Performance of Sessions and Servers.....	288

Chapter 12	Managing Printers for ICA Clients	
	Overview of Printing with MetaFrame XP	291
	Configuration of Printing Devices	291
	Client Printing in ICA Sessions	292
	Printing Configuration Scenarios	293
	Printer Management Features	295
	Using the Printer Management Node	295
	Using the Servers Node	298
	Setting Up Network Printers for ICA Client Users	299
	Installing and Replicating Printer Drivers	300
	Setting Up Automatic Replication of Printer Drivers	301
	Mapping Printer Drivers	302
	Managing Drivers for Client Printers	302
	Auto Creation of Client Printers for DOS and WinCE	303
	ICA Client Settings for Printer Access	304
	Using the Citrix Universal Print Driver	304
	Client Printing with the Universal Driver	305
	Configuring the Universal Driver for Client Printing	306
	Limiting Printing Bandwidth in ICA Sessions	308
Appendix A	MetaFrame XP Commands	309
	ACRCFG	310
	ALTADDR	313
	APP	315
	AUDITLOG	318
	CHANGE CLIENT	320
	CHFARM	324
	CLICENSE	325
	CLTPRINT	328
	CTXXMLSS	329
	DSMAINT	330
	ICAPORT	334
	IMAPORT	335
	QUERY	336
	TWCONFIG	345

Appendix B	MetaFrame XP Setup Properties	347
	Property Names and Values.....	347
	Creating Transforms.....	352
Appendix C	Glossary	357
	Index	365

Welcome



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.

Important Before you install MetaFrame XP, read SP2-FR2_readme.txt, which is in the root directory of the MetaFrame XP CD-ROM. For information about new features in MetaFrame XP and feature releases, see “Introduction to MetaFrame XP” on page 19.

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>. For more information, see “Citrix on the World Wide Web” on page 17.

MetaFrame XP Documentation

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

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

Documentation for additional management tools and features that are included with MetaFrame XPe is on the Components CD-ROM. Some of this documentation is also in the Docs directory on the MetaFrame XP CD-ROM.

Information about MetaFrame XP Feature Release 2 and Service Pack 2, including information about new features and about installing Feature Release 2 or Service Pack 2, is included in this manual. See “Deploying Feature Release 2 and Service Pack 2” on page 125 and “Features Included in Feature Release 2” on page 33.

Important additional documentation for Citrix products is available from the Product Documentation page in the Support area of the Citrix Web site at www.citrix.com/support. For example, the *Advanced Concepts* guide for MetaFrame XP is a manual that provides system sizing, deployment, configuration, optimization, and troubleshooting information, which supplements the *MetaFrame XP Administrator's Guide*.

On a MetaFrame XP server, documentation is installed in the 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 readme file and readmes for feature releases contain last minute updates, corrections to the documentation, and a list of known problems. These files are in the root directory of the MetaFrame XP CD-ROM.
- The *Citrix NFuse Classic 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 \Docs 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 Product Documentation. 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 access the Citrix documentation that is provided in PDF files, use Adobe Acrobat Reader 4 or later. Acrobat Reader lets you view, search, and print the documentation.

You can download Acrobat Reader 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
Boldface	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 F1 for the function key that is labeled F1.
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, { yes no } means you must type yes or no . Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [/ping] means that you can type /ping with the command. Do not type the brackets themselves.

Convention	Meaning
(vertical bar)	A separator between items in braces or brackets in command statements. For example, { /hold /release /delete } means you type /hold or /release or /delete .
... (ellipsis)	You can repeat the previous item or items in command statements. For example, /route:devicename [...] 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.

Providing Feedback About this Guide

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

You can send e-mail to the documentation authors at documentation@citrix.com. Please include the product name, product version number, and the title of the document in your message.

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.

Important Feature Release 2 for MetaFrame XP does not operate on Windows NT Server 4.0, Terminal Server Edition.

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 about application compatibility and deployment issues is available at the Microsoft Web site at <http://www.microsoft.com/Windows2000>
- For Windows NT 4.0, Terminal Server Edition, information about application compatibility and deployment issues is available at <http://www.microsoft.com/ntserver>

Instructions for installing and using Windows servers are included in the Microsoft documentation included in your Windows package and can also be found on the Microsoft Web site at <http://www.microsoft.com>.

Citrix on the World Wide Web

The Citrix Web site is at <http://www.citrix.com>. The site offers a variety of information and services for Citrix customers and users.

From the Citrix home page, you can access Citrix technical support services and other information designed to assist MetaFrame XP administrators.

The following are some of the resources available on the Citrix Web site:

Citrix Product Documentation Library. The library, which contains the latest documentation for all Citrix products, is at <http://www.citrix.com/support> (select Product Documentation). You can download updated editions of the documentation that ships with Citrix products, as well as supplemental documentation that is available only on the Web site.

Citrix ICA Clients. Downloadable Citrix ICA Clients for all supported platforms are available from <http://www.citrix.com/download>.

Support options. Program information about Citrix Preferred Support Services options is available from the Support area of the Citrix Web site at <http://www.citrix.com/support>.

Software downloads. An FTP server provides access to the latest service packs, hotfixes, utilities, and product literature for download.

Online knowledgebase. The online Solution Knowledge Base contains an extensive collection of application notes, technical articles, troubleshooting tips, and white papers.

Discussion forums. The interactive online Solution Forums provide outlets for discussion of technical issues with other Citrix users.

FAQs. Frequently Asked Questions (FAQ) pages provide answers to common technical and troubleshooting questions.

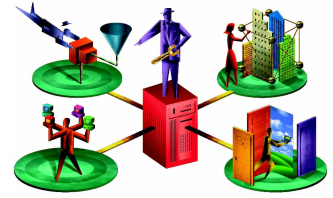
Education. Information about programs and courseware for Citrix training and certifications is available from <http://www.citrix.com/training/>.

Contact information. The Web site provides contact information for Citrix offices, including the worldwide headquarters and headquarters for European, Asia Pacific, and Japan operations.

Developer network. The Citrix Developer Network (CDN) is at <http://www.citrix.com/cdn>. This open-enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate Citrix computing solutions into their products.

SDKs. The Citrix Server Software Development Kit (SDK) is available for free from www.citrix.com/cdn. Most of the operations that you can perform through Citrix GUI tools can be scripted by using the Citrix Server SDK. The SDK also lets programmers customize most aspects of MetaFrame XP.

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 MetaFrame XP.

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.

The Citrix MetaFrame XP application server suite of software 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.

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 reduces the total cost of ownership of their application services.

Components of Citrix Server-Based Computing

The components and technologies that enable Citrix server-based computing include the MetaFrame XP application server suite, 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:

Multuser 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 multuser capabilities.

Note MetaFrame XP, Feature Release 2 is supported only on Windows 2000 Server operating systems. MetaFrame XP with Feature Release 1 is supported on both Windows 2000 Servers and Windows NT Server 4.0, Terminal Server Edition.

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. 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. See "Independent Computing Architecture and ICA Clients" on page 23 for more information.

Advantages of ICA and MetaFrame XP

The ICA protocol developed by Citrix supports all types of hardware, operating platforms, network connections, and network protocols. ICA lets organizations deliver a common set of applications to users with better performance than alternative technologies.

Because MetaFrame XP centralizes application delivery and management, it simplifies administration and unifies the enterprise computing environment.

Citrix technologies and MetaFrame XP deliver the following 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.

Support for client devices. 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.

Universal network connectivity. Users can connect to networked MetaFrame XP servers through standard telephone lines, WAN links, broadband connections, wireless and CDPD connections, and the Internet. The unique bandwidth-conserving nature of the Citrix ICA protocol makes it an efficient solution for any network type.

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 (28.8 Kbps is the recommended minimum speed). Dial-in async support eliminates the need to configure a RAS server or RAS connection for client computers.

Overview of MetaFrame Server Farms

MetaFrame server farms provide you with a flexible and robust way of deploying applications to ICA Client users. A MetaFrame server farm is a group of MetaFrame 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 about interoperability of MetaFrame XP with MetaFrame 1.8 servers, see “Interoperability with MetaFrame 1.8” on page 93.

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 shadowing events
- 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.

Independent Computing Architecture and ICA Clients

MetaFrame XP provides server-based computing to local and remote users through the Independent Computing Architecture (ICA) 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 for Web browsers that use the ActiveX control or Netscape plug-in.

Detailed instructions for installing and configuring Citrix ICA Clients are in the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Overview of the MetaFrame XP Family

MetaFrame XP is available in three tailored solutions:

- MetaFrame XPs is designed to give businesses outstanding performance from applications running on a central server.
- MetaFrame XPa is designed with the small to medium business in mind. A MetaFrame XPa license enables all of the features of MetaFrame XPs and also includes load balancing functionality.
- MetaFrame XPe is designed for single-point control of servers, licenses, and resources in large organizations and multinational corporations. A MetaFrame XPe license enables all of the features of MetaFrame XPa and also provides system monitoring and analysis, application packaging and delivery, and integration with third-party SNMP management consoles.

These solutions enable you to install and license only those features and components that you need on a specific server. Each solution is described in more detail in this chapter.

What's Included in MetaFrame XPs

Citrix MetaFrame XPs is designed to provide a predictable computing experience with outstanding performance from applications running on a central server.

This section describes the components of MetaFrame XPs.

MetaFrame XP

MetaFrame XP is the application server component of Citrix's server-based computing solutions.

You install MetaFrame XP on one or more servers, and install and publish the applications, server desktop, or other resource that you want users to access.

For each server farm, you need a database called a *data store*. 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. Using an external data store ensures a scalable and flexible system for managing your MetaFrame servers.

You can use client/server databases such as Oracle, Microsoft SQL Server, or IBM DB2 for your data store. Alternatively, you can use Microsoft Access, which is a database that is included with Windows server operating systems.

You can install MetaFrame XP from the MetaFrame Server CD-ROM.

For conceptual information about implementing a MetaFrame XP solution, see “Planning for MetaFrame XP Deployment” on page 43.

Citrix Management Console

You can install Citrix Management Console on MetaFrame XP servers, or install it stand-alone on any Windows NT, Windows XP, or Windows 2000 workstation for remote administration of MetaFrame XP server farms.

You install Citrix Management Console from the MetaFrame XP CD.

See the online help in Citrix Management Console for detailed information about using the console.

ICA Clients

After you install MetaFrame XP and publish your resources, you can connect to your Windows applications from virtually any client device and platform, including:

- All Windows platforms (for example, whether you are using Windows 3.1 or Windows XP, there is an ICA Client for your platform)
- Java
- Linux and UNIX Operating Systems
- Windows CE handheld computers and Windows-based Terminals
- DOS
- OS/2 Warp
- Macintosh

You can install the ICA Clients from the MetaFrame XP Components CD-ROM. For an introduction to the methods you can use to deploy clients, see “Deploying ICA Clients to Users” on page 215. Each ICA Client has a separate *ICA Client Administrator's Guide* to help you deploy and configure the client. These guides are on the MetaFrame XP Components CD-ROM.

Important Citrix continually updates its ICA Clients to support new client computing platforms and operating system versions. Visit the Citrix Web site download area at <http://www.citrix.com/download> for information about new and updated ICA Clients.

NFuse Classic

Using NFuse Classic, you can create stand-alone Web sites for application access or Web sites that can be integrated into your corporate portal. An NFuse Classic deployment involves the interaction of three network components:

- A MetaFrame server farm
- A Web server, on which you install NFuse Classic
- A client device with a Web browser and ICA Client

You can install NFuse Classic in two ways.

- The most common deployment is on a Web server, separate from your MetaFrame XP server farm. In a secure environment, you would most likely include NFuse Classic in the demilitarized zone (DMZ). If you want to install NFuse Classic, install it from the MetaFrame XP Components CD-ROM.
- You can also install NFuse Classic on one of your MetaFrame XP servers. If you do this, you need to set up the MetaFrame XP server as a Web server. If you want to install NFuse Classic in this way, you can select NFuse Classic as a feature when you install MetaFrame XP from the MetaFrame XP Server CD-ROM. Alternatively, you can install NFuse Classic from the MetaFrame XP Components CD-ROM.

Refer to the *Citrix NFuse Classic Administrator's Guide* for instructions about how to install, configure, and customize NFuse Classic. This guide is located in the NFuse directory on the Components CD-ROM.

Citrix Secure Gateway

Citrix Secure Gateway is a secure Internet gateway for ICA data traveling into and out of a MetaFrame XP server farm. You can secure all traffic traveling across the Internet between MetaFrame XP servers and SSL-enabled ICA Client workstations. Using Citrix Secure Gateway makes firewall traversal easier and provides heightened security by providing a single point of entry and secure access to your MetaFrame XP server farms.

To use Citrix Secure Gateway, you need to include the following additional components in your deployment:

- **A Secure Ticket Authority server.** When a user clicks on an application icon in an NFuse Classic Web page, NFuse Classic contacts a service running on a server called the *Secure Ticket Authority Server* for a “secure ticket.”
- **A Secure Gateway server.** The user’s connection to the application is then routed through a *Secure Gateway server* (which is usually in the DMZ). The Gateway server validates the ticket with the Secure Ticket Authority. If the ticket is valid, the Secure Ticket Authority provides the address of the MetaFrame XP server that can provide the application.

You install Citrix Secure Gateway server and the Secure Ticket Authority service from the MetaFrame XP Components CD-ROM.

For more information about Citrix Secure Gateway, see the *Citrix Secure Gateway Administrator’s Guide* on the MetaFrame XP Components CD-ROM and the Secure Gateway online help.

Citrix SSL Relay

If you want to secure all communications within your environment using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption, you can use SSL Relay to secure communications between supported ICA Clients, NFuse Classic, and MetaFrame XP servers.

To deploy SSL Relay, you need server certificates on each of your MetaFrame XP or NFuse Classic servers.

SSL Relay is a feature of all MetaFrame XP server installations.

For more information about SSL Relay, see “Setting Up Citrix SSL Relay” on page 182 and the online help for the SSL Relay configuration tool.

What’s Included in MetaFrame XPa

Citrix MetaFrame XPa is designed with the small to medium business in mind. A MetaFrame XPa license enables all of the features of MetaFrame XPs and also provides advanced load management using *Load Manager*.

Load Manager

You can set up, monitor, and balance the server and published application loads in a server farm so that users can run the published applications they need quickly and efficiently.

The criteria you define in Load Manager determine which servers are least busy and can best run an application. When a published resource is launched from an ICA Client, Load Manager selects which server will run the application or desktop session, based on server load. Load Manager ensures that the application runs on a server that is not overloaded, and so improves performance for users.

Using Load Manager also offers increased availability. By configuring a pool of servers capable of running your users' applications, you can easily bring servers off-line for maintenance or add more servers for increased performance without affecting application availability.

Load Manager is installed automatically when you install MetaFrame XPa.

For more information about Load Manager, see *Getting Started with Citrix Load Manager*, located on the MetaFrame XP Server CD-ROM.

What's Included in MetaFrame XPe

Citrix MetaFrame XPe offers robust management capabilities specifically designed for single-point control of servers, licenses, and resources. It is designed for IT administrators in large organizations and multinational corporations who must manage complex networks that include diverse devices and operating systems.

A MetaFrame XPe license enables all of the features of MetaFrame XPa and also provides:

- System monitoring and analysis using *Resource Manager*
- Application packaging and delivery using *Installation Manager*
- Systems management capabilities using *Network Manager* and third-party SNMP management consoles
- Aggregation of applications from multiple server farms using *Enterprise Services for NFuse*

Resource Manager

Resource Manager enables you to collect, display, and analyze data about system performance, application use, and user activity.

Resource Manager can track and store information about a wide variety of system and network processes and events. If the value of these metrics falls outside normal limits, Resource Manager can warn you by email and pager alerts.

You can also use Resource Manager to store longer term data in an external Microsoft SQL Server or Oracle database. You can use the *summary database* to retrieve historical records on processes, server events, server metrics, and user activities for individual servers or groups of servers. You can also generate bills based on resource usage.

Resource Manager is a feature of a MetaFrame XPe server installation. You can choose to include it in your installation when you run the installation program on your MetaFrame XP Server CD-ROM.

For more information about Resource Manager, see the *Resource Manager Administrator's Guide* located on the MetaFrame XP Server CD-ROM.

Network Manager

Network Manager allows you to remotely control and monitor the status of MetaFrame XPe servers using a third-party SNMP management console.

Network Manager consists of an SNMP agent installed as part of MetaFrame XPe and plug-ins for supported SNMP management console applications. Using a third-party SNMP management console, you can terminate processes on MetaFrame XPe servers, as well as send a message to, log off, or disconnect an active ICA session on a MetaFrame XPe server.

Network Manager also includes the MIB (Management Information Base) definition file for MetaFrame servers. You can use any SNMP management console application that supports MIB browsing to monitor and control MetaFrame XPe servers.

The Network Manager plug-ins interact with the SNMP management consoles through API calls provided by the SNMP management consoles. The Network Manager plug-ins automatically:

- Explore and gather information from MetaFrame XPe servers with the SNMP agent enabled
- Update the gathered data on the network map
- Log MetaFrame XPe server traps in the event database

Network Manager includes Windows plug-ins for the following SNMP management console applications:

- Tivoli NetView
- HP OpenView Network Node Manager
- CA Unicenter

Important Check the *Network Manager Administrator's Guide* for details about the versions of the SNMP management consoles that the Network Manager plug-ins support.

The Network Manager SNMP Agent is installed with a MetaFrame XPe server installation. For more information about the Network Manager, see the *Network Manager Administrator's Guide* located on the MetaFrame XP Server CD-ROM.

Installation Manager

You can use Installation Manager to install applications on the servers in your MetaFrame XP server farm from a central location.

Installation Manager lets you install an application package, such as Microsoft Office 2000, *from one server to all the servers* in a domain or in a server farm. Use Installation Manager whenever you need to deploy applications, files, service packs, or software patches on the servers in your server farm.

You can automate the application installation process, enabling the replication of published applications to MetaFrame XP servers across an enterprise. Automating the process enables you to save time and reduce errors when installing many applications or applications that are frequently updated.

Installation Manager is installed with MetaFrame XPe.

For more information about the Installation Manager, see the *Installation Manager Administrator's Guide* located on the MetaFrame XP Server CD-ROM.

Enterprise Services for NFuse

Enterprise Services for NFuse extends NFuse Classic by giving users resources published from multiple MetaFrame server farms on a single Web page. This process, called *aggregation*, greatly simplifies user access to applications in organizations that have more than one MetaFrame server farm.

You can configure and manage Enterprise Services for NFuse using a Web browser.

You install Enterprise Services for NFuse from the MetaFrame XP Components CD-ROM. For more information about Enterprise Services for NFuse, see the *Enterprise Services for NFuse Administrator's Guide* and the online help.

Features of MetaFrame XP for Windows

Major features of MetaFrame XP, including IMA and the Citrix Management Console, are discussed earlier in this chapter. This section describes other features of MetaFrame XP.

Application Server Features

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 215.

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 (ALE) 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 about 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. 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.

Audio support. MetaFrame XP provides audio support for most ICA Clients. Compression can be used to maximize bandwidth utilization. ICA supports audio through Sound Blaster Pro-compatible sound hardware in DOS and Windows client devices.

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 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 about using this feature on a particular ICA Client.

MetaFrame XP Feature Releases

Citrix periodically makes available feature releases in between major platform releases of MetaFrame XP.

To use the new features included with feature releases, you must install and activate feature release licenses. For more information about MetaFrame XP and feature release pricing and availability, see the Citrix Web site at <http://www.citrix.com>.

Features Included in Feature Release 2

With Feature Release 2, MetaFrame XP includes support for NFuse Classic 1.7, the latest version of NFuse, as well as for two new Citrix products, Enterprise Services for NFuse, and Citrix Secure Gateway. For information about these products, see the documentation in the corresponding Docs directories on the Components CD-ROM included with MetaFrame XP, Feature Release 2.

Note Features that were introduced with Feature Release 1 are included with Feature Release 2. For information about Feature Release 1, see “Features Included in Feature Release 1” on page 38.

MetaFrame XP

MetaFrame XP 1.0, Feature Release 2 includes the following new features and enhancements. You must install the appropriate Feature Release 2 licenses to enable these features.

Important New features in Feature Release 2 are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8.

Delegated administration. Citrix administrators can delegate areas of MetaFrame administration and farm management to IT staff. Administrators can assign these specialized staff members to perform specific MetaFrame farm management tasks such as managing printers, published applications, or user policies. Members of the enterprise’s IT staff can carry out their assigned tasks without being granted full access to all areas of farm management.

For more information, see “Configuring Citrix Administrator Accounts” on page 72 and “Configuring Citrix Administrator Accounts” on page 162.

User-to-user shadowing. Users can shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration.

For more information, see “Configuring User-to-User Shadowing” on page 286.

Smart card support. You can use smart cards with MetaFrame XP, supported ICA Clients, and NFuse to provide secure access to applications and data. Using smart cards with MetaFrame and the ICA Clients simplifies the authentication process while enhancing logon security. MetaFrame XP supports smart card authentication to published applications, as well as to “smart card enabled” applications such as Microsoft Outlook.

For more information, see “Using Smart Cards with MetaFrame XP” on page 90.

Content Redirection. Administrators can specify whether local or remote applications are used to open content, allowing for the appropriate application to be launched to better meet the needs of the user. With Content Redirection, you gain flexibility when considering application installation and content storage locations.

Use Content Redirection to redirect application launching from:

- **Client to server.** Content, such as a file attached to an email message, that the user encounters when running a local application is opened with an application published on the MetaFrame server. This capability is supported with the ICA Win32 Program Neighborhood Agent, the ICA Macintosh Client, and the ICA WinCE Client.
- **Server to client.** URL links that the user encounters when running an ICA session are opened using the locally installed Web browser. This capability is supported with the ICA Win32 Clients and the ICA Linux Client.

For more information, see “Making Information Available to Users” on page 241.

Content Publishing enhancements. When you publish content using the functionality introduced in Feature Release 1 for MetaFrame XP, you can direct users to open the published content with an application published on a MetaFrame XP server with Feature Release 2. Previously, users could open published content only with locally installed players or viewer applications. Content Publishing now allows “browser only” devices that do not have locally installed applications to open content published on MetaFrame servers. This capability is supported only when users connect to published content through NFuse.

For more information, see “Making Information Available to Users” on page 241.

User Policies. With User Policies, you can apply select MetaFrame settings, including shadowing permission settings, printer autocreation settings, and client device mapping settings, to specific users or user groups. Using policies, you can tailor your environment at the user level. User Policy settings override all other MetaFrame XP and Terminal Services settings.

For more information, see “Creating and Applying User Policies” on page 281.

Citrix Management Console enhancements. Citrix Management Console now includes the following enhancements:

- **Better integration with Active Directory.** When you add users to console areas such as published applications or user policies, the interface reflects the hierarchical relationships of the Active Directory Organizational Unit structure. This tighter integration allows improved usability and faster enumeration. User objects are not enumerated until their host container is expanded.
- **Pass-through authentication.** Citrix administrators can log on to the console using the credentials of the local user, eliminating the need to enter credentials each time.
- **Ticketing.** When using the pass-through authentication logon method, Citrix administrator credentials are not passed over the wire. Ticketing provides secure and confidential authentication.

- **Search capability.** You can search your published applications, user policies, and autocreated printers for users or user groups.

Windows Installer support. MetaFrame XP, MetaFrame feature releases, and many MetaFrame XP components are available in Windows Installer packages (.msi files). All family levels of MetaFrame XP (MetaFrame XPs, XPa, or XPe) are installed from a single setup program and a single CD-ROM.

For more information about MetaFrame XP Setup, see “Installing MetaFrame XP” on page 99 and “MetaFrame XP Setup Properties” on page 347.

IBM DB2 support. You can now use IBM DB2 for your farm’s data store. MetaFrame XP supports IBM DB2 Universal Database Enterprise Edition Version 7.2 with FixPak 5.

For more information, see “Choosing a Database for the Data Store” on page 50 and “Installing MetaFrame XP” on page 99.

Printer management enhancements. Enhancements to printer management allow you to:

- Set printing preferences for autocreated printers, including paper size and copy count
- Refresh users’ printer settings each time they log on to an ICA session
- Choose to save or purge the print queue when users log out
- Configure published applications to launch without waiting for all printers to be created

For more information, see the online Help for the Printers node in Citrix Management Console.

Citrix Web Console enhancements. The Citrix Web Console now includes searching and filtering capabilities and an improved layout, including static buttons.

Transport Layer Security (TLS) encryption. MetaFrame XP now includes support for TLS, the latest cryptographic security protocol. Client-to-server communication now passes through TLS and uses encryption modules certified with Federal Information Processing Standard (FIPS) 140 requirements.

For more information, see “Setting Up Citrix SSL Relay” on page 182.

MetaFrame XPe Components

The optional components of MetaFrame XPe include the following new features and enhancements.

Installation Manager

Enhancements to the application packaging and delivery function in Installation Manager allow you to:

- Group packages and stagger their delivery across MetaFrame XP server groups
- Configure multiple share points for WAN package delivery
- Add Windows Installer patch files to existing packages

For more information, see *Getting Started with Citrix Installation Manager* in the Docs directory on the MetaFrame XP CD-ROM.

Resource Manager

Enhancements to Resource Manager allow to you:

- Collect performance, session, and application data in a centralized database for the entire MetaFrame farm
- Produce reports, including billing reports for CPU usage or connection time, based on predefined templates created with Crystal Reports

For more information, see the *Citrix Resource Manager Administrator's Guide* in the Docs directory on the MetaFrame XP CD-ROM.

ICA Clients

With the release of Version 6.30, the ICA Clients include the following new features and enhancements. Version 6.30 of the ICA Clients is included with MetaFrame XP, Feature Release 2.

Roaming User Reconnect. Users can reconnect to a disconnected session with their user name rather than the device name. This functionality is supported by the full ICA Win32 Program Neighborhood Client, the Program Neighborhood Agent, and ICA Clients that connect to published applications through NFuse.

Enhanced Internet proxy support. ICA Clients support the following security enhancements.

- **Secure Proxy (HTTP/SSL Tunnel Proxy).** In addition to SOCKS proxy, ICA Clients now support Secure Proxy.
- **Proxy authentication.** ICA Clients now support proxy authentication with both SOCKS and HTTP/SSL Tunnel proxies.

- **Proxy auto-detection.** ICA Clients can now automatically detect proxy configuration by querying proxy information managed by Internet Explorer or Netscape browsers.
- **Proxy auto-configuration script interpreter.** ICA Clients can now interpret proxy auto-configuration (.PAC) JavaScript to derive the proxy configuration when this type of proxy configuration is detected.

For more information, see the *Administrator's Guides* for the ICA Clients you plan to deploy, located in the ICAClientDoc directory on the Components CD-ROM.

Features Included in Feature Release 1

MetaFrame XP 1.0, Feature Release 1 includes the following new features and enhancements. Features included in Feature Release 1 are installed when you install Feature Release 2.

Important New features in Feature Release 1 are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8

Automatic reconnection to ICA sessions. With the auto client reconnect feature, the ICA Win32 Client automatically reconnects to a session when it detects a dropped connection (when network issues outside of MetaFrame XP occur). Users can continue to work without reconnecting manually, re-entering credentials, and restarting applications. The ICA Java Client in embedded mode supports basic automatic reconnection without credential caching (users must re-enter their credentials to reconnect).

For more information, see “Reconnecting ICA Sessions Automatically” on page 276.

Content Publishing. This feature lets you publish document files, media files, Web URLs, and any other type of file from any network location. Icons for published content appear in Program Neighborhood, on the desktop, and in NFuse. Users can double-click published content icons to access content in the same way they access published applications.

For more information, see “Publishing Content” on page 258.

Connection control. This feature lets you set a limit on the number of connections that each user can have simultaneously in the server farm. You can also limit the number of concurrent connections to specified published applications, and you can prevent users from launching more than one instance of the same published application.

For more information, see “Controlling User Connections” on page 266.

Prioritizing CPU access by applications. You can use the CPU prioritization feature to assign each published application in the server farm a priority level for CPU access. This feature can be used to ensure that CPU-intensive applications in the server farm do not degrade performance of other applications. You can give a higher CPU priority to mission-critical published applications and a lower CPU priority to less-important applications.

For more information, see “Setting CPU Priority Levels for Applications” on page 262.

Universal printer driver. The new Citrix Universal Print Driver is included with Feature Release 1. This driver can be installed in the server farm and used as the driver for all printers that users running the ICA Win32 Client print to in the server farm. The Universal Print Driver eliminates the need to install many separate printer drivers for diverse printing environments.

For more information, see “Using the Citrix Universal Print Driver” on page 304.

NDS Support. Support for Novell Directory Services allows users in Novell network environments to log on using their NDS credentials to access applications and content published in MetaFrame XP server farms.

For more information, see “Using Citrix Management Console” on page 166.

SSL support for ICA. This feature enables use of the Secure Sockets Layer (SSL) protocol to secure communication between ICA Clients that support SSL and MetaFrame XP servers. SSL provides server authentication, encryption of the data stream, and message integrity checks. After configuring the Citrix SSL Relay, you can specify the use of SSL when you publish applications.

For information about configuring clients for SSL, see the *ICA Win32 Client Administrator's Guide*. For information about server configuration of the Citrix SSL Relay, see “Setting Up Citrix SSL Relay” on page 182.

Web-based administration. You can install the new Citrix Web Console on MetaFrame XP servers that have Internet Information Services 5.0 or later installed. You can then monitor MetaFrame XP server farms from any workstation with a supported Web browser. The Citrix Web Console lets you view information about the server farm, published applications, servers, and active sessions, and lets you reset, disconnect, and shadow ICA sessions and send messages to users.

For more information, see “Using Setup” on page 128 and the online help available from the console.

MetaFrame XPe components. Feature Release 1 includes enhancements to Citrix Resource Manager, Citrix Installation Manager, and Citrix Network Manager, which are part of MetaFrame XPe.

For feature descriptions and configuration information, refer to the documentation in the DOCS directory of the Feature Release 1-Service Pack 1 CD-ROM.

ICA session monitoring. New performance counters for ICA data let you use the Windows Performance Monitor to monitor ICA communication, including bandwidth and compression for sessions, servers, and individual virtual channels, and latency in ICA sessions. Performance monitoring can provide valuable information about utilization of network bandwidth and help determine if a bottleneck exists.

For more information, see “Monitoring Performance of Sessions and Servers” on page 288.

Citrix Management Console improvements. More detailed information about servers and licensing now appears in the Citrix Management Console. For example, the Licensing Summary tab now shows the name of feature releases that you install, the number of servers set up to use feature releases, and the feature release licenses that are installed in the server farm.

For more information, see “Viewing Feature Release License Information” on page 154. For information about all new options in Citrix Management Console, see the console’s online help.

Extended Parameter Passing. With Feature Release 1, you can associate a file type on a client device with an application published on a Citrix server. When a user double-clicks a local file, the ICA Client passes the file path as a parameter to the Citrix server. The Citrix server retrieves the file and opens it with the associated application in an ICA session. For more information, see “Associating Published Applications with File Types” on page 251.

Version 6.20 of the ICA Win32 Client was included with Feature Release 1 for MetaFrame XP. The following are brief descriptions of new features in that release.

For more information about features and improvements included in the ICA Clients that shipped with Feature Release 1, refer to the *ICA Client Administrator's Guides*, which are in the Doc folder on the MetaFrame XP Components CD-ROM.

Citrix Program Neighborhood Agent. The Citrix Program Neighborhood Agent lets you leverage Citrix NFuse to deliver published applications directly to users’ desktops, so users can access links to published applications with or without a Web browser. With the Program Neighborhood Agent, links to NFuse-enabled published applications appear in the Start menu, on the Windows desktop, or in the Windows System Tray. Remote applications are integrated into the desktop and appear to the user as local applications.

SSL support for ICA. Citrix SSL Relay secures data communications using the Secure Sockets Layer (SSL) protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks. You can now use Citrix SSL Relay to secure communications between an SSL-enabled ICA Win32 Client and a MetaFrame server.

Windows Installer Packages for ICA Win32 Clients. The ICA Win32 full Program Neighborhood Client and the Program Neighborhood Agent are now available in Microsoft Windows installer packages (.msi files), which you can deploy with Windows Installer technology.

New Features in MetaFrame XP

The following are new or significantly enhanced features in MetaFrame XP 1.0. For information about Feature Release 1, see “Features Included in Feature Release 1” on page 38. For information about Feature Release 2, see “Features Included in Feature Release 2” on page 33.

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 does 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 farm-wide connection license pooling among IMA-based MetaFrame 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 coexist 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 for MetaFrame XP Deployment



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

System Requirements

This section describes minimum configurations and recommendations for installing MetaFrame XP on servers. For information about system requirements of ICA Client devices, see the *ICA Client Administrator's Guide* for each client platform.

System Software Requirements

Feature Release 2 of MetaFrame XP is supported on Windows 2000 Servers with Service Pack 2 installed.

Important Feature Release 2 is not supported on Windows NT Server 4.0, Terminal Server Edition.

You can install MetaFrame XP, up to Feature Release 1, 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. Citrix recommends that you install the latest Microsoft service pack for the operating system.

Important You must install the Terminal Services component before you install MetaFrame XP. Terminal Services is not installed with Windows 2000 by default; you can install it with Add/Remove Programs in Control Panel. Install Terminal Services in Application Server mode.

CAUTION To use the Novell Client with MetaFrame XP on Windows NT Server 4.0, Terminal Server Edition, you must install the Novell Client and restart the system before installing MetaFrame XP.

Viewing Citrix Documentation

To access the documentation in Adobe Acrobat PDF files, you need Adobe Acrobat Reader 4 or later. Acrobat Reader lets you view, search, and print the documentation. You can download Acrobat Reader at no cost from Adobe System's Web site (<http://www.adobe.com>). The self-extracting file includes installation instructions.

Requirements for Citrix NFuse Classic

To install NFuse Classic on a MetaFrame XP server, Microsoft Internet Information Services (IIS) Version 5.0 or higher and the Microsoft Java Virtual Machine (JVM), included with IIS, must be installed before you install MetaFrame XP.

Naming Servers and Server Farms

You assign a name to your MetaFrame XP server farm when you install MetaFrame XP on the first server in the farm. The server farm name can contain 32 or fewer characters. Server farm names are case-sensitive.

For a MetaFrame XP server farm to operate in mixed mode with an existing MetaFrame 1.8 server farm, you must assign the name of the MetaFrame 1.8 server farm when you create the MetaFrame XP server farm.

MetaFrame server names must be unique, whether the servers are in MetaFrame XP server farms or in mixed-mode MetaFrame XP and MetaFrame 1.8 server farms. If necessary, change the name of a server before installing MetaFrame XP.

Important MetaFrame XP supports server names that contain extended characters only if your network's DNS server supports names with extended characters.

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 166MHz 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 cannot 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, use the following guidelines for MetaFrame XP:

- 250MB disk space for installing the MetaFrame XPe family level
- 150MB disk space for installing all ICA Client software

Modems and Multiport Adapters

In addition to ICA connections over network protocols (see “Configuring Network ICA Connections” on page 117), 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. When 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, Windows 2000, or Windows XP computer. You can install the console on your MetaFrame and MetaFrame XP servers, but the console does not require that MetaFrame XP be installed on the same computer.

Sun Java Runtime Environment (JRE). The console is a Java application and requires the Sun JRE Version 1.3.0. If your system does not have the JRE, Setup installs Version 1.3.0, the version required to run the console. The console does not run on JRE Version 1.3.1. If you have this version of the JRE installed on the target system, you must uninstall it before installing the Citrix Management Console.

Note If you are installing the console on a Windows NT 4.0 workstation, you may need to install the latest version of the Windows Installer, available from the Microsoft Web site.

Disk space. A minimum of 50MB of disk space is required for installation of Citrix Management Console and the Java Run-Time Environment.

Memory. A minimum of 64MB of RAM is needed 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.

Note For information about requirements for the Citrix Web Console, see “Using Setup” on page 128.

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.

Note More information about system sizing, optimization, configuration, and deployment scenarios is available in the *Advanced Concepts for MetaFrame XP*. The guide is available from the Support area of the Citrix Web site at www.citrix.com/support. Select Product Documentation.

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-1), Fast Wide SCSI, Wide Ultra SCSI, and Wide Ultra1 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.

Resource and network management and monitoring features are included with MetaFrame XPe. Updated documentation for these components of MetaFrame XPe is included in the Docs directory on the MetaFrame XP CD.

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.

For information about performance-monitoring counters available for monitoring ICA and MetaFrame XP servers, see “Monitoring Performance of Sessions and Servers” on page 288.

Choosing a Database for the Data Store

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

MetaFrame XP is compatible with the following database software:

- **Microsoft Access.** Access is a lightweight database that is included with Windows server operating systems. The Access database is created on the first MetaFrame XP server in a new server farm. It is most appropriate for small to mid-size server farms.
- **Microsoft SQL Server.** 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.** 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.
- **IBM DB2.** DB2 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.

When using Microsoft Access, the database is created when you run MetaFrame XP Setup. The database is stored on the first MetaFrame XP server in the farm.

When using Microsoft SQL Server, Oracle, or IBM DB2, the database is on a server dedicated to running the database product. This dedicated server must be set up prior to creating the server farm because you will need to configure an ODBC connection to it. MetaFrame XP servers must also have the appropriate database client software installed on them.

You should consider many factors before you decide which database product to use for your server farm's data store, including but not limited to:

- The number of MetaFrame XP servers you currently plan to have in the server farm and whether you plan to expand the number of servers in the farm
- Whether you have a database administrator on staff with the expertise to configure and manage a data store running on SQL Server, Oracle, or DB2
- Whether you foresee the organization expanding, and therefore expanding the number and type of published applications
- Whether the database can sustain an increase in the number of users and connections
- Whether a MetaFrame server has the appropriate hardware configuration to also run an Access database or whether you require that the database be located on a server that is not also running MetaFrame XP
- Any database maintenance requirements you may have, such as backup, redundancy, and replication

Important Microsoft SQL, Oracle, and IBM DB2 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 about supported database and ODBC driver versions, see “Data Store Database Requirements” on page 52.

CAUTION Do not install MetaFrame XP on the Microsoft SQL, Oracle, or IBM DB2 database server. Refer to your database product’s documentation for specific hardware requirements for the database server.

System Sizing for the Data Store Database

The choice of which database to use for your MetaFrame XP server farm’s data store depends greatly on your implementation and environment.

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
Servers	1-50	25-100	50-100	100 or more
Named Users	< 150	< 3000	< 5000	> 3000
Applications	< 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, Oracle, and IBM DB2 are suitable for any size environment and are especially 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.

Connecting to the Data Store

After you decide which database to use for the data store, decide whether MetaFrame XP servers will connect directly to it 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 MetaFrame 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 Server database eliminates the need to install and configure the ODBC drivers on every MetaFrame XP server. If you are using an SQL Server 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.

Important If you recreate the server farm's data store database, a Citrix administrator account with full administration rights is created using the local administrator account credentials. Be sure to create a new Citrix administrator with full administration rights in Citrix Management Console. Doing so replaces the default Citrix administrator account that uses the local administrator credentials.

Be sure to back up any database before you attempt to recreate it.

Data Store Database Requirements

You can use the Microsoft Access database engine or a Microsoft SQL Server, Oracle, or IBM DB2 database for the server farm's data store. The supported ODBC drivers and database versions are listed below.

Microsoft Access

Choosing **Use a local database (Microsoft Access) on this server** during MetaFrame XP Setup creates a Microsoft Access database on the MetaFrame server. This database acts as the server farm's data store.

The Microsoft Access database engine and ODBC drivers are default components of Windows 2000 Servers. The ODBC connection to Access uses the Microsoft Jet Engine. To use the database engine, you do not have to install any drivers or perform any database configuration prior to MetaFrame XP installation.

Minimum Requirements

The MetaFrame XP server that hosts the Access database should meet the following minimum requirements:

- Approximately 50MB of disk space for every 100 servers and 25 applications in the farm
- 32MB of additional RAM if the MetaFrame XP server will also host connections

Authenticating to the Access Database

If you decide to create a local Access database on the MetaFrame XP server, MetaFrame Setup creates a database called “mf20.mdb.” The default user name and password for this database file are “citrix/citrix.”

You can use the **Dsmaint** command (dsmaint config /pwd:newpassword) to change the password on the database. The Citrix IMA Service can be running when you use the command. Keep the new password in a secure place so you can access it if you want to migrate to another database.

Important Be sure to back up the Access database using the **Dsmaint** command (dsmaint backup) before changing the password used to access the database.

For more information about MetaFrame XP commands, see “MetaFrame XP Commands” on page 309.

Microsoft SQL Server

MetaFrame XP supports the following versions of Microsoft SQL Server for the server farm’s data store.

Microsoft SQL Server 7. Microsoft SQL Server 7 with Service Pack 2 or Service Pack 3 is supported on Windows NT 4.0 Server and Windows 2000 Server Family.

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, install Microsoft Data Access Components (MDAC) Version 2.6 with Service Pack 1, which can be downloaded for free from Microsoft's download site. Do not use MDAC 2.6 without Service Pack 1.

Important On Windows NT 4.0, TSE systems, stop the Terminal Services Licensing Service before installing MDAC. After installing MDAC, clear the event log, then restart the server before installing MetaFrame XP.

Microsoft SQL Server 2000. Microsoft SQL Server 2000 is supported on Windows NT 4.0 Server and the Windows 2000 Server family.

On Windows NT 4.0 Server, Windows NT Service Pack 5 (SP 5) or later must be installed for all SQL Server 2000 editions.

The following configurations have been verified by Citrix testing:

- MDAC 2.5, Windows 2000 Server, SQL Server 2000
- MDAC 2.51, Windows 2000 Server with SP1 or SP2, SQL Server 2000
- MDAC 2.51, Windows 2000 Server with SP1 or SP1, SQL Server 2000 with SP1
- MDAC 2.6 SP1, Windows 2000 Server with SP1 or SP2, SQL Server 2000 with SP1

Important MDAC 2.6 without SP1 is not supported because of an issue with the driver.

Minimum Requirements

The practices outlined in this section are suggested practices for using Microsoft SQL Server as the data store. Be sure to read the Microsoft SQL Server documentation before you install and configure Microsoft SQL Server.

The following minimum requirements can apply to MetaFrame XP implementations that use SQL Server as the farm's data store:

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- Set the "temp" database to automatically grow on a partition with at least 1GB of free disk space. 4GB is recommended if the MetaFrame server farm is large and includes multiple print drivers.

Note Make sure that enough disk space exists on the server to support growth of both the “temp” database and the data store database.

Authenticating to the Microsoft SQL Server Database

Consider the following issues when planning authentication to the SQL Server database:

- Microsoft SQL Server supports Windows NT and Microsoft SQL Server authentication. Consult the Microsoft SQL Server documentation for configuring Windows NT authentication support. For high-security environments, Citrix recommends using Windows NT authentication only.
- The user account used for connecting to the data store must have database owner (“db_owner”) rights to the database.
- When you are done installing the database with database owner rights, set the user permissions to read/write only. Doing this increases the security of the database.

Important If you change the rights from database owner to read/write, be sure to change the rights back to database owner before you attempt to install MetaFrame XP service packs or feature releases. Installation of MetaFrame service packs or feature releases can fail if the user account you use to authenticate to the data store during Setup does not have database owner rights.

Migrating to SQL Server

Migration of a MetaFrame XP server farm data store to Microsoft SQL Server is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 330.

Original platform	Target platform
Microsoft Access	SQL Server 7 with SP3
Microsoft Access	SQL Server 2000
Microsoft Access	SQL Server 2000 with SP1
Oracle 8.1.6	SQL Server 2000 with SP1
Oracle 8.1.7	SQL Server 2000 with SP1
Oracle9i	SQL Server 2000 with SP1
IBM DB2 with FixPak 5	SQL Server 2000 with SP1

Oracle

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

- Oracle9i, Enterprise Edition Database Release 1
- Oracle8i, Version 8.1.6 and 8.1.7
- Oracle 8, Version 8.0.6
- Oracle 7, Version 7.3.4

If you are using Oracle 8, install the Oracle Net8 client Version 8.1.5.5 or later and ODBC drivers provided by Oracle on each MetaFrame XP server that will directly access the database server. The MetaFrame farm's data store is stored as an object (schema) assigned to a user. You do not need a separate database for each data store.

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.

In some cases you will need to configure the DNS entry within the Oracle Net8 Assistant. To do this, click **Profile** and then select the **Oracle Names** tab. Enter the DNS suffix that the network is using. You can use the command `IPCONFIG /ALL` to gather the DNS suffix that must be used.

If you do not restart the server after you install the Oracle client, or if the client requires the DNS suffix to be specified, MetaFrame XP Setup reports the following error: "The procedure entry point OCIUnicodeToCharSet could not be located in the dynamic link library OCI.dll."

If you are using Oracle9i, install the Oracle9i Administrator client to obtain the Oracle ODBC driver Version 9.0.1.0.1. The Oracle9i Run-time client does not have ODBC driver support, which is required on each MetaFrame XP server that will directly access the database server.

Minimum Requirements

The practices outlined below are suggested practices for using an Oracle database for the server farm's data store. Be sure to read the Oracle documentation before you install and configure Oracle databases.

The following minimum requirements can apply to MetaFrame XP implementations that use Oracle as the farm's data store. Guidelines given here apply to Oracle7, Oracle8, and Oracle8i, except as noted otherwise.

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- The Oracle Client (Version 8.1.55 or later) must be installed on the MetaFrame server before you install MetaFrame XP. The 8.1.5 client is not supported with MetaFrame XP.

Authenticating to the Oracle Database

Consider the following issues when planning authentication to the Oracle database:

- Oracle for Solaris supports Oracle authentication only; it does not support Windows NT authentication.
- Oracle for Windows NT supports both Windows NT and Oracle authentication. Consult the Oracle documentation for information about configuring Windows NT authentication.
- The Oracle user account must be the same for every server in the farm because all servers share a common schema.
- If you are using one database to hold information for multiple MetaFrame XP farms, each farm represented in the database must have a different user account. This is because the data store information is stored in the Oracle user account's schema.
- The account used to connect to the data store database must have the following Oracle permissions:
 - Connect
 - Resource
 - Unlimited Tablespace (optional)

Migrating to Oracle

Migration of a MetaFrame XP server farm data store to an Oracle database is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 330.

Original platform	Target platform
Microsoft Access	Oracle 7
Microsoft Access	Oracle 8
Microsoft Access	Oracle 8.1.6
Microsoft Access	Oracle 8.1.7

Original platform	Target platform
Microsoft Access	Oracle9i
Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)	Oracle 7
Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)	Oracle 8
Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)	Oracle 8.1.6
Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)	Oracle 8.1.7
Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)	Oracle9i
IBM DB2 with FixPak 5	Oracle 7
IBM DB2 with FixPak 5	Oracle 8
IBM DB2 with FixPak 5	Oracle 8.1.6
IBM DB2 with FixPak 5	Oracle 8.1.7
IBM DB2 with FixPak 5	Oracle9i

IBM DB2

MetaFrame XP supports IBM DB2 Universal Database Enterprise Edition Version 7.2 for Windows 2000 with FixPak 5 for the server farm's data store.

Important MetaFrame XP uses the data type of binary large object (BLOB) to store information in an IBM DB2 database. IBM DB2 does not support the use of BLOB data types in an updateable replication scenario. Therefore, if your server farm needs to have updateable replicas, use Microsoft SQL Server or Oracle for the farm's data store instead of IBM DB2.

Install the IBM DB2 Run-Time Client and apply FixPak 5 on each MetaFrame XP server that will directly access the database server. If you have multiple MetaFrame XP farms, create a separate database/tablespace for each farm's data store.

Important Restart the system after you install the IBM DB2 Run-Time client and FixPak5 and before you install MetaFrame XP. You may also need to restart after you install the Run-Time client and before you install FixPak 5. See the DB2 documentation for more information.

Minimum Requirements

The practices outlined below are suggested practices for using an IBM DB2 database for the server farm's data store. Be sure to read the DB2 documentation before you install and configure DB2 databases.

The following minimum requirements can apply to MetaFrame XP implementations that use DB2 as the farm's data store.

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- If you create a data source name (DSN) for use with an unattended installation of IBM DB2, Citrix recommends that you create the DSN using the Microsoft ODBC Data Source Administration screen. Doing so ensures that the DSN is populated according to MetaFrame requirements for proper connectivity to the DB2 database or tablespace.

Migrating to IBM DB2

Migration of a MetaFrame XP server farm data store to an IBM DB2 database is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 330.

Original platform	Target platform
Microsoft Access	IBM DB2 with FixPak 5
Microsoft SQL Server 2000 with SP1	IBM DB2 with FixPak 5
Oracle 7	IBM DB2 with FixPak 5
Oracle 8	IBM DB2 with FixPak 5
Oracle 8.1.6	IBM DB2 with FixPak 5
Oracle 8.1.7	IBM DB2 with FixPak 5
Oracle9i	IBM DB2 with FixPak 5

The migration of an existing MetaFrame XP server farm data store to IBM DB2 is completed as a single transaction for roll-back purposes. Before migrating the database to DB2, verify that enough log space exists on the target DB2 server to support the migration. If the DB2 server runs out of log space, the migration will fail and roll back.

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 (non-Active Directory) and Active Directory domains and groups
- Security models and user access to applications
- Configuration of accounts for Citrix administrators
- Working with Novell Directory Services

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.
- MetaFrame XP Setup 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 61.

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, logging in using the User Principal Name (UPN) is not permitted for Program Neighborhood filtering. In addition, Citrix administrators cannot use a UPN to log on 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 Active Directory forest. If your server farm has MetaFrame XP servers in more than one forest, users cannot log on using UPNs.

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 who are no longer eligible to use the resource from the authorized users list.

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 cannot 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 account 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 to which network users can belong. 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 non-Active Directory 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 is 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 about user access issues and configuration issues, see “User Permission Scenarios with Active Directory” on page 64.

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 about 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
Domain Global Groups	No adverse effects	No adverse effects	No adverse effects
Domain Local Groups	<p>Recommendation: All servers in the farm must be in the same domain for Program Neighborhood filtering to work properly.</p> <p>Rationale: If a user is a member of a domain local group, the group is present in the user's security token only when logging on to a machine in the same domain as the domain local group. Trust-based routing (see page 62) 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>Recommendation: 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>Rationale: 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). 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>Recommendation: 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>Rationale: 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
Universal Groups	<p>Recommendation: No Active Directory domains in the forest to which the servers belong have explicit trust relationships with non-Active Directory domains.</p> <p>Rationale: Non-Active Directory 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>Recommendation: If universal groups are assigned permission to the application, all servers that manage the application must be in an Active Directory domain.</p> <p>Rationale: A server in a non-Active Directory 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 non-Active Directory domain to load balance an application with servers in an Active Directory domain if the domains have an explicit trust relationship.</p>	<p>Recommendation: 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>Rationale: Non-Active Directory domain controllers and domains outside a universal group's forest have no information about the universal group.</p>

Supporting Novell Directory Service Users

MetaFrame XP supports user authentication through Novell Directory Service (NDS).

NDS offers access by a secure logon and organizes network resources in a directory tree for administration. When an NDS tree is designated on a server farm, the tree is accessed directly for NDS user account information.

MetaFrame XP servers used for NDS applications need the Novell Client installed. Dedicate servers with the Novell Client to applications for NDS objects after NDS is enabled for a server farm. Do not host published applications assigned to Windows NT, Windows 2000, or Active Directory users on these servers. The server farm can be a mixture of servers used exclusively for NDS applications and other servers.

A Citrix administrator must have NDS credentials to manage applications and printers for NDS objects and to assign Citrix administrator privilege to NDS objects. To administer applications on a server dedicated to NDS, you must connect Citrix Management Console to a server that has Feature Release 1 or higher.

The following table lists NDS terms used in this section and their meanings:

Term	Meaning
Tree	A set of objects set up hierarchically in a tree structure. The root object of the NDS tree is at the top of the tree.
Container object	The tree may or may not branch to these NDS Container objects: <i>Country</i> (a country location for this part of the organization) <i>Organization</i> (a company, university, or departmental unit) <i>Organizational Unit</i> (a business unit, division, or project team)
Common Name	The name for a leaf object on the tree. Examples of leaf objects are: users, groups, servers, and printers.
Context	An object's position in the tree. One way to represent context is by a string of the Common Names of the objects in the path from the leaf or container object to the root.
Distinguished Name	A combination of an object's common name and its context that makes up a complete NDS path for an object. A full Distinguished Name (DN) starts with a period, for the root, and has a period between each object name.

Setting up Support for NDS

For MetaFrame XP to access NDS on Novell servers, one of the following must be installed:

- NDS Version 8.73 for NetWare 5.1
- NDS for eDirectory Version 8.5x for Windows NT 4.0, Windows 2000 Server, or NetWare 5.x

The minimum MetaFrame server software requirements are:

- Novell Client Version 4.8
- MetaFrame XP Feature Release 1 or higher

If you are setting up a server that does not yet have MetaFrame installed, install the Novell Client before you install MetaFrame XP and Feature Release 1. If the client is already installed, refer to the procedure below for information about specifying the correct logon.

Important If you install the Novell client on a MetaFrame XP server, set the following value in the [386Enh] section of the System.ini file before you install MetaFrame XP:

FileSysChange=off

Make this change in System.ini for all users. If this parameter is not set correctly, the MetaFrame XP installer reports that the FileSysChange parameter is not valid.

Novell technical document 10058117 refers to this issue. Please see the Novell knowledgebase on the Web at http://support.novell.com/search/kb_index.jsp for more information.

► **To change the registry on a server when the Novell Client is installed**

If MetaFrame XP is installed before you install the Novell client, you need to change registry settings on the server before and after you install the Novell Client.

CAUTION Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Make sure you back up the registry before you edit it. If you are running Windows NT, make sure you also update your Emergency Repair Disk.

1. Before installing the Novell Client, run **regedt32**.
2. Edit the registry under:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Winlogon

Double-click **GinaDLL**. In the **String Editor** window that pops up, type **Msgina.dll**, a new value for the GinaDLL entry.
3. Install the Novell Client **without rebooting** when prompted.
4. Edit the registry entry for **GinaDLL** as in Step 2. This time type **Ctxgina.dll** as the value.
5. With the key path for Winlogon still selected, click **Edit** on the top menu bar.
6. Click **Add Value**.
7. Type **ctxGinaDLL** in the **Add Value** dialog box. Data Type is REG_SZ.
8. Type **nwgina.dll** in the **String Editor** window. This is the new value for the new ctxGinaDLL entry.

9. Restart the server.

► **To enable or disable NDS support for a server farm**

NDS support is disabled for a server farm by default. Feature Release 1 supports one NDS tree per farm.

1. Connect to a server that has Feature Release 1 or higher and the Novell Client installed, using a Feature Release 1 or higher Citrix Management Console.
2. Right-click the farm node at the top of the tree and choose **Properties**.
3. Click the **MetaFrame Settings** tab.
4. To enable or disable NDS support, do either:
 - Enter the NDS tree name in the **NDS Preferred Tree** field
 - Clear the NDS tree name in the **NDS Preferred Tree** field
5. Click **OK**.

► **To assign Citrix administrator privileges to NDS objects**

A Citrix administrator can assign Citrix administrator privileges to objects in an NDS tree, such as a country, organization, organization unit, group, user, or an alias.

1. Right-click Citrix Administrators in Citrix Management Console and click **Add a Citrix Administrator**.
2. In the **Add Citrix Administrator** dialog box, double-click to open the NDS tree. Objects in the NDS tree represent container objects and leaf objects.
3. Select the **Show Users** box to see the user and alias objects in this hierarchy.
4. Double-click to open container objects until the object that you want to add to the Citrix Administrator list is in the dialog box. Select this object.
5. Click **Add**. Assign the tasks you want the Citrix administrator to be able to perform. Click **OK**.

This object and those below it have the selected Citrix administrator privileges.

► **To log on to Citrix Management Console as an NDS user**

You need a Distinguished Name, password, and NDS tree name to perform the following steps. If you don't have this information, consult the Novell or Citrix administrator who set up the NDS object to have Citrix administrator privileges.

1. Type a Distinguished Name in the **User Name** field. A full Distinguished Name starts with a period and has a period between each object name.

For example, User JoeX, within two container objects (the Admin organization unit within the PNQ organization) would type the following Distinguished Name in the User Name box:

.JoeX.Admin.PNQ

2. Type the password in the **Password** box.
3. Type the NDS tree name in the **Domain** box.

► **To publish an application for NDS users**

1. Log on to Citrix Management Console as an NDS user.
2. Verify that the intended host server has the Novell Client installed.
3. From the **Actions** menu, choose **New > Publish Application**.
4. Follow the instructions in the Publish Application wizard. Click **Help** to obtain detailed help for each step.
5. In the **Specify Users** dialog box of the Publish Application wizard, double-click to open the NDS tree.
6. Double-click to open container or leaf objects until the object to be granted access is in the window.
7. Select the object and click **Add**. Click **Finish**.

The object and those under it now have access to the application.

Configuring Printer Auto creation in NDS

Citrix Management Console can be used to choose Windows NT or Active Directory print queues and assign them to NDS objects for auto-creation. Print permissions to the queue must be granted to the Dynamic Local User created when the NDS user logs onto a server. This may involve enabling the Guest account on the print server. See Microsoft documentation for information about enabling the Guest account.

NDPS print queues cannot be chosen and assigned to NDS objects through Printer Management in Citrix Management Console. Consult Novell documentation for setting up NDPS print queues in ZENworks.

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. Citrix recommends that you restart the IMA service only during off-peak hours when the load on the servers is very low.

Configuring Citrix Administrator Accounts

Citrix administrators manage MetaFrame XP server farms. You can create Citrix administrator accounts with the following permission levels:

- Full administration rights to all areas of MetaFrame XP server farm management.
- View only access to all areas of server farm management.
- Mixed levels of access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.

When you install the first MetaFrame XP server in a new server farm, you specify an initial farm administrator. This user account is automatically configured as a Citrix administrator with full administration rights in Citrix Management Console.

To give other user accounts access to the console, a Citrix administrator with full administration rights logs on to the console and creates other Citrix administrator accounts. The level of permission for various areas of farm management depends on the specific business function of the administrator. For example, your system or network administrators may need complete access to all areas of farm and server management, while help desk personnel may need only view access to most areas.

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

When you create a Citrix administrator account for a user, you can grant or deny access to specific MetaFrame XP tasks, such as disconnecting users, or to an entire area of server farm management, such as managing sessions. You can create specialized Citrix administrators with the permission level to carry out specific tasks without granting these administrators full access to all areas of farm management.

For more information about delegating administration rights to Citrix administrators, see “Configuring Citrix Administrator Accounts” on page 162.

Note One Citrix administrator account with full administration rights must always exist in the server farm. MetaFrame prevents you from deleting the last Citrix administrator account with this level of permission. 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 MetaFrame XP 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 Classic 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

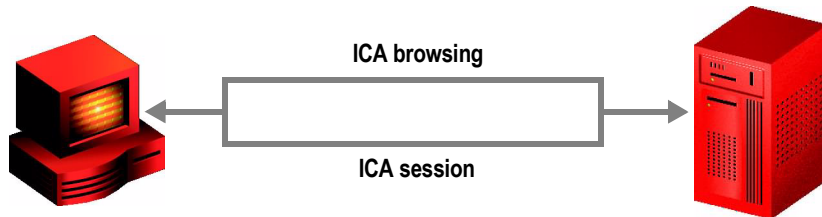
The first part of this section focuses on MetaFrame XP. For information about communication issues with MetaFrame XP and MetaFrame 1.8, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 86.

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 and later ICA Win32 Client features and server farm configuration with this client. For information about 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.



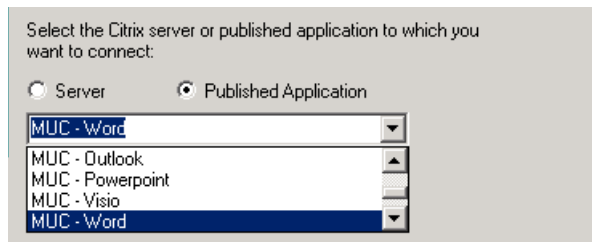
ICA Browsing

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 75.

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.

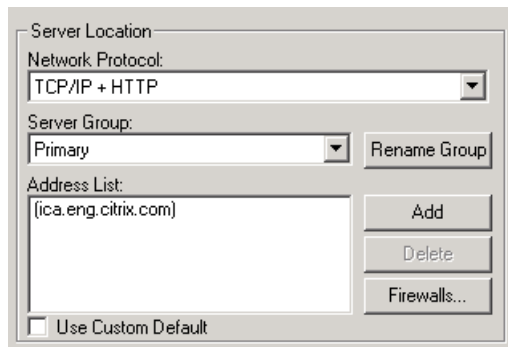
Important MetaFrame XP does not support multiple farms on the same subnet configured to respond to Master Browser requests.

Server Location Settings

The method that ICA Clients use for ICA browsing depends on the specified server location settings. Users running Program Neighborhood can configure server location settings using the Program Neighborhood user interface.

- 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.

The screenshot shows a dialog box titled "Server Location". It contains several fields and buttons. At the top, there is a "Network Protocol:" label followed by a dropdown menu currently showing "TCP/IP + HTTP". Below this is a "Server Group:" label followed by a dropdown menu showing "Primary" and a "Rename Group" button. Underneath is an "Address List:" label followed by a text box containing "(ica.eng.citrix.com)". To the right of the text box are three buttons: "Add", "Delete", and "Firewalls...". At the bottom left, there is a checkbox labeled "Use Custom Default" which is currently unchecked.

Note Some ICA Clients do not use ICA browsing and connect only to specified servers. The options described in this section are for the ICA Win32 Client. For information about other server location options, see the *Citrix ICA Client Administrator's Guides* 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 **Address List** box. 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 the Citrix 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.

You can use two configurations 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 about mixed mode operation, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 86. For information about data collectors, see “Configuring Zones and Data Collectors” on page 179. For information about configuring server response to broadcasts, see “Setting up Response to ICA Client Broadcasts” on page 174.

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 Classic 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.

If you intend to send NFuse data over a secure HTTP connection using SSL, be sure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

Note Port 80 is the default port for HTTP communication with Web servers. The Citrix XML Service includes an Internet Server Application Programming Interface (ISAPI) extension that you can plug into Internet Information Services (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 about configuring the XML Service port number, see “Configuring the Citrix XML Service Port” on page 117. For information about configuring the port that NFuse uses, see 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.

Using DNS Address Resolution

ICA Client browsing requests normally generate an IP address for connecting to MetaFrame servers. You can configure MetaFrame XP servers to respond with the fully qualified domain name (FQDN). This feature, called Domain Name System (DNS) address resolution, is available to clients using the Citrix XML Service.

MetaFrame XP servers reply with an IP address as the default. You can change the default setting, which applies to the entire server farm, in Citrix Management Console. In most situations, use of IP addresses works well and with less overhead. Depending on the situation and network configuration, it could be useful to set up servers to respond to client browsing requests with FQDNs.

For ease of administration, ICA Clients have a client file that is already configured to request FQDNs if DNS addressing is enabled in the server farm. ICA Clients connecting through NFuse request IP or DNS addresses based on a line in a Web server configuration file. This file is set up for IP addresses initially. Regardless of what ICA Clients are set up to request, unless DNS addressing is enabled for the server farm, IP addresses are returned.

DNS address resolution works only in a native mode MetaFrame XP server farm and you must be using ICA Client 6.20.985 or later.

Important If DNS addressing is enabled, clients cannot connect reliably unless they can resolve the fully qualified domain name of all servers in the server farm. Ping a server with its DNS host name to verify this. Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS address resolution in the server farm.

► **To enable or disable DNS address resolution in a server farm**

1. Open Citrix Management Console.
2. Right-click the farm node at the top of the tree and choose **Properties**.
3. Select the **MetaFrame Settings** tab.
4. Select or clear **Enable DNS address resolution**.
5. Click **OK**.

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

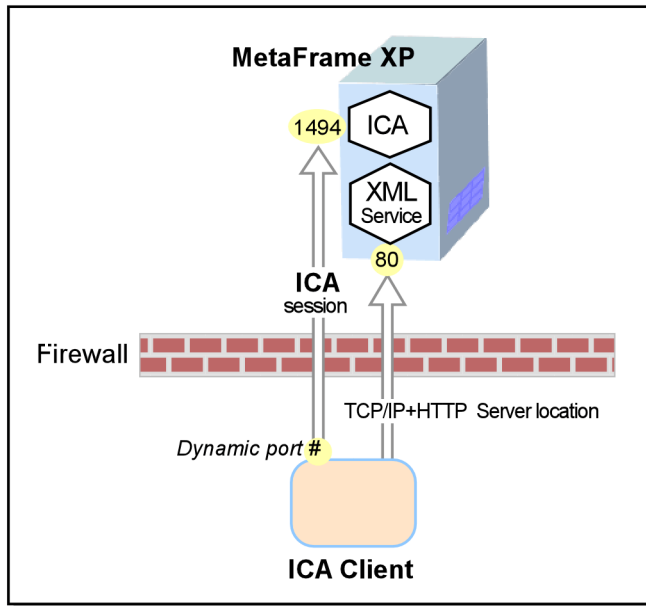
The diagrams below illustrate network configurations for Citrix server farms. The diagrams identify port numbers, components, and the recommended protocol for ICA browsing. See "Configuring ICA Browsing" on page 75 for more information.

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 Citrix 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.

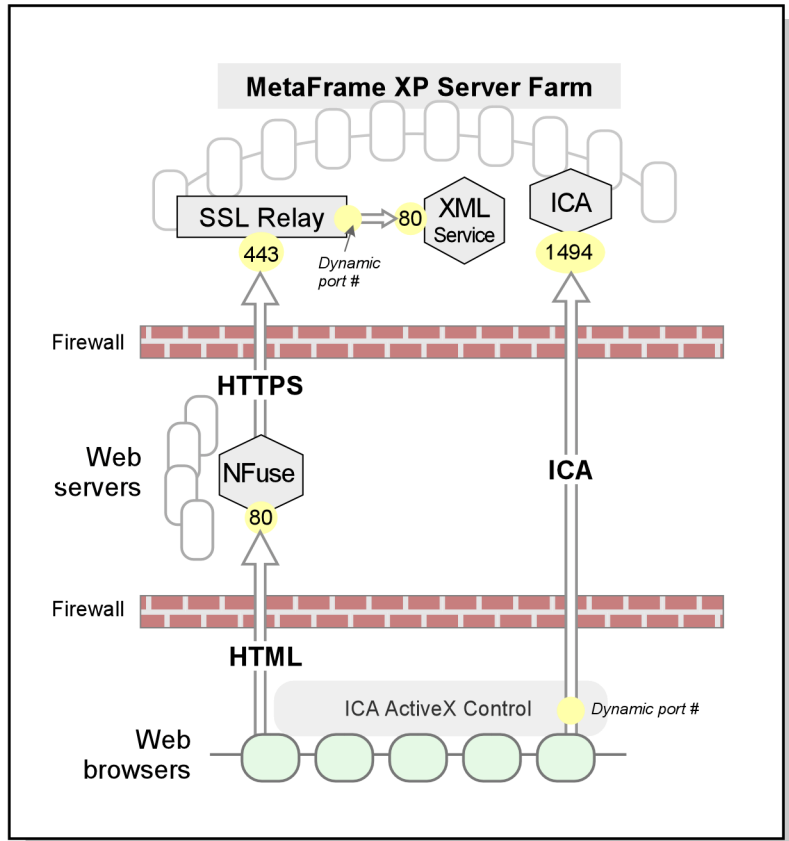
Organizations often place their Web servers in a demilitarized zone (DMZ) between firewalls. In this configuration, shown below, NFuse-enabled Web servers are between firewalls to isolate them from the MetaFrame server farm and ICA Clients.

Communication with NFuse Classic 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.

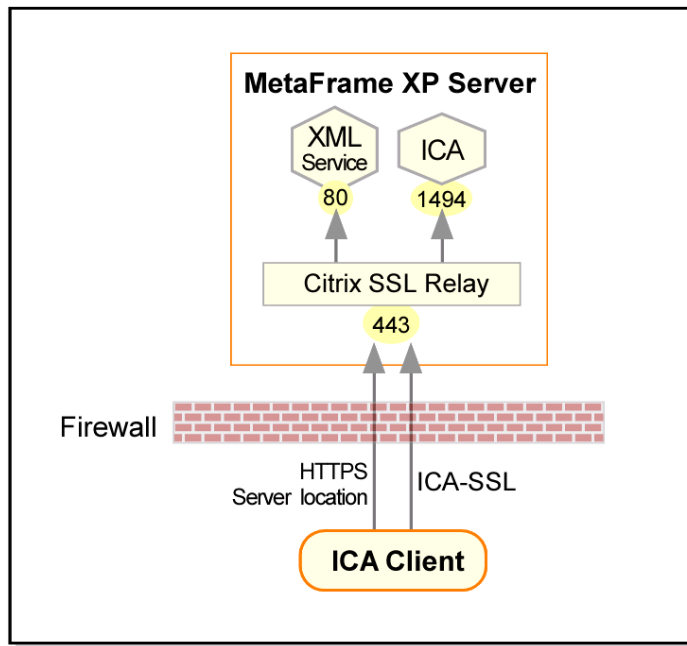
ICA Clients establish ICA sessions with MetaFrame XP servers on port 1494. The port used on the clients is configured dynamically.



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.

Client-to-server communication with SSL

For SSL communication, port 443 is open for inbound communication to the Citrix SSL Relay. The client communicates with the SSL Relay for server location and ICA session communication.



The diagram above illustrates communication between the ICA Client and MetaFrame XP server when SSL encryption is used.

The process of running the application begins with ICA browsing (server location). In this scenario, SSL+HTTPS protocol and server IP addresses are specified for server location in the ICA Client.

1. The client sends an encrypted request to the Citrix SSL Relay on port 443 on a specified server using HTTPS.
2. The SSL Relay decrypts the request and sends it to the Citrix XML Service on port 80.
3. The Citrix XML Service sends the address of a server that has the requested application to the SSL Relay.
4. The SSL Relay encrypts and sends the address of the server to the ICA Client.
5. The ICA Client establishes an SSL-encrypted ICA session with the MetaFrame XP server specified by the Citrix XML Service. ICA packets travel from the client to port 443 on the server and are then decrypted and passed to port 1494. SSL-encrypted ICA packets travel from the server to the client.

Configuring TCP Ports in Citrix Server Farms

The table below lists the TCP/IP ports that MetaFrame XP servers, ICA Clients, IMA, and other Citrix services use in a server farm. This information can help you configure firewalls and troubleshoot port conflicts with other software. The table includes configuration information when you can change default settings.

Communication	Default port	Configuration
ICA sessions (ICA Clients to MetaFrame servers)	1494	See "ICAPORT" on page 334 for instructions about 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	This port must be open on firewalls for inbound packets when ICA Clients use the TCP/IP+HTTP network protocol for server location. See "Configuring the Citrix XML Service Port" on page 117 for configuration instructions.
Citrix SSL Relay	443	See "Changing the SSL Relay Port" on page 187 for configuration instructions.
MetaFrame XP server- to-server	2512	See "MetaFrame XP Commands" on page 309 for information about the IMAPORT command.
MetaFrame XP server to 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	2513	See "MetaFrame XP Commands" on page 309 for information about the IMAPORT command.
ICA Clients to ICA Browser service (UDP)	1604	MetaFrame XP servers always respond to directed UDP requests. See "Setting up Response to ICA Client Broadcasts" on page 174 for enabling MetaFrame XP servers to respond to broadcasts.
Server-to-Server (directed UDP)	1604	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 93.

If you configure a MetaFrame XP server to use mixed mode, two separate farms—one that contains only MetaFrame 1.8 servers and one that contains only MetaFrame XP servers—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 75.

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 Citrix 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.

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 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
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

CAUTION If you intend to change a server's drive letters, do it when you install MetaFrame XP. 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 on to the MetaFrame server after you change the drive letters, references to the old drive letters in the user's profile are updated.

Using Smart Cards with MetaFrame XP

Feature Release 2 of MetaFrame XP includes support for smart cards. Smart cards are small plastic cards with embedded computer chips. Smart cards can contain memory only, memory with security logic, or memory with CPU capabilities, depending on the intended application.

In a business computer network setting, smart cards are an effective implementation of public-key technology and can be used to:

- Authenticate users to networks and computers
- Secure channel communications over a network
- Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published on MetaFrame servers. In addition, smart card functionality within these published applications is also supported.

For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the client device to log on to the MetaFrame server. Once users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix has tested smart cards that meet Standard 7816 of the International Organization for Standardization (ISO) for cards with electrical contacts (known as a contact card) that interface with a computer system through a device called a *smart card reader*. The reader may be connected to the host computer by the serial, USB, or PCMCIA port.

Citrix supports the use of PC/SC-based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card.

In addition, two-factor authentication can be used for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

Note Feature Release 2 of MetaFrame XP does not support RSA Security Inc.'s PKCS (Public-Key Cryptography Standard) #11 functional specification for personal cryptographic tokens.

You can also use smart cards with Citrix NFuse Classic. For details about configuring your NFuse Classic server for smart card support, see the *NFuse Classic Administrator's Guide*, located in the Docs directory on the MetaFrame XP CD.

Software Requirements

The following section presents the basic guidelines for using smart cards with MetaFrame XP. Consult your smart card vendor or integrator to determine detailed configuration requirements for your specific smart card implementation.

The following components are required on the MetaFrame XP server:

- PC/SC software
- Cryptographic Service Provider (CSP) software

These components are required on the device running the supported ICA Client:

- PC/SC software
- Smart card reader software drivers
- Smart card reader

Your Windows server and client operating systems may come with PC/SC, CSP, or smart card reader drivers already present. Please see your smart card vendor for information about whether these software components are supported or must be replaced with vendor-specific software.

If you are using Pass-Through Authentication to pass credentials from your Windows 2000 or Windows XP client computer to the smart card server session, CSP software must be present on the client computer.

You do not need to attach the smart card reader device to your server during CSP software installation if you can install the smart card reader driver portion separately from the CSP portion.

Configuring the Server

A complete and secure smart card solution may be relatively complicated and Citrix recommends that you consult your smart card vendor or integrator for details. Configuration of smart card implementations and configuration of third-party security systems such as certificate authorities are beyond the scope of this documentation.

Smart cards are supported for authenticating users to published applications, or for use within published applications that offer smart card functionality. Only the former is enabled by default upon installation of Feature Release 2 of MetaFrame XP.

To enable support for smart card usage within an application, run the Scconfig.exe command line utility on each MetaFrame XP server that hosts the application. This utility is used to specify the applications (for example, Outlook.exe) that you want to configure to have smart card transactions redirected from the server on which they execute to the client device that hosts the smart card reader. This utility may be executed remotely by specifying a target server according to the syntax below.

```
SCCONFIG /?
```

```
SCCONFIG ([/SERVER:servername] | [/FARM]) ([/QUERY] | [/Q])
```

```
SCCONFIG ([/SERVER:servername] | [/FARM]) [/LOGON:on|off]
[/ENABLE_PROCESS: processname] [/DISABLE_PROCESS:processname]
```

```
SCCONFIG [/SERVER:servername] [/INHERIT:on|off]
```

The parameters used in this utility are explained below.

- The `/?` option returns on-screen help for this utility.
- The `/SERVER:servername` option specifies the target server to configure.
- The `/FARM` option is used to set a farm-wide setting, but will not configure any servers. When the farm-wide setting is set, servers are configured according to the state of the `/INHERIT` option. When MetaFrame is installed on the server, “on” is the default state for `/INHERIT`.
- If neither `/SERVER` or `/FARM` option is specified, the local server is assumed.
- The `/QUERY` or `/Q` option can be used with the `/SERVER` or `/FARM` option to display currently configured settings.
- The `/LOGON` option is used to turn on or off support for smart card authentication during MetaFrame server logon. Upon MetaFrame server installation, “on” is the default state for `/LOGON`.
- The `/ENABLE_PROCESS` and `/DISABLE_PROCESS` options are used to enable or disable support for applications that can take advantage of smart card functionality when run as published applications. For example, to enable support for Microsoft Outlook, the processname would be `OUTLOOK.EXE`.

Setting Windows 2000 Policies for Smart Cards

Windows 2000 supports two security policy settings for interactive logon to a server session. ICA Client sessions can utilize the following policies:

- **Require smart card for interactive session logon.** This policy is a user policy that requires the user to insert a smart card for authentication.

- **Smart-card removal policy.** This policy is a computer policy that has three possible settings to determine the client device behavior when the user removes the smart card from the smart card reader:
 - None (no effect)
 - Lock Workstation (disconnects all MetaFrame user sessions)
 - Log-off Session (logs off all MetaFrame user sessions)

Configuring the Client

The following Citrix ICA Clients support smart cards:

- ICA Client for Windows 32
- ICA Client for Linux
- ICA Client for Windows-based terminals

To configure smart card support for users of these clients, please see the *Administrator's Guide* for the ICA Client or Clients in your environment.

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/>.

New features in feature releases for MetaFrame XP are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8

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 about configuring mixed mode during MetaFrame XP installation, see “Migrating Citrix Servers to MetaFrame XP” on page 121.

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.

Important Make sure users cannot log on to the server farm if you need to change the interoperability mode.

Mixed mode is designed to facilitate migration to MetaFrame XP; it is not designed to be a permanent solution. After all MetaFrame 1.8 servers in the MetaFrame 1.8 farm are 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 is 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 License 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 1 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 License 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 MetaFrame 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 licenses 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 licenses) + (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 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, Setup 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.

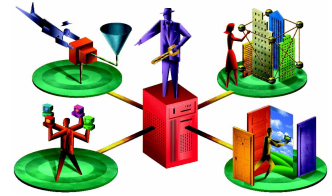
Publishing applications. If you create or edit settings for published applications using the version of Published Application Manager included with MetaFrame XP, you cannot edit or delete the published applications using the version of Published Application Manager from MetaFrame 1.8. Use the version of the utility included with MetaFrame XP or installed with Service Pack 1 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 to read “Planning for MetaFrame XP Deployment” on page 43 before you begin to install MetaFrame XP.

If you are installing MetaFrame XP for the first time, installing MetaFrame from the MetaFrame XP CD-ROM also installs Feature Release 1 and Feature Release 2. If you already installed MetaFrame XP and are preparing to deploy Feature Release 2 or Service Pack 2, see “Deploying Feature Release 2 and Service Pack 2” on page 125 for step-by-step instructions.

Creating the Data Store with SQL Server, Oracle, or DB2

To use Microsoft SQL Server, Oracle, or IBM DB2 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 sections include the basic procedures for creating databases using Microsoft SQL Server, Oracle, or IBM DB2.

If you are setting up your farm to use Microsoft Access, you do not need to read this section and can skip to “Using the MetaFrame XP Windows Installer Package” on page 101. Using a Microsoft Access database involves creating a database locally during the installation of MetaFrame XP on the first server in the farm.

► 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.

► **To create a data store database with IBM DB2**

1. If you do not already have an IBM DB2 database installed, install one using the default database.

2. Create a tablespace for MetaFrame XP using the following DB2 SQL script:

```
CREATE REGULAR TABLESPACE CTXSDB PAGESIZE 4 K MANAGED  
BY SYSTEM USING ('C:\CTXSDB\XPFR1') EXTENTSIZE 32  
OVERHEAD 8.3 PREFETCHSIZE 32 TRANSFERRATE 0.18  
BUFFERPOOL IBMDEFAULTBP  
COMMENT ON TABLESPACE CTXSDB IS ''
```

3. Create a local user account called “XPFR1ADMIN” and then use the following DB2 SQL script to grant this account use of the tablespace:

```
GRANT USE OF TABLESPACE CTXSDB TO USER XPFR1ADMIN WITH  
GRANT OPTION  
  
GRANT USE OF TABLESPACE CTXSDB TO PUBLIC WITH GRANT  
OPTION
```

In the example above, the tablespace is named CTXSDB and saved in C:\CTXSDB\XPFR1\sqltag.nam. The user is named XPFR1ADMIN.

Using the MetaFrame XP Windows Installer Package

MetaFrame XP Setup is compiled into a Windows Installer installation package. Windows Installer is a component of the Windows 2000 operating system that manages the installation and removal of applications. Windows Installer applies a set of centrally defined setup rules during the installation process that define the configuration of the application.

Windows Installer technology consists of the Windows Installer Service for the Windows operating systems and the package (.msi) file format used to hold information regarding the application setup. You use the Windows Installer Service to modify, repair, or remove an existing application that was installed using Windows Installer technology. Go to **Add/Remove Programs** in Control Panel to remove or modify Windows Installer packages installed on the system.

You can deploy Windows Installer packages using Windows 2000 Active Directory or Microsoft's Systems Management Server. For more information about Windows Installer technology and the Windows Installer Service, see the Windows 2000 online Help or the Microsoft Web site at <http://www.microsoft.com>.

Important Recommendations for Windows Installer

Windows Installer Version 1.1 is installed by default with Windows 2000. Citrix recommends that you install Windows Installer Version 2.0 or later on the server before you install MetaFrame XP. Unrecoverable errors have been encountered when attempting to install MetaFrame XP on a server running Windows Installer Version 1.1. These errors may require you to reinstall the server operating system.

You can download the latest version of Windows Installer from the Microsoft Web site at <http://www.microsoft.com>. Version 2.0 of Windows Installer is included on the MetaFrame XP CD in the directory \Support\MSI20.

MetaFrame XP Setup checks for the presence of Windows Installer 2.0 or higher on the server and exits if it is not installed. To identify the version of Windows Installer you are running, type **msiexec.exe** at a command prompt.

A Windows Installer transform file that you can use to override Setup's check for Windows Installer Version 2.0 is included on the MetaFrame XP CD. This transform file, titled "ignoremsicheck.mst," is located in the directory Support\Install.

To run MetaFrame XP Setup and override the check for Windows Installer Version 2.0, type the following at a command prompt, where "<path>\mfxp001.msi" is the path to the MetaFrame XP Windows Installer package and "<path>ignoremsicheck.mst" is the path to the Citrix-supplied Windows Installer transform file. If you are applying multiple transforms to an installation package, separate each entry in the list with a semicolon.

```
msiexec /i "<path>\mfxp001.msi"  
TRANSFORMS="<path>ignoremsicheck.mst"
```

Important If you want to use the answer file method for running MetaFrame XP Setup in unattended mode, you must install Windows Installer Version 2.0 or later. UnattendedInstall.exe does not run on servers running a version of Windows Installer lower than 2.0. For more information about running MetaFrame XP in unattended mode, see "Unattended Setup of MetaFrame XP Servers" on page 104.

If you encounter problems when running a Windows Installer package, you can check the Windows 2000 Event Viewer for a list of the problems. To open Event Viewer, go to **Start > Program Files > Administrative Tools > Event Viewer**. Check the Application Log for any entries in the Source column of the type "MSIInstaller."

Common Windows Installer Commands

You can use the Msiexec command to install, modify, and perform operations on Windows Installer packages from the command line. The MetaFrame XP Windows Installer package, named MFXP001.msi, is located on the MetaFrame XP CD-ROM in the directory \MF.

Some common options for the Msiexec command are listed below. For further information about the parameters and switches you can use with the listed options, go to the Microsoft Web site and search on “msiexec.”

Option	Syntax
Install or configure a product	<code>msiexec /i {package ProductCode}</code>
Uninstall a product	<code>msiexec /x {package ProductCode}</code>
Set a logging level	<code>msiexec /L [!][w][e][a][r][u][c][m][p][v][+][!]*LogFile.txt</code> To include the v option in a log file using the wildcard flag, type /L*v at the command prompt. The Windows Installer log file options can also be used with the uninstall process.
Install a transform	<code>msiexec /i packageTRANSFORMS=TransformList</code> If you are applying multiple transforms, separate each transform file with a semicolon.
Set the user interface level	<code>msiexec /q {n b f}</code>

Creating a Log File

Installation and uninstallation log files are not automatically created for Windows Installer packages in Windows 2000. You can create log files with the following methods:

- Use the logging command to create log files for only the Windows Installer operation you are carrying out.
- Turn on automatic logging for all Windows Installer operations by creating a new registry string value at.

Key: HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
String (REG_SZ) Value: Logging
Contents: iwearucmopv

A log file is created in the \Temp directory for each operation.

- Use Active Directory's Group Policy Editor to configure logging properties for an Active Directory group.

To configure logging properties, open Group Policy Editor and select **Computer Configuration > Administrative Templates > Windows Components > Windows Installer** to edit the Logging policy.

Important If you enable Windows Installer logging in Windows Installer Version 1.1 (included by default with the Windows 2000 operating system), passwords are saved in the log file in unencrypted plain text. Check the documentation included with later versions of Windows Installer for support of encrypted passwords in log files.

Unattended Setup of MetaFrame XP Servers

You can configure MetaFrame Setup to run without assistance with the following methods:

- Applying transforms to the installation database. A Windows Installer transform modifies the installation package file at installation time and applies the values you set. Sample transform files are located on the MetaFrame XP CD-ROM at Support\Install.
- Creating 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 Support\Install.

Important If you want to use the answer file method for running MetaFrame XP Setup in unattended mode, you must install Windows Installer Version 2.0 or later. UnattendedInstall.exe does not run on servers running a version of Windows Installer lower than 2.0.

The following sections describe creating and applying transforms and creating answer files.

Applying Transforms

You can manipulate the installation process by applying Windows Installer *transforms* (files with the .mst extension) to the installation database contained in a Windows Installer package. A transform makes changes to elements of the database. A transform file modifies the installation package when it is being installed and dynamically affects the installation behavior.

When you create a transform to apply to the MetaFrame XP Windows Installer package, you set your desired values for properties in the package. When you then apply the transform to the installation package, the “questions” you would be asked during Setup are answered. Creating a transform allows you to roll out MetaFrame XP in unattended mode.

Transforms that you create to customize a Windows Installer setup package remain cached on your system. These files are applied to the base Windows Installer package whenever the Installer needs to modify it. You can apply transforms only when you initially install Windows Installer packages; you cannot apply transforms to software that is already installed.

Citrix provides four sample transforms on the MetaFrame XP CD-ROM. You can open these transforms and edit the properties in them with some of the commercially available Windows Installer editing tools. The sample transforms include sample values for select properties, allowing you to determine which properties to edit to achieve a certain configuration.

For more information about each sample transform and the properties you can set for each configuration, see “MetaFrame XP Setup Properties” on page 347.

► **To create a customized transform using one of the sample transform files**

1. Using your preferred tool for editing Windows Installer packages, open the sample transform you want to modify.
2. Enter new values for the properties you want to change.
3. Save the file with a new name.

Creating an Answer File

You can create an *answer file* to provide answers to the questions asked when you run MetaFrame XP Setup. A sample answer file is located on the MetaFrame XP CD-ROM at Support\Install. Instructions are provided in the file for setup options. Copy the sample answer file to another location and modify it for your needs.

► **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 splash screen appears. Close the window.
2. Open the sample file XPFR2_UnattendedTemplate.txt, located in the directory Support\Install, in any text editor. Save the file with another name.
3. Enter the values for the entries you want to set. The sample file includes definitions and possible values for each entry.

4. Type the following at a command prompt where *<Windows Installer package>* is the name of the Windows Installer package you want to run, and *<answer file>* is the name of the text file you created in Step 2:

```
UnattendedInstall <Windows Installer package> <answer  
file>
```

Starting MetaFrame XP Setup

The following procedures explain how to install MetaFrame XP using the MetaFrame XP CD-ROM. For more information, including descriptions of Setup options, see “Choosing Options During Setup” on page 107.

► To begin MetaFrame XP Setup

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM into the CD-ROM drive. If your CD-ROM drive supports Autorun, the MetaFrame XP splash screen appears.
3. Click **Install or Update MetaFrame**.
4. Click **MetaFrame XP** to install MetaFrame XP and Service Pack 2. Click **MetaFrame XP Feature Release 2** to install MetaFrame XP and Feature Release 2.

Note Selecting the **MetaFrame XP with Feature Release 2** option installs Service Pack 2; you do not need to install Service Pack 2 separately. Features included in Feature Release 2 require Feature Release 2 licensing.

If you are installing MetaFrame XP on a clean system, selecting the **MetaFrame XP with Feature Release 2** option installs Feature Release 1, Service Pack 1, and Service Pack 2 in addition to MetaFrame XP and Feature Release 2.

When 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**, Setup stops without finishing.

Using the Command Line

You can also use the Msiexec command to install MetaFrame XP. Set properties by adding *<Property="value">* on the command line after other switches and parameters. For definitions of the properties in the MetaFrame XP Windows Installer package, see “MetaFrame XP Setup Properties” on page 347.

The following sample command line installs the MetaFrame XP Windows Installer package and creates a log file to capture information about this operation. Add the properties you want to set after the switches.

```
msiexec /i MFXP001.msi /l*v c:\output.log
```

Choosing Options During Setup

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

Selecting the MetaFrame XP Family Level

Select the family level you are licensed to run on the MetaFrame XP server. When you purchase MetaFrame XP, you can select from three family levels:

- **MetaFrame XPs** is designed to give businesses outstanding performance from applications running on a central server.
- **MetaFrame XPa** is designed with the small to medium business in mind. A MetaFrame XPa license enables all of the features of MetaFrame XPs and also includes load balancing functionality.
- **MetaFrame XPe** is designed for single-point control of servers, licenses, and resources in large organizations and multinational corporations. A MetaFrame XPe license enables all of the features of MetaFrame XPa and also provides system monitoring and analysis, application packaging and delivery, and integration with third-party SNMP management consoles.

If you have questions about which family level to choose, contact your MetaFrame XP reseller or go to the Product Information area of the Citrix Web site at <http://www.citrix.com/products>.

Based on which family level you are installing, Setup selects the components to install.

Choosing the Product Type

Select the MetaFrame XP product type you are installing. When you select a product type, the MetaFrame XP product code is automatically set. Be sure to verify that the correct product code is displayed on the Setup screen. You can find the product code on the MetaFrame XP media pack.

If you need to enter the product code manually, select **Other** on the Setup screen and then enter the correct product code.

For more information about licenses and product codes, see “Licensing MetaFrame XP” on page 135.

Selecting Components

Based on which family level of MetaFrame XP you are installing (MetaFrame XPs, MetaFrame XPa, or MetaFrame XPe), Setup selects the components to install.

The components to be installed are displayed on the **Component Selection** Setup screen. Click **Disk Cost** to check the amount of disk space the selected components require.

Configuring the Data Store

This section explains how to configure MetaFrame XP servers to connect to the data store for a server farm. For background information about the data store, see “Choosing a Database for the Data Store” on page 50. For background information about server farm zones, see “Configuring Zones and Data Collectors” on page 179.

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, use the IMAPORT command to change the port on the first server. For more information about this command, see “MetaFrame XP Commands” on page 309. 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 **Create or Join a Server Farm** Setup screen, select **Create a new farm** and click **Next**.
2. On the **Create a Server Farm** Setup screen, enter the following information:
 - Enter a name for the new MetaFrame XP server farm. Farm names can include spaces but cannot be more than 32 characters in length.
 - Select **Use a local database (Microsoft Access) on this server**.
 - The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option **Use Default Zone Name** and enter the new name.
3. Click **Next** to continue.
4. Continue with MetaFrame XP Setup.

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

1. On the **Create or Join a Server Farm** Setup screen, select **Join an existing farm** and click **Next**.
2. Select **Connect to a data store set up locally on another server**.
3. Enter the name of the server farm zone.
4. Enter the name and TCP port of the server that contains the Access data store.
5. Continue with MetaFrame XP installation.

Using SQL, Oracle, or IBM DB2 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, an Oracle database, or an IBM DB2 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 99, “To create a data store database with Oracle” on page 100, or “To create a data store database with IBM DB2” on page 101.

► **To create a server farm with an SQL, Oracle, or DB2 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 **Create or Join a Server Farm** Setup screen, select **Create a new farm** and click **Next**.
2. On the **Create a Server Farm** Setup screen, enter the following information:
 - Enter a name for the new MetaFrame XP server farm. Farm names can include spaces but cannot be more than 32 characters in length.
 - Select **Use the following database on a separate database server** and select the database from the list.
 - The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option **Use Default Zone Name** and enter the new name.
3. Click **Next** to continue.
4. Continue with MetaFrame XP Setup.
5. 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.

6. Follow the procedure “To configure the ODBC driver for Microsoft SQL Server” on page 110, “To configure the ODBC driver for Oracle” on page 113, or “To configure the ODBC driver for IBM DB2” on page 113.
7. Follow the remaining instructions in Setup.

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

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

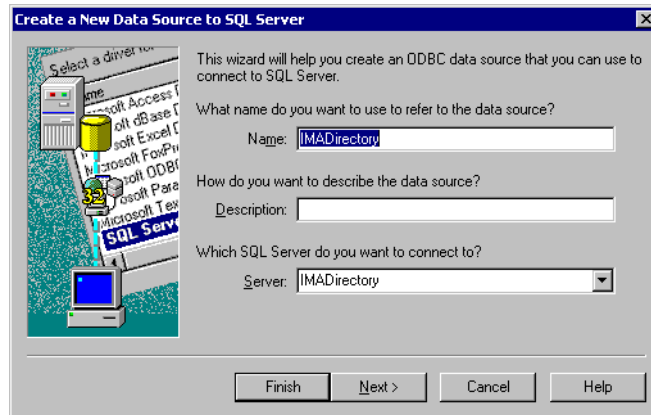
1. On the **Create or Join a Server Farm** Setup screen, select **Join an existing farm** and click **Next**.
2. Select the option to connect directly to the database you configured when you created the farm and click **Next**.
3. Follow the instructions in the procedure “To create a server farm with an SQL, Oracle, or DB2 data store” beginning with Step 3.

Configuring ODBC Drivers

This section provides step-by-step instructions for configuring ODBC drivers for Microsoft SQL Server, Oracle, and IBM DB2 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.

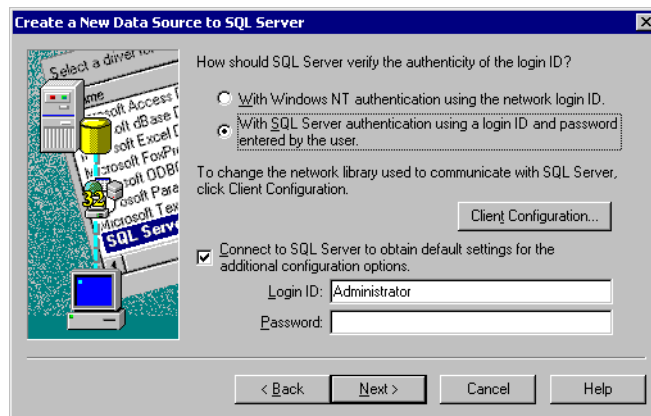
► **To configure the ODBC driver for Microsoft SQL Server**

1. When 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:

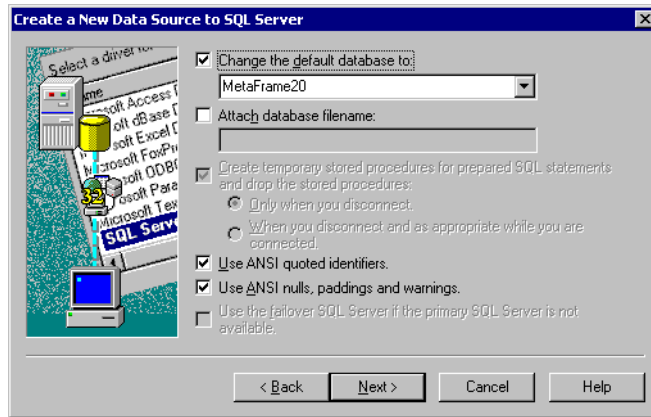


This dialog box lets you specify the method of authenticating the logon ID that MetaFrame XP will present to the SQL Server when accessing the data store. To authenticate successfully, the SQL Server and MetaFrame XP must use the same authentication method. Make sure the database created for MetaFrame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

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

If the ODBC manager is unable to authenticate to the database, you are prompted to re-enter the Logon ID and password.

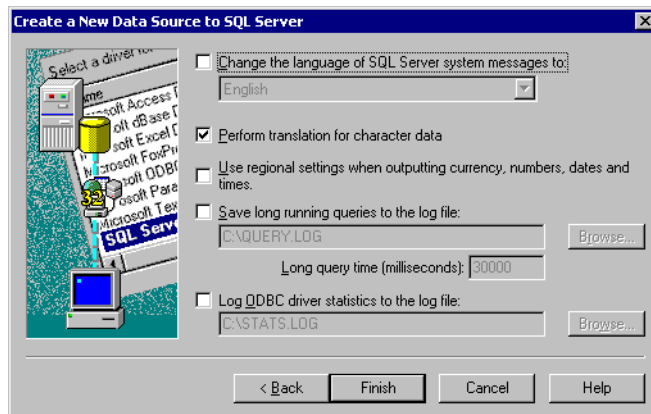
3. The following dialog box appears:



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 logon IDs can be configured to log on to a database by default. If in your SQL Server administrative program the logon ID is set to log on 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:

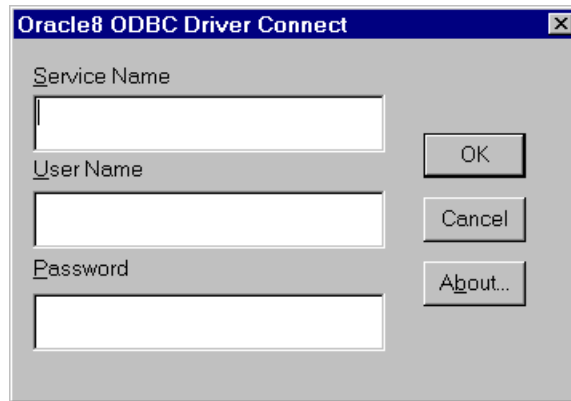


Click **Finish** to accept these values. A dialog box lets you test the new data source name. Click **Test Data Source**. If the test completes successfully, click **OK** and then click **OK** again to complete data source name configuration.

5. Follow the steps in the procedure, “To create a server farm with an SQL, Oracle, or DB2 data store” on page 109, 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:

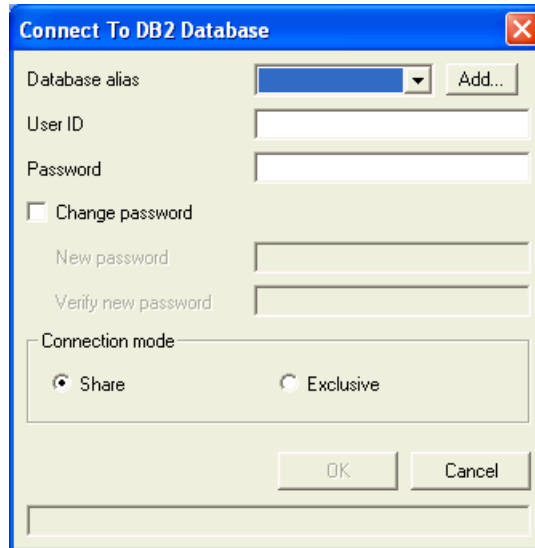


2. In the **Service Name** box, type the service name used when the Oracle client was installed. In the **User Name** and **Password** boxes, type the user name and password created on the Oracle server for the data store.
3. Click **OK**.

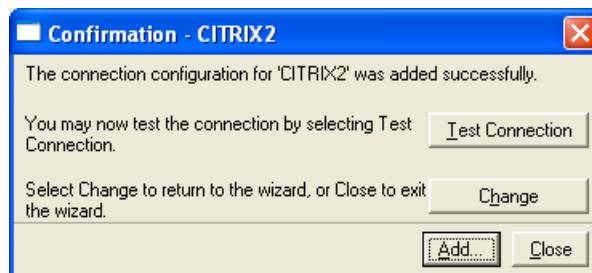
This completes the Oracle data store setup. You are now ready to install MetaFrame XP. Follow the steps in the procedure “To create a server farm with an SQL, Oracle, or DB2 data store” on page 109, beginning with Step 6.

► **To configure the ODBC driver for IBM DB2**

1. If you select “IBM DB2 ODBC DRIVER” from the **Installed ODBC Driver** list in MetaFrame XP Setup, the following dialog box appears:



2. Set the connection mode to **Share**.
3. Click **Add** to launch the IBM DB2 Client Configuration Assistant. This wizard walks you through configuring the ODBC connection to the DB2 database.
4. Follow the instructions in the Client Configuration Assistant. On the Protocol page, be sure **TCP/IP** is selected. Citrix recommends that you use this protocol to connect to the data store.
5. Click **Finish** when you are done configuring the connection. The following dialog box appears:



6. Click **Test Connection** to make sure that the connection to the database works.
7. Click **Close**.
8. Ensure that the connection mode is still set to **Share**.
9. Enter the User ID and Password.

10. Click **OK**.

This completes the DB2 data store setup. You are now ready to continue with MetaFrame XP Setup. Follow the steps in the procedure “To create a server farm with an SQL, Oracle, or DB2 data store” on page 109, beginning with Step 6.

Assigning Farm Administrator Credentials

Citrix administrators manage MetaFrame XP server farms. When you install the first MetaFrame XP server in a new server farm, you specify an initial farm administrator. This user account is automatically configured as a Citrix administrator with full administration rights in Citrix Management Console.

To give other user accounts access to the console, a Citrix administrator with full administration rights logs on to the console and creates other Citrix administrator accounts.

You can create Citrix administrators accounts with the following permission levels:

- Full administration rights to all areas of MetaFrame XP server farm management.
- View-only access to all areas of server farm management.
- Access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.

For more information about delegating administration rights to Citrix administrators, see “Configuring Citrix Administrator Accounts” on page 162.

Note One Citrix administrator account with full administration rights must always exist in the server farm. MetaFrame prevents you from deleting the last Citrix administrator account with this level of permission. 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.

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 user collaboration, 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 **Configure 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 when you run MetaFrame Setup, the restrictions cannot be changed at a later time. If you place restrictions on shadowing during Setup, any user policies you create to enable user-to-user shadowing have no effect.

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.

Prohibit shadowing of ICA sessions on this server. This option permanently disables shadowing by anyone of all ICA sessions on the server. If you disable shadowing during MetaFrame XP Setup, you cannot allow shadowing using other MetaFrame configuration utilities or by creating user policies.

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.** By default, MetaFrame XP gives users with permission to shadow the ability to input keystroke and mouse control during session shadowing. Select this option if you want these users to be able to shadow without input. In some cases, shadowing without input hides the user's presence.
- **Force a shadow acceptance popup.** By default, MetaFrame XP notifies users with a prompt when other users are attempting to shadow their sessions. Select this option to deny users the ability to shadow sessions without sending this notification.
- **Log all shadow connections.** 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.

Configuring Network ICA Connections

By default, MetaFrame XP Setup enables ICA connections over all network protocols already installed on the server.

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.

Installing Citrix NFuse Classic

Citrix NFuse Classic is a Web-based application deployment system that provides users with access to MetaFrame applications through a standard Web browser. When you install MetaFrame XP, NFuse Classic is also installed if the server is running Microsoft Internet Information Services Version 5.0 or higher.

NFuse Classic employs Java object technology executed on a Web server to dynamically create an HTML-based depiction of the MetaFrame server farm for each of your users. Included in each user's presentation are all the applications published in the MetaFrame server farm for that user.

For large-scale deployments, Citrix recommends that you run NFuse on dedicated Web servers. For smaller deployments, you can run Web server software and NFuse together on a MetaFrame XP server.

For more information about configuring Citrix NFuse Classic, see the *Citrix NFuse Classic Administrator's Guide*, located in the Docs directory of the MetaFrame XP CD-ROM.

Configuring the Citrix XML Service Port

MetaFrame XP uses the Citrix XML Service to supply NFuse Classic servers and ICA Clients with the names of applications published on MetaFrame XP servers. By default, MetaFrame XP Setup configures the Citrix XML Service to share the default TCP/IP communication port (port 80) with Microsoft Internet Information Services.

If you intend to send NFuse data over a secure HTTP connection using SSL, be sure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

If you do not want the Citrix XML Service to share the TCP port with IIS, you can use a separate port for the Citrix XML Service. On the **Configure Citrix XML Service Port** Setup page, select **Use a separate port** and enter the new port number. 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 Classic Administrator's Guide* for instructions about configuring NFuse Classic to use a different port. See the *ICA Client Administrator's Guides* for instructions about 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 Citrix XML Service. This requirement includes all MetaFrame 1.8 and MetaFrame XP servers when operating in mixed mode.

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 server before MetaFrame XP installation. You can change the port after installation as described below.

► **To change the Citrix XML Service port after installation**

Important Use this procedure only if you do not want to share the port used by Internet Information Services. If you entered a port number other than the default “Share with IIS” during MetaFrame XP Setup, you can change the port to another port number using the Citrix Management Console. However, if you want to change the setting to share the port with IIS after running MetaFrame XP Setup, you must follow the instructions for manually setting the Citrix XML Service to share the TCP port with IIS.

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.
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 Service 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.
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 the Server's Default Web Page

By default, MetaFrame XP Setup sets the server's default Web page to the NFuse Classic logon page. Users can access the NFuse Classic logon page by pointing their Web browsers to `http://<server name>`, where `<server name>` is the name of the MetaFrame XP server on which NFuse Classic is installed.

If you do not want to set the MetaFrame XP server's default Web page to the NFuse Classic logon page, be sure this option is not selected.

Installing ICA Client Software

At the end of MetaFrame XP installation, the ICA Client Distribution wizard installs ICA Clients and ICA Client-related utilities. Use the MetaFrame Components CD to access the initialization file needed to run this wizard. For more information about deploying and configuring ICA Clients, see "Deploying ICA Clients to Users" on page 215.

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 on the MetaFrame server 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 the server's desktop to allow users to access the Program Neighborhood interface. The ICA Client Distribution wizard installs the ICA Win32 Program Neighborhood 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 the MetaFrame Components CD in the server's CD-ROM drive and click **Next**. Alternatively, you can specify the location of a network-shared Components CD-ROM or CD image. In the **ICA Client CD Image** field, specify the location of your installation media. The wizard requires you to type in or browse to the location of the file ICASetup.ini. This file is located in the root directory of the Components 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.

Migrating Citrix Servers to MetaFrame XP

MetaFrame XP can run in mixed mode, with MetaFrame 1.8 servers and MetaFrame XP servers coexisting 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 93 for more information about the limitations of mixed mode.

Supported Migration Paths

MetaFrame XP, Feature Release 2 is supported on Windows 2000 servers only; it is not supported on Windows NT 4.0, Terminal Server Edition. Before you can migrate earlier versions of MetaFrame to MetaFrame XP with Feature Release 2, you must update your server’s operating system.

MetaFrame XP supports migration of Citrix servers that are running the following MetaFrame versions.

Starting MetaFrame Version	Upgrade Path (after upgrading to Windows 2000 at Service Pack 2 or higher)
MetaFrame 1.8 for Windows NT 4.0, Terminal Server Edition, at Service Pack 6	MetaFrame 1.8 for Windows 2000 to MetaFrame 1.8 for Windows 2000 with Service Pack 3 to MetaFrame XP with Feature Release 2 (includes Feature Release 1 and Service Pack 1)
MetaFrame XP 1.0 for Windows NT 4.0, Terminal Server Edition, at Service Pack 6	MetaFrame XP 1.0 for Windows 2000 to MetaFrame XP with Feature Release 2 (includes Feature Release 1 and Service Pack 1)
MetaFrame XP with Feature Release 1 on Windows NT 4.0, Terminal Server Edition, at Service Pack 6	MetaFrame XP for Windows 2000 to MetaFrame XP with Feature Release 2 (includes Feature Release 1 and Service Pack 1)
MetaFrame 1.8 at Service Pack 3 for Windows 2000	MetaFrame XP with Feature Release 2 (includes Feature Release 1 and Service Pack 1)
MetaFrame XP 1.0 for Windows 2000	MetaFrame XP with Feature Release 2 (includes Feature Release 1 and Service Pack 1)
MetaFrame XP with Feature Release 1 for Windows 2000	MetaFrame XP with Feature Release 2

Overview of the Migration Process

If you want to migrate a MetaFrame 1.8 for Windows server to a MetaFrame XP server, complete the following tasks:

► **To migrate a MetaFrame 1.8 server farm to MetaFrame XP**

1. Configure the database server if you are using Microsoft SQL Server, Oracle, or IBM DB2 for the MetaFrame XP server farm's data store.
2. Install MetaFrame XP on a server that is not the current master ICA Browser.
 - During MetaFrame XP installation, choose the option to create a new server farm.
 - Name the new MetaFrame XP server farm exactly the same as the existing MetaFrame 1.8 server farm.
3. Using Citrix Management Console, install and activate the migration licenses you received in your MetaFrame XP migration kit.

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.

4. Verify that you can connect to the MetaFrame XP server and check the migration log file to confirm that all applications were migrated successfully. MetaFrame XP Setup displays the name of the script file. The file is located in %SystemRoot%\System32.
5. Migrate additional MetaFrame 1.8 servers. During installation, choose to join an existing farm.
6. After all MetaFrame 1.8 servers are 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 License Counts in Mixed Mode" on page 95.

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.

For detailed information about cloning MetaFrame XP servers, see *Advanced Concepts for MetaFrame XP*, available from the Support area of the Citrix Web site at <http://www.citrix.com/support>.

Uninstalling MetaFrame XP

If you want to remove a MetaFrame XP server from a server farm, Citrix recommends that you uninstall MetaFrame. This removes the host information from the server farm's data store and removes the server from the list of servers displayed in Citrix Management Console.

You can uninstall MetaFrame XP using Add/Remove Programs in Control Panel or using the Windows 2000 Msiexec command. For more information about this command, go to the Microsoft Web site and search on "msiexec."

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

► To uninstall MetaFrame XP

1. Exit any applications running on the server.
2. Choose **Start > Settings > Control Panel > Add/Remove Programs**.
3. Click **Change or Remove Programs**, select **Citrix MetaFrame XP**, and click **Remove**.

If you need to force the removal of MetaFrame XP from the system, you can use the command line to add the property

```
CTX_MF_FORCE_SUBSYSTEM_UNINSTALL
```

and set its value to "Yes."

The following sample command line enables logging of the uninstallation operation and forces the removal of MetaFrame XP:

```
msiexec /x MFXP001.msi /l*v c:\output.log  
CTX_MF_FORCE_SUBSYSTEM_UNINSTALL="Yes"
```

Important If you rename a MetaFrame XP server on your network, the new server name is added to the list of MetaFrame servers in the server farm. However, you must remove the old server name because it is still listed as a member of the server farm. Before you remove the server name be sure to update all references to the new server name, including data collector ranking, published application references, and license assignments.

If you are planning to uninstall MetaFrame XP from the Resource Manager metric farm server or database connection server for a summary database, be sure to reassign the server before removing it from the farm. If you are using a summary database, Citrix recommends that you update it before removing any servers from the server farm. You should also create any necessary billing reports from the server before you remove it.

Installing Citrix Management Console on Other Computers

Citrix Management Console is a centralized management utility you use to administer a MetaFrame XP server farm. The console is automatically installed on MetaFrame XP servers when you install MetaFrame XP.

You can use the MetaFrame XP CD to install the Citrix Management Console on workstations that do not have MetaFrame XP installed. For compatibility information, see “Citrix Management Console Requirements” on page 46.

► To install Citrix Management Console on other computers

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM into the CD-ROM drive.
 - If your CD-ROM drive supports Autorun, the MetaFrame XP splash screen appears.
 - If the splash screen does not appear or you are installing from a network share point, choose **Start > Run** and type **d:\autoroot.exe**, where *d* is the letter of your CD-ROM drive or network share point.
3. Select **Other tools and components > Administration tools > Citrix Management Console**.
4. Follow the instructions in the Setup wizard.

Deploying Feature Release 2 and Service Pack 2



You can deploy Feature Release 2 and Service Pack 2 on servers that have MetaFrame XP already installed. If you have not yet installed MetaFrame XP, see “Installing MetaFrame XP” on page 99 before referring to this chapter.

Upgrading to Feature Release 2 or Service Pack 2

Citrix recommends that you deploy Feature Release 2 or Service Pack 2 in all server farms. The feature release updates your MetaFrame XP software to the latest version.

Note If you find that you need to run different releases of MetaFrame XP in your server farm on a temporary basis, configure a server running the latest release as the zone’s data collector. See “Configuring Zones and Data Collectors” on page 179 for more information.

Installation of Feature Release 2 includes Service Pack 2; you do not need to install Service Pack 2 separately. However, if you do not install Feature Release 2, you can install Service Pack 2 to apply its fixes for known issues and performance improvements to your MetaFrame XP servers.

If you do not have Feature Release 1 installed on the MetaFrame server, installing Feature Release 2 also installs Feature Release 1. If you do not have Service Pack 1 already installed, installing Service Pack 2 also installs Service Pack 1.

If you do not have MetaFrame XP installed, installing it using MetaFrame XP Setup installs Feature Release 1 and Feature Release 2. However, you must install and activate licenses for MetaFrame XP and for Feature Release 2. You are not required to install and activate separate Feature Release 1 licenses.

Deploying Feature Release 2 or Service Pack 2 does the following:

- Service Pack 2 provides performance improvements and fixes known issues. Installing Service Pack 2 on a MetaFrame XP server updates the application server software, Citrix Management Console, and the additional Citrix components that are part of MetaFrame XPa and MetaFrame XPe.
- Feature Release 2 includes new features and provides enhancements to existing features. Installing Feature Release 2 adds the enhancements and new features to the server's application server software, Citrix Management Console, and the additional Citrix components that are part of MetaFrame XPa and MetaFrame XPe.

Important When you restart your server after you finish upgrading to Feature Release 2, you need to wait for the Citrix IMA Service to start. It may take a minute or two for the IMA Service to start. During this time it may appear that the server is stalled.

You can upgrade to Feature Release 2 through an ICA or RDP session.

For a summary of new features and improvements that are provided by Feature Release 2, see “Features Included in Feature Release 2” on page 33.

If you do not receive a feature release or service pack on a CD, you can download the software from the Citrix Web site at www.citrix.com. See “Downloading and Installing a Service Pack” on page 130 for more information.

Choosing Installation Options

When you insert the MetaFrame XP CD into a CD-ROM drive, the Autorun splash screen appears. If the window does not appear, double-click the Autorun program in the CD's root directory.

You can browse the Autorun screens to the following installation options:

Service Pack 2. This option installs Service Pack 2 software to update the MetaFrame XP application server, Citrix Management Console, and related components. This option does not set the server's feature release level to Feature Release 2. If you want to activate Feature Release 2 later, use Citrix Management Console to set the server's feature release level to Feature Release 2 (see “Setting the Feature Release Level” on page 132).

Feature Release 2. This option installs Service Pack 2 and Feature Release 2 and sets the server's feature release level to Feature Release 2. The server then requests a Feature Release 2 product license from the server farm's license pool. You must add a Feature Release 2 product license to the server farm to make the features of the feature release available. For more information, see "Licensing Requirements for Feature Release 2" on page 152.

Citrix Management Console. This option installs or updates the Citrix Management Console on a non-MetaFrame XP workstation. You do not need to use this option to update a MetaFrame XP server if you use the Service Pack 2 or Feature Release 2 options to update the server. Use this option only to update the console on non-MetaFrame XP workstations.

Citrix Web Console. This option installs the Web-based Citrix server farm administration module on a MetaFrame XP server with Feature Release 2 or Service Pack 2 installed. The server must have Microsoft Internet Information Services 5.0 or later installed before you use this option. For more information, see "Using Setup" on page 128.

Network Management Components. To update the Citrix Network Management plug-ins, browse the Autorun screen to the options for installing SNMP plug-ins on network management consoles. The plug-ins interface MetaFrame server farms with compatible network management consoles.

Browse. This option displays the contents of the CD.

Important If you are upgrading MetaFrame servers that have a previous release of Resource Manager installed, upgrade the farm metric servers (primary and backup) before upgrading other MetaFrame servers in the server farm. Resource Manager uses the farm metric server to interpret information collected from other servers. This may cause inconsistencies if another server is running a later version of Resource Manager.

Updating Citrix Management Console

When you use the Feature Release 2 or Service Pack 2 installation option, Setup updates Citrix Management Console on a MetaFrame XP server. To update the console on a system that is not a MetaFrame XP server, browse the Autorun screen to the Citrix Management Console option.

If you upgrade servers in a server farm from MetaFrame XPs or MetaFrame XPa to MetaFrame XPe, you need to update the Citrix Management Console on any systems that are not MetaFrame XP servers. Refer to the MetaFrame XPe documentation for information about copying the required modules to the Citrix Management Console systems. After you complete this process, use the Citrix Management Console option on the MetaFrame XP CD to update the additional modules on the console system.

Backing Up Files Before Installation

Before Setup installs the service pack or feature release, it saves all files on the MetaFrame XP server that would be replaced during installation. The files are saved on the server so they can be restored if you uninstall the service pack or feature release. For information about uninstalling the software, see “Downgrading Feature Release 2 or Service Pack 2” on page 132.

Viewing Updated Documentation

Updated documentation for Citrix MetaFrame XP application server, Citrix Installation Manager, Citrix Resource Manager, Citrix Network Manager, Citrix Load Manager, and Citrix NFuse Classic is available in PDF files. The files are in the Docs folder on the MetaFrame XP CD.

Setup copies the documentation files to the server when it installs Feature Release 2 or Service Pack 2. The documentation files are stored in the %SystemDrive%\Program Files\Citrix\Documentation folder.

Using Setup

The following procedures describe how to select installation options and install software from the MetaFrame XP CD-ROM.

CAUTION Citrix recommends that you install Windows Installer Version 2.0 or later on the MetaFrame XP server before you install MetaFrame XP. Unrecoverable errors have been encountered when installing MetaFrame XP with Windows Installer Version 1.1 that may require you to reinstall the server operating system. You can download the latest version of Windows Installer from the Microsoft Web site at <http://www.microsoft.com>. Version 2.0 of Windows Installer is included on the MetaFrame XP CD in the directory \Support\MSI20.

For more information about this recommendation to install Windows Installer Version 2.0, see “Important Recommendations for Windows Installer” on page 102.

► **To install Feature Release 2, Service Pack 2, and other Citrix components**

1. Before beginning the installation process, do the following:
 - Verify that no ICA sessions are active on a MetaFrame XP server you are updating, and that no users need to connect to the server during the installation process. Setup for Feature Release 2 and Service Pack 2 disconnects all active sessions and does not allow new connections until the installation is complete.
 - If the MetaFrame XP server is an *indirect server*, which communicates with the server farm's data store through another MetaFrame XP server, you must update that server before you update the indirect server.
2. Insert the MetaFrame XP CD in the CD-ROM drive. Autorun displays the installation options window. If the window does not appear, enter `d:\autorun.exe` at a command prompt (replace *d* with the CD drive letter).
3. On the main Autorun screen, click **Install or update MetaFrame** and then click **MetaFrame XP Feature Release 2** to install Feature Release 2 and Service Pack 2 on a MetaFrame XP server. This option also sets the feature release level of the server to Feature Release 2.
4. On the main Autorun screen, click **Other tools and components** and then **Administration tools** to select one of the following options:
 - **Citrix Management Console** to install Service Pack 2 for the console on a workstation (not a MetaFrame XP server).
 - **Citrix Web Console** to install the Web-based Citrix console on a MetaFrame XP server that has Internet Information Services 5.0 or later installed.
5. On the main Autorun screen, click **Other tools and components** and then **Network Manager plugins** to display options for installing SNMP plug-ins on NetView, OpenView, and Unicenter TNG network management consoles.
6. On the main Autorun screen, click **Browse CD** for access to other information and utilities, including the full MetaFrame XP documentation set in the Docs directory.
7. After you choose an option, a wizard guides you through the installation process. When the installation is complete, Setup prompts you to restart the system.

Downloading and Installing a Service Pack

Use the following procedure if you want to download a service pack from the Citrix Web site.

► To download a service pack

1. Using your Web browser, connect to www.citrix.com and click the Download link.
2. On the Citrix download page, click the “Hotfixes, Service Packs and more” link.
3. Select MetaFrame XP for Windows and click **Go!**
4. Select the package that you want to download.
5. Double-click the downloaded file to extract the installation files. Note the location for the extracted files and click **Unzip**.
6. In the folder containing the extracted files, double-click **Setup** and follow the instructions displayed by Setup.

Updating ICA Client Software

During installation of Feature Release 2, Setup prompts you to update the ICA Client software on the MetaFrame XP server.

You can run the ICA Client Distribution wizard to update the ICA Client images on the server. When prompted, insert the Components CD-ROM and click **Next**.

For information about installing ICA Client software on client devices, see the *ICA Client Administrator's Guide* for the clients you want to install. These guides are in the ICAClientDoc directory on the Components CD-ROM.

Unattended Setup of MetaFrame XP, Feature Release 2

You can configure MetaFrame XP, Feature Release 2 Setup to run without assistance using one of two methods:

- Creating 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 Support\Install.
- Running the **Msixexec** command at the command line. For more information about this command, go to the Microsoft Web site and search on “msiexec.”

Creating an Answer File

You can create an *answer file* to provide answers to the questions asked when you run MetaFrame XP, Feature Release 2 Setup. A sample answer file is located on the MetaFrame XP CD-ROM at Support\Install. Instructions are provided in the file for setup options. Copy the sample answer file to another location and modify it for your needs.

► 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 splash screen appears. Close the window.
2. Open the sample file XPFR2_UnattendedTemplate.txt, located in the directory Support\Install, in any text editor. Save the file with another name.
3. Enter the values for the Feature Release installation options you want to set. For example, set the FeatureRelease property to “Yes” to install Feature Release 2. Set this option to “No” to install only Service Pack 2.
4. Type the following at a command prompt where *<Windows Installer package>* is the name of the Windows Installer package you want to run, and *<answer file>* is the name of the text file you created in Step 2:

UnattendedInstall.exe <Windows Installer package> <answer file>

Using the Command Line

You can also use the Msiexec command to install MetaFrame XP, Feature Release 2. Properties are set on the command line by adding <Property=“value”> on the command line after other switches and parameters. For example, set the FeatureRelease property to “Yes” to install Feature Release 2. Set this option to “No” to install only Service Pack 2. For definitions of the properties in the MetaFrame XP Windows Installer package, see “MetaFrame XP Setup Properties” on page 347.

The following sample command line installs MetaFrame XP, Feature Release 2 and creates a log file to capture information about this operation.

```
msiexec /i MFXP001.msi /l*v c:\output.log  
FeatureRelease="Yes"
```

Downgrading Feature Release 2 or Service Pack 2

You can downgrade a service pack or feature release if necessary. Downgrading the software returns the MetaFrame XP server to its state before the feature release or service pack was installed.

► **To downgrade to an earlier version of MetaFrame XP**

1. Choose **Start > Settings > Control Panel > Add/Remove Programs**.
2. Select the service pack or feature release from the list of installed programs.
3. Click **Change**. Do not click **Remove**. Doing so uninstalls MetaFrame XP from your system.
4. On the **Application Maintenance** screen, click **Remove** and then click **Next**.
5. On the **Citrix MetaFrame XP for Windows, Feature Release 2 Uninstall** screen click **Downgrade**.

Setting the Feature Release Level

The *feature release level* is a setting that enables a feature release on a MetaFrame XP server. Normally, the feature release level is set by using the Feature Release 2 installation option. You can set the feature release level manually to change a server's configuration.

For example, you can set the feature release level to Feature Release 2 if you used the Service Pack 2 installation option (which does not set the feature release level) and now you want to enable the Feature Release 2 software.

The feature release level affects the product license that the server requires. The following are examples of the effect of the feature release setting:

- If a server's feature release level is set to Feature Release 2, the server seeks a Feature Release 2 product license from the server farm's license pool. If the license is available, the feature release software is enabled and its features are available on the server. If the Feature Release 2 license is not available, the server does not accept connections from ICA Clients.
- If a server's feature release level is set to "Not Installed," the server does not seek a feature release product license and the features of the feature release are not available on the server.

► **To set the feature release level on a MetaFrame XP server**

1. In Citrix Management Console, right-click the server and choose **Set Feature Release Level**.
2. In the dialog box that appears, click the down-arrow to select the feature release level.
 - If you select **Feature Release 2**, the server attempts to acquire a Feature Release 2 product license from the license pool and the features of the feature release are available on the server. Do not set the feature release level if a feature release license is not available, because the server cannot accept connections from ICA Clients without the license.
 - If you select **None**, the server does not acquire a Feature Release 2 license and the features of Feature Release 2 are not available on the server.
3. Click **OK** to set the feature release level.

Licensing MetaFrame XP



This chapter describes Citrix licensing for MetaFrame XP and its feature releases and service packs. It includes an overview of licensing requirements and describes various types of licenses.

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 about **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, you 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 about 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 140.

► To enter licenses for Citrix products

1. Get the product code and serial number from your MetaFrame XP product packaging.
 - 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 and select a product type, the corresponding product code is automatically referenced.

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.
3. Use Citrix Management Console to enter the serial numbers for all of 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, you must then 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 the farm's data store, 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 about product and connection licenses, see "Product Licenses" on page 138 and "Connection Licenses" on page 139.

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. When 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 150.

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, NFuse Classic
MetaFrame XPa	MetaFrame XP with Load Manager, NFuse Classic
MetaFrame XPe	MetaFrame XP, Load Manager, NFuse Classic, 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 139.

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. Because of the client device licensing feature, one connection license count in the license pool supports multiple concurrent ICA sessions from one client device to the MetaFrame XP server 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 on to 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 using Citrix Management Console.

If you install MetaFrame XP on an existing Citrix server, Setup 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 140.

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.

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. One or more license serial numbers are also on the label.

MetaFrame XPa 1.0 -English	
Server:	XNNXX-NNXXN-XNXXN-NXNXN-NXNXN
Product Code	0100-0F4A
ICA Connect:	XNNXX-NNXXN-XNXXN-NXNXN-NXNXN

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.

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 **Actions > Servers > Set MetaFrame Product Code**.
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, using 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 15 letters, numbers, and symbols. The string has five groups of five characters each, with a hyphen between each group.

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. A serial number for a connection license is labeled "ICA Connect." A serial number for a product license is labeled "Server."

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 138 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 that 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 146.

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 about the basics of using Citrix Management Console, see “To use Citrix Management Console” on page 166.

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 the Citrix IMA protocol.

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. Use the **Refresh** command to ensure 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 11 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 activate licenses using the Web

1. Select a license number on the **License Numbers** tab in Citrix Management Console and choose **Actions > Activate**.
2. In the **Activate License** dialog box, click **Copy to Clipboard** to copy the license number to the Clipboard for the next step.
3. Go to the Citrix Activation System Web page at <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, 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.

Note Licensing changes might not appear immediately in Citrix Management Console. To refresh the display after adding or activating a license, press F5 or choose **View > Refresh**.

► **To activate licenses by phone or fax**

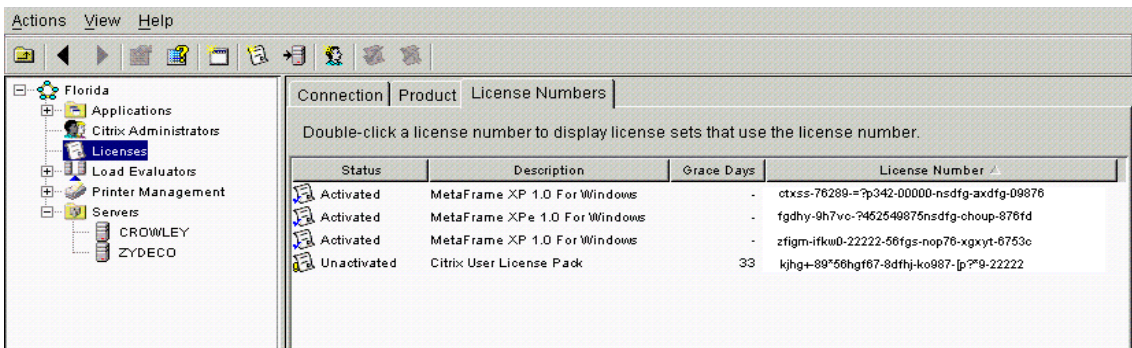
If you cannot use the Web for license activation, you can get an activation code by phone or fax.

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. Write down the license number that appears in the **Activate License** dialog box. You can leave the dialog box open for the following step.
3. Use one of the following methods to obtain an activation code for the license:
 - Fax the license number to (954) 267-9342 with your return fax number and customer information.
 - Call (800) 424-8749 to speak with a customer service representative and get an activation code.
4. After you obtain an activation code, enter the activation code in the **Activate License** dialog box and click **OK** to activate the license.

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 li
	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 includes 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 151.

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 ship 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 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, you might have two MetaFrame XPs licenses, one with a license count of 15 and one with a license count of 20. 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.

Note For some types of MetaFrame XP product licenses, the license count is unlimited, which means that the license authorizes the installation and use of the product on any number of servers.

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 expires, 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).

Licensing Requirements for Feature Release 2

Feature Release 2 includes new features that require licensing. To enable Feature Release 2, you must add a Feature Release 2 product license and Feature Release 2 connection license to the server farm.

Feature Release 2 product license. Most product licenses have an unlimited license count, which means the license can be used by all the MetaFrame XP servers in a server farm. You must install a Feature Release 2 product license in the server farm to make the features of the feature release available. Each MetaFrame XP server that has its feature release level set to Feature Release 2 requests a Feature Release 2 product license count from the server farm's license pool.

Feature Release 2 connection license. Each ICA session between an ICA Client and a MetaFrame XP, Feature Release 2 server requires one feature release connection license count. Subsequent connections to the same server do not use an additional license count.

In addition, subsequent connections to a different server in the same farm do not use an additional license count if the first session used a pooled feature release connection license. If the feature release level of a MetaFrame XP server is set to Feature Release 2, the server requests a Feature Release 2 connection license count from the license pool.

Important Configuring a MetaFrame XP server to use Feature Release 2 without installing the required licenses makes the server unable to accept connections from users. If a server's feature release level is set to Feature Release 2, but Feature Release 2 product and connection licenses are not installed, users cannot connect to the server and run ICA sessions.

You can disable the feature release on a server by setting the feature release level to "Not Installed." For more information, see "Setting the Feature Release Level" on page 132.

Citrix licensing terms can differ for enterprise customers, retail customers, evaluation software, and not-for-resale products packages. For information about the specific terms and conditions of your license, refer to the End-User License Agreement that is included with the software or license package.

► **To add Feature Release 2 licenses to a server farm**

1. Log on to Citrix Management Console by choosing **Start > Programs > Citrix > Citrix Management Console**.

Important To add licenses, you must be a Citrix administrator with rights to perform licensing tasks.

2. Choose **Actions > New > License** or click **Add License** on the toolbar. The **Add License** dialog box appears.
3. In the **Add License** dialog box, type a Citrix license serial number exactly as it appears. Include all hyphens (dashes) between the groups of characters. The serial number can include numerals, letters, and symbols such as plus signs, question marks, and stars.

Click **OK** after you type the license serial number.

- 4. A message confirms successful installation and prompts you to activate the license. Click **Yes** to activate the license at this time or **No** to activate the license later.
- 5. Repeat Steps 3 through 5 for each license you want to add to the server farm. After you add licenses to the server farm, be sure to activate the licenses as described next.

Activating Feature Release 2 Licenses

After you install Citrix licenses, you must activate each license to complete the licensing process. If a license is installed but is not activated, the MetaFrame XP server displays messages to remind you to activate the license.

If you do not activate a license, the license expires after a set period. If a license expires, the license is no longer valid. Lack of a valid license can prevent users from connecting to MetaFrame XP servers. You cannot assign non-activated licenses to servers.

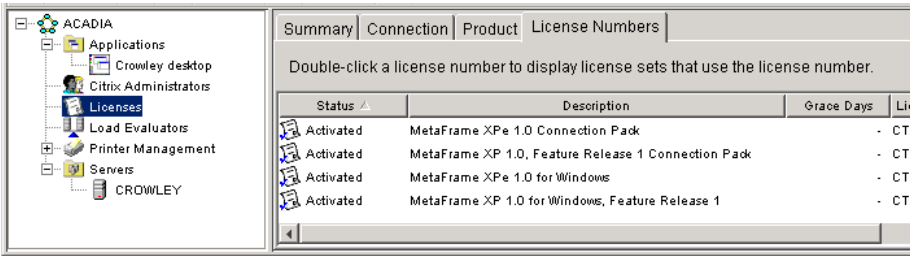
Viewing Feature Release License Information

When you install a feature release, Citrix Management Console displays information about the servers that are configured to use the feature release. The console also displays information about feature release licenses and license counts in use in the server farm.

When you select the Licenses node in the console, the tabs in the right pane display the following information related to licensing:

Viewing License Numbers

The **License Numbers** tab displays each license number that is added to the server farm. A license number consists of a license serial number followed by an eight-character code. A license number can be associated with a product or connection license for the base product (MetaFrame XP) or a feature release.



Viewing Feature Release Product Licenses

The **Product** tab displays information about Citrix product licenses, including feature release product licenses, that are in the server farm's license pool. You can use this tab to check the number of servers that are using a feature release product license. Add the values in the Pooled in Use and Assigned in Use columns to calculate the total number of servers that are using a feature release product license.

If the number of servers that use a feature release license is less than you expect, check the feature release level that is specified on each server. A server does not attempt to acquire a feature release product license if its feature release level setting is "Not installed." For more information, see "Setting the Feature Release Level" on page 132.

Server configuration. The lower pane of the **Summary** tab displays each feature release that servers in the server farm are configured to use. For example, if the feature release level of any servers is Feature Release 2, the pane displays "MetaFrame XP Feature Release 2" in the first column.

The appearance of a feature release on the **Summary** tab is not based on whether feature release licenses are installed in the server farm. If you install Feature Release 2 software, for example, or you set the feature release level manually on any server in the farm, the feature release name appears on the **Summary** tab, even if no feature release licenses are installed.

The lower pane of the **Summary** tab also displays the following information:

- The value in the Server Count column is the number of servers whose feature release level is set to the feature release listed in the first column. The data is not based on the licenses installed or in use in the server farm.
- The value in the Connection Count column is the total license count that is installed in the server farm for the listed feature release. If you install feature release connection licenses with license counts of 25 and 50, for example, this column displays 75.

Note The **Connection** tab displays base MetaFrame XP connection licenses; it does not display installed Feature Release 2 licenses. However, if Feature Release 2 connection licenses are installed, the total connection license count appears in the Connection Count column in the lower pane of the **Summary** tab, as described above.

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.

Some configuration options are part of MetaFrame XP Setup. For more information, see “Installing MetaFrame XP” on page 99.

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. MetaFrame XP Setup installs the Citrix Management Console and other tools on the MetaFrame XP server by default when you install MetaFrame XP.

Note Citrix Management Console can be installed on 32-bit Windows workstations (Windows NT, Windows 2000, or Windows XP) from the MetaFrame XP CD-ROM. Browse the Autorun screens to the Citrix Management Console option.

If you are installing the console on a Windows NT 4.0 workstation, you may need to install the latest version of the Windows Installer, available from the Microsoft Web site.

Overview of MetaFrame XP Management Tools

The following summaries of management tools for MetaFrame XP tell you where to find detailed information about 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 Connections” on page 191.

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 161.

Citrix Web Console Citrix Web Console lets you monitor MetaFrame XP server farms from a supported Web browser. You can view server farm information and manage sessions with the Web console. For more information, see “Using Setup” on page 128 and the online help available for the console.

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 222.

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 215.

Shadow Taskbar. Shadowing allows users to view and control other users’ 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 about shadowing, see “Shadowing ICA Sessions” on page 284.

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 “Setting Up Citrix SSL Relay” on page 182.

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.

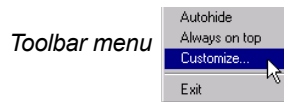
► **To display the Administrator Toolbar**

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 about 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 server farms. Citrix Management Console is a Java-based, extensible program that ships with MetaFrame XP.

The features and capabilities of the console depend on the MetaFrame XP family level installed and licensed in a 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 components you install.

Installation Manager, Load Manager, Resource Manager, and Network Manager are optional components that are installed with MetaFrame XPe. When these components are installed and activated with a MetaFrame XPe license, additional features and functions are added to Citrix Management Console.

MetaFrame XP Setup 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 MetaFrame XP server farms.

In a MetaFrame XP server farm, use Citrix Management Console to:

- Configure server and farm settings
- Create Citrix administrator accounts and assign access to tasks
- Create policies for users or user groups
- 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 users and shadow their ICA sessions

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

To use Citrix Management Console, you must be a Citrix administrator. Citrix administrators can have varying levels of access to areas of MetaFrame XP farm management. For example, you can be a Citrix administrator but have view-only access or even no access to some areas of MetaFrame XP administration. If you try to access an area of the console that you are not authorized to use, the right pane of the console may be blank.

Configuring Citrix Administrator Accounts

When you create a Citrix administrator account, you can select individual user accounts and group accounts from Windows and NDS account authorities. For information about management of Windows domains and user accounts, refer to your Windows system documentation or online help. For information about enabling NDS accounts in server farms, see “Using Citrix Management Console” on page 166.

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.

Citrix administrators manage MetaFrame XP server farms. You can create Citrix administrators accounts with the following permission levels:

- Full access to all areas of MetaFrame XP server farm management.
- View-only access to all areas of server farm management.
- Access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.

Important If you try to access an area of the console that you are not authorized to use, the right pane of the console may be blank.

Restricting access to areas of farm management may not prevent administrators from running some MetaFrame XP command line utilities.

To take full advantage of new features, Citrix recommends that you do not mix releases of MetaFrame XP in the same server farm. For example, do not run Feature Release 1 on some servers in the server farm and Feature Release 2 on other servers in the same farm.

If you use a version of Citrix Management Console released prior to MetaFrame XP, Feature Release 2 to connect to a MetaFrame XP server running a version of MetaFrame XP released prior to Feature Release 2, custom settings applied to Citrix administrators accounts are not recognized.

During MetaFrame XP setup, you must 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 for the new server farm. This Citrix administrator account has full access to all areas of MetaFrame XP. You must log on to Citrix Management Console with this account to add other users to the Citrix Administrators group.

Note One Citrix administrator account that has full access must always exist in the server farm. Therefore, no administrator can delete the last full access Citrix administrator account from the Citrix Administrators group.

Creating Customized Citrix Administrators

You can delegate areas of MetaFrame XP administration and farm management to your IT staff. You can create specialized Citrix administrators and allow them to perform specific administration tasks such as managing printers, published applications, or user policies. Citrix administrators can carry out their assigned tasks without being granted full access to all areas of farm management.

The level of permission to grant for various areas of farm management depends on the specific business function of the administrator. For example, your system or network administrators may need complete access to all areas of farm and server management, while help desk personnel may need view-only access to most areas. You can also grant access to MetaFrame XP features and functions without granting access to Citrix Management Console.

To add users to the Citrix Administrator group, a Citrix administrator with full access logs on to Citrix Management Console and creates other administrator accounts.

Important If you recreate the server farm's data store database, a Citrix administrator account with full administration rights is created using the local administrator account credentials. Be sure to create a new Citrix administrator with full administration rights in Citrix Management Console. Doing so replaces the default Citrix administrator account that uses the local administrator credentials.

Be sure to back up any database before you attempt to recreate it.

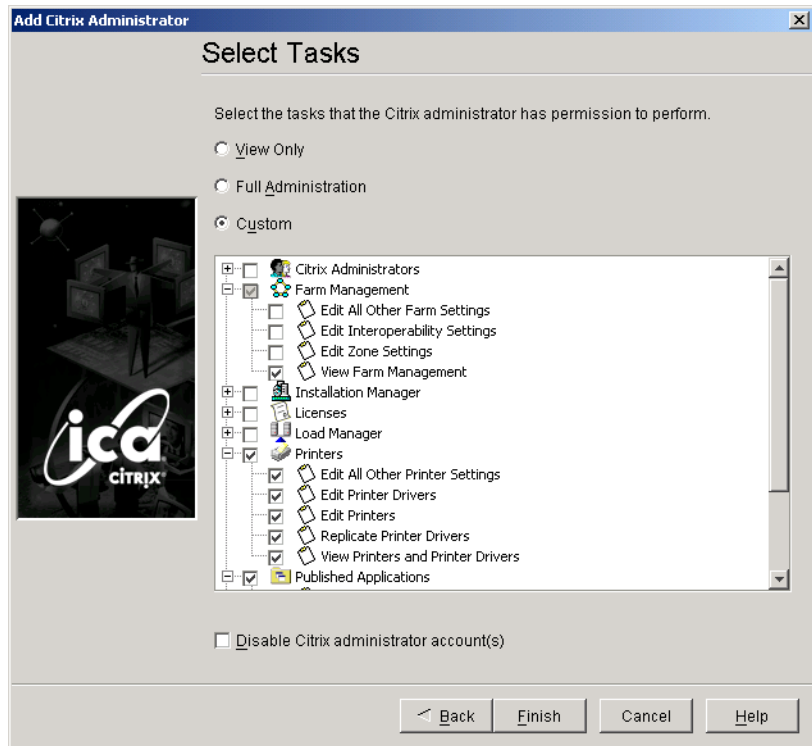
► **To create Citrix administrator accounts and assign tasks**

1. Right-click the Citrix Administrators node in the left pane of the console and choose **Add Citrix Administrator**. The first page of the Add Citrix Administrator wizard appears.

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.

2. Select the user account or group accounts that you want to add to the Citrix Administrators group and then click **Add**.
Click **Add List of Names** to enter user names in a separate dialog box. Select **Show Users** to display all user names in the selected domain.

3. Click **Next** when you have added the users or groups to the list of configured accounts. The second and final page of the Add Citrix Administrators wizard appears.



4. Select the level of permission you want this Citrix administrator account to have.
Select **View Only** to allow view-only access to all areas of MetaFrame XP administration. Select **Full Administration** to allow full access to all areas.
5. To grant access to only some areas of MetaFrame XP administration, select the areas or specific tasks within an area you want the administrator to be able to access.
For example, you can create one Citrix administrator account that has full access to all printer management tasks, but view-only access to published application information.

Important You can deny access to Citrix Management Console and Citrix Web Console by expanding the Citrix Administrators node and clearing the check mark from the **Log on to Citrix Management Console** task. This capability is allowed by default for all new Citrix administrator accounts.

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.

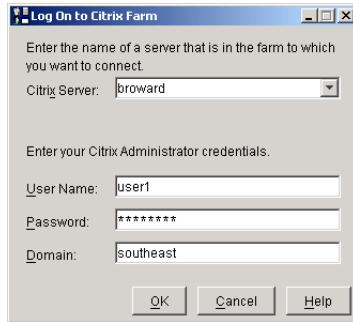
To log on to a Citrix server farm with the console, specify any Citrix server in the server farm. The console connects to the Citrix server and then displays information for the entire Citrix server farm and for the individual servers in the farm.

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 You can use Citrix Management Console to monitor and manage MetaFrame XP server farms. However, you cannot use the console to manage MetaFrame 1.8 server farms. When MetaFrame XP servers are set to interoperate with MetaFrame 1.8 servers, the console displays information about MetaFrame XP server farms only.

► To use Citrix Management Console

1. From the **Start** menu, choose **Programs > Citrix > Citrix Management Console**, or click the corresponding 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 on 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.

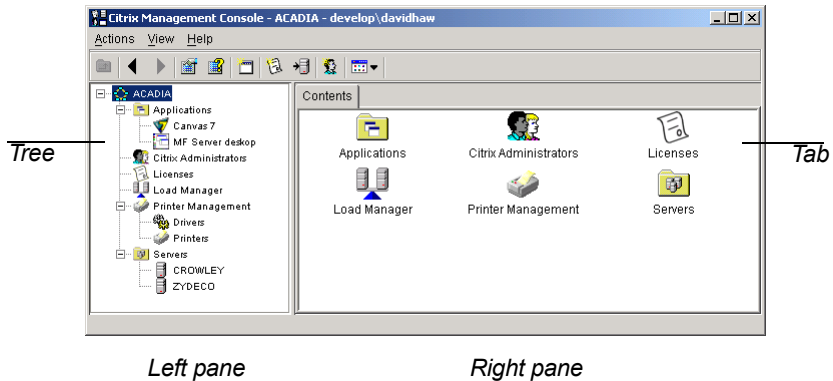
► To view online help in Citrix Management Console

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.

Citrix Web Console

Citrix Web Console lets you monitor MetaFrame XP server farms by using a Web browser. You can view information about a server farm, including its active sessions, published applications, servers, and users.

With the Web console, you can also manage sessions by logging off sessions, shadowing sessions, disconnecting sessions, and sending messages to users, the same as you would with Citrix Management Console.

You can use the MetaFrame XP CD to install the Web console on MetaFrame XP servers or on servers not running MetaFrame XP. From the Autorun screen, browse to the option to install the Web console.

The Web console server must be in the same security context as the MetaFrame server. Local accounts work only if the Web console server is also acting as a MetaFrame server. You cannot use Novell Directory Services (NDS) accounts with the Web console.

For more information about using the Citrix Web Console on a computer that is not running MetaFrame, see *Advanced Concepts for MetaFrame XP*, available from the Citrix Web site. This document is revised for each new feature release, so be sure to read the latest version.

Citrix Web Console supports Microsoft Internet Explorer 4.0 and later Web browsers.

To use Citrix Web Console, the server must have Microsoft Internet Information Services (IIS) 5.0 (or later) installed.

Important Citrix Web Console does not encrypt information that it sends to Web browsers. When a user logs on to the console, the user's Citrix administrator credentials are sent to the Web console as unencrypted text. For maximum security, configure your Web browser and IIS to use SSL encryption. For information about setting up SSL communication, refer to the documentation for IIS and your Web browser.

After you install the Web console, the default URL for accessing the console is `http://hostname/Citrix/WebConsole`, where *hostname* is the name of the MetaFrame XP server on which the Web console is installed.

When you browse to the URL for the Web console, a logon dialog box appears. Enter your Citrix administrator username and password to log on to the console. If the Citrix administrator account is not a local administrator account on the host server, you must enter the domain and username in the **User Name** box, as follows:

domain/username

For more information about using the Web console, log on to the console and click Help.

Configuring MetaFrame XP Properties

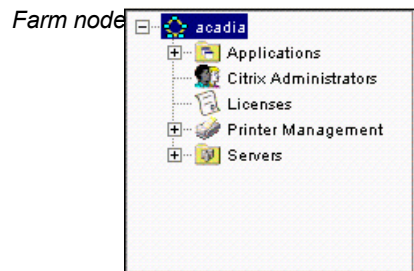
Configuring options and settings for MetaFrame XP servers and Citrix server farms takes place in two stages. First, you set options when you install MetaFrame XP on the first server in a server farm and on other servers that you add to the farm. Then, as the server farm is operating, you can adjust settings 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 about setup options for MetaFrame XP servers and server farms, see “Installing MetaFrame XP” on page 99.

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 interoperation 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 99.

MetaFrame XP also includes some commands that you can run from the command prompt to monitor and configure servers. For information about 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 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 Settings** 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 Settings** 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 Settings** 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 that 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 Settings** 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.

Content Redirection from Server to Client

Enable Content Redirection from server to client for the entire server farm on the **MetaFrame Settings** tab. When you enable Content Redirection from server to client, embedded URLs are intercepted on the MetaFrame server and sent to the ICA Client using the ICA Control virtual channel. The user's locally installed browser is used to play the URL. Users cannot disable this feature. You can use the farm-wide setting, or enable the feature on selected servers only.

ICA Client Time Zones

If users 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 the **SNMP** tab in the **Properties** dialog box for individual servers or for the farm.

To enable SNMP notification messages on a farm-wide basis, select **Enable SNMP Agent** on the **SNMP** tab in the **Properties** dialog box for the farm.

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

SNMP notification is available when you install the Citrix plug-ins for Tivoli NetView, HP OpenView, or CA Unicenter TNG network management consoles. For information about which SNMP management consoles you can use with Network Manager, see the documentation for Network Manager in the Docs directory on the MetaFrame XP CD-ROM.

Configuring 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 99. MetaFrame XP also includes some commands you run from the command prompt to monitor and configure servers. For information about 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 175.

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 140.

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 Settings options. The options on the **ICA Settings** 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 Settings** 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.

Content Redirection from Server to Client. Enable Content Redirection from server to client for the selected server on the **MetaFrame Settings** tab. When you enable Content Redirection from server to client, embedded URLs are intercepted on the MetaFrame server and sent to the ICA Client using the ICA Control virtual channel. The user's locally installed browser is used to play the URL. Users cannot disable this feature. You can use the farm-wide setting, or enable the feature on the selected server only.

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 297.

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 Zones and Data Collectors

In a MetaFrame XP server farm, a *zone* is a grouping of MetaFrame XP servers that share a common *data collector*, which is a MetaFrame XP server that receives information from all the servers in the zone.

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, to change the zones of MetaFrame XP servers, and to configure zone data collectors.

Important If you change a server's zone membership (move the server to another zone), incorrect information can appear in Citrix Management Console until the server updates the data collector. To ensure data synchronization, restart a MetaFrame XP server after you change its zone membership.

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.

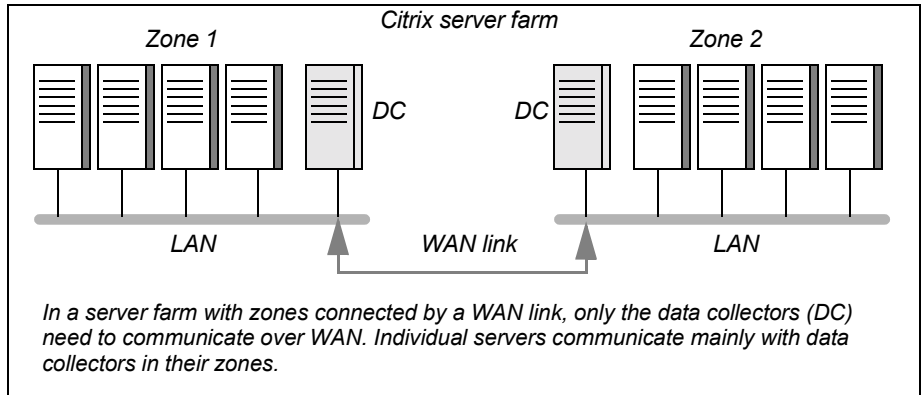
- If all the servers in a farm are in one location, you can configure the farm with a single zone without causing slower performance or making the farm more difficult to manage.
- If you manage an enterprise server farm with servers in different geographic regions, you can place servers into zones based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

Functions of Data Collectors

Each zone in a server farm contains one Citrix server that is designated as the data collector for 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.

Setting Up Citrix SSL Relay

The Citrix SSL Relay can secure communications between ICA Clients, NFuse Classic Web servers, and MetaFrame XP servers using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

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 the port must be open on firewalls to MetaFrame XP servers running the SSL Relay.

Note When you install MetaFrame XP, Feature Release 2, members of the User group are allowed to edit registry entries in the registry hive
HKEY_LOCAL_MACHINE\SOFTWARE\Secure\Citrix\Citrix SSL Relay.

You can use the Microsoft Security Configuration and Analysis tool to prevent members of the User group from editing these registry entries.

Important If you change the default Citrix SSL Relay port, you must set SSLProxyHost to the new port number in the ICA Win32 Client's Appsrv.ini file. For more information about client settings, see the *ICA Win32 Client Administrator's Guide*.

► To configure the SSL Relay

1. Obtain a server certificate.
2. Change the SSL Relay port number, if necessary. To use the SSL Relay and Internet Information Services (IIS) on the same server, you must change the port number used by IIS or the SSL Relay. See "Changing the SSL Relay Port" on page 187.
3. Install the server certificate on the SSL Relay server.
4. Select the allowed ciphersuites. See the online 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 and Installing Server Certificates

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 use 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>.

Important The common name for the certificate must be the fully-qualified domain name of the server.

Citrix NFuse Classic and the Citrix ICA Clients include 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 client devices. See the documentation for the client operating system for instructions about installing a root certificate.

Importing an Existing Certificate

If you have certificates that were used for the previous version of SSL Relay, you can use the PEMtoPVK utility to convert PEM-formatted certificates into PVK-formatted certificates, which can then be imported into the Microsoft Certificate store.

If you already have a server certificate installed in IIS, you can use it with the Citrix SSL Relay. See “To use the Microsoft Management Console (MMC) to import an existing certificate” below.

► To convert a PEM format certificate to PVK format

At the command prompt, type:

pemtopfx <space> <pem cert path>

The PEMtoPVK utility creates a new PVK-formatted certificate file that can be imported into the correct Microsoft Certificate store.

Important You can import a PEM-formatted certificate directly; however, this will not maintain the private key and invalidates the certificate for use with the SSL Relay.

- ▶ **To use the Microsoft Management Console (MMC) to import an existing certificate**
 1. Run the Microsoft Management Console by choosing **Start > Run**, typing **mmc**, and clicking **OK**.
 2. If you do not see a Console Root folder, you must add the Certificates Snap-in.
 1. From the **Console** menu, choose **Add/Remove Snap-in**. The **Add/Remove Snap-in** dialog box appears.
 2. Click **Add**. The **Add Standalone Snap-in** dialog box appears.
 3. Select **Certificates** and click **Add**. The **Certificates snap-in** dialog box appears.
 4. Click **Computer account** and then click **Next**. The **Select Computer** dialog box appears.
 5. Verify that **Local computer** is selected and then click **Finish**.
 6. Click **Close** to close the **Add Standalone Snap-in** dialog box.
 7. Click **OK** to close the **Add/Remove Snap-in** dialog box.
 3. In the left pane of the console, click the plus sign for **Certificates (Local Computer)** to expand the folder.
 4. In the left pane of the console, click the plus sign for **Personal** and then click **Certificates**.

If the Personal\Certificate store already contains a certificate for the computer, the following steps can be omitted.
 5. In the right pane of the console, right-click the certificate to import, select **All Tasks**, and then click **Import**. The **Certificate Import** wizard appears.
 6. Click **Next** and then click **Browse** to search for the certificate file to be imported.
 7. Select the certificate file and click **Next**.
 8. Enter the private key password in the **Password** box and click **Next**.
 9. Click **Next** to accept the default values in the next window and then click **Finish** to import the certificate.

Requesting a Certificate Using the Microsoft Management Console

The MMC certificate snap-in can be used only to request certificates if the server is part of an active directory domain that has a Microsoft Certificate Server installed.

See the Microsoft documentation for further details.

Requesting a Certificate Using IIS

If you already have a certificate for an HTTPS Web server, you can use this certificate for SSL Relay. In this instance you can omit the following steps and directly configure SSL Relay.

► To create a certificate request using the IIS

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 choose **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.
5. Click **Next** and select **Create a New Certificate**.
6. Click **Next** and select **Prepare the Request Now, but send it later**.
7. In **Bit Length**, enter the bit length to be used for the certificate's encryption strength. Citrix recommends that you select 1024 or higher. Click **Next**.
8. Enter details in the **Organization Information** field and click **Next**.
9. Ensure that the **Common Name** matches the FQDN of the MetaFrame server on which the SSL Relay will run and click **Next**.
10. Enter details into the **Geographical Information** field and click **Next**.
11. Type the path and file name for the certificate request, or accept the default value, and click **Next**.
12. Ensure that the information in the **Request File Summary** is correct. Click **Next** and then **Finish**.

The information in the Certificate Signing Request can be sent to any Certificate Authority for signing.

► **To import a certificate from the Certificate Authority**

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 choose **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.
5. Click **Next** and select **Process Pending Request**.
6. Ensure that the path for the certificate file is correct; otherwise select **Browse** to search for the file.
7. Click **Next**.
8. Ensure that the information is correct. Click **Next** and then **Finish**.

Microsoft Internet Information Services saves the certificate in the Local Computer\Personal store so that the certificate can also be used by SSL Relay.

Exporting a Certificate Using the Microsoft Management Console

Before you can install the server certificate on SSL Relay, you must export the certificate to PKCS #12 (Personal Information Exchange Syntax Standard) format.

► **To export a certificate**

1. Run the **Microsoft Management Console** and load the snap-in for **Certificates**. The **Certificates snap-in** dialog box appears.
2. Select **Computer Account** and click **Next**. The **Select Computer** dialog box appears.
3. Select **Local Computer** and click **Finish**.
4. Click **Close** and then **OK**.
5. In the console tree, select **Certificates > Personal > Certificates**. A list of available certificates is displayed in the right pane.
6. In the details pane, click the certificate you want to export.
7. From the **Action** menu, choose **All Tasks > Export**. The Certificate Export wizard screen appears. Click **Next**.
8. In the **Export Private Key** dialog box, select **Yes, export the private key**. (This option appears only if the private key is marked as exportable and you have access to the private key.) Click **Next**.

9. In the **Export File Format** dialog box, check the **Enable strong protection** box. Click **Next**.
10. In the **Password** dialog box, type a password to encrypt the private key you are exporting. Take precautions to keep the specified password safe because you are required to enter this password when you install the certificate. Click **Next**.
11. In the **File to Export** dialog box, type a file name and path (for example, *filename.pfx*) for the PKCS #12 file that will store the exported certificate and private key. Click **Next**.
12. Click **Finish** to complete certificate export.

You can now import the certificate into SSL Relay. See “To use the Microsoft Management Console (MMC) to import an existing certificate” on page 184.

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 client devices and the MetaFrame XP server running the SSL Relay.

Important Microsoft Internet Information Services (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. You must install a server certificate on IIS before you change the port number. The following procedure includes instructions for adding a server certificate to IIS. You can use the same server certificate with IIS and the SSL Relay.

► To change the SSL port for Internet Information Services 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 choose **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 create or import a certificate.
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 Citrix SSL Relay port number**

1. Choose **Start > Programs > Citrix > MetaFrame XP > Citrix SSL Relay Configuration Tool** to run the SSL Relay configuration utility.
2. On the **Connection** tab, type the new port number in the **Relay Listening Port** box.
3. Click **OK**.

See the *NFuse Classic Administrator's Guide* for the procedure to reconfigure NFuse Classic Web servers with the new port number.

► **To run SSL Relay on port 443 without using HTTPS**

1. Stop the Microsoft Internet Information Service.
2. Configure and start the SSL Relay service.
3. Restart the Microsoft Internet Information Service.

SSL Relay will use port 443 before IIS, including when the server is restarted.

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.

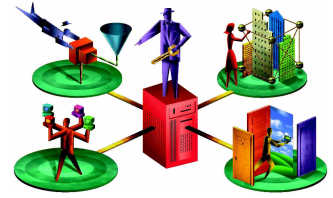
Deploying SpeedScreen Settings

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 apply SpeedScreen settings to a specific instance of the application.

Configuring ICA Connections



MetaFrame XP lets 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.

Overview of ICA Connections and Sessions

Users can 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 about 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 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 (Windows 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 are 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 about procedures for adding and modifying connections, choose **Contents** from the **Help** menu in Citrix Connection Configuration.

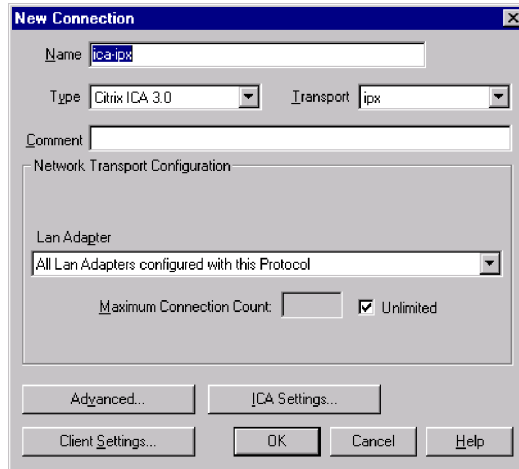
Adding ICA Connections

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”).
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 cannot 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.

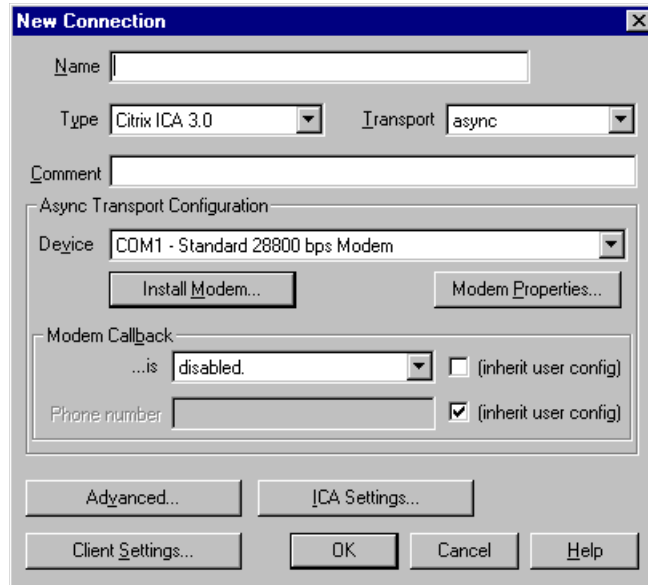
When you set up an asynchronous ICA connection in Citrix Connection Configuration, you avoid the overhead of Dial-Up Networking and TCP/IP on the server. MetaFrame XP supports modem configuration through the Windows Telephony Application Programming Interface (TAPI).

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 193).
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 cannot 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 time-out value in the **Advanced Connection Settings** dialog box. This time-out 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 dial-in settings for Windows NT or Windows 2000.

For more information about 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 about 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.

Important You can create user policies to enable some connection settings for specific users or user groups. User policies override similar settings configured in Citrix Connection Configuration. However, if you disable functionality in Citrix Connection Configuration, you cannot enable the functionality by creating user policies. For more information about user policies, see “Creating and Applying User Policies” on page 281.

Configuring ICA Connection Options

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 about 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.

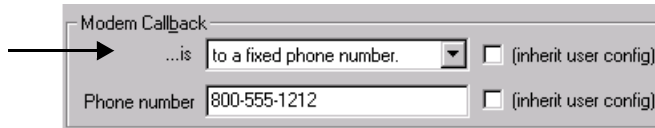
Modem callback to a fixed number can provide a small level of security based on telephone numbers. Using this feature verifies that authorized users are dialing in by calling back to specified numbers to complete dial-in ICA connections.

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, 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, you enter a callback phone number in the **Dialin Information** dialog box, which is available from the **User Properties** dialog box for each user account. In Windows 2000, you enter a phone number 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 uses 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.

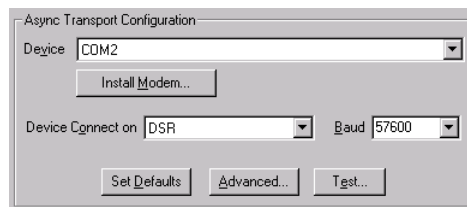
Configuring Direct Cable Connections

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.

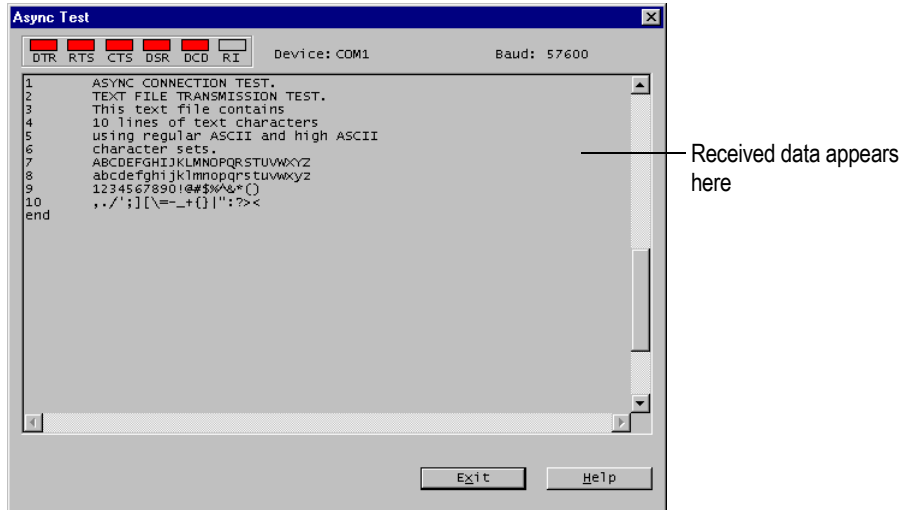
Advanced. Opens the **Advanced Async Configuration** dialog box for configuring additional serial port settings. These settings are described in the next section.

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.

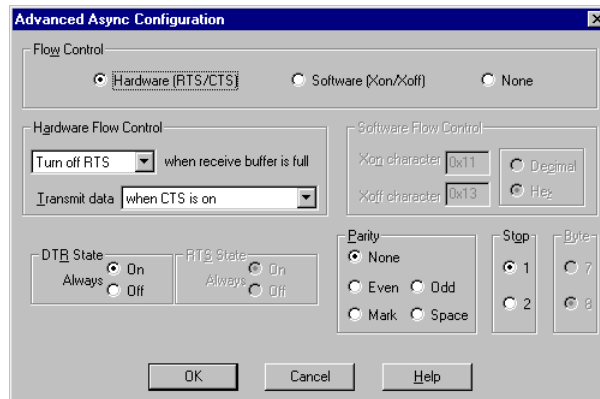
Configuring Advanced Async Options

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.

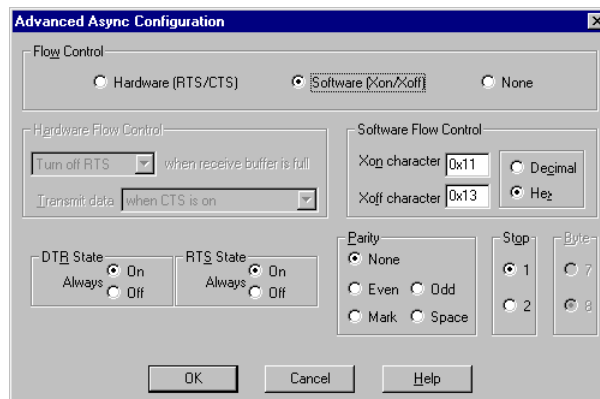
Hardware Flow Control. If you select Hardware in the Flow Control area, the options in the Hardware Flow Control area are available to specify signals used for flow control. Hardware flow control is the default configuration.

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 for 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

Logon
☐ Disabled ☒ Enabled

Timeout settings (in minutes)
 Connection: ☐ No Timeout
☐ (inherit user config)
 Disconnection: ☐ No Timeout
☐ (inherit user config)
 Idle: ☐ No Timeout
☐ (inherit user config)

Security
 Required encryption:
☐ Use default NT Authentication

AutoLogon
 User Name:
 Domain:
 Password:
 Confirm Password:
☐ Prompt for Password

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, the session. ☐ (inherit user config)
 Reconnect sessions disconnected ☐ (inherit user config)
 Shadowing ☐ (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.

MetaFrame XP provides additional options for controlling connections from ICA Clients, limiting ICA sessions, and restricting application usage. For more information, see “Controlling Logons by ICA Clients” on page 265 and “Controlling User Connections” on page 266.

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 log on only or to all data transmission.

Using Shadowing to Monitor ICA Sessions

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 about how to shadow sessions, see “Shadowing ICA Sessions” on page 284.

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

During installation of MetaFrame XP, if you select the option that prohibits shadowing, 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 unavailable. For more information about user configuration, see “Precedence of Settings” on page 197.

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. “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. “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.

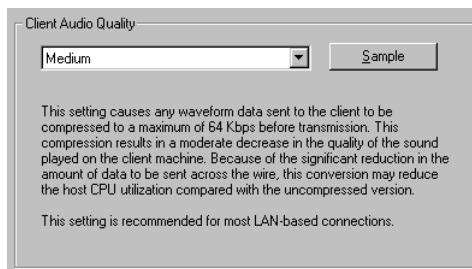
When you click the **ICA Settings** button, the **ICA Settings** dialog box appears. From the drop-down list in the Client Audio Quality area, you can specify the audio quality to use for the connection. High, Medium, and Low audio quality settings are available.

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 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 about 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 about 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, and so forth. 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 cannot map client device drives to letters that are assigned to the server's own disk drives.

During MetaFrame XP installation, Setup 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 users, because they 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.

CAUTION 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 When Using NetWare Logon Scripts

Client drive mapping and NetWare logon script execution occur in parallel. If the logon 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:

CAUTION Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Make sure you back up the registry before you edit it. If you are running Windows NT, make sure you also update your Emergency Repair Disk.

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 devices). 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 291. 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 about the **change client** command.

For more information about client COM port mapping, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

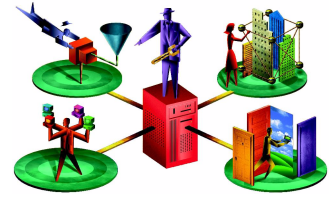
Client Audio Mapping

Client audio mapping allows applications running on the Citrix server to play sounds through a sound device on the client device. 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 about 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 ICA Client software to end users.

Choosing a Deployment Method

To access applications on MetaFrame XP servers, 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 Microsoft Systems Management Server (SMS) or Active Directory Services in Windows 2000 (for ICA Clients that can be installed with Windows Installer packages)
- 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 MetaFrame XP Components 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 or deploying with Active Directory or Microsoft Systems Management Server are the best choices.

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 Classic	Users click links on their desktops or run a supported Web browser (see the <i>NFuse Administrator's Guide</i> for a full list).
Enterprise, ASP, small business	Active Directory or Systems Management Server (SMS)	Users download ICA Client software from a centralized location. See your Windows 2000 or SMS documentation for more information.
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 Classic, or the Application Launching and Embedding (ALE) feature in MetaFrame XP. When you deliver applications using a Web-based method, users click links on their desktops using the Program Neighborhood Agent or launch Web browsers to access applications published on MetaFrame XP servers.

If you do not want to deliver applications to your users through 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 Classic

If you implemented or plan to implement a corporate Web-based portal, use Citrix NFuse Classic with MetaFrame XP to integrate personalized application sets and information into your company's Web site. With NFuse, users can access published applications through program icons on their desktops, or in their Start menus (with the Program Neighborhood Agent), or through Web browsers.

An NFuse Classic system consists of three components: a MetaFrame XP server farm, a Web server, and client devices. 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 presents the appropriate ICA Client software for download and setup.

Important You can install NFuse Classic on the MetaFrame XP server as part of MetaFrame XP Setup. Install NFuse on the MetaFrame XP server only if IIS 4.0 or IIS 5.0 is also present on the server.

If you choose to install NFuse, an NFuse Web site is installed on your MetaFrame XP server in a Citrix directory under the Web document root; for example, `c:\inetput\wwwroot\citrix\NFuse`.

This Web site contains logic that at runtime references the server's document root directory for the presence of ICA Clients. To use the ICA Client installation feature of NFuse, copy the ICA Clients from the Icaweb directory on the MetaFrame XP Components CD to a directory named Icaweb in the Citrix directory in the Web document directory; for example, `c:\inetpub\wwwroot\citrix\icaweb`.

You must copy the entire Icaweb directory to this directory to enable Web-based ICA Client installation from the NFuse Web site.

If you plan to implement a Citrix NFuse system, see the *NFuse Administrator's Guide* for more information. If you do not implement a Citrix NFuse system but want to deploy ICA Client software using the Web, see "Web-Based Installation" on page 221.

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 about 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 users. Providing a simple installation process that requires little interaction from 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 MetaFrame XP Components CD

The MetaFrame XP Components CD contains setup and installation files for all ICA Clients. You can use the MetaFrame XP Components CD to directly install ICA Client software on client devices that have CD-ROM drives, or copy the CD image to a network share point on a file server. For more information about installing ICA Client software, see the *Administrator's Guide* for the required ICA Client.

You can copy the necessary files from the MetaFrame XP Components 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 **Start > Programs > Citrix > MetaFrame XP > ICA Client Distribution Wizard**.

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 about running the ICA Client Distribution wizard, see “Installing ICA Client Software” on page 119.

Pass-Through ICA Client

The ICA Client Distribution wizard installs the pass-through ICA Win32 Client on the server. You can give users who run 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 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 MetaFrame XP Components 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.

Using Installer Packages for Client Deployment

The ICA Client for Win32—full Program Neighborhood and Program Neighborhood Agent versions—are both available in Microsoft Windows installer packages (.msi files), so you can use Windows Installer technology to deploy and install them. You can distribute the ICA Win32 Client installer package files to users by using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows 2000.

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

The ICA Win32 installer package files are located in the following directories (substitute *language* with the language of the ICA Client software) on the MetaFrame XP Components CD included in the MetaFrame XP Feature Release 2 media pack:

Icaweb\language\ica32

where *language* is one of:

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

The installer package for the Program Neighborhood Agent is also located in the directory Icainst\language\ica32\pnagent.

Note The Windows Installer service is present by default on computers running Windows 2000. If the computer is running Windows NT 4.0 or Windows 9x, you must install Windows Installer.

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.

If you want to set up an ICA Client download Web site on a Windows-based Web server, you can download the components and documentation for Web-based installation from the download area of the Citrix Web site at <http://www.citrix.com/download>.

Tip If you are planning to implement a Citrix NFuse system, see the *NFuse Classic Administrator's Guide* for information and instructions about deploying the ICA Clients with NFuse Classic.

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 MetaFrame XP Components 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 client software setup program. .
4. To install the ICA Client software, launch Setup to begin the installation process. For more information about 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 about 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 MetaFrame XP Components CD to your MetaFrame XP 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 MetaFrame 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.

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.

The process of updating ICA Clients with new versions uses the standard ICA protocol.

- If an update is needed, by default, the MetaFrame XP 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 MetaFrame XP 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 MetaFrame XP 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 drive.

Configuring the Client Update Database

You can configure a Client Update Database on each MetaFrame XP server in a server farm, or configure one database to update the ICA Clients for multiple MetaFrame XP 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 119.

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

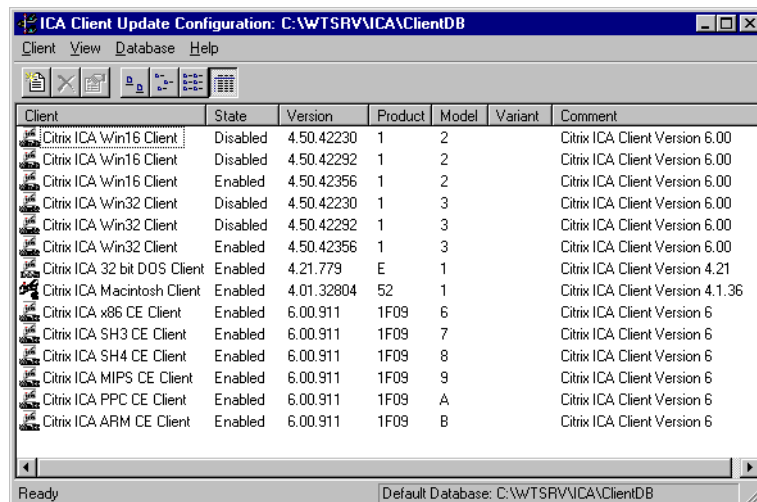
Use the Client Update Configuration utility to manage the client update database. From this utility, you can:

- 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 MetaFrame XP server uses to update ICA Clients. The window shows the ICA Clients in the database.



Creating a New Client Update Database

The ICA Client Distribution wizard creates the Client Update Database in the location %SystemRoot%\Ica\ClientDB. You can create a new update database in any location on a server disk or on a network share point.

► To create a new update database

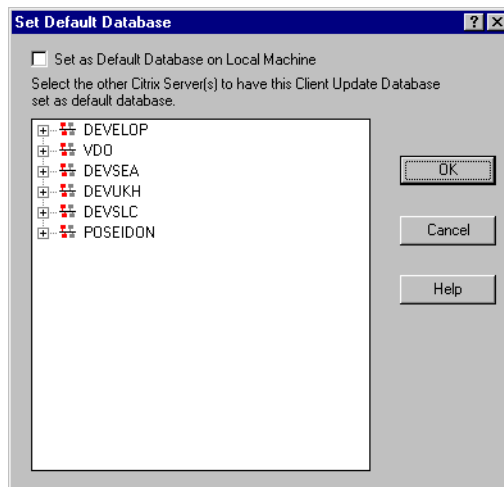
1. From the **Database** menu, choose **New**. The **Path for the new Client Update Database** dialog box appears.
2. Enter the path for the new update database and click **Save**. The utility creates a new update database in the specified location and opens the new database.

Specifying a Default Client Update Database

You can configure one Client Update Database to be used by multiple MetaFrame XP servers. If the Client Update Database is on a shared network drive, use the ICA Client Update Configuration utility to configure your MetaFrame XP servers to use the same shared database.

► To set the default database for MetaFrame XP servers

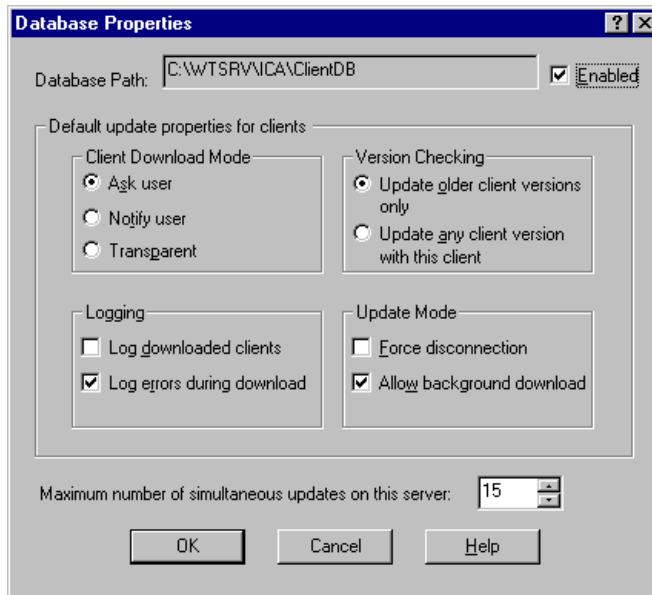
1. From the **Database** menu, choose **Open**.
2. Specify the path to the default database and click **Open**. The database opens.
3. On the **Database** menu, click **Set Default**. The **Set Default Database** dialog box opens:



4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other MetaFrame XP 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.

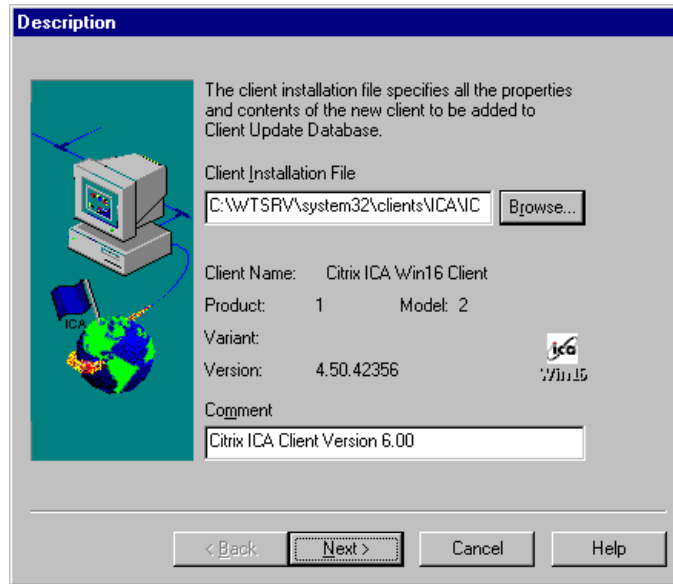
Click **OK** when you finish configuring the database settings.

Adding ICA Clients to the Client Update Database

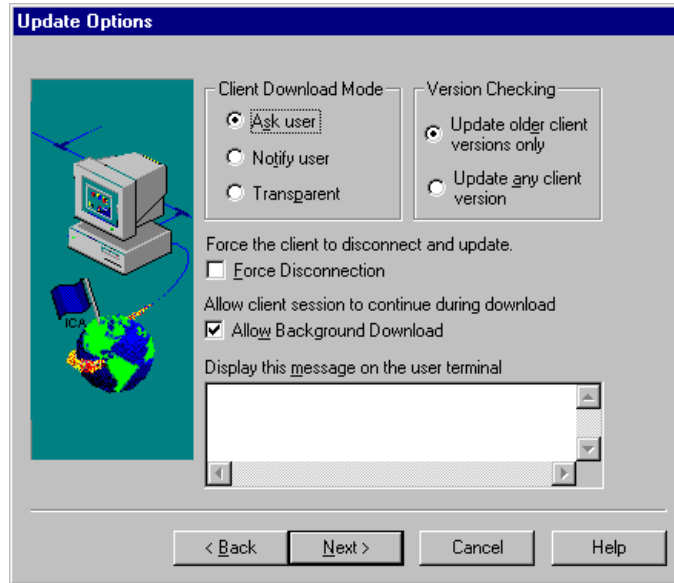
When you want to deploy a newer version of the ICA Client, add it to the Client Update Database. You can download the latest ICA Clients from the Citrix Web site at <http://www.citrix.com/download>.

► 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 MetaFrame XP Components CD.

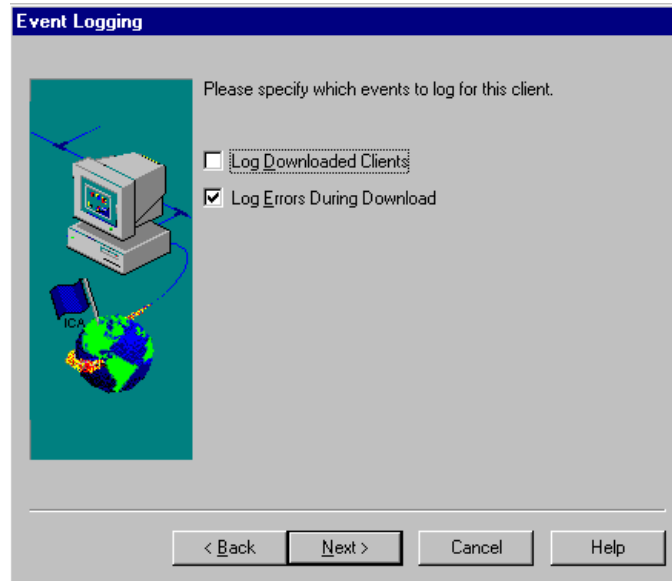


3. The client name, product number, model number, and version number are displayed. The **Comment** text box displays a description of the new client. You can modify this comment. Click **Next** to continue.
4. The **Update Options** dialog box appears. The options in this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients.



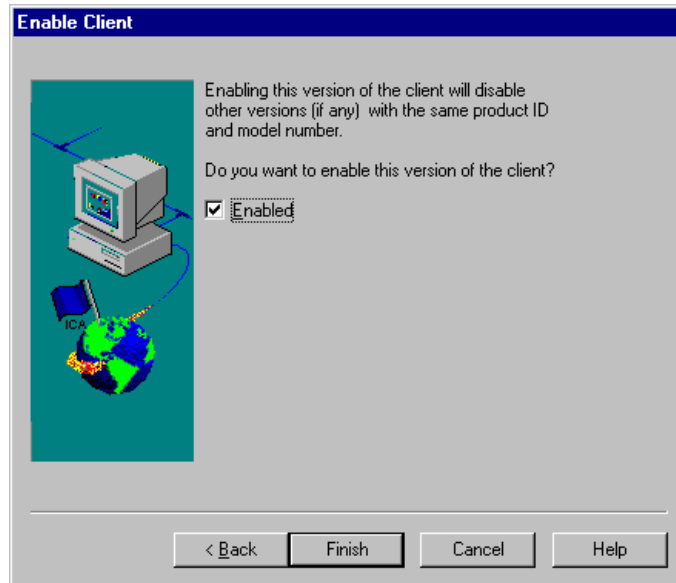
For definitions of the options in this dialog box, see “Configuring Default Client Update Options” on page 227, or see the online help for this dialog box. Click **Next** when you finish configuring the client update options.

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** to continue.

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.

7. 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

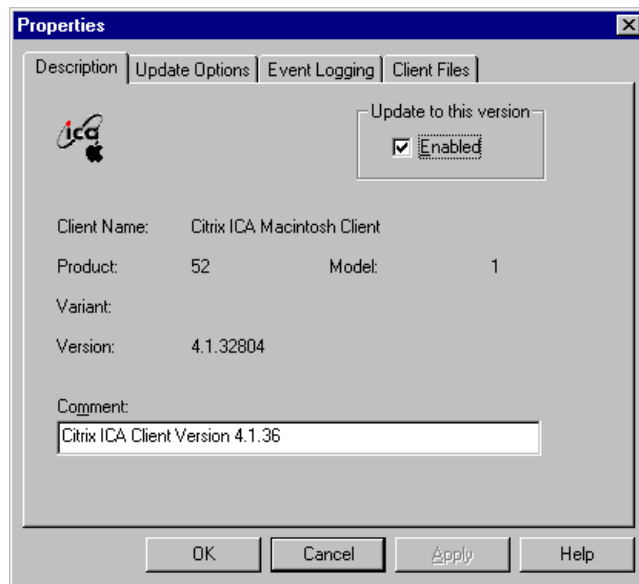
1. Select the ICA Client you want to remove from the database.
2. From the **Client** menu, choose **Delete**. A message asks you to confirm the deletion.
3. Click **Yes** to remove the client.

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.

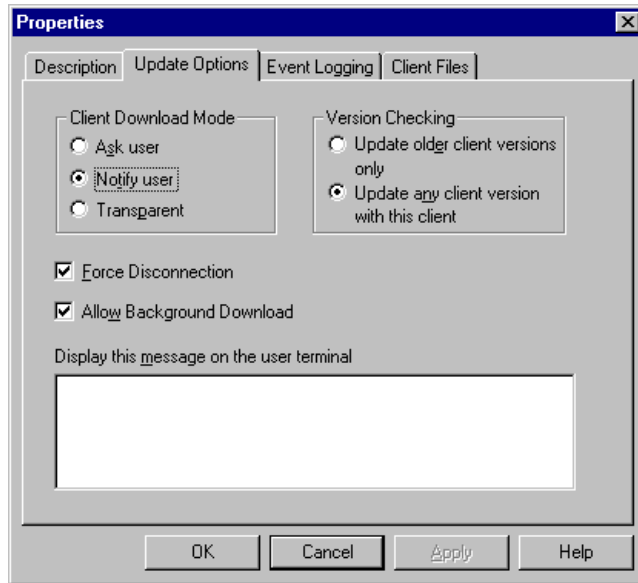
► **To change the properties of an ICA Client in the Client Update Database**

1. Select the client you want to change.
2. On the **Client** menu, choose **Properties**. The **Properties** dialog box appears.

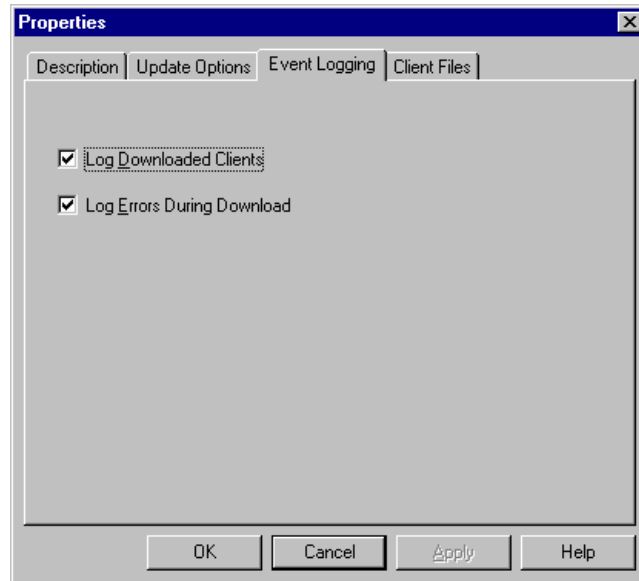


3. The **Description** tab lists the client name, product number, model number, and version number. Select the **Enabled** check box to update the same platform ICA Client to this version. Optionally, enter a new comment in the **Comment** box.
4. Use the **Update Options** tab to configure update options 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.

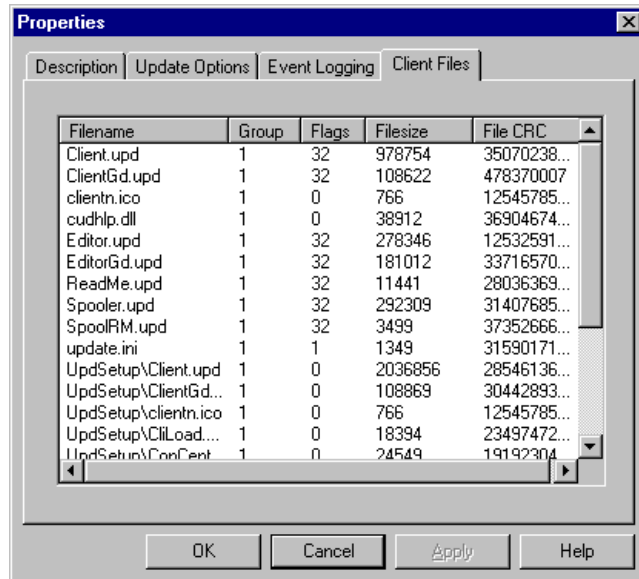
- Select the **Force Disconnection** option to require users to disconnect and complete the update process after downloading the new client.
- Select the **Allow Background Download** option to allow users to download new client files in the background and continue working. Clear this check box to force 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

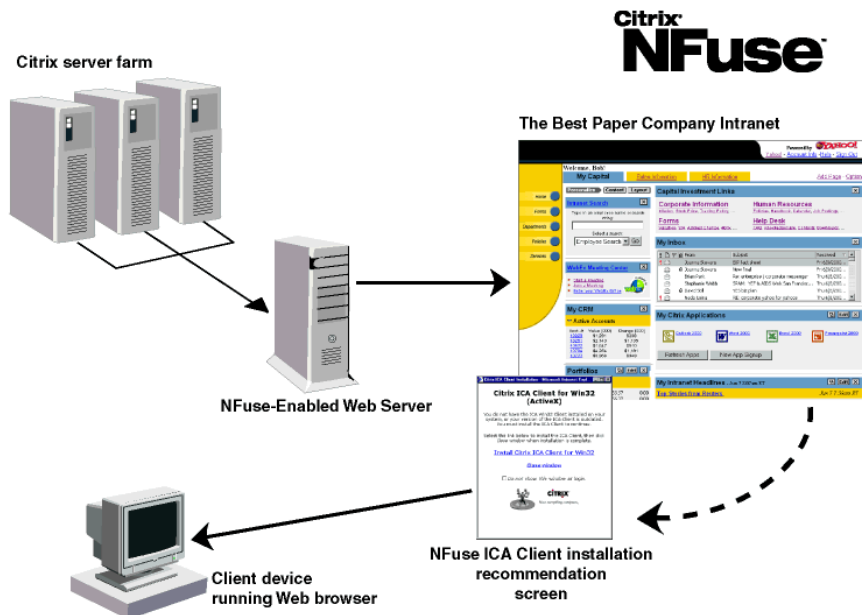
This section provides examples of ICA Client deployment practices for a large manufacturing enterprise, a regional bank, an application service provider, and an insurance company.

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 Classic to give users access to critical applications. The company's existing MetaFrame XP 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 Classic logon page. 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 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 Ceridian 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
- One hundred 486 PCs, Wyse Winterm Windows-based terminals

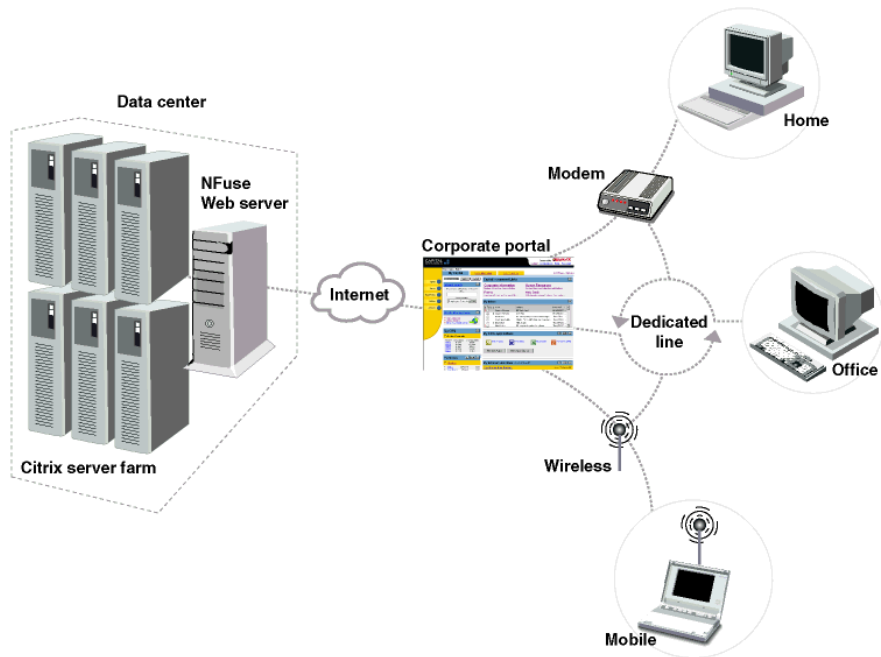
The bank's IT department used the Web-based ICA Client Installation package (without NFuse) to construct an ICA Client download Web site, integrated into the bank's Intranet, for ICA Client software deployment. The IT department posted user-friendly instructions that walk users through downloading and installing the ICA Client software.

For more information about constructing an ICA Client download Web site, see "Using Installer Packages for Client Deployment" on page 221 of this guide. The elements required to construct an ICA Client download Web site can also be obtained 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.15 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 MetaFrame XP server farms, including MetaFrame XP for Windows and MetaFrame for UNIX servers, in a single Web page.

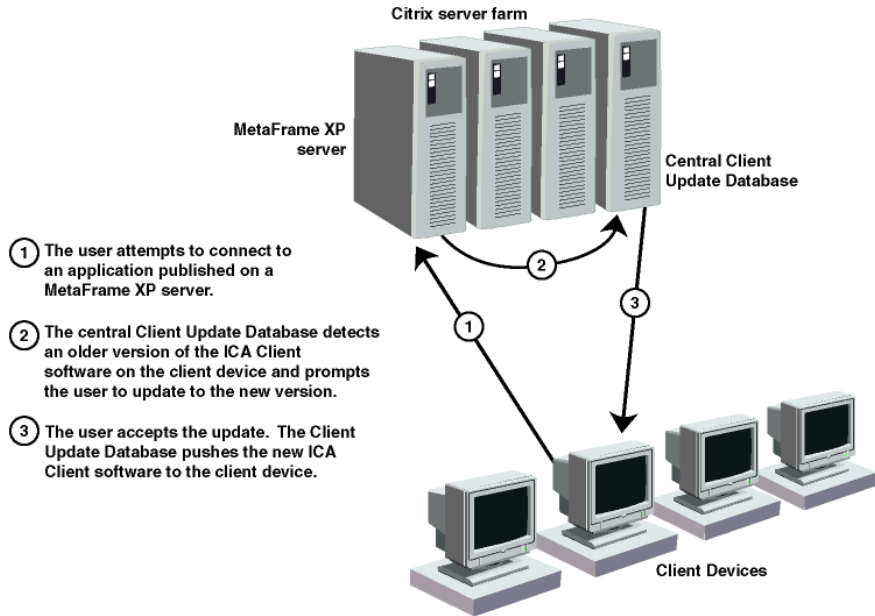
The Web developers at LinkToUs created a simple script that allows automatic download and install of the ICA Win32 Web Client. When end-users access the corporate portal hosted by LinkToUs for the first time, the ICA Client is automatically downloaded and installed on the user's computer.

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

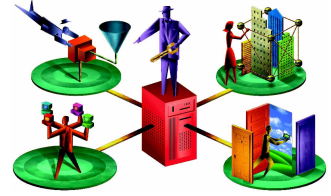


The purchasing department preconfigures users' systems to include the latest version of the ICA Win32 Client. When applications are published, a shortcut to each application is placed on the user's **Start** menu. Users can also launch Program Neighborhood to access other application sets they have permission 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 223 of this guide.

Making Information Available to Users



With MetaFrame XP, you can expand users' access to information. You make information available to users by *publishing* applications and files on MetaFrame XP servers. You then decide whether users should open certain file types with these published applications or with applications running locally on client devices.

Using MetaFrame's publishing capability, you can make the following types of resources available:

- Applications installed on MetaFrame servers. When users access them, the published applications appear to be running locally on client devices.
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).
- The MetaFrame server's desktop, so users can access all of the resources available on the server.
- Data files such as Web pages, documents, sound files, spreadsheets, and URLs. In MetaFrame XP, the combined total of data types you can publish is referred to as *content*.

Load Managed Applications

If you are licensed for MetaFrame XPa or MetaFrame XPe, you can use Citrix Load Manager to publish an application to be hosted on multiple servers.

When a 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 about configuring load evaluators, see *Getting Started with Citrix Load Manager*, available in the Docs folder on the MetaFrame XP CD-ROM.

Installation Manager Applications

If you are licensed for MetaFrame XPe, you can install and publish Installation Manager packages for users to access. Using Installation Manager, you can simultaneously install an out-of-the-box application on all MetaFrame XP servers on your network from a single point without manual intervention.

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.

For more information about using Installation Manager, see *Getting Started with Citrix Installation Manager*, located in the Docs directory on your MetaFrame XP CD-ROM.

Using NFuse Classic to Present Applications

If you want to provide users with access to published applications and content with a Web-based solution, you can use NFuse Classic if you have a single MetaFrame XP server farm, or Enterprise Services for NFuse if you have multiple server farms. For more information about these products, see the *Administrator's Guide* for each of them. These guides are located in the Docs directory on your MetaFrame XP CD-ROM.

Deciding How Users Access Information

Before you begin publishing applications and content, review your network to identify obstacles that interfere with effectively managing resources. For example, you may encounter problems in the following areas:

- **Heavy server loads.** Users are viewing and downloading applications and files that consume a lot of bandwidth, which makes your network slow or unusable.
- **Security of servers and client devices.** Users frequently introduce viruses into the environment.
- **Desktop integrity.** Users damage client systems or make them unusable by misconfiguring them or by installing unauthorized or incompatible software.

To use MetaFrame XP to solve many of these types of problems, review the following questions:

- Which types of applications should users run on MetaFrame servers?

For example, if users introduce viruses and other destructive elements into the network, publishing email applications, or perhaps all applications, for users to access on MetaFrame XP servers can add a layer of protection.

If you prefer to have users run applications such as email programs locally, you can use MetaFrame's content redirection capability in conjunction with the ICA Win32 Program Neighborhood Agent to redirect application launching from client device to MetaFrame server. When users double-click email attachments encountered in an application running locally, the attachment opens in an application that is published on the MetaFrame server, associated with the corresponding file type, and assigned to the user.

- Which types of applications should users run locally on client devices?

For example, users may frequently access file types such as Web and multimedia URLs when running published applications. Opening these file types with Web browsers or streaming media players present on MetaFrame servers can consume a lot of network bandwidth or result in heavy server load.

To free servers from processing these types of requests, you can redirect application launching for supported URLs from the MetaFrame server to the local client device.

- Which users should access applications locally and which should access applications published on MetaFrame XP servers?

To provide a smoother user experience, review your user base, client hardware, and client operating systems to determine which users should open which types of applications.

For example, you may publish a financial spreadsheet on a MetaFrame server for users in your accounting department to access. For security reasons, you want these users to open the published file with the associated application published on the MetaFrame server. However, you also published an audio file of a keynote speech given by the company president. To prevent the MetaFrame servers from becoming overloaded, you want users to open this file with player applications on their local client devices.

Managing Users' Access to Information with Content Publishing and Content Redirection

With MetaFrame's capability to redirect application and content launching from server to client or client to server, referred to as *content redirection*, access to information is expanded even more. You decide whether users access information with remote applications published on MetaFrame servers or with applications running locally on client devices.

Content redirection provides flexibility when considering application management and information storage locations and allows you to more effectively manage all of the resources available in the enterprise. You can also use this capability if your users connect to resources published on MetaFrame servers through NFuse.

You can use the following methods, or combination of methods, to broaden information access.

- Use *content publishing* to provide access to document files, media files, Web pages, and any other type of file, regardless of storage location. Shortcuts to the published content are presented to users the same way shortcuts to published applications are presented.

You can decide whether users open published files with local applications or with remote applications published on MetaFrame XP servers.

For more information about publishing content, see “Publishing Content” on page 258.

- Use *content redirection* to redirect application launching from server to client or client to server. If a user receives an email attachment in a locally running email program, you can use content redirection to allow the attachment to be opened in a remote application published on a MetaFrame server. You can also allow users to open any Web and multimedia content they encounter while running a published application with local players, freeing server resources.

You can determine which applications — remote or local — users launch in which situations.

For more information about content redirection, see “Configuring Content Redirection” on page 256.

Publishing Applications and Content

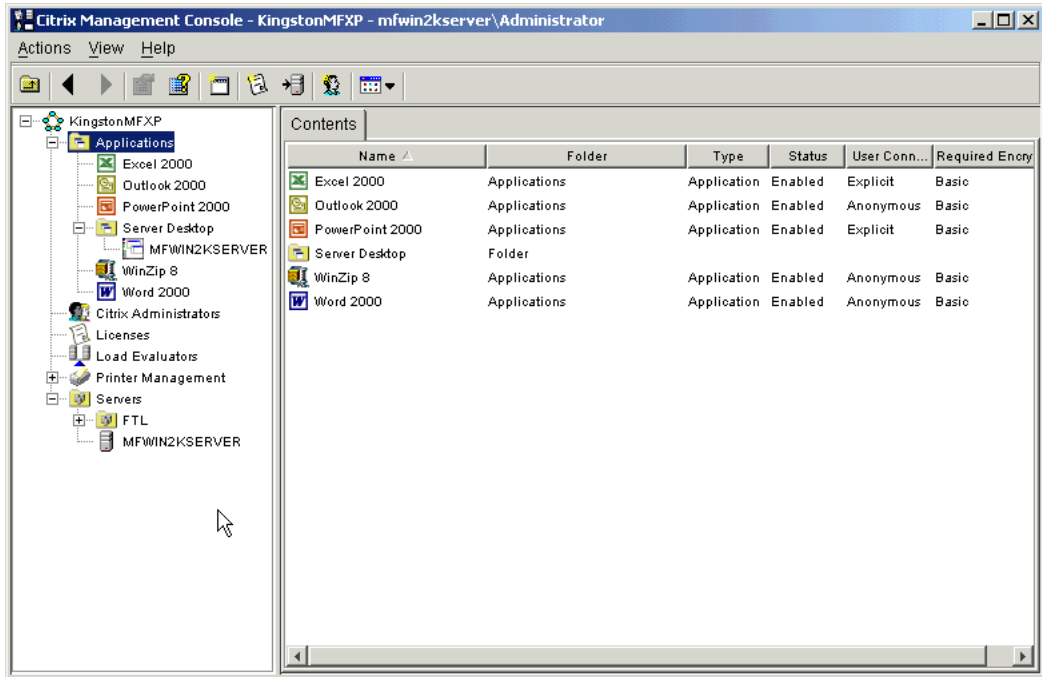
When you *publish applications*, you make applications that are installed on a MetaFrame XP server easily available to users. Similarly, you *publish content* to make documents, media files, URLs and other files available to users.

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 and the Program Neighborhood Agent

Use the Citrix Management Console to publish applications. 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.

Citrix Management Console shows the server farm's published applications under the Applications node (below)



User Access to Published Applications

When you publish applications, user access to those applications is simplified in several areas.

Addressing. Instead of connecting to a MetaFrame XP server by its IP address or server name, 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 host which applications.

Navigation. Instead of requiring users to navigate the Windows interface on MetaFrame XP servers to find and start installed applications, users can connect directly to published applications.

User authentication. Instead of logging on to and logging off from multiple MetaFrame XP servers to access applications, Program Neighborhood users can be authenticated once 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 249.

Published applications are presented to users running the ICA Win32 Program Neighborhood Client as *application sets*. An application set is a user's view of the resources published on MetaFrame XP servers that the user is authorized to run.

Note Users running the ICA Win32 Program Neighborhood Client open the Program Neighborhood interface to connect to applications and content published on MetaFrame XP server farms. The Program Neighborhood Client runs on Windows NT 4.0 Workstation, Windows 95, Windows 98, Windows Me, Windows 2000, and Windows XP platforms.

Publishing applications in your server farm benefits users of most ICA Clients. Although the UNIX, Macintosh, DOS, and Web Clients 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.

With the ICA UNIX, Macintosh, and DOS Clients, users benefit from application publishing's simplified addressing and desktop navigation when they configure connections to published applications using their connection configuration managers.

With 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 click a link in a Web page to start a published application. You can use NFuse Classic, Enterprise Services for NFuse, or the application launching and embedding process to achieve this.

Setting up a Pass-Through ICA Client

When you install MetaFrame, the ICA Win32 Program Neighborhood Client is installed on the MetaFrame server. To give a broader range of your users the benefits of Program Neighborhood, you can publish the ICA Win32 Client application on your MetaFrame XP 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.

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%\Program Files\Citrix\Ica PassThrough.

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 part of MetaFrame when you license the family levels MetaFrame XPa and MetaFrame XPe. Load Manager provides features for managing server loads in MetaFrame XP server farms. For information about Load Manager, refer to *Getting Started with Citrix Load Manager*, available in PDF format in the Docs directory of the MetaFrame XP CD-ROM and in the Documentation directory on a MetaFrame XP server.

Using Published Applications

When you publish an application, configuration information for the application is stored in the data store for the server farm. The configuration information includes which types of files are associated with the application; 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 users, published applications appear very similar to applications running locally on the client device. The way users start applications depends upon which ICA Client they are running on the client device.

ICA Win32 Program Neighborhood Client. After starting Program Neighborhood, users find a list of applications, called an application set, published for their user account or user group.

ICA Client users on UNIX, Macintosh, and DOS. Using connection managers, these 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 Web Client or the ICA Java Client can access applications using their Web browsers. You can use NFuse or the application launching and embedding process to present hyperlinks to published applications. When users click these links, the published application or content is launched on the MetaFrame server. For more information about application launching and embedding, see “Deploying ICA Clients to Users” on page 215.

The ICA Win32 Program Neighborhood Agent integrates hyperlinks to published applications into the Windows desktop. You must use NFuse to allow users to connect using the Program Neighborhood Agent. For more information about using the Program Neighborhood Agent, the ICA Win32 Web Client, or the Program Neighborhood Client, see the *ICA Win32 Client Administrator's Guide*, located in the IcaClientDoc directory on the Components CD-ROM included in your MetaFrame XP box.

For information about configuring Web access with NFuse, see the *NFuse Administrator's Guide*, located in the Docs directory on your MetaFrame XP CD-ROM.

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 about user account configuration, including use of Windows NT domains, Windows Active Directory, and Novell Directory Services (NDS), see “Network Configuration and Account Authority Issues” on page 60.

Publishing applications in MetaFrame 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 on to a MetaFrame 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, Setup 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 Citrix Management 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 about configuration of ICA connections on MetaFrame XP servers, see “Configuring ICA Connections” on page 191.

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 user accounts, which you create, configure, and maintain with standard user account management tools.

Explicit users who log on 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 user profile.

Important Do not assign any explicit users to the Anonymous group.

Procedures for Publishing Applications

Making applications and content available to users is an integral function of MetaFrame XP. Use the Citrix Management Console to publish applications on any server in the farm to which you log on. You do not have to run the Citrix Management Console from the MetaFrame XP server on which the applications are installed. The server or servers hosting a published application must be a member of the server farm.

► **To publish an application**

1. Open Citrix Management Console.
2. Verify that the server you want to host the application is a member of the server farm. You can find the intended host server or servers under the Servers object.
3. From the **Actions** menu, choose **New > Published Application**.
4. Follow the instructions in the Application Publishing wizard. Detailed help for 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.

Associating Published Applications with File Types

When you publish applications on MetaFrame XP servers, you can associate the published applications with certain file types present in the server's Windows registry.

Associate published applications with file types to:

- Implement Content Redirection from client to server for users running the ICA Win32 Program Neighborhood Agent
- Have users open content published on MetaFrame XP servers with applications published on MetaFrame XP servers

Important If you install and then publish applications after installing MetaFrame XP, Feature Release 2, you must update the file type associations in the server's Windows registry. For instructions for doing this, see "Updating File Type Associations in the Server Farm" on page 253.

When you associate published applications with file types and then assign the applications to users, you automatically implement the following:

1. Users running the ICA Win32 Program Neighborhood Agent open all files of the associated type encountered in locally running applications with applications published on the MetaFrame XP server.

For example, when users double-click email attachments encountered in an application running locally, the attachment opens in an application that is published on the MetaFrame server, associated with the corresponding file type, and assigned to the user. This feature is named *Content Redirection from client to server*.

If you do not want this to occur for *any* Program Neighborhood Agent users, do not associate the published application with any file types. If you do not want this to occur for *specific* Program Neighborhood Agent users, do not assign those users to the published application associated with the file type.

For more information about Content Redirection, see "Configuring Content Redirection" on page 256.

2. Users connecting through NFuse Classic or using the Program Neighborhood Agent open published content of the associated file type with the application published on the MetaFrame server.

For example, you publish a document of the Microsoft Word for Windows type. This feature is named *Content Publishing*. When you also publish the Microsoft Word application, associate it with a list of file types (files with the .doc extension, for example), and assign it to a group of users, the published content is opened in the Microsoft Word application published on the MetaFrame server. This occurs for users when they log on to the NFuse Classic default Web page and click the link to the published content (the document, in this case).

If you do not want this to occur for any users, do not associate the published application with any file types. If you do not associate the published application with any file types, users open the published content with local player or viewer applications if they are installed on the client devices.

For more information about Content Publishing, see “Publishing Content” on page 258.

You associate published applications with file types on the last page of the Publishing wizard or on a published application's property page.

Depending on how or if you want to redirect application launching, you may need to publish the same application more than once. Follow the procedures below to associate published applications with file types:

► **To associate a published application with file types when running the Publishing wizard**

1. Open Citrix Management Console.
2. If you have not yet published the application, select **New > Published Application** from the **Actions** menu.
3. Follow the instructions on the pages of the Publishing wizard. For detailed online help, click **Help** on each page.
4. On the last page of the wizard, select the file types you want to associate with the published application.

Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Click **Finish** when you are done.

- ▶ **To associate a published application with file types for an application you already published**
 1. Open Citrix Management Console.
 2. Expand the Applications node in the left pane to display your published applications.
 3. Right-click the application you want to associate with file types and choose **Properties** from the short-cut menu that appears.
 4. On the **Content Redirection** tab, select the file types you want to associate with the published application.

Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Click **OK** when you are done.

Updating File Type Associations in the Server Farm

If you install and then publish applications after installing MetaFrame XP, Feature Release 2, you must update the file type associations in each server's Windows registry.

You can verify which file types are associated with a published application on an application's property sheet. You can view all file types associated with published applications for the entire server farm on the **Content Redirection** tab, displayed when you select the server farm in the left pane of the console.

Follow the procedure below to update file type associations in your server farm. If you publish applications to be hosted on more than one server, be sure to update the file types for each server.

- ▶ **To update file type associations in the server farm**
 1. Open Citrix Management Console.
 2. Expand the Servers node in the left pane.
 3. Right-click a server and select **Update File Types from Registry**.

Passing Parameters to Published Applications

When you associate a published application with file types, MetaFrame XP appends the symbols “%*” (percent and star symbols enclosed in double quotation marks) to the end of the application’s command line. These symbols act as a placeholder for client-passed parameters.

If a published application doesn’t launch when expected, verify that its command line contains the symbols cited above. If you do not see these symbols in an application’s command line, you can add them manually.

If the path to the application’s executable includes directory names with spaces (such as Program Files), you must enclose the command line for the application in double quotation marks. To do this, follow the instructions below for adding quotation marks around the %* symbols and then add a double quotation mark at the beginning and the end of the command line. Be sure to include a space between the closing quotation mark and leave the double quotation marks around the percent and star symbols.

For example, change the command line for the published application Windows Media Player to the following:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

The following procedures assume you want to add the symbols to the Notepad application, which is published on a MetaFrame XP server.

► To add a parameter placeholder to a published application

1. In Citrix Management Console, expand the Applications node. Select the application to use and choose **Properties**.
2. In the **Properties** dialog box, select the **Application Location** tab.
3. In the **Command Line** box, add a space and “%*” (percent and star symbols enclosed in quotation marks) to the end of the command line. For example, for the following command line:

```
C:\Winnt\System32\Notepad.exe
```

Add “%*” to the end, as follows:

```
C:\Winnt\System32\Notepad.exe "%*"
```

4. Choose **OK** to save the changes.

Creating Files for Application Launching and Embedding

When you run the Application Publishing wizard, you can create the files you need to allow users to access published applications from a Web page. You must create two types of files — an HTML file and an ICA file — to enable users to do this. This process is called *Application Launching and Embedding*.

If you are using Citrix NFuse Classic or Enterprise Services for NFuse, you do not need to manually create these separate HTML files and ICA files.

The Create HTML File wizard and the Create ICA File wizard walk you through creating these files. You can create these files during the process of publishing an application or after you finish publishing an application.

Creating an ICA File

An ICA file contains published application information in Ini file format. You can create ICA files and distribute them to users. When users double-click ICA file icons, the published application is launched.

When a user receives an ICA file, the user's client device initializes a session to run the specified application on the MetaFrame XP server.

► 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. When 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 presents users with links to published applications. When users click the link in the HTML file you create, 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.

► **To remove a published application**

1. Select the application you want to remove under **Applications** in the left pane of the Citrix Management Console.
2. From the **Actions** menu, choose **Delete Published Application**.
3. When prompted, confirm the deletion by clicking **OK**.

Configuring Content Redirection

With Content Redirection, you determine which applications — remote or local — users launch and in which situations. Use Content Redirection to redirect application launching from:

- Client to server
- Server to client

Redirecting Content from Client to Server

When you configure **Content Redirection from client to server**, users running the ICA Win32 Program Neighborhood Agent open all files of the associated type encountered in locally running applications with applications published on the MetaFrame XP server. You must use NFuse Classic to allow users to connect to published applications with the Program Neighborhood Agent.

The Program Neighborhood Agent gets updated properties for published applications from the NFuse Classic server. When you publish an application and associate it with file types, the application's file type association is changed to reference the published application in the client device's Windows registry.

If you have users who run applications such as email programs locally, you can use MetaFrame's content redirection capability in conjunction with the ICA Win32 Program Neighborhood Agent to redirect application launching from client device to MetaFrame server. When users double-click attachments encountered in an email application running locally, the attachment opens in an application that is published on the MetaFrame server, associated with the corresponding file type, and assigned to the user.

Important You must enable client drive mapping to use this feature. You can enable client drive mapping for the entire server farm, for specific servers, or for specific users with user policies. For more information about user policies, see "Creating and Applying User Policies" on page 281.

If you do not want this to occur for *any* Program Neighborhood Agent users, do not associate the published application with any file types. If you do not want this to occur for *specific* Program Neighborhood Agent users, do not assign those users to the published application associated with the file type.

Follow the procedure below to configure Content Redirection from client to server.

► **To configure Content Redirection from client to server**

1. Determine which of your users connect to published applications using the Program Neighborhood Agent. Content Redirection from client to server applies only to those users connecting with the Program Neighborhood Agent.
2. Verify that client drive mapping is enabled. You can enable client drive mapping for a specific connection using Citrix Connection Configuration or for specific users by creating user policies.
3. Publish applications you want the Program Neighborhood Agent users to open on the MetaFrame server.
4. When you publish the application, associate it with file types on the last page of the Application Publishing wizard.

Redirecting Content from Server to Client

When you enable **Content Redirection from server to client**, embedded URLs are intercepted on the MetaFrame server and sent to the ICA Client using the ICA Control virtual channel. The user's locally installed browser is used to play the URL. Users cannot disable this feature.

For example, users may frequently access Web and multimedia URLs they encounter when running an email program published on a MetaFrame server. If you do not enable Content Redirection from server to client, users open these URLs with Web browsers or multimedia players present on MetaFrame servers.

To free servers from processing these types of requests, you can redirect application launching for supported URLs from the MetaFrame server to the local client device.

The following URL types are opened locally on ICA Win32 and Linux Clients when this type of content redirection is enabled:

HTTP (Hypertext Transfer Protocol)

HTTPS (Secure Hypertext Transfer Protocol)

RTSP (Real Player and QuickTime)

RTSPU (Real Player and QuickTime)

PNM (Legacy Real Player)

MMS (Microsoft's Media Format)

Note Content Redirection from server to client requires Internet Explorer Version 5.5 with Service Pack 2 on Windows 98 systems.

Follow the procedures below to enable Content Redirection from server to client.

► **To enable Content Redirection from server to client**

1. Determine if you want Content Redirection from server to client to apply for the entire server farm, for specific MetaFrame servers, or for specific users only.

To apply the behavior to the entire server farm, select the farm in Citrix Management Console and then click **Properties**. On the **MetaFrame Settings** tab, select the option **Enable Content Redirection from server to client**.

To apply the behavior to a specific server, select the server in the **Servers** node in Citrix Management Console and then click **Properties**. On the **MetaFrame Settings** tab, select the option **Enable Content Redirection from server to client**.

To apply the behavior to specific users, create a user policy and enable the rule **Server Content Redirection**. Select the option **Use Server Content Redirection**. Assign the policy to only those users you want to open supported URL file types on client devices. For more information about user policies, see "Creating and Applying User Policies" on page 281.

Publishing Content

You can give users access to information, such as documents, Web sites, and video presentations, by publishing content for users in the same way that you publish applications in a MetaFrame XP server farm.

With content publishing, you can publish and manage various types of content and present it to users with the applications they need. Published content and published applications appear together through NFuse, Program Neighborhood, and Program Neighborhood Agent interfaces.

You can configure MetaFrame to allow users to open published content in local player or viewer applications running on client devices or in applications published on MetaFrame servers.

Publishing Content to be Opened with Applications Published on MetaFrame Servers

Follow these basic steps if you want users to open published content with applications published on MetaFrame XP servers.

1. Publish the data file you want users to access. For more detailed instructions for publishing content, see “Publishing Content on MetaFrame XP Servers” on page 261.
2. Determine which users you want to open the published content with a published application.
3. Publish the application that corresponds to the content file type. For example, if you published a Microsoft Word for Windows document file named “Quarterly_Sales.doc,” publish Microsoft Word on a MetaFrame XP server. For more information about publishing applications, see the online Help for the Application Publishing wizard.
4. When you publish Word, associate the file type “Word document” with the application.

Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Assign the published Word to the users you want to open the published document with the published application.

Publishing Content to be Opened with Applications on Local Client Devices

When you configure MetaFrame XP to allow users to open published content with applications running locally on client devices, the ICA Client passes the name of the published content file to the local viewer application. The MetaFrame XP server does not download the file to the ICA Client. Instead, the local viewer application accesses the file the same as it would if a user double-clicked the file in Windows Explorer (and a file type association specified the application to use).

For example, when a user opens a published Microsoft Streaming Media file in Program Neighborhood, the Windows Media Player application runs on the client device to play the content. You can publish any content for users to view with a local viewer application.

Publishing content does not use ICA Client or MetaFrame XP server resources or licenses, because local viewer applications do not use ICA sessions to display the published content.

Follow these basic steps for publishing content for users to access with applications running locally on client devices.

1. Publish the data file you want users to access. For more detailed instructions for publishing content, see “Publishing Content on MetaFrame XP Servers” on page 261.
2. If you happen to publish the application that corresponds to the content file type, do not associate it with any file types if you want all users to open the published content with locally installed applications.

However, if you want some users to open the published content with the published application, you can associate the published application with the content file type, but only assign the application to those users. For more information about publishing applications, see the online Help for the Application Publishing wizard.

Content Publishing Requirements and Limitations

The following requirements and limitations apply when publishing content in MetaFrame XP server farms:

- You can publish content using Citrix Management Console when a server farm is in mixed mode for interoperability with MetaFrame 1.8. However, users do not see published content in Program Neighborhood, Program Neighborhood Agent, or NFuse if the server farm is in mixed mode.
- Published content appears in Program Neighborhood, Program Neighborhood Agent, and NFuse Classic application sets, so access to published content requires that the ICA Client support those features. You cannot create custom ICA connections to access published content.
- You cannot publish a UNC directory path to display a folder to users of Netscape Navigator versions prior to 6.0. See “Specifying Locations for Publishing Content” on page 261 for more information.
- When you publish a file using a network path, users must have permission to access the file on the network to be able to access it as published content through MetaFrame XP.

Publishing Content on MetaFrame XP Servers

You publish content using Citrix Management Console and the Publishing wizard. You can select options in the wizard when you publish content, and you can later check and modify the settings in the **Properties** dialog box for the published content.

If you want users to open published content with local applications, the applications must be associated with published content through Web browser MIME types or Windows file associations on the client device. No other client-side configuration is necessary once viewer applications are installed and associations are configured.

► To publish content

1. In Citrix Management Console, choose **Actions > New > Published Application** to open the Publishing wizard. Enter the information requested in the wizard and select the options you want to use. To move between pages, click **Next** to continue or **Back** to return to a previous page.
2. Type a name for the content you are publishing in the **Display Name** box. This text appears as the name of the icon that represents the published content.
3. When the wizard asks what you want to publish, select **Content**.
4. In the **Content Address** box, specify the location of the content by entering a URL or UNC address. See “Specifying Locations for Publishing Content” below for more information.
5. After specifying the content address, continue using the wizard to specify other settings and publish the content.

Specifying Locations for Publishing Content

When you publish content, you can specify the location using a variety of address formats. You can enter any of the following types of information (examples shown in parentheses):

HTML Web site address (<http://www.citrix.com>)

Document file on a Web server (<https://www.citrix.com/press/pressrelease.doc>)

Directory on an FTP server (<ftp://ftp.citrix.com/metaXP>)

Document file on an FTP server (<ftp://ftp.citrix.com/metaXP/Readme.txt>)

UNC file path (<file://myServer/myShare/myFile.asf>) or
(\\myServer\\myShare\\myFile.asf)

UNC directory path (<file://myServer/myShare>) or (\\myServer\\myShare)

Important Specifying a UNC directory path does not correctly display the specified directory to users of Netscape Navigator prior to Version 6.0. Earlier versions of Navigator incorrectly interpret the path as relative to the Web server. To publish a directory to such users, consider specifying an FTP directory or listable Web server directory.

Setting CPU Priority Levels for Applications

By default, MetaFrame XP gives all published applications equal priority for access to CPU cycles. All application instances run with normal CPU priority.

The default configuration assumes that CPU access by all applications is equally important. The default configuration does not prevent one application from consuming resources that are required by other, mission-critical applications running on the same server.

You can manage some aspects of resource usage by applications through your deployment methods. For example, you can isolate mission-critical applications by publishing them on separate servers so less-important applications do not compete for server resources. You achieve better performance by publishing CPU- and memory-bound applications on high-performance servers.

MetaFrame XP provides a setting you can apply to published applications to prioritize their CPU access. You can use the CPU priority settings on servers running Windows 2000 Server family products.

Note The term *published application* in this section refers to applications and MetaFrame XP server desktops that are published for users in the server farm. It does not refer to published content such as documents and media files.

You can apply a CPU priority setting to each published application. Each instance of the application that runs in the server farm is affected by the setting. When multiple servers host the same published application, the setting applies to each server on which the application runs in the server farm.

If you publish the same application more than once—for separate groups of users, different host servers, or with different settings, for example—you create separate published applications; each can have its own CPU priority setting.

You can use this setting in any size server farm, independent of load management features in MetaFrame XPa and MetaFrame XPe. Load management distributes connections to MetaFrame servers based on the servers' loads. In contrast, the CPU priority setting applies to a published application that runs on any server in the server farm.

Assigning CPU Priority Levels to Applications

When you assign a CPU priority level to a published application, the priority level that you specify is used by the CPU scheduler on all servers that host the published application (and for every instance of the application that runs on a server). When a server is executing multiple applications, the CPU scheduler prioritizes CPU access by application threads according to the priority level that you assign or the default priority level.

With this option, you can assign normal or lower CPU priority to Microsoft Internet Explorer, for example, and assign high CPU priority to an application whose performance is more important to the enterprise, such as PeopleSoft Human Resources Management. A higher priority setting gives Human Resources Management a performance advantage over Internet Explorer when both applications run on the same server.

You can assign five priority levels (in order from lowest to highest priority): low, below normal, normal, above normal, and high. The default is normal.

Important High priority indicates a process that performs time-critical tasks. The threads of a high-priority process preempt the threads of low- and normal-priority processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the system. Use extreme care when using the high-priority setting. A CPU-bound application assigned high priority can consume nearly all available CPU cycles, which can cause unacceptable performance by other applications running on the server.

The CPU priority option is in the Application Publishing wizard and on the **Application Limits** tab in the **Properties** dialog box for each published application. You can set the priority level when you first publish applications and set or change the level for published applications using Citrix Management Console.

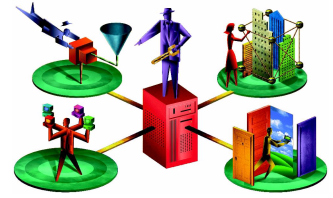
► To publish an application and set its CPU priority

1. In Citrix Management Console, choose **Actions > New > Published Application** to run the Application Publishing wizard.
2. Proceed through the wizard pages, entering information and selecting options for the application you are publishing.
3. Select an option from the **CPU priority level** menu. The default setting is Normal.
4. Click **Next** and then proceed through the subsequent screens until you complete the wizard's steps.

► **To modify the CPU priority of a published application**

1. In Citrix Management Console's left pane, expand the Applications node. Select the application you want to modify and choose **Properties**.
2. In the **Properties** dialog box, select the **Application Limits** tab.
3. Select an option from the **CPU priority level** menu. The default setting is Normal.
4. Click **OK** to apply the setting and close the dialog box.

Managing Users and ICA Sessions



This chapter describes how to manage users and their ICA sessions in a MetaFrame XP server farm. It includes information about using Citrix Management Console and Citrix Web Console to monitor users' connections and the status of ICA sessions and about creating and applying user policies to control select MetaFrame settings for users or user groups.

You can perform session-management activities, including logging off, shadowing, disconnecting, and sending messages to users, using either Citrix Management Console or Citrix Web Console. Some management and monitoring activities can be performed only in Citrix Management Console. For more information about Citrix Management Console, see "Citrix Management Console" on page 161. For more information about Citrix Web Console, see "Using Setup" on page 128.

Note You may not see some or all of the data described below if you have not been granted permission to perform these tasks. See your primary Citrix administrator for more information.

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 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**.

Controlling User Connections

When logons are enabled, MetaFrame XP servers have no default limit on access to ICA sessions and published applications by users. In general, users can launch multiple connections and can connect to any published application that they are authorized to use.

You can use the *connection control* feature to control connections to MetaFrame XP servers and published applications. This feature can help you maintain availability of resources in a server farm.

Having no limit on connections works best in an environment where users and published applications are well-behaved. All users have equal access to the published applications.

Adverse usage conditions in a server farm can degrade performance and reliability. In an unregulated environment, you might encounter the following problems:

- Errors caused by individual users who run more than one instance of a published application at the same time.
- Denial-of-service attacks by malicious users who run multiple application instances that consume server resources and connection license counts.
- Over-consumption of resources by non-critical activities such as Web browsing.

Connection control provides two types of limits, as shown in the following table.

Limit type	Description
Concurrent connections in the server farm	Restricts the number of concurrent connections (ICA sessions) that each user in the server farm can establish. See "Limiting Total Connections in a Server Farm" on page 267.
Published application instances	Restricts the total number of instances of a published application that can run in the server farm at one time, and prevents users from launching more than one instance of a published application. See "Limiting Application Instances" on page 267.

Limiting Total Connections in a Server Farm

When a user launches a published application, the ICA Client establishes a connection to a MetaFrame XP server and initiates an ICA session. If the user launches a second published application (without logging off from the first one), this creates a second concurrent connection in most cases.

Note The seamless session option in the ICA Client enables *session sharing*, a mode in which more than one published application runs with a single connection. If a user runs multiple applications with session sharing, the session counts as one connection.

To conserve resources, you can limit the number of concurrent connections that users are permitted to establish. The limit applies to each user who connects to the server farm. A user's active sessions and disconnected sessions are counted for the user's total number of concurrent connections.

For example, you can set a limit of three concurrent connections for users. If a user has three concurrent connections and tries to establish a fourth, the limit you set prevents the additional connection. A message tells the user that a new connection is not allowed.

Limiting connections can help you maintain availability of ICA connection license counts as well as prevent over-consumption of server resources by a few users.

You can apply the concurrent connections limit to all users, including members of the local administrators group. The option **Enforce limit on administrators** on the **Connection Limits** tab in the **Properties** dialog box for the farm refers to local administrators. By default, local administrators are exempt from the limit so they can establish as many connections as necessary.

Limiting Application Instances

By default, users in a server farm have unlimited access to the published applications that they are authorized to use. MetaFrame XP servers do not limit the number of instances of a published application that can run at one time in a server farm. Also, by default, a user can launch more than one instance of a published application at the same time.

With connection control, you can specify the maximum number of instances of a published application that can run at one time in the server farm.

For example, you can publish Autodesk AutoCAD and set a limit of 30 concurrent instances in the server farm. When 30 users are running AutoCAD at the same time, no more users can launch the application because of the limit of 30 concurrent instances.

Use the concurrent instances limit to enforce an application's licensing requirement, for example.

Another connection control option lets you prevent any user from running multiple instances of a particular published application. With some applications, running more than one instance in a single user context can cause errors on the server.

You can apply application limits independently to each published application. For example, you can apply the limitations on total concurrent instances and multiple instances by a single user to one published application. You can limit only the total concurrent instances of another application. You can configure a third application to limit launching of multiple instances by individual users.

Configuring Connection Control Settings

You can use connection control to manage published applications and published desktops only. Connection control options do not apply to published content such as documents and media files, which execute on the client device. For more information about publishing, see "Making Information Available to Users" on page 241.

Connection control is implemented entirely on MetaFrame XP servers. The ICA Client contains no configuration options related to connection control. Connection control affects ICA Client users only if a connection attempt is prevented. If a user's connection exceeds a connection limit, the client displays a message that describes why the connection is not available.

You configure connection control settings, including the option to log events related to connection control, in Citrix Management Console.

The option to limit each user's total concurrent connections in the server farm is on the **MetaFrame Settings** tab in the **Properties** dialog box for the server farm.

Options for limiting application instances are on the **Connection Limits** tab of the **Properties** dialog box for each published application. These options also are available in the wizard that you use to publish applications.

► To limit concurrent connections in a server farm

Use this procedure to set the number of concurrent connections that each user can establish in the server farm.

1. In Citrix Management Console, right-click the farm node and choose **Properties**.
2. In the **Properties** dialog box, select the **Connection Limits** tab.
3. Select **Maximum connections per user** to limit each user's concurrent connections. Enter the number of concurrent connections to allow for each user.

4. If you want the connection limitation to apply to everyone, including local administrators, select **Enforce limit on administrators**.
5. Click **OK** to apply the settings and close the dialog box.

► **To publish an application or desktop with application limits**

1. In Citrix Management Console, choose **Actions > New > Published Application** to run the Application Publishing wizard.
2. Proceed through the wizard pages, entering information and selecting options for the application you are publishing.
3. Under **Concurrent Instances**, select one or both of the following options:
 - **Limit instances allowed to run in server farm.** Select this option and enter the maximum number of instances that can run at one time in the server farm (without regard to who launches the application).
 - **Allow only one instance of application for each user.** Select this option to prevent any user from running more than one instance of this application at the same time.
4. After you enter all required information and select the options to use, click **Finish** to publish the application.

► **To set application limits on a published application or desktop**

1. In Citrix Management Console, right-click the published application or desktop and choose **Properties**.
2. In the **Properties** dialog box, select the **Application Limits** tab.
3. Configure the following options:
 - **Limit instances allowed to run in server farm.** Select this option and enter the maximum number of instances of this application that can run in the server farm at one time.
 - **Allow only one instance of application for each user.** Select this option to prevent each user from running more than one instance of this application at the same time.
4. Click **OK** to apply the settings and close the dialog box.

Logging Connection Control Events

A setting that controls logging of connection control events is on the **MetaFrame Settings** tab in the **Properties** dialog box for the server farm. Use the option to enable or disable event logging for the entire farm. By default, event logging is disabled.

Event logging records an entry in the System log each time a server denies a user connection because of a connection control limit. Each server records the data in its own System log.

The following limits can result in connection denials, which the system records if logging is enabled.

Maximum connections per user. You can limit users to a maximum of five connections, for example. If a user tries to launch a sixth connection, the server denies the connection request and records the user's name and the time in the System log.

Application instances. You can limit a published application to 10 concurrent instances, for example. If a user tries to launch the application when 10 instances are running, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

This limit option is labeled "Limit instances allowed to run in server farm" on the Properties sheet for each published application.

Application instances per user. You can configure a published application to allow each user to run only one instance of the application. If a user tries to launch a second instance of the application, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

This limit option is labeled "Allow only one instance of application for each user" on the Properties sheet for each published application.

► **To enable logging of connection control events**

1. Right-click the farm node in Citrix Management Console and choose **Properties**.
2. In the **Properties** dialog box, select the **MetaFrame Settings** tab.
3. Select **Enable logging of over-the-limit denials**.
4. Click **OK** to apply the setting and close the dialog box.

Monitoring and Managing ICA Sessions

You can use Citrix Management Console and Citrix Web Console for monitoring and management of your user's ICA sessions. You can use the consoles 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

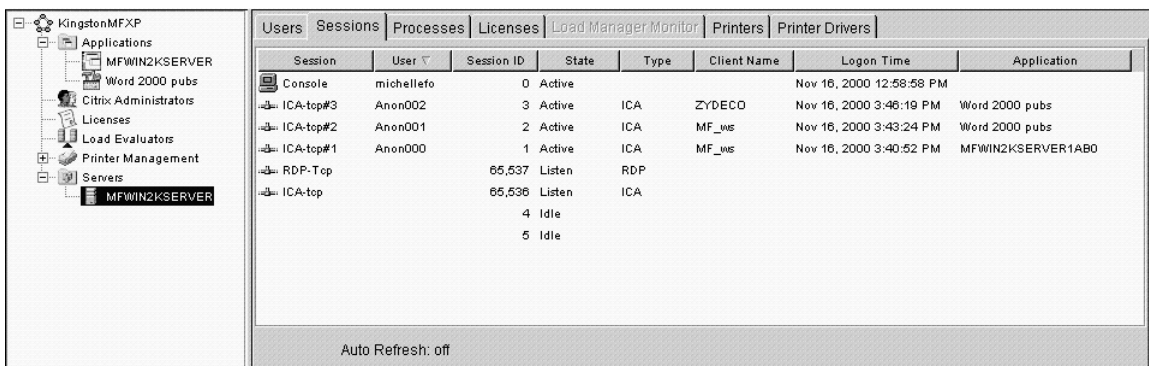
This section describes how to use Citrix Management Console for session monitoring and management. If you need help performing these actions in Citrix Web Console, click the Help button that is displayed in the Web console.

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



The screenshot shows the Citrix Management Console interface. On the left is a tree view with nodes: KingstonMFXP, Applications, MFWIN2KSERVER, Word 2000 pubs, Citrix Administrators, Licenses, Load Evaluators, Printer Management, Servers, and MFWIN2KSERVER. The right pane has tabs: Users, Sessions, Processes, Licenses, Load Manager Monitor, Printers, and Printer Drivers. The 'Users' tab is active, displaying a table of sessions.

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_ims	Nov 16, 2000 3:43:24 PM	Word 2000 pubs
ICA-top#1	Anon000	1	Active	ICA	MF_ims	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.

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.

Type. The type of connection being used to connect to the server, ICA or RDP, for example.

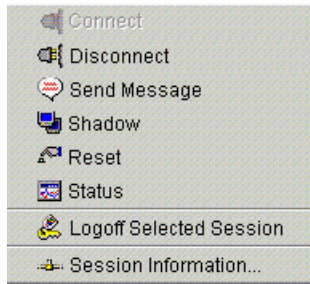
Client name. This column displays the name of the client device that is running the session.

Idle Time. The amount of time during which the user has not interacted with the application.

Using Session Management Commands

In Citrix Management Console and Citrix Web Console you can select ICA sessions and choose commands to manage the sessions.

In Citrix Management Console, use the **Actions** menu and the toolbar buttons to choose session management commands. You can right-click a session in the console and choose commands from the menu that appears.



In Citrix Web Console, session-management commands are available when you select a session by clicking the check box to the left of the User name.

Sessions

All Sessions

[Logoff](#)
[Disconnect](#)
[Send Message](#)
[Shadow](#)

	User	Application	Server	State	Session ID
<input checked="" type="checkbox"/>	davidhaw	Netscape Navigator	CROWLEY	Active	1

To display session information, click the Session link on the left of the Web console page.

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 are still running 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.

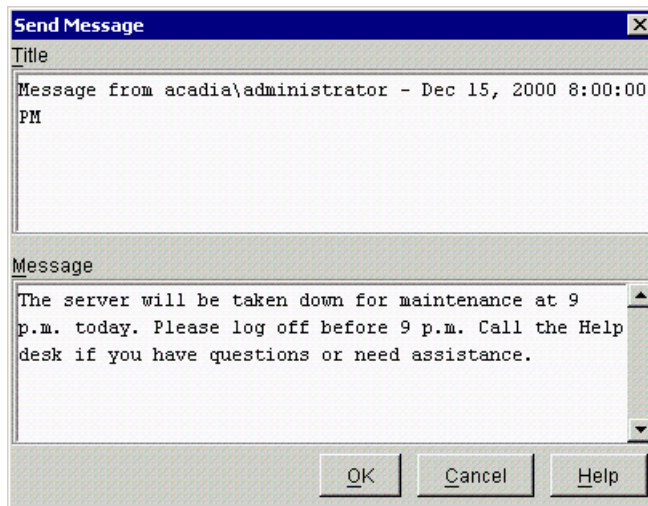
Sending Messages to Users

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 about viewing sessions, see "Viewing Information About ICA Sessions" on page 271.

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 on 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. (In Citrix Web Console, click **Send Message** to send the message.)



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 is 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 command 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 a process and choose the **Terminate** command to terminate the process.

Reconnecting ICA Sessions Automatically

If ICA sessions are disconnected because of unreliable networks, highly variable network latency, or range limitations of wireless devices, the result is lost productivity for users who must manually reconnect to their applications. Unreliable connections, such as WAN links, frequently cause time-out of TCP retransmission, which can cause loss of an ICA connection.

The *auto reconnect* feature can detect broken ICA connections and automatically reconnect to the disconnected sessions. When this feature is enabled, users do not have to reconnect manually or enter their logon credentials to continue their work.

The ICA Clients for Win32, WinCE, and Java (applet mode only) support auto reconnect for ICA sessions over TCP. This feature cannot automatically reconnect anonymous ICA sessions. Also, auto reconnect does not work with the ICA Client Object.

How Automatic Reconnection Works

When the ICA Client detects unintended disconnection of an ICA session, the client initiates a reconnection sequence. A message tells the user that the client will reconnect after a specified interval. Reconnection requires no action by users, although they can click a button to reconnect immediately or to cancel the process.

Depending on network conditions, it might be necessary to briefly wait before reconnecting to give the network time to recover from the problem that caused the disconnection.

The auto reconnect feature does not create additional sessions, which sometimes are created by manual reconnection. If a server does not detect a dropped connection and the client reconnects manually, a new ICA session that does not contain the user's current workspace is created. Additional sessions are avoided with auto reconnect because it disconnects a session before reconnecting to it.

Auto reconnect incorporates a re-authentication mechanism based on encrypted user credentials. When a user initially logs on to a server to use an application, MetaFrame XP encrypts and stores the user credentials in memory, and sends the encryption key to the ICA Client. For reconnection, the client submits the key to the server. The server decrypts the credentials and submits them to Windows logon for authentication.

For maximum protection of users' credentials and ICA sessions, use SSL encryption for all communication between ICA Clients and MetaFrame XP servers.

The ICA Client attempts auto reconnection a set number of times (three by default). When the server detects a broken connection, it disconnects the session and allows the client to automatically reconnect during a set time period (five minutes by default).

The client and server detect broken connections independently. If the server does not detect a broken connection (the server considers the session active), the server does not begin timing the autoreconnection allowed period.

If a client disconnects a session normally (not because of a broken connection), the server does not allow automatic reconnection. Automatic reconnection does not occur when users disconnect ICA sessions by exiting applications without logging off.

Configuring Reconnection Settings

You can do the following to configure automatic reconnection:

- Enable or disable the auto reconnect feature at the server farm level or on individual MetaFrame XP servers
- Enable or disable auto reconnect functionality at the ICA Client
- Change settings such as the delay between reconnection attempts by the ICA Client
- Enable or disable logging of reconnection events for the server farm or individual servers

Use Citrix Management Console to enable and disable automatic reconnection and reconnection event logging, as described next. Auto reconnect is enabled by default for all servers in the server farm. Reconnection event logging is disabled by default.

You can use the **AcrCfg** command to configure autoreconnect settings on MetaFrame XP servers. See page 310 for information about the command.

By default, auto reconnect is enabled on the ICA Win32 Client. You can disable auto reconnect functionality completely by setting `AutoReconnectEnabled=0` in the [WFClient] section of the client's `Appsrv.ini` file. For more information about client configuration, see the *ICA Win32 Client Administrator's Guide*.

Settings for ICA connections also affect the auto reconnect feature. See “Setting Up ICA Connections for Auto Reconnect” on page 278 for information.

► To enable auto reconnect at the server farm level

By default, the auto reconnect feature is enabled. Use the following procedure to change the current setting for the server farm.

1. In Citrix Management Console, select the server farm node and choose **Properties**.
2. In the **Properties** dialog box, select the **ICA Settings** tab.

3. Click **Enable Auto Client Reconnect** to enable or disable automatic reconnection at the server farm level.
4. Click **OK** to apply the setting and close the dialog box.

► **To enable or disable auto reconnect at the server level**

By default, each server inherits the server farm setting for auto reconnect. Use the following procedure to change this setting and configure auto reconnect on individual servers.

1. In Citrix Management Console, select a server and choose **Properties**.
2. In the **Properties** dialog box, select the **ICA Settings** tab.
3. Deselect **Use Farm Settings**. You can now select **Enable auto client reconnect** to enable the feature on the selected server. To disable auto reconnect, clear the check box.
4. Click **OK** to apply the settings and close the dialog box.

Setting Up ICA Connections for Auto Reconnect

By default, automatic reconnection is enabled in a server farm. However, if a server's ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. The auto reconnect feature works only if the server disconnects sessions when there is a broken or timed-out connection.

In this context, the *ICA TCP connection* refers to a MetaFrame XP server's virtual port (rather than an actual network connection) that is used for ICA sessions on TCP/IP networks.

By default, the ICA TCP connection on a MetaFrame XP server is set to disconnect sessions with broken or timed-out connections. Disconnected sessions remain intact in system memory and are available for reconnection by the ICA Client.

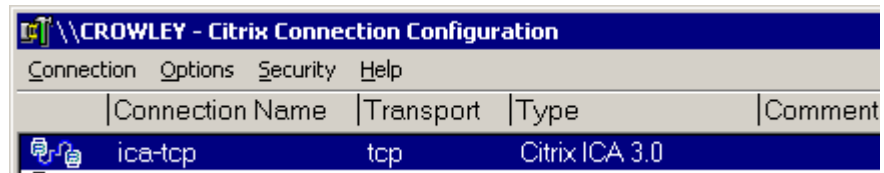
The ICA connection can be configured to *reset*, or log off, sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new ICA session; rather than restoring a user to the same place in the application in use, the application is restarted.

If MetaFrame XP servers are configured to reset sessions, the automatic reconnection sequence creates a new ICA session on the initial host. This process requires users to enter their credentials to log on to the server.

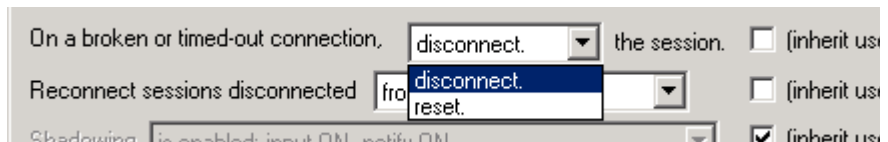
► **To configure the ICA TCP connection for auto reconnect**

1. Run Citrix Connection Configuration (choose **Start > Programs > Citrix > MetaFrame XP > Citrix Connection Configuration**).

2. In the Citrix Connection Configuration window, double-click the **ica-tcp** connection. The **Edit Connection** dialog box appears.



3. In the **Edit Connection** dialog box, click **Advanced**.
4. In the **Advanced Connection Settings** dialog box near the bottom, the first pop-up menu sets the behavior for a broken or timed-out connection.



- If **Inherit User Config** is selected, you cannot change the setting because the connection inherits the setting from each user's profile.
- When **Inherit User Config** is not selected, you can select one of the following options to configure the ICA TCP connection:
 - **Disconnect.** The server places broken connections in the disconnected state. The ICA Client can reconnect automatically without any action by users.
 - **Reset.** The server resets broken connections. Automatic reconnection creates a new ICA session and requires users to re-enter credentials.

Be sure to select **Disconnect** to set up the ICA TCP connection to work with the autoreconnect feature.

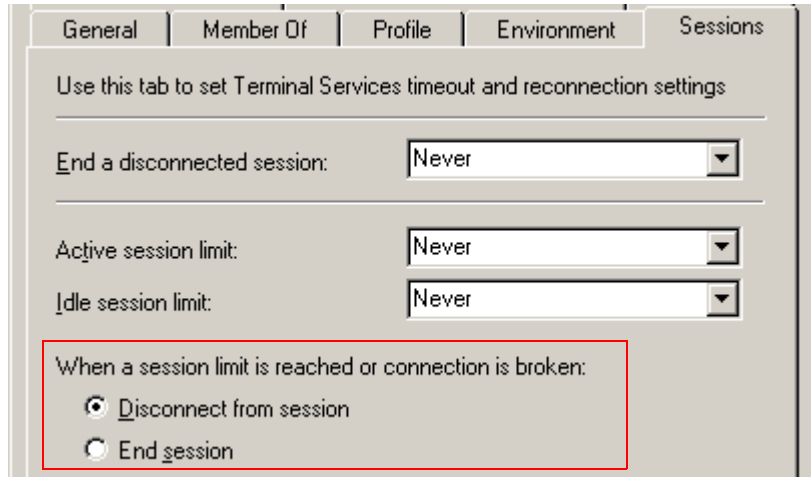
5. Click **OK** to close the dialog box and the previous dialog box. Then, choose **Connection > Exit** to close Citrix Connection Configuration.

► To configure an ICA connection for individual users

In the **Advanced Connection Settings** dialog box, if **Inherit User Config** is selected for the setting labeled **On a broken or timed-out connection**, the connection inherits the setting from each user's profile. To view or change the setting for broken or timed-out connections, do the following to display the properties for each user.

On Windows 2000 Server family, use **Computer Management** to configure user profiles.

1. Double-click a user to open the **Properties** dialog box.
2. On the **Sessions** tab, check the setting under **When a session limit is reached or a connection is broken**.
3. Select **Disconnect from session** to allow automatic reconnection.



Logging Reconnection Events

To enable or disable log entries for automatic reconnection events, use the **ICA Settings** tab in the **Properties** dialog boxes for the server farm or individual MetaFrame XP servers.

Logging is disabled by default. When logging is enabled, the server's System log captures information about successful and failed automatic reconnection events to help with diagnosis of network problems.

Automatic reconnection can fail if the ICA Client submits incorrect authentication information (which might occur during an attack) or the server determines that too much time has elapsed since it detected the broken connection.

Each server stores information about reconnection events in its own System log. The server farm does not provide a combined log of reconnection events for all servers.

Creating and Applying User Policies

You can create user-based policies to apply select MetaFrame settings to specific Windows domain users or user groups.

By creating and applying user-based policies you can:

- Allow users to shadow other users' ICA sessions
- Control access to drives, ports, and printers on client devices
- Set a required encryption level for ICA sessions
- Turn off the Auto Client Update feature for specific users

Because policies are applied to users or user groups when they log on to the MetaFrame XP farm, policies follow users no matter which client devices they use. A policy's rules remain in effect for the length of the user's ICA session. User policies override similar MetaFrame settings configured farm-wide, at the server level, or on the ICA Client.

With user policies, you can tailor MetaFrame to meet users' needs based on their job functions, geographic locations, or connection types (LAN, WAN, or dial-up). For example, for security reasons you may need to place restrictions on user groups who regularly work with highly sensitive data. You can create a policy that requires a high level of encryption for ICA sessions and prevents users from saving the sensitive files on their local client drives.

However, if some of the people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one should take precedence.

Policy rules have three states: enabled, disabled, or not configured. By default, all rules are not configured. All unconfigured rules are ignored when users log on to the MetaFrame server, so the rule only comes into play when the state is enabled or disabled.

The basic steps for effectively creating and using policies are as follows. These steps are explained in more detail below.

1. Decide the criteria on which to base your MetaFrame policies.

You may want to create policies for users and user groups based on job function, connection type, or geographic location, or you may want to use the same criteria that you use for your Windows 2000 Active Directory group policies.

2. Create the policy. Creating a policy involves the following steps:

- Naming the policy
- Assigning the policy to users
- Setting the policy's rules

3. Prioritize or rank your policies

When you create policies for entire user groups, you may find that some members of the group require exceptions to some policy rules. To more effectively manage your policies, you can create new policies for only those users who need exception to a policy's rules, and then rank the policy for those individual users higher than the policy for the entire group.

Note Policies are listed in alphabetical order in the right pane of Citrix Management Console. To view a policy's priority number and description, you must set the console's view mode to **Details**. Select **Details** on the **View** menu.

You can use the Search tool in Citrix Management Console to find which policies are applied to which users, and to determine the effective rule settings when more than one policy is applied to the same user.

To use the Search tool, open Citrix Management Console and click the **Search** button. See the console's online Help for more information about Search.

► **To create a new user policy**

1. In Citrix Management Console, right-click the Policies node in the left pane and choose **Create Policy** or click the **Create Policy** button on the console toolbar.
2. Enter the name of the policy in the **New Policy** dialog box and then click **OK**. Examples of policy names are "Accounting Department" or "Remote Users." The policy name is displayed in the right pane of the console.
3. You can add a description of the policy by right-clicking the policy and selecting **Edit Description**.
4. Apply the policy to users or user groups by right-clicking the policy name and choosing **Assign Users**. Double-click a domain name to display user groups. Select **Show users** to display individual user accounts.
5. Select the user group and/or users to whom you want to assign the policy and then click **Add**.

By default, the policy is allowed for any users or user groups you add to the configured accounts list. If there are members of the user group you do not want assigned to this policy, you can add the individual members of the group and then select **Deny** to prevent the policy from being applied to them.

Click **OK** when you are done adding users.

6. You set the policy's rules on the policy's property sheet. Double-click the policy to open its property sheet. Some policy rules are organized into folders. Expand the folders to view the rules you can apply.

7. When setting policy rules, determine which settings you want to apply. Click **Enabled** to apply the rule to the assigned users or user groups. For more information about policy rules, select the rule in question and then click **Help**.
8. Click **OK** when you are done.

Prioritizing Policies

After you create basic policies using your primary criteria, you may find that you need to create additional policies for individual users who require exceptions to some policy rules.

In the following procedure, the interwoven example assumes that you created a policy for your “Accounting” user group. One of the rules enabled in this policy prevents the user group from saving data to their local drives. However, two users who are members of the Accounting group travel to remote offices to perform audits and need to save data to their local drives.

The steps below describe creating a new policy for Accounting group members Carol and Martin that will allow them access to their local drives while allowing the other policy rules to work the same way for them as for all other members of the Accounting group.

► To create exceptions and prioritize policies

1. Determine which users need additional policies to create exceptions.

The policy named “Accounting Profile” that is assigned to the Accounting group includes a rule that prevents access to local drives. Carol and Martin, members of the Accounting group, need access to their local drives.
2. Determine which rule or rules you do not want to apply to these users.

You want most of the rules in this policy to apply at all times to all users, with the exception of the rule that prevents access to local drives.
3. Create a new policy. See “To create a new user policy” on page 282 for more information. You may want to name this policy “Accounting Profile - local drive access.”
4. Edit the description of the policy by right-clicking the policy and selecting **Edit Description**. You can use policy descriptions to help you keep track of your policies.
5. Open the policy’s property sheet and locate the rule you do not want to apply to Carol and Martin. Set the rule’s state to **Disabled**.
6. Assign users Carol and Martin to the policy by right-clicking the policy name and choosing **Assign Users**. Select the **Show Users** option to display individual user accounts.

7. Click **OK** when you are done adding users.
8. Rank the “Accounting Profile - local drive access” policy higher than the “Accounting Profile” policy. By default, new policies are given the lowest rank. To view a policy’s priority number, you must set the Citrix Management Console’s view mode to **Details**. To do this, select **Details** on the **View** menu.

Right-click the “Accounting Profile - local drive access” policy and select **Priority > Increase Priority** until this policy’s priority number is higher than the “Accounting Profile” policy.

Shadowing ICA Sessions

You can monitor the actions of users in ICA sessions by shadowing their sessions. A shadowed session is displayed in the session of the *shadower*, the user 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.

You can create a user policy to enable user-to-user shadowing. When you create a policy allowing user-to-user shadowing, users can shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration. See “Configuring User-to-User Shadowing” on page 286 for more information about user-to-user shadowing.

A shadower can remotely control a shadowed session through the shadower’s mouse and keyboard, if this action was not prohibited by options selected when MetaFrame XP was installed on the server.

Important If shadowing restrictions are selected during MetaFrame XP installation, the restrictions cannot be changed later. For more information, see “Configuring Session Shadowing” on page 115.

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 Citrix Management Console

When you use Citrix Management Console for shadowing, you must start each shadowing session individually; if you select multiple sessions to shadow, the **Shadow** command and button are not available. To start shadowing multiple sessions at once, use the Shadow Taskbar.

To use Citrix Management Console for shadowing, you must have the ICA Client installed on the system with the console. The ICA Client is installed by default when you install MetaFrame XP on a server, but the client is not installed when you install Citrix Management Console separately on a workstation. You can use the Citrix MetaFrame XP Components CD-ROM to install the ICA Client on a workstation.

► To shadow a session from the console

1. On the **Users** or **Sessions** tab in the right pane of the console, right-click the user or session that you want to shadow.
2. Choose **Shadow** from the pop-up context menu.

To begin shadowing, you can also select a user or session listing 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 about shadowing with the Shadow Taskbar, press F1 to view online help when the Shadow Taskbar is running.

Configuring User-to-User Shadowing

You can monitor the actions of users in ICA sessions by shadowing their sessions. A shadowed session is displayed in the session of the *shadower*, the user who establishes shadowing.

With user-to-user shadowing, you can allow users to shadow other users, without requiring them to be members of the Citrix Administrators group. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration.

With user-to-user shadowing, you can enable Help Desk personnel to shadow users' ICA sessions or allow your sales department to hold an online meeting to review sales leads.

The basic steps for configuring user-to-user shadowing are as follows. These steps are explained in more detail later in this section.

1. Create a user policy that identifies the users who can shadow other users' sessions
2. Assign the policy to the users to be shadowed
3. Publish the Citrix Shadow Taskbar and assign it to the users who will shadow
4. Instruct these users how to initiate shadowing from their client devices

Note You are prompted to configure shadowing settings during MetaFrame Setup. If you elected to prohibit shadowing during Setup, you cannot enable shadowing with user policies. You can also disable shadowing for a particular connection type using the Citrix Connection Configuration utility. If you disable shadowing in Citrix Connection Configuration, you cannot enable shadowing with user policies.

Creating User Policies for User-to-User Shadowing

You configure user-to-user shadowing by creating user policies that define users who can shadow. You then assign the policies to the users you want to be shadowed.

Important You can create and apply a policy that allows Novell Directory Services (NDS) users to be shadowed. However, you cannot configure NDS users to have shadowing permissions.

In the following procedure, the interwoven example assumes that you want to create a policy for your "Sales" user group that allows them to shadow the department manager, AnthonyR. The sales department uses the user-to-user shadowing feature for online collaboration on sales leads.

► **To create a user policy for user-to-user shadowing**

1. Create a new policy. The policy for the sales department is named “Sales Group Shadowing.” See “Creating and Applying User Policies” on page 281 for step-by-step instructions for creating user policies.
2. Open the Sales Group Shadowing policy’s property sheet by double-clicking the policy name.
3. Open the Shadowing folder in the left pane. Select the rule named Configure User Shadowing.
4. Set the rule’s state to enabled by clicking **Rule Enabled**.
5. Click **Allow shadowing** to enable shadowing.

Because the sales manager may work with sensitive data, select the option **Prohibit being shadowed without notification**.

If the sales manager does not want other users to be able to take control of his mouse and keyboard, select the option **Prohibit remote input when being shadowed**.

6. Select the rule named Assign Shadowing Permissions in the left pane of the property sheet.
7. Set the rule’s state to enabled by clicking **Rule Enabled**.
8. Click **Configure** to select the users who will shadow the sales manager.

To allow the members of the sales department to shadow the sales manager, select the Sales user group and then click **Add**. The user group is listed in the Configured Accounts list.

Click **OK** when you are done adding users.

9. The users and user groups you added to the Configured Accounts list are listed in the right pane of the policy’s property sheet. By default, the shadowing permission for each user or user group is set to **Allow**. You can deny shadowing permissions by clicking **Deny**.
10. Click **OK** at the bottom of the policy’s property sheet when you are done configuring the shadowing rules.

After you create the policy and configure the rules, you must assign the policy to the users who you want to be shadowed.

► **To assign the shadowing policy to users**

1. Right-click the Sales Group Shadowing policy and select **Assign Users**.
2. Select the users you want to be shadowed. To allow the sales manager, AnthonyR, to be shadowed, select the domain of which he is a member. Click **Show Users** to display the individual user accounts in the selected domain.
3. Select the user AnthonyR and then click **Add**. AnthonyR's user account is displayed in the Configured Account list.
4. Click **OK** when you are done adding users.

Important The list of users permitted to shadow is exclusive for each user to whom a policy is assigned. For example, if you create a policy that permits user MichelleF to shadow user LorenaB, this policy allows *only* MichelleF to shadow LorenaB, unless you add more users to the list of users who can shadow in the same policy's property sheet.

To allow users to shadow other users' ICA sessions, you can publish the Shadow Taskbar utility to the users you want to be able to shadow. When users open this published application, the Shadow Taskbar appears at the top of users' screens.

For more information about using the Shadow Taskbar to shadow ICA sessions, see "Using the Shadow Taskbar" on page 285 and the Taskbar's online help.

Monitoring Performance of Sessions and Servers

Performance monitoring counters for ICA data are installed with MetaFrame XP and can be accessed from Performance Monitor, which ships with Microsoft Windows NT 4.0, TSE and the Windows 2000 Server family.

By using Performance Monitor, you can monitor the following ICA-specific counters:

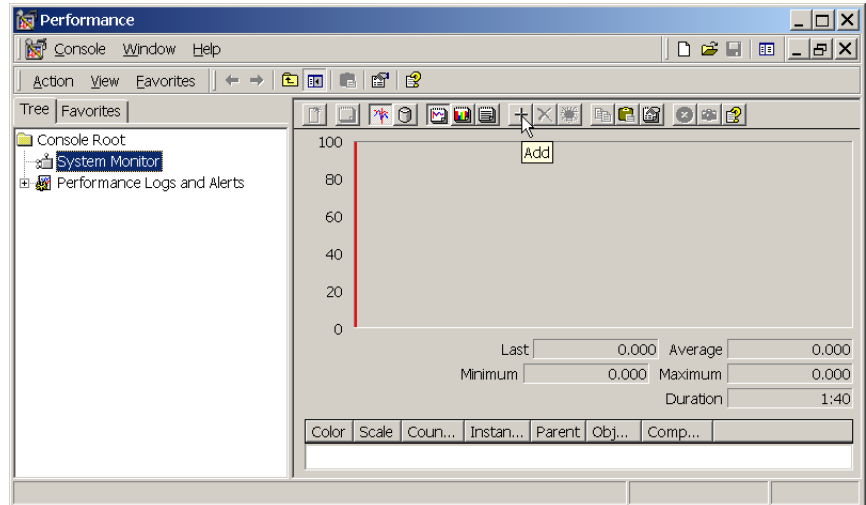
- Bandwidth and compression counters for ICA sessions and MetaFrame XP servers
- Bandwidth counters for individual virtual channels within an ICA session
- Latency counters for ICA sessions

Note The entire ICA counter list is exposed only on a MetaFrame XPe server. On a MetaFrame XPa or MetaFrame XPs server, only latency-related counters are available.

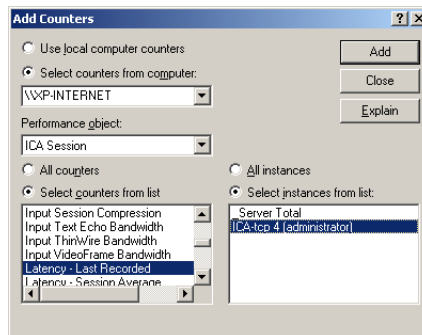
Performance monitoring provides valuable information about utilization of network bandwidth and helps determine if a bottleneck exists.

► **To access ICA performance counters**

1. Select **Start > Programs > Administrative Tools > Performance**.
2. Select **System Monitor** in the Tree view.



3. Click **Add**.
4. In the **Add Counters** dialog box, click the **Performance object** drop-down list and select **ICA Session**.



The ICA performance counters are listed under **Select counters from list**.

5. Select **All Counters** to enable all available ICA counters or select **Select counters from list** and then highlight the individual counters you need.

6. Select **All Instances** to enable all instances of the selected ICA counters or select **Select instances from list** and highlight only the instances you need.

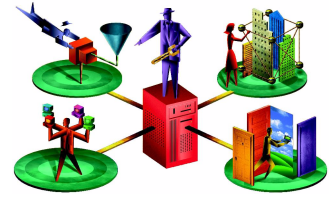
In Performance Monitor, the instance list contains all active ICA sessions, which includes any session (shadower) that is shadowing an active ICA session (shadowee). An active session is one that has been successfully logged on to and is in use; a shadowing session is one that initiated shadowing of another ICA session.

Note In a shadowing session, although you are able to select ICA counters to monitor, you will see no performance data for that session until shadowing is terminated.

7. Click **Add** and then click **Close**.

You can now use Performance Monitor to view and analyze performance data for the ICA counters you added. For more information about using Performance Monitor, see your Windows documentation.

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.

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.

For more information about printing configuration and options for ICA Clients, see 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 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 is 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 Scenarios

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.

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 devices (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 Windows 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 devices. 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 auto creates 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 on to the console as a Citrix administrator with access to manage the Printer Management node. If you log on as an administrator with view-only privilege, you can view printer configuration information but you cannot make changes to existing settings.

For information about using Citrix Management Console, see “To use Citrix Management Console” on page 166.

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 MetaFrame XP 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 machine to which the console is connected 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 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 308.

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 auto creation 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 auto created printer in the users' ICA sessions. If you want to assign the same users to another printer, select the printer and copy its auto creation 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 auto creation 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 302.

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 is 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.

After 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 that have different names for the same printer 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, Wtspnt.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 302), 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 to a client printer with a badly behaved driver can crash a server, you might need to prevent auto creation of client printers that use certain printer drivers.

If a defective 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 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 (auto creates) 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.

Auto Creation of Client Printers for DOS and WinCE

MetaFrame XP provides auto creation of client printers (printers that are locally connected to client devices) for DOS and WinCE Clients. Auto creation makes these printers available for the client user for printing from the applications they run in ICA sessions.

Auto created 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 auto creation for DOS and WinCE Clients.

MetaFrame XP can make the client printers available if you set up auto creation for these ICA Clients from the console. MetaFrame 1.8 can enable auto creation 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 is 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.

ICA Client Settings for Printer Access

Settings that affect the auto creation 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 about ICA Client capabilities and settings, see 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 auto created 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. 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.

Using the Citrix Universal Print Driver

As described previously in this chapter, MetaFrame XP automatically creates client printers when users log on to MetaFrame XP. With auto creation of client printers, users print to their regular printers from applications that are running on MetaFrame XP servers, without having to set up their printers each time they log on.

Auto creation of client printers requires drivers for client printers to be available on MetaFrame XP servers. The driver replication feature helps ease printer driver management (see “Managing Drivers for Client Printers” on page 302). However, maintaining drivers for many different printing devices can cause problems.

The Citrix Universal Print Driver is designed to avoid problems with driver maintenance and other client printing issues in diverse environments.

Client Printing with the Universal Driver

The Citrix Universal Print Driver eliminates the need for many native printer drivers to be installed on every MetaFrame XP server in a server farm. The Universal Print Driver feature comprises the following two components:

- The Citrix PCL4 Universal Driver, a standard PCL4 printer driver that is used on all MetaFrame XP servers.
- A PCL4 interpreter and rendering agent that is integrated into the ICA Win32 Client. Version 6.20 or later of the ICA Win32 Client is required.

When using this feature, the user prints from an application and the Citrix PCL4 Universal Driver on the server generates a print job in PCL4 format. The server sends the PCL4 print job to the ICA Client, where the PCL4 interpreter renders the print job. The client uses the local printer driver and print services to output the rasterized print job on the client printer.

The PCL4 interpreter in the ICA Client rasterizes print pages in monochrome at 300 dots per inch (dpi) resolution. The universal driver feature works with any client printer, including PCL, PostScript, and Windows printers. Color images can be printed in grayscale (dithered black and white) on color printers. The PCL4 interpreter does not support special printer options or features such as duplex printing.

To use the Universal Print Driver feature, you do not need to install a printer driver on MetaFrame XP servers. The Citrix PCL4 Universal Driver is listed on the **Drivers** tab in Citrix Management Console after you install and activate MetaFrame.

Benefits of Using the Universal Driver

With the Universal Print Driver feature, you can avoid the following issues:

- Some native printer drivers, especially those that do not use an advanced page description language such as PCL or PostScript, generate very large print files. These files can cause unacceptable delays when print jobs are spooled from the server to the client over a WAN or other slow connection.

- Many printer drivers are not well tested in a terminal server environment. Some drivers cause frequent system crashes and spooler faults. Installing many printer drivers for a large user base can destabilize servers.
- Although driver maintenance is more convenient with MetaFrame XP, the effort required to obtain, install, and manage many different printer drivers for a diverse environment can be substantial. Even with careful maintenance, drivers required for printing to every device might not be installed in the server farm. Missing drivers prevent auto creation of client printers for users.

Configuring the Universal Driver for Client Printing

To configure printing options for the server farm, right-click **Printer Management** in the Citrix Management Console tree and choose **Properties**. Use the **Drivers** tab to select which printer drivers should be used for creating printer connections. Use the **Printers** tab to select settings for auto creating client and network printers.

Configuring Client Printer Auto Creation

You can use the **Auto-Create Client Printer Connections at Login** option to allow client printers to be automatically created when users log on to ICA sessions. This option is selected by default. If you clear this option, no client printers are automatically created although users can set up connections to client printers manually.

When **Auto-Create Client Printer Connections at Login** is selected, you can configure how the printers work using the following options:

Update printer properties at each logon. Select this option to update client printers on the server using settings from printers on the clients. The client printers are updated when users log on. Do not select this option if you want to retain changes made during ICA sessions to client printers on the server.

Inherit client printer's setting for keeping printed documents. Select this option to use the client printer setting, Keep printed documents, on auto created client printers. The setting determines if printed jobs are saved after users log off from ICA sessions. Saving printed jobs can take a lot of space.

Delete pending print jobs at logout. Select this option to delete pending print jobs when a user logs off. Do not select this option if you want users to see print jobs from prior ICA sessions when they log on.

You can specify which printers are auto created by selecting one of the following options:

Default client printer only. Select this option to auto create only the default printer on each client device.

Local (non-network) client printers only. Select this option to auto create only the local client printers on a user's client device. Local client printers are connected directly to the client device through an LPT, COM, USB, or other local port.

All client printers. Select this option to auto create all of the client printers on a user's client device.

Use connection settings for each server. Select this option to accept the settings specified for the ICA session connection used in Citrix Connection Configuration. This option is selected by default.

The term *connection* here refers to the virtual ports on MetaFrame XP servers, which are associated with a network protocol. To change the connection configuration, launch Citrix Connection Configuration (choose **Start > Programs > Citrix > MetaFrame XP > Citrix Connection Configuration**), double-click the connection in the Citrix Connection Configuration window, and click **Client Settings**.

Network printers assigned to users can be updated when the users log on. To update network printers with the printing preferences assigned to the printer through the console, select **Update printer properties at each logon** in **Auto-Created Network Printers**. Do not select this option if you want to retain changes made by users to their network printer settings during ICA sessions.

Specifying Printer Drivers for Client Printing

When client printers are auto created, you can specify whether they use native printer drivers that must be installed on the server, the Universal Print Driver, or both. Select one of the following options:

Native drivers only. Select this option to use native printer drivers when client printers are auto created. If the native driver is not available on the MetaFrame XP server, the client printer cannot be created on the server. This option disables the Universal Print Driver feature.

Universal driver only. Select this option to use the Citrix PCL4 Universal Print Driver to create client printers on the server. The universal driver is limited to monochrome at 300 dots per inch (dpi).

Use universal driver only if native driver is unavailable. Select this option to use native drivers for client printers if available. If the driver is not available on the server, the client printer is auto created with the Citrix PCL4 Universal Driver. This is the default and it allows fault tolerance. Printers are auto created for users even if native drivers for their printing devices are not available or are incompatible with terminal server systems.

Both universal and native drivers. Select this option to create two versions of each client printer: one with the Citrix PCL4 Universal Driver and the other with the printer's native driver (if it is installed on the server). Users can print using either printer version. This option is useful if users need to access special printer features occasionally. Users can identify the universal driver by the text "[UPD:PCL4]" at the end of the printer name.

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 about views for bandwidth management, see "Using the Printer Management Node" on page 295 and "Bandwidth Tab" on page 297.

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
acrcfg	Configure autoreconnect settings
altaddr	Specify server alternate IP address
app	Run application execution shell
auditlog	Generate server logon/logoff reports
change client	Change ICA Client device mapping
chfarm	Change the server farm membership of the server
clicense	Maintain Citrix licenses
cltprint	Set the number of ICA Client printer pipes
ctxmlss	Change the XML Service port number
dsmaint	Configure the IMA data store
icaport	Configure TCP/IP port number
imaport	Change IMA ports
query	View information about server farms, processes, servers, ICA sessions, and users
twconfig	Configure ICA display settings

ACRCFG

Use **acrcfg** to configure autoreconnect settings on a MetaFrame XP server or server farm.

Syntax

acrcfg [/server:*servername* | /farm] [/query | /q]

acrcfg [/server:*servername* | /farm] [/enable:on | off] [/logging:on | off]

acrcfg [/server:*servername*] [/inherit:on | off] [/enable:on | off]
[/logging:on | off]

acrcfg [/?]

Parameters

servername

The name of a MetaFrame XP server.

Options

/query, /q

Query current settings.

/server

The server to be viewed or modified by the other command line options. The server specified by *servername* must be in the same server farm as the server on which the command is run. This option and the **/farm** option are mutually exclusive. The local server is the default if neither **/server** nor **/farm** is indicated.

/farm

The options on the command line after **/farm** are applied to the entire server farm.

/inherit:on | off

To use the autoreconnect setting from the server farm set **/inherit** to **on** for a server. To disregard the server farm autoreconnect setting, set **/inherit** to **off**. By default, this is set to **on** for a server.

/enable:on | off

To enable autoreconnect for a server or a server farm, set **/enable** to **on**. Servers inherit the server farm setting unless **/inherit** is **off**. To disable autoreconnect for a server or server farm, set **/enable** to **off**. **/enable** is set to **on** for both a server and a server farm by default.

/logging:on | off

To enable logging of client reconnects for a server or server farm, set to **on**. To disable logging, set to **off**. Logging is set to **off** for both servers and server farms by default.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

Autoreconnect disconnects a broken session and reconnects it. The user's current workspace is preserved and the user is restored to the same place in the application. Intentional disconnections by users do not trigger autoreconnect. The autoreconnect feature is enabled by default.

Use **/query** or **/q** to display the current settings. The **/enable** and **/logging** options are valid with either **/server** or **/farm**, but **/inherit** is not used with **/farm**. If neither **/server** nor **/farm** is selected and the **/inherit**, **/enable**, or **/logging** options are used, they are applied to the local server.

When **/logging** is no longer valid it disappears from later queries. If **/logging** is **on** and you set **/enable** to **off**, there is no longer anything to log, so the logging line is no longer shown in a query. A query shows the enable setting whether or not it is in effect, but **acrcfg** will not change the enable setting on the server if inherit is enabled.

Examples

The next four commands disable autoreconnect on the server farm, show the results, enable autoreconnect and logging from the local server, and show the results.

```
C:\>acrcfg /farm /enable:off
```

```
Update successful
```

```
C:\>acrcfg /farm /q
```

```
Auto Client Reconnect Info for Server: Farm
```

```
ENABLED:          off
```

```
C:\>acrcfg /inherit:off /enable:on /logging:on
```

```
Update successful
```

```
C:\>acrcfg /q
```

```
Auto Client Reconnect Info for Server: Local Server
```

```
INHERIT:          off
```

```
ENABLED:          on
```

```
LOGGING:          on
```

Security Restrictions

You must be a Citrix administrator to make changes.

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 MetaFrame XP server on which to set an alternate address.
Defaults to the current MetaFrame XP 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 the utility's 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 displays 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 1.1.1.1:

```
altaddr /set 1.1.1.1 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” type files to user directories before starting an application, or to perform application-related cleanup after an application terminates. The script commands are described below.

Syntax

app *scriptfilename*

Parameter

scriptfilename

The name of a script file containing app commands (see script commands below).

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*.

Script 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 (*,?).

sourcedirectory

The directory and path from which files are to be copied.

targetdirectory

The directory and path to which files are to be copied.

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 time-out for hard drive cache entries is ten minutes and the time-out 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 time-out 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. A and B Drives are always mapped to drives 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 drives C and D, the client drives C and D 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 LPT1 ports are mapped to the server's LPT1 and LPT1 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 drives A and B 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 drives C and D, the client drives C and D 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, drives C and D 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

Change farm 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. Citrix recommends that you back up your data store before running **chfarm**.

Important If the server you want to move provides information for a Resource Manager summary database, update the summary database before using **chfarm**. If you do not update the summary database, you will lose approximately 24 hours worth of summary data stored on the server. To update the summary database, click the Resource Manager node in Citrix Management Console, select the **Summary Database** tab, and click **Update Now**.

The **chfarm** utility is installed in %program files%\citrix\system32\citrix\IMA. To run this utility, choose **Run** from the **Start** menu. Enter **chfarm**.

While running **chfarm**, you are prompted for the username and password of the user you want to designate as the initial Citrix administrator for the farm. **Chfarm** 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 about data store setup and server farm configuration, see “Selecting the MetaFrame XP Family Level” on page 107. If **chfarm** reports any error, continuing the process can corrupt the data store. If you cancel out of the data store configuration part of the MetaFrame XP Setup wizard, the server you are switching rejoins the original farm.

After the farm membership is changed or a new farm is created, reboot the MetaFrame XP server.

Do not remove a server that hosts a server farm’s data store from the server farm. Doing so renders the farm unstable.

CLICENSE

You can use **clicense** to add, remove, query, and maintain license information for MetaFrame XP servers within a server farm. For more information about Citrix licensing, see “Licensing MetaFrame XP” on page 135.

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 database 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 is located on the software packaging. See *license_string*.

server_name

The name or IP address of a MetaFrame XP 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 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 **clicense** commands can be executed only by a member of the Citrix Administrators group.

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 represented by *nn* 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 [/rnnn] [/u] [/knnn] [/?]

Options

/rnnn

Changes the port number for the Citrix XML Service to *nnn*.

/u

Unloads Citrix XML Service from memory.

/knnn

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 “Configuring the Citrix XML Service Port” on page 117.

Security Restrictions

None.

DSMAINT

Use **dsmaint** to configure the IMA data store for a MetaFrame XP server farm.

When using this command, user names and passwords may be case-sensitive, depending on the database product you are using and the operating system it runs on.

Syntax

dsmaint config [/user:username] [/pwd:password] [/dsn:filename]

dsmaint backup *destination_path*

dsmaint failover *direct_server*

dsmaint compactdb [/ds] [/lhc]

dsmaint migrate [{ /srcdsn:*dsn1* /srcuser:*user1* /srcpwd:*pwd1* }] [{ /dstdsn:*dsn1* /dstuser:*user1* /dstpwd:*pwd1* }]

dsmaint publishsqllds {/user:username /pwd:password}

dsmaint recover

dsmaint recreatelhc

dsmaint [/?]

Parameters

destination_path

Path to the backup data store.

dsn1

The name of the source data store.

dsn1

The name of the destination data store

filename

The name of the data store.

direct_server

The name of the new direct server for IMA data store operations.

password

The password to connect to the data store.

pwd1

The source data store password.

pwdl

The destination data store password.

userl

The source data store user logon.

userl

The destination data store user logon.

username

The 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

The username to connect to a data store.

/pwd:password

The password to connect to a data store.

/dsn:filename

The 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 share point 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 database.

/srcdsn:*dsn1*

The name of the data store from which to migrate data.

/srcuser:*user1*

The user name 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:*dsn1*

The name of the data store to which to migrate the data.

/dstuser:*user1*

The username to use to connect to which the data store the data is migrating.

/dstpwd:*pwd1*

The password to use to connect to which the data store the data is migrating.

publishsqlds

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.

/recreatelhc

Recreates the local host cache database.

/?

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.

publishsqlds

Execute **publishsqlds** 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 for changing the port number on ICA Clients, see the *Citrix ICA Client Administrator's Guide* 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**.

IMAPORT

Use **imaport** to query or change the IMA port.

Syntax

```
imaport {/query | /set {IMA:nnn | ds:nnn | cmc:nnn}* | /reset {IMA | DS | CMC | ALL} }
```

Options

/query

Queries the current setting.

/set

Sets the designated TCP/IP port(s) to a specified port number.

ima:nnn

Sets the IMA communication port to a specified port number.

cmc:nnn

Sets the Citrix Management Console connection port to a specified port number.

ds:nnn

Sets the data store server port to a specified port number (indirect servers only).

/reset

Resets the specified TCP/IP port to the default.

ima

Resets the IMA communication port to 2512.

cmc

Resets the Citrix Management Console connection port to 2513.

ds

Resets the data store server port to 2512 (indirect servers only).

all

Resets all of the applicable ports to the defaults.

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      [/online | /online zonename]  
query farm      [/offline | /offline zonename]  
query farm      [/zone | /zone zonename]  
query farm      [/?]
```

Parameters

appname

The name of a published application.

server

The name of a server within the farm.

zonename

The name of a zone 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.

/online

Displays servers online within the farm and all zones. The data collectors are represented by the notation "D".

/online *zonename*

Displays servers online within a specified zone. The data collectors are represented by the notation "D".

/offline

Displays servers offline within the farm and all zones. The data collectors are represented by the notation "D".

/offline *zonename*

Displays servers offline within a specified zone. The data collectors are represented by the notation "D".

/zone

Displays all data collectors in all zones.

/zone *zonename*

Displays the data collector within a specified zone.

/?

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

*

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.

Options

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.

Security Restrictions

None.

Query Server

Syntax

query server [*server* [/ping [/count:*n*] [/size:*n*] | /stats | /reset | /load
| /addr]]

query server [/tcp] [/ipx] [/netbios] [/tcpserver:*x*] [/ipxserver:*x*]

query server [/netbiosserver:*x*]

query server [/license | /app | /gateway | /serial | /disc | /serverfarm | /video]

query server [/continue] [/ignore] [/?]

Parameters

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.

Options

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.

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

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.

Options

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.

Security Restrictions

None.

Query Termserver

Syntax

query termserver [*servername*] [/domain:*domain*] [/address] [/continue]

query termserver [/?]

Parameters

servername

The name of a server within the farm.

domain

The name of a domain to query.

Options

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.

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

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.

Options

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.

/?

Displays the syntax for the utility and information about the utility's options.

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 kilobytes) to use for each session's graphics (150KB minimum, 8192KB 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 be used only 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.

MetaFrame XP Setup Properties



This chapter describes the properties in the MetaFrame XP Windows Installer package that you run to install MetaFrame XP. This chapter also explains the four sample Windows Installer transform files included on the MetaFrame XP CD-ROM in the directory Support\Install. Refer to these properties when creating a Windows Installer transform file to apply to the MetaFrame XP Windows Installer package.

Property Names and Values

Property names are case-sensitive. Values are not case-sensitive but must be enclosed in quotation marks (""") if you are using them in a command line.

CTX_MF_USER_NAME

Definition: User name for the initial Citrix administrator credentials; applies only when creating a farm

Possible values: User defined

Default value: "UserName"

CTX_MF_DOMAIN_NAME

Definition: Domain name for the farm administrator credentials; applies only when creating a farm

Possible values: User defined

Default value: "DomainName"

CTX_MF_SHADOWING_CHOICE

Definition: Turn shadowing on or off

Possible values: "Yes" - turn it on, or "No" - turn it off

Default value: "Yes"

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA

Definition: Prohibit or do not prohibit remote control ICA sessions

Possible values: “Yes” - Prohibit, or “No” - Do not Prohibit

Default value: “No”

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION

Definition: Prohibit or do not prohibit shadow connections without notification

Possible values: “Yes” - Prohibit, or “No” - Do not Prohibit

Default value: “No”

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING

Definition: Prohibit shadow connections without logging

Possible values: “Yes” - Prohibit, or “No” - Do not Prohibit

Default value: “No”

CTX_MF_FARM_SELECTION

Definition: Create/Join Farm

Possible values: “Create” - create a farm, or “Join” - join a farm

Default value: “Create”

CTX_MF_NFUSE_DEF_WEB_PAGE

Definition: Change default Web page (make NFuse your Web server's default Web page)

Possible values: “Yes” or “No”

Default value: “No”

CTX_MF_XML_CHOICE

Definition: Share IIS&XML or Use separate port

Possible values: “Share” - share with IIS, or “Separate” - use separate port as mentioned by CTX_MF_XML_PORT_NUMBER

Default value: “Share”

CTX_MF_XML_PORT_NUMBER

Definition: XML port number when you choose not to share it with IIS

Possible values: User defined

Default value: “80”

CTX_MF_FARM_SELECTION

Definition: Specifies whether a user can join or create a farm

Possible values: “Create” or “Join”

Default value: “Create”

CTX_MF_CREATE_FARM_DB_CHOICE

Definition: Specifies whether the database is a local access database or third-party database

Possible values: “ThirdParty” or “Local”

Default value: “Local”

CTX_MF_ODBC_PASSWORD

Definition: Password for a third-party database

Possible values: User defined

Default value: “Password”

CTX_MF_ODBC_USERNAME

Definition: User name for a third-party database

Possible values: User defined

Default value: “Username”

CTX_MF_SILENT_DSNFILE

Definition: DSN File for the silent install to be used for the data store

Possible values: Complete path to the DSN File

Default value: “” (null)

CTX_MF_JOIN_FARM_DB_CHOICE

Definition: Specifies the type of join farm — direct or indirect

Possible values: “Direct” or “Indirect”

Default value: “Direct”

CTX_MF_INDIRECT_JOIN_DOMAIN_NAME

Definition: Domain name to be used in the event of an “Indirect” join farm

Possible values: Can be any user’s domain (the user account must have administrative privileges in MetaFrame)

Default value: “DomainName”

CTX_MF_NEW_FARM_NAME

Definition: The name of the new farm; always specify if you are creating a new farm

Possible values: User defined

Default value: "NewFarmName"

CTX_MF_INDIRECT_JOIN_USER_NAME

Definition: User Name if this is an "Indirect" join

Possible values: Can be any user who has administrative privileges in MetaFrame

Default value: "UserName"

CTX_MF_INDIRECT_JOIN_PASSWORD

Definition: Password to use if this is an "Indirect" join

Possible values: The password for the user name entered in CTX_MF_INDIRECT_JOIN_USER_NAME

Default value: "Password"

CTX_MF_JOIN_FARM_SERVER_NAME

Definition: Name of the Indirect join server

Possible values: Any server that has MetaFrame installed

Default value: "ServerName"

CTX_MF_JOIN_FARM_SERVER_PORT

Definition: Name of the Indirect join server port

Possible values: User defined

Default value: "2512"

REBOOT

Definition: Standard Windows Installer property that controls whether you restart a server or prompt for the server to be restarted

Possible values: "Force" - Forces reboot to occur, no further prompts are displayed

"Suppress" - Forces reboot to *not* occur by default; a prompt occurs if action is necessary

"ReallySuppress" - Force reboot to *not* occur, no questions asked

Default value: "Force"

CTX_MF_ZONE_NAME

Definition: Name of the zone to which the server belongs

Possible values: Not applicable

Default value: "ZoneName"

CTX_MF_LAUNCH_CLIENT_CD_WIZARD

Definition: Specifies whether to launch the ICA Client Distribution wizard (to update the ICA Clients on the MetaFrame server)

Possible values: "Yes"- Launch wizard, or "No" - Do not launch wizard; that is, do not update clients

Default value: "No"

CTX_MF_CLIENT_CD_PATH

Definition: Path to the MetaFrame XP Components CD-ROM to be passed to the ICA Client Distribution wizard

Possible values: Complete path to the Components CD-ROM

Default value: "" (null)

CTX_MF_PRODUCT_CODE

Definition: Product code of the MetaFrame server you are trying to install. If you are performing a silent install and using a command line, the command line arguments for this property must be set to the correct value

Possible values: The product code on the MetaFrame XP CD-ROM

Default value: "0D00-06A7"

CTX_MF_SERVER_TYPE

Definition: The family level of MetaFrame to be installed. If you are performing a silent install and using a command line, the command line arguments for this property must be set to the correct value

Possible values: "E" for MetaFrame XPe, "A" for MetaFrame XPa, or "S" for MetaFrame XPs

Default value: "E"

Creating Transforms

You can manipulate the installation process by applying Windows Installer *transforms* (files with the .mst extension) to the installation database contained in a Windows Installer package. A transform makes changes to elements of the database. A transform file modifies the installation package when it is being installed and dynamically affects the installation behavior.

Transforms that you create to customize a Windows Installer setup package remain cached on your system. These files are applied to the base Windows Installer package whenever the Installer needs to modify it. You can apply transforms only when you initially install Windows Installer packages; you cannot apply transforms to software that is already installed.

When you create a transform to apply to the MetaFrame XP Windows Installer package, you set your desired values for properties in the package. When you then apply the transform to the installation package, the “questions” you would be asked during Setup are answered. Creating a transform allows you to install MetaFrame XP in unattended mode.

There are several commercially available tools you can use to create or edit transforms.

Citrix provides four sample transforms on the MetaFrame XP CD-ROM. The sample transforms include sample values for select properties, allowing you to determine which properties you can edit to achieve a certain configuration.

You can use these sample transforms to create a MetaFrame XP server farm using Microsoft Access or Microsoft SQL Server as the farm’s data store.

Important Do not apply the sample transforms to MetaFrame XP Setup without editing them to include your required values. Some of the commercially available Windows Installer packaging tools allow you to edit existing transforms. Use the sample transforms as a guideline to achieve the desired configuration.

► **To create a customized transform using one of the sample transform files**

1. Using your preferred tool for editing Windows Installer packages, open the sample transform you want to modify.
2. Enter new values for the properties you want to change.
3. Save the file with a new name.

You can apply transforms when you install the Windows Installer package by using the **Msiexec** command.

► To apply a transform

Type the following at a command prompt where *<package>* is the name of the MetaFrame XP Windows Installer installation package and *<TransformList>* is the list of the transforms that you want to apply.

msiexec /i package TRANSFORMS=TransformList

If you are applying multiple transforms, separate each transform with a semicolon. For further information about the parameters and switches you can use with these options, go to the Microsoft Web site at <http://www.microsoft.com> and search on “msiexec.”

The properties to set to achieve the results of each sample transform are listed in the following sections.

Create a New MetaFrame XP Server Farm

This sample transform shows possible values for creating a farm that uses a Microsoft Access database as the server farm’s data store. The database is stored locally on the MetaFrame server and is configured for direct access by the other servers in the farm. The name of the file is **Localdb_access_create.mst**.

Properties and Sample Values

CTX_MF_NEW_FARM_NAME= FarmAccess

CTX_MF_USER_NAME=Administrator

CTX_MF_DOMAIN_NAME=Domain1

CTX_MF_FARM_SELECTION=Create

CTX_MF_NFUSE_DEF_WEB_PAGE=Yes

CTX_MF_SHADOWING_CHOICE=Yes

CTX_MF_XML_PORT_NUMBER=80

CTX_MF_XML_CHOICE=Share

CTX_MF_SERVER_TYPE=a

CTX_MF_PRODUCT_CODE=0A00-0C32

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

CTX_MF_CLIENT_CD_PATH=H:\image

CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes

Join an Existing MetaFrame XP Server Farm

In this sample transform, the existing server farm uses a Microsoft Access database stored on one of the MetaFrame XP servers. The new server joining the farm accesses the data store indirectly — through the data store created for direct access. The name of the file is **Join_Indirect.mst**.

Properties and Sample Values

CTX_MF_FARM_SELECTION=Join

CTX_MF_INDIRECT_JOIN_USER_NAME=Administrator

CTX_MF_INDIRECT_JOIN_DOMAIN_NAME=Domain1

CTX_MF_JOIN_FARM_SERVER_NAME=Server1

CTX_MF_JOIN_FARM_SERVER_PORT= 2512

CTX_MF_JOIN_FARM_DB_CHOICE=Indirect

CTX_MF_NFUSE_DEF_WEB_PAGE=Yes

CTX_MF_XML_PORT_NUMBER=80

CTX_MF_XML_CHOICE=share

CTX_MF_SERVER_TYPE=a

CTX_MF_PRODUCT_CODE= 0D00-06A7

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=Yes

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package. If you have a blank password, do not add the password property. In general, if a property exists in the .msi file and you want to set it to NULL, delete the property in the transform file.

CTX_MF_CLIENT_CD_PATH=H:\image

CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes

CTX_MF_INDIRECT_JOIN_PASSWORD=Password

Create a New MetaFrame XP Server Farm

This sample transform creates a farm that uses a Microsoft SQL Server, Oracle, or IBM DB2 database as the server farm's data store. The database is stored on a dedicated database server and is configured for direct access by the servers in the farm. The name of the file is **thirdpartydb_create_direct.mst**.

Properties and Sample Values

CTX_MF_NEW_FARM_NAME=Farm-ThirdParty
CTX_MF_CREATE_FARM_DB_CHOICE=ThirdParty
CTX_MF_USER_NAME=Administrator
CTX_MF_DOMAIN_NAME=Domain1
CTX_MF_FARM_SELECTION=Create
CTX_MF_ODBC_USER_NAME=sa
CTX_MF_ODBC_PASSWORD=Citrix
CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix
CTX_MF_NFUSE_DEF_WEB_PAGE=Yes
CTX_MF_SHADOWING_CHOICE=Yes
CTX_MF_XML_PORT_NUMBER=180
CTX_MF_XML_CHOICE=Separate
CTX_MF_SERVER_TYPE=e
CTX_MF_PRODUCT_CODE=0D00-06A7
CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No
CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes
CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

CTX_MF_CLIENT_CD_PATH=H:\image
CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes
CTX_MF_SILENT_DSNFILE =C:\TestSQL.DSN

Join an Existing MetaFrame XP Server Farm

In this sample transform, the existing server farm uses a SQL, Oracle, or IBM DB2 database stored on a dedicated database server. The new server joining the farm accesses the data store directly. The name of the file is **thirdpartydb_join_direct.mst**.

Properties and Sample Values

CTX_MF_FARM_SELECTION=Join
CTX_MF_JOIN_FARM_DB_CHOICE=Direct
CTX_MF_ODBC_USER_NAME=sa
CTX_MF_ODBC_PASSWORD=Citrix
CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix
CTX_MF_NFUSE_DEF_WEB_PAGE=Yes
CTX_MF_SHADOWING_CHOICE=Yes
CTX_MF_XML_PORT_NUMBER=180
CTX_MF_XML_CHOICE=Separate
CTX_MF_SERVER_TYPE=e
CTX_MF_PRODUCT_CODE=0D00-06A7
CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No
CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes
CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

CTX_MF_CLIENT_CD_PATH=H:\image
CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes
CTX_MF_SILENT_DSNFILE=C:\TestSQL.DSN

Glossary



account authority The platform-specific source of information about user accounts used by a MetaFrame XP 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 MetaFrame XP server, or server farm, and its published applications.

anonymous user account A user account defined on a MetaFrame XP 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 MetaFrame XP 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 MetaFrame XP 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 set A user's view of the applications published on a server farm that the user is authorized to access.

automatic client update The MetaFrame XP 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.

- automatic client reconnect** The feature that prompts supported ICA Clients to automatically reconnect to a session when dropped connections are detected (when network issues outside of MetaFrame XP occur).
- 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, and so on.
- Citrix Management Console** The extensible, platform-independent tool for administering MetaFrame XP servers and management products.
- Citrix administrators** System administrators responsible for installing, configuring, and maintaining MetaFrame XP servers. In a UNIX environment, it is the user group assigned to these administrators, which has the default name ctxadm.
- Citrix Program Neighborhood Agent** The Citrix Program Neighborhood Agent allows you to leverage Citrix NFuse to deliver published applications directly to users' desktops so users can access links to published applications with or without a Web browser. With the Program Neighborhood Agent, links to NFuse-enabled published applications appear in the Start menu, on the Windows desktop, or in the Windows System Tray. Remote applications are integrated into the desktop and appear to the user as local applications.
- Citrix SSL Relay** A Windows NT service that runs on a MetaFrame server to support an SSL-secured connection between an NFuse Classic server and the MetaFrame server. See also "Secure Sockets Layer (SSL)" on page 363 and "SSL support for ICA" on page 364.
- 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 MetaFrame XP server to access peripherals attached to COM ports on the client device.
- client device** Any hardware device capable of running the ICA Client software.
- client device mapping** The feature that enables remote applications running on the MetaFrame XP 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 MetaFrame XP server to access physical and logical drives configured on the client device.
- client printer mapping** The feature that enables applications running on the MetaFrame XP server to send output to printers configured on the client device.
- client update database** The database MetaFrame XP servers use to automatically update ICA Clients. It contains copies of the clients themselves and configuration information about how to perform the updates.

- connection control** The feature that allows you to set a limit on the number of connections that each user can have simultaneously in the server farm. You can also limit the number of concurrent connections to specified published applications, and you can prevent users from launching more than one instance of the same published application.
- connection license** A license that enables ICA connections between a client device and a MetaFrame XP server farm. Connection license counts can be assigned to specific servers; they are automatically pooled among all servers in the farm.
- content publishing** This feature allows you to publish document files, media files, Web URLs, and any other type of file from any network location. Icons for published content appear in Program Neighborhood, on the desktop, and in NFuse. Users can double-click published content icons to access content in the same way they access published applications.
- content redirection** This feature allows administrators to specify whether ICA Clients open published content, applications, browsers, and media players locally or remotely. There are two types of content redirection: from server to client and from client to server.
- custom ICA connection** A user-created shortcut to a published application or Citrix server.
- CPU prioritization** The feature that allows you to assign each published application in the server farm a priority level for CPU access. This feature can be used to ensure that CPU-intensive applications in the server farm do not degrade the performance of other applications.
- 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 MetaFrame XP server farm has a single data store.
- delegated administration** The feature that allows you to delegate areas of MetaFrame administration and farm management to your IT staff. Administrators can assign specialized staff members to perform specific MetaFrame tasks such as managing printers, published applications, or user policies. Specialized staff members can carry out their assigned tasks without being granted full access to all areas of farm management.
- disconnected session** An ICA session in which the ICA Client is no longer connected to the MetaFrame XP 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 MetaFrame XP 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.
- file type association** You configure content redirection from client to server by associating published applications with file types and then assigning them to the users you want to be affected.
- 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 MetaFrame XP 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 MetaFrame XP 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** The logical port used by an ICA Client to connect to, and start a session on, a MetaFrame XP server. 1. 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 MetaFrame XP 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 MetaFrame XP server specified in the file.
- ICA protocol** The protocol that ICA Clients use to format user input (keystrokes, mouse clicks, and so forth) and address it to MetaFrame XP servers for processing. MetaFrame XP 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 MetaFrame XP 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 MetaFrame XP 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 server installations 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 MetaFrame XP 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 MetaFrame XPa and MetaFrame XPe 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.

MetaFrame servers Servers on which Citrix MetaFrame software is running. You can publish applications, content, and desktops for remote access by ICA Clients on these servers.

mixed mode The mode in which MetaFrame XP servers operate when a server farm contains both MetaFrame XP servers and MetaFrame 1.8 servers. *See also* interoperability.

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. *See also* interoperability.

NDS support Support for Novell Directory Services allows users in Novell network environments to log on using their NDS credentials to access applications and content published in MetaFrame XP server farms.

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 1100 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 Authentication When you enable pass-through authentication, Citrix Management Console uses your local user credentials from the server on which the console is running. You can log on without re-entering credentials.

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.

policies Policies are used to apply MetaFrame settings, for client device mapping, for example, to specific users or user groups. They override similar MetaFrame settings configured farm-wide, at the server level, or on the ICA Client.

product code A nine-character string that identifies a MetaFrame XP server product. A server farm can contain MetaFrame XP 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 MetaFrame XP 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 MetaFrame XP 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.
- published content** A document, media clip, graphic, or other type of file or URL that you publish for access by ICA Client users. Published content is executed by local applications on client devices.
- 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 are 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 MetaFrame XP servers managed as a single entity, with some form of physical connection between servers and a database used for the farm's 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 MetaFrame XP server.

Shadow Taskbar The taskbar on a MetaFrame XP server desktop that you can use to shadow multiple users and to quickly switch between shadowed sessions.

shadowing A feature of MetaFrame XP servers that enables an authorized user to remotely join or take control of another user's ICA session for diagnosis, training, or technical support. *See also* user-to-user shadowing.

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.

SSL support for ICA This feature enables use of the SSL protocol to secure communication between the ICA Clients that support SSL and MetaFrame XP servers. SSL provides server authentication, encryption of the data stream, and message integrity checks. After configuring the Citrix SSL Relay, you can specify the use of SSL when you publish applications. *See also* Citrix SSL Relay.

Universal printer driver This driver can be installed in the server farm and used as the driver for all printers that users running the ICA Win32 Client use in the server farm. The Universal Printer Driver eliminates the need to install many separate printer drivers for diverse printing environments.

User-to-User Shadowing The feature that allows users to shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration. *See also* shadowing.

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

- Acrecfg command 310
- Acrobat Reader program 15
- activation codes 136, 143–144, 146–147
- Active Directory Services 60, 221
- Address List for client browsing 78
- administration tools
 - see* management tools
- administrator accounts
 - see* Citrix administrators
- ALE 254
- Altaddr command 313
- anonymous applications and users 249
- anonymous users 249
- App command 315
- applications
 - associating with file types 251
 - data about 271
 - launching and embedding 254
 - passing parameters to published applications 254
 - publishing 244, 250
 - see* publishing applications
 - redirecting launching 256
 - setting CPU priority for 262
- assigning licenses to servers 149
- Async Test dialog box 201
- asynchronous connection options 200–202
- asynchronous ICA connections 45, 194
- audio mapping 213
- Auditlog command 318
- authentication, user 62, 65–66, 71–72, 99, 111, 237, 245, 276, 280
- Auto Client Reconnect feature 276
- Auto Refresh Settings command 170
- automatic client update 223

B

- bandwidth and compression counters 288
- broadcasts
 - MetaFrame server response to 78
 - UDP 174
- BUILTIN group 71

C

- Change Client command 320
- Chfarm command 324
- Citrix Activation System 146
- Citrix administrators 72
 - creating customized administrators 163
 - delegated administration of tasks 162
 - delegating tasks 34
- Citrix Connection Configuration 191–192, 194–198, 200–202
- Citrix Documentation Library 18
- Citrix ICA Client Administrator's Guides 14
- Citrix licensing
 - see* licensing
- Citrix Management Console 40, 126–127, 161–171
 - controlling access to 163
 - installing separately 124
 - Java Run-Time Environment 46
 - online help 16
 - refreshing data 170
 - selecting server farms 167
 - updating 127
- Citrix NFuse Classic 14, 41, 44, 71, 73, 79–80, 83, 117, 217, 237–238
 - setting the MetaFrame server's default Web page 119
- Citrix Server Administration 96
- Citrix SSL Relay 39, 182, 187
 - changing the port 187
 - configuring 182
- Citrix Universal Print Driver 304
- Citrix Web Console 39, 127, 158, 170, 273
- Citrix Web site 17
- Citrix XML Service 79, 117, 329
- Clicense command 325
- client device mapping 210
- client documentation 14
- client printers 292
- Client Update Configuration utility 225
- Client Update Database 224–235, 240
 - adding clients 228
 - changing client properties 233
 - configuring update options 227
 - creating a new database 226
 - removing clients 232

- specifying a default database 226
- cloning MetaFrame XP servers 123
- Cltprint command 328
- COM port mapping 213
- commands 309–347
- Components CD 219
- configuring
 - anonymous user accounts 249
 - Citrix administrators 72, 162
 - Citrix SSL Relay 182
 - client device mapping 209
 - client reconnection settings 277
 - Connection Control settings 268
 - content redirection 34
 - data collectors 179
 - direct cable connections 200
 - ICA Administrator Toolbar 160
 - ICA audio settings 208
 - ICA browsing 75
 - ICA Client connections 191
 - ICA encryption 205
 - ICA network connections 117
 - IMA zones 179
 - MetaFrame XP servers and farms 157–189
 - mixed mode operation 93
 - network firewalls 81
 - ODBC drivers 110
 - ports 85
 - printer autocreation in NDS 70
 - shadowing 115
 - user access to applications 248
- Connection Control feature 266
- connection licenses 139, 143
- connections, controlling 266
- content 252
 - publishing 243–244, 258, 261
 - enhancements to 35
 - publishing to be opened on client 259
 - publishing to be opened on server 259
- content redirection 34, 243–244, 251
 - configuring 256
 - from client to server 251, 256
 - from server to client 257
- controlling
 - access to Citrix Management Console 163
 - client logons 265
- conventions, documentation 15
- counters, performance 288
- CPU priority for applications 262
- creating and applying 281

Ctxmlss command 329

D

- data collectors 179
 - election preference 180
 - response to UDP broadcasts 174
- data store
 - see* IMA data store 99
- data, refreshing 170
- dial-in account properties 199
- Dialin Information dialog box 199
- direct cable connections 200
- disconnecting ICA sessions 273
- DNS address resolution 80
- DNS and server names 44
- documentation 14, 128
 - Citrix NFuse Classic Administrator's Guide 14
 - conventions 15
 - Frequently Asked Questions 18
 - ICA Clients 16
 - MetaFrame XP 14
 - online help, using 16
 - online Product Documentation Library 17
 - submitting comments 18
- documents and files, publishing 258
- DOS-based printers 292
- downgrading a feature release 132
- drive mapping 210
- Drivers tab 297
- Dsmaint command 330

E

- Edit Connection dialog box 198, 200
- election of data collectors 180
- encryption, configuring 205
- explicit users 250
- extended characters in server names 44
- external IP addresses 313

F

- Feature Release 2 and Service Pack 2 125–133
- feature release level 132, 153
- feature releases 33
 - downgrading 132
 - features included in Feature Release 1 38
 - features included in Feature Release 2 33
 - upgrading to 125
- file type association 251

firewalls 52, 73, 75, 77, 81–83, 85
Frequently Asked Questions 18

G

global groups 63
grace period for licenses 144

H

hardware requirements 45
HTML files 255

I

IBM DB2

- creating an IMA data store 99
- migrating to 59
- requirements 58
- using DB2 for the data store 109

ICA (Independent Computing Architecture) 23

ICA Browser 86–87

ICA browsing 74–76, 78, 80–84, 86

ICA Client Creator 222

ICA Client Distribution wizard 119, 224

ICA Client Object 220

ICA Client Update Database 219

ICA Clients

- automatic client update 223
- automatic reconnection 276
- client printer auto-creation 306
- client printers 292
- Client Update Configuration utility 225
- Client Update Database 224
- client update process 224
- Components CD 219
- connection licenses 143
- connections, limiting 267
- deploying 215–240
- deploying from network shares 222
- deploying with diskettes 222
- deploying with NFuse Classic 238
- deployment methods 215–216
- deployment practices 236
- deployment scope 218
- documentation 14
- downloading 17
- features 23
- ICA Client Distribution wizard 119, 219, 224
- ICA Client Object 220
- ICA Client Update Database 219

- installation diskettes, creating 222
- installing using NFuse Classic 218
- logging activity 318
- logons to servers, controlling 265–266
- NDS logons 66
- pass-through ICA Client 219–220
- printer mapping 212
- Program Neighborhood Agent 217
- server location methods 77
- server response to broadcasts 78, 174
- shadowing 158
- SSL support 39
- time zone support 175
- updating 130, 223, 240
- Web-based installation 237
- with Citrix NFuse 217
- with Citrix NFuse Classic 237

ICA connections 191–213

- adding 193
- asynchronous 45, 194, 200
- audio mapping 213
- client device mapping 210
- COM port mapping 213
- drive mapping 210
- Edit Connection dialog box 198
- encryption 205
- modem callback options 198
- network connections 117
- null modem cables 198
- printer mapping 212
- restricting connections 205

ICA Display options 173

ICA files 255

ICA session monitoring 40, 288

ICA sessions 75, 191, 241, 270

- browsing configuration 75
- controlling logons 265
- disconnecting sessions 273
- encrypting 205
- monitoring session status 271
- performance monitoring 288
- published application data 271
- resetting sessions 274
- sending messages to users 274
- Session ID 272
- shadowing 158, 205, 284
- states of 272
- terminating processes 275

Icaport command 334

IMA 21–23, 85, 145, 174, 324

- changing the IMA port 335
- data collectors 179
- IMA service 71, 86, 138, 314
- zones 179
- IMA data store 309, 330
 - configuring during Setup 108
 - configuring ODBC drivers 110
 - connecting to 52
 - database choices 50
 - migrating to IBM DB2 59
 - migrating to Oracle 57
 - migrating to SQL Server 55
 - using IBM DB2 58, 99
 - using Microsoft Access 52
 - using Oracle 56, 99
 - using SQL Server 53, 99
- imaging MetaFrame XP servers 123
- Imaport command 335
- Independent Computing Architecture (ICA)
 - see* ICA
- Independent Management Architecture (IMA)
 - see* IMA
- installation
 - Citrix NFuse Classic 44, 117
 - common Windows Installer commands 103
 - configuring ODBC drivers 110
 - configuring the IMA data store 108
 - creating a log file 103
 - creating an answer file for unattended installation 105
 - creating Windows Installer transforms 104
 - Feature Release 2 and Service Pack 2 127
 - feature release level, setting 132
 - imaging MetaFrame XP servers 123
 - MetaFrame Setup properties explained 347
 - MetaFrame XP 99, 109, 122
 - product type 107
 - sample MetaFrame Setup transforms 352
 - shadowing restrictions 115
 - unattended Feature Release installation 130
 - unattended installation 104, 130
 - uninstalling MetaFrame XP 123
 - using Microsoft Access for the data store 108
 - using SQL, Oracle, or IBM DB2 for the data store 109
 - using the MetaFrame Windows Installer package 101
- Internet Information Services 44
- interoperability 86, 93
 - migrating MetaFrame 1.8 to MetaFrame XP 121
 - mixed mode 78
- IP addressing 80, 84, 313

- IP connectivity 21, 76–77, 81
- IP ports 31, 79, 85

J

- Java objects 117
- Java Run-Time Environment (JRE) 16, 46
- Java Virtual Machine (JVM) 44
- Jet database
 - see* Microsoft Access

L

- licensing 135–155
 - activation 144
 - adding feature release licenses 153
 - assigning licenses 149
 - connection licenses 139
 - feature release licensing 152
 - grace period 137, 144
 - license counts 150–151
 - license numbers 144, 146
 - machine codes 144
 - MetaFrame for UNIX connection licenses 96
 - migrating from other products 139
 - overview of 135
 - pooling license counts 95, 151
 - product codes 137, 140
 - product licenses 138, 143
 - serial numbers 142
 - upgrading licenses 140
 - viewing license information 154
- Load Manager 241
- local printers 292
- logons
 - controlling 265
 - reporting 318

M

- machine codes 144
- management tools 96, 157
- master ICA Browser 86–87
- messages, sending to users 274
- MetaFrame
 - Feature Release 2 127
 - MetaFrame XPa 27
 - MetaFrame XPe 28
 - MetaFrame XPs 24
 - overview of MetaFrame XP family of products 24
 - policies 281

- Service Pack 2 126
 - setup options 107
 - upgrading to feature releases 125
- MetaFrame 1.8 157
 - interoperability 86, 93
 - migrating to MetaFrame XP 121
- MetaFrame components
 - Citrix Secure Gateway 26
 - Citrix SSL Relay 27
 - Enterprise Services for NFuse 30
 - Installation Manager 30
 - Load Manager 27
 - Network Manager 29
 - NFuse Classic 26
 - Resource Manager 28
- MetaFrame for UNIX 96
- Microsoft Access 52
- Microsoft Internet Information Services 44
- Microsoft Systems Management Services (SMS) 221
- migrating licenses 139
- migrating MetaFrame 1.8 to MetaFrame XP 121
- migrating to MetaFrame XP 121
- mixed mode 78, 86, 93
 - server farm naming for 44
- modems 45
 - callback options 198
 - ICA connections with 198
- monitoring ICA sessions 271, 288
- moving a MetaFrame server to a different farm 324
- msiexec command 103

N

- names of servers and server farms 44
- native mode 93
 - Active Directory 61, 63
 - MetaFrame XP 77–78, 94–97
- NetWare drive mapping assignments 211
- network connections 117
- network firewalls 52, 73, 75, 77, 81–83, 85
- Network management plug-ins 127
- network management, SNMP 175
- network printers 292, 294, 299
- network protocols 76–77, 81
- New Connection dialog box 198
- NFuse Classic
 - see* Citrix NFuse Classic
- Novell Directory Service 66
- Novell ZENworks 71
- null modem cables, ICA connections with 198

O

- ODBC drivers, configuring 110
- online documentation 14
- Oracle
 - creating an IMA data store 99
 - migrating to 57
 - requirements 56
 - using Oracle for the data store 109

P

- parameter passing 254
- parameters
 - passing to published applications 254
- pass-through ICA Client 219, 246
- performance counters 288
- performance monitoring 288
- policies 281
 - about 35
 - configuring user-to-user shadowing with policies 286
 - creating a policy 282
 - prioritizing 283
- ports used by Citrix software 85
- print servers, importing 296
- printer drivers 300
 - managing 297
- printer management 291–304
 - client printer mapping 212
 - Drivers tab 297
 - importing print servers 296
 - installed printers 298
 - managing printer drivers 300
 - printer autcreation in NDS 70
 - replicating printer drivers 301
 - setting up network printers 299
 - user permissions 64
- printers
 - bandwidth consumption 297
 - Citrix Universal Print Driver 304
 - client 292–293
 - local 292
 - managing 291
 - network 292, 294, 299
 - printer drivers 300
 - shared 291
- Printers tab 298
- processes, terminating 275
- product codes 137, 140
- product licenses 143
- product type 107

- Program Neighborhood Agent 217
- protocols, networking 76–77, 81
- proxy servers 75
- Published Application Manager 97
- published content 252
- publishing applications 244–256
 - CPU prioritization 262
 - data on running applications 271
 - for access to Program Neighborhood 246
 - license usage 151
 - limiting application instances 267
 - pass-through ICA Client 246
 - procedures 250
 - publishing content 258
 - standard applications 241
 - user authentication 245
 - user permissions 64
- publishing applications and content 244
- publishing content 252, 258, 261

Q

- Query command 336

R

- reconnecting ICA Clients automatically 276
- redirecting application launching 34
- refreshing data in Citrix Management Console 169
- remote control
 - see* shadowing ICA sessions
- removing servers from server farms 123
- replicating printer drivers 301
- requirements
 - data store database 52
 - disk and memory 45
 - hardware 45
 - IBM DB2 58
 - Microsoft Access 52
 - Oracle 56
 - SQL Server 53
 - system sizing 47
 - system software 43
- Reset command 274
- resetting ICA sessions 274

S

- security
 - Secure Sockets Layer (SSL) 182
 - Transport Layer Security (TLS) 182

- sending messages to users 274
- serial numbers 142
- serial port mapping 213
- server certificate, SSL 183
- server location 75–84, 86
- server names, extended characters in 44
- server-based computing 19
- Service Pack 2 125–133
- Session ID 272
- sessions 191
 - see* ICA sessions
- setup
 - see* installation
- Shadow Taskbar 158, 284
- shadowing 115, 158, 205, 284
 - user-to-user shadowing 34, 286
- shared printers 291
- sizing systems for MetaFrame XP 47
- smart cards 34
 - software requirements 91
 - using SSCONFIG 91
 - using with MetaFrame 90
- SMS (Microsoft Systems Management Services) 221
- SNMP network management 175
- SNMP plug-ins 127
- Solution Knowledgebase 18
- SQL Server
 - creating an IMA data store 99
 - migrating to 55
 - requirements 53
 - using SQL for the data store 109
- SSCONFIG 91
- SSL
 - see* Citrix SSL Relay
- SSL encryption 183
- states of ICA sessions 272
- system requirements
 - see* requirements

T

- TCP ports 85
 - SSL relay (443) 182
 - XML Service (80) 117
- TCP/IP Network Protocol 77
- TCP/IP+HTTP Network Protocol 76
- terminating processes 275
- time zone support 175
- TLS 182
- tools and utilities 96, 157, 159

transforms 352
 Transport Layer Security (TLS) 182
 Twconfig command 345

U

UDP broadcasts 77, 174
 unattended installation 104, 130
 creating an answer file 105
 creating Windows Installer transforms 104
 uninstalling MetaFrame XP 123
 universal groups 63
 universal printer driver 304
 updating ICA Clients 223, 240
 upgrading MetaFrame 1.8 to MetaFrame XP 121
 user account properties 199
 user authentication 61–62, 65–66, 71–72, 99, 111, 237, 245, 276, 280
 user groups 249
 user permissions 64
 user policies 35, 281
 creating a policy 282
 prioritizing 283
 User Properties dialog box 199
 user-to-user shadowing 286
 utilities 309–347

V

virtual printers 291

W

Web-based ICA Client installation 237
 WinCE 292
 Windows 2000 17
 Windows Installer
 common commands 103
 creating a log file when installing MetaFrame 103
 creating transforms 104, 347
 installing MetaFrame using the Windows Installer package 101
 msiexec command 103, 106, 131
 Windows Installer packages 221
 Windows Installer transforms 347
 sample MetaFrame Setup transforms 352
 Windows NT 4 17

X

XML
 Citrix XML Service 79, 117
 data 77
 XML Service 329

Z

ZENworks Dynamic Local Users 71
 zones 179
 see IMA zones

