

### Citrix CCA MetaFrame Presentation Server 3.0 and 4.0 Exam Cram™ (Exams 223 and 256)

By Todd Mathers, Elias Khnaser

Publisher: Que

Pub Date: December 21, 2005

Print ISBN-10: 0-7897-3246-7

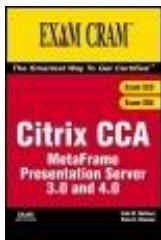
Print ISBN-13: 978-0-7897-3246-0

Pages: 672

[Table of Contents](#) | [Index](#)

## Overview

If you are studying for the Citrix CCA exam, the *Citrix CCA MetaFrame Presentation Server 3.0/4.0 Exams 223/256 Exam Cram* is your smartest, most efficient way to study and get certified. Your time to study is limited, so spend it with the best. This study guide provides you with a concise review of the new features for the MetaFrame XP Presentation Server, Feature Release 3, and it clearly maps your exam objectives for easier, more efficient studying. An accompanying CD includes a fully customizable test engine with questions, answer keys and detailed score reports. You'll also receive a Cram Sheet tear-out card that is perfect for last-minute studying. For a concise study guide that strictly focuses on exam objectives, choose *Citrix CCA MetaFrame Presentation Server 3.0/4.0 Exams 223/256 Exam Cram*.



## Citrix CCA MetaFrame Presentation Server 3.0 and 4.0 Exam Cram™ (Exams 223 and 256)

By Todd Mathers, Elias Khnaser

Publisher: Que

Pub Date: December 21, 2005

Print ISBN-10: 0-7897-3246-7

Print ISBN-13: 978-0-7897-3246-0

Pages: 672

[Table of Contents](#) | [Index](#)

[Copyright](#)

[About the Authors](#)

[About the Contributing Author](#)

[Acknowledgments](#)

[We Want to Hear from You!](#)

[Introduction](#)

[The Citrix Certification Program](#)

[Taking a Citrix Certification Exam](#)

[Tracking Your Citrix Certification](#)

[How to Prepare for the Exam](#)

[About This Book](#)

[How to Use This Book](#)

[Self-Assessment](#)

[CCA in the Real World](#)

[Chapter 1. Introducing Citrix MetaFrame Presentation Server 3.0, Enterprise Edition](#)

[Introduction](#)

[The Components of MetaFrame Presentation Server 3.0, Enterprise Edition](#)

[Exam Prep Questions](#)

[Need to Know More?](#)

[Chapter 2. MetaFrame Presentation Server Architecture](#)

[Independent Computing Architecture](#)

[MultiWin](#)

[SpeedScreen Technology](#)

[Independent Management Architecture](#)

[Exam Prep Questions](#)

[Chapter 3. Installation Prerequisites for MetaFrame Presentation Server 3.0](#)

[Licensing Requirements](#)

[Server Software Requirements](#)

[Server Hardware Sizing](#)

[Management Console Requirements](#)

[Firewall Configuration](#)

[MetaFrame Data Store Requirements](#)

[Server Farm Distribution and Availability](#)

[Exam Prep Questions](#)

[Chapter 4. Installing and Managing MetaFrame Access Suite Licensing](#)

[MetaFrame Access Suite License Architecture](#)

- [Installing MetaFrame Access Suite Licensing](#)
- [Managing MetaFrame Access Suite Licensing](#)
- [Exam Prep Questions](#)
- [Chapter 5. Installing MetaFrame Presentation Server 3.0](#)
  - [Remapping Server Drive Letters](#)
  - [Standard MetaFrame Presentation Server 3.0 Installation](#)
  - [MetaFrame 1.8 Server Migration to MPS](#)
  - [Unattended MPS Installation Support](#)
  - [Uninstalling MetaFrame Presentation Server 3.0](#)
  - [Exam Prep Questions](#)
  - [Need to Know More?](#)
- [Chapter 6. Configuring and Administering MetaFrame Presentation Servers](#)
  - [Components of the Management Console](#)
  - [Administering MetaFrame Using the Management Console](#)
  - [Using the Shadow Taskbar](#)
  - [Connection Management Using Citrix Connection Configuration](#)
  - [SpeedScreen Latency Reduction Manager](#)
  - [Exam Prep Questions](#)
- [Chapter 7. MetaFrame Presentation Server Policy Management](#)
  - [What Are MetaFrame User Policies?](#)
  - [Policy Priority](#)
  - [Policy Filtering and Assignment](#)
  - [Available MetaFrame Policy Rules](#)
  - [Creating a User Policy](#)
  - [Determining the Resultant Set of Policies](#)
  - [Exam Prep Questions](#)
  - [Need to Know More?](#)
- [Chapter 8. Citrix Load Management](#)
  - [Overview of Citrix Load Management](#)
  - [Load Evaluators and Rules](#)
    - [Rules](#)
    - [Creating a New Load Evaluator](#)
    - [Assigning a Load Evaluator](#)
    - [Editing and Deleting a Load Evaluator](#)
    - [Copying a Load Evaluator](#)
    - [Using Load Manager](#)
  - [Exam Prep Questions](#)
- [Chapter 9. MetaFrame Security](#)
  - [Administrative Delegation](#)
  - [MetaFrame Access Security](#)
  - [Exam Prep Questions](#)
- [Chapter 10. Application Integration](#)
  - [Preparing a Server for Application Installation](#)
  - [Application Compatibility Scripts](#)
  - [Performing an Application Installation](#)
  - [Delivering the Application to the User](#)
  - [Published Application Properties](#)
  - [Installation Manager](#)
  - [Exam Prep Questions](#)
- [Chapter 11. Deploying Applications Using Installation Manager](#)

- [Components of Installation Manager](#)
- [Installing and Configuring Installation Manager](#)
- [Application Deployment Using Installation Manager](#)
- [Creating ADF Packages Using the Packager Utility](#)
- [Exam Prep Questions](#)
- [Chapter 12. Printing](#)
  - [Supported Printer Types](#)
  - [Printer Management Features in MetaFrame](#)
  - [Printer Driver Management](#)
  - [Printer Configuration](#)
  - [Exam Prep Questions](#)
- [Chapter 13. Citrix ICA Session and Client Configuration](#)
  - [ICA Client Types](#)
  - [The Win32 Presentation Server Client](#)
  - [Win32 Client Features](#)
  - [Program Neighborhood Client Configuration](#)
  - [Program Neighborhood Agent Client Configuration](#)
  - [Web Client Configuration](#)
  - [Server-side ICA Connection and Session Configuration](#)
  - [Exam Prep Questions](#)
- [Chapter 14. Web Access to the MetaFrame Server Farm](#)
  - [The Web Interface 3.0 Feature Summary](#)
  - [Web Interface Installation Requirements](#)
  - [Installing the Web Interface](#)
  - [Configuring the Web Interface](#)
  - [Securing the Web Interface](#)
  - [Program Neighborhood Agent Console](#)
  - [Securing Server Access with the Secure Gateway](#)
  - [Exam Prep Questions](#)
- [Chapter 15. Managing and Monitoring Using Resource Manager](#)
  - [Resource Manager Overview](#)
  - [Resource Manager Components](#)
  - [Resource Manager Installation](#)
  - [Using Resource Manager](#)
  - [Exam Prep Questions](#)
- [Chapter 16. What's New in MetaFrame Presentation Server 4.0](#)
  - [MetaFrame Presentation Server Architecture](#)
  - [Installation Prerequisites](#)
  - [MetaFrame Access Suite Licensing](#)
  - [Installing MetaFrame Presentation Server](#)
  - [Configuring and Administering MetaFrame Presentation Server](#)
  - [MetaFrame Presentation Server Policy Management](#)
  - [MetaFrame Security](#)
  - [Application Integration](#)
  - [Deploying Applications Using Installation Manager](#)
  - [Printing](#)
  - [Citrix ICA Client Configuration](#)
  - [Web Connectivity to the MetaFrame Server Farm](#)
  - [Exam Prep Questions](#)
- [Chapter 17. Practice Exam 1](#)

- [Practice Exam](#)
- [Chapter 18. Answer Key 1](#)
- [Answer Key](#)
- [Chapter 19. Practice Exam 2](#)
- [Practice Exam](#)
- [Chapter 20. Answer Key 2](#)
- [Answer Key](#)
- [Appendix A. CD Contents and Installation Instructions](#)
  - [Multiple Test Modes](#)
  - [Question Types](#)
  - [Random Questions and Order of Answers](#)
  - [Detailed Explanations of Correct and Incorrect Answers](#)
  - [Attention to Exam Objectives](#)
  - [Installing the CD](#)
  - [Technical Support](#)
- [Appendix B. Need to Know More?](#)
  - [Chapter 1](#)
  - [Chapter 2](#)
  - [Chapter 3](#)
  - [Chapter 4](#)
  - [Chapter 5](#)
  - [Chapter 6](#)
  - [Chapter 7](#)
  - [Chapter 8](#)
  - [Chapter 9](#)
  - [Chapter 10](#)
  - [Chapter 11](#)
  - [Chapter 12](#)
  - [Chapter 13](#)
  - [Chapter 14](#)
  - [Chapter 15](#)
  - [Chapter 16](#)
- [Glossary](#)
- [Index](#)

 PREV

NEXT 

# Copyright

Citrix CCA MetaFrame Presentation Server 3.0 and 4.0 Exam Cram

Copyright © 2006 by Que Certification

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

International Standard Book Number: 0-7897-3246-7

Library of Congress Catalog Card Number: 2004108925

Printed in the United States of America

First Printing: December 2005

08 07 06 05 4 3 2 1

## Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

## Bulk Sales

Que Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

[corpsales@pearsontechgroup.com](mailto:corpsales@pearsontechgroup.com)

For sales outside the U.S., please contact

International Sales

[international@pearsoned.com](mailto:international@pearsoned.com)

Publisher Paul Boger

Executive Editor Jeff Riley

Acquisitions Editor Carol Ackerman

Development Editor Sean Dixon

Managing Editor Charlotte Clapp

Project Editor Seth Kerney

Copy Editor Chuck Hutchinson

Indexer Chris Barrick

Proofreader Juli Cook

Technical Editors Chris Walter Ben Klockner

Publishing Coordinator Vanessa Evans

Multimedia Developer Dan Scherf

Interior Designer Gary Adair

Cover Designer Anne Jones

## Dedication

*This book is dedicated to the loving memory of Valarie Moore, Katharina Hoffman, and my grandparents, William and Eugenie Duff. My life is better for having known you all. Love always.*

*Todd*

*To Didi, "Habibi": I never thought that I could love someone as much as I love you. I never thought that I could need someone as much as I need you. Girl, your smile lights up the sky! Thank you for your support and your love that inspired me and inspires me still to always outdo myself. I love you. "Bhibbik bibi"*

*Elias*

 PREV

NEXT 

# About the Authors

Todd W. Mathers, founder and lead consultant for Noisy River Software Corporation, has spent nearly 10 years specializing in the implementation of server-based computing solutions and the development of custom software for Microsoft Terminal Server and Citrix Presentation Server environments. A graduate of the University of Waterloo with an Honors Bachelor's degree in Mathematics, Todd certainly didn't imagine that his career would include being an author. But since 1998, he has written four books on the subject of Terminal Server and MetaFrame. If not buried in work (most likely), driving in the country with his lovely Linda (not often enough), or enjoying a great Canadian winter, he can be reached at [todd.mathers@noisyriver.com](mailto:todd.mathers@noisyriver.com).

Elias N. Khnaser (CCEA, MCSE, CCNA) is the server-based computing architect for General Growth Properties in Chicago, the second largest shopping mall owner and operator in the world. Elias's current focus is on server-based computing, primarily Citrix and Microsoft technologies. Elias is a contributing author at *Windows & .NET Magazine*, [Techrepublic.com](http://Techrepublic.com), [Certcities.com](http://Certcities.com), and [BrainBuzz.com](http://BrainBuzz.com). He is also the Citrix series trainer at [CBTNuggets.com](http://CBTNuggets.com). Elias's publications include *Configuring Citrix MetaFrame XP 1.0 for Windows Including Feature Release 1* (Syngress Media), *MCSE Designing Security for a Windows Server 2003 Network: Exam 70-298 Study Guide and DVD Training System* (Syngress Media), *CBTCitrix MetaFrame XP CCA Certification Package* ([CBTNuggets.com](http://CBTNuggets.com)), and *MetaFrame XP for Windows Admin Study Guide* ([BrainBuzz.com](http://BrainBuzz.com)[Cramsession.com](http://Cramsession.com)). He also has been profiled in several IT publications, including *Windows & .NET Magazine*, [CBTNuggets.com](http://CBTNuggets.com), [Techrepublic.com](http://Techrepublic.com), and [Certcities.com](http://Certcities.com).

[◀ PREV](#)[NEXT ▶](#)

# About the Contributing Author

Suzanne Sage London is a technologist, an expert in enterprise-class server applications, and an author who writes about social trends in technology, new media, and urban lifestyles. As a consultant, London has helped Fortune 500 fast companies and startups both in Silicon Valley and nationwide to spot trends and leverage new technologies for competitive advantage. London specializes in startups for web media and marketing, content portals, and ASPs.

[◀ PREV](#)[NEXT ▶](#)

# Acknowledgments

No book would ever come to fruition without the incredible work done by everyone behind the scenes, and as such, we must extend a huge "thank you" to all the people at Que for their amazing work. To Carol Ackerman, acquisitions editor extraordinaire, thank you so much for your persistence and your patience. We're very thankful to have had you on this project (honestly, it's true! :-)). You're a pleasure to work with and most certainly the main reason this book exists today. To Sean Dixon, Chuck Hutchinson and Seth Kerney: Thanks to you guys for correcting our shoddy grammar, pointing out the obvious mistakes, and tirelessly ensuring that we're actually saying what we think we're saying. Special thanks to all the production staff who silently (at least silently from our perspective) work to put everything together. As always, it looks fantastic! And finally, thanks to the great work of our technical editors, Ben Klockner and Chris Walter, who provided excellent insight, suggestions, and corrections to our work. Of course, any errors or omissions are strictly our doing. These guys can't be expected to find everything. :-)

And thanks to the friends and family who had to once again endure the pressures and pains of book writing. They'll get used to it someday. . . .

Happy reading and good luck!!

*Todd W. Mathers & Elias N. Khnaser*

# We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an executive editor for Que Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book as well as what we can do to make our books better.

*Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.*

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: [feedback@quepublishing.com](mailto:feedback@quepublishing.com)

Mail: Jeff Riley

Executive Editor

Que Certification

800 East 96th Street

Indianapolis, IN 46240 USA

For more information about this book or another Que Certification title, visit our website at [www.examcram.com](http://www.examcram.com). Type the ISBN (excluding hyphens) or the title of a book in the Search field to find the page you're looking for.

# Introduction

Welcome to *Citrix MetaFrame Presentation Server 3.0: Enterprise Edition Administration Exam Cram*. In this book, you will find information to help ensure success in your Citrix certification endeavors. Specifically, our goal is to aid you in preparing for and passing the Citrix certification exam titled Citrix MetaFrame Presentation Server 3.0: Enterprise Edition Administration (Exam 223). Here, we provide a general overview of Citrix's certification program and discuss how this *Exam Cram 2* book can help you to prepare for whatever Citrix certification path you want to travel.

This book, as with other *Exam Cram* books, is targeted specifically at test preparation and review. It does not attempt to teach you everything there is to know about a topic, but instead looks to present and review the material that you're likely to encounter on the test. As authors, we aim to present to you as much of this relevant information as possible so that you can prepare and take this exam with confidence.

Before you dive head-first into the information provided, we recommend that you begin by taking the self-assessment that immediately follows this introduction. This self-assessment will help you evaluate your knowledge of the Citrix material both in the real world and under ideal exam circumstances.

Based on the results of the self-assessment, you may feel that some additional education is necessary. Numerous resources are available, including

- Official Citrix-authorized classroom training. Exam CTX-1223AI is the official course for exam 223.
- Citrix product documentation and additional technical publications, all of which are available free of charge on the Citrix website (<http://www.citrix.com>).
- Other study or technical publications available in print or on the Internet.

We also recommend that you visit [www.examcram2.com](http://www.examcram2.com) to receive additional practice questions and advice regarding this Citrix exam.

Book learning alone will not guarantee success on the exam. We strongly recommend that you take the time to install, configure, and try out the various MetaFrame Presentation Server components covered on the exam. Even if you have some basic experience with this or previous versions of MetaFrame, hands-on learning, coupled with the right educational material, will go a long way to ensuring not only your practical exam success, but success in real-world environments as well.

# The Citrix Certification Program

Citrix currently provides five educational tracks: the Citrix Certified Administrator (CCA), the Citrix Certified Enterprise Administrator (CCEA), the Citrix Certified Integration Architect (CCIA), the Citrix Certified Instructor (CCI), and the Citrix Certified Sales Professional (CCSP). Before discussing the specific requirements for each of these certifications, we begin with a brief review of the general requirements for an exam and the way Citrix manages the discontinuation and eventual retirement of legacy certification exams. Understanding these points can help you to plan your certification course appropriately.

## Alternate, Discontinued, and Retired Exams

Each Citrix certification has one or more core exams that you must successfully pass to attain the desired certification. As new versions of the Citrix software become available, these core exams are updated and supersede previous exam versions. When this happens, the older exams are still considered as alternates for certification for a limited time. All Citrix exams go through the following life cycle:

- Release The exam is initially released and available as part of a particular certification track.
- Discontinued When an exam is discontinued, it is no longer available to be taken. It is still considered a valid qualification toward a certification track for those people who have already taken the exam.
- Retired After an exam has been retired, it no longer qualifies toward Citrix certification. To maintain certification status, you must take one or more updated exams that meet the qualifications for the certification track.

In general, it is recommended that you take the most current exam even if available alternates currently meet core requirements for certification. These alternate exams are often scheduled to be discontinued in the near future and likely will be retired well before the most current exam.

You can view the current list of release, discontinued, and retirement dates for all exams on the Citrix website at

<http://www.citrix.com/site/resources/content/education/CitrixEducationExamSchedule.pdf>

The main Citrix web page for certification can be found on its main education home page at

<http://www.citrix.com/site/ss/training/index.asp>

You can find the most current exam information here, and we highly recommend that you review this site before planning on the exams that you will take for your certification.

## Citrix Certification Tracks

The five certification tracks currently available are as follows:

- **CCA (Citrix Certified Administrator)** The CCA certification is the designation given to someone who has passed one of the core MetaFrame Presentation Server exams and is the foundation for other technical Citrix certifications. A CCA is recognized as having a thorough knowledge of Citrix MetaFrame Presentation Server (either Windows or Unix).

To attain the CCA designation, you must pass either exam 310, Citrix MetaFrame 1.0 for Unix, or exam 223 (discussed in this book). Passing one of the following courses is currently a suitable alternative:

- Exam 222Citrix MetaFrame XP Presentation Server, Feature Release 3: Administration. This exam is available in English, German, French, and Japanese.
- Exam 221Citrix MetaFrame XP Feature Release 2. This exam has been discontinued and can no longer be taken. People who have passed this exam can still count it toward the CCA designation.
- Exam 220Citrix MetaFrame XP 1.0 Administrator. This exam is available in French, German, Japanese, and Spanish only. The English version of this exam has been discontinued and can no longer be taken. People who have passed this exam can still count it toward the CCA designation.

At the time of this writing, no retirement dates had yet been set for these exams, although as of January 15, 2005, exam 218, Citrix MetaFrame 1.8, is retired. This exam was previously a suitable alternate for the CCA certification.

In addition to passing the core exam, you must also participate in one of the following two online eLearning courses and pass the assessment given at the conclusion of the course. The available courses are CTX-1300BW Citrix MetaFrame Secure Access Manager 2.2: Introduction or CTX-1320BW Citrix MetaFrame Password Manager 2.5: Introduction. Alternate eLearning courses that also are available can be substituted for these two courses if desired.

- **CCEA (Citrix Certified Enterprise Administrator)** The CCEA is an advanced certification specifically for those individuals who will be responsible for deploying and managing an environment consisting of one or more Citrix MetaFrame Access Suite products. To meet the requirements of this certification, you are required to successfully pass the following four core exams:

- Exam 223 or one of the suitable alternates (220, 221, or 222). This is the same requirement to qualify for the CCA certification. Note that exam 310, Citrix MetaFrame 1.0 for Unix, does not qualify toward the CCEA designation.
- Exam 913 Citrix MetaFrame XP Presentation Server, Enterprise Edition, Feature Release 3: Administration. This exam is the equivalent exam discussed in this book but targeted at MetaFrame XP, not MetaFrame Presentation Server 3.0. The English versions of the alternate exams 910 or 911 and 920 or 921 have all been discontinued, and retirement dates for 910 and 920 are set for January 15, 2005.
- Exam 962 Citrix MetaFrame XP: Securing and Deploying Applications Over the Web. The alternate exams for 962 are 930 or 931 and 950, 951, or 961. They have all been discontinued, with 930 scheduled for retirement on January 15, 2005.
- Exam 992 Citrix MetaFrame XP Presentation Server, Feature Release 3: Deployment and Support. The one alternate exam, 991, has been discontinued, but no retirement date has been set as of yet.

As of this writing, Citrix had not yet completed the introduction of equivalent MetaFrame Presentation Server 3.0 exams for all of the core CCEA exams. Check the Citrix website prior to booking an exam to ensure a more up-to-date exam has not been made available.

In addition to the four core exams, one of two elective tracks must also be completed:

- Track 1Pertains to the MetaFrame Secure Access Manager and requires that you pass the eLearning course CTX-1300BW Citrix MetaFrame Secure Access Manager 2.2: Introduction and exam 722 Citrix MetaFrame Secure Access Manager 2.2: Administration. Allowable alternatives to exam 722 are exams 720, 721, or 723.
- Track 2Focuses on MetaFrame Password Manager and requires that you pass the eLearning course CTX-1320BW Citrix MetaFrame Password Manager 2.5: Introduction and exam 973 Citrix MetaFrame Password Manager 2.5: Administration. The previous exam 972 is an acceptable alternate and has not yet been discontinued.

After you complete the core required exams and the chosen elective track, the final step to attain the CCEA certification is to accept the terms of the CCEA certification agreement.

- CCIA (Citrix Certified Integration Architect) The CCIA certification has been designed to teach would-be architects the best practices recommended by Citrix for analyzing, designing, and testing Citrix-based implementations. Whereas the CCEA focuses on the actual implementation and support of the MetaFrame Access Suite, the CCIA narrows in on the planning and preparation that are so critical to a successful MetaFrame Access Suite implementation. Proper planning ensures that deployment costs and implementation time are reduced while ensuring that the deployment as a whole is successful and meets the expectations of the target users.

The CCIA certification requires that you pass the following three core exams:

- Exam 223 or one of the suitable alternates (220, 221, or 222). This is the same requirement to qualify for the CCA certification and as part of the core CCEA certification. Note that exam 310, Citrix MetaFrame 1.0 for Unix, does not qualify toward the CCIA designation.
- Exam 610 Citrix Core Technologies and Architecture. No alternate exam exists as a substitute for this exam.
- Exam 611 Citrix Design, Integration, and Methodology. No alternate exam exists for this exam either.

Unlike other Citrix certifications, the CCIA designation also requires that you pass one Microsoft design exam from the following six exams:

- Exam 70-219: Designing a Microsoft Windows 2000 Directory Services Infrastructure
- Exam 70-220: Designing Security for a Microsoft 2000 Network
- Exam 70-221: Designing a Microsoft Windows 2000 Network Infrastructure
- Exam 70-226: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure
- Exam 70-298: Designing Security for a Microsoft Windows Server 2003 Network

After you meet the preceding requirements, you must accept the terms of the CCIA certification

agreement before you can participate in the final exam, 612 Citrix Certified Integration Architect Lab, a combination of written and hands-on work that you must pass to achieve the CCIA designation.

To date, the CCIA designation is certainly one of the most rigorous of the Citrix certifications.

- CCI (Citrix Certified Instructor) If your desire is to become a Citrix MetaFrame Access Suite instructor and teach at a Citrix Authorized Learning Center (CALC), you must acquire the CCI designation. To achieve this certification, you must meet the following requirements:
  - Attain the CCEA designation. Depending on your location, you either are required to have this certification prior to becoming a CCI or within six months of achieving the CCI designation.
  - Have certification as a Microsoft Certified Trainer (MCT), Certified Novell Instructor (CNI), or CompTIA Certified Technical Trainer+ (CTT+). Alternate instructional training exams may also be accepted, so you should contact the Citrix CCI representative from your region for full details.
  - Achieve a minimum of Microsoft Certified Professional (MCP) status for Windows 2000 Server or Windows Server 2003.
  - Complete the Citrix Train the Trainer course.
  - Complete the CCI application form (downloadable as a PDF file from the Citrix website at <http://www.citrix.com/site/resources/dynamic/ctracks/CCIAApplication.pdf>) and provide a signed copy of the CCI agreement.

As would be expected, the requirements for the CCI designation are very in-depth and require dedication if you are seeking this status.

- CCSP (Citrix Certified Sales Professional) The final Citrix certification, the CCSP designation, is the only certification offering that does not require passing the Citrix 223 (or equivalent) exam. The CCSP designation is specifically targeted at sales professionals who want to expand their sales into the Citrix suite of products. Successful CCSP candidates must have a thorough overview of the basic product suite, understanding the key features delivered by each product. CCSP designation requires passing all of the following exams:

- CTX-1601BW Citrix Access Infrastructure: Strategies and Solutions
- CTX-1602BW Selling Citrix Products and Services
- CTX-1603BW Citrix MetaFrame Access Suite 3.0: Selling and Positioning
- CTX-1604AW Citrix Access Infrastructure: Total Cost of Ownership and Return on Investment
- CTX-1605AW Citrix Access Infrastructure: Networking Concepts

In addition to these courses, any two eLearning courses from the following five must also be passed:

- CTX-1250AW Citrix MetaFrame Presentation Server 3.0: Selling and Positioning
- CTX-1242AW Citrix MetaFrame Presentation Server 1.2 for Unix: Selling and Positioning

- CTX-1302BW Citrix MetaFrame Secure Access Manager 2.2: Selling and Positioning
- CTX-1322BW Citrix MetaFrame Password Manager 2.5: Selling and Positioning
- CTX-1333AW Citrix MetaFrame Conferencing Manager 3.0: Selling and Positioning

As mentioned near the beginning of this section, the best place to keep tabs on the Citrix certification program is via the Citrix website and the training home page, found at the following URL:

<http://www.citrix.com/site/ss/training/index.asp>

 PREV

NEXT 

# Taking a Citrix Certification Exam

After you complete your preparations for the exam and are ready to actually take the test, you need to register at an authorized Citrix testing center in your area. All Citrix exams are administered by Thomson Prometric. You can register online for a Citrix exam at <http://www.prometric.com> or by calling 1-800-481-EXAM (1-800-481-3926) in Canada or the United States. Outside the United States and Canada, you can call the regional Prometric offices at +1-443-751-4300. These offices cannot schedule exams, but they can assist in locating a Prometric training center in your area. Web-based registration is the quickest and most convenient way of scheduling your Citrix certification exam.

Each Citrix exam typically costs \$100 (US) and must be booked a minimum of 24 hours prior and no more than eight weeks in advance. Cancellation charges may apply if you do not give adequate notice. Typically, notice is a minimum of 24 hours prior to the scheduled start of the exam. You can cancel online or by contacting the testing center directly.

When scheduling a test, you need to provide the appropriate personal identification to verify who you are, the name and number of the exam that you will be taking, and a method of payment. Online registration requires that you create a personal user account that can then be used to book all future exams. On the day of the exam, you must provide appropriate identification to verify who you are. Typically, two forms of identification are required, with at least one of them being a photo ID.

Plan to arrive at the exam location at least 1520 minutes early so that you can get seated, relax, and prepare prior to the start of the exam. All Citrix exams are completely closed book. No study aids or anything else for that matter are permitted into the testing area. This includes coats, bags, or purses, all of which must be left with the test administrator before entering the room. The best advice is to leave these items at home or locked in the car. The fewer distractions that you bring with you, the better focused you can be on the exam itself.

In the test room, the test administrator logs you in to your exam, verifying that your user ID and exam number are correct. After you review the introduction information, the exam begins.

The 223 Citrix certification exam has 79 questions, and native English speakers have 105 minutes to complete the exam. Non-native English speakers have an additional 30 minutes (135 minutes in total) to complete the exam. The testing software itself is Windows-based and presents a single question per screen. In the upper-right corner, a display shows the time and number of questions remaining.

Specific questions are typically a variant of the multiple-choice format, and the relative difficulty varies from question to question. The specific question usually falls into one of three categories:

- Select the correct answer With these typical multiple-choice questions, you are asked to choose the one correct response that most appropriately answers the given question. In some situations, different answers may be correct under slightly different server configurations, so make sure that you read the question carefully before selecting your answer.

You will not find traditional true/false questions on a Citrix exam. Instead true/false-type questions are posed as multiple-choice questions, asking you to select the truthful (or most truthful) statement from the list of statements provided.

- Select all that apply (or don't apply) These types of questions ask you to select all of the answers listed that correctly apply to the question given. None to all of them may apply, so be sure to read these types of questions very carefully. In many cases, subtle wording has been

purposely used to trip up those who aren't paying attention. Partial credit is not given for these types of questions. Unless only the correct answers are given, you receive no credit for the question.

- Complete the sentence or fill in the blank These types of questions ask you to complete the sentence with the appropriate word or words. The correct answer is most often chosen from a list of different words in multiple-choice format.

When your test is scored, no added penalty is given for a wrong answer compared to giving no answer at all, so answering every question asked is worthwhile even if you are not sure of some and must guess. To the best of its ability, Citrix has attempted to make the questions as fair as possible and to ensure that all questions have a single correct answer. Of course, mistakes do happen, and a "poor" question may find its way onto your test, presenting you with a poorly worded or ambiguous question that may not have a clearly correct answer.

In this situation, the best course of action is to answer the question to the best of your ability and try to follow up afterward in an attempt to determine what the correct answer actually should be. You are not allowed to leave the exam area with any written information, so you cannot write down the question for review later. You can attempt to remember the question and follow up afterward to determine the correct answer. Clearly ambiguous or incorrect questions can be reported to Citrix, which can correct the problem for future exams. Do not expect to have a test score reversed or corrected based on the results of a single question. If you have properly prepared for the exam, a single question should have no bearing on whether you pass or fail.

After you complete the exam, the testing software responds with your score after a few seconds, and informs you whether you have passed or failed. The 223 exam requires a minimum score of 67%, or 53 correct out of 79, to pass the exam.

If you don't pass the exam, the key thing is not to become discouraged. We have all had days when things just didn't quite go as well as we had hoped. Take some time after the exam to review areas where you struggled during the exam. Maybe a particular area caught you by surprise, or you felt you had a stronger handle on it than you actually did. The best method in this situation is to return as soon as possible to the study process and brush up on the weak areas in preparation for another exam attempt.

You can reschedule a new test through Prometric as soon as available if you so desire. We recommend that you attempt to schedule time in sooner rather than later so that material you have already studied is still fresh in your mind. You are required to pay the full fee to take another test, but there is no penalty with regards to certification for retaking an exam more than once.

 PREV

NEXT 

# Tracking Your Citrix Certification

After you pass your first Citrix certification exam, you are given access to Citrix's online tool for tracking certification information. You can find the website to track this information at <http://www.certmanager.net/citrix>. This website is also referred to as the I7 (the letter J) Certification Management site. All successfully passed exams automatically appear on this site, allowing you to track your progress toward certification.

## Note

After you pass an exam, it typically takes four business days before the exam results appear within your personal I7 Certification Management profile.

To create a logon to this site, you are required to provide information found on the Citrix exam score report that you receive after successfully completing a Citrix certification exam. With this information, you can create your logon for the site and begin tracking your Citrix certification progress.

You can also view the remaining requirements to attain a particular certification using the online Certification Wizard ([http://www.citrix.com/site/SS/cert\\_reqmt/cert\\_reqmt\\_tool-1.asp](http://www.citrix.com/site/SS/cert_reqmt/cert_reqmt_tool-1.asp)). This simple wizard-driven site allows you to provide information on the exams that you have passed and determine the requirements that you must attain to achieve your certification goal.

# How to Prepare for the Exam

Preparing for Citrix exam 223, as with any technical exam, requires that you dedicate time to both acquiring and studying information directly related to the 223 exam material. To successfully pass this exam, you are expected to have an intimate knowledge of the full spectrum of core features and functionality that make up the MetaFrame Presentation Server 3.0 product. For those readers with past MetaFrame experience but no formal training, you may be surprised, even initially overwhelmed, by the amount of material that must be reviewed to completely cover the scope of the 223 exam. Don't let the depth of material concern you. A practical approach to studying and reviewing this information will go a long way to preparing you for this exam.

## Note

You need to dedicate a fairly large amount of time to studying the information necessary to prepare for this exam. Therefore, if you review everything the night or even the weekend before, don't expect to be too successful in your certification test.

The following is a general list of materials that can help you in your 223 exam preparations:

- The MetaFrame Presentation Server 3.0 Enterprise Edition installation media package. This multiple-CD package contains both online documentation and the application software necessary to install and test the various aspects of MPS 3.0 in preparation for the exam. Various means exist for obtaining this software package. One avenue is through your nearest authorized Citrix reseller, a Citrix sales rep, or as a result of attending a Citrix course associated with this exam.
- Exam preparation materials available directly from Citrix. Citrix provides very little in the way of exam-specific information on its website beyond the basic exam enablement guides. Citrix does provide detailed technical documentation available both on the MPS 3.0 installation media and on its website that is vital to ensuring you have the knowledge necessary to pass the 223 exam. Specifically, you should review the following two publications in detail:
  - *MetaFrame Presentation Server 3.0 for Windows Administrator's Guide*
  - *MetaFrame Access Suite Licensing Guide*
- This *Exam Cram* book, which provides you with a concise and thorough review of the material considered vital to your exam-taking success. This book serves as a supplement to the basic study material that you'll review to ensure that you have a clear understanding of the key topics and are prepared for any pitfalls the 223 exam process may throw at you.
- Official Citrix-authorized classroom training. Citrix offers an intense five-day course (CTX-1223AI) geared specifically at individuals who are interested in passing the 223 exam on route to a CCA, CCEA, or CCIA designation.

- Citrix self-study courseware. Citrix now provides access to its classroom courseware material for those people who prefer self-study to a classroom environment. Courseware is available for sale through most Citrix Authorized Training Centers.
- Additional exam preparation materials such as practice exams, available on the *Exam Cram* website at <http://www.examcram.com>.

 PREV

NEXT 

# About This Book

Each chapter in this book follows the traditional *Exam Cram* structure, containing graphical cues that flag important or useful exam information. Here is the layout of a typical chapter:

- **Opening hotlists** At the beginning of each chapter is a list of the terms you need to understand and the techniques you need to master to thoroughly understand the subject matter of the chapter. Following the hotlist is a brief introduction to the chapter that prepares you for the following material.
- **Topic breakdown** Following the opening hotlists and introduction is a series of topics that break down the chapter's subject material into manageable chunks of information. Throughout the chapters, we highlight important information that is likely to appear on an exam. This information is highlighted using an exam alert:

## Alert

Exam alerts, similar to this one, can be found throughout the chapters in this book. An exam alert is used to highlight information pertaining to a concept, term, task, or tool that is likely to appear in some form on the exam. Alerts highlight information that you should note carefully. This alert information also appears on the Cram Sheet.

In addition to exam alerts, this book also offers tips and notes, both of which are used to flag information that is important to the topic currently being discussed but may not necessarily appear on the exam. In general, we attempt to use tips and notes to point out information that can be important to the day-to-day operation of the environment.

- **Practice questions** Near the end of each chapter is a section containing sample exam questions demonstrating both correct and incorrect answers, along with explanations as to why a particular answer is correct or incorrect.

Besides the study material, which follows the layout presented in the preceding list, two complete sample exams are included in [Chapters 16](#), "[Practice Exam 1](#)," and [18 "Practice Exam 2"](#). They provide an opportunity to review the material presented in the book and help to ensure that you are ready for the exam by covering all of the different information discussed. [Chapters 17](#) and [19](#), respectively, provide answers for the questions found in [Chapters 16](#) and [18](#).

The final study aid available in this book is the tear-out Cram Sheet attached to the inside front cover of this book. This Cram Sheet contains a condensed collection of facts and tips that we feel are worth having at your finger tips during the study process and should be thoroughly understood prior to taking the exam. The small size of this sheet makes it an ideal refresher sheet to review prior to taking the exam or wherever you may be when preparing for the exam.

## How to Use This Book

The individual chapters in this book have been structured in such a way as to continuously build on one another. Therefore, some topics later in the book make use of information discussed previously. When you examine the material in this book for the first time, particularly if you have little previous MetaFrame experience, we recommend that you review the book from front to back.

For those readers with previous MetaFrame Presentation Server administration or exam experience, you may want to target specific areas where you are technically weak in the subject matter. At the very least, we suggest that you perform the self-assessment and then test your knowledge with the sample questions in each chapter and the final set of sample questions as a means of assessing what areas you may need to target for further study.

 PREV

NEXT 

# Self-Assessment

A self-assessment is included in this *Exam Cram* to help you evaluate your readiness to tackle Citrix Certified Administrator for MetaFrame Presentation Server 3.0. It should also help you understand what you need to master the topic of this booknamely, Exam 223, "Citrix MetaFrame Presentation Server 3.0: Enterprise Edition Administration." Before you tackle this self-assessment, however, let's address the concerns you might face when pursuing a Citrix Certified Administrator certification and what an ideal candidate might look like.

 PREV

NEXT 

## CCA in the Real World

More and more people are attaining Citrix Certified Administrator (CCA) status, so you can take comfort in knowing that the goal of achieving this certification is definitely not an impossible task. However, it does require serious, dedicated effort to learn the product so that you can earn the certification and be able to do the job as well. At the end of the day, the certification is just a piece of paper that says you passed an exam. In the real world, if you don't know what you are doing, that piece of paper quickly becomes useless, especially in today's competitive marketplace.

The *Exam Cram* books are designed to make preparing for these exams as easy as possible, but prepare you must!

The same, of course, is true for these other Citrix certifications:

- Citrix Certified Enterprise Administrator (CCEA), the next level up from the CCA certification, is aimed toward administrators, engineers, and architects who administer or build enterprise-scale Citrix environments. Candidates for this certification must have already taken and passed the CCA exam. Five exams, including the CCA, are required to gain CCEA status.
- Citrix Certified Sales Professional (CCSP) is designed to ensure that salespeople have the necessary knowledge to properly present and sell Citrix solutions to prospective clients.
- Citrix Certified Integration Architect (CCIA) is the highest attainable Citrix certification. It is geared toward integrators and architects to test their knowledge of the nuts and bolts of Citrix technologies. To earn this certification, you need to pass the CCA exam in addition to two more Citrix exams, 610 and 611. In addition, you need to pass a Microsoft design exam, and finally, you need to pass a lab exam administered by Citrix. The CCIA is the most respected Citrix certification and is also the hardest to attain.

## The Ideal CCA Candidate

Citrix MetaFrame Presentation Server 3.0 is an add-on product to Microsoft Windows 2000/2003 Terminal Server, so the first prerequisite is a good working knowledge of the operating system on which you intend to install MPS 3.0. Prospective CCA candidates who have experience administering Windows 2000/2003 networks or candidates with any of the following Microsoft certifications should meet the necessary requirements to tackle the CCA:

- Microsoft Certified Professionals (MCPs) who are certified on Windows 2000/2003 Server
- Microsoft Certified Systems Administrator (MCSA), an intermediate Microsoft certification that requires good knowledge of Microsoft networking and emphasizes the server product and technology
- Microsoft Certified Systems Engineer (MCSE), an advanced Microsoft certification that requires thorough knowledge of Microsoft networking and in-depth knowledge of the server product and architecture

Although the certification process can be both educational and profitable, there is always a need for

hands-on experience. For this reason, the ideal CCA candidate should have working knowledge with the following technologies:

- Windows user profiles
- Group Policy
- Login scripts
- Domain Name System (DNS)

Basically, Windows 2000/2003 administrators with real-world experience have the necessary skills that would position them as ideal candidates for the CCA exam.

## Testing Your Exam-Readiness

Whether you attend a formal class on a specific topic to get ready for an exam or use written materials to study on your own, some preparation for the Citrix certification exams is essential. At \$100 a try, pass or fail, you should do everything you can to pass on your first attempt. That's where studying comes in.

Included in this book are several practice exam questions for each chapter and two sample tests, so if you don't score well on the chapter questions, you can study more and then tackle the sample tests at the end of each part. If you don't earn a score of at least 75% on the Part I test and 80% on the Part II test, you should investigate the other practice test resources available via the Web. (Locate them by using your favorite search engine.)

For any given subject, consider taking a class if you've tackled self-study materials, taken the test, and failed anyway. If you can afford the privilege, the opportunity to interact with an instructor and fellow students can make all the difference in the world. For information about Citrix classes, visit the Citrix website at <http://www.citrix.com> for more information.

If you can't afford to take a class, visit the Certification Program page anyway because it also includes free sample questions. Even if you can't afford to spend much at all, you should still invest in some low-cost practice exams from commercial vendors because they can help you assess your readiness to pass a test better than any other tool. Check out Boson on the web at <http://www.boson.com> or LearnCitrix at <http://www.LearnCitrix.com>. Their practice exams are pretty good and reasonably priced, at least at the time of this publishing.

After you take a practice exam, if you scored 75% or better on Part I and 80% or better on Part II you're probably ready to tackle the real thing. If your score isn't above that crucial threshold, keep at it until you break that barrier.

### Tip

There is no better way to assess your test-readiness than to take a good-quality practice exam and pass with a score of 75% or better on Part I and 80% or better on Part II. When I'm preparing, I shoot for 85+%, just to leave room for the "weirdness factor" that sometimes shows up on Citrix exams.

## Onward, Through the Fog!

After you've assessed your readiness, undertaken the right background studies, obtained the hands-on experience that will help you understand the products and technologies at work, and reviewed the many sources of information to help you prepare for a test, you'll be ready to take a round of practice tests. When your scores come back positive enough to get you through the exam, you're ready to go after the real thing. If you follow my assessment regimen, you'll not only know what you need to study, but also know when you're ready to make a test date at Prometric on the Web at <http://www.prometric.com>. Good luck!

 PREV

NEXT 

# 1. Introducing Citrix MetaFrame Presentation Server 3.0, Enterprise Edition

Terms you'll need to understand:

- MetaFrame platform solution
- Citrix server farm
- Cross-farm license sharing
- Management Console for MetaFrame Presentation Server
- Management nodes
- Load evaluator
- MetaFrame policies
- Citrix Secure Gateway
- Interoperability mode

Concepts and techniques you'll need to master:

- Listing and understanding the differences between the MetaFrame platform solutions available from Citrix
- Identifying each of the components that make up MetaFrame Presentation Server, Enterprise Edition, and understanding what role they serve
- Selecting the appropriate component required to solve a given problem
- Understanding the purpose of interoperability mode and the limitations introduced with a mixed mode server farm

# Introduction

In preparing for the MetaFrame Presentation Server 3.0, Enterprise Edition (MPS/EE) exam, you must clearly understand the role that the main components of the software play in the overall function of the MetaFrame environment. The segmentation of these features and functionality serves two main purposes. First, it simplifies the task of studying and learning the information required to pass the exam. Second, it provides a template for categorizing the solutions to a particular problem. When you understand the functional job that each component plays, how they interact with other components in the system, and how they affect the end user's computing experience, you can take any problem that is thrown at you and immediately begin to narrow down to the specific component in the system that can be used to resolve the problem.

When preparing for an exam, many people memorize as much information as possible and hope to be able to regurgitate the correct answer to a question. I have always found this approach to be much more difficult than actually understanding how the pieces of the software fit together. Some readers may argue that these approaches are really the same, but I feel that when you understand the fundamentals, you can easily picture the layout of the system in your mind and can quickly travel down the desired path to the correct answer. When you have simply memorized a bunch of key facts, you rely on specific words in a question to trigger the correct response. Variations in wording and the proverbial "trick" questions are included specifically to trip up this type of brute-force problem solving.

With these thoughts in mind, we have created this book. Not only are we going to review the material that is most appropriate for the exam, but we are also going to attempt to deliver this information in such a way that it helps you to develop an intuitive understanding of the subject matter. If we can illuminate a few of those mental light bulbs, we have succeeded and you will be well on your way to passing this exam with flying colors.

Now that we've gotten the motivational pep-talk out of the way, it's time to get down to the business of preparing for this exam. In the remainder of this chapter, we focus on clearly defining the main components that make up the MPS/EE environment, discuss their functional characteristics, and provide a reference to the corresponding study material in the following chapters of this book.

From the top level, we then drill into each of the components to review and discuss the exam-related details. This top-down approach allows you to build knowledge around the foundation you will become intimately familiar with. Throughout the book, we periodically examine the environment from the top level, reinforcing the association between the components and the individual tasks you need to be able to accomplish.

## Note

We have found this top-down approach particularly well suited for preparing for those types of exam questions that ask you to select the correct task (or tasks) from a given list of choices to accomplish the described objective. Even if you're not certain exactly how the described task should be performed, knowing what area in the system such a task is managed will help you discard invalid choices and narrow down to the most logical answer presented.

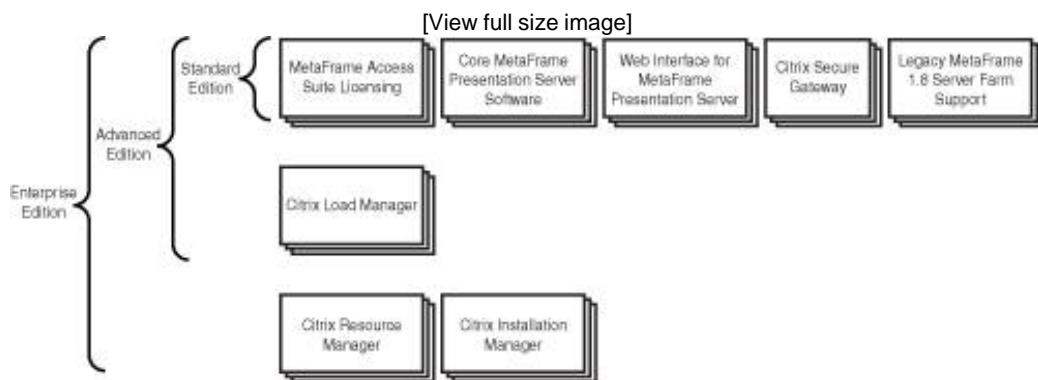
**◀ PREV**

**NEXT ▶**

# The Components of MetaFrame Presentation Server 3.0, Enterprise Edition

Figure 1.1 shows the topmost view of the main components of the MPS 3.0 environment, each of which we introduce in this chapter. When discussing each of these components, we provide a reference to the specific chapter where you can find more detailed review information.

Figure 1.1. Topmost component view of the MPS 3.0 environment.



## MetaFrame Presentation Server Platform Solutions

Even though exam 223 focuses on the administration of the Enterprise Edition of MPS, you still need to understand and identify the components supported by the different MPS 3.0 platform solutions available from Citrix. As shown in Figure 1.1 , three platform solutions are currently available:

- **Standard Edition** The Standard Edition of MPS 3.0 is targeted specifically at departments, workgroups, and small organizations that want to utilize MPS to deliver remote access to Windows 2000 Server or Windows Server 2003 from any supported client device. The Standard Edition is targeted at those organizations that require only one or two MetaFrame servers and do not require more advanced features such as resource-based load balancing.
- **Advanced Edition** The Advanced Edition provides all the features found in the Standard Edition as well as additional scalability and administration features such as CPU prioritization, resource-based load balancing, smooth roaming, and application performance controls.
- **Enterprise Edition** The Enterprise Edition includes all the features found in the Standard and Advanced Editions and includes additional enterprise-scale functionality, including zone preference and failover configuration, system analysis and monitoring, network management, and application packaging and delivery.

As we discuss the details of the various components throughout this book, we note those features available in certain platform solutions. Citrix provides a summary of the features by platform edition in a comparative

is available on their MetaFrame Presentation Server home page. The direct URL is <http://www.citrix.com/site/resources/dynamic/saledocs/CitrixPresentationServer40ComparativeMatrix0>

You can also reach the MPS home page by selecting Citrix Presentation Server from the Products/Product QuickFinder menu on the Citrix home page ([www.citrix.com](http://www.citrix.com) ).

## MetaFrame Access Suite Licensing

One significant change from earlier versions of MetaFrame is the new licensing infrastructure known as MetaFrame Access Suite Licensing (MASL). Citrix created MASL with the intention of using it as the new model for centralized licensing across the entire suite of applications that comprise the new 3.0 version of the MetaFrame Access Suite. MetaFrame Presentation Server 3.0 and MetaFrame Conferencing Manager (MCM) 3.0 are currently the only products supporting this licensing model.

With the introduction of the MASL model, the licensing component of MetaFrame is no longer coupled with the core MetaFrame software, as was the case in previous MetaFrame versions. Management of the licensing is now completely separate from all other aspects of the MPS environment.

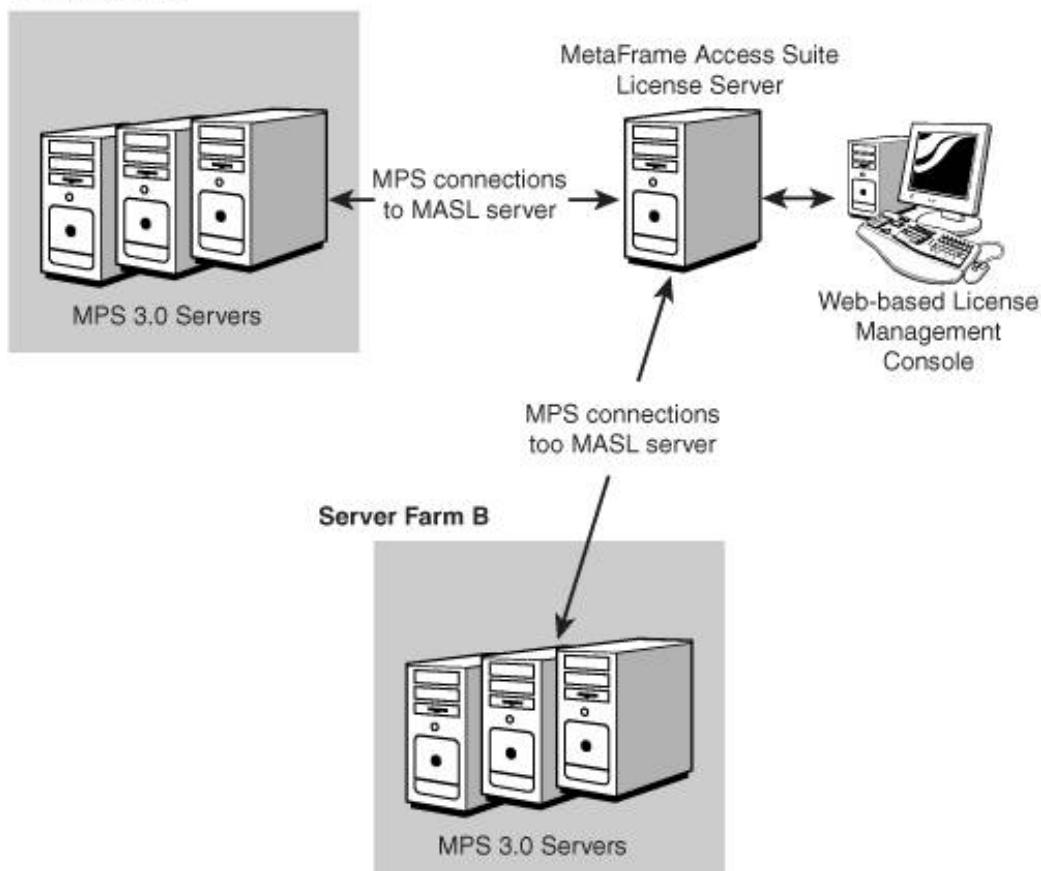
### Alert

The new MetaFrame Access Suite Licensing system is an essential part of the MetaFrame Presentation Server 3.0 environment and, as such, is also weighted rather heavily on the exam. Approximately 11% of the questions on the exam deal with MASL in one way or another, so understanding the material summarized here and presented in more detail in Chapter 4 , "Installing and Managing MetaFrame Access Suite Licensing," is essential to being properly prepared for the exam.

As part of a MetaFrame implementation, a server in the environment is chosen to host the MASL software and, as a consequence, becomes responsible for storing and issuing licenses when requested by a supported access suite application. Figure 1.2 demonstrates a pair of MPS 3.0 server farms, each with multiple MetaFrame servers, connecting to a single, separate server designated as the MetaFrame Access Suite License server. When a MetaFrame server first starts up, it looks to the license server to "check out" a special startup license. If this checkout is successful, the MetaFrame server establishes a continuous connection with the license server. When the connection exists, the MetaFrame server can send license issuance and revocation requests to the license server. License issuance and revocation details are discussed in Chapter 4 .

Figure 1.2. An MPS 3.0 environment with a single standalone MetaFrame Access Suite License server.

## Server Farm A



The following points summarize the key components and features of MASL reviewed in detail in Chapter 4 :

- *Shared or dedicated license server deployment* A shared license server combines the MASL software and MetaFrame Presentation Server (or another MetaFrame Access Suite product) onto one server. Other software, such as the Terminal Services licensing service, may or may not reside on the server. A dedicated license server runs only the MASL software and does not share resources with any other software in particular, MPS 3.0.

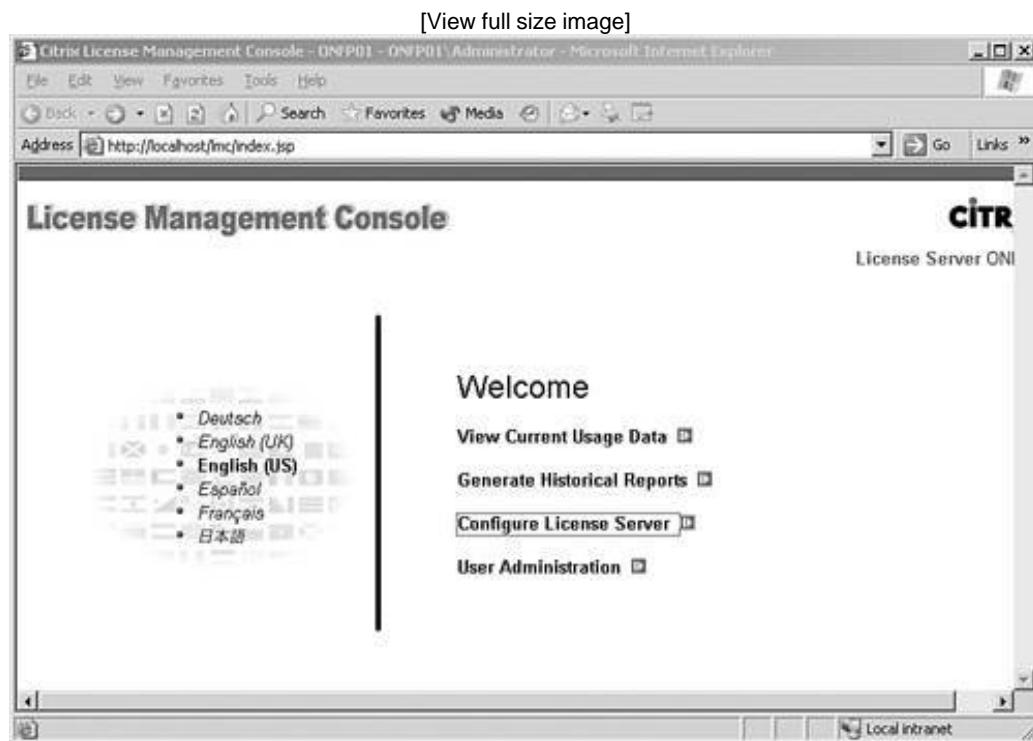
Citrix recommends deploying a shared license server configuration only in those environments with 50 or fewer MetaFrame servers. Between 50 and 500 servers, Citrix recommends a single dedicated license server, and for environments with more than 500 servers, a dedicated license server should be implemented for each type of MetaFrame Access Suite product being deployed. So, for example, if you deploy both MPS 3.0 and MCM 3.0 servers, you would have two dedicated license servers, one for each product type.

- *Centralized license activation and management* Licenses are no longer entered and activated within the Management Console for MPS (as they were in MetaFrame XP). Licenses are now activated and managed completely within the online Citrix Activation System (CAS), found through the My Citrix web portal (<http://www.mycitrix.com>). When you activate a license, a license file is generated; you must download and store that file directly on the license server. The contents of this file are then read to determine what types of licenses and their quantity are available. Copies of the license file can be retrieved from Citrix at any time without requiring that the licenses be reactivated.

License files are generated for a specific license server and cannot be directly copied from one license server to another. During the license activation process, you are required to provide the exact name of the license server. This name is case sensitive. The CAS does allow for license files to be "returned" and reissued. This then results in the generation of a new license file that is then deployed to the new license server.

- *License server management* An MASL server can be managed in two ways: either through a web-based management console, as shown in Figure 1.3 , or using a set of command-line tools, which are commonly referred to as License Administration Commands. You can perform basic administration using either method, but advanced report and alert capabilities are available only through the web-based console. The web-based console requires that Internet Information Server (IIS) 5.0 or greater be installed on the server *prior* to installation of MASL.

Figure 1.3. One way to manage a MetaFrame license server is through the web-based management console.



The specific commands will be discussed in Chapter 4 .

- *Cross-farm license sharing support* As Figure 1.2 illustrates, multiple distinct server farms can now share licenses through a single license server. When directed to the appropriate license server through the Management Console for MetaFrame Presentation Server, MetaFrame servers within a farm retrieve license information without any knowledge of other farms that may also be sharing the same license information.

One advantage of this configuration is that a client device can connect to multiple farms yet consume only a single license. Cross-farm license pooling is supported only with MPS 3.0 servers. Previous MetaFrame editions cannot leverage this cross-farm pooling. To leverage cross-farm license pooling, you need only to direct each farm or individual servers in the farms to the central license server.

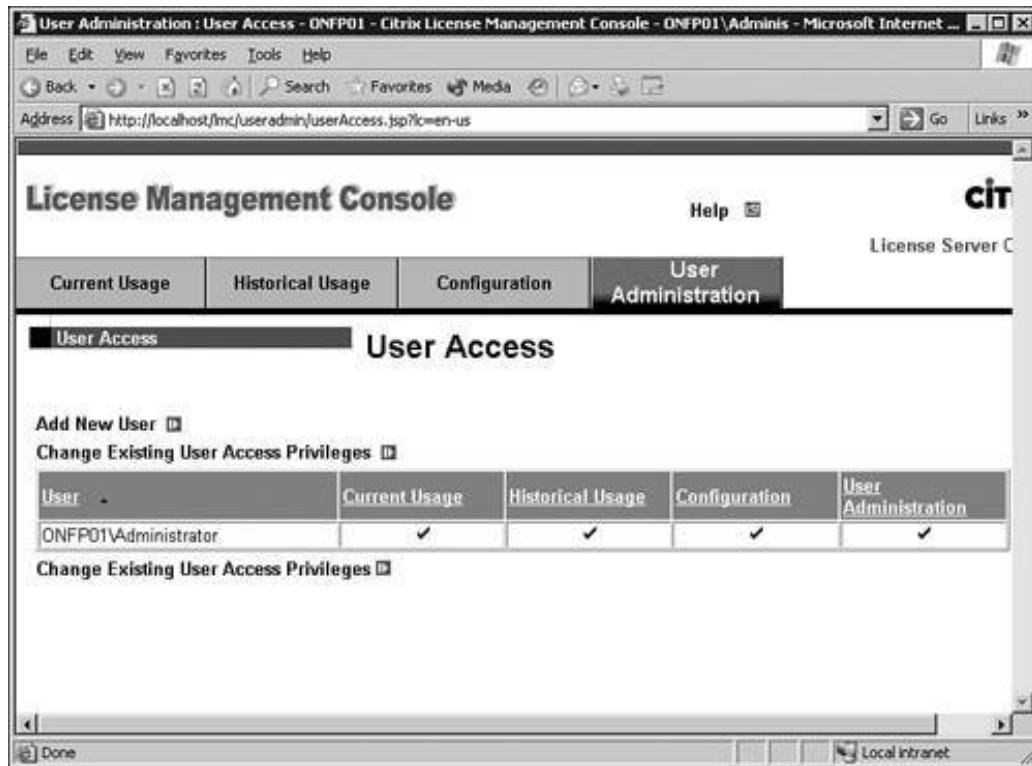
- *No license support for previous MetaFrame versions* The new MASL infrastructure is not backward compatible with previous MetaFrame versions. For example, if a mixture of MetaFrame XP and MPS 3.0 servers exist in the same environment, an MASL server must be used for MPS 3.0 licensing, while the MetaFrame XP servers continue to use their existing XP licensing.
- *Licensing is now time based and not version based* MetaFrame licenses are now valid for the length of the current subscription advantage period. When the subscription advantage expires, so does the license file, at which time the subscription must be renewed and a new license file downloaded. Until the current license expires, upgrades to the existing MPS software would not require any changes to the product licensing, unless, of course, you moved to a new product feature set (Advanced to Enterprise, for example).
- *It is recommended that MASL be installed and configured prior to installing MPS 3.0* MPS 3.0 requires the presence of a properly configured MASL server to provide basic functionality and must be able to retrieve the necessary license information before nonadministrators can access the environment beyond a brief grace period.
- *Limited grace period for nonadministrative users* Until a valid MASL server exists with the necessary license files, only two nonadministrative user connections are granted a temporary license. These temporary licenses are valid for only 96 hours (4 days). After this time, these licenses expire and the users can no longer access the MetaFrame server until a valid license file has been added to the MASL server.

Administrative users are not subject to this grace period and can connect indefinitely even if a valid license file does not exist.

- *Extended grace period in the event of MASL server failure* Originally, Citrix imposed the same 96-hour grace period limit for user connections in the event of an MASL server failure in a production environment. It was later decided that such a brief period was not acceptable and the time interval was increased to 30 days. This increase applies only to an existing license server that fails. The 96-hour limit for new installations with no license server remains unchanged.
- *Backup server support* MASL does not currently support pooling of licenses between multiple license servers, nor does it allow a farm or individual MetaFrame server to reference more than a single license server. Because of this, a failover solution would require that a second server remain on standby or be available for recovery from a disk image if the current production server should fail. One alternative solution is to utilize Microsoft clustering. Citrix supports the use of Microsoft clustering to provide a redundant MASL server solution.
- *Administrative delegation and control* MASL provides some basic administrative delegation settings. MASL grants access on a per-user basis, and any combination of four access rights can be granted. Figure 1.4 shows the access options available. Current Usage grants access to view the current license usage, and Historical Usage allows the user to run reports based on archived usage data. The Configuration setting controls access to modifying the license server configuration, and User Administration dictates who can add, delete, or modify the list of users authorized to access the license server. Access is based on the user's Windows domain account.

Figure 1.4. MASL provides basic administrative delegation settings.

[\[View full size image\]](#)



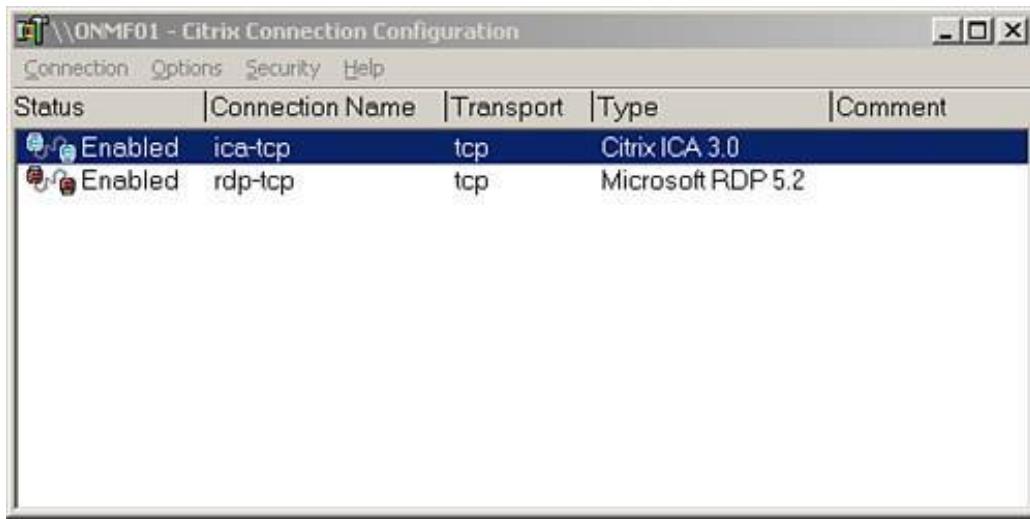
## Core MetaFrame Presentation Server Software

All platform versions of MetaFrame Presentation Server share the same core software set. This software is broken down into two categories: administrative tools and management consoles. Eight applications make up the administrative tools set and two management consoles. The administrative tools are as follows:

- *Citrix Connection Configuration (CCC) Tool* The CCC tool is Citrix's main utility for managing the connection settings for the MetaFrame server. As Figure 1.5 shows, you can manage the settings for both Citrix's Independent Computing Architecture (ICA) and Microsoft's Remote Desktop (RDP) protocols. The majority of the settings within the CCC can also be configured using Microsoft's Terminal Services Configuration tool, but a couple of settings are unique to the CCC, which is the reason this tool is still maintained. One important security setting allows you to restrict users to be able to access the MetaFrame server only through a published application. This prevents them from establishing a direct connection to a server using the ICA or RDP clients, depending on how the protocols have been configured. You can find a more detailed description of the CCC tool in Chapter 6 , "Configuring and Administering MetaFrame Presentation Servers."

Figure 1.5. Citrix provides its own tool for managing server connections: the Citrix Connection Configuration utility.

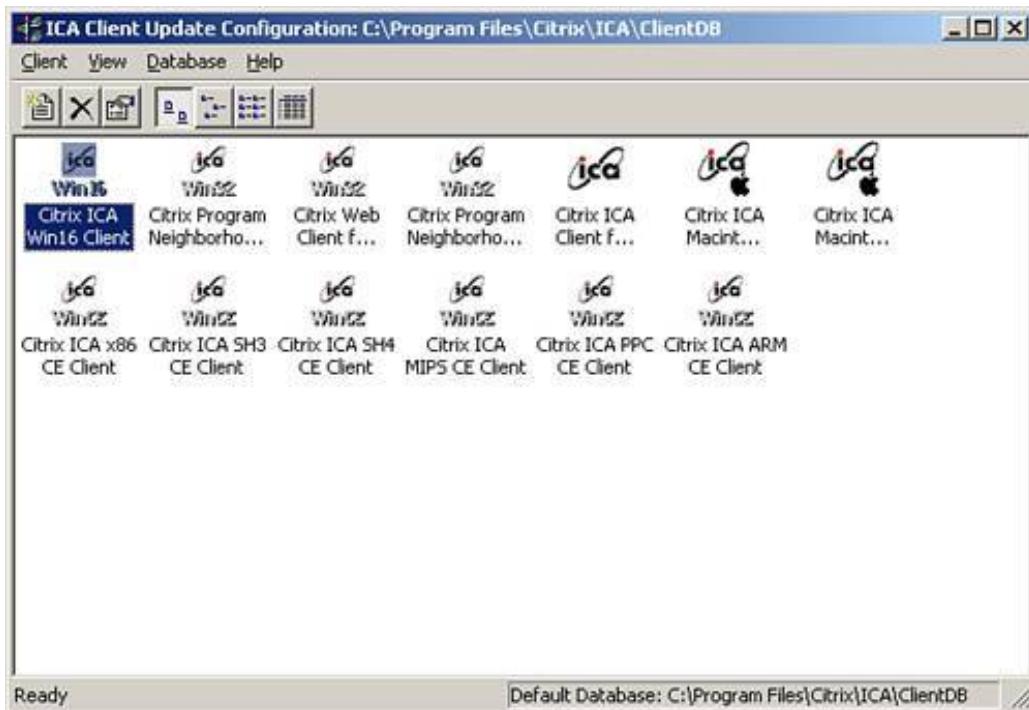
[View full size image]



- **SSL Relay Configuration Tool** When access to a MetaFrame environment has been provided through the Web Interface for MPS, communications between the web server and the MetaFrame servers can be secured using Secure Sockets Layer (SSL). Before this communication can be initiated, the SSL Relay must be properly configured using this tool. Through this tool, you define the appropriate certificate that will be presented when requested by the web server to initiate the SSL connection. You can find details on the configuration of this tool and certificates in Chapter 14 , "Web Connectivity to the MetaFrame Server Farm."
- **ICA Client Distribution Wizard** This tool serves two purposes. First, it updates the various ICA client image files and the update database for the ICA Client Update utility on the MetaFrame server. These files are used to automate the upgrading of the ICA client on the various client devices that support this feature. Second, this tool upgrades the ICA Pass-Through client installed on the MetaFrame server. The Pass-Through client is responsible for allowing published applications hosted on one MetaFrame server to be run from the desktop of another MetaFrame server. The seamless integration of applications from various servers and farms is one of the flexible benefits of running MetaFrame. All aspects of the client configuration, including the Distribution Wizard, are described in Chapter 13 , "Citrix ICA Sessions and Client Configuration."
- **ICA Client Printer Configuration** The primary purpose of this utility is to allow clients who connect to the MetaFrame server using either the ICA Clients for DOS or Windows CE to be able to establish connections with local printers. This tool is designed to be run by the user, allowing him or her to select and connect to any of the available listed printers. This tool can be used by anyone running a supported ICA client, but it was created specifically for DOS and Windows CE-based clients. You can find details on the ICA Client Printer Configuration, along with other printer-specific MetaFrame information, in Chapter 12 , "MetaFrame Presentation Server Printing Support."
- **ICA Client Update Configuration** Figure 1.6 shows the main window for this utility, which shows the details for the available ICA clients. The latest client deployment files corresponding to the various ICA clients that can be automatically updated are shown here. By manipulating the properties in this tool, you can determine which clients are updated and under what circumstances. The client images are updated using the ICA Client Distribution Wizard discussed earlier in this list. The ICA Client Update Configuration utility is reviewed in Chapter 13 .

Figure 1.6. Using the ICA Client Update Configuration utility, you can control what supported ICA clients are automatically updated.

[View full size image]



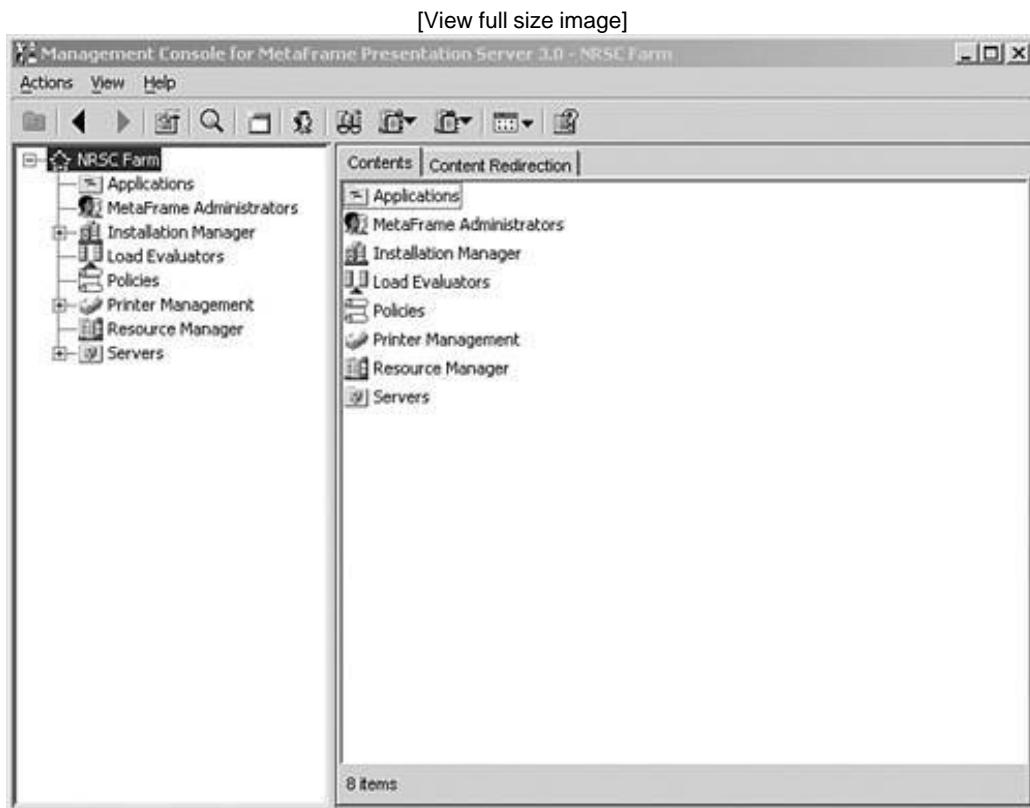
- *ICA Toolbar* This simple management toolbar appears by default down the right side of the desktop for any administrator who logs on to a MetaFrame server; it provides a means of quickly launching the other seven administrative tools and two management consoles discussed here. Additional applications can be added to the toolbar to expand its functionality. It can also be completely disabled for those administrators who prefer not to use it.
- *Shadow Taskbar* The Shadow Taskbar enables an administrator to centrally manage multiple simultaneous user shadow sessions. Traditionally, shadowing another user's session either from a command prompt or through the Management Console suspends your current session, preventing you from moving between your desktop and the shadowed session without having to terminate and re-establish the shadow session. The Shadow Taskbar allows you to manage multiple concurrent shadow sessions by establishing a new MetaFrame session specifically for shadowing. One drawback to this technique is the time required to load the session to shadow and the extra server resources consumed. The use of the Shadow Taskbar is discussed in Chapter 6 .
- *SpeedScreen Latency Reduction Manager* The final tool in this list, the SpeedScreen Latency Reduction Manager, allows you to specifically define the thresholds at which MetaFrame's SpeedScreen Latency Reduction features are automatically enabled or disabled. In addition to these thresholds, you can also set the default behavior for text echoing and mouse-click feedback on a per-server basis. Text echoing functionality can also be configured on a per-application basis if desired. SpeedScreen Latency Reduction settings are also discussed in Chapter 6 .

In addition to the eight administrative tools, the following two management consoles are available:

- *Management Console for MetaFrame Presentation Server* The single-most important configuration tool in the MPS 3.0 environment, the Management Console for MPS, is the centralized source for defining the majority of settings for both the server farm and the servers within that farm. Figure 1.7 shows the main window of the Management Console that appears when the application first loads. You can see the various management nodes in the left pane, each of which is used to configure or manage a certain portion of the MetaFrame environment. The specific nodes available within the Management Console depend on the MetaFrame edition

being used.

Figure 1.7. The Management Console is the main configuration and management tool for MetaFrame Presentation Server 3.0.



## Note

The Management Console is also referred to as the Presentation Server Console.

Using the properties of the parent server farm node, labeled as NRSC Farm in Figure 1.7 , you can manage the farm-wide settings that affect all servers and users in the farm. For example, the license server for the farm is defined here as well as the current server farm zones and MetaFrame 1.8 interoperability settings. Many farm-wide properties can be overridden on a server-by-server basis. Farm and server settings are discussed in Chapter 6 .

In the *Applications*node, published applications and content are created and monitored. This is also the place where you can configure applications to be monitored by the Resource Manager to limit total concurrent instances. Application publishing is covered in Chapter 10 , "Application Integration," while resource management is discussed in Chapter 15 , "Managing and Monitoring Using Resource Manager."

The delegation of administrative access to the MetaFrame farm via the Management Console is performed under the *MetaFrame Administrators*node. Access is broken down into different privilege levels for each of the nodes present. For example, you can define what access rights an individual administrator has on the Policies node. Access delegation is briefly reviewed in Chapter 6 .

From within the *Installation Manager* node, you manage the deployment of software packages to your MetaFrame servers. These packages can include full applications, service packs, hotfixes, or even individual files. The details of using Installation Manager are discussed in Chapter 11 . Installation Manager is available only with the Enterprise Edition of MPS.

The *Load Evaluators* node is the place where you create and modify the different load evaluators that can be utilized by the Load Manager. From this node, you can also access a usage report that tells you what servers or applications are associated with what load evaluator. The two standard evaluators, Advanced and Default, are read-only and cannot be modified or deleted. You can use copies of these evaluators when creating your own. Load evaluators for individual servers or applications can be modified from this screen. The Load Manager component is available with the Advanced and Enterprise Editions of MPS.

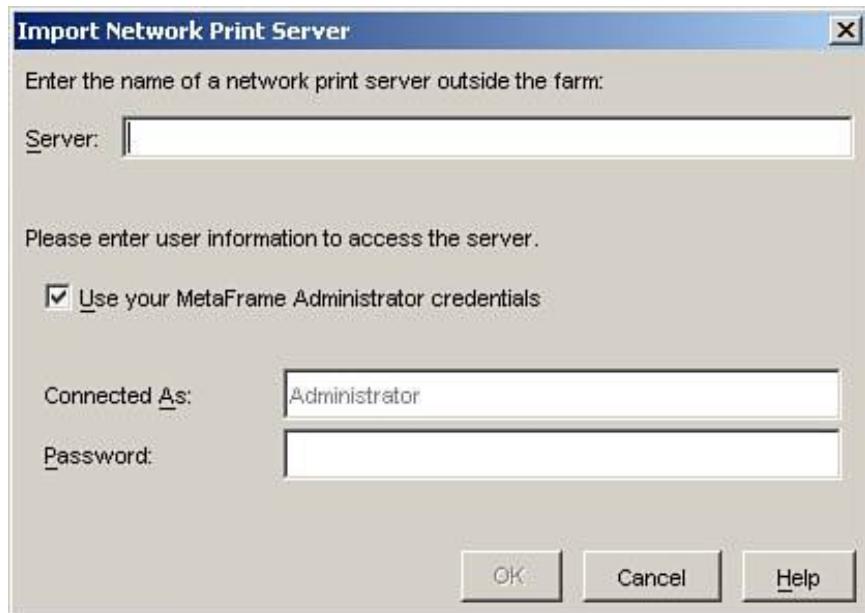
Under the *Policies* node, you can manage the MPS 3.0 policies that you define for your farm. Much like the group policies for a Windows Active Directory domain, the MPS policies allow you to manage many of the client session and connection-specific settings of your farm. Instead of being forced to define the same settings for all users on a MetaFrame server, through policies you can control the behavior of certain settings based on any combination of

- Client IP address (individual addresses or a range)
- ICA client name
- MetaFrame server name
- User ID or group membership

One powerful option managed through MPS policies is the Zone Preference and Failover setting. When a farm contains more than one zone, you can use this option to define which zone should be the preferred zone and which ones should be failover zones for specific groups of MPS clients. MPS policies are discussed in detail in Chapter 7 , "MetaFrame Presentation Server Policy Management."

The *Printer Management* node is the place where all the printer driver and autocreated network queue management is performed. If your task is somehow printer related, you are likely to find what you need within this node. The Import Network Print Server dialog box, shown in Figure 1.8 , allows you to import the shared printers from a particular print server and then configure them to automatically map for users when they log on to a MetaFrame server in the farm. Chapter 12 discusses the relevant printing features that you need to understand for this exam.

Figure 1.8. One feature of Printer Management allows you to import print queues from a print server and automatically have users connect to those printers based on their group membership.



## Note

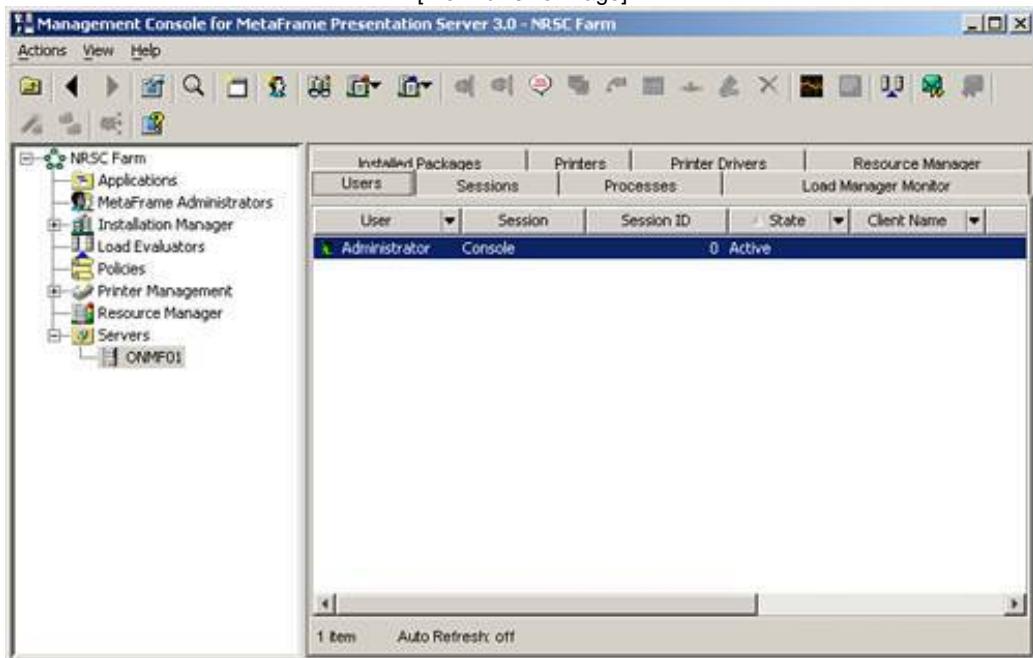
Printing is one area that often is not implemented properly. To ensure that this is not the case, Citrix has dedicated 13% of the 223 exam to material on printing.

Under the *Resource Manager* node, you can find the suite of tools for configuring, logging, and reporting on the resources of one or more MetaFrame servers in your farm. The information collected is referred to as a *metric*, and a wide variety of system and network metrics are tracked, allowing an administrator to monitor and analyze all aspects of the environment. These tracked metrics not only can be valuable when resolving issues in the environment, but can also provide insight into areas of the infrastructure that should be targeted for future growth. The Resource Manager, which is available only with the Enterprise Edition of MPS, is discussed in Chapter 15 .

The final node in the Management Console is the *Servers* node, which as expected is the container for all server objects in the farm. Within this node, you can view a wide assortment of server-related information, as well as define numerous settings, many of which are inherited from the same settings defined at the farm level. Figure 1.9 shows the tabs present when selecting a MetaFrame server farm. Whereas some tabs such as Installed Packages, Load Manager Monitor, Printers, and Printer Drivers provide access to read-only information, other tabs such as Users or Resource Manager allow you to define settings and interact with the information displayed. The Users tab in the Servers node is often used to initiate a shadow session with a user when attempting to assist the user with an application or session-related problem. Most of the information pertaining to the Servers node is discussed in Chapter 6 , although certain pieces, such as the Installed Packages and Resource Manager tabs, are covered in Chapters 11 and 15 , respectively.

Figure 1.9. Using the Servers node, you can view and configure information related to the MetaFrame servers in your farm.

[View full size image]



- *Access Suite Console* The MetaFrame Access Suite Console is intended to become the central location where you manage your MetaFrame Access Suite deployment. All the applications that make up the suite (MetaFrame Presentation Server, Secure Access Manager, Conferencing Manager, Password Manager) are accessible from this console. At present, only Presentation Server and Conferencing Manager are part of the new Access Suite, and only Presentation Server is currently supported within this Access Suite Console. The Access Suite Console is discussed briefly in Chapter 6 .

## The Web Interface for MetaFrame Presentation Server

The Web Interface for MPS is composed of a number of components that work together to provide users with access to their list of published applications either through a web browser, as shown in Figure 1.10 , or in conjunction with the Program Neighborhood Agent (PNAgent). The PNAgent is a special MPS client discussed in Chapter 13 .

Figure 1.10. When explicit logons are required (not anonymous logons), the main Web Interface page prompts the user to provide authentication information before published applications are displayed.

[View full size image]

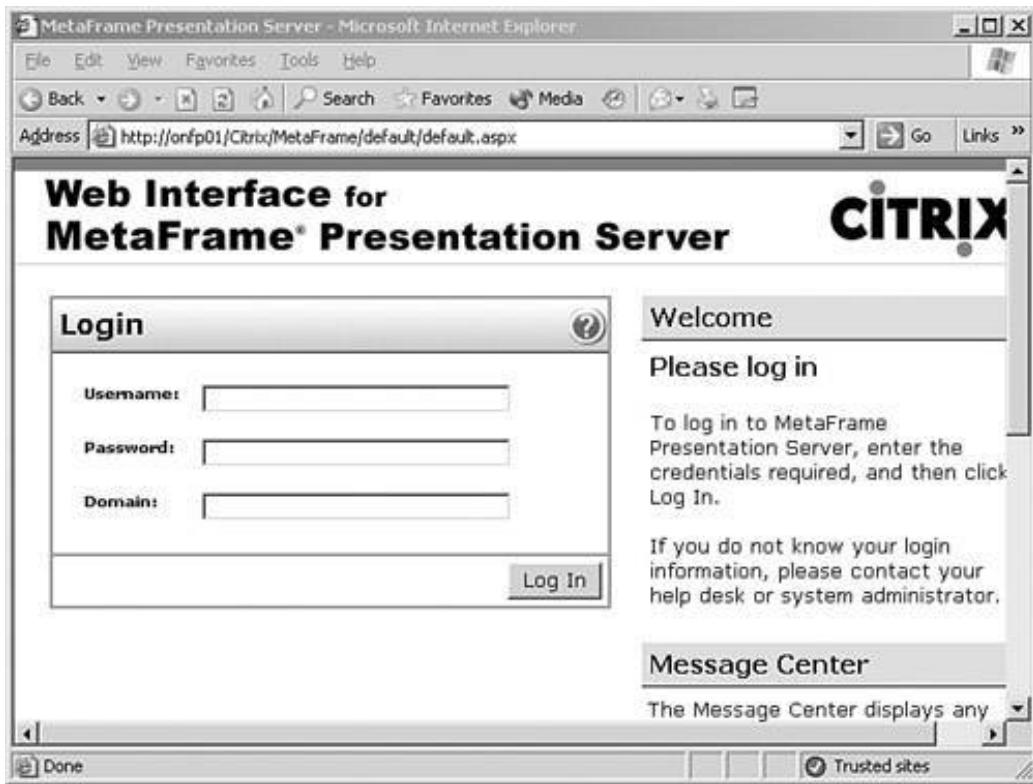
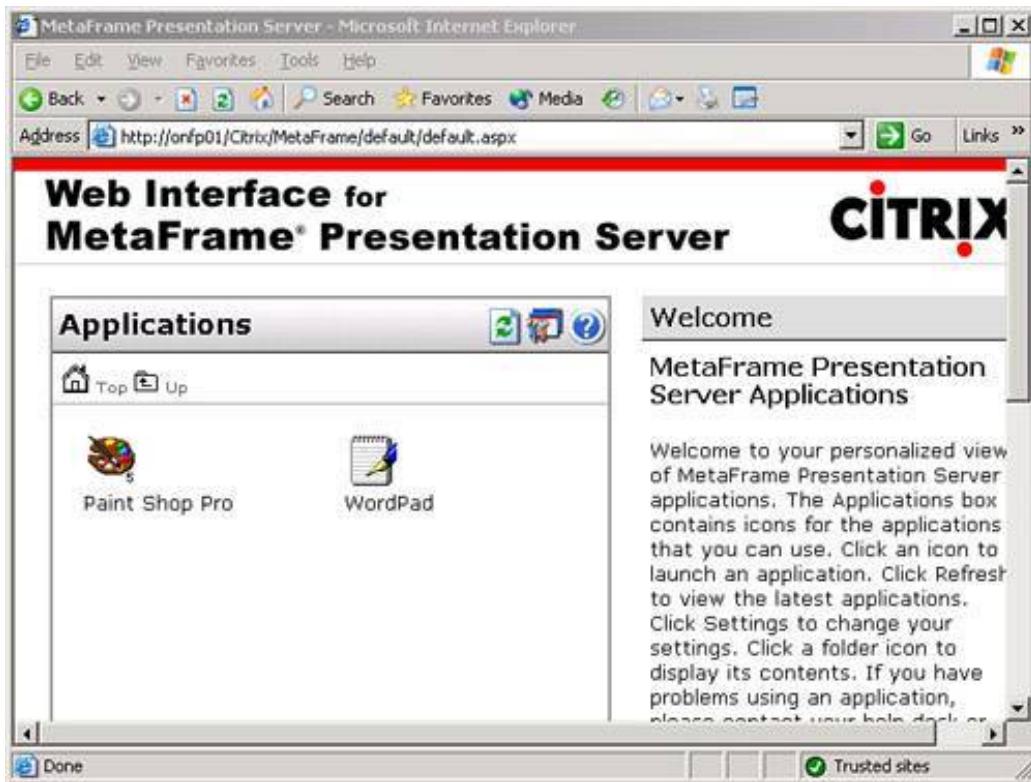


Figure 1.10 shows the main logon page for the Web Interface. After a user has been properly authenticated, he or she is presented with a new web page that contains links to the published applications to which he or she has been granted access (see Figure 1.11). Regardless of whether a user is going to be accessing a published application through the Web Interface or through any other MPS client, the applications are configured exactly the same way. That is, no special setup must be done on the MetaFrame server to make a published application accessible via the Web Interface. Chapter 14 discusses the configuration and use of the Web Interface, including the security concerns that need to be addressed before putting the Web Interface into production.

Figure 1.11. After an application has been published in the farm, it is accessible to authorized users regardless of whether they're using a traditional client or the Web Interface.

[View full size image]

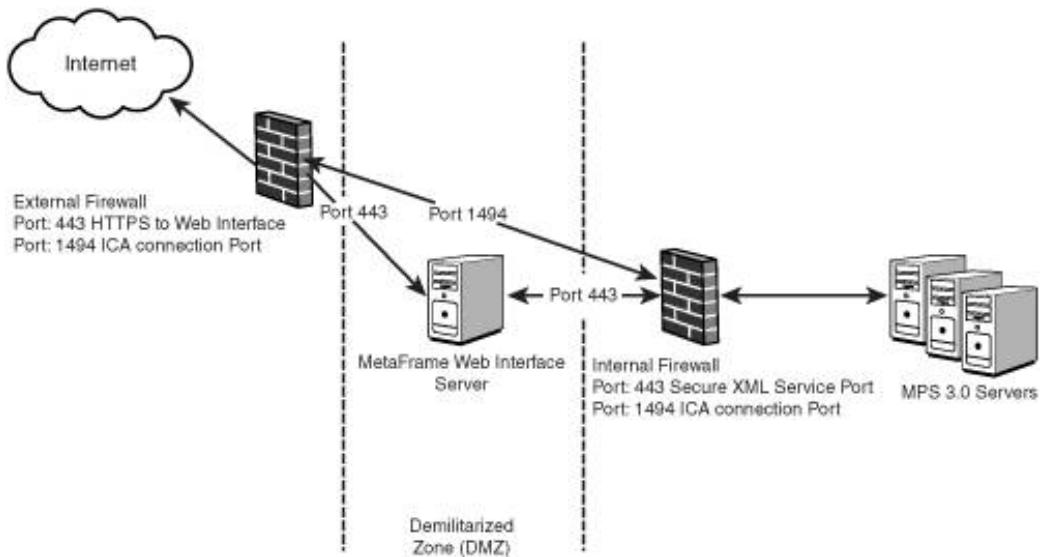


## Citrix Secure Gateway

Although the Web Interface provides a convenient and robust method for users to access their published applications, making such a configuration available via the Internet brings with it some serious security concerns. Figure 1.12 illustrates one possible Web Interface configuration accessible from the Internet. The server hosting the Web Interface is located in a *demilitarized zone* (DMZ), while the MetaFrame servers that will be accessed are located inside the internal network of the company. HTTPS has been implemented for connectivity to the Web Interface to ensure that user credentials are passed safely. SSL/TLS encryption is also used to secure communications between the Web Interface and the internal MetaFrame servers. This is configured using the SSL Relay Configuration tool discussed earlier in this chapter.

Figure 1.12. The Web Interface on its own would require opening firewall ports directly through to the internal network.

[View full size image]



## Note

The term *DMZ* (for *demilitarized zone*) is used to describe a network typically located between a secure internal network and an unsecure external network (typically the Internet). Devices in a DMZ are configured with very restricted access into the internal network, limiting the internal network's vulnerability should the DMZ-based device's security become compromised.

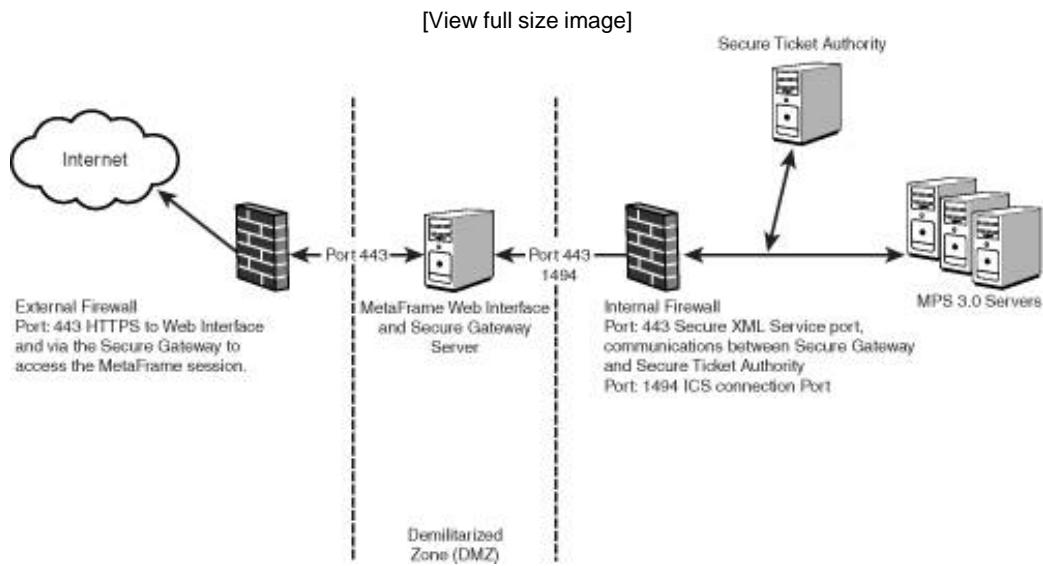
Next to the two firewalls shown in Figure 1.12 are listed the port numbers that must be open for external users to be able to access their desired published applications. One point of concern is the fact that ports must be open, allowing direct access from the Internet through to the internal MetaFrame servers. This Web Interface configuration would allow an Internet user who knew an external IP address and the open port to pull up the Windows logon screen for one of these servers, bypassing completely the Web Interface.

Citrix developed the Secure Gateway product to provide two main services:

- Act as a single point of access into a MetaFrame server farm, facilitating authentication in conjunction with the Web Interface.
- Encapsulate the communications between the MPS client and the internal MetaFrame servers via the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) security protocol.

Figure 1.13 shows the same Web Interface environment, this time with a Secure Gateway implementation. The only external port open is SSL/TLS port 443, and external clients no longer have direct access through to a specific MetaFrame server. Because the Secure Gateway brokers connectivity between the client and the MetaFrame server, direct communication from the client to the server is not possible without first going through the Secure Gateway. In Figure 1.13, the Web Interface and the Secure Gateway are configured on the same server. This is a fully supported and common deployment although these services can be deployed on separate servers if desired. Implementation of the Web Interface and Secure Gateway is discussed in Chapter 14.

Figure 1.13. The Citrix Secure Gateway encapsulates all communications using the SSL or TLS security protocols and ensures that only clients properly authenticated can even access the MetaFrame servers on the secured network.



## Citrix Load Manager

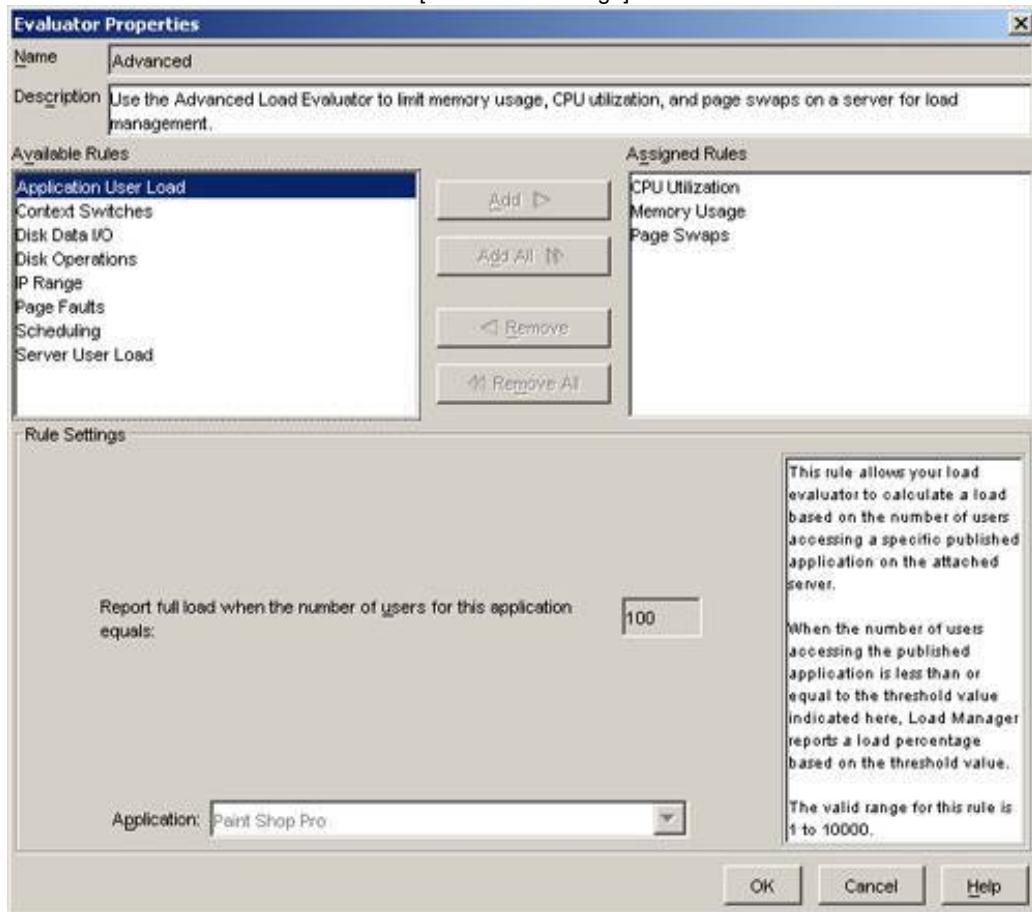
Included as part of the Advanced and Enterprise Editions of MPS, Citrix Load Manager comes preconfigured with basic settings that allow it to be used without the need for any special configuration by an administrator. The relative load of a MetaFrame server is calculated based on the settings of a load evaluator. As we mentioned briefly when discussing the settings in the Management Console, a load evaluator is simply an object with a particular set of defined criteria that dictate how MetaFrame should calculate the load of the server. Two evaluators are included with the Load Manager.

The Default evaluator determines the load based solely on the number of users accessing a specific published application on the server. The server is determined to be fully loaded when the number of concurrent users reaches a predetermined number. The default number for reaching full load is 100. If you want to modify this value, you need to create a custom evaluator. You cannot modify either of the evaluators included with MPS. The Default evaluator is automatically assigned to a server when MPS 3.0 Advanced or Enterprise Edition is installed.

The other evaluator included with MPS is the Advanced evaluator. It determines the load for an application based on the CPU utilization, memory usage, and page swaps. Each rule is evaluated to determine what the current load reported by the server should be. The cumulative results reported by all the listed evaluators are used to determine the load of the server. For example, the server reports full load only when all evaluators report full load. Figure 1.14 shows the properties for the Advanced evaluator. The rules that can be used are listed down the left side of the dialog box; each of these rules is discussed further in Chapter 8 , "Citrix Load Management."

Figure 1.14. A load evaluator for Citrix Load Manager includes a number of rules that you can use to best configure load balancing for the published applications in your environment.

[View full size image]



When a client device attempts to connect to a published application, the server with the lowest reported load is automatically provided to the client device as the target server from which to access the published application. If all available servers publishing a particular application report 100% load, the client is unable to connect to the application.

## Alert

The new Citrix Load Manager in MPS 3.0 is not compatible with MetaFrame 1.8 servers when operating in a mixed mode environment. In a mixed mode environment, the only load balancing support available is through the Load Balancing Services included with MetaFrame 1.8.

## Citrix Resource Manager

Citrix's Resource Manager component, available with the Enterprise Edition of MPS, allows an administrator to log and report on the resources of one or more MetaFrame servers in a server farm. The functionality of the Resource Manager can be broken down into three broad categories:

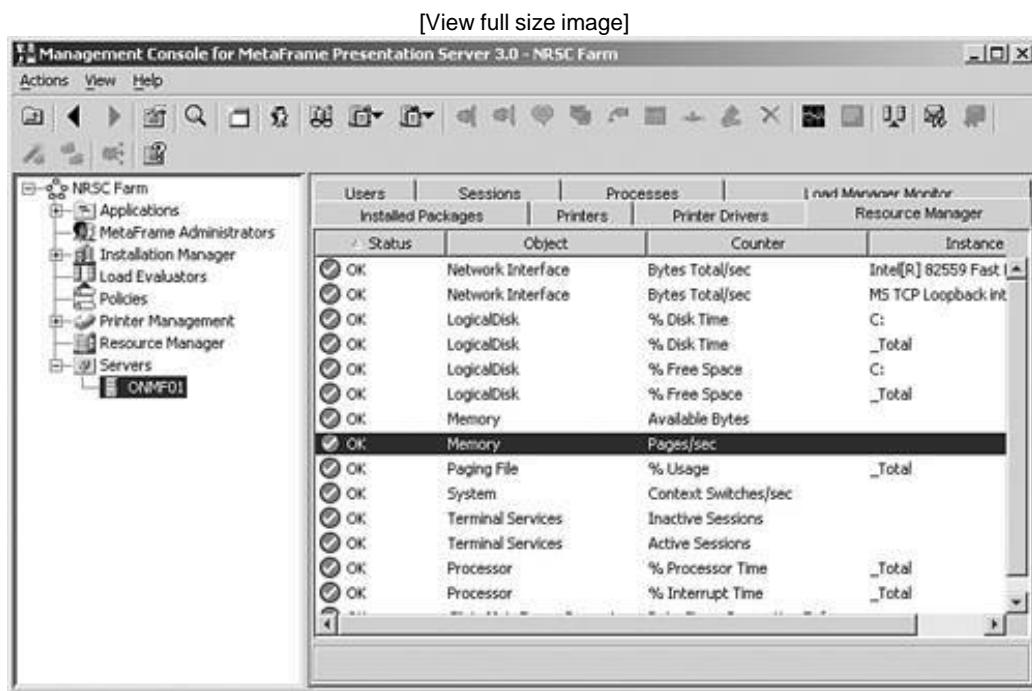
- *Real-time monitoring* The Resource Manager allows you to view what is happening with one or more systems in real-time.

- *Current and historical report generation* With the Resource Manager, you can generate reports both on real-time and historical data, which can then be used to resolve environmental issues or plan for future infrastructure growth.
- *Billing report generation* The Resource Manager allows you to track usage of various system resources on a per-user basis and then generate billing reports that can be used to charge by system resource use. The appropriate costs associated with the system resources are defined by an administrator.

Information, whether it is being tracked in real-time or logged for historical or billing report generation, is known as a server metric. Metrics are fully customizable, allowing an administrator to tailor the Resource Manager configuration to suite his or her needs. When the Resource Manager is installed, it automatically defines a set of metrics used to track information. For each metric, a default limit is also configured; this limit is used to raise alarms to alert you when a potential problem is occurring. For each alarm that can be raised, customizable alerts can be created, allowing an administrator to be informed of an alarm regardless of where he or she may be.

One way to view the list of metrics defined for a server is through the Management Console. This is achieved by highlighting a server and selecting the Resource Manager tab, as shown in Figure 1.15 . The current status is listed beside each metric, and from here, you can view real-time graph information on a particular metric or view the configuration for the metric by right-clicking and selecting Properties. Each of these three main areas is discussed in Chapter 15 .

**Figure 1.15.** Metrics are tracked by the Resource Manager, and alarms can be generated based on threshold criteria defined for each metric.



## Installation Manager

Citrix's Installation Manager centralizes the task of software deployment in a MetaFrame server farm, allowing you to rapidly and reliably push out a wide variety of software components (applications,

software patches, service packs, and so on) without having to repeat the installation steps on each server in your farm.

Software, regardless of the particular type, is bundled into what is known as a software package. This software package is then delivered to the target MetaFrame server, where it is extracted and installed. Citrix allows great flexibility in exactly how these packages are delivered and how a server processes a particular package it receives.

The Installation Manager is composed of four components:

- *Package Management Server* This component is nothing more than an MPS 3.0 Enterprise Edition server running the Management Console for MPS. Earlier in the chapter, we described the Management Console and the Installation Manager node. Through the Management Console, you can schedule and view package deployment jobs. There are no restrictions on what server must be used to manage the Installation Manager. It can be any server in the farm, including a server that is being updated with a particular package (Target Server).
- *Network Share Point Server* The application packages themselves are hosted through a standard file share on one or more Windows servers. Multiple different share points can be used if desired to localize the source of the application package for MetaFrame servers located in different physical locations.

There is no limitation on what type of server should act as the network share point server, and for small environments, even the Package Management Server itself can host the application packages.

- *Package Server (optional)* When you're creating your own custom packages using the Packager tool provided with the Installation Manager, a MetaFrame server in the farm is chosen to be the Package Server. The Packager, a tool used to create ADF packages, is a special tool that "records" the changes made to the server during the installation of an application and saves them in the ADF file to allow the duplication of these changes on a target server.

Citrix recommends that the MetaFrame server chosen to be the Package server be dedicated to the creation of packages only, and not used to service standard user sessions. The reason for this is to ensure that the server remains in "pristine" condition, minimizing the amount of extraneous information that may find its way into the package during the package's creation.

- *Target Server(s)* Any MPS 3.0 Enterprise Edition server that has the Installation Management Installer Service running can be chosen as a target server. When a target server receives the request to install a particular package, it looks to the appropriate Network Share Point Server to install that package.

The configuration and use of each of these components of the Installation Manager are discussed in Chapter 11 .

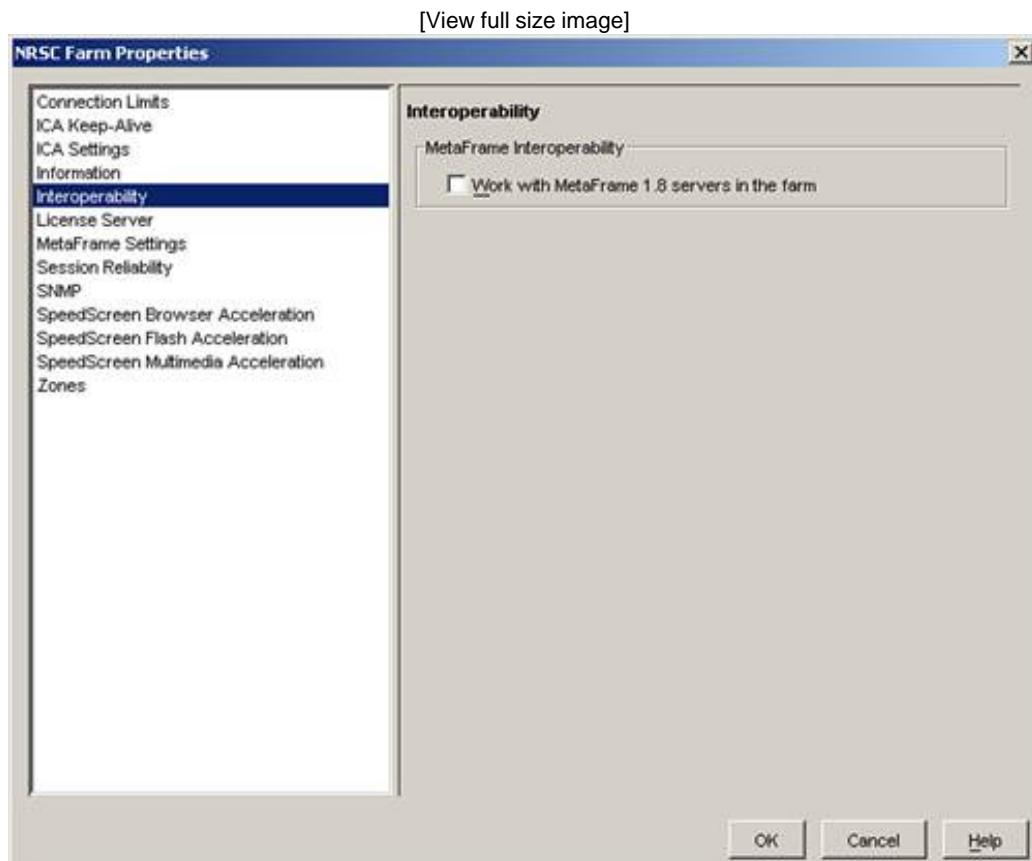
## **Legacy MetaFrame 1.8 Server Farm Support**

An important consideration for many MetaFrame administrators is the ability to slowly transition an existing MetaFrame 1.8 environment over to a new MPS 3.0 environment. To facilitate this migration process, Citrix allows an MPS 3.0 server farm to operate in one of two modes:

- *Native mode* This is the default mode for a new MPS installation and allows only MetaFrame XP 1.0 or higher servers to be members of the server farm. When operating in this mode, the MPS 3.0 server farm operates completely independent of any MetaFrame (MF) 1.8 server farms that may exist.

- **Mixed mode** Mixed mode operation provides backward compatibility with MetaFrame 1.8, allowing for the transparent introduction of MPS 3.0 servers into an existing 1.8 server farm. Mixed mode is also referred to as *interoperability* mode. You enable interoperability mode by selecting the Interoperability option under Server Farm properties, as shown in Figure 1.16 . Once enabled, MPS 3.0 servers appear as MF 1.8 servers to the other servers in the 1.8 farm. When interoperability is enabled, all existing 1.8 servers are forced to restart their ICA Browser and Program Neighborhood (PN) Services. During this time, new user connections are not serviced. Because of this, it is highly recommended that interoperability be enabled during off-peak hours to minimize the impact to the users.

Figure 1.16. Interoperability mode is enabled or disabled at any time from within the properties of the server farm.



When an MPS 3.0 server is running in mixed mode, you will see that the ICA Browser service is available and started. If it is subsequently switched to native mode, this service is stopped and removed from the service list.

## Note

Citrix recommends that you upgrade all your MetaFrame 1.8 servers to the latest available service pack (Service Pack 4) prior to enabling interoperability mode.

## Alert

Implementing interoperability mode is not the only solution for migrating from a MetaFrame 1.8 environment to MPS 3.0. Citrix's recommended solution is to implement a new MPS 3.0 farm and then migrate servers from the 1.8 environment to this new farm. Details on both options are covered in Chapter 6 .

Certain limitations do exist when MPS 3.0 servers are functioning in interoperability mode. These limitations are as follows:

- Licensing must be maintained for both environments. A user connecting to a 1.8 server consumes a 1.8 license, whereas a connection to an MPS 3.0 server consumes a 3.0 license. MF 1.8 servers cannot use the new MetaFrame Access Suite Licensing server.
- Although published application maintenance does work, Citrix strongly recommends that changes not be made to the configuration of existing published applications until all servers have been migrated to MPS 3.0 and interoperability is turned off.
- Any packages deployed using previous versions of the Installation Manager cannot be uninstalled using the new version supplied with MPS 3.0.
- Maintaining mixed mode support allows existing clients to possibly continue connecting to the environment using UDP broadcasts. This method of server location is not supported by default in an MPS 3.0 environment. Unless this option is explicitly enabled or clients are updated with new server location settings, such as TCP/IP+HTTP, after interoperability is deactivated, these users can no longer connect to the environment.
- While operating in mixed mode, users should not use the user-principal naming (UPN) method for logging on. The UPN format looks similar to an email address (<user name>@<domain name>). If a UPN name is used, authentication with an MF 1.8 server fails because these servers do not support logons with UPNs.

Interoperability is a powerful tool that can assist in the migration of an existing MetaFrame 1.8 environment. It is intended to be used only as a migration mechanism and not as a permanent implementation method.

## Exam Prep Questions

1. A small business owner wants to implement MetaFrame Presentation Server and wants to be able to use the load-balancing features of MPS. From the following list, choose the one product that most closely meets the needs of this customer.

A. MetaFrame Presentation Server 3.0, Standard Edition

B. MetaFrame Presentation Server 3.0, Small Business Edition

C. MetaFrame Presentation Server 3.0 with Load Balancing Option Pack

D. MetaFrame Presentation Server, Enterprise Edition

A1: Answer D is correct. The Enterprise Edition of MPS includes load-balancing support, a component also found in MPS Advanced Edition. Answer A is incorrect because MPS Standard Edition does not include the Citrix Load Manager component. Answers B and C are not actual MetaFrame platform solutions.

2. From the following list, choose the statements that do not accurately describe MetaFrame Presentation Server Access Suite Licensing. (Choose all that apply.)

- A. MASL must be installed on the same server as the data store.
  - B. For MASL to function properly, at least one MetaFrame server must be running IIS.
  - C. The installation of the Web Console for MASL is optional.
  - D. A single MASL server cannot pool client licenses for more than one MetaFrame server farm.
- A2: Answers A, B, and D are correct. Answer A is correct because MASL does not have to be installed on the same server as the data store. In fact, it does not interact in any way with the MetaFrame data store. Answer B is also correct because MASL requires IIS only if you want to use the web-based License Management Console, and in this case, IIS must be installed on the same server as MASL, not on another MetaFrame server in the farm. Answer D is also correct because a single MASL server actually can pool client licenses for more than one server farm.
- Answer C is the only truthful statement in this list. The Web Console, while a user-friendly management tool, is not required to implement MASL.
3. One benefit of MetaFrame Access Suite Licensing is that it now supports cross-farm license pooling, allowing a user accessing applications in multiple different farms to consume only one license. To configure cross-farm license pooling, what steps must be performed from the following list? (Choose all that apply.)
- A. Direct the farm or individual servers in a farm to use the desired license server.
  - B. Set the Multiple-Farm switch in the properties for MASL.
  - C. For each farm, ensure the Share Licenses option is enabled.
  - D. Reboot the MASL server.

A3: Answer A is the only correct answer. After a farm or server has been directed to a particular license server, it will start to share licenses with any other servers connected to that same server, regardless of what farm they may reside in. Answers B, C, and D are all incorrect. The listed options don't even exist, and a reboot is not required to configure a MetaFrame server to use a particular license server.

4. You have received the latest client image files and want to update the image files on your MetaFrame server. What tool would you use to accomplish this task?

A. The ICA Client Update Wizard

B. The ICA Client Rollout Wizard

C. The server's Update ICA Client Image button from the Client Images property page in the Management Console for MPS

D. The ICA Client Distribution Wizard

A4: Answer D is correct. The ICA Client Distribution Wizard is a utility that makes up part of the core MPS software and is used specifically for updating client image files and the update database for the ICA Client Update utility on the MetaFrame server. Answers A, B, and C are all incorrect and are not actual tools provided with MPS 3.0.

5. The Management Console for MPS is the main management tool for an MPS 3.0 environment. From the following list, select all the components that you would expect to find when running the Enterprise Edition of MPS. (Choose all that apply.)

A. Applications

B. Software Deployment Manager

C. Load Manager

D. Resource Manager

A5: Answers A and D are correct. Both Applications and Resource Manager are nodes that can be managed in the Management Console. Answer B is a fictitious name. Answer C is also incorrect. Even though Load Manager services are available in MPS Enterprise Edition, the particular component in the Management Console is not called Load Manager but is in fact called Load Evaluators.

6. Complete the following sentence: To limit a MetaFrame server to accept only published application connections, you need to enable the Allow Only Published Applications setting, located in the \_\_\_\_\_.

A. Terminal Services Configuration utility

B. Citrix Connection Configuration utility

C. Applications node of the Management Console for MPS

D. The Servers node of the Management Console for MPS

A6: Answer B is correct. To enable this setting, you must do so from within the Citrix Connection Configuration utility. Answer A is not correct. Although the Terminal Services Configuration utility allows you to modify many of the settings for both the ICA and RDP protocols, it does not specifically allow you to modify this setting. Answer C is also incorrect. The Applications node is the place where you manage the configuration of published content in your farm and the users who access this content. There is no mechanism for controlling connection settings from here. Answer D also is not correct. Although the Servers node would seem to be a logical place for connection management, it currently does not support configuration of any connection settings.

7. Your MetaFrame environment has servers distributed among three locations. You want to configure zone preference and failover for your users based on their current location. You do not want to enforce this based on their user ID because it is not uncommon for them to move between offices. Select the option that best describes how you would accomplish this task.

- A. Select the properties for the Application node, right-click and select Create New Configuration, choose Zone Preference and Failover, and then define the IP address ranges and associated settings that you want to configure.
  - B. Select the properties for the Servers node, right-click and select Create New Exception, choose Zone Preference and Failover, and then define the IP address ranges and associated settings that you want to configure.
  - C. Select the properties for the Policies node, right-click and select Create New Policy, choose Zone Preference and Failover, and then define the IP address ranges and associated settings that you want to configure.
  - D. Zone preference and failover settings can only be configured based on the user's ID.
- A7: Answer C is correct. Zone Preference and Failover is one of the settings defined as a custom MetaFrame policy and can be assigned based on the client IP address or range, ICA client name, MetaFrame server name or User ID, or group membership. By implementing a policy based on an IP address range, you can ensure that the particular policy is applied only for users connecting from that particular address range.
- Answers A, B, and D are all incorrect. Zone preference and failover information is not configured within the Applications or Servers nodes, and these options can be assigned based on more than just the user's ID.
8. You have just finished installing and configuring the Web Interface for MPS. You want to allow users to access their published applications through this interface. Choose the answer that best describes the steps that you must take to allow this to happen.

- A. Select the applications that you want to access through the Web Interface Management Console.
    -
  - B. You don't need to do anything. Published applications are automatically available through the Web Interface.
    -
  - C. Enable the Show in Web Interface property for each of the appropriate published applications. You can do this either when it is created or when you are modifying the properties for the application.
    -
  - D. Published applications are not accessible through the Web Interface. You must configure them separately using the Management Console for the Web Interface.
- A8: Answer B is correct. Published applications are automatically available using any number of ICA client devices and interfaces. The Web Interface is no exception. Answers A and D are both incorrect because the Web Interface is not responsible in any way for manipulating what published applications are accessible through the web browser. All this is determined through published applications and access control lists. Answer C is incorrect because no such option exists in the application configuration.
9. You have just returned from vacation to find that your assistant has implemented MPS 3.0 into your existing MetaFrame 1.8 environment. Instead of introducing a separate farm, he has chosen to leverage interoperability mode and currently has Microsoft Office published on two MPS 3.0 servers and three MF 1.8 servers. He is having an issue with load balancing that he desperately wants to fix. He is trying to configure load balancing based on memory and CPU usage, but he finds that users are being directed to the one highly loaded MPS 3.0 box even though other MPS 3.0 and MF 1.8 machines have lower CPU and memory utilization. Why is this not working?

- A. The advanced load-balancing features are supported only with the MPS 3.0 servers. All the MF 1.8 servers use their load-balancing services, and the new servers use the advanced load evaluator he has created.
  - 
  - B. When applications are published on both types of servers, the MPS 3.0 server is always chosen before the MF 1.8 server, unless the MPS server has reached full load. This is done to encourage users to migrate to MPS 3.0 more quickly.
  - 
  - C. When operating in interoperability mode the advanced load evaluators are ignored and the MF 1.8-compatible load-balancing services are used by all servers.
  - 
  - D. Citrix does not support the use of advanced load evaluators with MF 1.8, and the company warns that unpredictable results can occur.
- A9: Answer C is correct. To ensure compatibility between the two server types, interoperability mode allows only the load-balancing services supported by MetaFrame 1.8 to be used. This load configuration applies to both MF 1.8 and MPS 3.0 servers. Advanced load evaluators cannot be used until interoperability mode is turned off. Answers A, B, and D are all false statements.
10. To use Installation Manager, you must have what mandatory components identified and configured? Choose the answer that lists the components required to use Installation Manager.
- - A. Package Management Server, Network Share Point Server, Package Server, and Target Servers
  - 
  - B. Package Management Server, Package Server, and Target Servers
  - 
  - C. Package Management Server and Package Server
  - 
  - D. Package Management Server, Network Share Point Server, and Target Servers

A10: Answer D is correct. The only optional component is the Package Server, which is required only when creating your own custom ADF packages for deployment. Otherwise the package management server, network share point server, and target servers must be identified and configured appropriately.

 PREV

NEXT 

 PREV

NEXT 

## Need to Know More?



Citrix Systems, "Getting Started with MetaFrame Presentation Server." Available online at <http://support.citrix.com/docs>, and from the online documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.

 PREV

NEXT 

## 2. MetaFrame Presentation Server Architecture

Terms you'll need to understand:

- Independent Computing Architecture (ICA) protocol
- Independent Management Architecture (IMA) protocol
- SpeedScreen technology
- MultiWin
- Data Store
- Local Host Cache (LHC)
- Data Collector
- Virtual channels
- Zones

Concepts you'll need to master:

- Understanding the IMA protocol and its components
- Understanding the benefits of SpeedScreen technology
- Identifying the components of the ICA packet
- Understanding zones, Data Collectors, and their elections
- Understanding the Data Store

# Independent Computing Architecture

The Independent Computing Architecture (ICA) protocol is a presentation layer protocol on the Open System Interconnection (OSI) model and is the engine by which ICA clients and MetaFrame (MF) servers communicate data. It was designed by Citrix systems to be a powerful multichannel protocol that can exchange data over network bandwidth as low as 10 to 20Kbps. The protocol is fine-tuned to enhance the experience of users connecting from remote locations to the servers. The ICA protocol is made up of three components:

- Network The ICA protocol can use a variety of transport protocols to communicate data between ICA clients and MetaFrame servers. These protocols include TCP/IP, IPX, SPX, and NetBIOS.
- Server In a server-based computing environment, which MetaFrame is part of, the logic of the application is completely run on the server. This means that the CPU, memory, and disk input/output (I/O) of the servers are taxed and heavily utilized. Only screenshots showing what is happening on the server are transmitted back to the client. The client only interacts and manipulates the user interface (UI) of the application, but all the commands, keyboard strokes, and mouse clicks are executed on the server side.
- Client Because the logic of the application is executed on the remote server, all the client really needs to be able to do is view and interact with the application's UI. Today, ICA clients exist for almost any type of hardware device from Pocket PCs to laptops to traditional desktops. ICA clients also exist for almost any type of operating system from Windows to Linux, Unix, and Macintosh.

## ICA Packet

Let's break down the ICA packet and see how it is composed and encapsulated before it is sent to a transport protocol for delivery between servers and clients. The ICA packet is composed of one required byte known as Command and of several optional bytes that are used as necessary to meet certain criteria. Here is a list of the optional bytes and their uses:

- Frame Head An optional byte that is added whenever a streaming transport protocol is being used, such as TCP or Async. These protocols do not send the ICA packet as a single entity but rather split it and stream it in smaller bits; as such, they require a Frame Head that marks the beginning of the transmission and also require a Frame Trail that marks the end of the transmission to the receiving device.
- Reliable An optional byte that offers reliability. In the event that your chosen transport protocol is unreliable such as IPX, which has no method of verifying whether a packet sent has actually reached its destination you can ensure reliable delivery with this byte. In this case, the reliability byte is added to the ICA packet to ensure error-free communications between the server and the client.
- Encryption An optional byte that is used whenever encryption is configured. MetaFrame supports different levels of encryption between the servers and the client, and this byte carries the encryption information across the wire.

- Compression An optional byte that is added to manage packets that use compression.
- Command Data An optional byte that is associated with the command byte.
- Frame Trail An optional byte that is added whenever a streaming transport protocol such as TCP or Async is used; it functions as the last bit to be received. This byte ensures that all the data between the Frame Head and the Frame Trail have arrived at the destination error free.

## Note

The Command byte is the beginning of the base ICA packet. It is the only required byte that is always present in the ICA packet.

## Virtual Channels

Virtual channels are a mechanism by which MetaFrame extends its features and functionality. Using virtual channels, the ICA protocol can offer ICA clients audio and video support, among other things, without impacting performance. Virtual channels can be used to deliver audio or video that is running on the MetaFrame server through speakers attached to the ICA client device. On the opposite side, they can map devices that are physically attached to ICA clients and give the user access to these devices as if they were attached to the MetaFrame server. Virtual channels can provide one-way communication between the ICA client and the MPS server or can be a two-way communication process between the client and server.

For the ICA protocol to deliver these services and maintain the same level of performance, it bundles several virtual channels together in one ICA packet and sends them across the communication link. This technique ensures that transmission is less frequent, which conserves network bandwidth. By using this technique, the ICA protocol avoids sending an ICA packet for every virtual channel and keeps itself thin and light. The default virtual channels available with the ICA protocol include

- Audio Transports the audio that an application running on the MF server generates and delivers the sound through the speakers attached to the local ICA client device.
- SpeedScreen Control Maintains transmission of SpeedScreen data between the server and the client.
- Drive Mapping Displays the ICA client's local hard drives through the MPS server.
- ICA Display Transmits the UI of an application from the MPS server to the ICA client.
- Font and Keyboard Layout Ensures that the client and server font and keyboard layouts do not differ and, in the event that they do, unifies them.
- Clipboard Mapping Makes it possible to share the Clipboard between the server and client. So if you copy on the server, you can paste on the ICA client and vice versa.
- Printer Spooling Sends printer spooler data from the MF server to the ICA client.
- Serial Port Managing Allows the ICA session access to its local serial ports located on the ICA client.

- Parallel Port Managing Allows the ICA session to access the parallel ports of the ICA client.

## Note

The ICA protocol can support up to 32 virtual channels in one packet.

 PREV

NEXT 

## MultiWin

MultiWin, a technology developed by Citrix Systems, originally created the concept of Terminal Server on the Win32 platform. It allows multiple simultaneous users to log on to a Terminal Server, run applications, and share resources such as the CPU, memory, and I/O ports.

Microsoft's first release of Terminal Server was Windows NT 4.0 Terminal Server Edition (TSE), which was built on Citrix's MultiWin technology. Prior to Windows NT 4.0 TSE, Microsoft had licensed Windows to Citrix. Previously, Citrix offered WinFrame, which was essentially a multiuser operating system based on Microsoft Windows NT 3.51.

# SpeedScreen Technology

SpeedScreen is a technology developed by Citrix to improve the responsiveness of published applications and desktops over slow communications links. Server-based computing, in general, is always hungry for more network bandwidth because it is essentially the mechanism that makes the concept possible. On local area networks (LANs) or wide area networks (WANs) that have enough network bandwidth, performance is never an issue, and to the end user, everything seems to run perfectly. However, when you deal with slow network connections, you need to take some additional measures. Even though Citrix has made many advances by tweaking the ICA protocol and compressing the data so that it can travel the communications link faster, the frequency of the client screen updates can consume a significant amount of bandwidth and slow down the session. Just imagine what the impact on bandwidth would be like if every pixel on the screen needed to be re-created and retransmitted every time you moved your mouse around or double-clicked an icon or used your keyboard.

To alleviate this frequent transmission of screen updates, Citrix designed a technology, known as SpeedScreen, that improves the performance of slow sessions by at least four times over sessions that do not use SpeedScreen. SpeedScreen works by transmitting only the part of the screen that has changed. For example, assume that you hovered your mouse in the lower-right corner of the screen over the clock. SpeedScreen then compares your mouse movements to the last screen refresh it sent you and determines that only the lower-right corner of the screen has changed and thus refreshes just that part of the screen instead of resending the entire screen.

## SpeedScreen Latency Reduction

The robustness of SpeedScreen and its performance benefits have led Citrix to improve the technology further and add new features to the SpeedScreen family. SpeedScreen Latency Reduction is the name given to two SpeedScreen features: Local Text Echo and Mouse Click Feedback.

### Local Text Echo

Local Text Echo works on slow communications links such that when the user is entering data or using the keyboard to interact with the application, the response to the user's input lags behind the keyboard strokes. For example, if Joe is using a word processing application and is typing a memo, the letters may not appear on the screen at the pace he is typing, but rather seconds or even minutes later depending on the lag. This lag frustrates the user, forcing him to wait for the text to update before he can continue typing.

Local Text Echo addresses this issue in particular. If Local Text Echo is enabled on the server, as soon as a session is established between the ICA client and the MetaFrame server, the server pushes a series of screen images and basic fonts. As the user Joe is typing, Local Text Echo uses these initial screen images and fonts to keep up with his pace. In most cases, the user will not know the difference as he is typing and before the server has time to process the data and send the correct font and images. Local Text Echo intercepts the keyboard strokes and populates the input using the fonts that were transferred at connection time.

In the background, this feature gives the server time to process the data and send the correct information back to the client. The data is then refreshed. All this is seamless to the user. In rare

cases, if Local Text Echo cannot detect the font the user is using, it populates the screen with boxes or circles, basically informing the user "I acknowledge you are typing something, but I just don't know what it is yet." After the server receives and processes the data, it sends the data back to the client, and the boxes or circles are replaced with the proper fonts.

## Mouse Click Feedback

Mouse Click Feedback is also enabled at the server level and is used to remedy the lag that occurs between the time a user double-clicks an icon and the time needed to process this action and reflect it on her screen. Many times, users double-click an icon, and if they don't get a response immediately as they are used to with applications running locally on their machines, they assume the command did not register and attempt to double-click again and again. Mouse Click Feedback intercepts the command before it gets to the server. It then changes the cursor to an hourglass, telling the user "I know you double-clicked the icon. Don't double-click again because I am processing your command." As soon as the command is processed and sent back, the application is launched and the mouse pointer is changed back to its original shape.

We discuss how to configure SpeedScreen latency reduction on the server side in [Chapter 6](#), "Configuring and Administering MetaFrame Presentation Server," and on the client side in [Chapter 13](#), "Citrix ICA Client Software."

## SpeedScreen Browser Acceleration

SpeedScreen Browser Acceleration was designed specifically for web applications. It has a special compression algorithm that improves the performance of GIF and JPEG images in HTML pages. Applications such as Microsoft Internet Explorer, Microsoft Outlook, or Outlook Express can take advantage of this technology by presenting the user with the text on the page first and then gradually displaying the image as the packets arrive until the image is composed. We discuss how to configure this feature in greater detail in [Chapter 6](#).

## SpeedScreen Flash Acceleration

SpeedScreen Flash Acceleration addresses performance issues with Flash animations, which may run slow on a MetaFrame server. With the introduction of this technology, Citrix uses a technology known as *Lossy Compression*, which essentially reduces the size of the images in the animation, speeding up its delivery to the client. It does this by removing some of the image data reserved for advanced photo editing. Because this data is removed, the image size is reduced, and the flash animation is displayed quicker, improving performance. We discuss how to configure this feature in greater detail in [Chapter 6](#).

## SpeedScreen Multimedia Acceleration

SpeedScreen Multimedia Acceleration tackles streaming audio and video through an ICA session. When this feature is enabled, streaming media runs as smoothly as it does when run locally. SpeedScreen Multimedia Acceleration compresses the packets sent across the link and makes the client's CPU do all the processing instead of having the server CPU do it. This feature puts very little stress on the server CPU and does not require significant network bandwidth. We discuss how to configure this feature in greater detail in [Chapter 6](#).

**◀ PREV**

**NEXT ▶**

# Independent Management Architecture

Independent Management Architecture (IMA) is a unifying architectural framework for previously independent technologies and processes. The IMA protocol offers a platform for future Citrix products to plug into and utilize. It also offers scalability and centralization. It is the mechanism by which MetaFrame server-to-server communication occurs. Let's look at some of the features that were collapsed into the IMA from earlier versions and also look at what the IMA offers today.

## Centralized Administration

Centralized administration is at the core of the IMA, and no enterprise solution would be complete without a centralized management process, which is exactly what the Presentation Server Console does. This Java-based console uses the IMA protocol, gathers information from MetaFrame servers, and allows the user to make changes on a farmwide basis. It incorporates utilities that were standalones in MF 1.8 and earlier, such as Citrix Server Administrator. Today, you can configure and view Resource Manager counters and run reports, also previously standalone tools. You can configure Load Evaluators and Citrix policies as well.

## Data Store

The Data Store is a database that stores all the configuration information needed by the Citrix farm. Any time you make configuration changes to a MetaFrame server, the changes are recorded in the Data Store. In this respect, if you are adding a new MetaFrame server to spread the user load of an application, this new server can get all its information by tapping into the Data Store. The information stored in the Data Store includes

- Published Application Includes the name of the application and any configurable property available through the Management Console.
- Server Configuration Includes all the configuration information made through the Management Console.
- User Configuration Includes the MetaFrame administrators and any sort of user configuration configurable through the Management Console.
- Print Environment Includes the entire configuration you make through the Management Console. This includes print driver information and any configurable option under the Print Management node in the Management Console.

## A Blast from the Past

How does the Data Store differ starting with MetaFrame XP, and how did MetaFrame 1.8 handle this information? Prior to the IMA Data Store, all the pieces of configuration information from the preceding list were stored in the Registry of every server. As a server came online and loaded its Registry, it then broadcasted its changes to all the other servers in the farm. Any time the data changed on one server, it was broadcasted over User Datagram Protocol (UDP) to all the other servers in the farm.

In addition, the ICA Browser held a shadow copy of this information in its memory as well. All this generated a lot of network traffic, in addition to simply being a bad and very error-prone method as it was. Now, with the IMA Data Store, all the servers talk to the Data Store, which acts as a centralized repository for the entire farm. This reduces the amount of network traffic dramatically and also protects the information in a database, where it should be. If a server goes down or if a new one is brought into production, as soon as they connect to the Data Store, they gain access to the necessary configuration they need to fulfill their role.

### Alert

Prior to MetaFrame Presentation Server 3.0, licensing information was also stored in the Data Store. With the advent of MetaFrame Presentation Server (MPS) 3.0, licensing is stored on the Citrix Licensing Server.

### Note

All the information stored in the IMA Data Store is manipulated through the Management Console.

## Local Host Cache

Local Host Cache (LHC) is an Access database that is located on every MetaFrame Presentation Server and that holds a smaller version of the Data Store. It carries enough information to keep the server running in the event that the main Data Store should become unavailable for any reason. The Local Host Cache is located in `C:\Program Files\Citrix\Independent Management Architecture\IMALHC.MDB`. As changes are made to the IMA Data Store, the MetaFrame servers are notified of this change, and they, in turn, update or refresh their Local Host Cache database with the updated information. The LHC contains information about published applications in the farm and the servers that host them.

### Note

If the Data Store goes offline, the server continues to function normally using the Local Host Cache database for up to 48 hours. After 48 hours, if the server does not re-establish connectivity to the Data Store, its licenses expire, and the server refuses client connections.

## Zones

Zones provide a way of grouping geographically close servers to save network bandwidth and also improve performance. Every zone elects one Data Collector, which every server in that zone reports to. If the servers are in the same zone but are geographically very dispersed, significant network bandwidth is constantly used because the servers constantly talk with the DC and vice versa. This is why it is recommended that you group your servers in zones based on their location.

## Data Collectors

Data Collectors (DCs) are responsible for keeping zone-specific information. Every zone has one elected server that acts as the DC and maintains information gathered from all the servers in that zone, information such as server user load and active and disconnected sessions. Every MPS server in the zone will notify the DC of its changes every 60 seconds.

### Zone-to-Zone DC Communications

Prior to MetaFrame Presentation Server 3.0, every Data Collector in every zone communicated its information to other Data Collectors in other zones. With MPS 3.0, this capability has been disabled by default to preserve network bandwidth. This change was prompted because large organizations suffered network bandwidth problems due to the constant replication of information between DCs in different zones.

This change, however, comes at a cost. If a user now wants to connect to an application that is located outside his or her primary zone, the DC for that user's zone needs to request information from the DC in the other zones, and as such, application launch times may be delayed a bit.

To get around this delay, whenever you have more than one zone, you should configure the Zone preference and failover policy in the Policies node discussed in greater detail in [Chapter 7](#), "MetaFrame Presentation Server Policy Management."

We do, however, go over it briefly here just to get the idea across. With the Zone preference and failover policy, you can set a preferred primary and backup zone. Because Citrix policies can be applied to users, servers, client names, and client IP addresses, what you should do when you have more than one zone is create a policy for each zone. For example, you would create policy1, which would be applied to the client IP range of users at a particular location so that their preferred zone is their native zone and their backup zones are all the other zones. In this case, whenever these users need to access an application in a different zone, they would be able to query the backup zone. You would then create another policy for users at different locations doing the same thing for them.

## Alert

MetaFrame Presentation Server 3.0 introduced changes in the way zone DCs communicate with each other. This change will most likely make it on the exam in the form of a question or two. Make sure you understand this new change and why it was implemented.

## Data Collectors, Elections, and Priority

Every zone needs to hold TCP elections to determine which server is to become the zone DC. The election criteria and process are similar to the election of the Master ICA Browser in MF 1.8 and follow the same guidelines. The server with the highest priority wins the elections. Elections are held any time one of the following events occurs:

- You manually change the memberships of a zone or any time you make a change to the zone's election criteria within the Management Console.
- You manually trigger an election using the command `querydc -e`.
- An MPS server loses connectivity to the zone DC.
- A new MPS server is brought online.
- The zone DC is shut down or goes offline for any reason.

Election priorities are as follows:

- Most Preferred This is the favorite server; it always wins the election.
- Preferred This server is a favorite among others to win an election.
- Default Preference This server is neutral and can be selected to become a DC but is not a preferred candidate.
- Not Preferred This server should never win an election unless it is the only server in the zone or all the other preferred servers are unavailable.

As with any election, the DC elections can also be tampered with by an administrator. You can give each server in the farm the status that you see fit for its role via the Management Console, as you see later in [Chapter 6](#).

Data Collector elections are triggered if any of the following actions occur:

- The Data Collector goes offline.
- A new server is introduced into the farm.
- A server in the zone loses communication with the DC.
- A DC election is manually forced using the `querydc -e` command from a command prompt.
- The zone information and configuration changes such as the zone name, zone server memberships, or server priority settings change.

## IMA Subsystems

IMA subsystems are similar to plug-ins: They are core technologies that plug into the IMA and take advantage of its architecture. This architecture is the framework that unifies existing Citrix products and is the blueprint that Citrix will use in the future when developing new products to help integrate them all together. Currently, the IMA manages the following subsystems:

- ICA Browser Provides backward compatibility. Its services come into use only when the farm is in mixed mode to offer older MF servers UDP broadcast capability.
- Server Management Handles user sessions.
- Application Management Manages published applications and their related information.
- Runtime Offers services such as zone management and Data Collector.
- Persistent Storage Updates the local host cache on every MF server from the Data Store.
- Distribution Manages file transfers between different subsystems.
- Remote Procedure Call Allows external processes to communicate with IMA.
- User Management Provides authentication and security.
- Printer Management Allows for printer administration.
- Licensing Manages and enforces Citrix licensing guidelines.
- [Program Neighborhood](#) Handles PN communications with ICA clients.
- Load Management Handles load information and management.

## Listener Ports

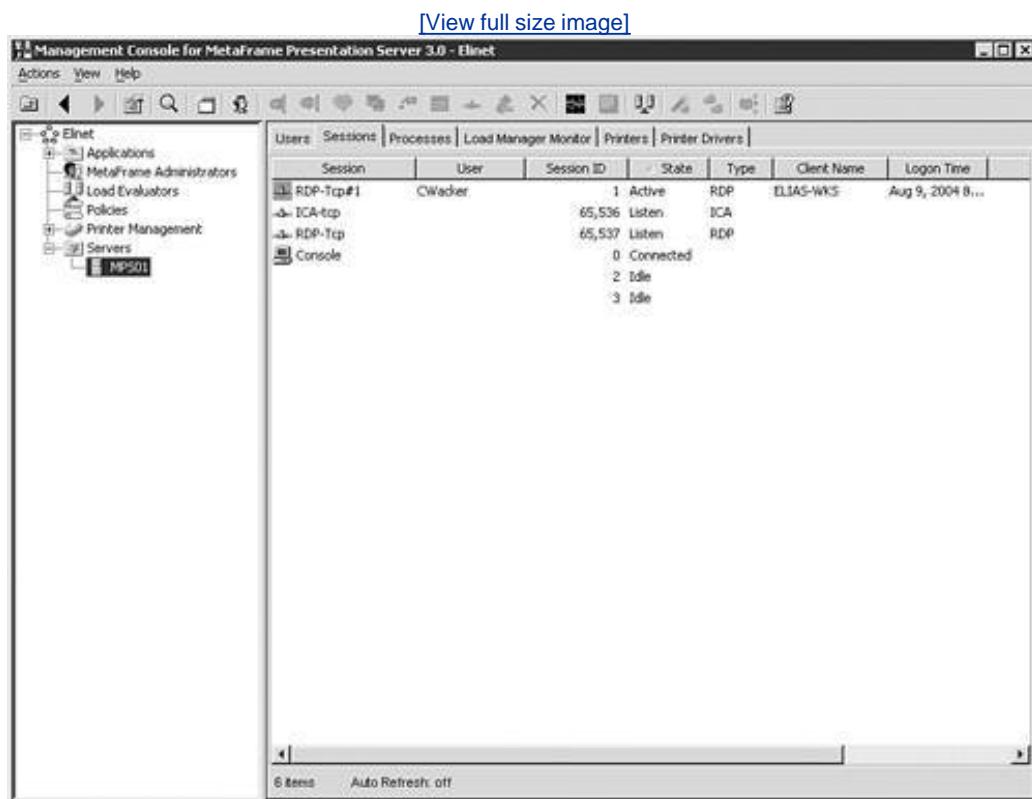
A listener port for every transport protocol is created automatically as soon as Terminal Services is installed. This service's sole function is to listen to and detect clients attempting to connect to the Terminal Server or, in this case, to the MetaFrame servers. After it establishes a connection with a client session, it then proceeds to connect that client with an idle session on the server. Think of the listener port as a host at a restaurant. A restaurant is always waiting to receive, greet, and seat customers, after which a waiter or a maitre d' serves them. The same thing is true of a listener port: It listens for, detects, and initiates contact with incoming client sessions and connects them with an available idle session for servicing.

### Note

One listener port exists for every transport protocol that is installed on the server, such as TCP or IPX.

You can view the listener port by opening the Management Console for MPS 3.0 and clicking on a server from the Servers node in the left control pane. Click the Sessions tab in the right control pane, as shown in [Figure 2.1](#). You can see the listener port under the State column.

Figure 2.1. Windows 2000 view of the listener port and idle sessions.



## Tip

If users experience problems connecting to or establishing a session with an MPS server, you can try resetting the listener port in an attempt to remedy the problem. Right-click the listener port in the Management Console and click Reset.

## Idle Sessions

On Windows 2000 servers, when Terminal Services is installed in Application Server mode, every transport protocol has two idle sessions created by default. The primary function of these idle sessions is to accept an incoming connection from the listener port and turn it into an ICA session. Every time one of these two idle sessions is turned into an ICA session, a new idle session is created and awaits a connection. Following up on the example we used for listener ports, idle sessions can be considered the waiters or maitre d's that serve the customers the host or listener ports seated. Now the same way a busy restaurant may require more waiters and more maitre d's to service its customers, sometimes you may need to increase the number of idle sessions available to handle peak logon times. In large

organizations, especially in the morning hours when all the users are trying to connect, the server does not have enough time to create a new idle session. Thus, some of your users may not be able to connect right away and will be required to try again.

For this reason, large organizations that have users in the thousands are advised to add more idle sessions to cope with heavy logon attempts. You can do this by editing the Registry in the following location: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\idlewinstationpoolcount`. Modify the value accordingly. It is recommended that you add these idle sessions in multiples of two.

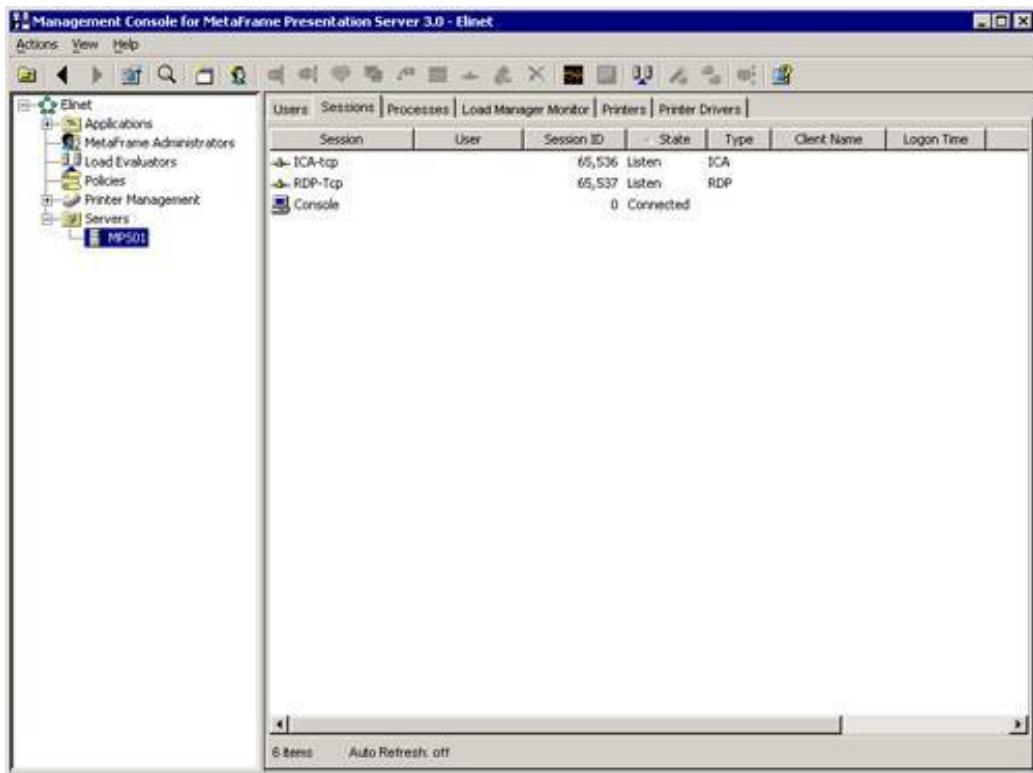
## Tip

For performance reasons, it is recommended that you do not exceed a total 10 idle sessions. The more idle sessions you create, the more memory and other server resources are consumed.

In Windows Server 2003, Microsoft changed the architecture of Terminal Server a bit. The two idle sessions that were created by default for every transport protocol have disappeared. The functionality remains the same, but the connection from the listener port to the idle session has been made a seamless one. In addition, you can no longer control how many idle sessions exist, and the Registry key mentioned earlier has no effect on it. As you can see in [Figure 2.2](#), a Windows Server 2003 server does not show the idle sessions anymore. Compare this figure to [Figure 2.1](#), which clearly shows a Windows 2000 server with the idle sessions.

Figure 2.2. Windows Server 2003 no longer has idle sessions.

[\[View full size image\]](#)



## ICA Sessions

As we mentioned earlier, as soon as an incoming connection is connected with an idle session, it then proceeds to make that session into an ICA session. The state of the session is immediately changed to ConnQ, which means it is in the process of being connected. It then changes its status again to Conn after a connection with the MF server has occurred, and it changes its status one final time after the connection is successful and the session state becomes Active. It remains Active as long as the user is using the application with no problems.

A session may go into the following different states:

- Listen The listener port is listening for any connection attempts.
- ConnQ The session is in the process of being connected with a MetaFrame server.
- Conn The session has established a connection with the MetaFrame server.
- Active The session has successfully logged on to the server and can now be used by the user.
- Idle The session is idle and is awaiting a connection transfer from the listener port.
- Disc The session is in disconnect mode, which means it has not logged off the server but has been disconnected from the ICA client.
- Shadow The ICA session is shadowing another session.
- Down The listener port has not initialized successfully and is down. Also, when a session has been lost, it changes to a down state.
- Init The ICA session port is initialized.

## **Published Application Discovery Process**

Back in the MetaFrame 1.8 days, whenever an ICA client requested information or queried the farm for published applications, it broadcasted a message via UDP port 1604. A Master ICA Browser residing in the same subnet as the client requesting the information responded to the request. Now if an ICA client computer that is broadcasting the request does not have a browser gateway configured, it can view only information that the Master ICA Browser in its same subnet carries, thereby getting only a partial listing.

Beginning with MetaFrame XP 1.0 and later, Citrix solved this problem by storing all the information in the IMA Data Store and then replicating it to the Local Host Cache on every MF server. It also eliminated the need for the UDP broadcast and replaced it with IMA. Now when an ICA client queries any server, a full list of published applications is provided.

## **SNMP**

Simple Network Management Protocol (SNMP) is known and widely used by various organizations for the purposes of monitoring their systems. Companies can use third-party tools such Microsoft Operations Management (MOM), HP OpenView, or various other tools to monitor and manage their servers. In addition, if you are using the Enterprise Edition of MetaFrame, you can use Citrix Network Manager as an SNMP agent to gather farmwide performance monitoring and management information.

## **Auditing Shadowed Sessions**

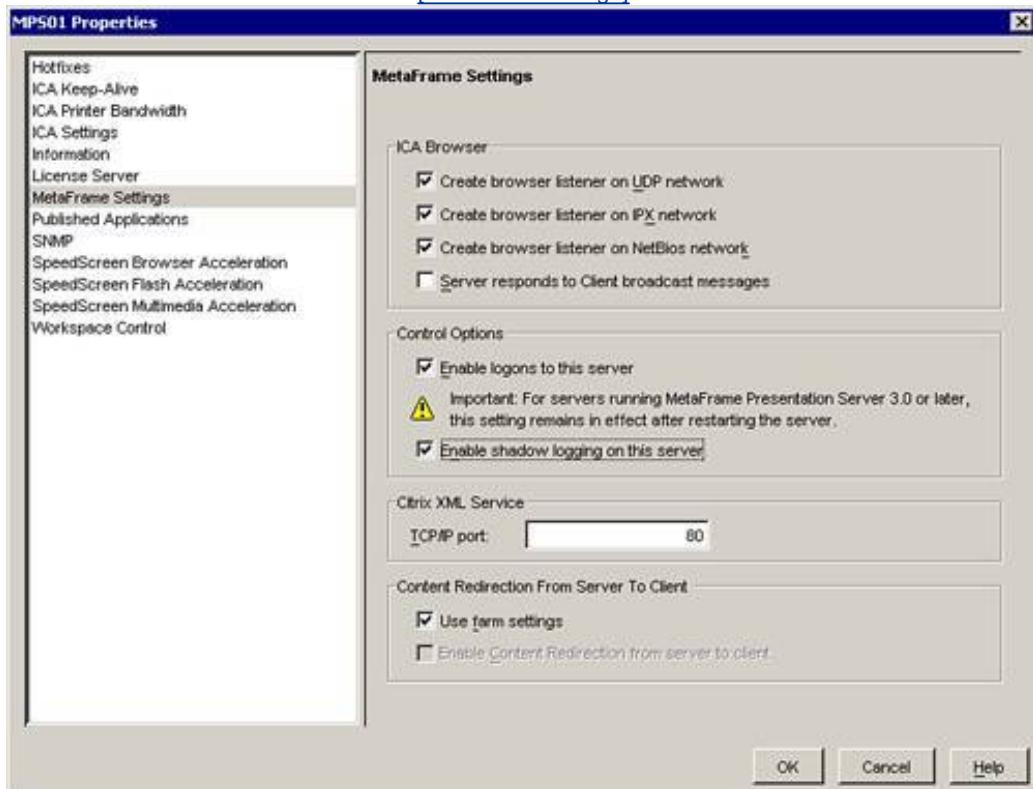
Shadowing is probably one of the most useful troubleshooting tools available to administrators, engineers, and helpdesk technicians alike. It allows a technician to remotely view and interact with a user's session. However, this tool can also be potentially misused by nosy or malicious users and technicians. Therefore, many companies that implement shadowing require a way of monitoring its usage to ensure no one is using the tool other than in its intended framework.

When you enable shadow auditing, every time a session is shadowed, an event is logged in the Event Viewer on the Windows Server specifying the shadowing and shadowed sessions. Shadowing is not enabled by default on the servers. To enable it, follow these instructions:

1. Open the Management Console.
2. Select a server from the Servers node in the left control pane.
3. Right-click it and select Properties.
4. Select MetaFrame Settings and check the box next to Enable Shadow Logging on This Server, as shown in [Figure 2.3](#).

Figure 2.3. Enable Shadow Logging.

[View full size image]



◀ PREV

NEXT ▶

## Exam Prep Questions

1. How many idle sessions are created by default on a Windows Server 2003 server with MetaFrame Presentation Server 3.0 installed?

- A. 2
- B. 4
- C. None
- D. 6

A1: Answer C is correct. On Windows Server 2003, Microsoft changed the Terminal Server architecture, so idle sessions are no longer created. On Windows 2000, two idle sessions are created by default.

2. What type of information does a zone Data Collector store? (Choose all that apply.)

- A. Server load information
- B. Connected user information
- C. Published application information
- D. Printer information



E. Disconnected user information

A2: Answers A, B, and E are correct. A Data Collector stores information about server load so that it can direct users who are connecting to the farm to the least busy server. It also keeps track of connected and disconnected users. Choice C is incorrect because Data Collectors do not store published application information. Choice D is incorrect because DCs don't store printer information.

3. On a Windows Server 2003 server with MetaFrame Presentation Server 3.0 installed, if you have both TCP and IPX transport protocols loaded, how many listener ports are available?



A. 1



B. 2



C. None



D. 4

A3: Answer B is correct. Every transport protocol has a listener port created by default: in this case, one listener port for TCP and one for IPX.

4. If you are using TCP/IP on your network, which headers will be added to the ICA packet? (Choose all that apply.)

A. Frame Head

B. Reliability

C. Compression

D. Security

E. Frame Trail

A4: Answers A and E are correct. TCP/IP is a streaming protocol and, as such, requires a Frame Head to mark the beginning of the transmission and a Frame Trail to mark the end. Choice B is incorrect because Reliability is added to a nonreliable protocol such as IPX; TCP is a reliable protocol and does not need this. Choice C is incorrect because it is not relevant to TCP/IP. Choice D is incorrect because it is not relevant to TCP/IP.

5. What is used for server-to-server communications in MetaFrame Presentation Server 3.0?

A. TCP + HTTP

B. IMA

C. TCP 1494

D. DNS

A5: Answer B is correct. With the introduction of MetaFrame XP, the Independent Management Architecture, or IMA, is used for server-to-server communications. Choices A, C, and D are incorrect because they are not the method by which server-to-server communication occurs.

6. Which two components make up the SpeedScreen Latency Reduction technology?  
(Choose all that apply.)

A. Mouse Click Feedback

B. Local Text Feedback

C. Mouse Click Response

D. Local Text Echo

A6: Answers A and D are correct. Mouse Click Feedback and Local Text Echo are the two components that make up the SpeedScreen Latency Reduction technology. Choice B is incorrect because there is no such thing as a Local Text Feedback. Choice C is incorrect because there is no such thing as Mouse Click Response.

7. Every MetaFrame server has an Access database that contains a portion of the Data Store used to keep the server functioning in the event of a Data Store failure. What is this database called?

A. Local Data Store Cache

B. Local Host Database

C. Local Host Cache

D. Local Store Cache

E. Local Data Cache

A7: Answer C is correct. The Local Host Cache is the name of the Microsoft Access database that is created locally on every MPS server and that stores portions of the Data Store to keep the server functioning in the event of an outage. Choices A, B, D, and E are incorrect because there is no local Data Store Cache, Local Host Database, Local Store Cache, or Local Data Cache.

8. At which layer of the OSI model is the ICA packet built?

A. Application

B. Session

C. Presentation

D. Network

E. Transport

A8: Answer C is correct. ICA is a Presentation layer protocol, and as such, the ICA packet is built at the Presentation layer. Choice A is incorrect because the Application layer is not the layer at which the ICA packet is created. Choice B is incorrect because the Session layer is not the proper level at which the ICA protocol is created; the Session layer handles session reliability and management. Choice D is incorrect because the Network layer deals with protocols such as IP. Choice E is incorrect because the Transport layer deals with the way to get packets from point A to point B and, as such, deals with transport protocols such as TCP.

9. What event triggers a Data Collector election?

A. A new server is added to the farm.

B. A server is rebooted.

C. The Data Collector goes offline.

D. A server is shut down.

E. All the above.

A9: Answer E is correct. All the choices trigger a Data Collector election.

10 In an ICA packet, which is the only required byte?

A. Command Data

B. Frame Head

C. Security

D. Command

A10: Answer D is correct. The Command byte is the only byte in the ICA protocol that is always present. Choice A is incorrect because it is an optional byte, not a required one. Choice B is incorrect because it is an optional byte. Choice C is incorrect because it is neither an optional nor a required byte; it is simply wrong.

# 3. Installation Prerequisites for MetaFrame Presentation Server 3.0

Terms you'll need to understand:

- Terminal Services Licensing
- Terminal Services Client Access Licenses (TSCALs)
- Citrix Connection Licenses
- Application Server mode
- Remote Administration mode
- Remote Desktop
- Citrix Migration License
- Citrix Upgrade License

Concepts you'll need to master:

- Direct access to the Data Store
- Indirect access to the Data Store
- Installing Terminal Services in Application Server mode in Windows 2000 Server
- Installing Terminal Server in Windows Server 2003

As much as we would love to tell you to just place the MetaFrame software in the CD-ROM, install it, and you'll figure out what you need to do as you go, we can't. With complicated systems that host hundreds of users, as is the case with MetaFrame Presentation Server, that approach can quickly turn into a recipe for disaster. Sure, you can install a graphics program and figure it out as you go, but thin client solutions require careful planning and educated design approaches.

In this chapter, we cover the necessary prerequisites that should be met prior to your attempting to install MetaFrame Presentation Server 3.0. In addition to the hardware and software requirements, we cover licensing and the types of licenses involved in this process. Although you probably don't need to know the ins and outs of licensing, you should know what is required for your environment and what can break from not providing proper licenses.

# Licensing Requirements

Licensing is easily the most complex subject in a server-based computing environment. The reason is not that the topic is hard to understand but that the vendors are constantly changing the requirements, and with frequent operating system upgrades and application upgrades, figuring out how to stay compliant is always a challenge. In this chapter, we briefly touch on the requirements because going into detail is beyond the scope of this book, which concentrates on the Citrix Certified Administrator exam.

You need to familiarize yourself with two major components: server licenses and client licenses. Let's tackle the server licenses first.

## Server Licenses

The first component to license should be the server operating system that will host all the other applications installed on it. It is important to understand what needs to be licensed on a Windows 2000 Server and Windows Server 2003 OS to avoid connection issues later.

Both Windows 2000 Server and Windows Server 2003 have the same licensing requirements with different upgrade paths. It is best to consult your Microsoft representative to ensure you are abiding by the Microsoft guidelines for Terminal Server (TS).

Two types of licenses are required when you are running Terminal Services with Citrix MetaFrame Presentation Server 3.0:

- *Windows 2000/2003 Server License* This is the core product license, the base Windows server operating system. You need a license to install the operating system.
- *Citrix MetaFrame Presentation Server 3.0 Server license* A license is required to install the MetaFrame server software. The nice thing about Citrix MetaFrame is you have to buy only one copy of the MetaFrame Presentation Server product. After you own a license, you can install it as many times as you want on as many servers as you like. The catch is that Citrix wants to charge on the connection licenses, which we discuss in the next section, instead of charging every time you install the server product.

## Client Licenses

After tackling the server licensing requirements, we arrive at the client licensing requirements. Every client that accesses a Microsoft Terminal Server or a Citrix MetaFrame Presentation Server needs a client license to be able to access the resources on the server. You also need a client license to be able to log in and use the functionality of the MPS server.

The following license requirements should be addressed in any Terminal Server or Citrix MPS environment:

- *Windows 2000/2003 Server Client Access Licenses (CALs)* You need a CAL to authenticate and

use other server resources such as printing or file sharing.

- *Windows 2000/2003 Terminal Server Client Access Licenses (TSCALs)* In addition to the CALs that are required, a TSCAL is also required. For a user to log in and use the Terminal Services functionality of the server, a TSCAL is necessary. It simply licenses the TS portion of the operating system.
- *Citrix MetaFrame Presentation Server 3.0 Connection Licenses* These licenses are needed to allow users to log in to the MetaFrame Presentation Server and take advantage of its services.
- *Citrix Migration Licenses* These licenses are used to migrate to a newer version of MetaFrame. For example, if you are upgrading to MPS 3.0 from MF 1.8 or MetaFrame XP, you can use your existing licenses and migrate them. Consult with your Citrix representative to see whether you qualify for these licenses.
- *Citrix Upgrade Licenses* These licenses are used to upgrade the version of MetaFrame within the same family. For example, if you have deployed MPS 3.0 Advanced Edition and you decide you need the features of the Enterprise Edition, you would purchase upgrade licenses from Advanced Edition to Enterprise Edition.
- *Application Licenses* These licenses are required for any applications that you install on the MPS server. You should consult with each application's vendor as to how licensing is treated on a Terminal Server.

## Citrix Connection Licenses

Citrix Connection Licenses allow users to connect to any resource in the farm and launch as many applications as they want and yet consume just one license. These licenses are the equivalent of Per Seat licensing in Windows 2000 Server or Windows Server 2003. The difference is that this type of license is not permanently attached to the user using it. Licenses are assigned from a pool for a user to use during his or her sessions; after the user logs off, all session connectivity to the farm for the license is released and made available for other users to use.

In other words, if Didi logs on to the server farm and launches Microsoft Word on Server A, then launches JDEdwards One World (a financial software package) on server B, and then launches Report Writer on Server C, she is still consuming just one license yet running three sessions to three different servers in the server farm. After Didi logs out of all three applications, the license assigned to her is put back into the pool.

### Alert

Given a license scenario, make certain you can identify any missing licenses and provide the proper recommendations to ensure license compliance and avoid outages due to a shortage of available licenses.

# Server Software Requirements

Citrix MetaFrame Presentation Server 3.0 can be installed on Microsoft Windows 2000 Server provided that it is at Service Pack 4 or higher. It can also be installed on Windows Server 2003. In addition to installing the server software, you have to enable Terminal Services in both Windows 2000 Server and Windows Server 2003.

In Windows 2000 Server, you have to put the server in Application Server mode before users would be able to log in and before you can install Citrix MPS 3.0. With the introduction of Windows Server 2003, Microsoft shuffled things around a bit. For example, with Windows 2000 Server, you needed to enable Terminal Services in one of two modes: either Remote Administration, which allows only two simultaneous connections for administrative purposes, or Application Server, which allows multiple users to simultaneously log in to the TS.

Windows Server 2003 has Remote Desktop enabled by default and is no longer a component of Terminal Services. Now when you need to place Terminal Server in what used to be Application Server mode, you need to enable Terminal Server from the Add/Remove Windows Components screen in Add or Remove Programs.

## Note

In Windows Server 2003, some Terminal Services components have been renamed. For example, Remote Administration mode has now become Remote Desktop and is installed by default.

You've surely heard the expression "a picture is worth a thousand words." In the exercises to follow, notice the difference between enabling Terminal Services in Windows 2000 Server and Windows Server 2003.

In Windows 2000 Server, do the following:

1. Choose Start, Settings, Control Panel, Add or Remove Programs, Add/Remove Windows Components.
2. Scroll down and check the box next to Terminal Services, as shown in [Figure 3.1](#). Then click Next.

Figure 3.1. Enabling Terminal Services in Windows 2000 Server.



3. The next screen allows you to select between Remote Administration mode or Application Server mode, as shown in [Figure 3.2](#). Choose Application Server mode and click Next.

Figure 3.2. Terminal Server Mode selection screen.



4. You are prompted to make a decision on the default permissions for application compatibility. You can choose between Permissions Compatible with Windows 2000 Users or Permissions Compatible with Terminal Server 4 Users. Unless you have an old application that requires more relaxed Registry permissions, choose the first option, which is Permissions Compatible with Windows 2000 Users.
5. Click Next and then Finish to exit the wizard.

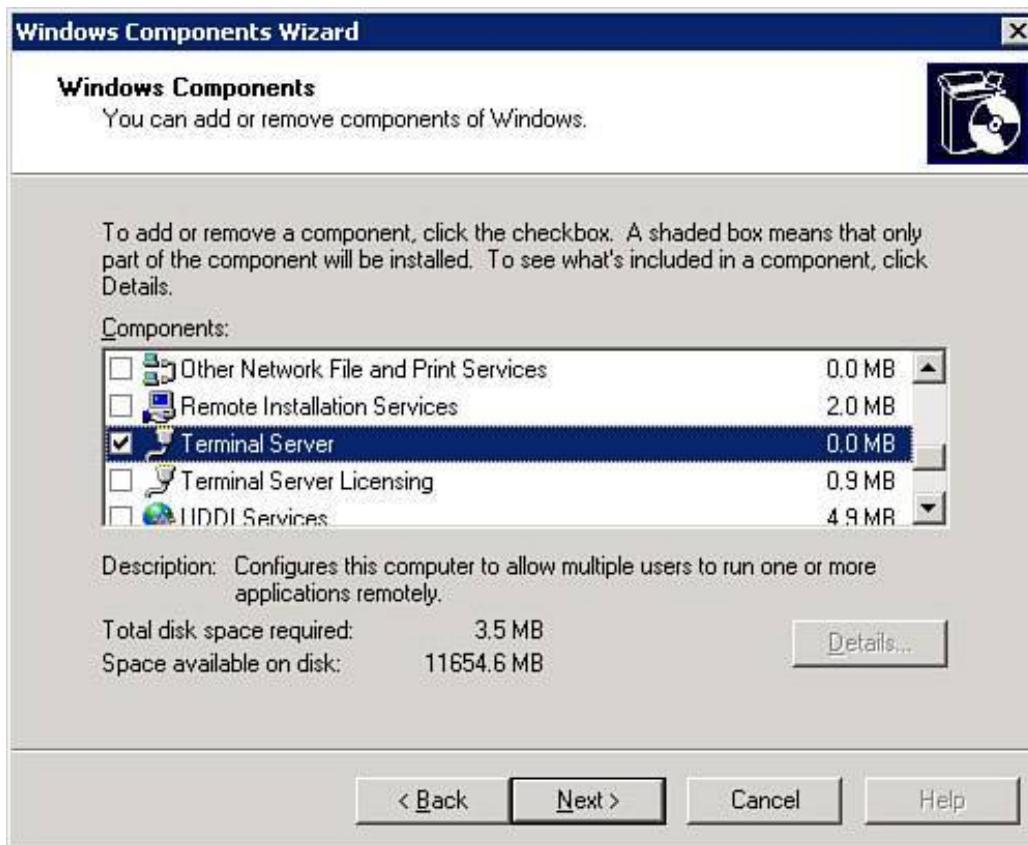
### Note

In Windows 2000 Server, the component that allows multiuser access on the server is named Terminal Services, whereas in Windows Server 2003 it is renamed Terminal Server.

To enable Terminal Server in Windows Server 2003, do the following:

1. Choose Start, Settings, Control Panel, Add or Remove Programs, Add/Remove Windows Components.
2. Scroll down and check the box next to Terminal Server, as shown in [Figure 3.3](#). Then click Next.

Figure 3.3. Enabling Terminal Server in Windows Server 2003.



3. You are presented with a window informing you that you are enabling Terminal Server to allow for multiple simultaneous connections. Click Next to continue.
4. Similar to Windows 2000 Server, you are prompted to choose the application permissions you want to enable on the Terminal Server. You can select between Full Security, which offers the latest security enhancements that Windows Server 2003 offers, or Relaxed Security if you want to allow users more access to the Registry and file system.

Relaxed permissions may be necessary depending on whether your application was designed for Windows Server 2003. Consult your application's vendor and then click Next to continue.

5. Click Next and then Finish to exit the wizard.

## Terminal Services Licensing

Whether you are installing Citrix MetaFrame Presentation Server 3.0 on Windows 2000 Server or on Windows Server 2003, you need to install the Terminal Services Licensing component on a server. This

server must be accessible to all your TS/MPS servers and should be activated with valid Terminal Services Client Access Licenses. If you don't install any licenses, the Terminal Services Licensing Server will issue temporary licenses that are valid for a period no longer than 90 days. After this period, if no valid license is installed, connections will be refused.

In addition, a TS or MPS server has a grace period of no longer than 120 days to find and contact a Terminal Services Licensing Server. After this period, connections will also be refused.

## Caution

As of this publication, Windows Server 2003 does not enforce TSCALs when the server is in Per User mode; it relies on the honor system. However, based on previous versions such as Windows 2000 Server, Microsoft is poised to enforce this policy once again. We strongly recommend you install proper TSCALs on your TS Licensing Server so that you avoid any interruptions in the event that a hotfix should be installed to address this issue.

## Note

Terminal Services Licensing does not have to be installed on a domain controller but is recommended.

## Protocols

Both Windows 2000 Server and Windows Server 2003 install TCP/IP by default. If this is the only protocol you will be using on your network, you don't have to worry about doing anything else. However, if you plan to use any other protocols such as IPX, SPX or NetBIOS, it is recommended that you install them prior to installing Citrix MPS 3.0.

Installing these protocols configures Independent Computing Architecture (ICA) to use these protocols properly by creating the necessary connections. In addition, if you plan to use SNMP in your environment to monitor and manage your servers, this would be a good time to install that as well.

## Note

With Windows Server 2003, the *only* protocol that remote users can use to connect to MPS 3.0 is TCP/IP. Support for IPX/SPX and asynchronous connections has been disregarded.

# Server Hardware Sizing

You must consider many factors when sizing your MetaFrame server, but you should start with the basics. Make sure you fulfill the operating system requirements based on vendor recommendations as follows:

- *Windows 2000 Server and Advanced Server* Microsoft's minimum recommended hardware for these operating systems includes a 166MHz Pentium with 256MB RAM and a 2GB hard drive with at least 1.5GB of free disk space.
- *Windows 2000 Datacenter Server* The vendor recommends eight Pentium III or better processors with at least 256MB RAM and a 2GB hard disk drive with 1.5GB free disk space.
- *Windows Server 2003 Standard Edition* A 550MHz Pentium III or better processor is recommended with 256MB RAM and a 1.5GB hard disk drive with 1.5GB free disk space.
- *Windows Server 2003 Enterprise Edition* A 733MHz Pentium III with 256MB RAM and a 2GB hard disk drive with 1.5GB free disk space.
- *Windows Server 2003 Datacenter Edition* A 733MHz Pentium III with 1GB of RAM and at least 2GB hard disk drive with 1.5GB free disk space.

These recommended hardware requirements are the minimum needed to operate just the operating system. In today's world with fast-changing technology, you probably can't even buy a 166MHz Pentium from a computer vendor.

In addition to the base Microsoft hardware requirements for the operating system you are using, you are also required to take into consideration disk space requirements for installing Citrix MetaFrame Presentation Server 3.0 and all the ICA clients as follows:

- 250MB of disk space for MPS 3.0
- 150MB for installing all the ICA clients on the MPS server

## Alert

You are expected to know the basic hardware requirements for both Presentation Server and the underlying Windows operating system.

## User Load

Because MetaFrame Presentation Server will support multiple user logins to one server, server resources are needed to adequately service these users. When you are sizing your server hardware, it is very important that you have an idea of how many users will log in to each of your servers and also

the types of users who will log in. When we say "types of users," we are trying to identify what the users will do when logged in to an MPS server. Typically, you can categorize users into two categories:

- *Typical user* A typical user is one who logs in, uses one application at a time, and does not copy and paste many items between the ICA session and the ICA client.
- *Power user* A power user is one who logs in and typically uses multiple applications at the same time and runs more advanced tasks.

A good rule would be to allocate twice the number of resources to a power user than you would for a typical user. By resources, we mean CPU and memory utilization.

## Note

To determine how much CPU and memory utilization a typical user will use, you need to run performance tests. Typically, you would run Performance Monitor while the user is logged in and running the application(s) needed to perform all normal tasks his or her job requires.

## Types of Applications

The types of applications installed on the servers have a great impact on the sizing of the servers. Some applications may be poorly written and may bog down an MPS server with as little as 10 users on it. If you are using a mixture of 16-bit and 32-bit applications, you may want to separate them on different servers to improve performance and responsiveness of each application and not allow a faulty application to affect another one.

On the flip side, well-written applications allow you to add more users. Thorough testing of an application using all its functionality is crucial prior to sizing the server's resources.

## Network Bandwidth Considerations

A robust, well-configured, and primed network can drastically improve application response and better the user experience. As we discussed in [Chapter 2](#), "MetaFrame Presentation Server Architecture," one of the three components that make up the ICA protocol is the network, which is the transport mechanism by which data is exchanged. For this reason, it is important to avoid bottlenecks. Try the following to ensure higher performance on your network:

- Keep all Citrix MPS servers and Citrix-related servers on the same subnet to localize traffic and improve performance.
- Use Switched Ethernet when possible.
- Set the link speed to Full Duplex on your servers, the switch ports, and your ICA client devices for optimal performance.

# Management Console Requirements

The Management Console for MetaFrame Presentation Server 3.0 is the centralized administration tool that allows you to configure all aspects of the farm and administer users, among other tasks. The console is installed by default on every MPS 3.0 server in your farm, but in many cases, you will want to install it on your workstation so you do not have to log in to a server every time you want to run any administrative tasks. The Management Console can be installed from the MPS 3.0 CD on any workstation that meets the following hardware and software requirements:

- Microsoft Windows NT 4.0, Windows 2000, or Windows XP.
- Sun Java Runtime Environment (JRE) 1.4.1 or better. The Management Console is a Java-based application and thus requires the JRE to run.
- 50MB of disk space is required to install the Management Console and the Sun JRE 1.4.1.
- A Pentium class processor is recommended to run the console properly.
- The console requires at least 64MB of RAM for itself to run properly.

## Note

When installing the Management Console on a workstation, you do not need to install MPS 3.0. The console runs independently of the server software.

# Firewall Configuration

One of the main reasons Citrix MetaFrame is deployed in most organizations is that it provides the capability to access your office applications from anywhere in the world with an Internet connection. This service, however, comes at a cost, as you now have to protect your environment from malicious users who would want nothing more than an opportunity to wreak havoc on your network.

Firewalls are deployed to protect you from potential users who will be using the Internet as their vehicle of penetration into your servers. A firewall governs what type of data is exchanged between the outside and inside networks. For this reason, it is important to know what ports would need to be opened to allow ICA traffic in and out of your network. These ports are also useful because many times organizations even deploy firewalls internally to create layers of security.

The ports used in a Citrix MetaFrame Presentation Server environment are as follows:

- **1494** An ICA session is established and maintained over this TCP port. Knowing whether clients are connecting from outside the network or inside this port is necessary for ICA traffic between clients and servers.
- **80** The Citrix XML Service is used by ICA clients to query MPS servers for published applications.
- **2512** Server-to-server communications are exchanged over TCP port 2512.
- **2513** The Management Console uses this TCP port to plug into the IMA.
- **1604** UDP is usually enabled if the MPS server is used in interoperability mode or mixed mode, which means there are MetaFrame 1.8 servers in the farm. It is used by ICA clients to broadcast a query to find the Master ICA Browser.
- **443** Secure Sockets Layer (SSL) Relay is used to secure communications between the Web Interface server (formerly NFuse) and MPS servers.
- **139, 1433, 443** MPS servers use these ports to communicate with Microsoft SQL or Oracle databases hosting the Data Store.

# MetaFrame Data Store Requirements

Because the IMA Data Store is the central repository for storing all the farm settings for the MetaFrame Presentation Servers, careful planning and database software consideration are necessary. The IMA Data Store supports the following database software:

- *Microsoft Access* This database software is intended for use by organizations that have up to 50 MetaFrame servers in their farms. It is provided to you free with the MPS operating system and is installed automatically if you choose to deploy the Data Store as an Access database. It is also ideal in organizations in which experienced database administrators are not available.
- *Microsoft SQL Server Desktop Engine (MSDE)* MSDE, database software based on Microsoft SQL server, is a lightweight database installed on the first MPS server prior to installing MetaFrame. MSDE is geared toward small to medium-size businesses and is much more robust than Microsoft Access. It can be administered using standard Microsoft SQL Server tools.
- *Microsoft SQL Server* This complete database software is recommended for any size organization. It can be costly in terms of price, so if cost is a major factor and the company is small to medium sized, other options such as Access or MSDE would be more appropriate. SQL is very robust and scalable.
- *Oracle* Similar to Microsoft SQL Server, Oracle is recommended for any size organization, but because of price considerations and the expertise needed for installation and administration, it is recommended for medium to large organizations. It is a very robust and scalable database system.
- *IBM DB/2* Another enterprise class database software similar to Oracle and Microsoft SQL, IBM DB/2 is suited for medium to large organizations. It is very scalable and robust. It also requires extensive expertise to install and maintain.

When you use Microsoft Access or Microsoft MSDE as the Data Store database, they should be installed on the first MetaFrame server in the farm.

## Direct and Indirect Data Store Connection

A MetaFrame Presentation Server can connect to the IMA Data Store in two ways. Depending on the type of database software you decide to use, MPS servers make either a *direct connection* or an *indirect connection*.

A direct connection to the IMA Data Store means that the database software resides on a dedicated server and all the MetaFrame servers connect directly to this dedicated database server and plug into the IMA Data Store. This type of connection is associated with Microsoft SQL Server, Oracle, and IBM DB/2 databases.

An indirect connection to the IMA Data Store means that the first MetaFrame server you install in the farm hosts the Data Store, which is in the format of a Microsoft Access or an MSDE database. All MPS servers added thereafter will connect to the first MPS server, which hosts the IMA Data Store and will then connect to the Data Store, thereby making an indirect connection. The MPS servers can't connect directly to the Data Store database but first have to connect to the MPS server and then to the Data

Store it hosts.

## Caution

When in indirect mode, all the servers explicitly rely on the first MPS server in the farm because it holds the IMA Data Store. This renders the first server very critical, and thus it should be properly backed up and maintained to avoid any potential issues from the loss of the database it hosts in the event of a disaster.

## Alert

You are expected to clearly understand the differences between a direct and an indirect Data Store connection. Given a farm configuration, you should be able to determine whether the Data Store is directly or indirectly available to Presentation Servers in the farm.

 PREV

NEXT 

# Server Farm Distribution and Availability

One of the major strengths that attracts companies of any size to deploy Citrix MetaFrame Presentation Server is that it is more redundant and more available than any other system. For example, suppose you have 10 MetaFrame servers in the farm serving users. If one server fails or goes down for any reason, the users connected to that server will lose their connection, as well as any unsaved work they were working on. However, they can immediately connect back and will be directed to another server in the farm that supports the same application, enabling them to keep working.

Ideally, you would want all your MPS servers to be in one geographical location, which is what server-based computing or centralized computing is all about. However, in many cases and mostly in larger organizations, you may find groups of servers located in different regions serving different users. For these types of scenarios, you should investigate clustering the IMA Data Store and distributed databases.

## Clustering, Distributed Databases, and Multiple Farms

In large, enterprise-class organizations where numerous servers may be located in different geographical locations, you should rethink the way you design your IMA Data Store for performance reasons and for failover or disaster recovery reasons.

If your organization requires zero downtime or very minimal downtime and is willing to spend the money, you should consider clustering the IMA Data Store to avoid the single point of failure scenario. You can use a number of different clustering methods, but most notable here is the Microsoft Clustering service. The topic is beyond the scope of this exam, but as an administrator, you should be aware of the different options available to you.

Another method you should be aware of is the distributed databases method, which is useful for organizations that have groups of servers in different geographical locations. Because the servers do many reads to the IMA Data Store to query it for data, if these servers are located far away from the Data Store and must travel the WAN to query it, performance is affected for all servers in the farm. For this reason, you should consider using distributed databases, which means you will add a database server at every location where the number of servers warrants a database server. This database server would be an exact replicated copy of the original Data Store and would be used to serve these servers in the remote locations. Again, this topic is beyond the scope of the CCA exam but is mentioned here because, as an administrator, you should be aware of it.

Organizations usually consider creating a second farm when servers are located in geographically dispersed areas and separation of communication is critical. For example, an organization that has a presence in the United States and also in Europe with servers in every continent should consider having separate farms for each region, which would improve performance and reliance on each other. This would mean separate Data Store databases for each farm, which in this scenario is required and recommended.

## Redundant Hardware

The quest of building the "ultimate" environment where no component will ever go down is the dream of every techie in the industry. Many of us dream of a server with so much redundancy that it can

never go down. Even though that dream is far from being realized, components in the server can be redundant, which means you have two or more of the same component, and in the event that one of them goes down, the other picks up automatically without any interruption of service.

Today, you can order servers with redundant hard drives that are built on RAID technology, so if a hard drive fails, the server continues to function properly, and all you need to do is exchange the bad hard drive with a new one.

You can also have redundant network interface cards (NIC) and redundant power supplies so if one goes down, power is picked up from the other one without affecting the server's uptime.

Even if you spend thousands on redundant components, in our opinion, you can never ensure that a server will never go down. For example, what if the motherboard goes bad? All the other redundant components will not help.

A much better solution would be to spend the money on an additional server, rather than on redundant components. More servers improve performance, and they do not cost that much more than the redundant components. This is, of course, the advice we give for MPS servers. For database servers, we recommend some redundant components such as power supplies and hard drives, but we strongly recommend clustering in environments where extended downtime is not tolerated.

## Load Balancing

Citrix MetaFrame Presentation Server Advanced Edition and Enterprise Edition have the capability of automatically load balancing MPS servers either based on user load or based on a more advanced set of calculations. We discuss load balancing in more detail in [Chapter 8](#), "Citrix Load Management." Load balancing is an automated method of spreading user load to the least busy server in the farm. You should be careful, though, as load balancing is not fault tolerant, which means in the event that an MPS server goes down, the users connected to that server will lose their connection. They will not be automatically routed to another server, but they will have to initiate a new ICA session and then be directed to a new server.

### Note

Citrix MetaFrame Presentation Server Standard Edition does not come with load balancing; therefore, MPS Standard Edition cannot direct users to the least busy server, as is the case with the Advanced and Enterprise Editions.

## Exam Prep Questions

1. On which of the following operating systems can MetaFrame Presentation Server 3.0 be installed? (Choose all that apply.)

A. Microsoft Windows NT 4.0 TSE

B. Microsoft Windows 2000 Advanced Server SP2

C. Microsoft Windows 2000 Server SP4

D. Microsoft Windows Server 2003 Datacenter

A1: Answers C and D are correct. Answer C is correct because all flavors of Windows 2000 Server are supported provided that they are at SP4. Answer D is correct because all flavors of Windows Server 2003 are supported. Answer A is incorrect because MPS 3.0 does not support Windows NT 4.0 TSE. Answer B is incorrect because Windows 2000 should be at Service Pack 4 or later; because it is at SP2, it is not supported.

2. When installing MetaFrame Presentation Server 3.0 on Windows Server 2003 Standard Edition, what is the minimum recommended amount of RAM required for the operating system?



A. 128MB



B. 256MB



C. 512MB



D. 1GB

A2: Answer B is correct. Answers A, C, and D are incorrect because Microsoft's minimum RAM requirement for Windows Server 2003 is 256MB RAM.

3. When an MPS server connects to a Microsoft SQL MSDE IMA Data Store database, the connection is known as



A. Host Mode



B. Direct Mode



C. Straight Mode



D. Indirect Mode

A3: Answer D is correct. When an MPS server connects to a Microsoft SQL MSDE or Microsoft Access IMA Data Store database, it is connecting to this database via another MPS server that is hosting the database; therefore, this is known as Indirect mode because it indirectly access the database. Answer A is incorrect because no such mode exists. Answer B is incorrect because a Direct mode is not supported with Microsoft SQL MSDE; it is supported with Microsoft SQL, Oracle, or IBM DB/2. Answer C is incorrect because no such mode exists.

4. What is the minimum recommended RAM size when installing Windows Server 2003 Datacenter server?

A. 2GB

B. 1.5GB

C. 1GB

D. 256MB

A4: Answer C is correct. The recommended size of RAM when installing Microsoft Windows Server 2003 Datacenter server is 1GB. Answers A, B, and D are incorrect because they are not the minimum recommended size.

5. What is the minimum recommended size of free disk space necessary when you are planning to install Windows Server 2003 Standard Edition in preparation for an MPS 3.0 install?

A. 2GB

B. 1.5GB

C. 1GB

D. 512MB

A5: Answer B is correct. The minimum recommended free disk space required for a Windows Server 2003 Standard Edition install is 1.5GB. Answers A, C, and D are incorrect because they are not the minimum recommended free disk space size on a Windows Server 2003 Standard Edition.

6. A Terminal Server Licensing Server must be installed on a domain controller when using Windows 2000 or Windows Server 2003 domains?



A. True



B. False

A6: Answer B is correct. TS Licensing Server does not have to be installed on a domain controller in either Windows 2000 or Windows Server 2003. It is recommended for more reliable querying but is not mandatory and can run on other servers.

7. Which of the following licenses are not required in an MPS 3.0 environment? (Choose two.)



A. Microsoft Windows 2000/2003 Server License



B. Microsoft Windows 2000/2003 CALs



C. Microsoft Windows 2000/2003 TSCALs



D. Citrix MPS 3.0 Server License



E. Citrix Connection License



F. Citrix Load Balancing License



G. Citrix ICA Client device License

A7: Answers F and G are correct. You do not need a specific Citrix load balancing license. Depending on the edition of MPS you purchase, you will either get this feature or not. The Standard Edition of MPS 3.0 does not include load balancing, but the Advanced and Enterprise Editions do. Citrix load balancing was licensed separately in the MF 1.8 days. There is no such thing as the Citrix ICA Client Device License. Answers A through E are incorrect because they are all requirements.

8. Which of the following ports is used to establish and maintain an ICA session?

- A. 2512
- B. 2523
- C. 1604
- D. 1494

A8: Answer D is correct. TCP port 1494 is used to establish and maintain an ICA session.

Answers A and B are incorrect because 2512 and 2513 are used for MPS server-to-server communication and server-to-IMA communications. Answer C is incorrect because 1604 is a UDP port used for client broadcast.

9. Your Citrix MPS 3.0 farm is composed of 25 servers supporting the accounting package in your organization. On a daily basis, you have 30 users on each server. Servers 10 and 11 have just failed with hardware problems. What happens to the users who were actively connected to these two servers?

- A. Users are rerouted automatically to another server, but they lose any unsaved data they were working on.
- B. Users are automatically rerouted and spread over to the other servers in the farm. Users do not lose the data they were working on, and the operation is seamless to the user.
- C. Users are disconnected from the server and have to reconnect, but they do not lose any data and can pick up where they left off before the servers went down.
- D. Users are kicked off the servers; they need to reconnect, and any unsaved data is lost.

A9: Answer D is correct. Load balancing is not fault tolerance. In the event of a server failure for any reason, users connected to that server lose their connection, thereby needing to reconnect, and any unsaved data is lost. Answers A, B, and C are incorrect because they are incorrect statements.

10. What is the grace period for an MPS server to find and communicate with a terminal Server Licensing server before it starts to refuse connections?

A. 120 days

B. 90 days

C. 60 days

D. 30 days

A10: Answer A is correct. An MPS 3.0 server has 120 days to locate and communicate with a TS Licensing server; otherwise, it will start refusing connections. Answers B, C, and D are incorrect because they do not provide the correct grace period value.

 PREV

NEXT 

# 4. Installing and Managing MetaFrame Access Suite Licensing

Terms you'll need to understand:

- MetaFrame Access Suite Licensing (MASL)
- MyCitrix.com

Concepts you'll need to master:

- Planning for the deployment of MetaFrame Access Suite Licensing

When Citrix released MetaFrame Presentation Server (MPS) 3.0 and MetaFrame Conferencing Manager (MCM) 3.0, the company also released a new licensing infrastructure for these products called MetaFrame Access Suite Licensing (MASL). Citrix's plan is to integrate future releases of the MetaFrame Access Suite product family in with the MASL technology.

Central to the new licensing infrastructure is the need to have a designated licensing server that is responsible for storing and issuing licenses when requested. Unlike earlier versions of MetaFrame that required the entry of license and activation codes directly within the Management Console, after a license has been activated within the Citrix Activation System (CAS) in the MyCitrix web portal (<http://www.mycitrix.com>), an associated license file is downloaded and stored directly on the license server. The information contained within this file is used by the license server to determine characteristics such as the types of licenses and the quantity available for use.

## Alert

The new MetaFrame Access Suite Licensing system is not backward compatible with earlier versions of MetaFrame. A MetaFrame XP server cannot query an MASL server for license information. It must continue to retrieve license information from the Data Store. After a MetaFrame XP server is upgraded to MPS 3.0, it requires the MASL server to function properly.

This chapter covers the key areas involved in planning, installing, and managing the MetaFrame Access Suite License server. Not only is this technology new, but it is also such a critical part of the installation and deployment of MPS that you will want to have a very thorough understanding of this topic in preparation for the exam.

The following key topics are reviewed in this chapter:

- *MetaFrame Access Suite Licensing Architecture* MASL is made up of several different components that must all be configured and deployed properly to ensure the licensing server is functioning

and able to service MetaFrame server requests.

- *Installing MetaFrame Access Suite Licensing* After you have a conceptual understanding of how MASL works, it is time to perform the actual software installation.
- *Managing MetaFrame Access Suite Licensing* After MASL is installed, a number of configuration tasks can be performed within the Management Console.

A MetaFrame Presentation Server 3.0 environment cannot function without the existence of a license server. In fact, before you install MetaFrame Presentation Server, it is recommended that you have the MASL server installed and accessible.

 PREV

NEXT 

# MetaFrame Access Suite License Architecture

Unlike Microsoft Terminal Services licensing, which works on either a per-device or a per-user basis, Citrix employs true concurrent user licensing for its MetaFrame Presentation Server product. For example, if you have 600 employees in your company but only 200 are ever logged on to a MetaFrame environment at one time, you are required to have only 200 MetaFrame Client Access Licenses (CALs).

A MetaFrame Client Access License is not required to install the MPS client. The MetaFrame client could be installed on all 600 clients from the preceding example. The MetaFrame CAL requirement goes into effect only when a user actually attempts to log on to a MetaFrame Presentation Server. At that time, one of three things will occur:

- If the client device has already been issued a license for a session that is currently active, no additional license is required. A license is consumed only when the first connection is made by a device. All subsequent connections will share that same license.

There is one caveat to this point. To consume only a single license when connecting to two or more servers, all the servers in question must be communicating with the same license server. If a user connects to a MetaFrame server that utilizes a different license server, an additional license is issued by that license server. Currently, Citrix does not support the pooling of licenses between different MASL servers.

## Note

In addition to the requirement that MetaFrame servers reside within the same server farm, license sharing is supported only between servers running the same version of MetaFrame. A user who is simultaneously connected to both a MetaFrame 3.0 and a MetaFrame XP server will consume one license from each environment.

- If the client device currently has no active sessions, the MetaFrame server to which the client is connecting queries the MASL server and requests a license on the client's behalf. A license is checked out from the license database and assigned to that client. When the last active session from that client is terminated, the license is checked back into the license database. At that time, it becomes available for use by another client.
- If the MASL server has no free licenses available, the checkout attempt (along with the user's connection attempt) fails, and no additional user logons are accepted until an existing user session ends and a CAL becomes available.

## Note

Unlike a Microsoft Terminal Services License server, which allocates temporary licenses to allow a user to log on, a MetaFrame Access Suite License server does not issue temporary

licenses. With the exception of a limited number of licenses available during the installation grace period, if a CAL is not available when a user tries to log on, that user's connection attempt is simply refused.

Until a license file has been downloaded and applied to a license server, it operates in what is known as the *startup* grace period. During this grace period, the MASL server issues a maximum of two Client Access Licenses to nonadministrators. These licenses allow access to the MetaFrame server for a maximum of 96 hours (4 days). After that, the users cannot log on until a valid product license file is downloaded and installed on the license server. This 96-hour grace period does not apply to an administrator, who is granted access to the product indefinitely.

This startup grace period differs from the grace period that exists if a MetaFrame server loses connectivity to a license server due to a license server failure, network issues, or some other problem. In this configuration, the MetaFrame server immediately begins operating in a failover mode, which has a separate grace period of operation before the license server must once again be available. The time frame for the failover grace period was initially 96 hours when MASL was first released, but this has since been updated to 30 days. For the failover grace period to be valid, the license server must have a valid license file installed. A license server with no valid license file does not allow a MetaFrame server to function in failover mode.

## Alert

Remember that this failover grace period has been increased since the original license server documentation was released. The existing documentation available with MPS 3.0 still states that the grace period is only 96 hours (4 days). If the license file was downloaded after August 19, 2004, it allows for the new 30-day grace period.

Also, remember that this grace period does not apply to the startup grace period. The startup grace period applies only when no license file has been downloaded and so still remains at 96 hours.

Two different grace periods exist for MASL:

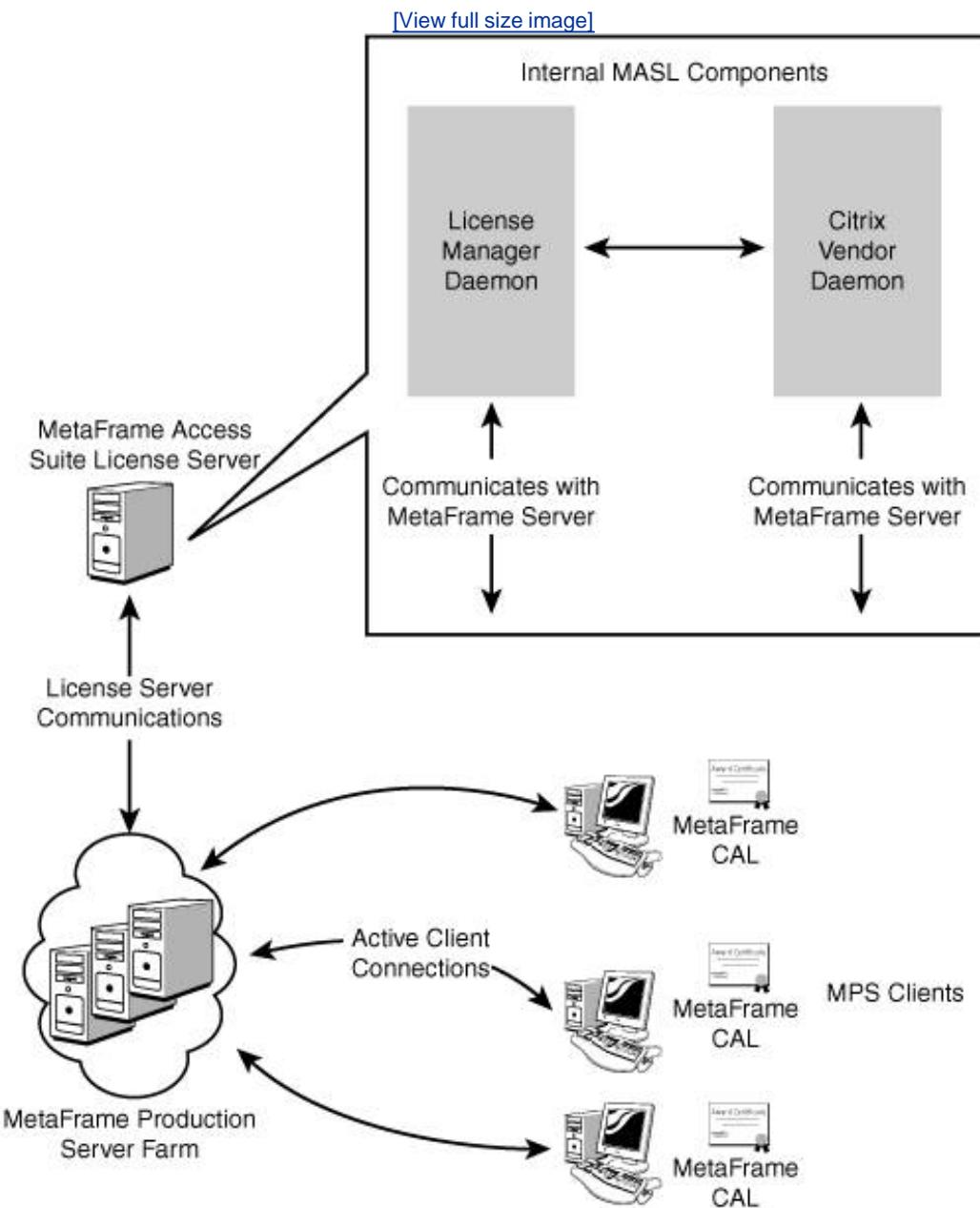
- Startup grace period96 hours (4 days)
- Failover grace period30 days

## MetaFrame Access Suite Licensing Overview

[Figure 4.1](#) illustrates the components that make up a typical MetaFrame Presentation Server 3.0 environment with a MetaFrame Access Suite License server and multiple MPS clients. This figure also depicts the internal breakdown of the MASL server, illustrating the two internal services (daemons) that combine to deliver the license server's functionality. These services are called the License Manager Daemon ([LMGRD.EXE](#)) and the Citrix Vendor Daemon ([CITRIX.EXE](#)).

Figure 4.1. A typical MetaFrame Access Suite License server

implementation.



Two distinct types of licensing activity take place in an MPS 3.0 environment:

- *Initial server connection phase* Occurs when the MetaFrame Presentation Server initially boots up
- *Client Access License retrieval* Occurs when a client device connects to a MetaFrame server

### MetaFrame Server Initial Connection Phase

The first license activityserver connectiontakes place when an MPS 3.0 server boots up. In this situation, the MetaFrame server performs the following tasks:

1. During bootup, MetaFrame retrieves the associated license server address from the Data Store.
2. It then communicates with the License Manager daemon on the license server (see the Internal MASL Components in [Figure 4.1](#)) to retrieve the port on which the Citrix Vendor Daemon is running. The default listening port for the License Manager Daemon is 27000, whereas the default listening port for the Citrix Vendor Daemon is randomly selected during startup. The process for modifying these defaults is discussed in the "[Modifying the Listening Ports for the MASL Server](#)" section of this chapter.
3. Using this information, the MetaFrame server opens a connection with the Citrix vendor daemon, a connection that remains open as long as the MetaFrame server is up. After this connection is established, the MetaFrame server checks out a startup license. This license is required for the server to be able to check out Client Access Licenses.
4. The MetaFrame server is now fully operational and ready to accept client connections.

## Note

During the initial connection to the license server, the MetaFrame server stores a replica of the license information locally. This information is then updated once every hour to reflect the current license availability. This replica is maintained in case connectivity with the license server is lost and the MetaFrame server must begin issuing licenses for the failover grace period of 30 days, which was discussed earlier.

Each MetaFrame server maintains its own personal copy of the license information from the license server and does not perform any kind of license pooling on its own. For example, if the license server had 75 licenses available for allocation before it crashed, and there were four MetaFrame servers, each MetaFrame server would be capable of issuing up to 75 CALs during the failover grace period.

## Client Access License Retrieval

When an MPS client attempts to connect to a MetaFrame server, the following occurs:

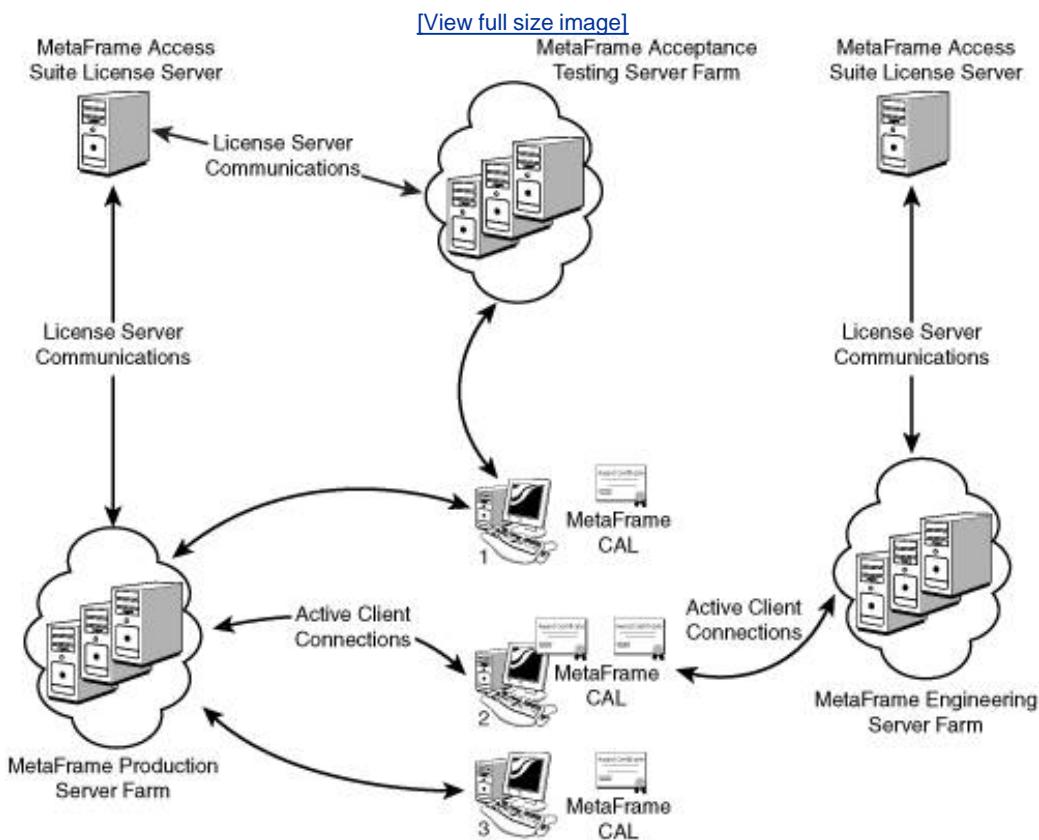
1. The MetaFrame server communicates directly with the Citrix Vendor Daemon (see [Figure 4.1](#)) to determine whether licenses are available. If one exists, the vendor daemon checks out the license and allocates it to the requesting MetaFrame server.  
If the license server is unavailable, the MetaFrame server allocates a license, if available from the replica information it has stored locally.
2. If a client access license is available, the MetaFrame server allows the client to connect; otherwise, access to the server is denied.

[Figure 4.1](#) illustrates that each client device has been allocated a single MetaFrame CAL, regardless of how many server connections it actually has open.

[Figure 4.2](#) expands on the previous figure, demonstrating a more complex MASL configuration. This

time, it involves two distinct license servers and three separate Citrix server farms (Production, Acceptance Testing, and Engineering). Two of these farms (Production and Acceptance Testing) share the same license server, while Engineering communicates with its own.

Figure 4.2. Multiple farms can share the same license server.



This diagram also demonstrates the behavior of Client Access License allocation, depending on the server farm that a client is connecting to. You can see that Client 1 has a connection to both Production and Acceptance Testing, but consumes only one license because these farms both share the same license server.

Client 2, on the other hand, has a connection to Production and Engineering, but because two different license servers are involved, this client consumes two licenses.

Even though these examples depict only server *farms* assigned to different license servers, Citrix also allows you to perform a more granular assignment at the individual server level.

MetaFrame servers within the same server farm can be directed to different license servers. This is not the default behavior nor a typical deployment scenario, but if desired, it can be defined within the properties for an individual server.

Regardless of whether servers are in the same or different server farms, if they are directed to different license servers, a client connected to these servers consumes multiple Client Access Licenses.

## Alert

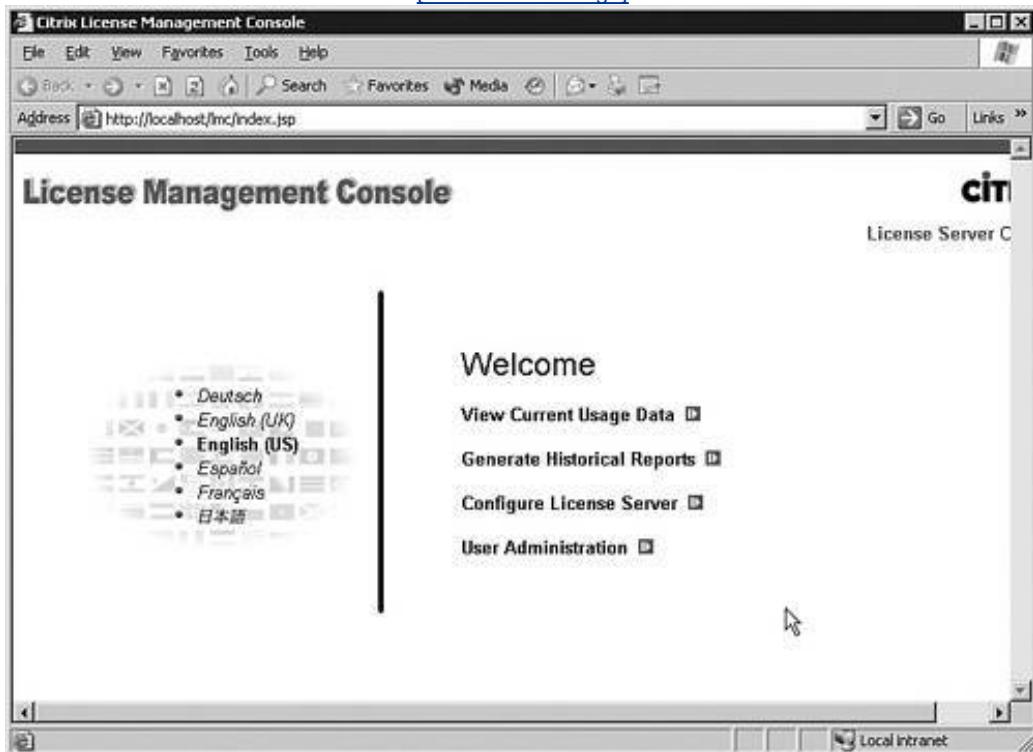
It is important to understand under what conditions a new CAL is allocated, instead of an existing CAL being used.

## License Management Console

The main management tasks for MASL are performed using the License Management Console (LMC), a web-based application that must be installed and run on the same server as the MASL component. [Figure 4.3](#) shows the welcome screen that is visible when an authorized user connects to the main LMC web page.

Figure 4.3. The majority of the MASL management tasks are performed using the web-based License Management Console.

[View full size image]



Through this web interface, licensing for your MetaFrame environment can be managed from any machine with a supported web browser. The only requirement for using the LMC is that the necessary web components must be installed on the same server as the MASL service. This means that you are also required to run Microsoft Internet Information Service on your MASL server. Details on the requirements for MetaFrame Access Suite Licensing are reviewed in the next section, with the actual management tasks that can be performed using MASL discussed later in this chapter.

# MASL System Requirements

The system requirements for a MetaFrame Access Suite License server are summarized in [Table 4.1](#).

Table 4.1. MASL System Requirements

System Component	Comments
Processor	<p>The MetaFrame Access Suite Licensing application is a single-threaded application, and so cannot directly benefit from running on a multiprocessor server.</p> <p>If MASL is to be deployed on dedicated server hardware, choose a faster single-processor machine over multiple slower processors.</p> <p>If MASL is to be deployed on a server that will be tasked with additional roles such as a file/print server, Terminal Services Licensing server, or even a MetaFrame server, multiple processors allow other application threads to run simultaneously with MASL.</p> <p>The majority of the processor load is generated when running the License Management Console.</p> <p>A 1GHz Pentium III is the recommended minimum processor specification for running an MASL server.</p>
Memory	<p>Because each MetaFrame server maintains a constant connection with a license server, a small amount of memory is consumed on the license server for each active connection.</p> <p>In addition, memory usage can also be affected by the following:</p> <ul style="list-style-type: none"><li>• A large number of user logons and logoffs, which force the license server to process an equally large number of license checkin/checkout requests.</li><li>• Many concurrent user sessions.</li><li>• The license server has a large number of custom configuration options defined within the special configuration file. These custom configuration options are discussed in the "<a href="#">MASL Administration Commands</a>" section of this chapter.</li></ul> <p>The recommended amount of RAM for a server that will be running the MASL service is 512MB.</p>
Hard disk space	<p>MASL requires 30MB of disk space during the installation. It also requires disk space to accommodate the creation and updating of two different log files:</p> <ul style="list-style-type: none"><li>• Debug log fileThis file, which is enabled by default, logs status and error messages. This log, named Imgrd_debug.log, is located in the C:\Program Files\Citrix\Licensing\LS folder. The contents of this file</li></ul>

System Component	Comments
	<p>are overwritten every time the licensing manager daemon service is stopped and restarted. Left in the default configuration, the debug log file consumes very little disk space.</p> <ul style="list-style-type: none"> <li>• <b>Usage logs</b>The usage logs are also created by default and, if left unattended, can grow quite large. The default configuration does not overwrite the usage log when the license server is restarted. Unlike the debug log, which is a human-readable plain-text file, the usage log, while stored in plain text, is not intended to be human-readable. It is for viewing only through the License Management Console.</li> </ul> <p>The rate and amount at which the usage log grows depend on the number of MetaFrame servers and concurrent user connections.</p>
Network bandwidth	<p>An MASL server utilizes only minimal network bandwidth. On average, this is around 1KB per transaction. A transaction is any checkin/checkout request from a MetaFrame server to the license server.</p> <p>Approximately 200 bytes of "heartbeat" data are transmitted every 2 minutes from each connected MetaFrame server to verify the availability of the license server.</p>
Operating system	<p>Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, all running a minimum of Service Pack 3.</p> <p>Windows Server 2003, Standard, Enterprise, or Datacenter Edition.</p> <p>The licensing server is not required to run on the same hardware as MetaFrame Presentation Server.</p>

## Caution

The Citrix document titled "MetaFrame Access Suite License Server Customizations" incorrectly states that the usage log is overwritten when the license server is restarted. This information is incorrect. By default, the usage log is *not* overwritten.

The License Management Console (LMC), which must also be run on the license server, has the following system requirements:

- *A web browser that supports HTML 3.2 or later*The LMC has been verified to be accessible using Netscape 4.7 and 7.0 or higher. It is also accessible with Internet Explorer 5.0 and 6.0 or higher.
- *Microsoft Internet Information Services (IIS) 5.0 or higher*IIS 5.0 comes with Windows 2000 Server, and 6.0 comes with Windows Server 2003. IIS must be installed on the same server as the MASL component. The LMC does not support the use of the Apache web server.  
IIS must be installed *before* you install the License Management Console.
- *Tomcat 4.1.24 or higher servlet engine*Tomcat, which is automatically installed along with MASL,

is a web application container within which you run Java servlets and JavaServer Pages (JSP).

## Note

Tomcat is an open source project, and although details on the technology are not part of the exam, if you're interested, you can find out more information on the project at <http://jakarta.apache.org>.

- *Sun Java Runtime Environment (JRE) 1.4.1 or higher* Version 1.4.1 ships with MASL and is installed automatically if a version does not already exist on your server. You can find the latest version of JRE at <http://www.java.com>. The License Management Console does not run with JRE version 1.3.1.

## Deployment Considerations

When planning the deployment of the licensing server, you should consider a couple of different configuration scenarios:

- *Implementing a dedicated or shared license server* Although MASL can be deployed on the same server as MetaFrame, you may want to consider assigning it to a dedicated server depending on your production environment configuration.
- *Sharing licenses among multiple server farms* A single license server can be used to pool the available licenses between two or more server farms.

## Implementing a Dedicated or Shared License Server

For the most part, the decision whether to run MetaFrame Access Suite Licensing on a dedicated server or one that is also running MetaFrame depends on the size of the environment. [Table 4.2](#) summarizes the guidelines to use when considering whether to use a dedicated or shared license server.

Table 4.2. MetaFrame Access Suite License Host Server Guidelines

Number of MetaFrame Servers	Comments
Fewer than 50	<p>Shared server. Hosting MASL and MetaFrame Presentation Server together on the same machine is a suitable configuration when the environment has fewer than 50 MetaFrame servers.</p> <p>When running both applications on the same hardware, you need to be certain that the minimum server requirements are met for both packages.</p> <p>When the environment is running a large number of MetaFrame servers, additional load may be experienced on the MetaFrame server that is also running MASL. In a load-balanced environment, you may want to consider implementing a load evaluator that allocates fewer connections to this server than others in the farm.</p>
Between 50 and 500 servers	<p>Dedicated server. In an environment that has more than 50 and fewer than 500 MetaFrame servers, a single dedicated license server is the recommended configuration.</p>
More than 500 servers	<p>Multiple dedicated servers. When a single environment has more than 500 MetaFrame servers, Citrix recommends deploying multiple license servers and dividing up the MetaFrame servers so that they point at these different servers.</p> <p>Conceptually, this configuration would look similar to the multiple license servers displayed back in <a href="#">Figure 4.2</a>. Remember, when multiple license servers are implemented, licenses do not pool between these servers, so a client consumes a separate license each time it connects to a MetaFrame server that uses a different license server.</p> <p>Theoretically, a single license server can support a maximum of 2,000 active MetaFrame server connections.</p>

## Note

If you're implementing an environment that also contains MetaFrame Conferencing Manager (MCM) 3.0 and if you have MPS and MCM servers directed to the same license server, they both count toward the maximum number of supported servers.

In this configuration, it is recommended that each MPS and MCM server be directed to its own MASL servers. Licenses for one product cannot be used by another, so having them on a single license server is not necessary if there are concerns about the total server connections that may need to be supported.

Besides the total number of MetaFrame servers that will be hitting a license server, some additional criteria might dictate when one or more dedicated license servers may be necessary:

- If you have MetaFrame servers spread across a large geographical area and wide area network connectivity is a concern. A lack of a secured connection between sites can also dictate the need

for a separate license server at each location.

- If administrative authority is segregated within a single product or across multiple products that utilize MASL. A simple example is the situation in which one set of administrators manages MetaFrame Conferencing Manager, while the others manage MetaFrame Presentation Server. Even if there are only a few servers, maintaining separate servers allows for the management of different security privileges for products that require MASL.

Citrix does not support running multiple instances of MASL on the same physical server. If you want to run multiple license servers, they must be deployed on separate hardware.

### Tip

Although not directly related to the exam, one alternative to running separate hardware that you might be interested in is to implement multiple license servers running on separate virtual servers using software such as Microsoft's Virtual Server 2005 or VMWare's ESX or GSX Server. Note that this configuration is not supported by Citrix, so there are no guarantees that it will work properly in your environment.

## License Sharing Among Multiple Server Farms

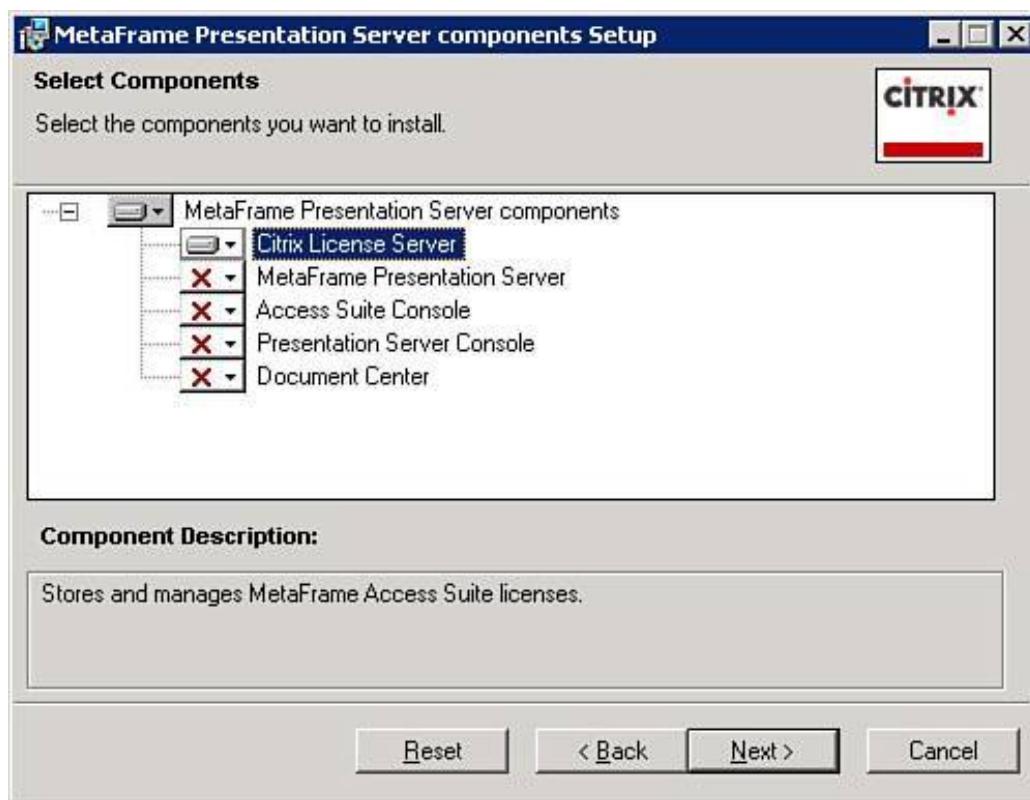
As was demonstrated in [Figure 4.2](#), a single license server can be shared among multiple server farms, decreasing the cost of license duplication and increasing the effective use of the purchased licenses. In general, if the licensing requirements are not such that multiple license servers are necessary, sharing a single license server among multiple farms is the recommended deployment strategy.

# Installing MetaFrame Access Suite Licensing

The actual installation steps for the MASL server are as follows:

1. Begin by logging on to the server that will host MASL and launch the Autorun feature from the installation CD-ROM. This feature usually launches automatically when you insert the CD-ROM, but if not, you can double-click the CD-ROM icon under My Computer or the `Autorun.exe` file on the CD itself.
2. When the setup window appears, select MetaFrame Access Suite Installations and then click the Install MetaFrame Access Suite License Server option.
3. Click Next to move past the first couple of informational screens until you come to the screen titled Select Components (see [Figure 4.4](#)). Ensure only the license service option has been enabled and then click Next. The Windows Installer component for the license server immediately begins.

Figure 4.4. The MetaFrame Presentation Server Select Components dialog box.



4. When the Welcome to the Citrix MetaFrame Access Suite Licensing Installation Wizard dialog box appears, click Next to proceed. If you agree with the terms of the license agreement, click the appropriate radio button and then Next to proceed.
5. Choose the desired destination folder for the application and then click Next.
6. The Select Features dialog box for the Licensing setup appears. IIS must have already been installed for the License Management Console Web Service option to be enabled. Select the desired options to install and then click Next to continue.
7. You are prompted to define a folder to store the license files downloaded from Citrix. The default license location is usually adequate, but you can change it if desired. Click Next to proceed.
8. If you are installing the web interface, the next dialog box requires you to authorize the restart of the IIS service to complete the installation.

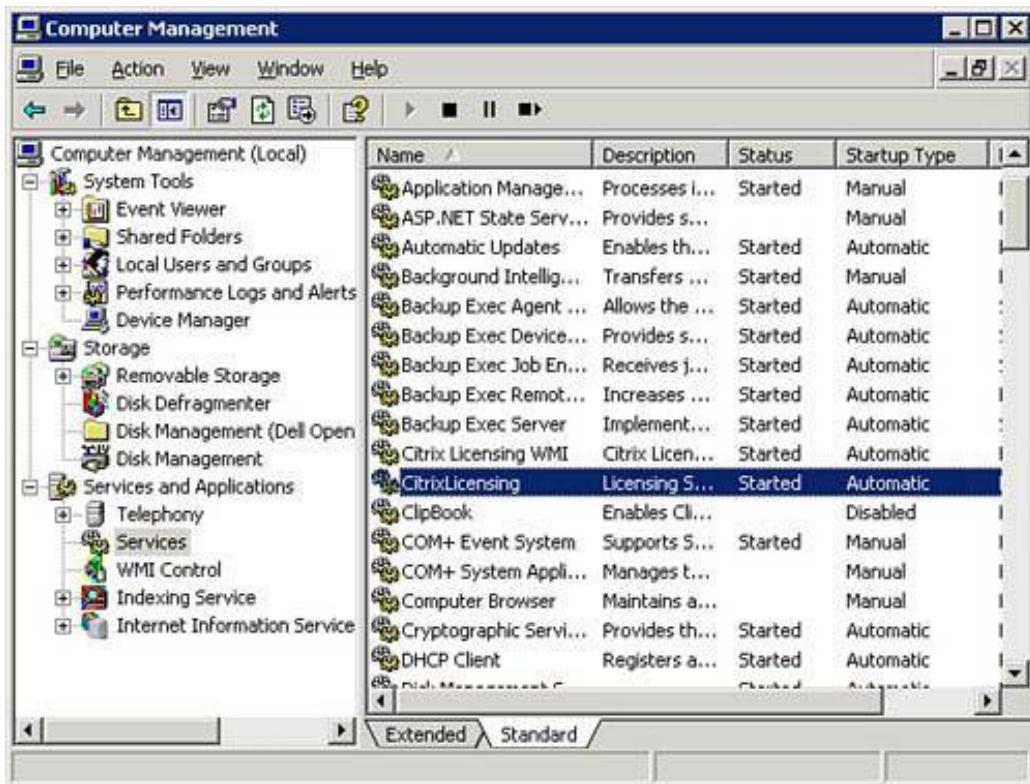
Stopping and restarting the IIS service impact any other web services that may be running on this server. If this machine is currently in production, make certain that stopping the IIS service will not affect the currently active production users. A complete server reboot is not required to enable the licensing services, and after the IIS service has restarted, the installation is nearly complete.

9. Upon completion, an installation summary is presented for your review. After you click Finish, the Licensing Server is available for use, allowing you to download and assign server licenses, as well as providing this server's information when requested during the MetaFrame Presentation Server installation.

You can easily determine the current status of the licensing service (running or not) by viewing the CitrixLicensing service entry through Computer Management. If it is operational, the service's status is set to Started (see [Figure 4.5](#)).

**Figure 4.5.** You can verify that the license service is running by checking that the CitrixLicensing service is set to Started.

[\[View full size image\]](#)



## Uninstalling MetaFrame Access Suite Licensing

The task of removing MASL is straightforward. You simply select Citrix MetaFrame Access Suite Licensing from Add/Remove Programs under the Start menu and follow the wizard to complete the uninstall. Note the following after MASL has been uninstalled:

- If you're going to be reinstalling MASL on a server with a different hostname, you need to download new license files from Citrix to install on that server. The existing license files will not operate on a server with a different hostname.
- If license files were downloaded in the past, all MetaFrame servers that use this license server have the 30-day grace period in which to operate before a new license server must be built and available.

If the license server did not previously license files, any MetaFrame servers that point to this license server have only the 96-hour startup grace period (minus any time that may have already expired for that period) in which to work.

- Any license files along with the Options file and the usage logs are not deleted as part of the uninstall process. In addition to reusing the license files if the hostname remains the same, you can reuse the existing Options file simply by copying it to the proper location on the new license server. [Table 4.3](#) lists the names and locations of these files.

Table 4.3. MetaFrame Access Suite License Server File Locations

Filename	Location and Purpose
*.lic	The default location is % Program Files%\Licensing\MyFiles\  However, this location can be modified during the MASL installation. The file citrix_startup.lic represents the startup license, whereas MetaFrame CAL files can have any name desired, which can be set during the download or renamed at any time.
CI TRI X.opt	Same location as the license files.  This is the Options file where special MASL settings can be defined.
reportlog.rl	% Program Files%\Licensing\LS\  This file contains the usage history for the license server. If the license server will retain the same hostname, you can preserve the usage history by copying this file to the same folder on the new license server.

## Providing License Server Fault Tolerance

Because of the inability to pool licenses between MASL servers, an inherent single point of failure exists with the MASL server in an MPS implementation. Citrix provides the following safeguards to minimize the impact of a license server failure and help to ensure a seamless recovery of the licensing server without an impact to the MetaFrame administrator:

- The failover grace period for licensing has been extended from 96 hours to 30 days. By increasing this time interval to 30 days, Citrix has ensured that more than adequate time exists to build a new license server or correct the issues with the existing server that are preventing its proper operation. During the 30-day time period, each MetaFrame server is capable of issuing licenses without requiring the presence of the license server. Each server periodically polls for the license server, so it will automatically be discovered when it does come back online.

To facilitate a quick recovery, backup copies of the current license files should be maintained so that a new host with the same license server name can be created. You could also look to maintain a backup image of the license server using backup or drive imaging software.

- Citrix provides support for running a pair of MASL servers in a Microsoft Cluster operating in Active-Passive mode. This configuration provides automatic failover capabilities to a second MASL server if the first one fails. When you request a license file from MyCitrix for the cluster, the hostname used for the license file must reflect the name of the cluster, and not an individual node name.

### Note

Citrix provides a brief Adobe Acrobat document outlining step by step how to configure MASL to operate in a two-server Active-Passive Microsoft Cluster. This document can be found on the Citrix website. It has knowledgebase document ID CTX104878.

If Microsoft Clustering is not an option in your environment, you could maintain a second MASL

server with the exact same name but kept offline, ready to be implemented if the existing server fails.

 PREV

NEXT 

# Managing MetaFrame Access Suite Licensing

All license server management can be done through the License Management Console, which is accessed by pointing a web browser at

`http://<server name>/lmc/index.jsp`

where `<server name>` is the name of the server where you installed the licensing service and Management Console. If you are logged on locally to the server hosting MASL, you can select License Management Console from the Citrix folder on the Start menu.

The main LMC window provides the following four options:

- *View Current Usage Data* This option displays the current license usage as reported by the LMC, including any special alerts. Information on this screen does not update automatically and must be manually refreshed.
- *Generate Historical Reports* This option allows you to generate reports based on the license usage data logged by the license server.
- *Configure License Server* All aspects of the licensing server including the Citrix licenses are managed through this page.
- *User Administration* From this page, you manage user access to your license server via the LMC.

From within any of these options, you can access any of the other options simply by clicking on the appropriate toolbar across the top of the screen.

## Note

If, after pointing your web browser to the main LMC URL, you are unable to see any of the main LMC options, then you are not currently authorized to administer the license server. You must ensure that you access the website using an account that has been delegated administrative access to the MASL server. Administrative delegation for MASL is reviewed later in this chapter.

## Managing and Assigning Citrix Licenses

When you are managing MetaFrame Access Suite Licensing, your first task should be to acquire and assign the appropriate licenses to the license server so that they are available to the MetaFrame servers. License assignment involves the following steps:

1. Go to the MyCitrix.com website ([www.mycitrix.com](http://www.mycitrix.com)) and complete the entitlement process for your specific licenses.
2. Download the associated license files generated as part of the entitlement process.
3. Install the license files on the license server.

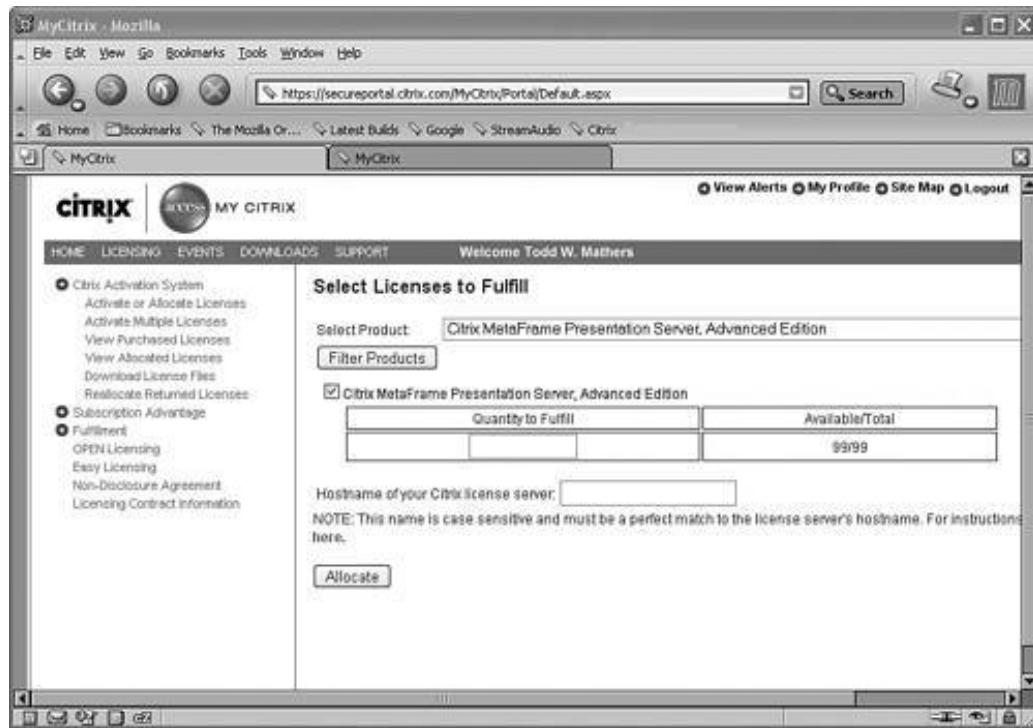
## Processing License Entitlements and Downloading the License Files

The license file acquisition process can be completed as follows:

1. Go directly to the MyCitrix site from your web browser or from within the LMC by selecting the Configuration menu and then selecting Download License File from Citrix Web Site. When prompted, log in to your MyCitrix session.
2. Begin by selecting Licensing, Fulfillment, Fulfill Eligible Products. Select the appropriate license to fulfill and then complete the wizard. You then receive a license code, which you use to perform the license activation and receive your license file.
3. Select Activate or Allocate Licenses and enter the license code you just received. You then see a web page listing the product(s) that you are eligible to fulfill (see [Figure 4.6](#)). Select the check box next to the product(s) that should be fulfilled and then enter the actual license quantity desired. You are not required to fulfill the entire license quantity at once. However, you are required to provide the hostname of your Citrix license server.

Figure 4.6. Performing license fulfillment in the MyCitrix portal.

[\[View full size image\]](#)

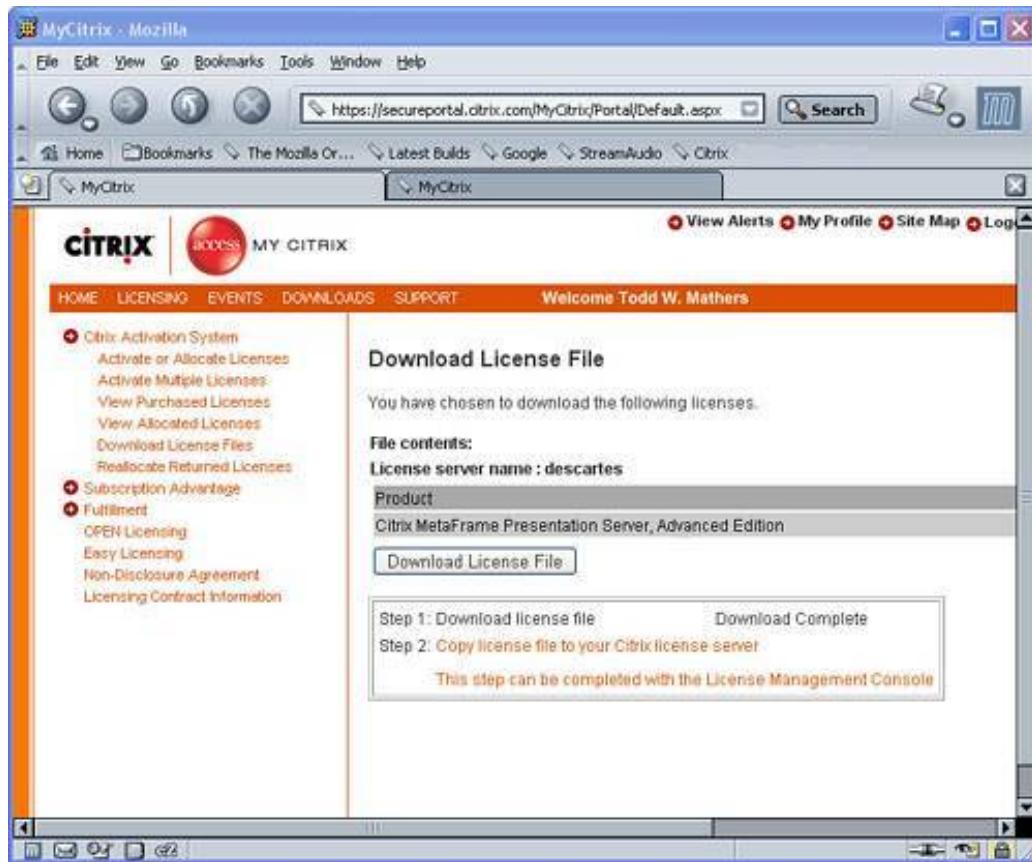


When entering the hostname of your Citrix license server, be certain that you match the spelling exactly. This includes any uppercase letters. You can find the hostname by right-clicking My Computer and loading the System Properties. On the Computer Name tab, you can find the full computer name showing the proper spelling of the hostname. Provide only the hostname, *not* the fully qualified domain name.

4. After you enter the correct information, click the Allocate button. Then, after you review that the information on the confirmation page is correct, click the Confirm button to complete the fulfillment. If the fulfillment is processed correctly, you are presented with the option to download the license file, as shown in [Figure 4.7](#). Click Download License File and save the file onto the license server or a network-accessible folder if you are not actually performing the download from the license server.

Figure 4.7. The Download License File web page.

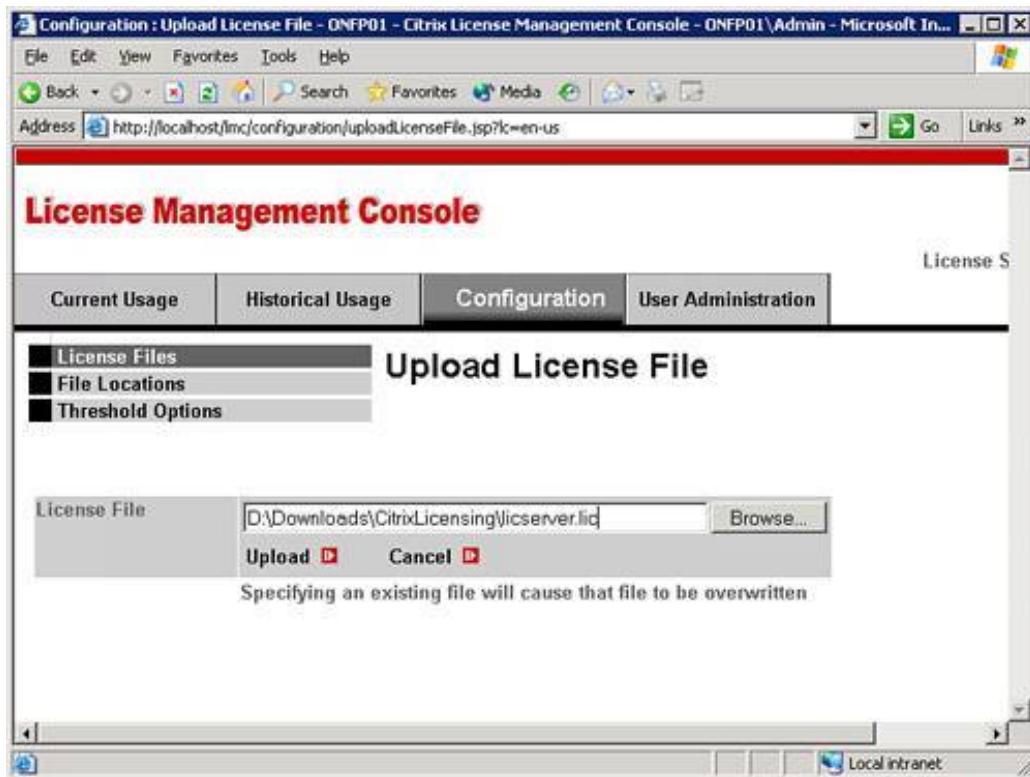
[\[View full size image\]](#)



5. You need to copy the license file onto the license server. You can do this from within the LMC by selecting Copy License File to License Server from the Configuration menu, or you can do this directly from the download page of MyCitrix. You can see this option by referring to [Figure 4.7](#).
6. On the Upload License File page of the LMC (see [Figure 4.8](#)), click the Browse button and locate the saved license file. When you find it, select the Upload button to upload the file and add it to the license server. You should then be able to go to the Current Usage page of the LMC and see the licenses that you have just added. You may need to select the Refresh button or even close and reopen your browser for the new license information to appear properly.

Figure 4.8. The Upload License File page of the License Management Console.

[\[View full size image\]](#)



## Monitoring License Usage

You can monitor the license usage of the environment through the Current Usage page of the LMC. This page provides quick access to the following license information:

- The types of product licenses currently available for issuance.
- The total number of licenses available for distribution.
- The number of licenses that currently have been issued, the number remaining available, and the overall usage percentage. You can quickly view who has been issued what type of license by clicking the small red box next to the In Use count, as shown in [Figure 4.9](#).

Figure 4.9. Current usage statistics from the License Management Console.

[\[View full size image\]](#)

Product	Model	Type	Installed	In Use	Available
Citrix Start-up License	Server	System	5,000	500	4,999
MetaFrame Presentation Server, Advanced Edition	Concurrent User	Retail	40	10	30
MetaFrame Presentation Server, Advanced Edition	Concurrent User	Technology Preview	25	0	25
MetaFrame Presentation Server, Enterprise Edition	Concurrent User	Technology Preview	25	0	25
MetaFrame Presentation Server, Standard Edition	Concurrent User	Technology Preview	25	0	25

From the Current Usage page, you can also view any alerts that may be raised based on threshold settings defined under the Configuration menu. Alert thresholds are discussed in the next section.

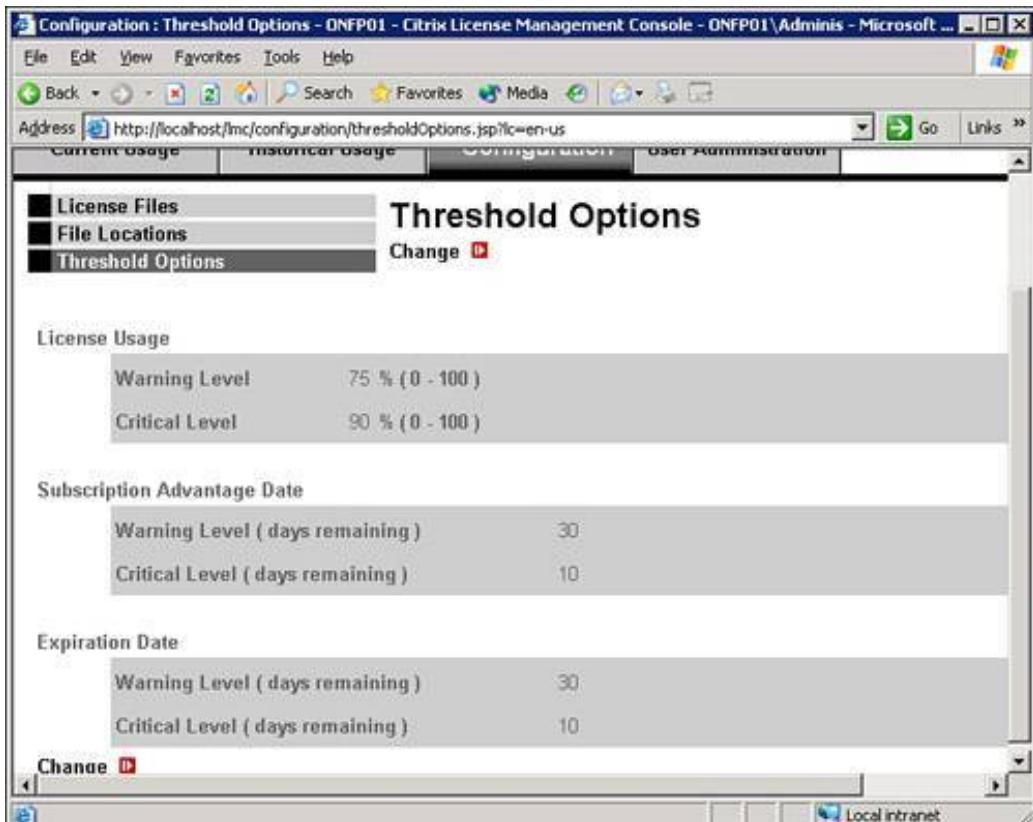
## Alert Thresholds

License alert thresholds are maintained from the Configuration tab, as shown in [Figure 4.10](#). Three categories of thresholds can be defined:

- *License Usage* These threshold levels are based on the percentage of total licenses in use.
- *Subscription Advantage Date* The subscription advantage values represent the days remaining before subscription advantage must be renewed.
- *Expiration Date* Similar to the subscription advantage values, these values represent the number of days prior to the expiration date of a license.

Figure 4.10. Alert thresholds are defined on the Configuration tab.

[\[View full size image\]](#)



For each category, the desired values for a particular implementation depend on the length of time the organization requires to procure the necessary licensing. If the turnaround time is relatively short, it may be reasonable that alert thresholds are increased to reflect this fact, thereby preventing the premature raising of alert messages.

## Historical Usage

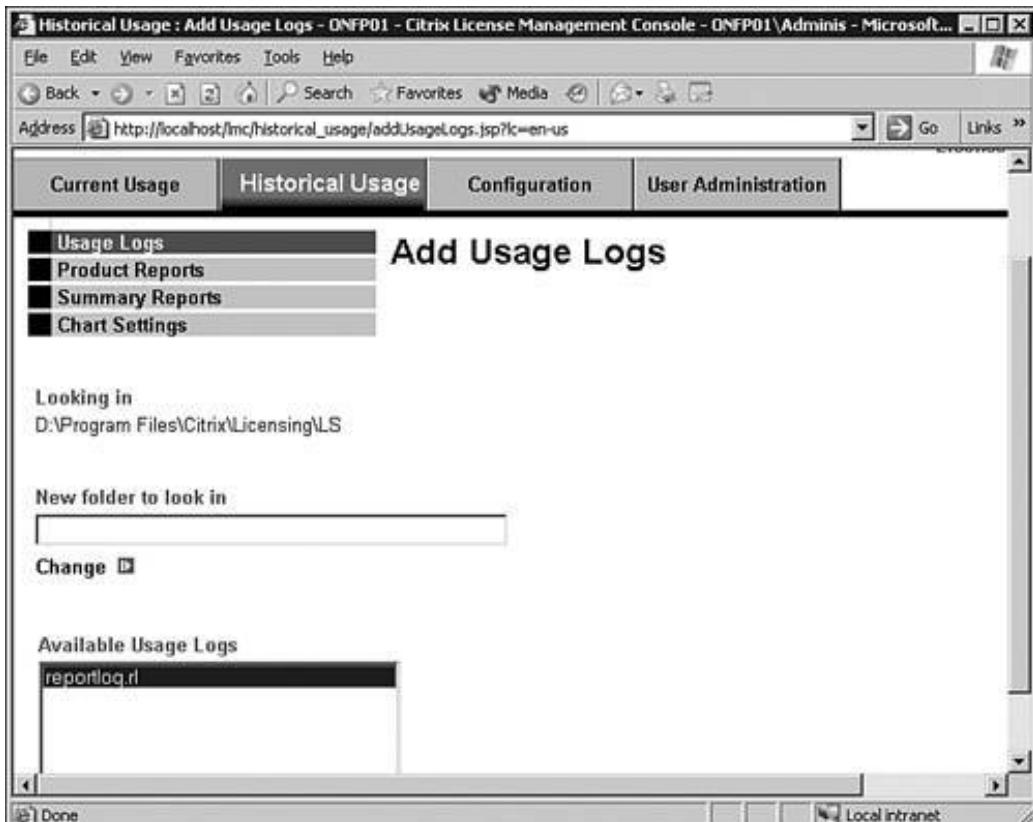
The Historical Usage tab allows you to generate reports based on the data that has been logged in the usage report. Usage reports are enabled by default, and data is automatically logged as license requests are processed by the server. The default report filename and location are

```
%Program Files%\Citrix\Licensing\LS\reportlog.rl
```

After you select Historical Usage and the corresponding page loads, you need to select the usage logs that will be used to generate the desired historical report. When you click the Add button, the Add Usage Logs page opens and populates the list of available usage logs automatically from the default log location (see [Figure 4.11](#)).

Figure 4.11. You need to manually add the desired usage logs to generate historical reports against them.

[\[View full size image\]](#)



Click any of the desired logs to highlight them; then click the Add button on this screen when finished. You return to the main Usage Logs screen, where the selected entries are now visible. As long as at least one log file exists, you can create reports by selecting either Product Reports or Summary Reports.

## Administrative Delegation

When MASL is installed, the administrative account used to perform the installation is automatically added to the list of users with full access to manage the configuration of the MASL server. You can grant additional user accounts access to the Management Console by selecting the User Administration option. On this page, you see the list of all currently assigned users along with the privileges that have been granted to them. The privileges defined dictate what portions of the LMC the user can access.

These privileges correspond to the four available menu tabs:

- Current Usage
- Historical Usage
- Configuration
- User Administration

To add new users, click the Add New User link, which opens a new page where you can add the desired users and define their access privileges.

You also can modify existing accounts by selecting Change Existing User Access Privileges. The list of

existing users is then displayed, and you have the option to select or deselect the appropriate privilege. User accounts are also deleted from the Change User Access window.

## Tip

Because the information stored in the License database is sensitive and critical to the proper functioning of MetaFrame, you should keep the list of users with access to this server as small as possible.

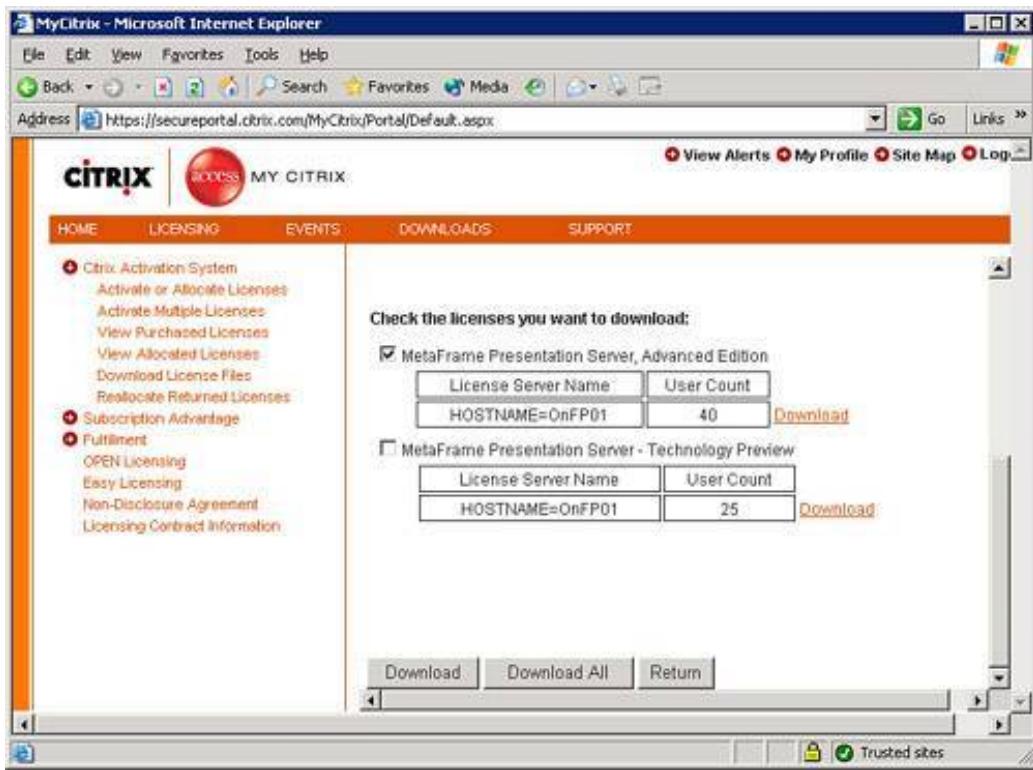
## Moving License Files to a New License Server

Citrix has greatly simplified the task of migrating license files from one license server to another. Recall that the license server's hostname is used as a key in generating the license file, which is unique to that server. A license file cannot simply be copied to a new server for use unless that server maintains the exact same hostname as the original license server.

If you want to retrieve a new license file, the existing licenses must first be "returned" within the Citrix Activation System portion of the MyCitrix portal. License files are returned on the same web page where they can be downloaded, as shown in [Figure 4.12](#). Returning a license simply eliminates the existing license file reference for a particular license server name, allowing you to reallocate returned licenses to a new license server hostname.

Figure 4.12. License files can easily be returned through the MyCitrix portal and then reallocated to a new license server.

[\[View full size image\]](#)



## Modifying the Listening Ports for the MASL Server

To accommodate specific TCP/IP port requirements, Citrix allows you to modify the listening port for both the License Manager Daemon and the Citrix Vendor Daemon.

### Modifying the License Manager Daemon Listening Port

To modify the listening port for the License Manager Daemon from the default of 27000, you must modify all license files currently in use. Specifically, you must make the following change to each file:

1. Back up all license files in case you need to recover the originals. Copying them to an alternate folder is a suitable backup method.
2. Ensure that the license files do not have the read-only attribute set.
3. Open the `citrix_startup.lic` file using a text editor such as Notepad. Near the top of the file, locate the line of text that reads `SERVER this_host ANY`.
4. Append a space to the end of this line, followed by the desired port number. For example, if you want to use port 28880, modify the text to read `SERVER this host ANY 28880`.
5. Save and close this file. Ensure that it maintains the `*.LIC` extension.
6. Open each of the remaining license files and append the same port number after the `ANY` keyword. If the file contains an explicit hostname entry, it should look like `SERVER this_host HOSTNAME=OnFP01`. In this case, append a space and the port number after the hostname. This example would then look like `SERVER this_host HOSTNAME=OnFP01 28880`.

7. After modifying all the files, you can either stop and restart the CitrixLicensing service or use the `lmreread` command-line tool to reload the license files into memory. The command-line tools for the MASL server are summarized in the final section of this chapter.

## Modifying the Citrix Vendor Daemon Listening Port

As we already discussed, the Citrix Vendor Daemon randomly selects a listening port every time the license server is restarted. This random port is adequate in most deployments where the MASL server resides on the internal network. If the license server must be accessed through a firewall or across a router that limits the port traffic that is accessible, you will be required to hard-code a specific listening port for the Citrix Vendor Daemon.

To modify the listening port for the Citrix Vendor Daemon, you must also modify all the licensing files in use by the MASL server. Specifically, you must make the following change to each file:

1. Back up all license files in case you need to recover the originals. Copying them to an alternate folder is a suitable backup method.
2. Ensure that the license files do not have the read-only attribute set.
3. Open the `citrix_startup.lic` file using a text editor such as Notepad. Near the top of the file, locate the line of text that reads `VENDOR CITRIX`.
4. Append a space to this line, followed by this specific text:

```
options="path to options file" port="desired port number"
```

For example, if you want to hard-code the listening port to be 2222, the line might look as follows:

```
VENDOR CITRIX options="c:\Program Files\Citrix\Licensing\MyFiles" Port=2222
```

5. Save and close this file. Ensure that it maintains the `*.LIC` extension.
6. Now open each of the remaining license files and append the same `options` setting after the `VENDOR CITRIX` text.
7. After modifying all the files, you can either stop and restart the CitrixLicensing service or use the `lmreread` command-line tool to reload the license files into memory. The command-line tools for the MASL server are summarized in the final section of this chapter.

After you make these changes, the Citrix Vendor Daemon will always use the same port (2222) instead of selecting a random port on startup.

## MASL Administration Commands

Command-line tools (license administration commands) can be used to perform most of the tasks available through the License Management Console as well as additional troubleshooting and support tasks not available within the LMC. The seven administration commands are summarized here:

- `lmdiag` Diagnoses license checkout problems. Using `lmdiag`, you can test the availability of a license server and ensure that licenses can be checked out properly. It reports on any invalid

listening ports that may be defined.

This tool does not attempt to contact any MetaFrame servers in the farm. It validates only the accessibility of the MASL server itself.

- **lmdown** Shuts down the License Manager and Citrix Vendor Daemons. The Citrix Vendor Daemon alone can be shut down if you use the `-vendor CITRIX` parameter.
- **lmhostid** Returns the host ID of the license server with the proper case required to create a license file for download from Citrix. If you are unsure of the proper name of the license server, this tool will return the information you require.
- **lmremove** Releases a checked-out or "hung" MPS product license. If a license is shown as being in use when it actually is not, this tool can free up that license. If **lmremove** is used to free up a license that is currently assigned to a functioning MetaFrame server, the server will automatically check out that license again within a few minutes of its being freed up. Issuing this command against an active server does not impact the availability of the server in any way.
- **lmreread** Forces the Citrix Vendor Daemon to reread the license files if any changes have been made since the last time it was loaded. If the Vendor Daemon is not running, the **lmreread** command will restart the service.
- **lmstat** Provides you with information on licensing activity, including complete license checkout information and Citrix Vendor Daemon status. The information displayed here is basically equivalent to the data displayed in the usage window of the License Management Console.
- **lmswitchr** Temporarily changes the usage log file by closing the current file and opening a new one with the name you specify. The effect of the **lmswitchr** command lasts until the license files are reread using the **lmreread** command or until the Citrix Vendor Daemon is stopped and restarted.

## Note

You can find a detailed summary of the command-line switches available for all the license administration commands in the "MetaFrame Access Suite License Server Customizations" guide, which you can download from the Citrix website ([www.citrix.com](http://www.citrix.com)).

 PREV

NEXT 

## Exam Prep Questions

1. Which of the following statements about MetaFrame Access Suite Licensing are *not* true? (Choose all that apply.)

A. MetaFrame Access Suite Licensing is an optional component included with MetaFrame Presentation Server 3.0 Advanced and Enterprise Editions.

B. MetaFrame Access Suite Licensing is not backward compatible with MetaFrame XP Server. A MetaFrame XP server cannot query an MASL server for license information.

C. MetaFrame Access Suite License servers maintain a continuous connection with all other license servers on the network. These connections are used to share license information between the license servers.

D. If a MetaFrame Access Suite License server has no Client Access Licenses available, it issues a temporary client license that is good for 30 days. After 30 days, this license will expire, and the user will no longer be able to connect.

A1: The trick to this question is recognizing that we're asking for the statements that are not true about MASL. For this question, answers A, C, and D are correct. Answer A is not a truthful statement because MASL is not an optional component and is required by all versions of MPS 3.0 (Standard, Advanced, and Enterprise). Answer C is also not truthful. MASL servers do not maintain a connection with any other MASL servers and do not share information. It is the MetaFrame 3.0 server that maintains a continuously open connection with the assigned license server. Answer D is the final untruthful statement. An MASL server never issues temporary licenses if no valid licenses are available. If all available licenses are currently in use, any new connections are denied until a license becomes available.

Of the four answers, only answer B is a truthful statement because the new MASL is *not* backward compatible with MetaFrame XP or earlier versions. Licensing for earlier versions will operate completely independent of MASL.

2. You have set up a test environment with a single MetaFrame Presentation Server (Standard Edition) and MetaFrame Access Suite Licensing on the same server. You have decided to hold off on downloading the license files from MyCitrix and want to begin doing some work with a test user who does not have administrative privileges. How long a

grace period do you have before the user will no longer be able to connect and you will need to install the license file?

A. 30 days

B. 45 days

C. 4 days

D. 96 days

A2: Answer C is correct. Until you add a license file to the MASL server, it operates in the startup grace period, which allows for a maximum of two nonadministrators to log on to a MetaFrame server for a maximum of 96 hours (4 days) before a valid license file must be installed on the license server. Therefore, answers A, B, and D are incorrect.

3. When MetaFrame Access Suite Licensing is installed, services added as part of the installation work together to provide the licensing management functionality. What are these services? (Choose all that apply.)

A. The Independent Management Architecture (IMA) service

B. The License Manager Daemon

C. The ICA Vendor Daemon

D. The Citrix Vendor Daemon

A3: Answers B and D are correct. The License Manager Daemon and the Citrix Vendor Daemon are the two services installed as part of MASL and are responsible for managing the issuance of licenses to both the MetaFrame servers and the clients that connect to them. Answer A, while a valid service, is not installed with MASL. The IMA service runs on a MetaFrame Presentation Server and manages communications between MetaFrame servers and the Data Store. Answer D is also incorrect because there is no such service

called the ICA Vendor Daemon.

4. During startup of the MetaFrame Access Suite License server, by default the License Manager Daemon listens on \_\_\_\_\_, while the Citrix Vendor Daemon listens on \_\_\_\_\_.

A. port 80, port 2700

B. a randomly selected port, 27000

C. 27000, 80

D. 27000, a randomly selected port

A4: Answer D is correct. The License Manager Daemon listens by default on port 27000, while the Citrix Vendor Daemon chooses to listen on a random available port during startup. You can modify these defaults if you want. A MetaFrame Presentation Server determines what port the Citrix Vendor Daemon is listening on by first contacting the License Manager Daemon. Therefore, answers A, B, and C are incorrect. Port 80 is the default listening port for the Citrix XML Service.

5. When a MetaFrame Presentation Server first starts up, it retrieves what kind of license from the license server?

A. An activation license

B. A product key

C. A startup license

D. A server access license

A5: Answer C is correct. The initial license retrieved from a MetaFrame Access Suite License server by a MetaFrame server when it first starts up is called a startup license. These licenses are required to allow the MetaFrame server to check out client licenses and are built into the license server. You do not need to install a startup license. Therefore, Answers A, B, and D are incorrect.

6. You have four MetaFrame Presentation Servers, all connected to the same license server. The license server has a total count of 160 installed licenses. Unexpectedly, the license server bursts into flames and then explodes in a shower of sparks. Being the calm and cool administrator you are, you know that you have 30 days to rectify the situation. In the meantime, how many total Client Access Licenses will be available for use in the environment until a new license server is brought back online?

A. 40 Client Access Licenses

B. 80 Client Access Licenses

C. 160 Client Access Licenses

D. 640 Client Access Licenses

A6: Answer D is correct. Each MetaFrame server that was connected to that license server would have a replica of the licenses on the license server. So each server would have noted that there are 160 available licenses ( $160 \times 4 = 640$  total Client Access Licenses). Without the existence of a license server, the MetaFrame servers do not perform license pooling on their own, but instead operate in isolation until the license server returns. Answers A, B, and C are incorrect.

7. Joe User has been configured by his Citrix administrator to be able to connect to a group of published applications that are divided between the Customer Service, Sales, and Marketing server farms. Each server farm has been configured to point to its own licensing server.

At one point during the day, Joe is connected to three applications in Customer Service, two applications in Sales, and one application in Marketing. How many Client Access Licenses is he consuming?

A. 3 CALs

B. 1 CAL

C. 6 CALs

D. None of the above

A7: Answer A is correct. Because each server farm has its own licensing server, a separate client license is consumed when the client connects to the first application in that farm. Each subsequent connection to an application in a farm for which a license has been issued will simply reuse that same license. An additional license is not required. Therefore, answers B, C, and D are incorrect.

8. The main management tool for MASL is what?

A. The License Management Console

B. The Management Console for MetaFrame Presentation Server

C. MetaFrame License Manager

D. Citrix Licensing

A8: Answer A is correct. MASL is managed using the web-based application called the License Management Console. Answer B is incorrect because the Management Console for MetaFrame Presentation Server used to be the source for license management in MetaFrame XP, but this has changed with MPS 3.0. There is no such application called the MetaFrame License Manager, so answer C is incorrect. Citrix Licensing is the application that was used back in the days of MetaFrame 1.8 to manage MetaFrame licenses, so answer D is incorrect.

9. To deploy the web-based management tool for MASL, you must install it \_\_\_\_\_\_. (Choose the answer that best completes this sentence.)

- A. on a web server running Microsoft Internet Information Services (IIS) 5.0 or higher or Apache HTTP Server 2.0.52 or later

- B. on any available web server in your environment that is a member of your main Windows domain

- C. on the server running the License Manager and Citrix Vendor daemons

- D. on a server that is also running MetaFrame Presentation Server 3.0

A9: Answer C best completes the given sentence. If you want to use the License Management Console, it must be installed on the same server as the MASL application itself. Answer A is incorrect because the LMC does not currently support any version of Apache. Answer B is incorrect because the LMC does not require domain membership in order to run, nor does it require running on a MetaFrame server, which means that answer D is also incorrect.

10. The majority of the processor load generated by the MetaFrame Access Suite License server can be attributed to \_\_\_\_\_.

- A. the License Management Console

- B. the Citrix Vendor Daemon

- C. the License Management Daemon

- D. the fact that MASL is a single-threaded application

A10: Answer A is correct. The operation of the LMC on an MASL server typically generates the majority of the server's processor load. Answers B, C, and D are all valid components of the MASL server but do not contribute to the majority of the server's processor load.

11. The \_\_\_\_\_ log file is created by default but is not automatically overwritten every time

the License Manager Daemon is stopped and restarted.

- A. User Connection
- B. Debug
- C. Usage
- D. License Count

A11: Answer C is correct. The Usage log file is created by default but is never overwritten. As a consequence, it can grow quite large over time and must be managed by the MetaFrame administrator to ensure drive space is managed appropriately. Although the Debug log file (answer B) is also created by default, every time the License Manager Daemon is restarted, the log is cleared and re-created. Answers A and D both refer to log files that do not exist in MASL; therefore, answers A, B, and D are all incorrect.

12. Complete the following sentence: Hosting MASL and MetaFrame Presentation Server together on the same machine is a suitable configuration when the environment has fewer than \_\_\_\_\_ servers.

- A. 10 print
- B. 50 MetaFrame
- C. 2 Licensing
- D. 5 load-balanced

A12: Answer B is correct. Citrix recommends that, in an environment with more than 50 MetaFrame servers, the MASL component be installed onto its own dedicated server instead of sharing resources with client sessions on one of the MetaFrame servers. Therefore, answers A, C, and D are incorrect.

13. To verify the availability of the license server and ensure that licenses can be checked out properly for a given MetaFrame platform edition, you would use the \_\_\_\_\_ command-line tool.



A. `lmdiagnose`



B. `lmstat`



C. `lmcheckout`



D. `lmdiag`

- A13: Answer D is correct. The `lmdiag` command-line utility is used to test the availability of a license server and ensure that licenses can be checked out properly. Answer A is incorrect because such a tool does not exist. Answer B is incorrect because even though `lmstat` is a valid tool, it returns information on the current number of licenses that are checked out and available. It does not provide information on whether a new license can be checked out. Answer C is incorrect because `lmcheckout` is not a valid tool.

PREV

NEXT

# 5. Installing MetaFrame Presentation Server 3.0

Terms you'll need to understand:

- Citrix XML Service
- ICA Session shadowing

Concepts you'll need to master:

- Understanding interoperability mode
- Understanding shadowing permissions
- Understanding unattended installation

So far, the chapters have discussed theories and technologies; in this chapter, we describe how to install Citrix MetaFrame Presentation Server 3.0. Because MetaFrame is an add-on product that installs on top of Microsoft Windows Terminal Services, it is imperative for you, as a Citrix Certified Administrator, to have a good understanding of how to install Windows 2000 Terminal Services and Windows Server 2003 Terminal Server.

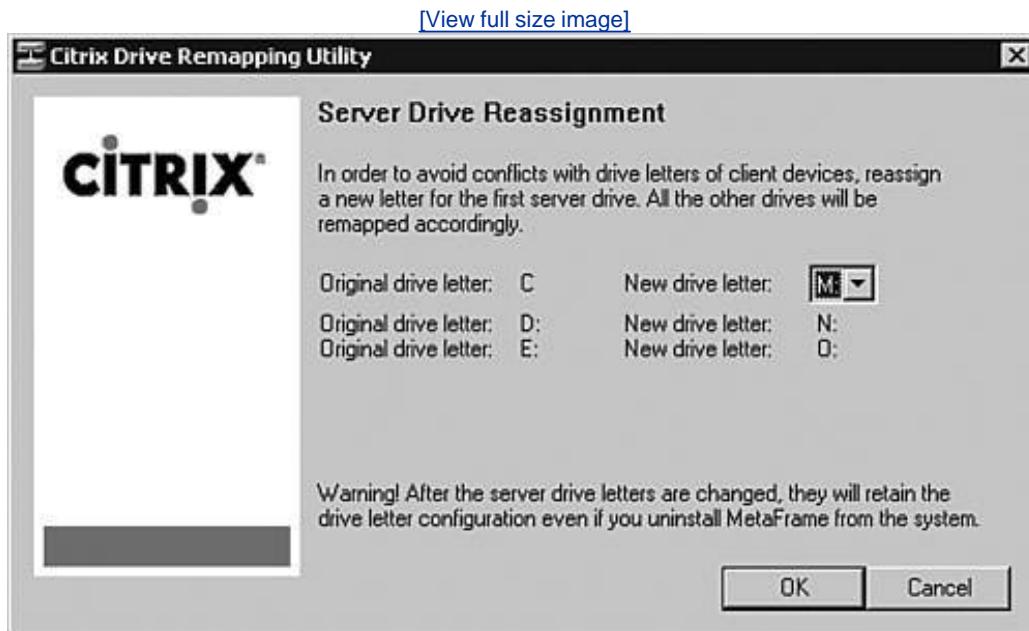
## Remapping Server Drive Letters

When a user launches an Independent Computing Architecture (ICA) session, the MPS server tries to map the client's disk drives on the server so that the user can use them as he or she would when working on a local workstation. If the server tries to map drive C:\, for example, but notices that this drive letter is being used on the server, it is forced to use another letter, which may confuse the user. So the user's local drive C:\ may be drive M:\ on the server.

To avoid this confusion and to offer users drive letters that correspond to their own, you can remap the server's drive letters in advance, thereby freeing up the necessary drive letters needed to avoid user confusion. So, on a server that has drive letters remapped, when a user logs in, the MPS server maps his or her local drive C:\ to a drive letter on the server C:\.

To remap a server drive, locate the utility named `DriveRemap.exe` in the root of the MPS 3.0 CD-ROM. Double-click this file, and a window shows up, as shown in [Figure 5.1](#), allowing you to remap the drive as you like. All you have to do is choose the drive letter for the first drive; the others will be incremented. In other words, if you have C:\, D:\, and E:\ on the server, when you run the `DriveRemap.exe` utility, all you have to do is select what C:\ will be remapped to and the others will be incremented. So, if you select C:\ to be remapped to M:\, then D:\ becomes N:\, and E:\ becomes O:\ automatically.

Figure 5.1. The Citrix Drive Remapping utility.



Note

It is very important to keep in mind that Server Drive remappings are permanent. Even if you uninstall MPS from the server, the drive remaps will still be there and will not be returned to their original state.

## Alert

Citrix strongly recommends that if you decide to remap server drive letters, you do so prior to the installation of any applications, including MPS 3.0, on the server. Failure to do so will render the server unstable.

 PREV

NEXT 

# Standard MetaFrame Presentation Server 3.0 Installation

The steps necessary to install Citrix MetaFrame Presentation Server (MPS) 3.0 are virtually the same whether you are installing it on Windows 2000 Server or on Windows Server 2003, provided that you meet the prerequisites we discussed in earlier chapters. MPS can be installed using various methods; you can use the CD, of course, or you can copy the contents of the CD to a network share and run it from that location. For the purposes of this book, we use the CD as our installation method.

After you insert the CD in the CD-ROM drive, if your server is configured for Autorun, you immediately see the Citrix splash screen, which offers you several options to choose from. If Autorun is disabled on your server or if you are installing from a network share, you should look for `autorun.exe`, which is the file that the Autorun would have run had it been enabled on the server. If you double-click this file, the Citrix splash screen should appear.

To start the installation of MPS 3.0, select the second option, Product Installations. This selection takes you into a submenu where you can elect to install several different Citrix components. Because you are trying to install MetaFrame, choose the second option, Install MetaFrame Presentation Server and Its Components. This selection kicks off the installation wizard, and the first screen you are presented with is the license agreement window. You should, of course, read the whole agreement and then accept it if you want to continue. Next is an informational window listing the installation prerequisites, which you should have met by now. Browse through and make sure you didn't miss anything; then click Next to move on with the wizard.

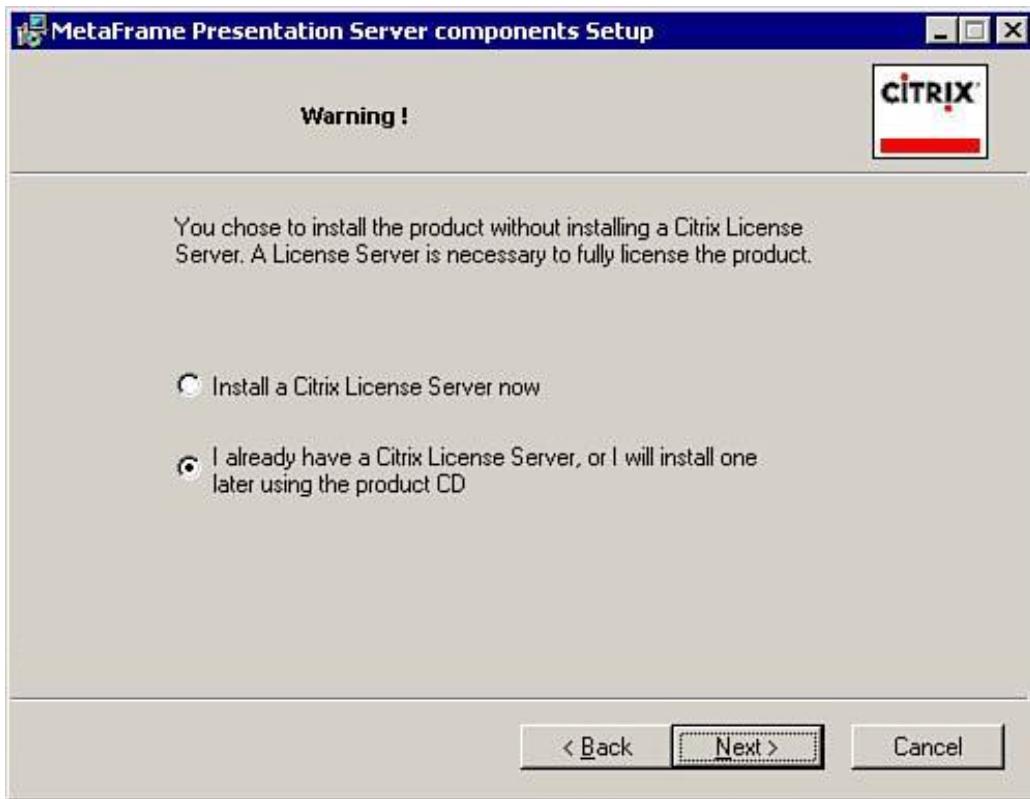
## Choosing Components to Be Installed

You are now prompted to select the components you want to install. You should have installed Citrix License Server in [Chapter 4](#), "Installing and Managing MetaFrame Access Suite Licensing," so you can choose not to install it here. The other options available for install are MetaFrame Presentation Server, Access Suite Console, Presentation Server Console, and Documentation Center. For this chapter, choose to install MetaFrame Presentation Server, Presentation Server Console, and Document Center. Generally, it is a good idea to have the Presentation Server Console on your MPS servers, and the Document Center can always be useful. As for the Access Suite Console, usually you install it on your administrative workstation, but you can install it on the servers if you choose to do so. After making the appropriate choices, click Next to continue with the setup wizard.

## Installing the Citrix License Server

On the next page of the setup wizard, you must choose either Install a Citrix License Server or the second option, I Already Have a Citrix License Server, or I Will Install One Later Using the Product CD. Because we covered the installation of a Citrix License Server in [Chapter 4](#), we assume you have done that already, so you can choose the second option, as shown in [Figure 5.2](#). Click Next, and the wizard launches the installation of MetaFrame Presentation Server 3.0.

Figure 5.2. Citrix License Server configuration.



## Installing MetaFrame

The MetaFrame installation wizard kicks off by presenting the standard Welcome screen. Feel free to read though it and then click Next to continue. Again, you are presented with the license agreement, which you must accept before you can go to the next step. This second license agreement is for the MetaFrame Presentation Server product, so it is different from the one presented earlier. Select I Accept the License Agreement and click Next to continue.

## Choosing Product Editions

Next, you arrive at the first screen where you actually have to make a decision that will affect the features installed and available to you. You have to choose which flavor of MPS you are installing. Depending on the type of licensing you have purchased, you must select Enterprise Edition, Advanced Edition, or Standard Edition. For the purposes of this example, select Enterprise Edition. Click Next to continue.

## Choosing MetaFrame Components

Depending on the MetaFrame edition you selected in the preceding step, you have to choose the components that you can install with that edition. Because you selected the Enterprise Edition, select all the options available except Program Neighborhood Agent, which requires the installation of the Web Interface covered in [Chapter 14](#), "Web Connectivity." Also, accept all the other components, which include the Management Console, Installation Manager, Resource Manager, Load Manager, Network Manager, Program Neighborhood (PN), and WMI Providers. Click Next to continue.

## Enabling the Pass-Through Client

You are now prompted to choose between enabling the Pass-Through Authentication for the Pass-Through client. Your options are Yes or No. For the purposes of this example, select Yes. The Pass-Through client is used by users of operating systems other than Win32. As you will learn in [Chapter 13](#), "Citrix ICA Client Software," the Program Neighborhood interface, which is the most powerful ICA client, is available only for Win32. For users of other operating systems to take advantage of PN, Citrix offers the Pass-Through client.

But you might be wondering why you need it. Let's look at an example illustrating when and why the Pass-Through client is useful. When you use the Win32 ICA client, also known as Program Neighborhood, you take advantage of all its dynamic features and options. Most importantly, you can authenticate once to the server farm and get a list of all the applications you have access to. After you get this list, you can double-click on any of these applications and can launch them without any further steps on your part. If an administrator adds or removes applications or content, these changes are reflected dynamically and automatically for you.

All other ICA clients lack this dynamic nature, which means if you are connecting from a Mac or a Linux box, you have to create a manual connection to every application you want to launch. If anything changes on the server side, you have to manually make these changes. You also lack many of the performance enhancements available with the Win32 client.

For this reason, Citrix offers the Pass-Through client. To take advantage of this client, you have to configure a connection from your ICA client to the server that hosts the Pass-Through client. When you do that, you can then launch the Pass-Through client as an application and authenticate to it. You can then take advantage of all its features, and you would have created only one manual connection. Granted, when you launch an application from within the Pass-Through client, you launch a session within a session, but Citrix has tweaked the ICA protocol to sustain and perform adequately under these circumstances.

## Creating or Joining a Server Farm

Next, you arrive at the Create or Join a Server Farm screen. Because this is the first server in the example, choose Create a New Farm. If this was the second server in your farm, you would select the second option, Join an Existing Farm. Click Next to continue.

The next screen is very important because you have to make three choices here. The first is to name your new server farm. For this example, call it **Elinet**. The second choice is to select between direct or indirect mode for access to your IMA Data Store. By now, you should have made a decision about how you will host your IMA Data Store and, as such, should choose accordingly. If your choice is to host the Data Store on a dedicated database server, you should select the second choice, Use the Following Database on a Separate Database Server, which takes you through the steps to configure your ODBC connection to point to your database on your server.

For the purposes of this example and because you are running a small farm, select the first option, Use a Local Database on This Server. Now that you have made your choice, select between Microsoft Access and Microsoft SQL Server Desktop Engine (MSDE) Database. We chose Microsoft Access.

The final decision you have to make on this screen is the zone name. You may choose to accept the default zone name, which is the subnet address where this server is configured. You can always rename the zone later from within the Management Console. For now, accept the default and click Next.

## Selecting the Farm Administrator

You now have to select a user account that will be the first Citrix Farm Administrator account. This step is necessary because you will use this account later to log on through the Management Console. Later, you can add more Citrix Farm Administrators from within the Management Console. Enter the local Administrator account of the server you are on, and for the Domain field, enter the name of the server that you are on, as shown in [Figure 5.3](#). Click Next to continue.

Figure 5.3. Citrix Farm Administrator.



## Identifying the Citrix License Server

The next window that pops up requires you to enter information about the Citrix License server. You are presented with two choices. First, you can choose Enter the Hostname of the Machine Hosting Your Citrix License Server and specify which port it is configured to operate on. Then if you did not change the default port number, you can simply check the box next to Use Default Port. The second choice is Enter the Correct Host Name Later. You can always correct the hostname later from the Management Console. For the purposes of this example, enter the host name **Elinet** and click OK to continue.

### Note

Citrix recommends that during the installation of the first MPS server in the farm, you always

manually enter the correct hostname of the license server. This is important because during the installation of MPS, you can skip this step and use the Management Console later to specify a server.

## Configuring Microsoft Remote Desktop Web Authentication

With the introduction of Citrix MetaFrame Presentation Server 3.0, administrators can now publish applications for users of Microsoft's Remote Desktop Web Connection software. Because the application is no longer limited to ICA, you can also publish Remote Desktop Protocol (RDP) applications. At this point in the installation process, you are asked whether you want to allow users of RDP-published applications to enter a password when launching applications or to pass their credentials through. Usually, when you deploy applications using the Citrix Web Interface, you log on to the web server, which prompts you for a username and password.

The web server uses this username and password combination to query the farm for the published applications that you have access to. When it knows which applications you are allowed to use, it displays them for you. Now when you attempt to launch a published application, users of the ICA protocol are not prompted again to enter credentials. However, RDP users are prompted by the server that is hosting the application for a second authentication. This setting allows you to control that behavior. The default setting is No, which always prompts users for a second authentication. For the purposes of this example, choose Yes, as shown in [Figure 5.4](#). This setting passes the credentials that the user submits at the web server and thus does not prompt him or her a second time. Click Next to continue through the installation wizard.

Figure 5.4. Remote Desktop web authentication.



## Alert

With the introduction of Remote Desktop Web client support, Citrix now assigns a Presentation Server client access license (CAL) to any RDP-based connection. Even direct RDP connections will now consume a Citrix CAL.

## RDP Passthrough Authentication

If at any time you want to revert back to the old setting and want users to be prompted for a secondary authentication for any reason, such as added security for RDP applications, do the following to reset the permissions:

1. Choose Start, Programs, Administrative Tools, Terminal Services Configuration.
2. Click the connection type in the left control pane.
3. Right-click RDP-TCP in the right control pane and select Properties.
4. Select Logon Settings.
5. Check the box next to Always Prompt for a Password.
6. Click OK.

## Note

Microsoft Remote Desktop Web Authentication is supported only on Windows 2000 Terminal Services. It is not supported with Windows Server 2003.

## Note

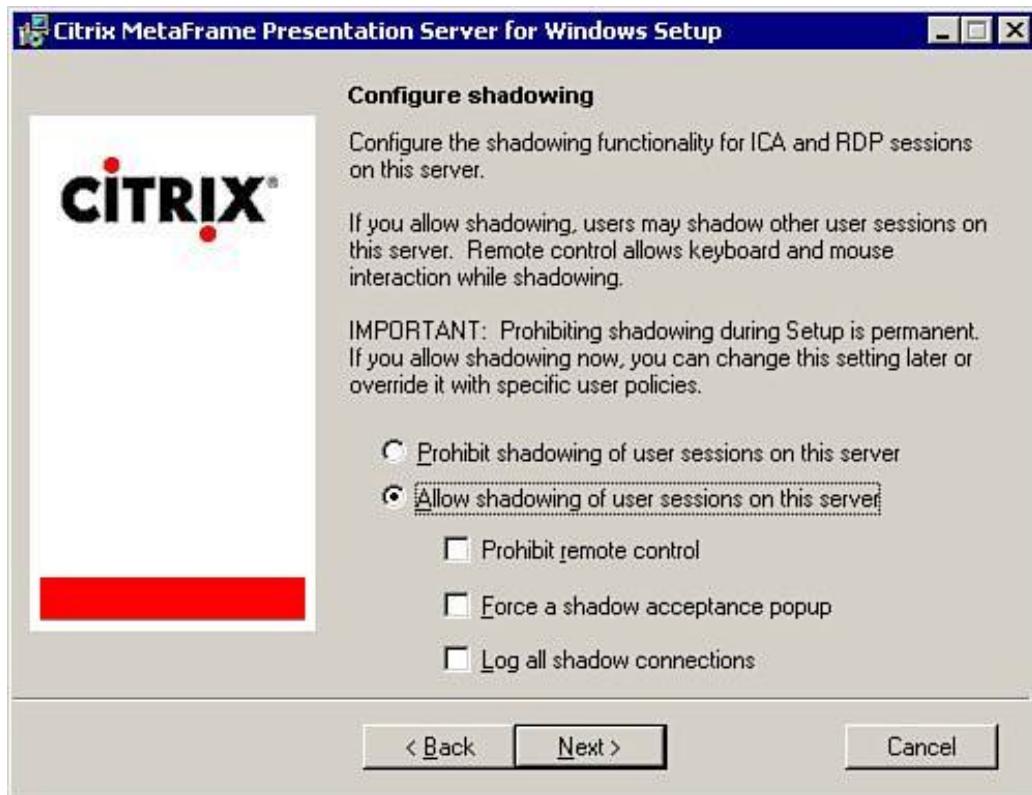
Even though selecting Yes on this wizard screen does not prompt users for a username and password to launch applications, users are still prompted to enter the proper credentials when logging in to the Web Interface.

## Configuring Shadowing

It is crucial that you make the proper choice on the next installation wizard screen because the choices you make here can be undone or modified only by reinstalling MPS 3.0. This screen configures the shadowing permissions on this server. [Shadowing](#) is a fancy name for remote control of user sessions. You are offered two options. You can choose either Prohibit Shadowing of User Sessions on This Server, which means no shadowing of any sort will occur on this server, or you can choose Allow Shadowing of User Sessions on This Server, at which point you can select from three choices to further configure this second option.

For the purposes of this example, choose the second option. You can now further customize the permissions by selecting one of the three choices shown in [Figure 5.5](#).

Figure 5.5. Configuring shadowing permissions.



The Prohibit Remote Control option allows the administrator or user to shadow another session, but this user cannot control the mouse or use the keyboard to input data.

The second choice, Force a Shadow Acceptance Popup, means that the administrator or any user with shadow capabilities cannot shadow another user's session without that user's consent. This is a great setting that prevents the misuse of this tool. Select this option for now.

The third option, Log All Shadow Connections, is also a great feature that keeps a record of all sessions shadowed in the event that you need to refer back to them. Select this option as well and click Next to continue.

## Installing the Citrix XML Service

You next arrive at the Citrix XML Service Port window. This window prompts you to enter a port number on which the XML services will listen. The default is port 80. The XML port is used in conjunction with the Web Interface (WI) and is the method by which the WI queries the MPS server for a list of published applications to which the user has access. So when a user enters credentials at the WI portal, the web server queries a server in the server farm on the configured XML port and returns a list of published applications the user has access to. Accept the defaults and click Next to continue.

## Note

To modify the Citrix XML Service Port after you have installed MPS 3.0, stop the Citrix XML Service, open a command prompt, and enter the command

```
ctxxmlss /rxx
```

where **xx** is the number you wish to change it to. So if you want to change it to port 90, the command would look like this:

```
ctxxmlss /r90
```

## Wrapping Up!

The final installation wizard window is a review window that gives you one summarized look at the options you selected before the wizard starts the installation. Ensure everything is the way you want and click Finish to begin the installation.

Installation is under way, and when it's finalized, you are presented with a window that offers two check boxes. The first is to launch the ICA Client Distribution Wizard, which we cover in [Chapter 13](#). The second option is to view the Readme file. For this example, leave both check boxes unchecked and click Close to exit the wizard.

You are then presented with a window that summarizes what was installed on this server. Click Finish. When you are finally prompted to reboot the server, click Yes or No.

 PREV

NEXT 

## MetaFrame 1.8 Server Migration to MPS

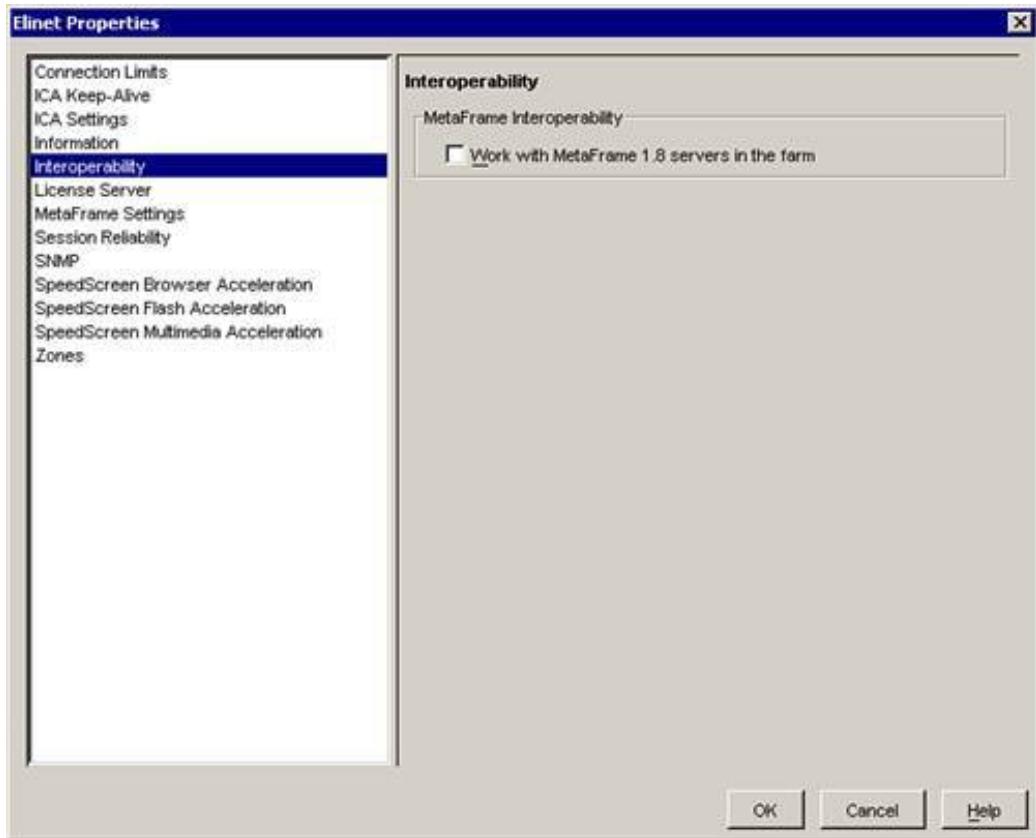
The migration process from MetaFrame 1.8 to MPS 3.0 requires the completion of certain steps to ensure that the environment continues to run properly. Because of the architectural changes evident between MF 1.8 and MPS, it is imperative that the farm be placed in "interoperability" mode, which basically means that the server farm is backward compatible. This allows MF 1.8 and MPS servers to coexist and serve users. Interoperability mode, however, is temporary, and Citrix strongly recommends that this be a transitional phase. After the last MF 1.8 server has been migrated, the farm should be placed in Native mode so that you can take full advantage of all the new features and technologies of MPS.

Here are the steps required to complete a migration from MF 1.8 to MPS 3.0:

1. If you plan to use a dedicated database server for your IMA Data Store, make sure your database is ready.
2. Install and configure your Citrix License server.
3. Upgrade an existing MF 1.8 server that is not the current Master ICA Browser. This step is very important; otherwise, all sorts of problems will occur in your environment.
4. During the installation of the first MPS server, give your new server farm the same name as your existing one.
5. After the installation is complete and the server is restarted, this upgraded server automatically becomes the new Master ICA Browser.
6. Place your new server farm in interoperability mode by launching the Management Console, right-clicking the Farm node, and selecting Properties. Now select Interoperability on the left and check the box next to Work with MetaFrame 1.8 Servers in the Farm (see [Figure 5.6](#)).

Figure 5.6. Remove the server farm from interoperability mode.

[\[View full size image\]](#)



7. Begin migrating existing MF 1.8 servers and make sure that during installation you choose Join an Existing Farm.
8. After the last MF 1.8 server has been migrated and there is no need for the farm to remain in interoperability mode, launch the Management Console, right-click the Farm node on the left, and click Properties. Select Interoperability and uncheck the box next to Work with MetaFrame 1.8 Servers in the Farm so the screen looks like [Figure 5.6](#).

[PREV](#)

[NEXT](#)

# Unattended MPS Installation Support

In many cases, you will find that having the capability to do an unattended installation of MPS is very useful. An unattended installation basically means that you prepopulate all the prompts that you are faced with during a normal installation within a text file; then you run the installation, pointing it to that text file for answers to prompts.

This capability is especially useful if you are deploying a large number of servers or if you are installing MPS from a remote location or to several locations.

Citrix provides you with a sample answer file that you can customize and use for your unattended installs. This sample file is located on the MPS 3.0 CD-ROM in the following path:

`Support\Install\UnattendedTemplate.txt`. You can use another file in the same directory, called `UnattendedInstall.exe`, to trigger the unattended install.

The process for running an unattended install is as follows:

1. Make a copy of the `UnattendedTemplate.txt` file and name it something else; we called ours `unattend.txt`.
2. Open the file with any text editor such as Notepad.
3. Configure the file with your configuration. The file also provides suggestions about every setting.
4. Save the file.
5. Copy the `mps.msi` package, the `unattend.txt` file, and the `unattendedinstall.exe` file into one directory. You can find the `mps.msi` file in the `MetaFrame Presentation Server` directory on the CD-ROM.
6. From a command prompt, switch to the directory where you saved all three files and run the following command:

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

In our case, the command would look like this:

```
UnattendedInstall mps.msi unattend.txt
```

# Uninstalling MetaFrame Presentation Server 3.0

As with any software, at some time you may have to uninstall MPS from a particular server, whether for troubleshooting purposes or to install a newer version. In most cases, you can go into Control Panel and Add/Remove Programs and then just remove MPS. However, in some cases, when the server has lost connectivity to the Data Store and must be forcefully removed from the server, you can follow these steps to force an uninstall:

1. Make sure no applications are open.
2. Copy the `mps.msi` file from the `MetaFrame Presentation Server` folder on the MPS CD-ROM to a location on your hard drive. For the purposes of this example, copy it to the root of `C:\`.
3. Open a command prompt and run the following command:

```
msiexec /x c:\mps.msi /L*v CTX_MF_FORCE_SUBSYSTEM_UNINSTALL=Yes
```

4. The wizard runs and uninstalls MPS from the server.

## Note

You can output the results of the MPS uninstall that was triggered by the `msiexec` command by adding a path and filename to the command like this: `msiexec /x c:\mps.msi /L*v c:\output.log CTX_MF_FORCE_SUBSYSTEM_UNINSTALL=Yes`.

## Exam Prep Questions

1. If you are installing MetaFrame Presentation Server and your CD-ROM doesn't display the splash screen automatically, which program do you use to trigger the installation?

- A. `autoboot.exe`
- B. `autostart.exe`
- C. `autoroot.exe`
- D. `autorun.exe`

A1: Answer D is correct. When running the installation manually whether from a network share or by double-clicking the file on your CD you need to run the `autorun.exe` file. Choices A, B, and C are incorrect because no such files exist on the MPS 3.0 CD-ROM.

2. How should you configure your server farm if you intend to have MetaFrame 1.8 servers in the farm?

- A. Both farm names must be in all lowercase letters.
- B. Both farm names can contain only letters.
- C. Both farm names must be in all uppercase letters.
- D. Both farms should be named the same.

A2: Answer D is correct. During a migration from a 1.8 farm, the MPS 3.0 farm's name should match exactly the name of the 1.8 farm for them to coexist. Choices A, B, and C are incorrect because these requirements are not a necessity for MF 1.8 and MPS 3.0 server farms to coexist.

3. Which of the following database types is not supported and cannot host the IMA Data Store?

A. IBM DB2

B. Microsoft Access

C. Microsoft SQL MSDE

D. FoxPro

A3: Answer D is correct. FoxPro is not a supported database type that can host the IMA Data Store. Choices A, B, and C are all supported database types.

4. Which of the following statements is true given that shadowing restrictions are configured during the installation of MetaFrame?

A. A Citrix administrator can change the shadow settings at any time from within the Management Console.

B. A Citrix administrator can change the shadow settings at any time by running the command-line utility `secedit`.

C. A Citrix administrator can change the shadow settings at any time from within the Citrix Connection Configuration.

D. A Citrix administrator cannot change shadowing settings. When setup is complete, the shadow settings can be changed or modified only by reinstalling the MPS software.

A4: Answer D is correct. As a security measure, after the shadow settings have been configured during the installation of MPS, they can be changed or modified only by reinstalling the software. Choice A is incorrect because you cannot change shadow settings from the Management Console. Choice B is incorrect because `secedit` is not a Citrix command and thus cannot be used to change shadow settings. Choice C is incorrect because the Citrix Connection Configuration tool cannot change shadow settings.

5. If you intend to run a server farm that has MetaFrame 1.8 servers being used in conjunction with MPS 3.0, in what mode should your farm be running?

A. Integrated

B. Interoperability

C. Native

D. Balanced

A5: Answer B is correct. For MF 1.8 and MPS 3.0 servers to coexist in the same farm and service users, the MPS 3.0 farm should be in interoperability mode; this mode allows MPS 3.0 servers to play the role of the Master ICA Browser. Choice A is incorrect because there is no such thing as an integrated mode. Choice C is incorrect because native mode means there are no MF 1.8 servers in the farm, and Choice D is incorrect because there is no such thing as a balanced mode.

6. You are upgrading your first server from MF 1.8 to MPS 3.0, and you want to use Microsoft SQL MSDE as the database software for the Data Store. Which option(s) should you select? (Choose all that apply.)



- A. Create a New Farm.
- 
- B. Join an Existing Farm.
- 
- C. Use a Local Database for the Data Store.
- 
- D. Use a Third Party Database for the Data Store.

A6: Answers A and C are correct. When upgrading the first MF 1.8 server to MPS 3.0, you should first choose to create a new farm, which will then be hosted using a database on that server. Microsoft SQL MSDE is a database type that can be hosted on one of your MPS servers, and as such, choice C is correct. Choice B is incorrect because there is no IMA Data Store yet, so you cannot join an existing farm. Choice D is incorrect because Microsoft SQL MSDE is not a third-party database software that will be hosted on its separate server.

7. If, during setup, you choose to use the default zone name, what would that name be?



A. The name of the server



B. The domain or workgroup of which the server is a member



C. The IP address of the server



D. The subnet ID where the server is a member

A7: Answer D is correct. The default name for the zone during setup is the subnet ID to which that server belongs. Choices A, B, and C are incorrect because they are not the default names given to a zone during setup.

8. You have been hired to build the Citrix MPS server farm for company XYZ. As part of your design plan, you want to remap server drives to minimize user confusion and allow users to see their local drive letters when logged in through an ICA session. What tool should you use to accomplish this?



A. ServerDriveRemap.exe



B. RemapDrives.exe



C. DriveRemap.exe



D. RemapServerDrives.exe

A8: Answer C is correct. The tool used to remap server drive letters is called `DriveRemap.exe`. Choices A, B, and D are incorrect because no such tools or utilities exist.

9. One of your MPS servers is not behaving properly, and you decide to uninstall MPS from this server. When you try using Add or Remove Programs in Control Panel, the uninstall process does not complete successfully. After researching the issue, you figure out that there is a way to force the uninstall of MPS via a command line. The first part of the command is `msiexec/x c:\mps.msi /L*v c:\output.log`. What is the proper syntax for this command to force an uninstall of MPS 3.0?



A. `CTX_MPS_FORCE_SUBSYSTEM_UNINSTALL=Yes`



B. `CTX_MF_FORCE_SUBSYSTEM_UNINSTALL=Yes`



C. `CTX_MF_FORCE_SUBSYSTEM_UNINSTALL /Y`



D. `CTX_MPS_FORCE_SUBSYSTEM_UNINSTALL /Y`

A9: Answer B is correct. The correct continuation of this command is `CTX_MF_FORCE_SUBSYSTEM_UNINSTALL=Yes`. Choices A, C, and D are incorrect because they are not the proper syntax and don't exist.

10. Which tool can you use to modify the default port that the Citrix XML service listens on? And what is the proper syntax for modifying the XML port?



A. `ctxxmlss /rxx`



B. `ctxxmls /rxx`



C. `ctxmlss /rxx`



D. `ctxxmlss /pxx`

A10: Answer A is correct. The correct tool and syntax to modify the XML port number is `CTXXMLSS /rxx`, where `/r` represents your request to change the port and `xx` represents the new port number you want to configure. Choices B, C, and D are incorrect because either the tool does not exist or the syntax is incorrect.

 PREV

NEXT 

## Need to Know More?

In [Chapter 3](#), "Installation Prerequisites for MetaFrame Presentation Server 3.0," we explained the Data Store requirements and the different methods by which you can implement the Data Store. This step in the installation wizard allows you to implement the Data Store type that best suits your deployment.

# 6. Configuring and Administering MetaFrame Presentation Servers

Terms you'll need to understand:

- Management Console
- SpeedScreen Latency Reduction
- Citrix Connection Configuration
- MetaFrame administrators

Concepts you'll need to master:

- The Shadow Taskbar
- SpeedScreen technology
- The Farm node properties
- The Servers node properties

The Management Console is the single-most important administration tool that you will be using on a daily basis to manage and configure your server farm. Since Citrix introduced MetaFrame XP and now MetaFrame Presentation Server (MPS) 3.0, it has consolidated all the previous management tools into one console. Tools that were standalone in MetaFrame (MF) 1.8, such as Published Applications Manager and Citrix Server Administration, have seen their functions incorporated into the console.

This chapter eases your introduction to the Management Console, covering all its functionality and configurable parameters. We discuss how the Management Console allows you to remotely plug in to your servers and configure them along with other resources and services such Resource Manager and Installation Manager, which are described in later chapters. You should also note that depending on the version of MetaFrame you load, the Management Console will populate itself with additional plugins to various tools. For example, if you load MetaFrame Presentation Server, Standard Edition, you do not see the Load Manager (LM) node, nor do you see the Resource Manager (RM); LM can be enabled with the Advanced and Enterprise Editions, while RM can only be enabled with the Enterprise Edition.

# Components of the Management Console

The Management Console is divided into two control panes. The left pane consists of the various nodes or plug-ins available to administer and configure the servers and farm. The pane on the right consists of the configurable values.

The left pane contains the following:

- *Farm node* The area of the console where you can configure settings on a global farm-wide range.
- *Applications node* The area where you can publish and configure applications.
- *MetaFrame Administrators node* The area where you can add, remove, or edit users who have access to log in to the console and the level of access they have.
- *Load Evaluators node* (Advanced and Enterprise Editions) The area where you can configure the load criteria for the servers.
- *Policies node* The area where you can configure policies that are enforced on ICA connections to the MPS servers.
- *Printer Management node* The area that contains all the printers and print drivers installed in the server farm.
- *Resource Manager node* (Enterprise Edition) The area that allows you to configure and monitor server resources.
- *Servers node* The area where all the MPS servers are located. From this node, you can configure, monitor, and manipulate all servers in the server farm.
- *Installation Manager node* The area where you can control the deployment of packages to MPS 3.0 Servers in the farm.

## Note

MetaFrame Presentation Server 3.0 introduced significant licensing changes. One of the most noticeable changes is that the Licenses node has been completely removed from the Management Console and placed in its own tool under the Citrix License Server. See [Chapter 4](#), "Installing and Managing MetaFrame Presentation Server," for more information.

# Administering MetaFrame Using the Management Console

The Management Console allows you to control all aspects of your farm. You can make global settings that are implemented farm wide by manipulating the different settings the Farm node offers, or you can make server-specific changes by making the changes directly to that server. In the following sections, we tackle both scenarios.

## The Farm Node

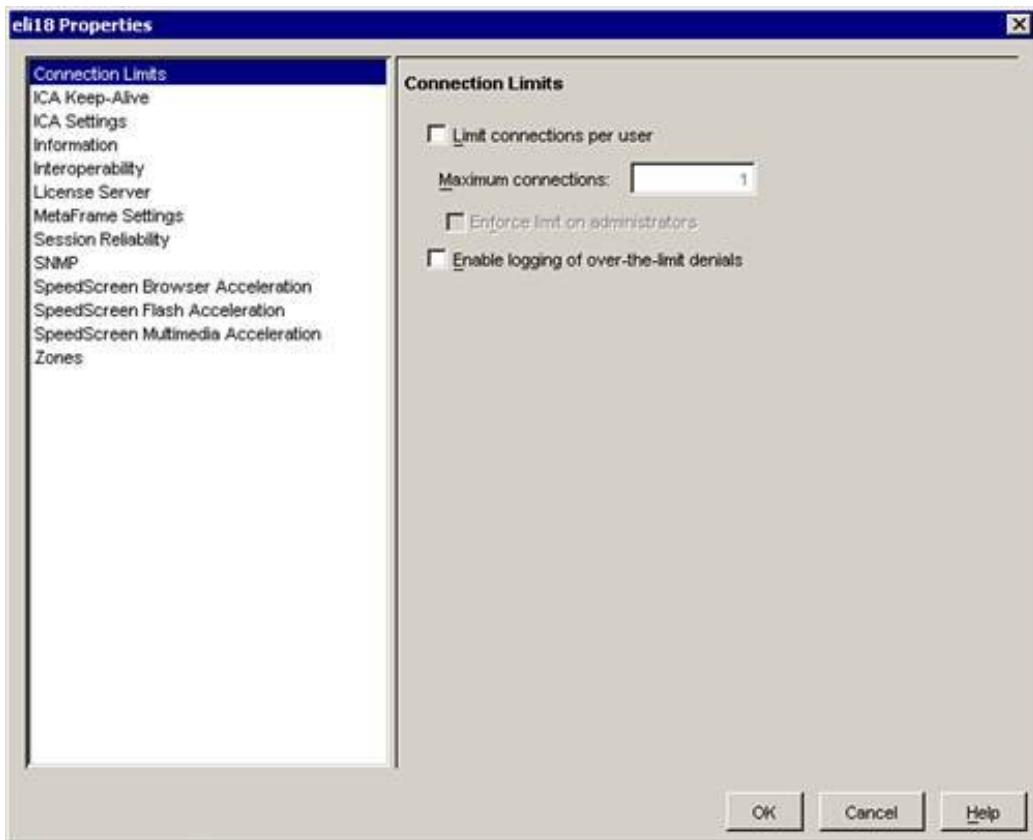
The Farm node allows you to make changes that will be enforced farm wide to all the servers. To access the farm properties, follow these steps:

1. Launch the Management Console and log in.
2. In the left control pane, right-click the Farm node, which is the first node and is always represented by the name of your farm, and then click Properties.

In the new window that opens, you can manipulate the different settings that can be applied farm wide (see [Figure 6.1](#)). These settings are described in the following sections.

Figure 6.1. Farm node properties.

[\[View full size image\]](#)



## Connection Limits

The Connection Limits option allows you to control how many ICA sessions a user is allowed to launch or have open at the same time. You can enable this setting by clicking the check box next to Limit Connections Per User and then enter a value in the Maximum Connections field. You can also choose to enforce this rule to administrators by checking the box next to Enforce Limit on Administrators.

You can also configure this rule to log repeated failed attempts to launch a session by checking the Enable Logging of Over-the-Limit Denials box.

## ICA Keep-Alive

Due to the nature of server-based computing, you always have clients who connect via various communications means. Some may connect from a WAN, whereas others may connect via a modem halfway across the world. In many instances, an ICA session is dropped; however, the Management Console may still report this session as being active. You can configure the ICA Keep-Alive setting to query ICA sessions at regular intervals for example, every 60 seconds. In the event that a response is not received within 60 seconds of a query, the server disconnects the user session automatically.

To enable ICA Keep-Alive, check the box next to Enable ICA Keep-Alive and set the Time-out value. The default setting is 60 seconds.

## Note

Prior to the release of MPS 3.0, you could configure ICA Keep-Alive only by creating the Registry entry `ICAKeepAlive`.

## ICA Settings

The settings you can configure on the ICA Settings window control how the server optimizes the display of graphics for optimal performance. The settings are as follows:

- *ICA Display* This section contains two configurable options: Discard Redundant Graphics Operations and Alternate Caching Method. The Discard Redundant Graphics Operations option strips the image from all the extra data it may contain (such as layers) and sends just enough information to properly display the graphic. Alternate Caching Method forces the server to use older algorithms that were used with MF 1.8. You can also specify the maximum amount of memory a session can consume for graphics by entering a value in kilobytes in the Maximum Memory to Use for Each Session's Graphics text box.
- *Degradation Bias* This section controls what actions need to be taken when the session's performance becomes unacceptable. You have two options: Degrade Color Depth First or Degrade Resolution First. Degrade Color Depth First means that when the session starts to lag, the server takes the first course of action; in this case, the action is to lower the color depth of the session to boost performance again. The second answer reduces the resolution of the session to boost performance. You also have the option of notifying the user when degradation will occur by checking the Notify User of Session Degradation box.
- *Auto Client Reconnect* This section controls the client auto reconnection to a dropped or disconnected session. You can force the user to reauthenticate to a dropped session for increased security by enabling Require User Authentication, and you can also enable Log Automatic Reconnection Attempts on the server to have some way of tracking these reconnections.

## Information

The Information window offers a summary of what is going on in your server farm. It is divided into three sections offering the following information:

- Connection Information offers information on current session count, which tells you how many sessions you currently have connected to different servers. It also shows how many Citrix MPS servers are members of this server farm.
- Published Resources summarizes and classifies your published resources. It gives you a count of published applications, published desktops, and published content.
- Zone Information offers a list of the different zones you have and the Data Collector for every zone.

## Note

Previously, the Information window listed the number of licenses in use. With the introduction of MPS 3.0, this information has been moved to the Citrix License Server.

## Interoperability

The Interoperability setting should be used only during a migration or an upgrade from MetaFrame 1.8 to MetaFrame Presentation Server. It has a single configurable setting: Work with MetaFrame 1.8 Servers in the Farm. Configuring this setting basically means that the MPS servers also respond to broadcasts by ICA clients. This setting should be temporary and should be disabled after the migration is over to take full advantage of the complete features of the Independent Management Architecture framework.

## License Server

The License Server window allows you to specify the hostname of the server that has the Citrix License Server software installed on it. That server should obviously also have activated connection licenses. The MPS servers query this server for licenses when they receive incoming ICA connections.

You can also configure the TCP port on which this license server is configured to function. The default is 27000.

## MetaFrame Settings

MetaFrame Settings can be applied to all MPS servers specifically in a global manner as follows:

- Broadcast Response allows you to enable or disable Data Collectors Respond to Client Broadcast Messages and also enable or disable RAS Servers Respond to Client Broadcast Messages. This capability typically is useful in a network with legacy applications where UDP is used to broadcast a message for a list of published applications.
- Client Time Zones allows you to enable or disable Use Client's Local Time. By enabling this feature, you allow the ICA client to broadcast its time to the server, and as such, any files the user creates are time-stamped with the user's local time as if he or she was creating this file locally on his or her machine. The second option is Disable Local Time Estimation. This option allows an administrator to disable local time estimation for the client; thus, any files the user creates are time-stamped with the server's time. Local time estimation is used in older clients where time could not be broadcasted; it uses the server's time in coordination with the user's time zone to estimate the local time where the user is working.
- Enable XML Service DNS Address Resolution allows you to enable or disable XML service DNS address resolution. For users to be able to take advantage of this, they must be using ICA client version 6.20.98 or higher.
- Novell Directory Services Preferred Tree allows you to specify a preferred tree for Novell Directory Services. Before you can configure a Novell Directory Services Preferred Tree, the Intranetware client should be installed on the MPS server.
- Enable Content Redirection from Server to Client allows you to enable or disable content redirection from the server to the client. For example, if you publish an HTML page, when the user clicks on the published content, it is launched via the Internet Explorer browser on his or her local machine rather than on the server.
- Enable Remote Connections to the Console is valid only with Windows Server 2003 servers.

If enabled, it gives you the option to right-click a server in the Servers node and launch a session directly to the server's console.

## Session Reliability

Session Reliability is a cool new feature introduced with MPS 3.0. It allows you to maintain a session even after you lose connectivity to the server in the event of a signal loss or an IP failure. Sometimes when you're working, all of a sudden your PC or mobile device may lose its signal or IP connectivity. With session reliability enabled, the session freezes for a period of time that you can preconfigure; the default is 180 seconds. After 180 seconds, or the interval you have specified, if the signal or IP connectivity is not restored, the session is dropped.

Session Reliability is enabled by default; you can set the time in seconds for how long it should remain active. To do this, enter the correct value in the Seconds to Keep Sessions Active field. MPS servers will listen on TCP port 2598 for attempts to restore a dropped connection.

### Note

Changes you make to the Session Reliability section take effect only after all the servers in the farm have been restarted.

## SNMP

The SNMP window allows you to configure how MetaFrame servers in your farm communicate notifications back to the SNMP Manager. The settings configured in this window have a farm-wide effect, which means they are enforced on every server. You can, however, override these settings on a server-by-server basis if you like. For more information on how to override the Simple Network Management Protocol (SNMP) settings on an individual server, check out the section "[The Servers Node](#)" later in this chapter.

To enable SNMP, you will, of course, need to install that component on your Windows machine by going to Add/Remove Windows Components in Add or Remove Programs from the Control Panel. You can add that component under the Management and Monitoring Tools. After it is installed, you can check the box next to Enable SNMP Agent on All Servers. When this feature is enabled, the following options in the Session Traps section are made available:

- Session Logon sends a trap notification every time a user logs on to a session.
- Session Logoff sends a trap notification every time a user logs off.
- Session Disconnect sends a trap notification every time a user's session is disconnected or if a user disconnects.
- Session Threshold Exceeded sends a trap notification when the session's threshold is exceeded. The session threshold is configured in the Session Limit Per Server text box.
- Session Limit Per Server allows you to specify the setting that should trigger a trap notification message. For example, if you enter **100** in the text box, as soon as the session count on a server reaches 100, a trap notification is sent out.

## **SpeedScreen Browser Acceleration**

SpeedScreen Browser Acceleration is the newest addition to the SpeedScreen technology family; it improves the performance of published applications that have GIF and JPEG images embedded in HTML pages. Examples of such applications include Microsoft Outlook, Microsoft Outlook Express, and Microsoft Internet Explorer 5.5 or later.

To take advantage of this technology, enable it by clicking the check box next to Enable SpeedScreen Browser Acceleration. After you enable this option, you can then enable another option that further allows you to tweak how much compression you want to apply. The higher the compression, the more bandwidth improvement is noticeable. Higher compression, however, means sacrificing image quality. Compression settings are Low, Medium, and High.

The Enterprise Edition of MetaFrame can take advantage of another option that you can enable by checking the box next to Determine When to Compress. This option allows the Enterprise Edition MPS server to determine when to compress based on bandwidth availability and image size.

## **SpeedScreen Flash Acceleration**

SpeedScreen Flash Acceleration is another new addition to the SpeedScreen technology family that improves the performance of Flash animations within an ICA session. The Flash Player would have to be installed on every MPS server that will play Flash animations. To enable this feature, you must click the check box next to Enable Macromedia Flash Player.

Selecting this check box, in turn, unlocks the option Optimize Flash Animations. Enabling Optimize Flash Animations, by clicking the check box next to it, allows you to then configure the optimization by either selecting Optimize Flash Animation for Restricted Bandwidth Connections or Optimize Flash Animations for All Connections.

## **SpeedScreen Multimedia Acceleration**

SpeedScreen Multimedia Acceleration improves the quality of streaming audio or video within an ICA session. The technology is developed in a very intelligent manner so as not to put strain on the server's CPU but rather lets the client's CPU take on the CPU utilization by rendering the stream.

To enable this technology, click the check box next to Enable SpeedScreen Multimedia Acceleration. You then have the option of tweaking the buffering settings by selecting one of two options in the Network Buffering section. You either can choose to select Use the Default Buffer of 5 Seconds, which is the recommended choice, or you can manually select the buffer settings by choosing the Custom Buffer Time settings and then setting it accordingly.

## **Zones**

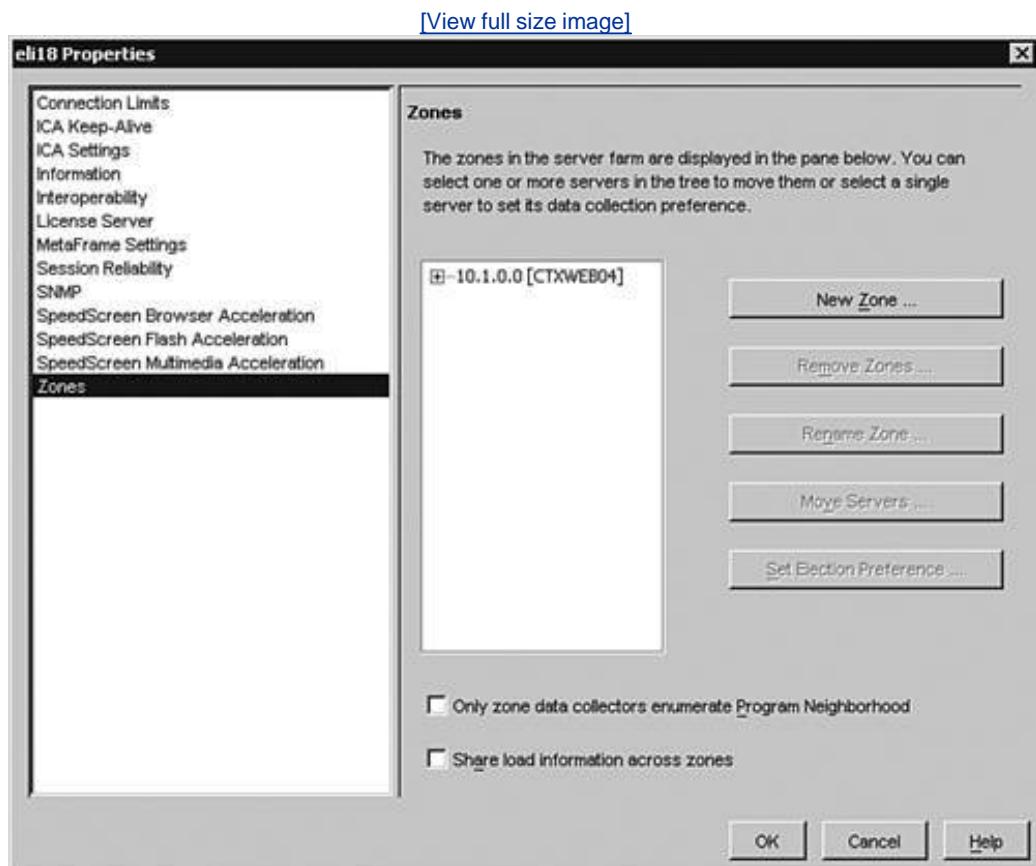
Zones are used to create a perimeter within which servers located in the same location can communicate. Servers should be divided into zones based on their geographical location to control the amount of inter-server communication and optimize performance. Zones are usually created by default based on servers' subnet memberships. However, in the event that servers belong to different subnets on the same network, you should create one zone, and you should make all the servers within a defined perimeter members of that zone. If, for example, you have two locations in the Chicago area that have MetaFrame servers, one downtown and one in Skokie, you should then have two zones, one

to group the downtown servers and the other to group the Skokie servers.

From within the Zones window, you can complete the following tasks (see [Figure 6.2](#)):

- New Zone allows you to create a new zone.
- Remove Zone allows you to remove an existing zone. Before you can remove an existing zone, however, you have to make sure that no servers are members of that zone.
- Rename Zone allows you to rename an existing zone.
- Move Servers allows you to move server memberships between zones.
- Set Election Preference allows you to specify the election criteria by which the zone Data Collector is chosen. You can set a server to have the Most Preferred setting, which means that this server will always be chosen as the Data Collector. Alternatively, you can set the preference to Preferred, which means this server is a favorite to win a Data Collector election. The third option is Default Preference, which basically means that this server may participate in the Data Collector election, and the last setting is Not Preferred, which means this server should never be elected as a zone Data Collector unless all the other servers with Most Preferred, Preferred, and Default Preference are unavailable.

Figure 6.2. Zones configuration window.



You also can enable the following two settings by checking the box next to each:

- *Only Zone Data Collectors Enumerate Program Neighborhood* When you check this box, you instruct the servers in the farm not to respond to client queries for published applications. You limit this role to the zone Data Collector by instructing it to respond to client queries or broadcasts for published applications.
- *Share Load Information Across Zones* When you check this box, you instruct the Data Collectors in every zone to share load information about their zone with each other.

## MetaFrame Administrators

The MetaFrame Administrators node allows you to add, remove, or edit a MetaFrame administrator. With MPS 3.0, you can now further customize an administrator's access rights based on a role that you create for him or her. For example, if your farm spans different geographical areas with servers in different cities, you can group your server in folders and then give MetaFrame administrators access to just that folder.

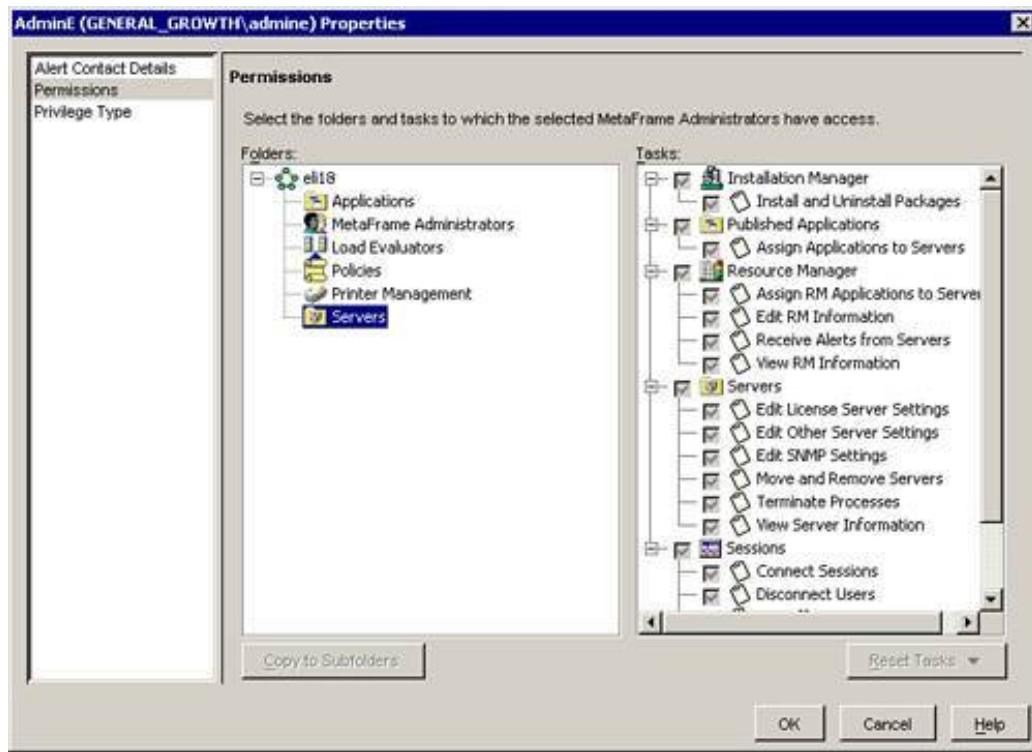
To add a MetaFrame administrator, right-click the MetaFrame Administrators node in the left control pane and click Add MetaFrame Administrator. Now browse your directory structure, locate the administrator account you want to add, click Add, and then click Next to proceed. The next screen allows you to provide information about the way alerts should be sent to this administrator; your options are Email, SMS Number, and SMS Gateway. Fill out the information accordingly and click Next to continue.

You are then presented with the following three options to choose from:

- View Only allows the administrator to browse the entire farm but does not give him or her the ability to make any changes.
- Full Administration grants the user account full administrative privileges over the farm.
- Custom allows you to tweak the permissions the user account gets. You have the option to limit permission on applications, servers, the nodes the user account can make changes to, and so on (see [Figure 6.3](#)).

Figure 6.3. MetaFrame Administrator custom settings.

[\[View full size image\]](#)



The last option on this window is Disable MetaFrame Administrator Account(s). This option creates the account with permissions you select but disables the account until such time when you are ready to allow the administrator to use it; at this point, you need to enable it.

## User Session Management

All user session management is administered via the Management Console. You can view user session information, interact with users, and provide any and all technical assistance needed. There are two ways to find, view, and interact with users in the Management Console. You can use either the Applications node or Servers node. The options in both scenarios are the same; the only difference is your preferred method on sorting the users and interacting with them.

If you use the Applications node to find users, all you have to do is expand that node, select the application the user is using, and then find the user in the right control pane. If you use the Servers node, all you have to do is expand that node and then select the server the user is connected to. You can also choose to remain at the top of the node, which means highlighting the actual Servers node, viewing all the users connected to all the servers, and interacting with them that way.

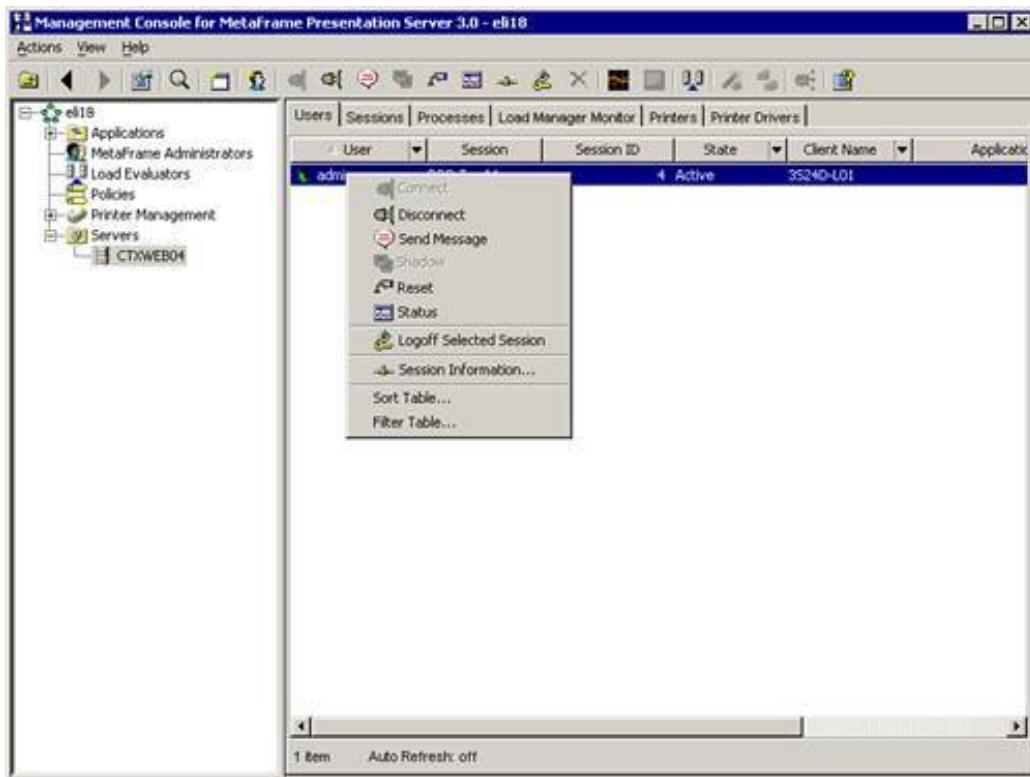
Regardless of your preferred method of finding the users, after you locate them, you can interact with them by right-clicking a user or users. The following options are then presented to you (see [Figure 6.4](#)):

- *Connect* This extremely useful option allows you, as an administrator, to connect a user's disconnected session. For example, if the user becomes disconnected from the server for any reason and his session remains in disconnect mode, you can connect to it, save the user's unfinished work, and log him off gracefully, thus saving hours of work.
- *Disconnect* This option can also be very useful. If you find a user who has been idle for two hours, for example, you may choose to place her session in disconnect mode to free up valuable server resources that would then be available to active users on that server.

- *Send Message* More often than not, you may need to communicate a message to your users. For example, if you see the server is running low on resources or a security vulnerability needs immediate attention, you can send your users a message asking them to save their work and log off.
- *Shadow* This is probably the most important and most sought-after feature. It allows you to control a user's session remotely for any number of reasonsmost importantly, technical support or training.
- *Reset* This action item resets a user's session. It kicks the user off the server immediately, so it should be used properly.
- *Status* This useful troubleshooting option allows you to query the user's session and ensure that it is still communicating and exchanging packets.
- *Logoff Selected Session* This option allows you to log off a user's session. The difference between logging off a user's session and resetting it is that this option logs off the user session in a graceful manner rather than just kicking the user off immediately.
- *Session Information* This option gives you vital information about the session, such as the Session Processes, Session Information, Client Modules, and Client Cache.
- *Sort Table* This option allows you to sort the method by which information is displayed, for example, username first, server the user is logged into second, logon time, and so on.
- *Filter Table* This option allows you to filter for certain fields. You can use this option when you have server names that begin with DLM, for example; you can set the filter so that it displays just these servers.

Figure 6.4. User administration and interaction menu.

[View full size image]



## The Servers Node

The Servers node allows you to administer and/or configure servers in the farm on an individual basis. It also allows you to organize the servers into folders for easier navigation and administration. In addition, the Servers node allows you to override farm-wide settings that were enabled on the Farm node. An example is the SNMP settings.

To get to the properties of a server, right-click it and select Properties. You are then presented with a window that allows you to make changes to that server only. You can select SNMP and uncheck the check box next to Use Farm Settings. Then you can enter manual information for that server.

From the Properties window of a server, you have the following options:

- Hotfixes displays a list of Citrix and Microsoft hotfixes. It also shows you who installed the hotfix and on which date.
- [ICA Keep-Alive](#) was discussed in the section on the farm. You can override the farm settings here and apply server-specific settings.
- ICA Printer Bandwidth allows you to control the amount of network bandwidth available for printing via this server. The options are Unlimited and Limited. When selecting the latter, you can set the amount of bandwidth that can be used in kilobytes by entering a value in the box labeled Bandwidth to Use (Kbps).
- ICA Settings were covered in the farm node section. You may choose to override the farm-wide settings and configure different settings for servers on an individual basis.
- Information displays information specific to this server such as the operating system it is running, the network it is configured on, MetaFrame version, ICA port, and so on.

- License Server allows you to override the farm settings specified for license server and configure the server manually to point to a specific license server. It also allows you to specify the port on which it should connect.
- MetaFrame Settings allows you to configure settings specific to this MPS server. You can choose Create Browser Listener on UDP Network, which allows this MPS server to respond to ICA client broadcasts on UDP networks. You can also enable Server Responds to Client Broadcast Messages, which responds to ICA client broadcast messages. This option is supported only in Native mode. You can control whether a server accepts ICA sessions by enabling or disabling Enable Logons to This Server. You can also choose to log the use of the shadowing capabilities by enabling or disabling Enable Shadow Logging on This Server. You can change the port for the Citrix XML service by modifying the value of the TCP/IP Port text box. The Enable Content Redirection from Server to Client option was discussed in the section on farm node settings; here, you have the option of overriding the farm node settings. In Remote Console Connections, you can choose to use farm settings, or you can override them and select Enable Remote Connections to the Console; this feature works only with Windows Server 2003.
- Published Applications displays information about applications published on this server.
- SNMP was covered in the section on farm node properties. You may override the farm settings and specify server-specific settings.
- [SpeedScreen Browser Acceleration](#) was discussed in the section on farm node settings. You may override those settings here and specify server-specific settings.
- [SpeedScreen Flash Acceleration](#) was discussed in the section on farm node settings. You may override those settings here and specify server-specific settings.
- [Workspace Control](#), also known as "follow-me roaming," is a new feature introduced with Web Interface 3.0. It basically allows a user to disconnect, reconnect, or log off one or all of his or her published applications. This feature is very useful for users who move around from device to device and want to quickly reconnect to their published applications. You can disconnect on one ICA device and then go to the next one and reconnect to all your disconnected applications. To enable this feature, select Trust Requests Sent to the XML Service.

 PREV

NEXT 

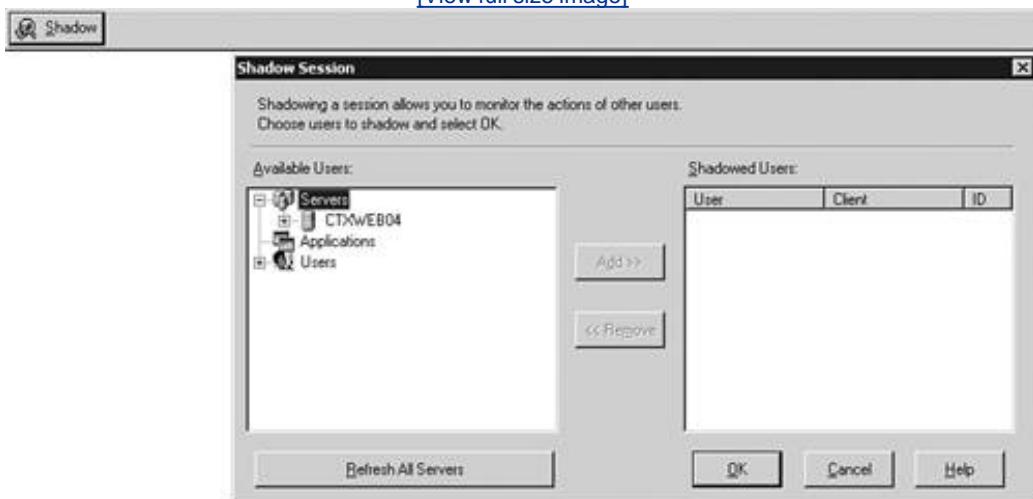
## Using the Shadow Taskbar

The Shadow Taskbar is another method by which you can shadow multiple users. It is a tool dedicated to shadowing. One benefit of using it is the ability to shadow multiple users and switch between shadowed sessions in an easy and convenient manner.

To start the Shadow Taskbar, click Start, Programs, Citrix, Administration Tools, Shadow Taskbar. Once launched, the Shadow Taskbar looks a lot like the Windows Start Taskbar, except it positions itself at the top of the screen and has the word *Shadow* instead of *Start* (see [Figure 6.5](#)).

Figure 6.5. The Shadow Taskbar.

[View full size image]



After you click *Shadow*, a window opens, giving you the following three methods by which you can search for users to shadow:

- Servers lists the users based on the server they are connected to.
- Applications lists the users based on the published application they are connected to.
- Users lists all the users, and you have to go through the entire list to find the user you are looking for.

After you locate a user you want to shadow, you simply click *Add*, which adds him or her to the list of users you plan to shadow. After you add all the users you want to shadow, click *OK*. This action launches separate shadow sessions to every user and places a tab on the Taskbar so you can easily toggle between sessions just as you toggle between applications in Windows.

# Connection Management Using Citrix Connection Configuration

The Citrix Connection Configuration (CCC) utility allows you to configure the ICA protocol to run over different types of communication and network protocols. For example, ICA over TCP is the most commonly used combination. The Citrix Connection Configuration then allows you to tweak the protocol setting limitations and configurations.

To launch the Citrix Connection Configuration, click Start, Programs, Citrix, Administration Tools and then select Citrix Connection Configuration. Once launched, the CCC displays all the transport protocols configured with ICA. If you have multiple network interface cards (NICs) in your server, the Network Transport Configuration section allows you to specify which one to associate with this protocol. You can also choose to leave the default setting All Network Adapters Configured with This Protocol, which uses any NIC that has a connection.

You may also want to specify the number of connections that can be made via this protocol. The default is set to Unlimited. If you wish to change the number, uncheck the box next to Allow Unlimited Connections to Winstation and then set a limit in the Maximum Connection Count text box.

From the same window, you also can further customize and configure the protocol using the three tabs: Advanced, ICA Settings, and Client Settings.

## The Advanced Tab

The Advanced tab allows you to configure numerous settings determining how the protocol should behave and what it should tolerate, allow, and disallow. The available configuration settings are as follows (see [Figure 6.6](#)):

- Logon provides two choices, Enabled and Disabled, for connecting to the server via this particular protocol.
- Connection Timeout Settings allows you to set the timeout setting in minutes for a connection. If you set it to 60 minutes, for example, a user session is disconnected after being in use for 60 minutes. This option is usually used for sensitive financial applications for which security is very strict.
- Disconnection Timeout Settings specify how long a session can remain in a disconnected state.
- Idle Timeout Settings control how long a session may remain idle before it is kicked off the server.
- Required Encryption controls the encryption level between the client and server. The default is Basic (less than 40 bits), but you can lower it to None or raise it to 128-bit (login only), 40-bit, 56-bit or 128-bit encryption. You also have the option to enable or disable Use Default NT Authentication. If this option is enabled, the server uses the default Windows NT authentication DLL ([MSGINA.DLL](#)), ignoring third-party software that may be installed on the server. If this option is left unchecked, authentication happens through a third-party DLL. In the case of Citrix,

authentication happens through the **CTXGINA.DLL**.

- On a Broken or Timed-Out Connection allows you to control the course of action that needs to be taken when a session times out or is broken. Your options are either to reset that session or disconnect it.
- Reconnect Sessions Disconnected controls a user's ability to reconnect to a disconnected session. You can allow a user to reconnect from any client or from this client only.
- Shadowing allows you to control how shadowing occurs on this server. You have three options. You can disable shadowing altogether. You can select Is Enabled: Input ON, Notify ON, which means the person shadowing can control the keyboard and mouse but has to notify the user and get permission to shadow his or her session. Or you can select Is Enabled: Input OFF, Notify ON, which means that you can shadow a user's session, but you cannot control the keyboard or mouse and you still need to get permission from the user before you shadow him or her.

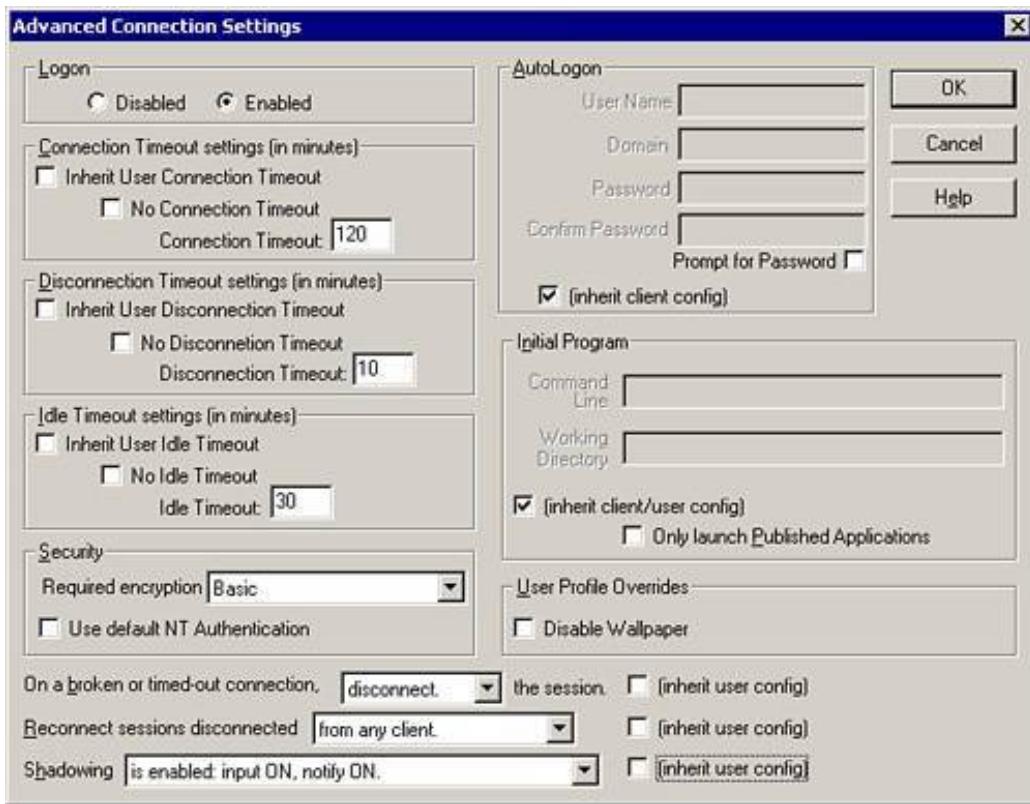
## Alert

Options that appear in the Shadow settings are subject to the way you configured shadowing during the installation of MPS. If, for example, you disabled shadowing during setup, you cannot enable it here. Options here work within the framework of the general settings you configured during setup.

- AutoLogon logs anyone who connects to this server automatically using the user credentials you provide. This section allows you to prepopulate the username, password, and domain information that will be presented to the server when a connection is made. For tighter security, you may want to check the option Prompt for Password, which forces the user to enter a password.
- Initial Program allows you to configure an application to launch as soon as a user logs on to this Terminal Server. Using it is a way to lock down the server by giving users access to run only this specific application.
- User Profile Overrides provides only one option, Disable Wallpaper. If this option is selected, if a user has a wallpaper defined, it is disabled and does not show up when he or she logs in.

Figure 6.6. Citrix Connection Configuration, Advanced settings.

[\[View full size image\]](#)



## The ICA Settings Tab

The ICA Settings tab allows you to configure the audio quality the user receives through his or her client device. It is a compression algorithm and allows for three options:

- Low compresses the data to 16KB before sending it to the client device.
- Medium compresses the data or audio stream to 64KB before sending to the client device.
- High sends the data uncompressed using its raw format. To get smooth, unbroken audio, you need 1.3 mbps of bandwidth when selecting this setting.

Using High taxes the server's CPU quite a bit because of the network traffic that it transmits.

## The Client Settings Tab

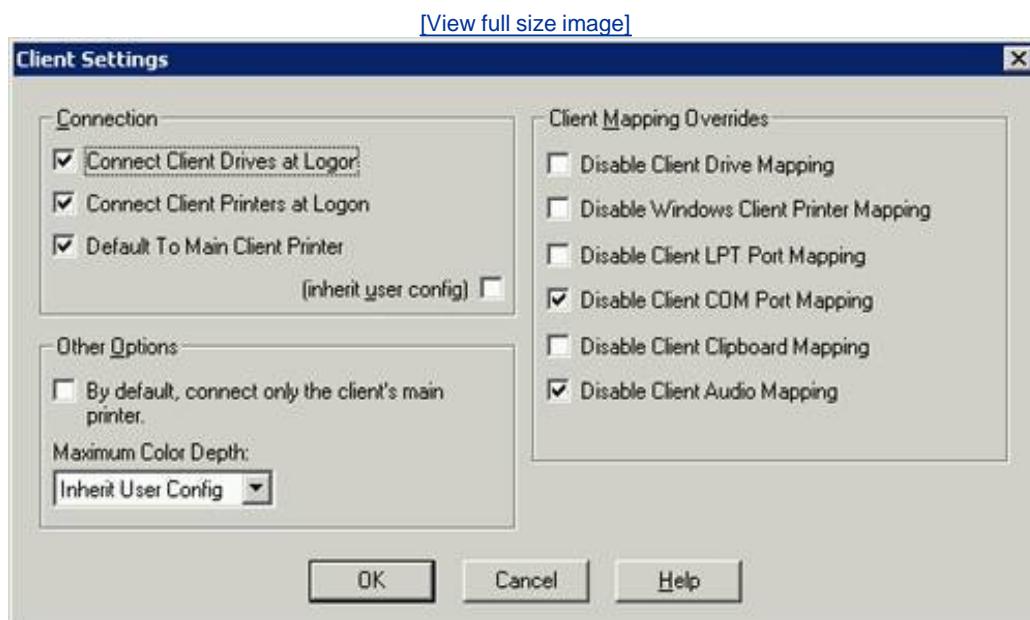
The Client Settings tab allows you to configure global settings that affect all users connecting to this MPS server. The configurable settings are as follows (see [Figure 6.7](#)):

- *Connect Client Drives at Logon* The server remaps the client's local drives on the server and gives users access to their local drives from the server.
- *Connect Client Printers at Logon* The users see their locally installed printers appear within their ICA session.
- *Default to Main Client Printer* A user's default printer on his or her local machine is made the

default printer within his or her ICA session.

- *By Default Connect Only the Client's Main Printer* The server connects only the user's default printer from his or her local machine.
- *Maximum Color Depth* This setting controls the maximum color depth of the session. The available options are 8 bit, 15 Bit, 16 Bit, and 24 Bit.
- *Disable Client Drive Mapping* This setting disables the client's local hard drives from being mapped within an ICA session.
- *Disable Windows Client Printer Mapping* No printer mapping from the client to the server occurs, and the user cannot get access to his or her locally installed printers.
- *Disable Client LPT Port Mapping* LPT port mapping from the client to the server does not occur, and any devices configured on the client's LPT port are not available through the ICA Session.
- *Disable Client COM Port Mapping* The client's COM port is not mapped on the server, and any devices configured on the client's COM port do not map to the server.
- *Disable Client Clipboard Mapping* The Clipboard option is disabled between the server and the client, and the copy paste commands do not work.
- *Disable Client Audio Mapping* Audio is not available through an ICA session.

Figure 6.7. Citrix Connection Configuration, Client settings.



◀ PREV

NEXT ▶

# SpeedScreen Latency Reduction Manager

In [Chapter 2](#), "MetaFrame Presentation Server Architecture," we discussed SpeedScreen technology and the way it uses a set of algorithms to update the portion of the screen that has changed rather than refreshing the entire screen. We also discussed how SpeedScreen does this with the help of two features: Local Text Echo and Mouse Click Feedback. In this chapter, we discuss how you can configure the applications on the MPS servers to take advantage of this technology through the SpeedScreen Latency Reduction Manager.

To launch the SpeedScreen Latency Reduction Manager, click Start, Programs, Citrix, Administration Tools, SpeedScreen Latency Reduction Manager. The first window displays the server name and allows you to add an application to take advantage of SpeedScreen. To add an application, follow these steps:

1. Click New to trigger the Add New Application Wizard.
2. The first screen informs you what the wizard does. Click Next to continue.
3. Next, you can browse the application executable. For the purposes of this example, choose notepad.exe and then click Next.
4. The next window asks whether you want to enable Local Text Echo for this application. It is enabled by default. Click Next.
5. The next wizard window allows you to apply the SpeedScreen settings to all instances of this application or to just the instance you specified in step 3. If you select to apply to all instances of this application, it registers the executable name, and whenever this application is triggered on this server, it will apply the SpeedScreen settings to it. Applying the settings to the instance you specified applies the SpeedScreen changes to the application only in the way you specified. Choose Apply to All Instances and click Next.
6. Click Finish to end the Add New Application Wizard.

Now that you have added an application to take advantage of SpeedScreen Latency Reduction, you can further tweak its settings for optimal Local Text Echo performance. If you right-click an application in the SpeedScreen Latency Reduction Manager, you are provided with two options. You can either delete the application or view the application properties, which is where we concentrate our attention next.

## Alert

Although configuring SpeedScreen Latency Reduction enables the technology on the server side, a user cannot take advantage of this technology until he or she enables it on the ICA client as well. This topic is discussed in greater detail in [Chapter 13](#), "Citrix ICA Client Software."

## Application Properties

The Application Properties window has two main tabs: Application Properties and Input Field Configuration. The Application Properties tab has two main sections. The Application Name section basically displays the name of the application you are currently working on, and the Application Settings section has the following configurable options:

- *Disable Local Text Echo for This Application* This option is self-explanatory. If checked, it disables the Local Text Echo feature of SpeedScreen technology for this application.
- *Limit Local Text Echo for This Application* This option offers two settings to choose from. You can configure it so it displays text only in the text fields by selecting Display Text in Place, or you can choose to replace text with bubbles until the server finishes processing and has had enough time to update the client screen, at which point the bubbles are replaced with the actual text. The bubbles are there to acknowledge to the user that "I know you just typed something, but I don't quite know what it is yet." To configure this option, select Display Text in a Floating Bubble.

You can also click the Advanced button and enable Force SpeedScreen to Treat All Input Fields in This Application in Native Mode. If this option is selected, it strips SpeedScreen of the two most important enhancements to it, Mouse Click Feedback and Local Text Echo, and reverts to simply using its algorithms to determine which portion of the screen has been updated and sends refreshes accordingly.

The real configuration of SpeedScreen Latency lies in the Input Fields tab. From this tab, you can tweak every text box or field in an application to respond according to a preconfigured action you specify here. Because different applications have different text fields that need special configuration, the SpeedScreen Latency Reduction Manager provides a wizard that allows you to select the field you want to customize within an application. To do this, follow these steps:

1. Click New to trigger the wizard and then click Next to bypass the welcome screen.
2. The next window asks you to launch the application you want to configure fields for. Launch that application, and when it is running, click Next to continue.
3. After you launch the application, you can drag the icon from the wizard to the text field you want to configure (see [Figure 6.8](#)). This action automatically adds that field. You also have the option to hide the SpeedScreen Latency Reduction Manager if it is getting in the way of your ability to select a text field from the application. Click Next to continue.

Figure 6.8. Input Field Selection Wizard.

[\[View full size image\]](#)

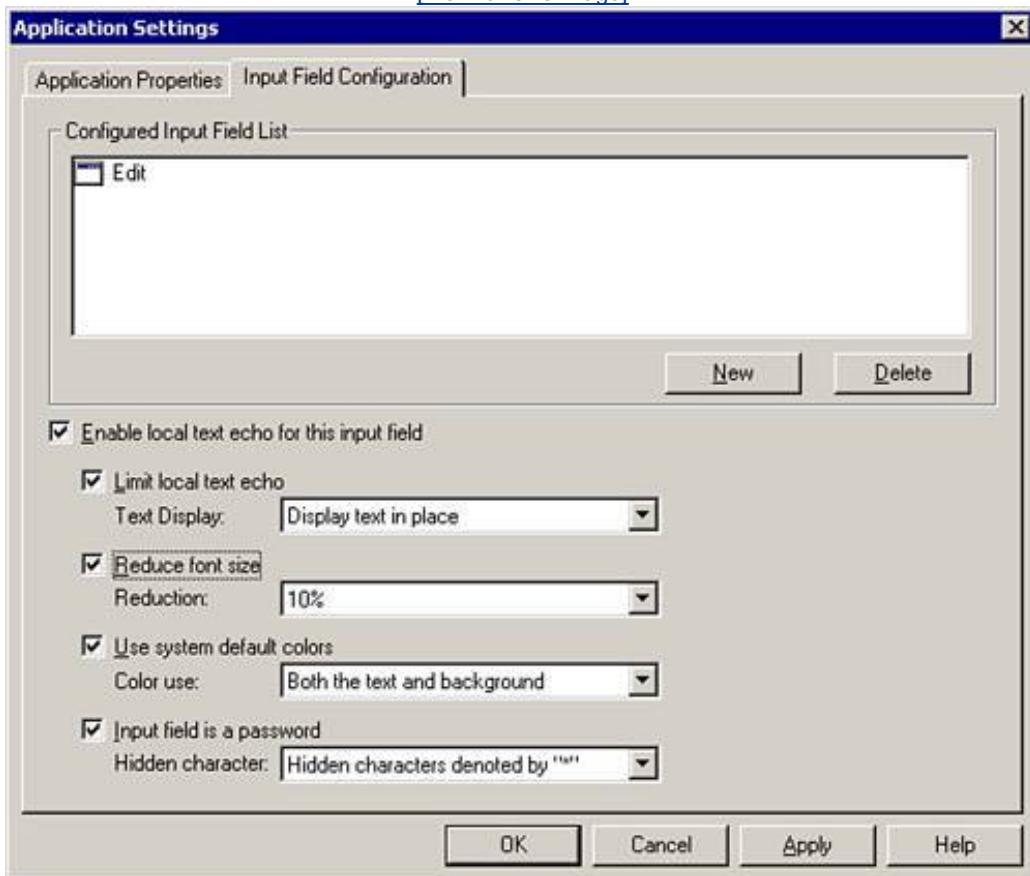


4. You are presented with a slider that allows you to control generic settings of this input field. Your options are Medium, which is the preferred choice and will use the text window; Low, which you should resort to if the Medium setting does not show the text because it shows the text wrapped in a bubble; and Off, which disables Local Text Echo. Make the appropriate selection and click Next.
5. Click Finish to exit the wizard.

After you exit the wizard, the newly added input field shows up in the Configured Input Field List. You can now highlight this input field and tweak it even more as follows (see [Figure 6.9](#)):

- *Limit Local Text Echo* This option was described and explained earlier in the "[Application Properties](#)" section.
- *Reduce Font Size* If you enable this option, you can reduce the font size by 10%, 20%, or 30%. This reduction in font size allows for a quicker refresh due to a smaller packet having to travel to the client device.
- *Use System Default Colors* This option allows you to force the application to use system colors. You can choose Both the Text and Background or The Background Only.
- *Input Field Is Password* This option instructs Local Text Echo to treat this input field as a password field. You have two options to hide the text being typed. You can choose Hidden Characters Denoted By "\*" or Hidden Characters Denoted By Spaces.

Figure 6.9. Input Field Configuration tab.



As with everything else in a server-based computing environment, the best way to know how much to tweak your settings is to test the application until your settings offer an acceptable performance result.

## Replicating SpeedScreen Settings to Other Servers in the Farm

In many cases, you may need to replicate the changes you made to the SpeedScreen Latency Reduction Manager to other servers load balancing a particular application. Instead of going through the process on every server, which can be frustrating and time consuming, especially in larger farms, you can copy the settings from one server to another.

After you complete all the configurations and save the settings, the settings are stored on the server in the following location: %systemroot%\system32\ss3config. You can copy this directory to every server you want to inherit this configuration.

## Exam Prep Questions

1. You are the Citrix administrator for the Champ Company. You are in the process of installing an application on one of your MetaFrame Presentation Servers. What is the best way to prevent users from signing on to the server?
- - A. From within the Management Console, right-click the server in question and click Properties. Select MetaFrame Settings, uncheck the box next to Enable Logons to This Server, and click OK.
  - 
  - B. Open a command prompt on the server and type `Disable Logons`.
  - 
  - C. From within the Management Console, expand the Servers node and select the server in question. Right-click the server name and select Disable New Logons.
  - 
  - D. From within the Management Console, right-click the farm node in the left control pane and select Properties. Select MetaFrame Settings and remove the server from the list.

A1: Answer A is correct. To disable logons to an MPS server, you should expand the Servers node in the Management Console, right-click the server in question, and click Properties. Then select MetaFrame Settings, uncheck the box next to Enable Logons to This Server, and click OK. Answer B is incorrect because no such command exists; the correct command to disable logons from a command prompt is `change logon /disable`. Answer C is incorrect because the steps are incorrect, and you can't disable new logons by right-clicking a server. The Disable New Logons option does not exist. Answer D is incorrect because you can't disable logins from the farm node.

2. How can you easily copy the configuration settings for the SpeedScreen Latency Reduction Manager after you have created and configured settings on a particular server?

A. Copy the %systemroot% directory.

B. Copy the %systemroot%\system32\Citrix directory.

C. Copy the %systemroot%\system32\ss3config directory.

D. Copy the %systemroot%\system32\Citrix\SpeedScreen directory.

A2: Answer C is correct. The correct path where SpeedScreen Latency Reduction Manager stores its configuration files is %systemroot%\%system32\ss3config. Copying this directory to other MPS servers spares you the trouble of running the configurations on every server. All the other answers are incorrect because none of those folders contain the files needed.

3. What do you call the MPS server in a zone that stores information about the server loads and published applications?

A. Master ICA browser

B. Local Host

C. Master IMA browser

D. Data Collector

A3: Answer D is correct. The Data Collector is the server elected in every zone that would be responsible for collecting and distributing information about server loads and published applications. Answer A is incorrect because the Master ICA Browser existed in MF 1.8 but does not exist in MPS 3.0. Answer B is incorrect because the Local Host Cache is a Microsoft Access database that exists on every MPS server and does not gather information about user load and published applications in a zone. Answer C is incorrect because there is no such thing as a Master IMA Browser.

4. What happens if you have a user who is using an older version of the ICA client and is

unable to transmit the local time of the machine he is connected to, and you have disabled local time estimation on the server?

A. Nothing, all ICA clients are able to transmit their local time.

B. Any files that the user creates and saves through that session are time-stamped according the client's time.

C. The server uses Eastern Standard Time by default when it cannot query the client time and time-stamps any files accordingly.

D. Any files that the user creates and saves through the ICA session are time-stamped with the server's local time.

A4: Answer D is correct. When a user is using a legacy ICA client that cannot transmit its local time to the server, the server can estimate the time for the client. In this case, the time estimation option is disabled on the server; therefore, the server's local time is used to time-stamp files. Answer A is incorrect because the statement is incorrect; older ICA clients could not transmit time. Answer B is incorrect because the user is using an older client that can't transmit, so there is no way for the server to time-stamp files created with the client's time because that time is unknown. Answer C is incorrect because there is no default setting that reverts to Eastern Standard Time in the event that the client's local time is unknown.

5. You are a helpdesk technician who wants to multitask and help several people at the same time. Which utility at your disposal would allow you to shadow multiple users at the same time? (Choose all that apply.)

A. Citrix Connection Configuration

B. Citrix Server Administration

C. The Management Console

D. Shadow Taskbar

- A5: Answers C and D are correct. The only two utilities that allow you to shadow more than one user at a time are the Shadow Taskbar and Management Console. Answer A is incorrect because Citrix Connection Configuration is not a user manager utility. Answer B is incorrect because the Citrix Server Administration can shadow only one user at a time, and it is considered a legacy administration tool from the MF 1.8 days.
6. Which tool is considered the centralized management tool in your MetaFrame Presentation Server farm?
- 
- A. Citrix Server Administrator
- 
- B. Citrix Console Manager
- 
- C. Citrix Management Console
- 
- D. The Management Console for MetaFrame Presentation Server
- A6: Answer D is correct. The correct name of the console is the Management Console, and it is the centralized administration tool for an MPS server farm. Answer A is incorrect because Citrix Server Administration is a legacy administration tool and is by no means a centralized tool. Answer B is incorrect because there is no utility called Citrix Console Manager. Answer C is also incorrect because the name has changed for the Management Console; it is no longer called the Citrix Management Console but rather the Management Console for MetaFrame Presentation Server. I purposely put this question in here to warn you that Citrix may use tricky questions like these on the exam.
7. Because your network has heavy latency and you have users who connect over poor communications links, you have decided to enable Local Text Echo to improve application responsiveness to keyboard strokes. However, when you run an application, you notice that the Local Text Echo is not working and the lag is unbearable. Why do you think that is the case?

A. The application is not configured with Local Text Echo.

B. The connection is too weak to enable Local Text Echo.

C. The server is not configured to allow Local Text Echo.

D. The server is using the MPS 3.0 Standard Edition, and Local Text Echo is not supported.

A7: Answer A is correct. Even though you enabled the SpeedScreen Latency Reduction Manager, you should still add an application before it can take advantage of the technology. Answer B is incorrect because the whole point of Local Text Echo is to function over weak connections. Answer C is incorrect because you know that SpeedScreen is enabled. Answer D is incorrect because all flavors of MPS support SpeedScreen.

8. Which of the following can the Management Console be used to manage? (Choose all that apply.)

A. MetaFrame 1.8 servers

B. Printer drivers

C. License information

D. Published applications

A8: Answers B and D are correct. Answer A is incorrect because the Management Console cannot be used to manage MF 1.8 servers. Answer C is incorrect because starting with MPS 3.0, the licensing module has been moved from the Management Console into its own Citrix License Server.

9. Where would you go to configure the timeout settings for a disconnected session in the Citrix Connection Configuration utility?

A. Advanced

B. Client Settings

C. Session connection Settings

D. ICA Settings

A9: Answer A is correct. The Advanced button is the location in the Citrix Connection Configuration utility where you would go to control timeout settings for a disconnected session. All other answers are incorrect.

10. You have enabled SpeedScreen Latency Reduction for your accounting applications and have configured Local Text Echo. Your users are claiming that when they try to log in to the accounting package, their passwords are being displayed in clear text rather than in a hidden format. How should you address this situation so that the password file does not display the actual characters?

A. In the application's properties window, select the Input Field Configuration tab and check the box next to Input Field Is a Password.

B. In the application's properties window, select the Input Field Configuration tab, click the Advanced button, and select This Is a Password Field.

C. Disable Local Text Echo because there is no workaround for this problem.

D. This application cannot hide the password field and displays the text by design.

A10: Answer A is correct. The right place to enable a field as a password field and as such hide the characters being typed is the application's properties window. In the Input Field Configuration tab, a check box treats this field as a password field and therefore hides the characters. All other answers are incorrect.

 PREV

NEXT 

# 7. MetaFrame Presentation Server Policy Management

Terms you'll need to understand:

- MetaFrame user policy
- Policy rule
- Policy filter
- Allow and Deny filter properties
- Policy priorities
- Resultant policy

Concepts and techniques you'll need to master:

- Enforcing desired configuration through user policies
- Determining the current policies in effect based on the given criteria
- Understanding what options can be managed via MetaFrame user policies
- Searching for policies matching given criteria and calculating the resultant policies in effect

This chapter focuses on how you can use MetaFrame user policies as a means of defining different user configurations that are enforced based on criteria such as client name, IP address, or username. Part of the core MetaFrame Presentation Server software, MetaFrame user policies were first introduced with Feature Release 2 for MetaFrame XP Presentation Server. In addition to the core functionality of user policies, this chapter also looks at new features introduced with MPS 3.0.

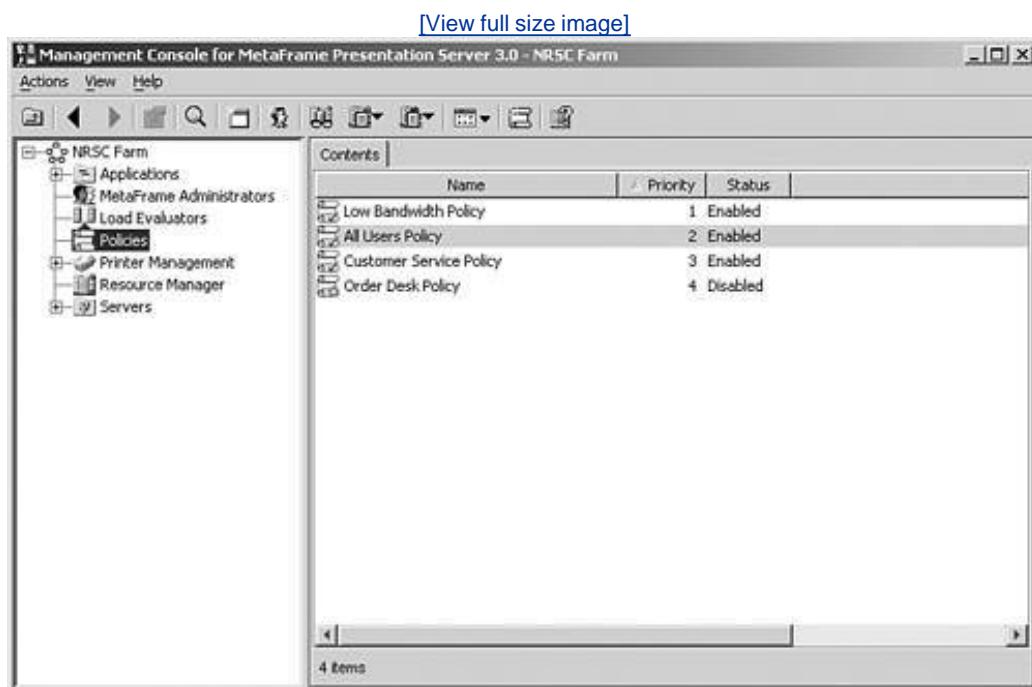
# What Are MetaFrame User Policies?

MetaFrame user policies allow an administrator to apply certain MetaFrame server settings to users based on their connection criteria. Hence, they can tailor the computing experience differently for different users.

For example, through MetaFrame user policies, you can enforce bandwidth caps on a user's client session when connecting from a client device located across a low-bandwidth WAN link. Alternatively, you might enable client drive mapping for only those users who belong to a special domain security group.

MetaFrame user policies are managed through the Policies object located in the Management Console for MetaFrame Presentation Server 3.0, as shown in [Figure 7.1](#).

Figure 7.1. MetaFrame user policies are managed through the Management Console for MPS.



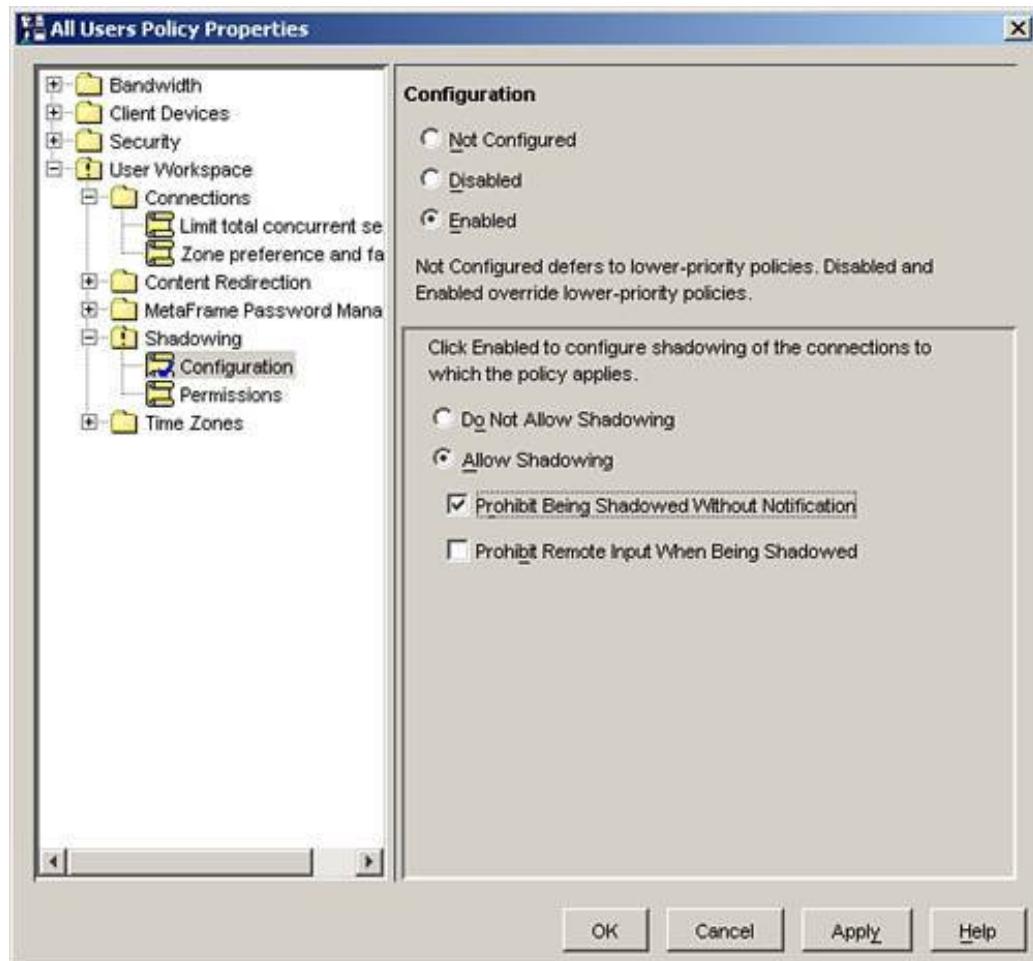
MetaFrame user policies have the following characteristics:

- Multiple policies can be defined in a server farm. You can see multiple policies listed in [Figure 7.1](#). A policy can be in one of two modes. It is either enabled, in which case it is applied to all connections that meet the membership criteria, or the policy is disabled, in which case it is ignored by MetaFrame.

- Each policy can have one or more rules defined within it. When a policy is applied to a user who is connecting to a MetaFrame server, all defined rules within that policy are applied.
- When more than one policy is applied to a connecting user, the order in which the rules are applied is based on the priority assigned to the policies. In general, a higher-priority policy overrides settings defined in a lower-priority policy. Details on policy priority are discussed in the next section, while available policy rules are reviewed in the "[Available MetaFrame Policy Rules](#)" section of this chapter.
- Each rule within a policy can be in one of three states, as shown in [Figure 7.2](#):
  - *Not Configured*This rule is ignored by the connecting user. If a lower-priority policy has this rule assigned a different state, the lower-priority rule is used.
  - *Disabled*The specific rule is disabled. This setting overrides any instance of the rule that has been enabled in lower-priority policies.
  - *Enabled*When enabled, the properties for the rule are applied to the connecting user. In [Figure 7.2](#), the Configuration rule for Shadowing is enabled. This means that when this policy is applied to a user, it is not possible for someone else to shadow him or her without the user first being notified.

Figure 7.2. A rule within a policy can be enabled, disabled, or not configured.

[\[View full size image\]](#)



## Alert

Make sure you know the three states for a policy rule and how they affect rules in both higher- and lower-priority policies.

- Policy assignment is dictated by filters (also known as memberships), which are any combination of one or more of client IP address (specific IP address or range), MPS client name, MPS server name, or individual username or group membership. During logon, MetaFrame determines all policies that should be applied to a given user based on this filter criteria. The applicable policies are then sorted in priority order and the defined rules are applied. Policy assignment is discussed in the "[Policy Filtering and Assignment](#)" section of this chapter.

PREV

NEXT

# Policy Priority

You need to understand two different types of policy priority for MPS exam 223. The first deals with the way user policies override similar MetaFrame farm or server settings, while the second looks at the way user policies override other user policies assigned to the same user during logon.

## MetaFrame Server Settings and User Policies

When user policies conflict with existing MetaFrame farm, server, or client settings, the user policies always take precedence, with two exceptions:

- When encryption settings are defined in a user policy, they override MetaFrame farm, server, or client encryption settings only if they are stronger. For example, if the minimum accepted encryption level for a connection is set to 128 bit on a MetaFrame server, a user policy that has a rule setting this level to 56 bit is ignored.
- If the MetaFrame farm, server, or client has defined a more restrictive shadowing configuration, it overrides a less-restrictive setting in a user policy.

### Note

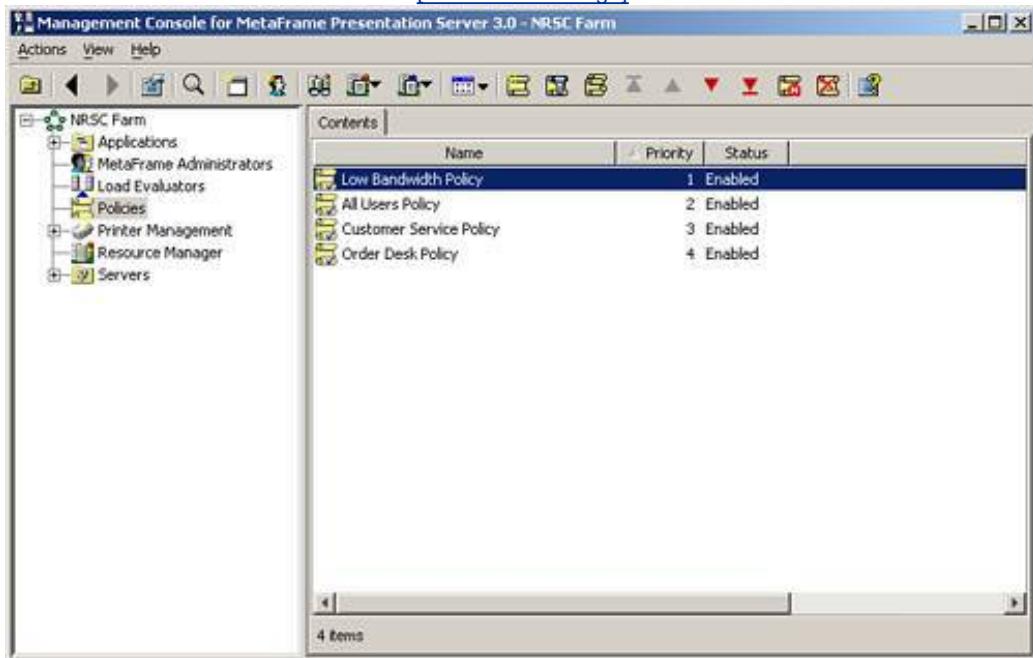
Similar precedence rules also apply to Microsoft Group Policy Objects. If a Microsoft Group Policy specifies a more restrictive configuration than a MetaFrame user policy, the Microsoft GPO typically takes precedence. Although specific details on these Microsoft policies are not required for the exam, be certain that you understand that this situation can arise and that unexpected MetaFrame user policy behavior may be due to Microsoft GPO settings that are also in effect.

## MetaFrame User Policy Priorities

In MetaFrame, user policies are given a priority ranking starting at 1, the highest, and decreasing in priority as the value increases. The closer the priority number to 1, the higher the ranking compared to other policies. [Figure 7.3](#) shows four policies defined for the server farm, ranked from 1 through 4. If a user connecting to a MetaFrame server is assigned more than one of these policies, they are applied in order starting from 4 and working up to 1. In [Figure 7.3](#), the Order Desk Policy is ranked lowest, and the Low Bandwidth Policy is ranked highest.

Figure 7.3. When a user is assigned multiple policies, the rules are applied based on the policy's ranking, starting at the highest number and counting down to number 1.

[View full size image]



If a user is assigned the Order Desk Policy, All Users Policy, and Low Bandwidth Policy, the corresponding rules for each policy would be applied in order of ranking, with the rules in the Low Bandwidth Policy having the final say in how the client session may be configured.

As we already mentioned, a specific policy rule can be set to one of three states:

- *Not Configured*This rule is ignored by the connecting user. If a lower-priority policy has this rule assigned a different state, the lower-priority rule is used.
- *Disabled*The specific rule is disabled. This setting overrides any instance of the rule that has been enabled in lower-priority policies. This rule remains disabled unless overridden by a higher rule that enables this setting.
- *Enabled*When enabled, the properties for the rule are applied to the connecting user, unless disabled by a higher-priority rule.

Whether a policy is enabled or not is best described with a demonstration. Assume that in the four policies shown in [Figure 7.3](#), each has the rules Turn Off Menu Animation and Turn Off Desktop Wallpaper defined, as shown in [Table 7.1](#).

Table 7.1. MetaFrame Policy Priority Example

Rank	Policy	Rule/State	
		Turn off menu animation	Turn off desktop wallpaper
1	Low Bandwidth Policy	Enabled	Enabled

Rank	Policy	Rule/State	
2	All Users Policy	Not Configured	Not Configured
3	Customer Service Policy	Disabled	Not Configured
4	Order Desk Policy	Enabled	Enabled

The final state for these rules depends on what policies are applied when a user logs on. If the Low Bandwidth Policy is applied, both of these rules are enabled because this is the highest priority rule. If a user belongs to both Order Desk Policy and Customer Service Policy, the two rules have the states Disabled and Enabled, respectively. The reason is that Customer Service Policy, with its higher ranking, takes precedence over Order Desk Policy, forcing the Turn Off Menu Animation setting to Disabled.

## Alert

Unlike stronger encryption and more restrictive shadowing settings that take priority when defined for the MetaFrame farm, server, or client, within user policies, shadowing and encryption settings are affected by policy order. If a higher-level policy defines a weaker encryption level, it overrides a stronger encryption level that may have been defined in a lower-ranked policy. Understanding this subtle difference is an important part of being properly prepared for the exam.

When a new policy is created, it is automatically assigned the lowest available priority. You can then modify the policy's priority either by highlighting the policy and selecting the up or down arrows located on the Management Console toolbar, or by right-clicking on the policy and selecting the appropriate arrow from the Priority menu.

## Note

Pay special attention to any rule that is being disabled. In most cases, disabling a rule simply means that if it was enabled in a lower-ranked policy, it is now effectively not configured, meaning it has no effect. It does *not* mean that the opposite setting is now enabled.

A good example is the Turn Off Desktop Wallpaper rule. When this rule is enabled, you force the desktop wallpaper to be turned off. But disabling the rule simply cancels out any instance in which it may have been enabled in a lower rule. Hence, the desktop wallpaper is no longer forced to be turned off. It does not mean that the wallpaper is now going to be forced to be turned on.

This subtle difference is a source of confusion for many administrators when they first become involved in working with MetaFrame user policies.

## Policy Exceptions

The ability to prioritize MetaFrame user policies makes it simple to create special exception policies that grant (or deny) access to certain features. For example, you may have a policy that enables server-to-client content redirection to all MetaFrame users, but a special exception rule that has been created and assigned a higher ranking specifically disables this rule when users belong to a group restricting such access.

Another example involves restricting access to client printers for all users in the organization except for those users who belong to a special printer access group. Creating a special policy specifically to override a lower-ranked policy setting is commonly referred to as creating a policy exception.

When asked to define an exception to a policy, you're simply being asked to create a policy that will counteract something that has already been defined for a more general group of users.

 PREV

NEXT 

# Policy Filtering and Assignment

Before the rules in a policy can be applied to someone logging on to a MetaFrame server, you must decide what users, clients, and/or servers will be affected. You must then define the appropriate filters to enforce this assignment. You can filter a policy on any combination of the following:

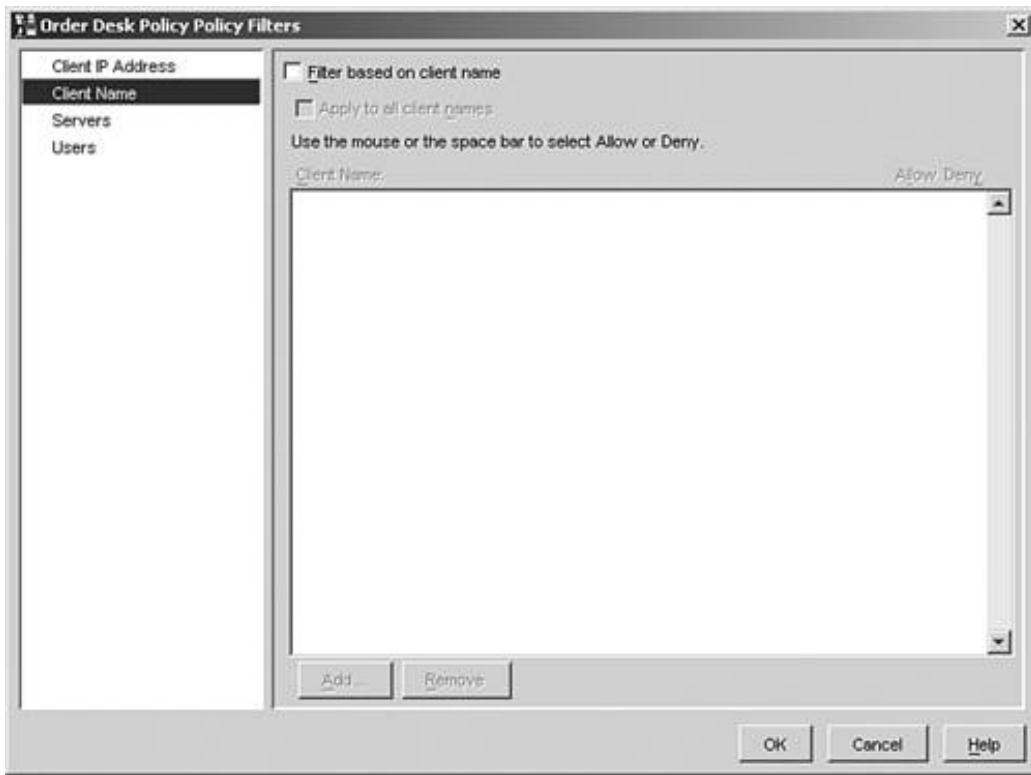
- *Client IP address* You can define specific IP addresses or a range of addresses on which to filter.
- *Client name* The MPS client name can be used as a filter. Although, in most cases, this name will match the device host or computer name, this does not always have to be true. Make sure you specify the MPS client name when using this filter.
- *Username or group name* You can also filter on individual usernames or a group containing multiple users.
- *MetaFrame server name* You can filter certain rules to apply only when users log on to a specific MetaFrame server.

Multiple instances of each filter type can be used to create a filter that applies a policy to a specific subset of MetaFrame connections in the environment.

[Figure 7.4](#) shows the policy filter dialog box. You open this dialog box either by highlighting a policy and pressing Alt+T, or right-clicking and selecting Apply This Policy To from the context menu. Selecting an available filter type in the left pane displays the associated window on the right where the filter can be enabled for this policy and the appropriate filter options defined.

Figure 7.4. Filters must be created for a policy before it can be applied to user connections in the farm.

[\[View full size image\]](#)



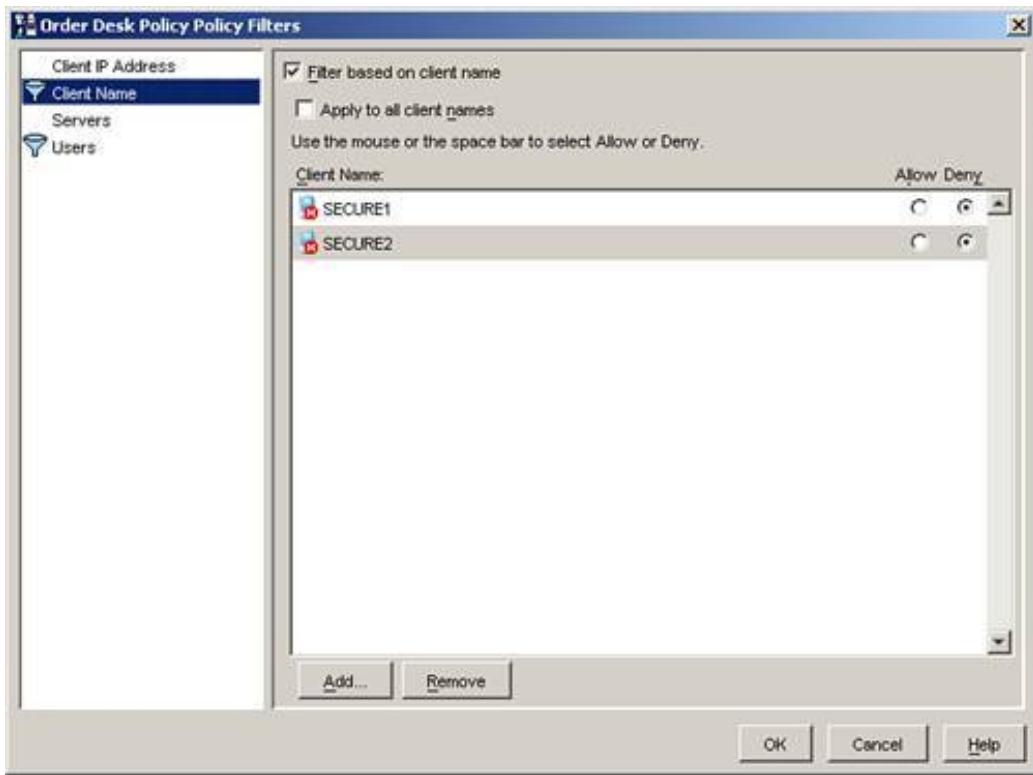
## Allow and Deny Access

All the supported filter types, with the exception of servers, allow you to specify whether a particular filter entry has a setting of Allow or Deny. When an entry has Allow access, the rules in the policy are applied to that entry. If an entry has Deny access, it is excluded from the filter and the corresponding policy rules are not applied.

Deny ensures that a particular policy is not applied to one or more objects that might otherwise be included as part of another filter condition. For example, you might specify that all members of the Remote Site group have a certain policy applied (they have Allow access), but you want to ensure that anyone using the special client devices with the names SECURE1 and SECURE2, regardless of whether they are in that group, are excluded from the policy. You would then add these two client names to the policy filter, but you would assign Deny access instead of Allow access. [Figure 7.5](#) shows how these two client name entries would appear.

Figure 7.5. The Deny property ensures that particular objects (users, IP addresses, or client names) are excluded from a policy that might otherwise be applied to them.

[\[View full size image\]](#)



## Client IP Address

The Client IP Address filter allows you to specify individual IP addresses, a range of addresses, or through a single click, all client IP addresses that connect to the server. Multiple addresses from different networks can be used, allowing you to create a filter that applies only to users from a particular network subnet.

## Client Name

You can define one or more client names, or you can select the check box that enables the rule for all client names. When entering a client name, you can specify the wildcard asterisk (\*) character to include multiple names that are similar. For example, if all client names in the California office begin with the prefix CAL, you could add the client name CAL\* to this filter, and it would automatically include all clients that matched this name. A network icon appears beside a wildcard name instead of the individual computer icon.

Client names are not case sensitive, but you must type them correctly. There is no mechanism for validating whether a client name you have entered actually matches an existing client name.

## Alert

Contrary to what is found in the online help for MPS 3.0, you can use client names to filter on users connecting through the Web Interface for MPS. All Web Interface users are assigned a client name that begins with WI\_ followed by 15 randomly generated ASCII characters. By specifying the client name WI\_\* you can create a filter that includes all users

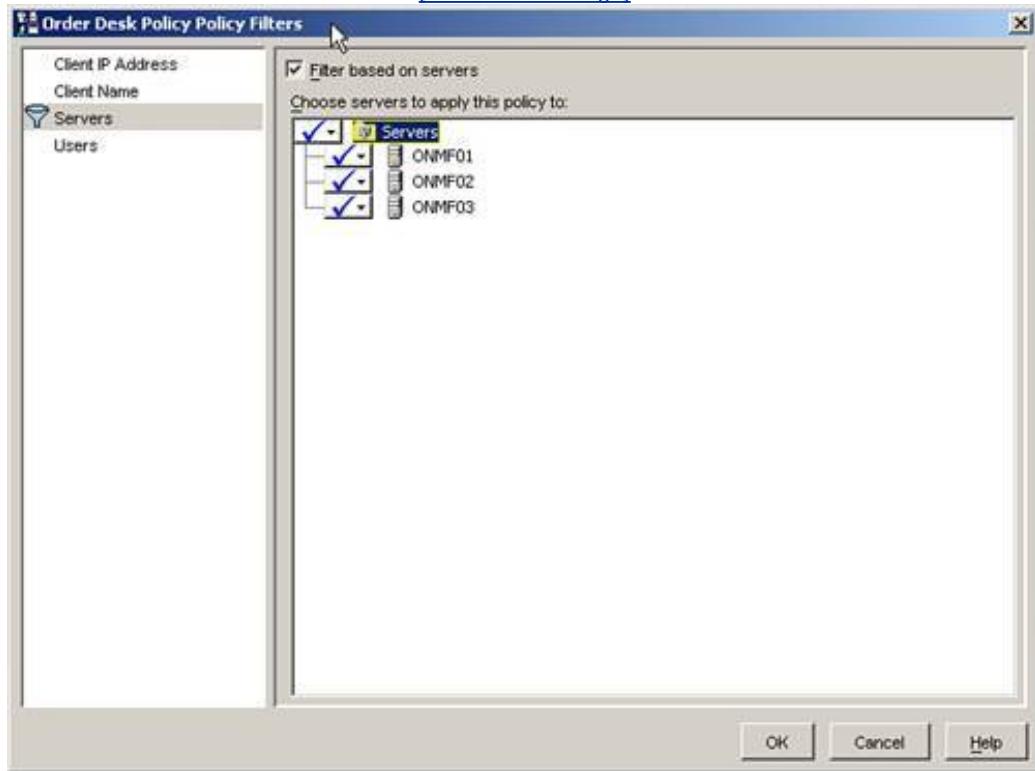
who may connect via the Web Interface.

## Servers

When choosing to filter a policy based on servers, you are presented with a tree view showing all available MetaFrame servers in the farm, along with a check mark beside each entry (see [Figure 7.6](#)). A check mark corresponds to the default filter setting Apply to This Server, which is conceptually equivalent to the Allow property for the other policy filters. By clicking the drop-down icon next to a server name, you can toggle between the Apply and Do Not Apply to Server properties. From the root servers folder you can also enable or disable application of filters to all servers simultaneously.

Figure 7.6. MetaFrame servers are included or excluded from a filter by selecting the Apply or Do Not Apply settings. By default, all servers are included when the filter is first enabled.

[View full size image]



## Users

The final policy filter in the policy filters dialog box is the Users filter (see [Figure 7.7](#)). A user filter can be configured with the following information:

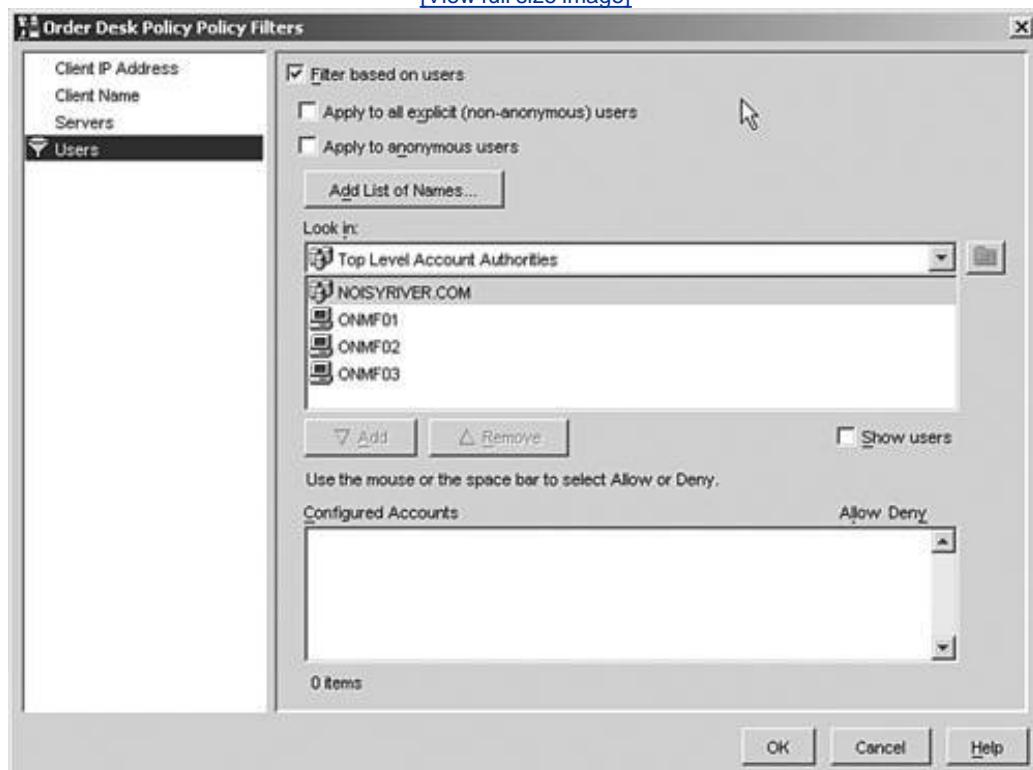
- *All explicit (nonanonymous) users* This represents all MetaFrame users who log on to a server in the farm with a user ID password, regardless of whether they are administrators or regular

users. You filter on this setting simply by clicking the corresponding check box under the Users filter.

- *Anonymous users* A filter can be defined so that it is applied only to those users who connect to a server via an anonymous Citrix user account. When anonymous logons have been enabled, a user is immediately logged on to a MetaFrame server without first being required to provide user ID and password information. You enable this filter option by selecting the Apply to Anonymous Users check box.
- *User groups* Filters can also be defined based on a user's membership in a domain or local server group. The Users filter allows you to drill into the desired group location and select one or more groups to include in the filter. Groups can be configured with the Allow or Deny setting.
- *User accounts* In addition to groups, you can also select individual users to include in the filter. As with groups, individual users may be set with the Allow or Deny setting. A common reason for including individual users is to explicitly allow or deny them access to this policy. Sometimes it is easier to include a single domain group that contains a large number of users and allow or deny a small subset than it is to create an entirely new group that excludes these few users.

Figure 7.7. The Users filter provides you with a number of different assignment options.

[View full size image]



◀ PREV

NEXT ▶

## Available MetaFrame Policy Rules

MetaFrame Presentation Server 3.0 saw the number of available policy rules rise from 20 in MetaFrame XP FR2/FR3 to 37 rules. [Table 7.2](#) summarizes the different user-connectionrelated rules that can be defined when creating a user policy.

Table 7.2. MetaFrame User Policy Summary

Policy Rule	Description
Bandwidth	All rules defined under this category are related to bandwidth optimization.
Session Limits	<p>By configuring the options under the Session Limits category, you can assign the maximum bandwidth that particular channels in the ICA data stream can consume. All bandwidth caps are assigned a value in kilobits per second (Kb/s). Settings under here are rarely assigned based on a user ID but more often are assigned based on the client device name or IP address because they are location specific more than user specific.</p> <ul style="list-style-type: none"> <li>Audio</li> <li>Clipboard</li> <li>COM Ports</li> <li>Drives</li> <li>LPT Ports</li> <li>OEM Virtual Channels</li> <li>Overall Session</li> <li>Printer</li> </ul>
SpeedScreen	<p>SpeedScreen-related settings are managed under this category. Currently, the only setting available under here dictates behavior of the lossy compression for image acceleration.</p> <p>Lossy compression is enabled by default and set to High to maximize the compression used and minimize the bandwidth consumed. You can adjust the default compression as well as set the bandwidth threshold in which lossy compression is automatically enabled.</p>
Visual Effects	<p>The Visual Effects rules dictate what features are available to increase the visual presentation of the environment at the expense of performance. Enabling these settings reduces bandwidth by eliminating features that are not essential to the running of MetaFrame Presentation Server.</p> <ul style="list-style-type: none"> <li>Turn Off Desktop</li> <li>Wallpaper</li> <li>Turn Off Menu Animation</li> </ul>

Policy Rule	Description
Turn Off Window Contents While Dragging	
Client Devices	The rules under this category are all related to MetaFrame server-to-client device connectivity.
Maintenance Turn Off Auto Client Update	Only one rule exists under this category; it controls how client updates are performed.  The one option controls whether the Auto Client Update feature is enabled for a particular client. MetaFrame supports automatic updating of a number of client types. The Auto Client Update feature is covered in <a href="#">Chapter 13</a> , "Citrix ICA Sessions and Client Configuration."
Resources	The Resources category refers specifically to the availability and configuration of accessible client devices.
Resource\Audio Microphones Sound Quality Turn Off Speakers	The Audio category is the place where you can find the rules that deal specifically with the client audio-related settings. For example, you might use the Sound Quality option to specify the maximum allowable client audio quality the client can use.  The better the audio quality, the greater the bandwidth consumption, so environments in which bandwidth is limited should have restrictions on audio resources.
Resources\Drives Connection Mappings	The Drives category allows you to define whether client drives are connected as well as what specific client drive types are available for use. Disabling floppy or CD-ROM drive access is but one example of how this could be used.
Resources\Local Printers Auto Creation Default Drivers Turn Off Client Printer Mapping	The Local Printers category is the place where you can find rules that influence the behavior of local client printer mapping. Auto Creation manages whether client printer mapping is enabled, and if so, what printers are actually mapped. Default controls whether the local default printer is also the MetaFrame session default. The Drivers rule controls what drivers (native, universal printer driver, or both) are used, while client printer mapping can be disabled completely when the last rule in this category is enabled.
Resources\Network Printers Print Job Routing	This category contains only a single rule, which dictates whether a job destined for a network client printer is sent via the client or directly through the network.  When the print job is sent via the client device, it is compressed before sending, reducing the bandwidth consumed but resulting in a slower printout. Directly sending the print job to the printer consumes more bandwidth but is faster.  Direct routing to the printer occurs only when the printer is on the same network as the MetaFrame server. If MetaFrame

Policy Rule	Description detects that the client network printer is not on the local network, the job is automatically routed through the client.
Resources\Other  Turn Off Clipboard Mapping  Turn Off OEM Virtual Channels	The Other category contains rules that allow you to turn off clipboard mapping and OEM virtual channels. When clipboard mapping is disabled, you cannot cut and paste between the MetaFrame session and the local client device.  Disabling OEM channels does not affect any of the native MetaFrame functionality but prevents third-party applications that utilize ICA virtual channels from functioning properly.
Ports  Turn Off COM Ports  Turn Off LPT Ports	Under the Ports category, you can turn off either COM or LPT port redirection.
Security	The Security category itself contains only one category with a single rule.
Encryption  SecureICA Encryption	<p>The SecureICA Encryption rule allows you to set the minimum encryption level required by the client to connect to the server. After the level is set, if a user attempts to connect with a lower encryption level, his or her connection is denied.</p> <p>Remember, this setting cannot override a stronger encryption level set directly at the MetaFrame connection configuration. In this case, you can require a stronger encryption, but you cannot reduce the minimum encryption required.</p> <p>The same is not true when you're looking at other policies that may also set this option. Standard priority rules apply. If a higher-level policy sets this encryption level higher or lower, it overrides the same setting in a lower-priority policy.</p>
User Workspace	User Workspace rules manage some of the settings for the session in which the user runs his or her applications.
Connections  Limit Total Concurrent Sessions  Zone Preference and Failover	<p>Two rules exist for the Connections category. The first limits the total number of unique client connections that a user can run concurrently in the server farm. This setting prevents a user from logging on simultaneously from multiple different workstations. It does not limit a user from running multiple simultaneous published applications in the farm from the same client device.</p> <p>Zone Preference and Failover allows you to define the preferred and failover zones in which users will attempt to connect to load-balanced applications. Without zone preferences, a user is always directed to the least-loaded server, even if it is located across a WAN. When a zone preference has been defined, the user looks only to the current zone for determining the least-loaded server. If no servers are available within a zone, the failover option will direct users to another zone, ensuring business continuity in the event of</p>

Policy Rule	Description
	<p>network or system issues.</p> <p>Zone Preference and Failover is valid only for the Enterprise Edition of MPS. For you to be able to set this option, there must be more than one zone in the farm.</p>
Content Redirection  Server to Client	<p>The Content Redirection category contains only one setting, which lets you enable or disable redirection of server content to the client. By default, web URLs are processed using web browsers and multimedia players running on the server, but enabling this option causes the local web browser or multimedia player to process the URL. This option is supported only by the MetaFrame Win32 and Linux clients. Other clients ignore these options.</p>
MetaFrame Password Manager  Central Credential Store  Do Not Use MetaFrame  Password Manager	<p>Rules under the MetaFrame Password Manager category allow configuration of settings related to the integration of the Citrix MetaFrame Password Manager application into the MetaFrame Presentation Server environment. These rules can be used to control which users can use Password Manager for server farm authentication.</p> <p>These rules also allow you to more effectively manage which file-based central credential store users are contacting, eliminating unnecessary WAN traffic that can occur when users request credentials from a remote credential store.</p> <p>Zone Preference and Failover settings have no effect on the central credential store that is contacted. If the credential store is located in a failed zone, users who authenticate with the Password Manager cannot log on, even if the zone failover allows them to contact an alternate MetaFrame server.</p>
Shadowing  Configuration  Permissions	<p>Shadowing rules are used to enable and manage permissions to shadow the policy recipients. The Configuration rule either allows or denies access to being shadowed, whereas the Permissions rule is the place where you specify the list of users and/or groups that can perform the shadowing.</p> <p>Remember, this policy dictates whether the policy recipients can be shadowed and who has the ability to shadow them. Users affected by this policy are not directly granted access to shadow other people unless they are included in the list of users in the Permissions rule.</p> <p>Make sure users clearly understand this policy because many people get it mixed up and think you enable it to grant recipients shadowing capabilities.</p> <p>These policies have no effect if shadowing support was explicitly disabled during the installation of MetaFrame.</p>
Time Zones  Do Not Estimate Local	<p>The final set of user policy options manage the time zone settings.</p>

Policy Rule	Description
Time for Legacy Clients Do Not Use Clients' Local Time	<p>The first option allows you to turn off the MetaFrame server's default behavior of attempting to estimate the local time zone for those ICA clients that do not provide time zone information to the server.</p>
	<p>When the farm is configured to accept local time information from the client, if the client does not support passing such information, by default the server will attempt to estimate the client's local time. In many instances, this information is not accurate and can lead to strange time settings for the user's session. This is usually noticed when the client runs an email program such as Outlook. If users are receiving inaccurate time information, this is likely the cause; either this policy should be enabled or the MetaFrame client upgraded.</p> <p>If client time estimating is disabled, these clients use the current time information of the server.</p> <p>The last option controls whether the client provides time zone information, or the local time of the MetaFrame server is used instead.</p> <p>These settings override the same options that can be defined for the entire server farm.</p>

## Alert

You should be familiar with all 37 policy rules available in MPS 3.0 and understand under what category a particular rule can be located.

 PREV

NEXT 

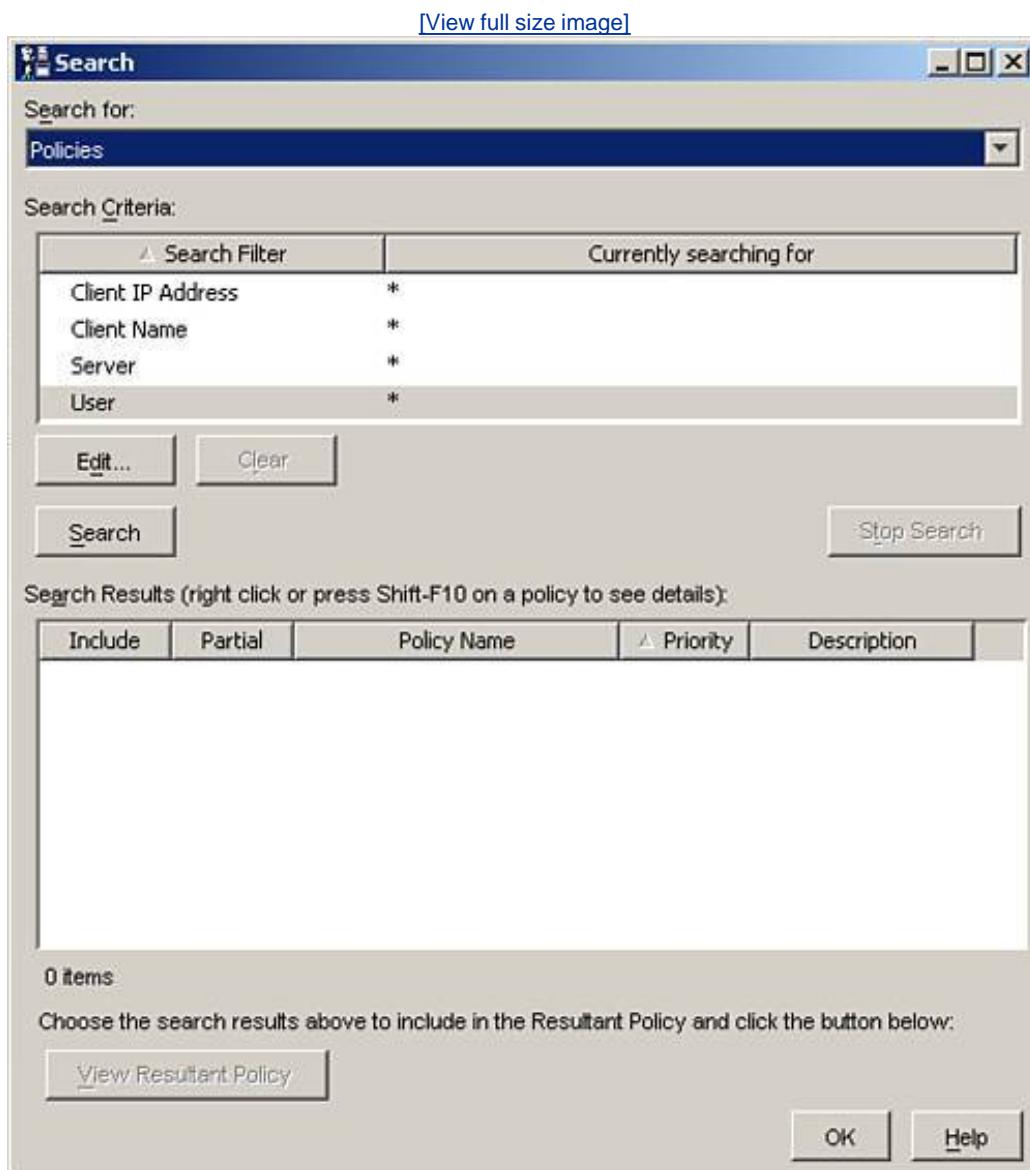
## Creating a User Policy

The task of actually creating a MetaFrame user policy is straightforward. You simply right-click the Policies object in the Management Console or press Alt+P, select Create Policy from the context menu, and then provide a name for the new policy in the dialog box that appears. The new policy is then added to the list in the right pane of the Management Console. Opening the properties for the new policy displays the different rules discussed in the preceding section. After you set the desired rules, you can assign the appropriate filters, which were described in the "Policy Filtering and Assignment" section earlier in this chapter. Although there is no published limit on the number of policies that can be created, from both an administration and a performance standpoint, it is wise to limit the number of policies as much as possible. Do not create new policies simply for the sake of doing so. Group rules within the same policy as much as possible.

## Determining the Resultant Set of Policies

The final area to discuss regarding MetaFrame user policies is the way you can determine the effective policies being applied to an IP address, client name, user, or server. You perform this task by using the Search function of user policies. By right-clicking the Policies object and selecting Search, you are presented with the dialog box shown in [Figure 7.8](#).

Figure 7.8. You can search user policies to determine whether one or more policies apply to a particular user connection.



By specifying the desired search criteria, you can retrieve a list of all policies meeting that criteria. For example, you could search on a particular user ID or group name and receive a list of policies that apply to that user or group. To determine the exact set of policies that apply in a given situation, you need to include all the appropriate criteria. For example, you need to include the IP address of the network the user is on, the name of the user's device, the MetaFrame server he or she is logged on to, and the user's actual username. If you omit any information from the query, you receive only a partial match. Providing all this information does not guarantee that a particular policy will apply in all situations, because, for example, it may have a Deny setting included for a particular server that would not be captured by the search.

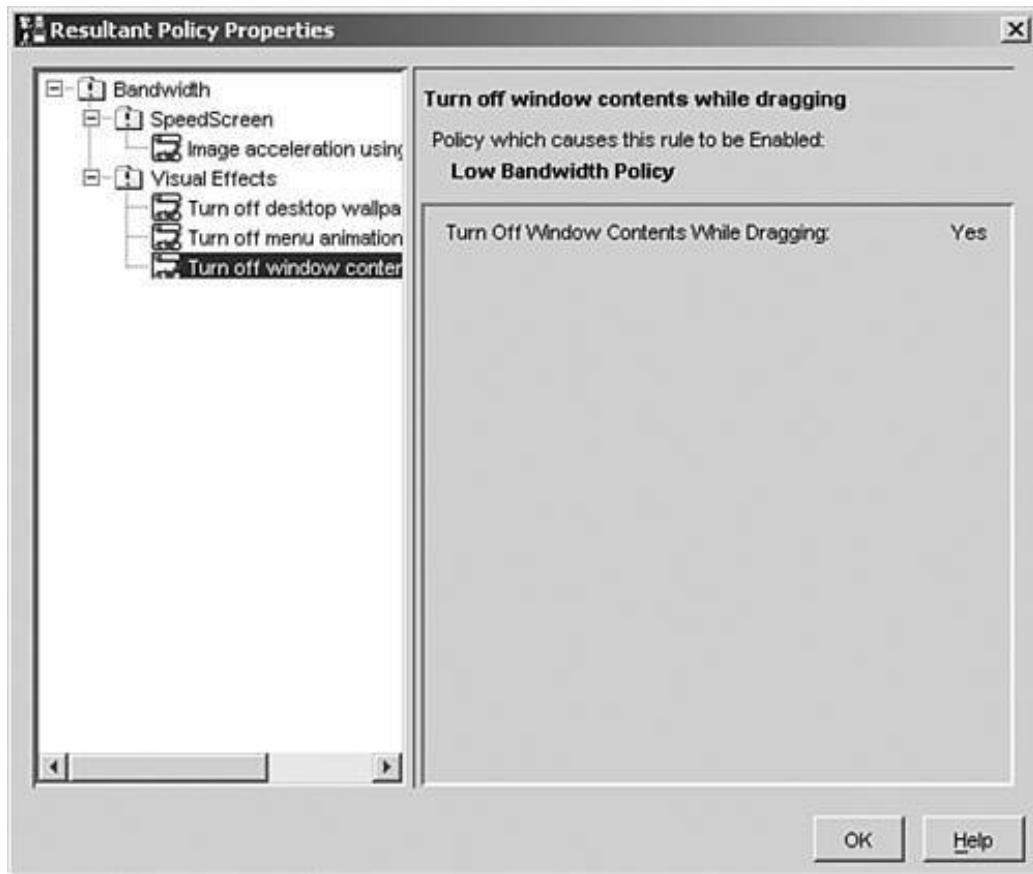
To view the specific settings based on the resultant set, you must provide all necessary search criteria. Otherwise, when you calculate the resultant set, it will show the rules that may be affected but will not display the actual setting for that rule (enabled or disabled).

After you initiate a search, a list of matching policies is returned. There are a couple of different tasks that you can now perform. You can view the properties of the listed policies and edit rules directly, without having to load up the policy from the main Policies window. You can also calculate the resultant set of policies.

To perform these tasks, you must ensure that the Include check box appears beside each policy you want included in the resultant calculation and that the Partial column does not contain a warning exclamation mark. If it does, the resultant policy calculation will not be able to return the proper results. If this partial column is not flagged, you can click the View Resultant Policy button. A new dialog box opens showing only those policy rules currently in effect. [Figure 7.9](#) demonstrates what this window may look like. As you can see, it displays only those policy categories and resulting rules in effect based on the search criteria provided.

Figure 7.9. After you provide all the necessary search criteria, you can view the resultant set of policies to determine which rules are in effect for a particular user.

[\[View full size image\]](#)



If search criteria were omitted or produce ambiguous results, you cannot view the specific setting for a rule. Instead, a red question mark appears next to the property and, when clicked, text appears in the right pane explaining why the result cannot be calculated.

[◀ PREV](#)

[NEXT ▶](#)

## Exam Prep Questions

1. An administrator has defined a MetaFrame user policy that she wants to apply to all users who belong to the Customer Service group. When she logs on as a member of this group, the defined rules are not being applied as expected. Why might the policy rules not be applied properly? (Choose all that apply.)

A. A policy with a higher priority level has disabled these particular rules.

B. A policy with a lower priority level has disabled these particular rules.

C. The Use MetaFrame Policies setting has not been enabled in the server farm properties.

D. The policy in question is currently disabled.

A1: Answers A and D are correct. If a policy with a higher priority explicitly disables these policies, the net result is that the policy is canceled out and the configuration change is not applied to the user's session. It is also possible that the policy itself has a status set to Disabled. In this case, the policy is completely ignored and no rules are applied. Answer B is incorrect because a lower-priority policy rule takes precedence only if a higher-priority rule is set to Not Configured. Answer C is incorrect because such a setting does not exist in the server farm properties. All aspects of MetaFrame user policies are managed through the Policies object in the Management Console for MPS.

2. The following table shows three policies, their ranking as shown in the Management Console, and the state defined for the rule Turn Off Desktop Wallpaper. Assuming that the desktop wallpaper behavior has not been modified by any other group policy or Terminal Server setting, what would the rule's final state be if a user had User Policy #1 and User Policy #2 applied during his or her logon to the farm?

Rule/State		
Rank	Policy	Turn Off Desktop Wallpaper
1	User Policy #3	Enabled
2	User Policy #1	Disabled
3	User Policy #2	Not Configured

A. Enabled

B. Disabled

C. Not Configured

D. None of the above

A2: Answer B is correct. Because User Policy #1 has a higher ranking than User Policy #2, the state of the rule defined in User Policy #1 ultimately dictates what the setting will be. Answer A is incorrect because the filter does not apply User Policy #3 to the user. Answer C is incorrect for the same reason that Answer B is correct.

3. The following table shows three policies, their ranking as shown in the Management Console, and the state defined for the rule Turn Off Client Printer Mapping. Assuming that client printer mapping is enabled for all users and that no other group policy modifies this setting, what would the rule's final state be if a user was assigned all three user policies?

Rule/State		
Rank	Policy	Turn Off Client Printer Mapping
1	User Policy #1	Not Configured
2	User Policy #2	Not Configured
3	User Policy #3	Enabled



- A. Enabled
- 
- B. Disabled
- 
- C. Not Configured
- 
- D. None of the above

A3: Answer A is correct. Even though User Policies #1 and #2 have a higher ranking than User Policy #3, neither one has this rule defined. The not configured state has no effect on a policy setting (enabled or disabled) made lower down in the policy ranking.

Because of this, User Policy #3 enables turning off client printer mapping, and no other policy overrides this setting.

4. Bob, the administrator, has configured his MetaFrame environment to allow sales staff on the road to connect into the environment via the Web Interface for MetaFrame Presentation Server. This configuration allows these users to connect from any device, whether from their laptop or a remote PC. To help secure the environment, Bob wants to set up user policies that take effect when the sales staff attempt to connect remotely. Knowing that the internal network is 192.168.10.0 and that users connect both internally and externally using the Web Interface, choose all the filters listed that would need to be applied to ensure that this policy is applied only when the users connect remotely.



- A. Filter: Client IP Address  
Setting: IP Range 192.168.10.1192.168.10.254  
State: Deny



- B. Filter: Client Name  
Setting: WI\_\*State: Allow



- C. Filter: Servers

Setting: All Web servers

State: Allow

D. Filter: Users

Setting: Apply to all explicit (nonanonymous) users

State: Deny

A4: Answers A and B are correct. The IP Address range ensures that if a user is connecting from an IP address located on the internal network, the extra security settings are not enforced. Likewise, using the wildcard WI\_\* ensures that all Web Interface clients otherwise receive the policy settings defined. Answer C is not a valid server setting and is therefore incorrect. Answer D, while a valid setting, would effectively deny anyone from accessing this policy, counteracting the settings that should apply to Web Interface users who are connecting externally.

5. Given the following list, select all that are valid MetaFrame user policy rules.

A. Local Printers, Auto Creation

B. Audio, Microphones

C. Visual Effects, Turn Off Desktop Wallpaper

D. Ports, Turn Off USB Ports

A5: Answers A, B, and C are correct. These three answers represent valid MetaFrame user policy rules. Answer D is incorrect. There are Port rules to turn off COM and LPT ports, but no rule exists to turn off USB ports.

6. As part of your MetaFrame implementation, you have configured the default shadowing for your server not to display a notification to the user, and to allow remote input. The environment requires that shadowing be configured so that users in the Customer Service group can be shadowed by Terminal Server Administrators (who have full administrator access to the MetaFrame server) without being prompted to accept the request. At the same time, you must ensure that the two managers Alice and Bob, who are also in the Customer Service group, receive notification when they are being shadowed. From the following list, select the filter that would correctly, and most effectively, configure this scenario.

- A. Create a new policy and apply it to the Terminal Server Administrators group. Under Shadowing, Configuration, click Enabled and then Allow Shadowing.

Go to Shadowing, Permissions, click Enabled, and then add the Customer Service group to the list with the Allow privilege set. Add the users Alice and Bob and set the privilege to Deny.

- B. Create a new policy and apply it to the Customer Service group. Under Shadowing, Configuration, click Enabled, and then click Allow Shadowing. Next, click the Prohibit Being Shadowed Without Notification setting.

Go to Shadowing, Permissions, click Enabled, and then add the users Alice and Bob to the list with the Allow privilege. Next, add the Customer Service group and grant them the Deny privilege.

- C. Create a new policy and apply it to the Customer Service group with the Allow privilege. Apply it to the users Alice and Bob with the Deny privilege. Under Shadowing, Configuration, click Enabled, and then click Allow Shadowing. Next, click the Prohibit Being Shadowed Without Notification setting.

- D. Create a new policy and apply it to the users Alice and Bob with the Allow privilege. Under Shadowing, Configuration, click Enabled, and then click Allow Shadowing. Next, click the Prohibit Being Shadowed Without Notification setting.

- A6: Answer D is correct. Because shadowing has been configured by default on the server not to require notification, and because the administrators have access to shadow users on a MetaFrame server, the only policy rule that must exist is one that will force the managers to be notified when a shadow request is being initiated. Answer D does this by filtering on the two managers (Alice and Bob) and then setting the rule that shadowing is prohibited without first notifying the user.

Answer A actually creates a rule that allows members of the Customer Service group to shadow Terminal Server Administrators without the administrators being prompted. The only two users who cannot do this are the two managers, Alice and Bob. Answer B modifies shadowing so that members of the Customer Service group are notified before shadowing. Even though Alice and Bob are granted access to shadow Customer Service users, the fact that this policy is denied for Customer Service members means that the managers effectively have no access to perform shadowing. The Deny privilege overrides the Allow privilege. Answer C does the exact opposite of what we want. Instead of ensuring that only managers receive the notification, this rule would ensure that all members of the Customer Service group required notification, with the exception of the two managers, who would not receive this policy because they were omitted from the filter with the Deny setting.

7. A policy called Lockdown has been created, and the following filter settings have been defined:

- IP address range: Not defined.
- Client names: SECURE01, SECURE02, WI\_\*
- Server: DEVMF01
- User names: DEVAD\todd, DEVAD\linda, DEVAD\liane

Choose the following search criteria that will allow you to successfully determine the resultant set of policies for a client.



- A. Client IP Address: \*

Client Name: SECURE01

Server: DEVMF01

User: DEVAD\linda



- B. Client IP Address: 192.168.1.10

Client Name: SECURE\*

Server: DEVMF01

User: DEVAD\toddm



- C. Client IP Address: 192.168.1.10

Client Name: SECURE01

Server: DEVMF01

Users: DEVAD\Domain Users



- D. Client IP Address: 192.168.1.10

Client Name: SECURE01

Server: DEVMF01

Users: DEVAD\liane

A7: Answer D is correct. To ensure that you do not have any partial results returned from the search, you must provide all the necessary information, even if none was included when creating the filter for the policy. Answer A is incorrect because the IP Address was omitted. Answer B is incorrect because SECURE\* is an invalid client name when searching. The wildcard character is valid only when creating a filter for a policy. Answer C is incorrect because DEVAD\Domain Users will return no results; the reason is that the policy was not filtered on that group but was filtered only on the specific usernames Todd, Linda, and Liane.

8. When configuring ICA connections using the Citrix Connection Configuration tool, Adam, the administrator, disabled the display of desktop wallpaper. Now, within his policy called Wallpaper Exception, he has set the Visual Effects rule Turn Off Desktop Wallpaper to Disabled. But when he logs on as a user who should be assigned the policy, the desktop wallpaper is still not displayed. Select all the valid reasons why this policy is not taking effect.

A. A higher-ranking policy is overriding this setting and turning off the desktop wallpaper.

B. The user is not being assigned the policy because of an alternate filter that Adam is not aware of.

C. This policy only turns off the desktop wallpaper; it does not turn it back on.

D. The user is connecting via the Web Interface. The desktop wallpaper is never displayed for Web Interface users.

A8: The only valid answer for this question is C. Because the desktop wallpaper has been turned off at the connection level, it will remain off, regardless of the policies that are implemented. The Turn Off Desktop Wallpaper rule only turns off the wallpaper. It never turns it on. Although Answers A and B would be valid when dealing with policy troubleshooting, they are not valid reasons why the desktop wallpaper is not being displayed in this situation. Answer D is completely false. Users accessing a full desktop via the Web Interface would still see the desktop wallpaper if it was not disabled.

9. From the following statements regarding MetaFrame user policies, select the statements that are not true. (Select all that apply).

- A. Multiple policies can be defined for a server farm, and each policy can have one or more rules defined within it.
  - B. Each user is automatically assigned the Default policy, which contains the main server farm settings. The rules in this policy always take precedence unless the priority of the policy is reduced through the Management Console.
  - C. When a new policy is created, it is automatically assigned the priority of 1. You can then adjust this as necessary to suit your environment.
  - D. Policy assignments are dictated by filters. When a policy is first created, no filters are assigned to it. You must define a filter before the rules in the policy apply to anyone connecting to the farm.
- A9: Answers B and C are both invalid. There is no such thing as a Default policy that is assigned to all users. Unless you create a policy, the system has no policies available by default. When new policies are created, they are automatically assigned the lowest available priority, not the highest. Answers A and D are both valid statements.
10. From the following statements regarding MetaFrame user policies, select the statements that are true. (Select all that apply.)
- A. User policies cannot be applied to users connecting via the Web Interface. If you have users connecting in this fashion, it is recommended that you not implement user policies.
  - B. The easiest way to filter on servers is to use the wildcard (\*) character. This saves you from having to type in the name of each server in your farm.
  - C. When filtering on user groups, you can specify only domain groups. Local MetaFrame server groups are not supported.
  - D. You can turn off the Auto Client Update feature through MetaFrame group policies.

A10: Only answer D is a truthful statement. The Auto Client Update feature can be turned off using the rule found under the Maintenance category. Answer A is invalid because Web Interface users can be filtered using the WI\_\* wildcard for client names. Answer B is invalid because MetaFrame does not allow you to type in server names when creating a filter. You must select it from the list provided. Answer C is also invalid because local MetaFrame server groups can be used when defining a policy filter.

11. A colleague asks you to help resolve an issue that she is having setting up the zone preference and failover option. Which of the following questions would you ask her to help troubleshoot the problem? (Select all that apply.)

A. What edition of MetaFrame Presentation Server are you running?

B. Have you created a MetaFrame user policy; assigned it to the proper IP address, client name, username, or server; and defined the settings for the Zone Preference and Failover rule?

C. Have you enabled Zone Preference support in the properties for the farm?

D. Do you have more than one zone?

A11: Answers A, B, and D are all valid questions to ask. Zone preference and failover requires the Enterprise Edition of MPS, so if your colleague is running Standard or Advanced Edition, she cannot configure this option. To set this option, you must have configured the user policy properly. If the right filter is not in place, it will not behave as expected. Zone failover is supported only when there is more than one zone in the farm. When only a single zone is present, the option cannot be edited. Question C is the only one that you would not ask your colleague because no such option exists under the Properties for the server farm. All zone preference and failover settings are managed through MetaFrame user policies.

## Need to Know More?



Citrix Systems, "MetaFrame Presentation Server Administrator's Guide." Available online at <http://support.citrix.com/docs>, and from the online documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Extended Policies FAQ." Available in the Citrix knowledgebase online at <http://support.citrix.com>. Document ID CTX103793.

# 8. Citrix Load Management

Terms you'll need to understand:

- Load evaluators
- Rules
- Default
- Advanced
- Boolean
- Moving Average
- Incremental
- Moving Average Compared to High Value

Concepts you'll need to master:

- How load management works
- What load evaluators are
- What rules are

Citrix's load management system, Load Manager, available as a component of MetaFrame Presentation Server, is one of the most sought-after features of MPS. It therefore is in a class of its own when compared to other server-based computing products. It's important for enterprise-class IT shops to be able to direct users to the least busy servers to maximize the users' experience when using a remote session to connect to applications. So what makes Citrix's load management so special and different? Citrix allows you to customize the criteria by which a load is spread across servers. Usually, the standard load balancer spreads user load across servers evenly, so if you have three servers in your farm, it ensures that user load is always equal on all servers.

Being able to spread the load is good, but what if you have processor-intensive applications, for example? If you spread user load evenly, users may become frustrated because a single user can hog the CPU on a server if the application he or she is running is CPU intensive. In this case, the other sessions that are connected to this server will be very slow, rendering them incapable of being productive.

With the Citrix load balancer, however, you can alleviate this problem by configuring your load based on a number of different resource criteria. You can, for example, configure it so it points users to a server that has very little CPU utilization. So using the preceding example, you may end up with a server that has 4 users on it and another server that has 10 users on it. The result is that all users are happy.

# Overview of Citrix Load Management

Let's examine how the process of load balancing occurs in a MetaFrame environment:

1. A user clicks a published application.
2. The request is forwarded to the Data Collector of the zone that holds load information from all the servers in that zone.
3. The Data Collector returns the ID of the server with the lowest load.
4. A session is established between the user and that server.

This series of steps provides a simplified version of the way the process actually works. As you read through this chapter, I will elaborate on the more detailed steps showing how the process actually unfolds.

The load-balancing feature's sole purpose is to spread application load over to the server with the most available resources. In other words, if you have installed an application on 10 servers, it's the load balancer's duty to direct connecting users over to the server that will most adequately serve them. This result is accomplished based on a set of rules and load evaluators that govern how this process should work.

## Alert

It's important that you clearly understand that Citrix load balancing does not provide clustering or "hot" fail-over support. If a server crashes, the user connection is still lost, along with any unsaved data. Load balancing will allow that user to immediately log back on to a different server (if available) and resume working.

## Requirements

Like any other component, Load Manager has a set of requirements that must be met before it functions properly. Ensure that you meet the following criteria:

- Load Manager is available only with the Advanced and Enterprise Editions of MPS. The Standard Edition does not come with Load Manager.
- You must use the same network protocol (TCP/IP, IPX, and so on) across all servers you intend to load balance. If, for example, you have four servers in your environment, two running TCP/IP and two running IPX, the two that are running TCP/IP load balance between each other, and the two that are running IPX load balance between each other. If you want all four of them to load balance, both TCP/IP and IPX have to be loaded on all servers.

- You need MetaFrame administrative rights to manipulate or configure Load Manager.

 PREV

NEXT 

# Load Evaluators and Rules

Citrix MetaFrame was built with enterprise scalability in mind. In any IT shop, you will notice that not all servers have the same hardware. This is obviously due to the different times at which servers were purchased, and with the constant advances in the IT world, you are almost certain to get a different CPU clock speed and newer, better components in every server you purchase.

When you add newer, better servers to your farm, you expect these servers to handle more load than existing servers with older hardware. Now imagine if you were doing just standard load balancing, which means spreading user load across all available servers equally. In this case, you do not really benefit from the new hardware you purchased because all the servers get an equal amount of load.

Citrix load management was designed with this fact in mind, and that is why it allows you to customize how load is spread based on load evaluators and rules. A load evaluator is a grouping of several rules that can be applied to servers to provide load balancing. Load evaluators consist of one or more rules. Rules are configurable agents that measure or monitor specific resources on the servers. Two load evaluators are available with MetaFrame Presentation Server Advanced and Enterprise Editions: the Default load evaluator and the Advanced load evaluator. The following sections closely examine each of these two components.

## Default

The Default load evaluator is assigned to all servers by default. This evaluator's function is reasonably simple: It balances the load based on the user load rule. You can also set a maximum user limit. For example, if you set the limit to 150 users, when the 151<sup>st</sup> user tries to establish a session, that user is rejected by the server. This evaluator cannot be modified or deleted. Using this load evaluator is probably a good idea if you are dealing with servers that have the same hardware configurations. When you start mixing and matching servers with different hardware, however, this evaluator does not meet the challenge.

## Advanced

The advanced load evaluator is much more powerful than the default and is better suited to handle servers with different hardware resources. It balances the load based on the CPU utilization, memory usage, and page swaps rules.

### Note

Both the default and advanced load evaluators are preconfigured and cannot be changed or altered. You should consider creating your own load evaluator based on the set of rules that best suit your environment to achieve the best performance and optimization possible.

It's important to note that load evaluators can be assigned to either servers or published applications.

It's also important to know that only one load evaluator can be assigned to a server or published application. In the event that a published application has a load evaluator and also is hosted on a server that has a load evaluator assigned to it, the evaluator with the highest threshold is used.

## Alert

Default and Advanced evaluators cannot be directly modified, but they can be copied and used to create new rules if desired.

 PREV

NEXT 

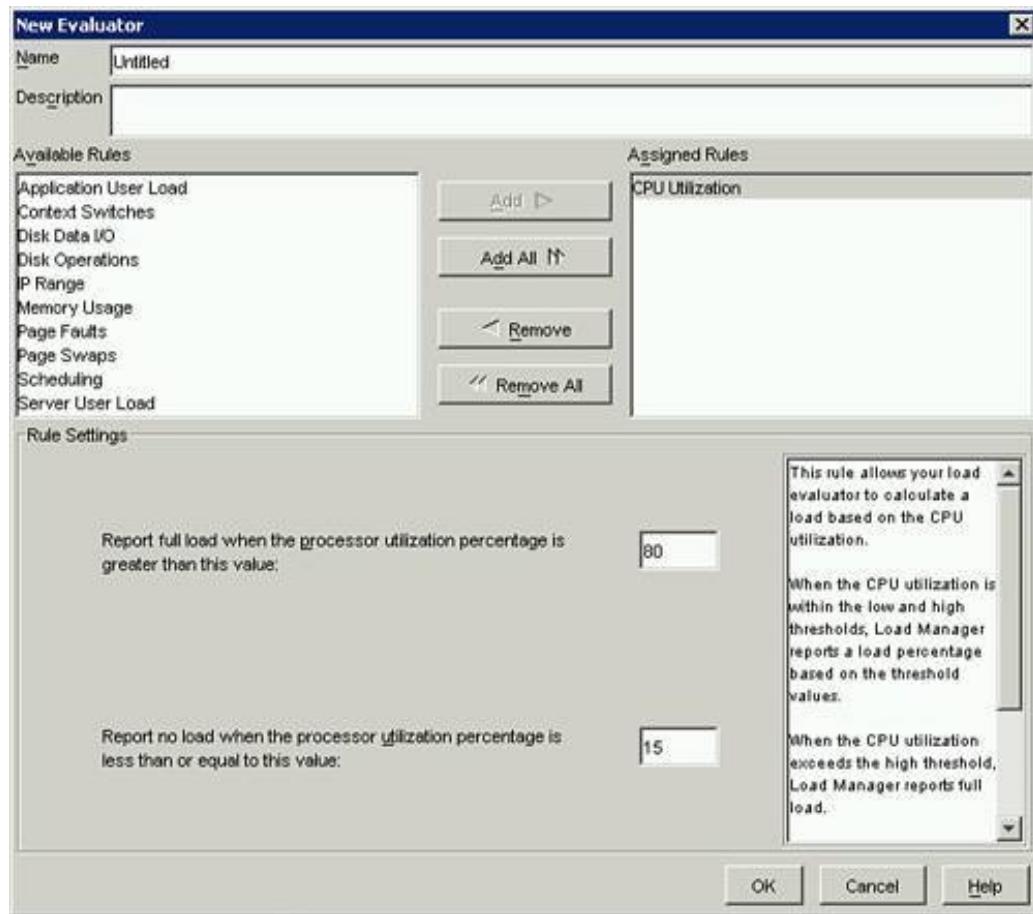
## Rules

Rules are the metrics by which the hardware resources are measured or monitored. One rule, for example, reports the CPU utilization of a particular server. Rules make up a load evaluator. You can choose from the following 11 rules provided by Citrix MPS to create an evaluator that will meet your server farm's needs:

- Server User Load This rule balances load based on the number of users who log in to a particular server. It spreads load evenly between servers. You can specify any value between 1 and 10,000 to indicate that the server is at 100% capacity. So if you set the value to 100, when the number of users on this server reaches 100, new connections are denied.
- Application User Load This rule is fairly straightforward; it calculates load based on the number of users accessing a published application. You can specify any value between 1 and 10,000 to indicate that the server is at 100% capacity.
- CPU Utilization As the name implies, this rule calculates load based on CPU utilization. It allows you to set a low and a high threshold. When the CPU is within the low/high threshold you configured, load management reports a load. If the threshold reaches the high value that you set, it reports a 100% capacity reached on the server and denies new connections. If the CPU is below the low threshold you configured, no load is reported. The values that you can configure for this rule are between 1 and 100 and are in percentage of utilization. [Figure 8.1](#) shows the CPU Utilization rule configured with a high threshold of 80 and a low threshold of 15.

Figure 8.1. A load evaluator with the CPU Utilization rule added.

[\[View full size image\]](#)



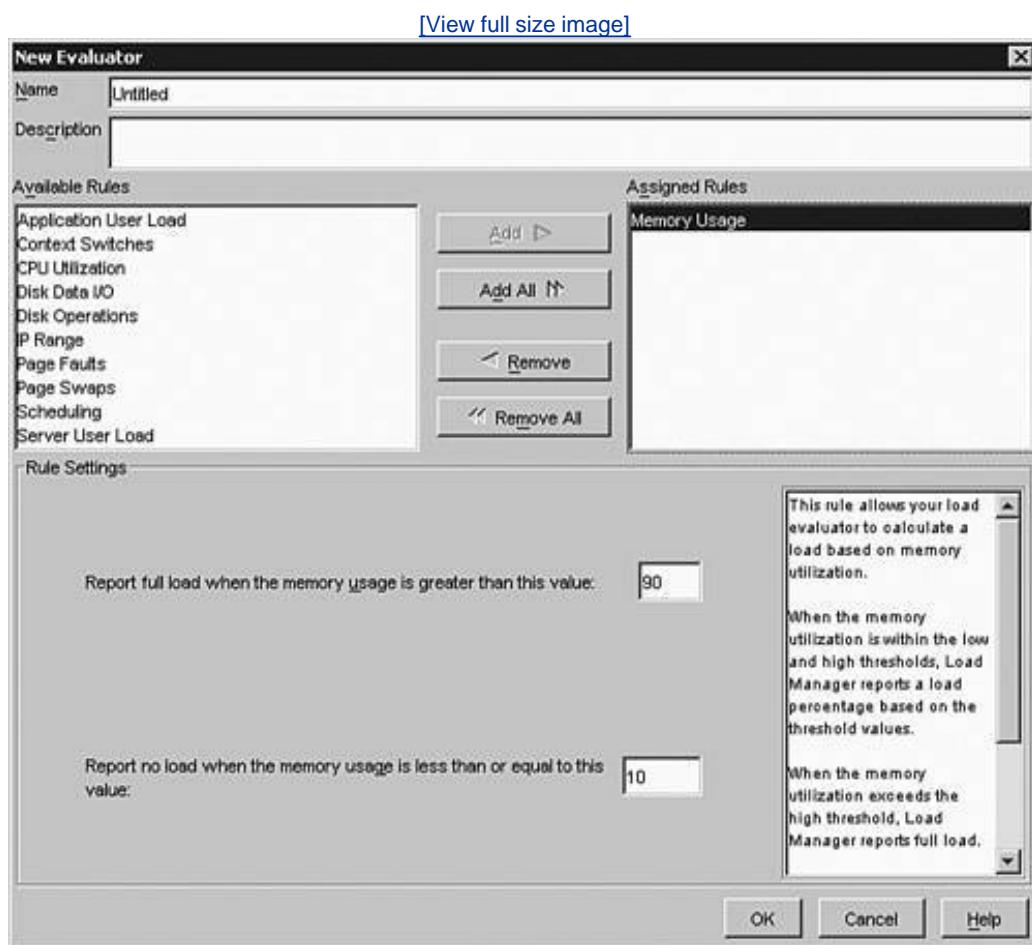
- Context Switches This rule calculates load based on the number of times a CPU context switch occurs. A context switch occurs every time the operating system switches from one executing process to the other. Similar to CPU Utilization, this rule enables you to configure a low/high rule whereby once context switching is within the configured threshold, load is reported. The valid configurable values are 02147483647.
- Disk Data I/O This rule calculates load in kilobytes based on disk data I/O. It has a low/high configurable threshold, and the same as the other rules, when the disk data I/O is within the low/high threshold, load is reported. The valid configurable values are 02147483647.
- Disk Operations This rule calculates load based on disk operations per second. It has a low/high configurable threshold, and the same as the other rules, when the Disk Operations are within the low/high threshold, load is reported. The valid configurable values are 02147483647.
- IP Range This rule is not really a load rule because it does not actually use any criteria to spread load. Instead, it is used to control access to published applications based on an IP range. For example, if a client's computer falls within this IP range, this rule allows or does not allow access. This rule should be used in conjunction with another rule to achieve some level of load management. [Figure 8.2](#) shows the configurable values of the IP Range rule.

Figure 8.2. The IP Range Rule value settings.



- **Memory Usage** This rule calculates load based on memory utilization. It allows you to set a low and a high threshold. When the memory is within the low/high threshold you configured, load management reports a load. If the threshold reaches the high value that you set, it reports a 100% capacity reached on the server and denies new connections. If the memory utilization is below the low threshold you configured, no load is reported. The values that you can configure for this rule are between 1 and 100. In [Figure 8.3](#), Memory Usage is configured with a high threshold of 90 and a low threshold of 10.

[Figure 8.3. The Memory Usage Rule settings window.](#)

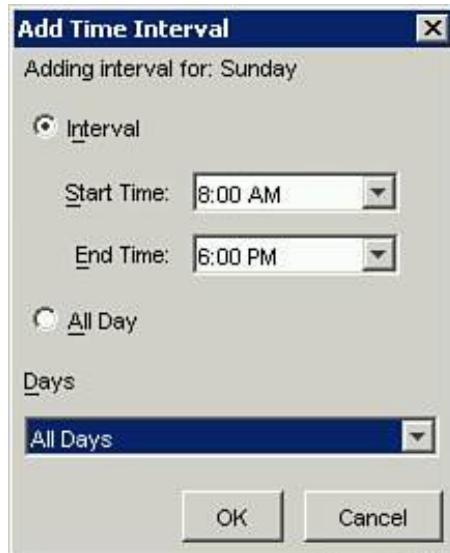


- **Page Fault** This rule allows the load evaluator to calculate load based on the number of page faults per second that occur. A page fault occurs every time the operating system uses physical memory flushed to the hard disk. It has a low/high threshold configuration. The valid configurable values are 02147483647.
- **Page Swap** This rule allows the load evaluator to calculate load based on the number of page

swaps per second that occur. A page swap occurs every time the operating system uses physical memory instead of virtual memory. It has a low/high threshold configuration. The valid configurable values are 02147483647.

- Scheduling This rule, similar to the IP Range rule, is not considered a load-balancing rule. It is used to allow or disallow access to a server or published application during specific days of the week or times of the day. This rule should be used in conjunction with another rule so that load management can really spread load. As you can see in [Figure 8.4](#), you can set the time and date for the Scheduling rule.

Figure 8.4. Configuring the Scheduling rule.



## A Blast from the Past

Prior to MetaFrame Presentation Server 3.0, there was a 12th rule that you could add to a load evaluator. That rule, called the License Threshold, has been removed in MPS 3.0 because the licensing module has been removed and is now available in the Citrix License server.

The License Threshold rule allowed you to control or balance load based on the number of licenses that users consumed when accessing a particular application. Imagine you had three applications in your organization, each belonging to a different department. Department 1 did not want Department 3 to take advantage of its licenses and wanted to ensure that when its users logged in, a license would be available. With this rule, you could configure the licensing threshold for each published application with a certain number of available licenses. When that amount was reached, the load was reported as full, and no further connections were allowed. The valid range was between 0 and 9,999.

Now that you have learned the rules available, it's time to look at the categories or types that these rules fall within. These rules can belong to the following four categories:

- Moving Average This type or category hosts rules that are based on the percentage of the resource being used.
- Moving Average Compared To High Value This type hosts rules that use a percentage to calculate high and low thresholds based on the values 02147483647.
- Incremental This type hosts rules that use an integer value to determine when the server or published application has a full load. For example, if you set a value to 30, when you have 30 users on a server, no more connections can be allowed.
- Boolean This type hosts rules that simply allow or disallow connections.

Table 8.1 organizes the rules within their respective types.

Table 8.1. Rule Types

Type	Moving Average	Moving Average Compared to High Value	Incremental	Boolean
Rule	CPU Utilization	Context Switches	Server User Load	IP Range
	Memory Usage	Disk Data I/O	Application User Load	Scheduling
		Disk Operations		
		Page Fault		
		Page Swap		

## Alert

You should be aware that prior to MetaFrame Presentation Server 3.0, there existed a 12th rule by which load could be calculated; it was known as the License Threshold. Because licensing has been moved to a separate licensing server in MPS 3.0, this rule is no longer a configurable option and does not show up. Be aware of trick questions on the exam.

 PREV

NEXT 

## Creating a New Load Evaluator

Now that you have read the theory and definitions, it's time to look at how you can create a load evaluator using the Management Console. Follow these steps:

1. Open the Management Console, and in the left control pane, select Load Evaluators.
2. Click the Actions menu, scroll to Load Evaluators, and click New Load Evaluator.
3. Name and describe your new load evaluator.
4. On the right, you are presented with the available rules you can add to this load evaluator. Add the appropriate ones to the Assigned Rules list.
5. Highlight each rule in the Assigned Rules list and configure its thresholds and/or values as you see necessary.
6. Click OK to save your new load evaluator.

# Assigning a Load Evaluator

Creating a load evaluator is just a first step, and the servers or published applications don't know yet of this load evaluator's existence. This section covers how to assign a load evaluator to a server or published application.

As mentioned earlier, all servers are assigned the default load evaluator as soon as they are joined to the farm, provided that these servers have either an Advanced or Enterprise license.

You can assign different load evaluators to different servers or published applications depending on what you deem appropriate for optimized performance. Some applications may be CPU intensive and as such need a load evaluator that addresses that resource, whereas others are memory intensive.

To assign a load evaluator to a server or published application, follow these steps:

1. Open the Management Console and select the Load Evaluator node in the left control pane.
2. On the Actions menu, scroll to Load Manager and click on Load Manage Server or Application (depending on whether you are attaching the evaluator to a server or published application).
3. Select the appropriate load evaluator and click OK.

## Editing and Deleting a Load Evaluator

After you create the load evaluator and assign it, you often may need to come back to it and edit its properties and tweak them a bit more to further enhance the load management. You may need to update or change the thresholds you configured on a particular rule, for example. To make these changes, follow these steps:

1. Open the Management Console and select Load Evaluators in the left control pane.
2. In the right control pane, right-click the load evaluator you want to edit and click Load Evaluators Properties.
3. Change the name, description, assigned rules, values, and thresholds of rules as necessary.
4. Click OK to save your changes and exit.

To delete a load evaluator, simply right-click it and click Delete Load Evaluator.

### Note

The default and advanced load evaluators cannot be edited or deleted.

## Copying a Load Evaluator

You will find copying load evaluators a handy task when you are familiar with load management and have designed load evaluators for different servers and published applications. Instead of re-creating an evaluator from scratch, you can copy an existing one that might have most of your settings and then edit it by removing or adding rules and changing settings.

To copy a load evaluator, follow these steps:

1. Open the Management Console and select the Load Evaluators node in the left control pane.
2. Right-click the evaluator you want to copy and select Duplicate Load Evaluator.

# Using Load Manager

The following sections concentrate on the methods by which you can monitor and get useful information out of Load Manager based on the evaluators you created and rules you configured. After all, this is what using the Load Manager is all about watching the load and ensuring servers aren't being taxed and users' sessions are smooth and performing the way they should.

## Monitoring Load

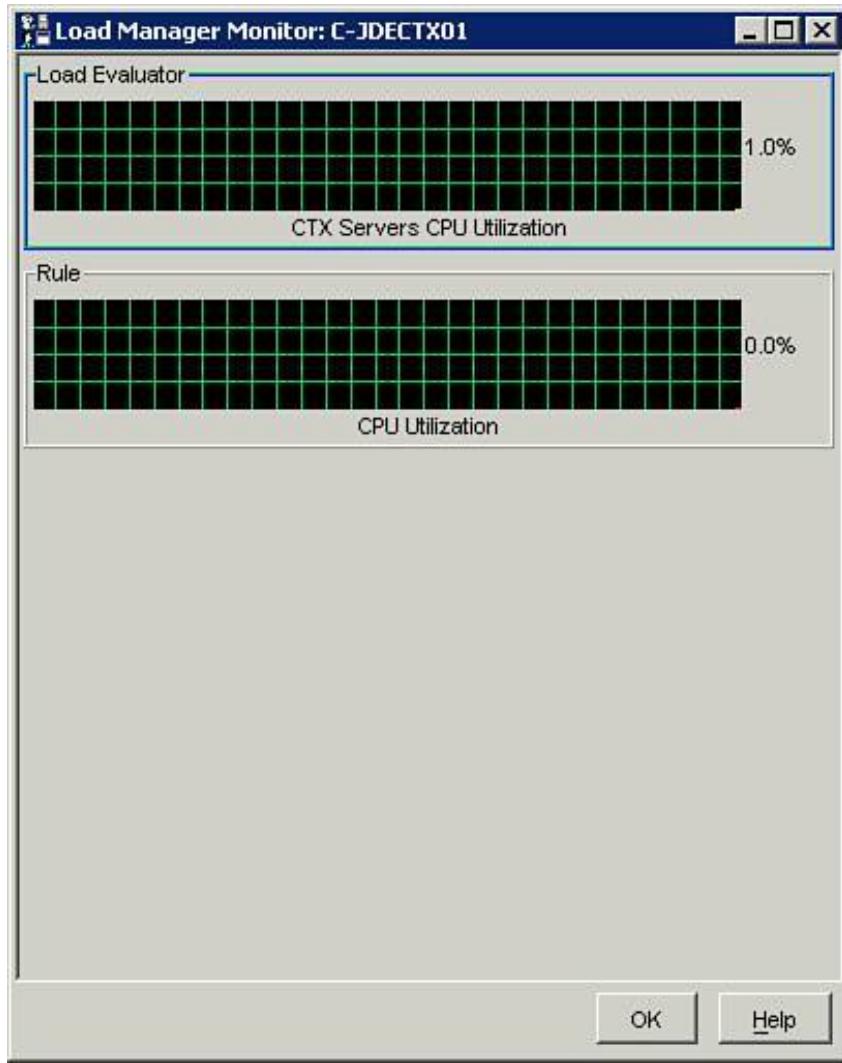
One of the most frequent tasks a Citrix administrator does during the day is monitor the load on the servers. Performing this task not only indicates how things are running, but it also gives the administrator an idea of whether additional servers are needed to maintain the user's level of expectation from the system and to accommodate new users who may be added to the different applications in the server farm.

To monitor the Load Manager on a particular server, follow these steps:

1. Open the Management Console and expand the Servers node in the left control pane.
2. Choose the server where you want to view the Load Manager and click the Load Manager Monitor tab in the right control pane.

If you want to view the Load Manager Monitor (LMM) in a separate window, you can right-click the server in question and click Load Manager Monitor. This launches a separate window displaying the Manager (see [Figure 8.5](#)).

Figure 8.5. Load Manager Monitor in a separate window.



You may choose to clear the graph that displays the Load Manager Monitor data. To do so, select the server in question, and from the Actions menu, scroll to Load Manager Monitor and click Clear Monitor Display.

## Load Manager Log

The Load Manager log records all ICA connection requests made to the server farm. Obviously, it monitors only those ICA connections made to servers that have load balancing installed. Remember that the log is disabled by default. If you choose to enable it, follow these steps:

1. Open the Management Console and select Load Evaluators in the left control pane.
2. Select the Log tab in the right control pane.
3. On the Actions menu, select Log and then click Enable Logging.

To view the log after you have enabled it, do the following:

1. From the Management Console, select the Load Evaluators node.
2. In the right control pane, click the Log tab.

To save the log, from the Actions menu, select Log and then choose Save Log. Similarly, to clear the log, from the Log menu, select Clear Log.

## Information Updates

The information displayed in the Load Manager Monitor and the load that the servers report are based on settings that are set by default. The LMM updates every minute, and the load evaluators report every five minutes. You have the option of changing the frequency of updates that occur. To do so, follow these steps:

1. Open the Management Console and select the Load Evaluators node in the left control pane.
2. From the Actions menu, select Load Manager and then select Load Manager Settings.
3. Change the frequency of the updates to your liking (see [Figure 8.6](#)).

Figure 8.6. Load Manager frequency update settings.



4. Click OK to save the settings and exit.

## Usage Reports

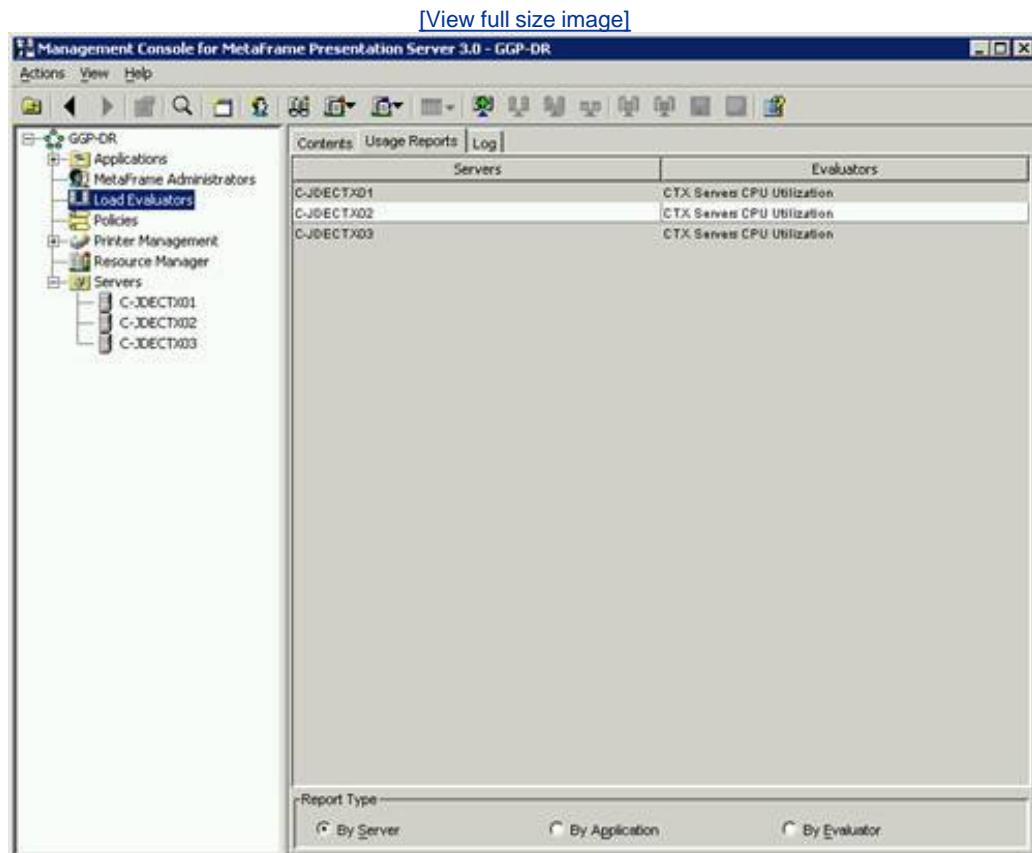
The usage reports are a quick way of showing how load evaluators are distributed in your server farm. In other words, they provide a snapshot of which load evaluator is attached to which server or published application, making it easier for you to consolidate and administer the load management process. To use usage reports, follow these steps:

1. Open the Management Console and select the Load Evaluators node in the left control pane.
2. In the right control pane, select the Usage Reports tab.

You are presented with three options by which you can view reports:

- By Server This view lists every server in the farm and its assigned load evaluator, as shown in [Figure 8.7](#).

Figure 8.7. Usage Reports view by server.



- By Application This view lists all the published applications in the farm and their assigned load evaluators.
- By Evaluator This view lists all the load evaluators and the servers or published applications they are assigned to.

## Alert

Recognize the different ways in which you can determine what load evaluators are associated with which server or application.

## Uninstalling Load Manager

Because Load Manager is installed by default as part of any MPS Advanced or Enterprise Edition server, you can uninstall it only by removing MPS from the server or by changing the MetaFrame edition from Advanced or Enterprise to Standard. To do this, follow these steps:

1. Open the Management Console and expand the Servers tab.
2. Right-click a server and select Set MetaFrame Edition.

 PREV

NEXT 

## Exam Prep Questions

1. If you decide to use the default load evaluator to spread user load among servers, when will the evaluator report a full load and start refusing incoming user sessions?

- A. When the user load reaches 100 users
- B. When the user load reaches 1,000
- C. When the user load reaches 1,500
- D. When the user load reaches 2,000

A1: Answer A is correct. The default load evaluator is preconfigured to report a full load when the server reaches 100 users. Choices B, C, and D are incorrect because the configured values do not reflect the number that is preconfigured by default.

2. Your Citrix server farm consists of 10 load-balanced servers that were all purchased at the same time, and they all have identical hardware. The servers load balance your CRM application, which is very CPU intensive. Your organization has just acquired another company, and this acquisition now requires the expansion of your server farm. You order 5 new servers with faster CPUs. What should you do to make sure the load is properly spread?

A. Create or modify your load evaluator to include the CPU Utilization rule.

B. Create or modify your load evaluator to include the Page Swaps rule.

C. Create or modify your load evaluator to spread load based on the Server User Load rule.

D. Create or modify your load evaluator to spread load based on the Memory Usage rule.

A2: Answer A is correct. Because your new hardware has faster CPUs, the ideal load evaluator would be to load manage servers based on CPU Utilization. This way, you ensure that all servers can handle the proper number of users. Obviously, the more advanced servers will handle more sessions than the ones with older hardware. Choice B is incorrect because this configuration does not take advantage of the new CPUs installed with the new hardware, and because the application is CPU intensive. Choice C is incorrect because Server User Load is not the correct configuration when you are dealing with server hardware that is not identical. Choice D is incorrect because there is no mention of the new servers having more memory than the older ones. In addition, the CRM application is CPU intensive.

3. Which of the following can be classified in the Boolean type or category? (Choose all that apply.)

A. Memory Usage

B. Context Switches

C. Disk Operations

D. IP Range

A3: Answer D is correct. The Boolean type or category consists of a permit or deny rule. Members of this category include IP Range and Scheduling. Choice A is incorrect because

Memory Usage belongs to the Moving Average category. Choice B is incorrect because Context Switches belongs to the Moving Average Compared to High Value category. Choice C is incorrect because Disk Operations also belongs to the Moving Average Compared to High Value category.

4. When you activate an MPS 3.0 Advanced or Enterprise Edition license, which load evaluators come preconfigured? (Choose all that apply.)

A. Static

B. Standard

C. Advanced

D. Default

A4: Answers C and D are correct. The two preconfigured load evaluators that come with MPS 3.0 Advanced and Enterprise Editions are advanced and default. Choices A and B are wrong because no such load evaluators exist.

5. Your environment consists of five load-balanced MPS 3.0 Advanced Edition servers. You have published the Microsoft Office suite on all five servers named Servers 1 through 5. Server 1 has gone down due to hardware issues. What happens to the users who are connected to this server?

A. The sessions are lost, but when users reconnect, their session will be in the state where they left it before the server went down. No data is lost.

B. Because the servers are running MPS 3.0 Advanced Edition, which supports load balancing, all the sessions are automatically spread over the remaining servers.

C. The sessions are lost. The users will have to reconnect to the published application. Any unsaved data is lost, and a new session is started.

- D. Because MPS 3.0 Advanced Edition is being used, built-in code will notice the server is experiencing hardware issues and will save users' work automatically and log them off gracefully, thus not causing any loss of work in progress.
- A5: Answer C is correct. As mentioned earlier, load balancing is not fault tolerance; therefore, in the event that a server goes down for any reason, all sessions on that server are lost and cannot be recovered; plus, any unsaved work is lost. Choices A, B, and D are incorrect because they do not describe the true functionality of load balancing.
6. When you create a load evaluator with multiple rules in it, how do these rules interact together to determine the load on the server? Which of the following statements is true?
- 
- A. When any of the rules reach the defined threshold, the server reports a full load.
- 
- B. The rules conflict, but you can set values to determine which rule takes precedence.
- 
- C. Multiple rules cannot be assigned to the same load evaluator.
- 
- D. Multiple rules automatically interact together to determine the server or published application load.
- A6: Answer D is correct. When multiple rules are assigned to the same load evaluator, the rules automatically work together to determine the overall server or published application load. Choices A, B, and C are incorrect because they are false statements that do not reflect the method by which Load Manager handles multiple rules in load evaluators.
7. You have just been hired to tweak the Citrix server farm for company ABC. When you launch the Management Console and look at the default load evaluator, you notice its value is set to 100. You want to lower this parameter but notice that all the fields are grayed out. Why?

- A. The default load evaluator is loaded as part of the Advanced and Enterprise Editions and cannot be edited or modified.
  - B. You are logged in to the Management Console with a user account that does not have enough privileges to make changes.
  - C. The server that holds the load evaluators is down; therefore, you can only view but not modify the values.
  - D. Another Citrix administrator has the load evaluator open; therefore, you are prevented from making changes.
- A7: Answer A is correct. The default load evaluator cannot be modified or edited. This is by design. To get around this limitation, you can create a new load evaluator, give it the same rule as the default one, and modify the value to your liking. Choices B, C, and D are incorrect because they are all false statements.
- 8. To maximize your users' ICA session experience, you have created a load evaluator that load balances your users across your 10 servers. The load evaluator allows only 30 users per box. This number ensures a smooth session. Your servers are currently all reporting 30 users. What happens to a new user who tries to connect?
  - A. The load evaluator ignores the rule and continues to spread load evenly among all the servers.
    - B. The connection is refused.
  - C. The load evaluator automatically increases the values of the load evaluator in increments of 10.
  - D. The load evaluator automatically increases the values of the load evaluator in increments of 5.

A8: Answer B is correct. When the servers report a full load, new connections are refused. This is the purpose of setting a value for full load. Setting the value ensures the existing users continue to have a smooth session and the servers are not overloaded to the point where no one can work. Choices A, C, and D are incorrect because they don't reflect the true behavior of the Citrix load-balancing module.

9. Which application or utility would you use to monitor application load within your Citrix server farm?

A. The Management Console

B. Citrix Server Administration

C. Citrix Load Manager Monitor

D. Citrix Load Balancing Monitor

A9: Answer A is correct. The Management Console is the program that you would run to monitor all types of loads on your servers and on your published applications. Choice B is incorrect because Citrix Server Administration is a legacy application that was available with MF 1.8 and has long been replaced and incorporated into the Management Console. Choice C is incorrect because the Load Manager Monitor is part of the Management Console and cannot run independently of it. Choice D is incorrect because no such application exists.

10. Which flavor of MetaFrame Presentation Server is needed to use the features and functionality of load balancing? (Choose all that apply.)



A. MPS 3.0, Advanced Edition



B. MPS 3.0, Standard Edition



C. MPS 3.0, Corporate Edition



D. MPS 3.0, Enterprise Edition

A10: Answers A and D are correct. To use load balancing, you need an MPS 3.0 Advanced or Enterprise Edition license. Choice B is incorrect because Citrix does not offer the load-balancing functionality with MPS 3.0 Standard Edition. Choice C is incorrect because there is no Corporate Edition.

11. You have a server farm consisting of 10 Citrix servers. Five of these servers are running the TCP/IP protocol and are load balanced among each other. The other 5 are running IPX and are load balanced among each other. What must you do to allow load balancing to occur among all 10 Citrix servers?



A. You can't. An MPS 3.0 server can listen on only one protocol at a time.



B. Install TCP/IP on the IPX servers.



C. Install IPX on the TCP/IP servers.



D. Install IPX on the TCP/IP servers and TCP/IP on the IPX servers.

A11: Answer D is correct. If you want to load balance MPS servers with different protocols, both protocols should be present on all the servers. Choice A is incorrect because it is a false statement; two protocols can exist on the same server. Choices B and C are incorrect because they address only part of the issue.

 PREV

NEXT 

# 9. MetaFrame Security

Terms you'll need to understand:

- Administrative delegation
- Privilege types
- ICA connection encryption and SecureICA
- Minimum required encryption level
- Kerberos client authentication
- SSL Relay
- Server certificate
- Root certificate
- Certificate authority

Concepts and techniques you'll need to master:

- Planning and defining administrative privileges
- Delegating privileges based on different server farm zones
- Troubleshooting administration issues caused by delegation settings
- Defining the minimum required ICA encryption level
- Troubleshooting encryption issues from connecting clients
- Configuring a MetaFrame server farm to support Kerberos client authentication
- Recognizing the differences between ICA encryption and Kerberos authentication
- Assigning a server certificate to a MetaFrame server
- Describing the role of a certificate authority and the reason for root certificates

No MetaFrame Presentation Server (MPS) implementation would be complete without an administrator ensuring that the server farm had been properly secured. In this chapter, we focus on the client and server methods available as part of the core MPS software that allow an administrator to secure his or her server farm. Another access security component, called the Secure Gateway for MPS, will be discussed in [Chapter 14](#), "Web Access to the MetaFrame Server Farm." The Secure Gateway for MPS is implemented only if you're leveraging the Web Interface for MPS to provide secure web browserbased access to the server farm. The four security-specific MPS components—administrative delegation, ICA connection encryption, Kerberos client authentication, and SSL Relay—are part of the core MPS software and are reviewed in this chapter.

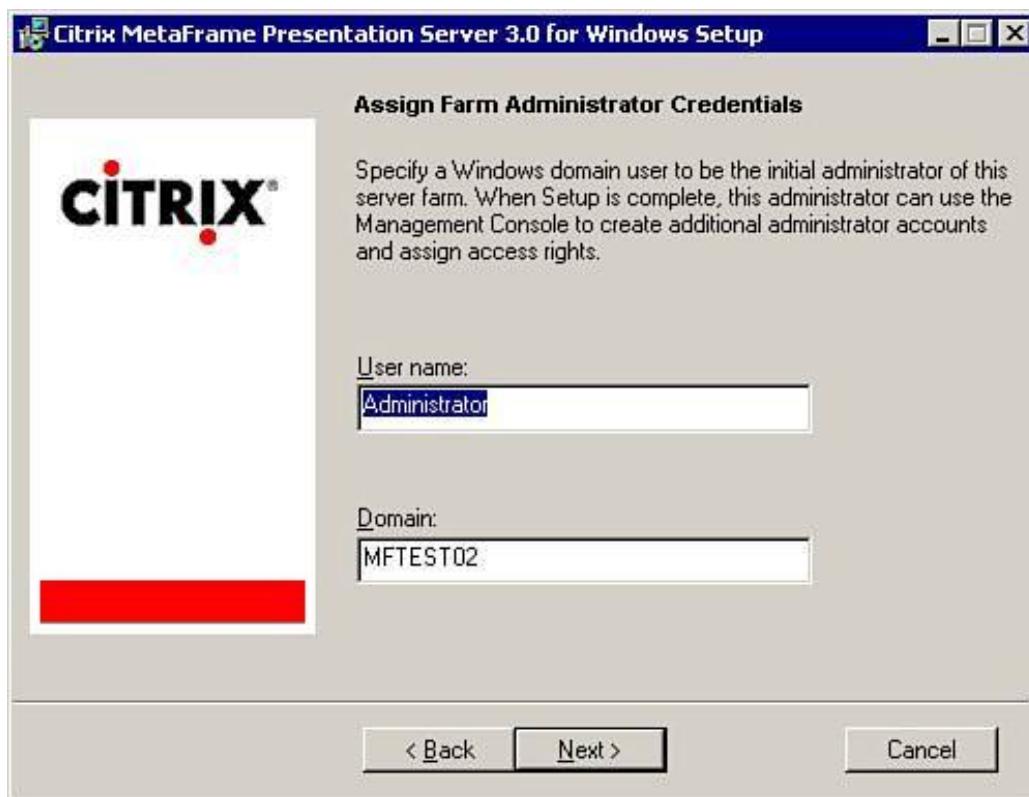
 PREV

NEXT 

## Administrative Delegation

Securing an MPS environment begins when you install MetaFrame onto the first server in the farm. You should remember that during the creation of the new data store for the server farm, you are prompted to provide the username and domain that will be assigned as the first administrator for the farm (see [Figure 9.1](#)). Any member of a Windows or a Novell Directory Services (NDS) domain can be granted access to administer a MetaFrame server farm.

Figure 9.1. Full access is delegated for the first time during the installation of the first server in a new farm.



This user is automatically granted full administrative authority over the farm and is the account that must be used when logging in to the Management Console for the first time.

When you are logged in to the Management Console, you then can delegate varying levels of administrative authority to specific users and/or user groups.

## Delegation Examples

Although the existence of only a few administrators with full authority to the server farm is usually

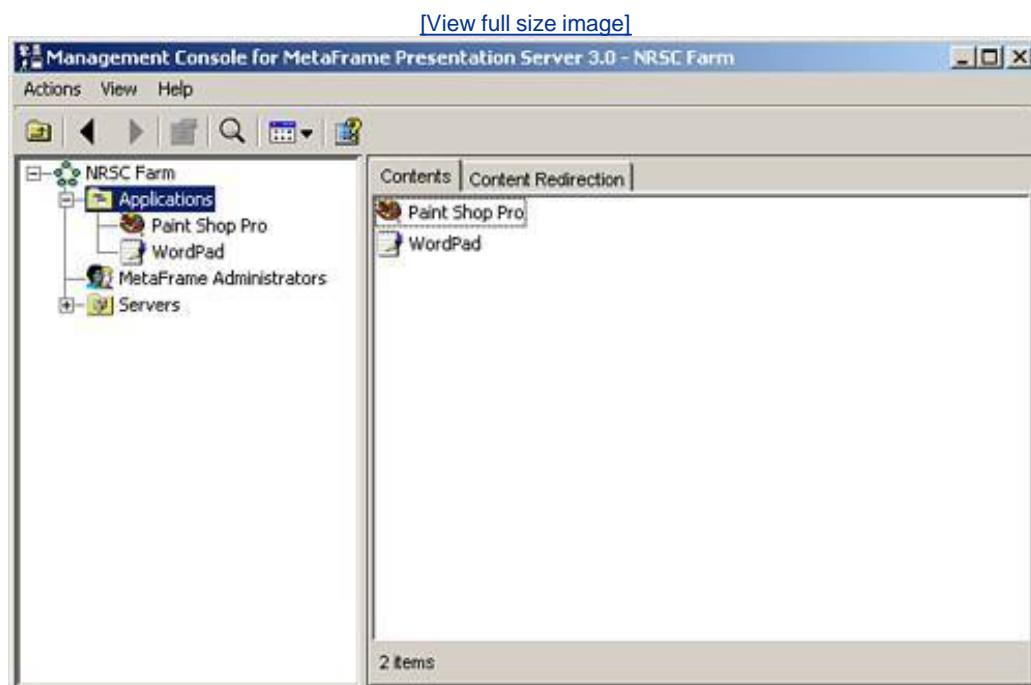
sufficient in small MetaFrame implementations (one server farm zone and a single geographic location), in larger farm deployments, it may be desirable to delegate a subset of the administrative features to different "classes" of administrators.

One common example involves granting help desk staff access to open the Management Console, view published applications, and manage user sessions connected to those applications. This staff can also manage sessions (logoff, shadow, and so on) through the Servers folder. No other Management Console features are available to the user.

Delegating this limited access to manage the environment allows help desk representatives to troubleshoot and resolve typical first-level support issues without an administrator having to worry that they may modify other configuration settings on the server.

Figure 9.2 illustrates the limited view within the Management Console that would be available to a help desk representative in this example. This help desk representative does not even see the nodes to which he or she has not been granted access.

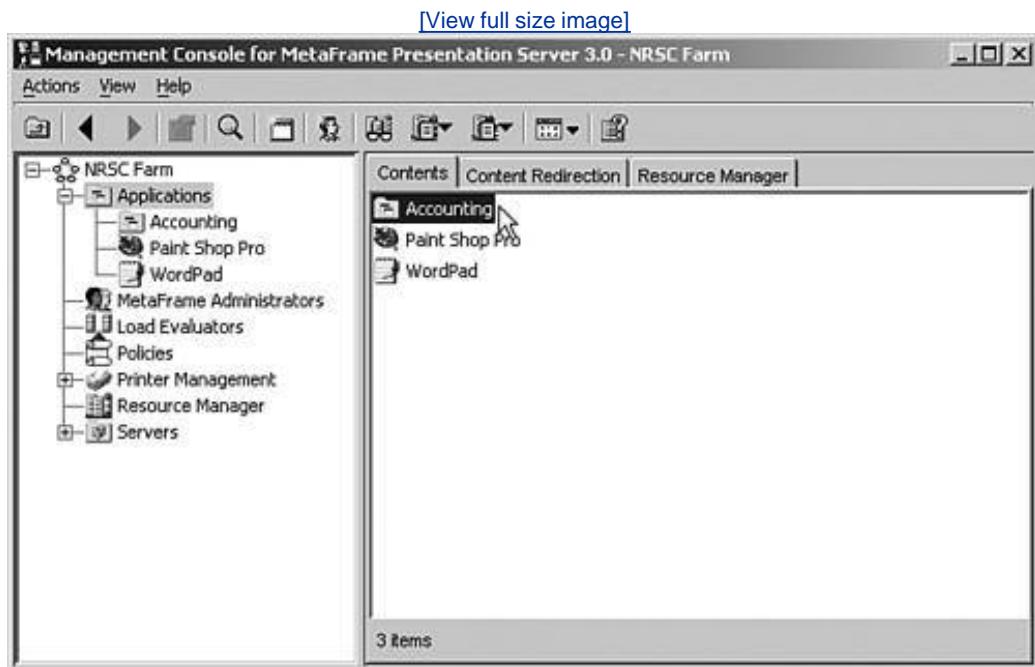
Figure 9.2. Through delegation, you can limit what portions of the Management Console are available to the user.



Through the creation of subfolders under Applications or Servers, you can further subdivide the delegation of authority. In the example given here, you may have certain applications that contain sensitive information (accounting or payroll, for example) that you do not want the help desk directly supporting. Instead, you may have a special subset of administrators who are authorized to manage only the accounting applications or maybe an accounting-specific server. By creating subfolders and placing the appropriate applications/servers into those folders, you can then delegate access to the folder just as you would the root Applications or Servers folder. Figure 9.3 shows an example of a subfolder called Accounting defined under Applications. When this subfolder is first created, you have the option of automatically copying the permissions from the parent folder. If users are not assigned permissions to view this folder, they will not even see it appear when they query the contents of the

Applications folder.

Figure 9.3. Subfolders are used to assign more granular control to applications or servers when necessary.



## Note

Access delegated to a management node (MetaFrame Administrators, Installation Manager, Load Evaluators, Policies, Printer Management, Resource Manager) applies farm-wide, while permissions set on either the Applications or Servers folder (and all subfolders) apply only to the corresponding objects within the folder. The following "Creating and Delegating Administrators" section provides examples on how this is done.

## Creating and Delegating MetaFrame Administrators

All MetaFrame administrative delegation is done through the Management Console. After you have logged in to the Management Console as an administrator with full authority, you can add and configure additional users who will be able to access and manage the server farm.

Administrators are easily added to the system either by right-clicking the MetaFrame Administrators node or selecting the Action menu and choosing Add MetaFrame Administrator.

## Alert

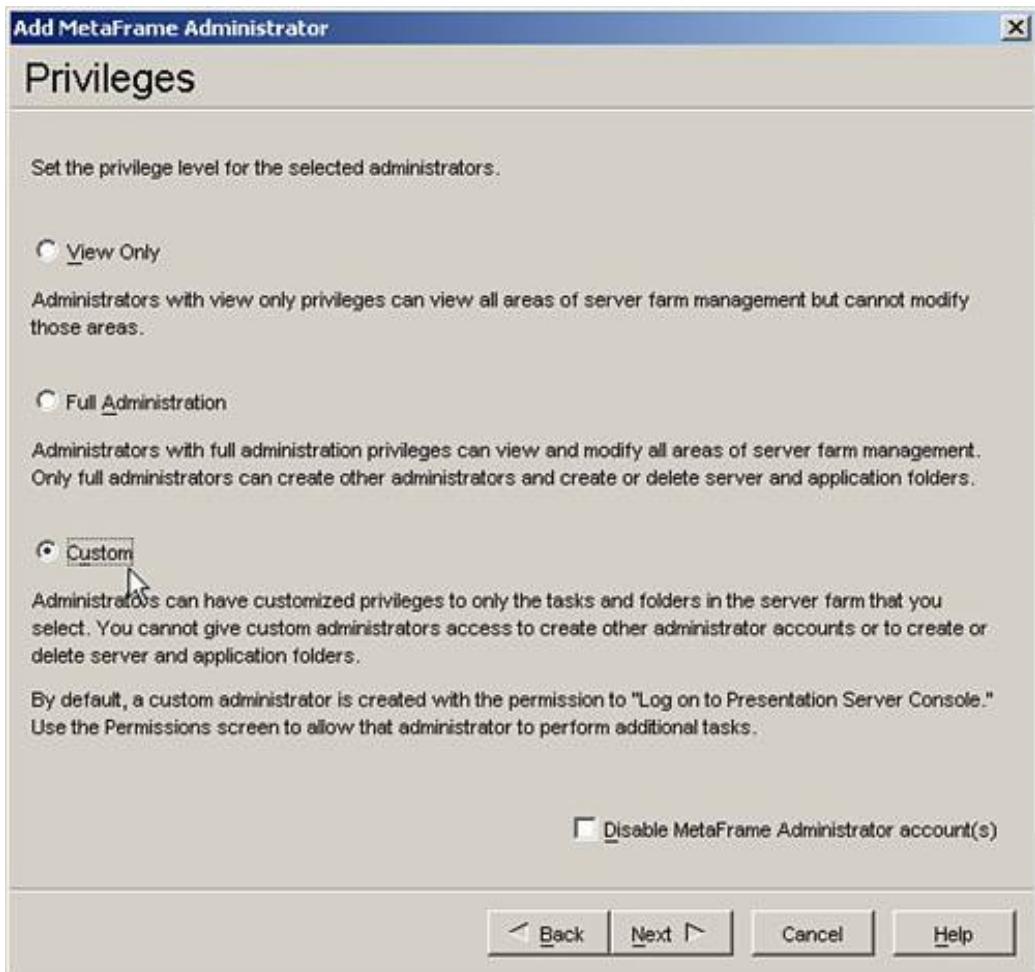
Only those administrators granted full administrative authority are able to add, modify, or delete other administrator accounts in the farm. You cannot delegate these privileges as a subset of full authority.

You are then presented with the Add MetaFrame Administrator Wizard, which guides you through the steps of configuring the new administrator accounts. The basic steps for delegating administrative privileges in the farm are as follows:

1. Choose the desired users and/or groups, either from the local server or from the domain. Citrix recommends adding your network administrators group to ensure continuity in managing resources in the network. We recommend that you provide read access to all the network administrators and limit full farm control to only those administrators authorized to actually manage the farm.
2. You're prompted to provide alert contact details. When granted the Receive Alerts from Servers privilege, the Resource Manager uses this information to send administrative alerts. It is recommended that the necessary alert information be configured in the Resource Manager before you configure these options. Settings such as the desired SMS Gateway will not be accessible until they have been set up. Details on configuring these alerts are covered in [Chapter 15](#), "Managing and Monitoring Using Resource Manager."
3. You're required to delegate the desired privileges to these new administrators. [Figure 9.4](#) shows the three categories of privilege types available:
  - View Only This category provides read-only access to all areas of the system. This privilege may be assigned to those administrators responsible for end-user or operations support who would need to be able to view aspects of the farm but are not authorized to make any changes.
  - Full Administration The second category grants complete access to view and modify all areas of the farm configuration. A very limited number of users should ever have this full access.
  - Custom When this selection is chosen, you can define specific privileges for the different nodes in the Management Console.

**Figure 9.4.** Administrative privileges fall into one of three categories: View Only, Full Administration, and Custom.

[\[View full size image\]](#)



Note the final option on this screen, the Disable MetaFrame Administrator Account(s) check box. When you select this option, the associated accounts are completely disabled from having administrative access to the farm. This option exists so that access can be temporarily disabled without losing the settings. You reinstate access simply by deselecting the check box.

4. If you've chosen View Only or Full Administration, simply click Finish to complete. If you chose Custom, click Next to define the specific privileges within each node of the Management Console (see [Figure 9.5](#)). Details on the options available are discussed in the next section. After you have selected the desired options, click Finish to create the account.

Figure 9.5. You define the desired privileges within the different nodes of the Management Console.

[\[View full size image\]](#)



## MetaFrame Administrative Privileges

Table 9.1 summarizes the privileges that can currently be configured when the Custom privilege configuration is chosen. In preparation for the exam, you should be able to identify the privileges that exist and understand how they affect the portions of the Management Console that are accessible to the administrator. Many of the permissions are self-explanatory from the description, so we don't go into too much detail here on stating exactly what they manage unless you should be aware of something of particular importance.

Table 9.1. Privileges Available in the Custom Privilege Configuration Option

Management Console Node Permissions Comments	Permissions	Comments
Applications	<p>Published Applications</p> <ul style="list-style-type: none"> <li>• Publish Applications and Edit Properties</li> <li>• View Published Applications and Content</li> </ul>	When these permissions are applied to a subfolder, they affect only the applications in that folder.
	<p>Resource Manager</p> <ul style="list-style-type: none"> <li>• Create RM Applications and Edit Properties</li> <li>• Receive Application Alerts</li> <li>• View RM Applications and Content Sessions</li> <li>• Connect Sessions</li> <li>• Disconnect Users</li> <li>• Log Off Users</li> <li>• Reset Sessions</li> <li>• Send Messages</li> <li>• View Session Management</li> </ul>	All aspects of session management for an application can be controlled from the Sessions permissions, with the exception of shadowing and process termination capabilities. To enable shadowing access, you need to create a user policy and assign the desired shadowing permissions. User policies were discussed in <a href="#">Chapter 7</a> , "MetaFrame Presentation Server Policy Management."
		Notice that the one session privilege (process termination) is not listed here. This option is managed as a server privilege and is discussed in the Servers node of this table.
MetaFrame Administrators	<ul style="list-style-type: none"> <li>• Log on to Presentation Server Console</li> <li>• View MetaFrame Administrators</li> </ul>	The logon privilege is the only one enabled by default when a new administrator is created and assigned custom privileges.
		Unless the View MetaFrame Administrators permission is checked, a user sees only his or her account listed in the MetaFrame Administrators node.

Management Console Node Permissions Comments	Permissions	Comments
Installation Manager	<ul style="list-style-type: none"> <li>• Edit Installation Manager</li> <li>• View Installation Manager</li> </ul>	
Load Evaluators	<ul style="list-style-type: none"> <li>• Assign Load Evaluators</li> <li>• Edit Load Evaluators</li> <li>• View Load Evaluators</li> </ul>	
Policies	<ul style="list-style-type: none"> <li>• Edit User Policies</li> <li>• View User Policies</li> </ul>	
Printer Management	<ul style="list-style-type: none"> <li>• Edit All Other Printer Settings</li> <li>• Edit Printer Drivers</li> <li>• Edit Printers</li> <li>• Replicate Printer Drivers</li> <li>• View Printers and Printer Drivers</li> </ul>	
Resource Management	<ul style="list-style-type: none"> <li>• Configure Resource Management</li> <li>• Generate Billing Reports</li> <li>• Generate Current and Summary Reports</li> <li>• Receive Summary Database Alerts</li> <li>• View Resource Management Configuration</li> </ul>	
Servers	Installation Manager	As with Applications, permissions for

Management Console Node Permissions Comments	Permissions	Comments
	<ul style="list-style-type: none"> <li>• Install and Uninstall Packages Published Applications</li> <li>• Assign Applications to Servers Resource Manager</li> <li>• Assign RM Applications to Servers</li> <li>• Edit RM Information</li> <li>• Receive Alerts from Servers</li> <li>• View RM Information Servers</li> <li>• Edit License Server Settings</li> <li>• Edit Other Server Settings</li> <li>• Edit SNMP Settings</li> <li>• Move and Remove Servers</li> <li>• Terminate Processes</li> <li>• View Server Information Sessions</li> <li>• Connect Sessions</li> <li>• Disconnect Users</li> <li>• Log Off Users</li> <li>• Reset Sessions</li> <li>• Send Messages</li> <li>• View Session Management</li> </ul>	the Servers node can be applied to the root or to subfolders and affect only those servers located within that folder.

## Note

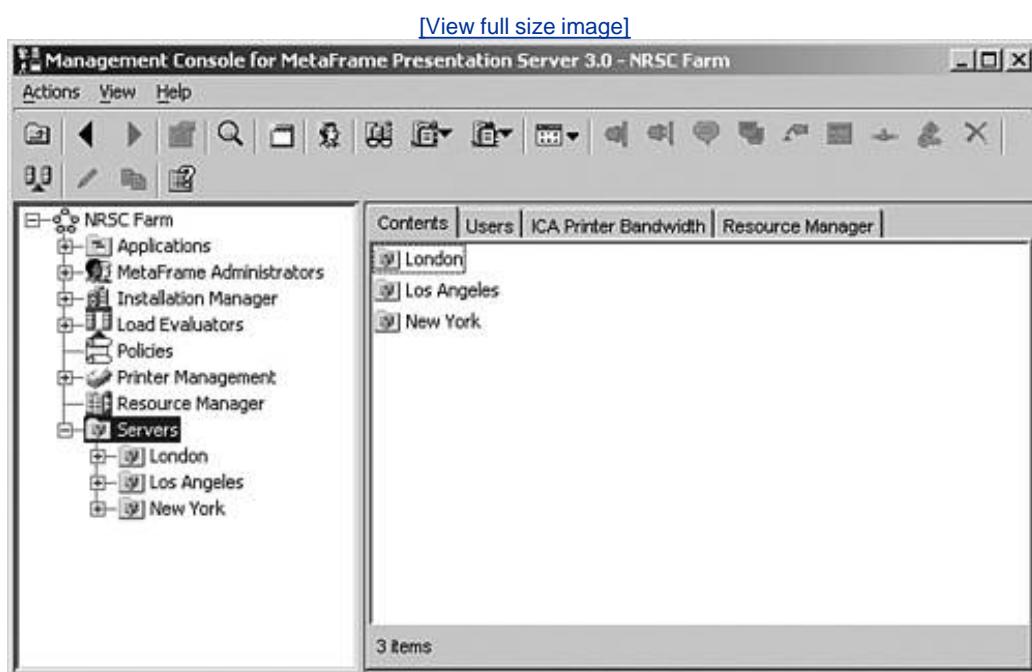
If you want to assign permissions to subfolders of the Applications or Servers nodes, you need to create the desired folders before you assign permissions. Folders cannot be created while creating new (or modifying existing) administrative delegations.

You create subfolders by highlighting Applications or Servers and then choosing New Folder from the Actions menu or right-clicking and choosing New Folder from the context menu.

## Zone-Based Administrative Delegation

We mentioned earlier that administrative privileges could also be delegated based on the location or zone breakdown of the MetaFrame servers in the farm. The actual mechanism for doing this is not automatically controlled by the existing zones in your farm, but is managed by creating corresponding server groups and allocating servers in such a way that it mirrors the zone (or geographical) layout of the farm. [Figure 9.6](#) demonstrates this by showing three subfolders under the Servers node labeled New York, Los Angeles, and London. Within these subfolders are the MetaFrame servers that are physically divided into these locations.

Figure 9.6. Leveraging the support of subfolders for the Servers node, you can mirror your zone layout in the server farm and delegate access to different groups of administrators for each zone.



From this, you can then assign different administrative privileges based on the requirements of the servers in each location. As you can see, this manual process must be undertaken to correspond to the layout of the servers. Currently, this support is not automatically kept in sync with the zone breakdown in the server farm. If you move servers or create a new zone, you have to *manually* update the subfolders to reflect these changes.

## Modifying Existing Delegations

Existing MetaFrame administrators can have their privileges modified at any time. You do so simply by modifying the properties for the administrator in the MetaFrame Administrators node. The three dialog boxes that appeared when the administrator was first created are all accessible and can be modified from within the properties of an administrator.

If the administrator currently has the Management Console open, he or she is presented with a message stating that permissions have been modified and that he or she must log in again to the Management Console. The administrator is immediately logged out of his or her current Management Console session.

The option to disable the administrator account can be quickly enabled or disabled by right-clicking the name and choosing the one that is currently active. If the account is currently enabled, the disable option is available and vice versa.

If an existing administrator is deleted, the settings are lost. If the administrator to be deleted is the last one in the farm with full authority, MetaFrame does not allow you to delete the account.

### Note

You can also modify the permissions for a node or folder at any time from within the Management Console simply by right-clicking the item and selecting Permissions from the context menu.

## Managing Access to External Citrix MetaFrame Tools

One important note is that the delegation of permissions within the Management Console affects management of the farm through the console only. It does not enable or disable access or execution of other external Citrix MetaFrame tools such as the Citrix Connection Configuration tool or the command-line tools used for managing MetaFrame sessions.

For example, even though an administrator may have been granted access to disconnect user sessions through the Management Console, unless that administrator has similar access at the connection level, he or she cannot use the command-line tool **TSDISCON** to disconnect active sessions. Attempting to do so results in an access-denied message. The same error would be generated if the user attempted to disconnect sessions using the Terminal Services Management GUI (**TSADMIN.EXE**).

Understanding the scope of delegated permissions is an important part of effectively managing the environment. Security best practices recommend that access to external tools be controlled through local or domain security groups and that permissions defined at the connection level be restricted. This ensures that external tools cannot be used to modify or manage the environment outside the Management Console.

Configuration and administrative techniques were discussed in [Chapter 6](#), "Configuring and Administering MetaFrame Presentation Servers."

 PREV

NEXT 

## MetaFrame Access Security

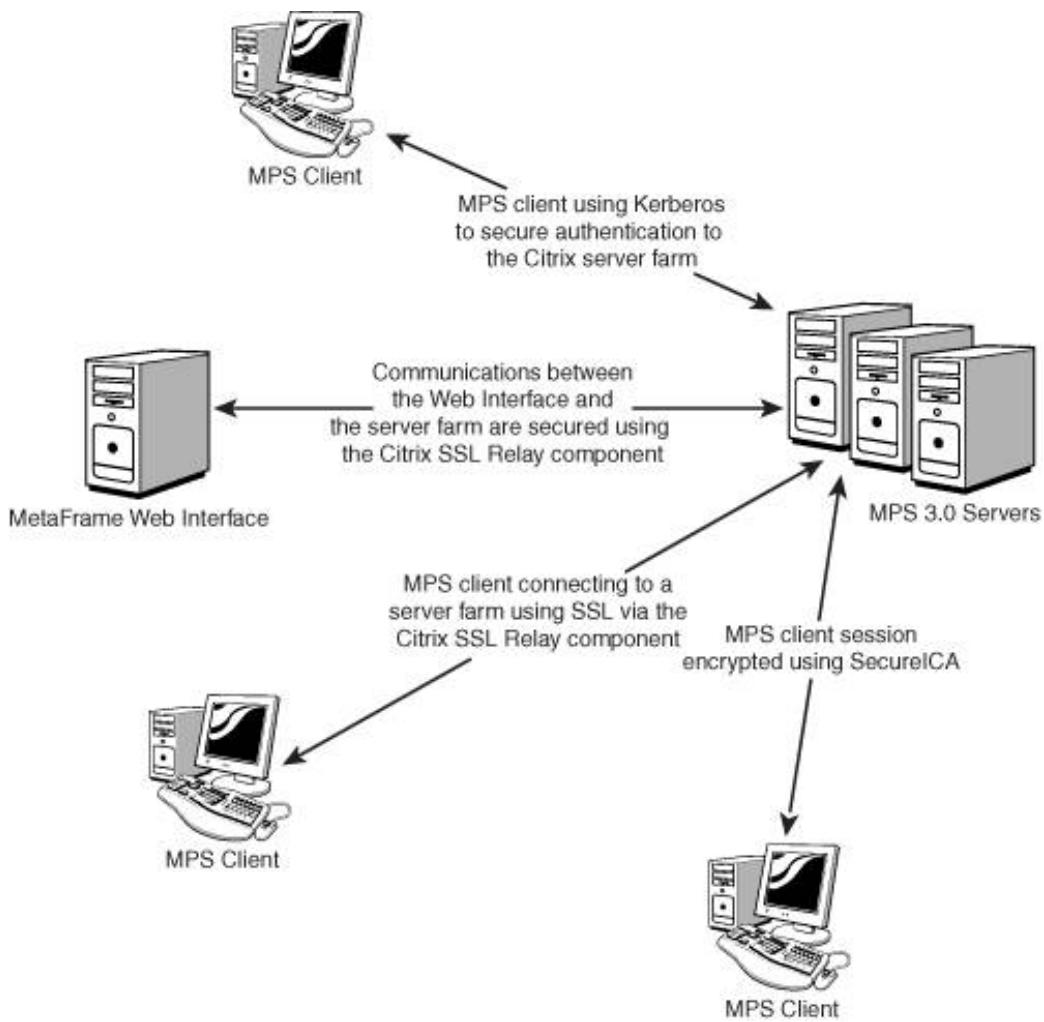
We are now going to focus on the three security components available as part of the core MetaFrame product. Although each is functionally unique, they all are used to achieve the common goal of securing connectivity to the MetaFrame server. The three security components are

- ICA Connection Encryption Also known as SecureICA, ICA encryption is used to secure the communications between a MetaFrame Presentation Server and an MPS client.
- Kerberos Client Authentication When version 8.x of the Win32 MPS client is employed, you can use Kerberos authentication to strengthen the authentication security from the Win32 client to an MPS 3.0 server farm. Kerberos client authentication is supported only in a Windows 2000 or Windows 2003 domain.
- SSL Relay The Citrix SSL Relay component allows you to secure communications between MPS clients and/or the Web Interface to MetaFrame servers using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

[Figure 9.7](#) shows the layout of a simple MPS environment and where these three security components fit into the structure of the environment.

Figure 9.7. The three security components provide the ability to secure different areas of the MetaFrame environment.

[\[View full size image\]](#)



## ICA Connection Encryption

All MPS clients, with the exception of the minimal web client, provide support for encrypting the communications between the client and the MetaFrame server. ICA connection encryption, also known as Citrix SecureICA, supports five encryption configurations:

- Basic encryption Citrix's basic encryption employs a simple encryption algorithm using an encryption key of fewer than 40 bits. This is not considered a secure encryption setting.
- 128-bit encryption for logon only A 128-bit encryption key is used for the authentication process only, leaving the remainder of the session data to transmit with only Basic encryption.
- 40-, 56-, and 128-bit encryption Regardless of the choice made, 128-bit encryption is used during authentication; then the actual session data is transmitted at the selected encryption level.

### Note

All encryption configurations higher than Basic employ the RSA RC5 encryption algorithm.

RC5 is known as a fast block cipher, which takes a fixed-length block of data and transforms it into an encrypted block of data that is the same size. The data block is encrypted and decrypted using the same secret key. This type of secret key sharing is known as *symmetric-key encryption*. Specifically, ICA encryption employs a 64-bit block size; 12 rounds of encryption (the encrypted data is passed through and encrypted again 12 consecutive times); and a secret key 40, 56, or 128 bits in size.

The sharing of this common secret key is carried out using the Diffie-Hellman key agreement algorithm. The Diffie-Hellman algorithm describes a way for the client and the server to exchange key information in a secure fashion over an insecure data link. The algorithm is known as a public-private key algorithm because users exchange a well-known public key from which they can derive the common, shared secret key.

Details on the specific steps involved in sharing the private key can be found in the "Citrix SecureICA Services Administrator's Guide," a slightly dated document from Citrix that still includes relevant information on the ICA encryption process.

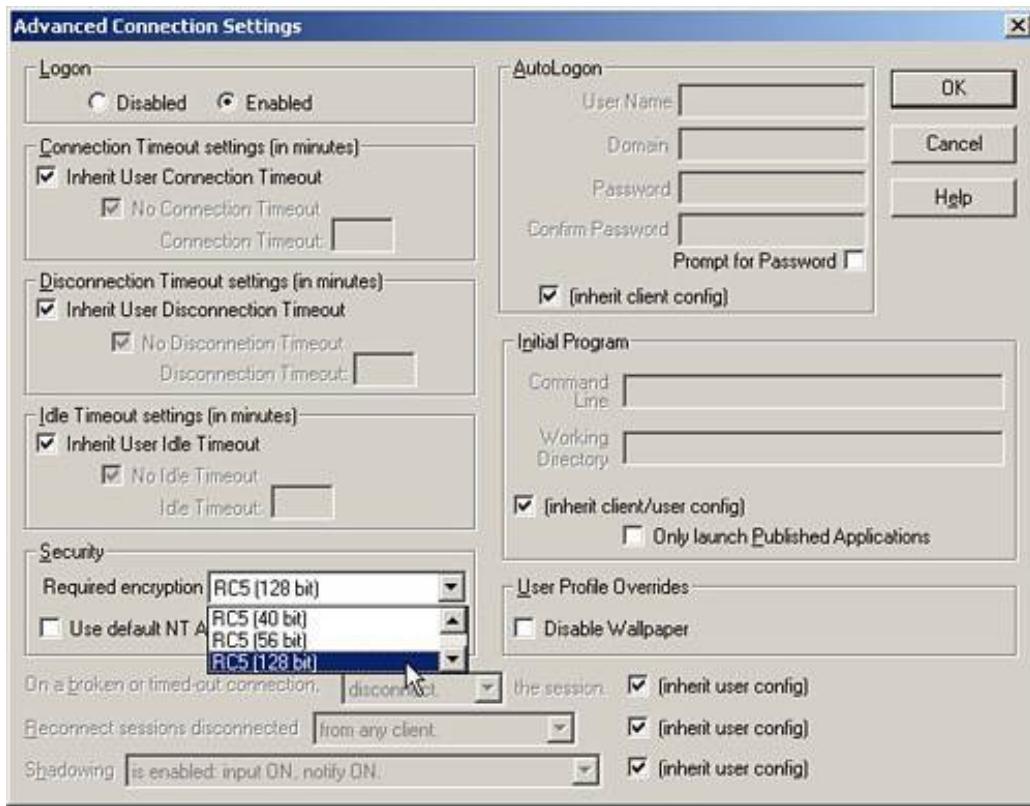
ICA connection encryption has configurable settings on both the client and server. On the client side, the desired encryption settings for the session are defined *prior* to establishing the connection to the MetaFrame server. For example, when defining the properties for a connection within the ICA Client for Linux, you specify the level of encryption that you want to establish when connecting to the MetaFrame server.

When the client connects to a MetaFrame server, it attempts to negotiate the use of this encryption level for the session. Three factors may prevent this encryption level from being employed, and consequently, the user being denied access to log on to the MetaFrame server:

- The first factor is the minimum required encryption level that has been defined for ICA connections on the server. The minimum required encryption level is configured from within the Citrix Connection Configuration tool. Within the Advanced Connection Settings window, you define the minimum required encryption level (see [Figure 9.8](#)). The default level is Basic, allowing a client to connect to the server with the desired encryption set to Basic or higher.

Figure 9.8. The Required Encryption setting dictates the minimum encryption level that must be defined for the MPS client.

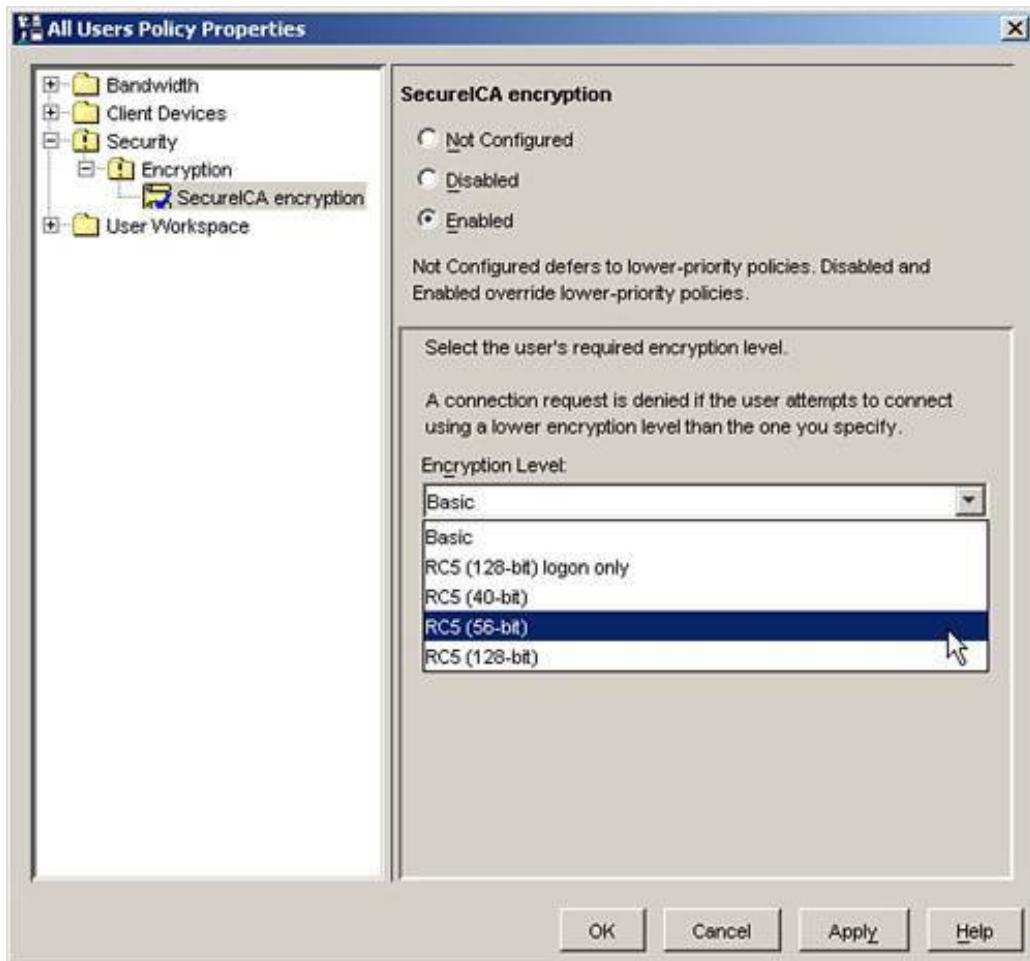
[\[View full size image\]](#)



- The second factor is whether a MetaFrame user policy has been defined to enforce a minimum encryption level for the user (see [Figure 9.9](#)).

Figure 9.9. The required encryption setting can also be managed through user policies.

[\[View full size image\]](#)



- If the client is connecting to a published application, the final factor is whether a minimum encryption level has been defined for the published application itself. One of the properties within a published application is the encryption level that will be enforced.

When a minimum encryption requirement has been defined (either in the connection settings, a policy, or a published application's properties), only the clients with their encryption level configured to meet or exceed this requirement can log on to the MetaFrame server. Anyone with lower encryption settings receives an error message stating "You do not have the proper encryption level to access this session."

## Note

When encryption settings have been defined in multiple locations, the most restrictive encryption requirement always takes precedence.

For example, if the required encryption level is set to RC5(56 bit), only those clients configured with 56-bit or 128-bit encryption are able to log on. All clients with lower encryption settings are rejected, and the user is unable to log on to the server until his or her setting has been adjusted accordingly.

## Limitations of ICA Encryption

Although ICA encryption does help to protect client/server communications, Citrix does *not* recommend that this be the sole means of securing access to a MetaFrame server across a public network, such as the Internet. A lack of client/server authentication does make ICA encryption, and the ICA protocol itself, theoretically susceptible to a man-in-the-middle attack.

Basically, in a man-in-the-middle attack, someone intercepts transmission between two sources, views and even modifies the information before it is passed on to the intended target. Without an authentication mechanism, the ICA protocol is unable to validate whether the encrypted transmission actually did originate from the source that it said it did.

ICA encryption is most often employed within a corporate network (LAN or WAN), where the threat of such attacks is typically low.

## Kerberos Client Authentication

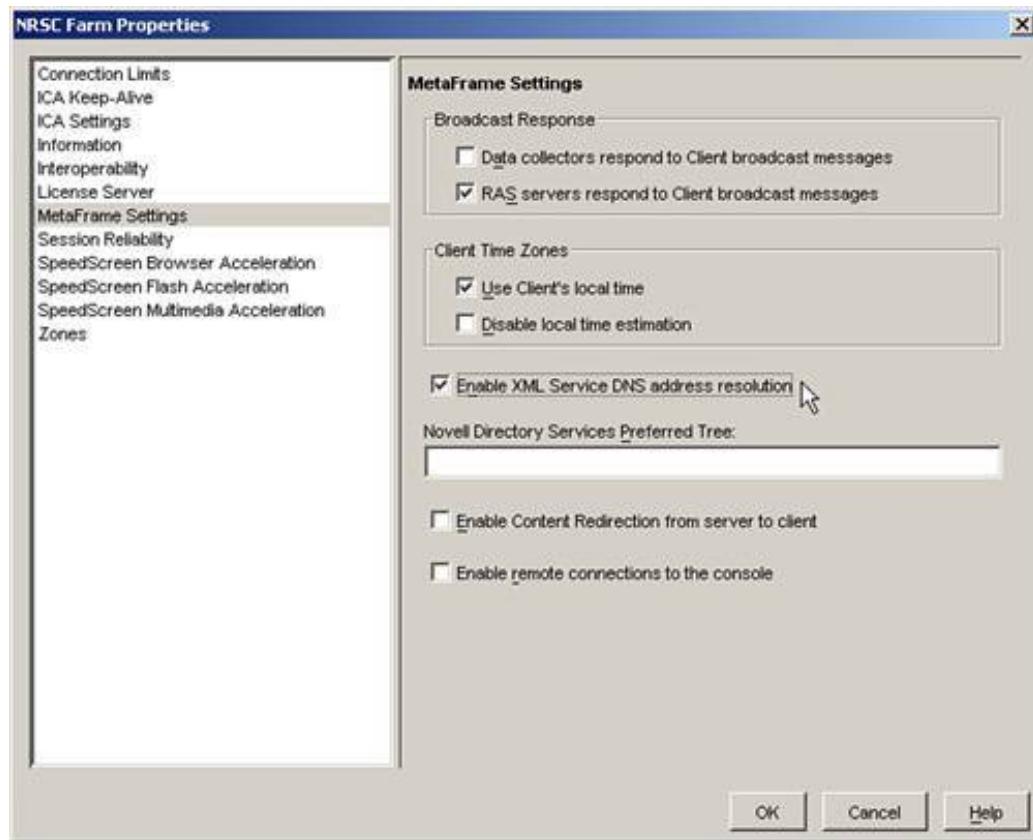
Version 8.x of the Win32 MPS client supports the use of Kerberos authentication as an alternative to sending the user's password across the network. Kerberos is an industry-standard network authentication system that allows machines communicating over networks to prove their identity to each other. Kerberos is an effective method of protecting against eavesdropping and attacks based on the replay of captured network traffic. Kerberos helps to ensure that authentication information travels safely and securely between the client and the MetaFrame server.

Kerberos is an integrated component of Windows Server 2003 and Windows 2000 Server and as such is supported only in a Windows 2000 or 2003 domain. Support for Kerberos client authentication is a new feature of MetaFrame Presentation Server 3.0 and leverages the Security Support Provider Interface (SSPI) in Windows Server. To use Kerberos client authentication, you must ensure the following in the MetaFrame server farm:

- The MetaFrame servers and the MPS clients must belong to the same or trusted Windows 2000 or 2003 domains.
- The MetaFrame servers must be configured to Trusted for Delegation. You set this by selecting the properties of the server through the Active Directory Users and Computers MMC snap-in.
- The use of SSPI within MetaFrame requires that the setting Enable XML Service DNS Address Resolution be enabled in the server farm. This setting is located under MetaFrame Settings in the server farm's properties (see [Figure 9.10](#)).

Figure 9.10. The DNS address resolution setting allows the server to return the fully qualified name to ICA clients, a requirement for Kerberos authentication.

[\[View full size image\]](#)



MetaFrame supports the use of Kerberos authentication with or without pass-through authentication. The difference is that if Kerberos authentication fails, either the user is prompted to provide logon credentials or the local user account is used to attempt pass-through authentication to the MetaFrame server. Kerberos authentication without pass-through authentication is considered more secure.

The use of Kerberos without pass-through authentication is supported only with Custom ICA Connections or through the Web Interface for MPS. When you are using Application sets in Program Neighborhood or the Program Neighborhood Agent, if you want to use Kerberos, you must use Kerberos with pass-through authentication.

After the server-side components have been properly configured, the client side must be configured to utilize Kerberos authentication. For new client deployments, you can create a custom installation package configured to employ Kerberos authentication; otherwise, you can modify the `Wfclient.ini` file on each of the client devices.

The configuration of the MPS client, including enabling Kerberos authentication, is discussed in [Chapter 13](#), "Citrix ICA Session and Client Configuration."

## Citrix SSL Relay

Citrix SSL Relay supports full encryption of the data stream between the MPS client (or the Web Interface) and the MetaFrame Presentation Server.

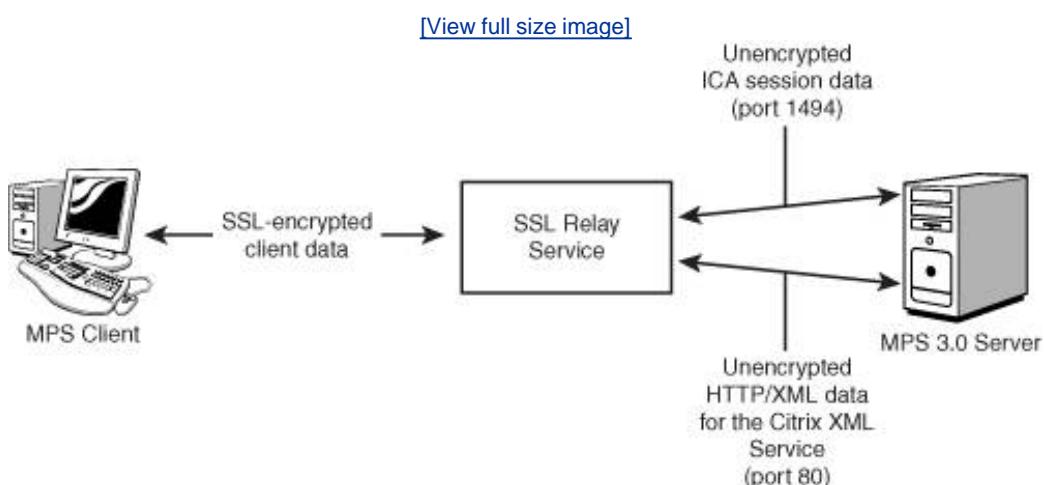
### Note

In this chapter, we focus on the use of SSL Relay to secure communications between the

MPS client and the MetaFrame server. The use of SSL Relay and the Web Interface is discussed in [Chapter 14](#).

[Figure 9.11](#) illustrates how Citrix SSL Relay would fit into a typical MPS environment. Instead of the client contacting a MetaFrame server directly to retrieve server farm information or establish a MetaFrame session, when SSL Relay is employed, the client encrypts the data and transmits it to a server running the SSL Relay, which in turn decrypts the data and forwards it onto the appropriate resource (MetaFrame session connection or Citrix XML data request). Data transmitted back from the server is also directed through the SSL Relay, where it is also encrypted before being sent to the client.

Figure 9.11. SSL Relay encrypts the traffic between a client and the MetaFrame server using the industry-standard SSL/TLS protocol. When the data reaches the SSL Relay service, it is decrypted and sent onto either port 1494 if it is session data or onto port 80 (Citrix XML Service) if it is server location information.



Because the communications are secured using SSL/TLS, not only is the information encrypted, but message integrity checks exist that verify the data transmitted to ensure it has not been tampered with. SSL Relay ensures both identity verification and data integrity, something that ICA Connection Encryption alone cannot do.

## Citrix SSL Relay Client Requirements

The general client requirements for implementing SSL Relay are as follows:

- The client device must support 128-bit encryption. Most clients now support this encryption level in regards to SSL/TLS connections. You can verify this by examining the Help, About setting for Internet Explorer and verifying that Cipher Strength is 128 bit.
- The client device needs to have the appropriate root certificate installed so that it can verify the certificate authority that issued the certificate for the server. To be able to properly validate and

secure the communications, all MetaFrame servers running the SSL Relay service must have a valid server certificate installed. When a client connects, it must be able to verify the authenticity of the certificate. Having the necessary root certificate available ensures this is the case.

- The client must be configured so that it is aware of the SSL port used by the SSL Relay service in the farm. It is normally port 443, but this is configurable and can be changed if necessary to avoid conflicts with other software.

Full details on configuring the MPS client are discussed in [Chapter 13](#).

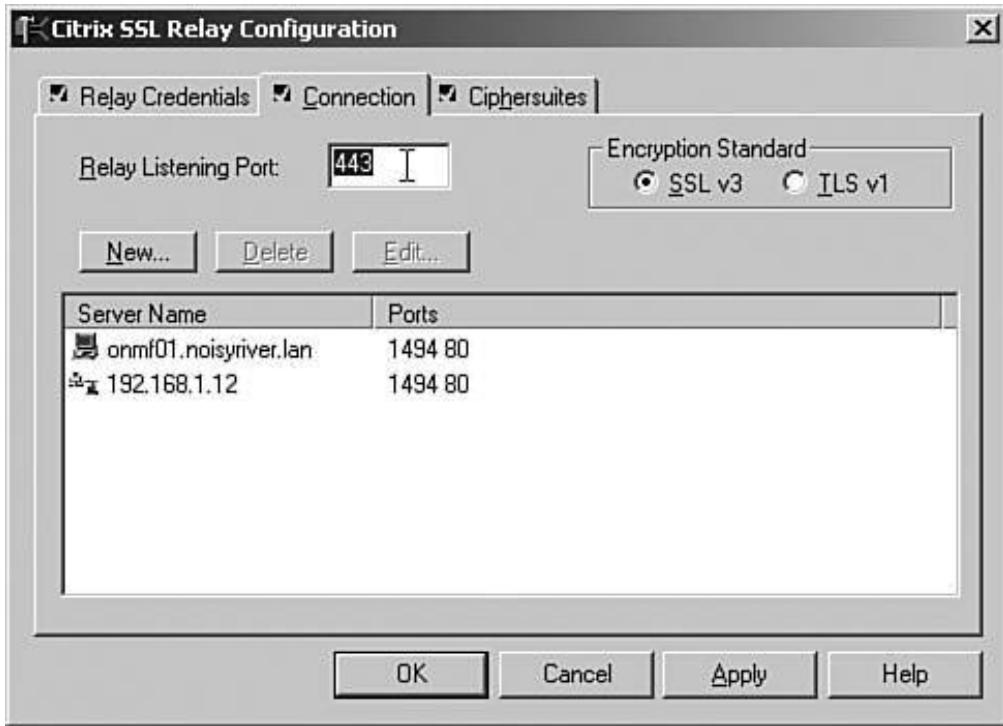
## Citrix SSL Relay Server Requirements

To utilize SSL Relay, you must configure the service on at least one MetaFrame server within your server farm. You can configure the SSL Relay service by completing the following four steps:

1. Obtain a server certificate for each server that will run the SSL Relay service. This certificate must be issued by a trusted certificate authority (CA) and is used to electronically prove that the server is actually who it says it is. The root certificate for this CA must be available on each MPS client that will connect so that it is able to verify the authenticity of the server certificate.
2. Install the corresponding certificate on each server. You install certificates on the MetaFrame server using either the Certificate MMC snap-in or the Web Server Certificate Wizard if IIS is also installed on the MetaFrame server.
3. If Microsoft Internet Information Services (IIS) is running on the MetaFrame server, you must modify either the IIS server or the SSL Relay port so that they do not conflict. You can easily modify the IIS SSL port by assigning an alternate port within the properties of a website.

To redirect the SSL Relay port, you use the SSL Relay Configuration tool. Under the Connection tab, you can find the field to modify the relay listening port (see [Figure 9.12](#)).

**Figure 9.12.** You can easily modify the SSL Relay listening port, if necessary, from within the SSL Relay Configuration tool.



## Note

Modifying the listening port requires you to adjust the default port setting on the MPS client. This topic is discussed in [Chapter 13](#).

4. From within the SSL Relay configuration utility, you need to select the server certificate to use and the available ciphersuites. After you configure these settings, the SSL Relay is ready to accept and process connection requests from MPS clients configured to use SSL/TLS.

## Obtaining Root and Server Certificates for a MetaFrame Server

For a server running SSL Relay to be able to prove that it actually is who it says it is, it must have a server certificate, issued by a trusted authority, that it can present to clients when requested, allowing for the initiation of the secure connection between the SSL Relay service and the client. Without such a certificate, the validity of the connection would be in question.

Server certificates are issued by a trusted entity, known as a certificate authority (CA). A request for a server certificate is sent to a CA, which in turn performs due diligence to ensure that the requester is actually who he or she says. After the identity is proven, the CA issues a digital certificate containing information that verifies the identity of the server.

How you choose the CA from which to receive your certificates can depend on a number of factors. Large companies can configure their own internal CA and issue certificates for their servers, or they can look to a well-known third-party CA and purchase the necessary server certificates.

In conjunction with the server certificate issued by the CA, you also require the root certificate from that CA deployed to all connecting clients so that these clients are able to verify the authenticity of the server certificate. By comparing the information in the root certificate with the data in the server certificate, the client can electronically verify the signature in the certificate. Assuming that the client

trusts the root certificate, it can trust the information in the server certificate to be accurate.

Many operating systems come with root certificates available from the most common commercial CAs. The MetaFrame Web Interface and the MPS clients come with integrated support for two of the most common CAs, which are VeriSign Inc. (<http://www.verisign.com>) and Baltimore Technologies (<http://www.baltimore.com>). If your organization has acquired server certificates from either of these vendors, there is no need to manually deploy the corresponding root certificate. It is already available on the client.

When requesting a certificate, you generate what is known as a *certificate signing request (CSR)*, which is then sent to the CA, and in return you receive a digitally signed server certificate for use. A common way to generate a CSR is through the Microsoft Web Server Certificate Wizard, a component of IIS. Using this tool, you provide the necessary information, which is then stored in a file that is sent to a CA for signing. The following steps summarize how to generate a CSR using the IIS Web Server Certificate Wizard:

1. Start the IIS Manager from under Administrative Tools.
2. Expand the Web Sites folder, right-click the Default Web Site entry, and select Properties.
3. Select the Directory Security tab, and then click on the Server Certificate button. This launches the Web Server Certificate Wizard.
4. When prompted, select Create a New Certificate and continue through the wizard.
5. When you see the question "Prepare the request now or send it later," choose Send It Later and click Next.
6. You are prompted to provide a friendly name for the certificate. This can be any name you desire, but it is recommended that the name match the server name for which it is being created. On the same screen, you enter the desired bit length. The larger the bit length, the greater the security but the greater performance hit incurred to manage the key. Citrix recommends 1,024 bits or higher. If you choose a higher bit length, you need to ensure that the client supports this length. Do not select the Cryptographic Service Provider (CSP) check box.
7. Provide the requested organizational information. This should distinguish this certificate from other organizations.
8. Correctly entering the common name for the certificate is vital to ensuring the certificate properly represents the MetaFrame server. For SSL Relay to function properly, make sure you enter the fully qualified domain name for example, **onmf01.noisyriver.com**, as in [Figure 9.13](#).

**Figure 9.13.** Fully qualifying the MetaFrame server name is vital to ensuring the certificate properly identifies the MetaFrame server running SSL Relay.



9. Provide the requested geographical information.
10. The next screen prompts you to provide a name for the resulting request file. Viewing this file after it has been created will reveal what looks like meaningless letters and numbers. This information is provided to the CA when requesting the certificate.
11. The final two screens provide summary information and complete the Web Server Certificate Wizard.

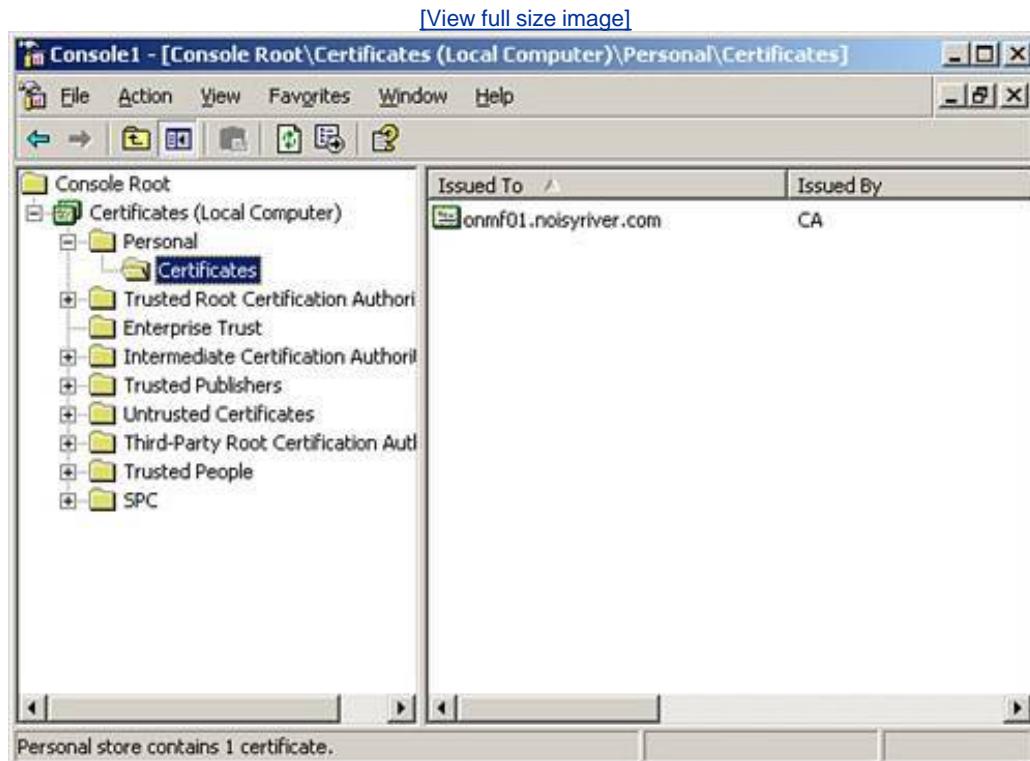
## Installing a Server Certificate

After a certificate request has been approved by the CA, you will receive the digital certificate for the server along with a password that will be used when installing the certificate on the MetaFrame server. If you have IIS installed on the MetaFrame server, you can restart the IIS Web Server Certificate Wizard and complete the installation of the retrieved certificate. When using this wizard on a MetaFrame server, make certain that you select an alternate port for SSL instead of 443; otherwise, you will have to redirect the SSL Relay service to an alternate port. Port redirection is discussed in the next section.

If you are not running IIS on your MetaFrame server, you can add the certificate using the Certificates MMC snap-in as follows:

1. Open the MMC. The easiest way to do this is to type **mmc** at the Run prompt and press Enter.
2. If the Certificates snap-in is not visible, you can add it by selecting Add/Remove Snap-in from the File menu. Click the Add button; then select Certificates from the list of available snap-ins.
3. When prompted, choose Computer Account for the location to manage certificates, and then choose Local Computer when prompted. Close out of the Add/Remove dialog box, and return to the main MMC window.
4. Select the Personal folder, and then select Action, All Tasks, Import. This launches the Import Wizard. Browse to the location where the imported certificate file is located.
5. When prompted, provide the password for the import file, and then specify the target location for the certificate. The server certificate should be located under the Personal folder. [Figure 9.14](#) shows the certificate added to a MetaFrame server.

Figure 9.14. After the server certificate has been imported into the MetaFrame server, it will appear in the Certificates folder under the Personal folder of the local computer.



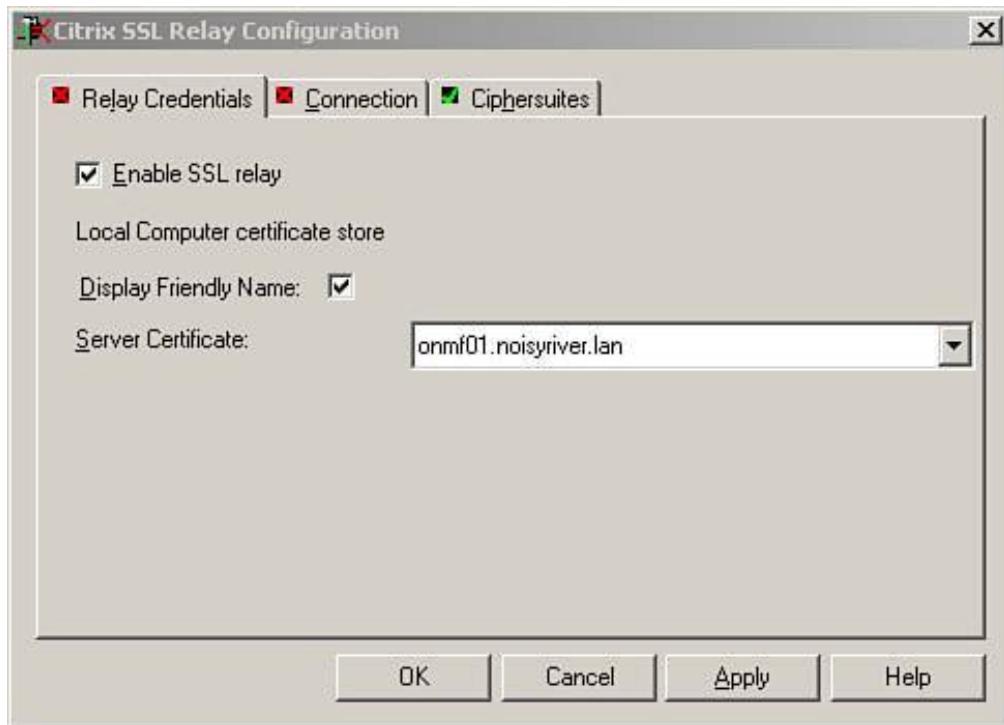
6. The server certificate is now installed and available on the MetaFrame server.

## Configuring the SSL Relay Service

The final step in preparing SSL Relay for use in your MetaFrame environment is to configure the SSL

Relay service. You do this using the SSL Relay Configuration tool. When this tool is opened for the first time, you receive a message stating that the relay configuration data is not complete because data is being loaded for the first time from the system but has not yet been saved for SSL Relay. This includes information on the server certificate, which should automatically appear in the Server Certificate drop-down list box (see [Figure 9.15](#)). This information is automatically pulled from the local certificate store on the server. If there are multiple certificates, make sure you select the correct one.

Figure 9.15. You can change the server certificate using the SSL Relay Configuration tool.



On the Connections tab, you list the address and port combinations for the servers to which the SSL Relay service will direct information. SSL Relay directs information only to the servers listed here. Add any additional servers and ports that you want to include. Make sure to create two entries for the server one being the fully qualified name and the other being the IP address of the server.

The final tab of the SSL Relay Configuration tool is Ciphersuites. Here, you select the ciphersuites available for use in SSL Relay. The COM and GOV entries are both enabled by default, and you typically are not required to change them.

Ensure the Enable SSL Relay setting is checked on the Relay Credentials tab and click OK to save the changes. To enable the SSL Relay, you are now required to reboot the server. After rebooting, you can connect to the server using SSL/TLS encryption.

Steps on configuring and connecting with the MPS client are discussed in [Chapter 13](#).

## Changes from SSL Relay in MetaFrame XP Feature Release 1

SSL Relay in FR2 of MetaFrame XP and later now access server certificates directly out of the Microsoft

server store instead of the file system folder employed in earlier versions. When upgrading from MetaFrame XP FR1 to MPS 3.0, you need to import the certificates stored in the `\keystore\certs` folder into the Microsoft Certificates store. If the files are stored in PFX format, you can directly import them using the Certificates MMC snap-in as discussed earlier. If the files are stored in PEM format, you must run the tool PEMtoPFX to convert these files to a format that can be imported by the Certificates snap-in. After they are imported, these certificates will be available to the new SSL Relay version.

 PREV

NEXT 

## Exam Prep Questions

1. An associate has offered to complete the configuration of a MetaFrame Presentation Server that you have just finished installing. He asks you what user account he should use to log on to the MetaFrame Presentation Server 3.0 Management Console. From the following list, choose the response that best answers your associate's question.

- A. Use the account that was defined during the installation of the last MetaFrame server in your farm.

- B. Use the account that was defined during the installation of the first MetaFrame server in your farm.

- C. Use the local administrator account on the MetaFrame server. This account always has access to log on to the Management Console.

- D. Before you can log on to the Management Console, you must create the local group called MetaFrame Administrators and assign the desired users.

A1: Answer B is correct. When the first MetaFrame server is installed, the data store is also created. At this time, you're prompted to provide the name and domain of a user who will have full authority within the Management Console for MPS. Without knowing this account, you cannot log on to the Management Console.

Answer A is incorrect. After the farm is created, you are never again asked to provide the administrative account during the MetaFrame installation. Answer C is also incorrect. No user or group is automatically assigned access to the Management Console. You must define the desired users who will have access. Answer D is incorrect because the Management Console has no fixed dependency on a local group. You could define such a group if you want, but until you create the group and assign the privileges, it would not allow access to the Management Console.

2. You're going away on a well-deserved vacation and want to delegate limited access to another administrator who will be covering for you while you're gone. Which of the following options could you employ to ensure that she cannot modify the access of other administrators while you're away? (Select all that apply.)

- A. Assign her the View Only privilege type.
  - B. Assign her the Full Administration privilege type and then remove her access to View MetaFrame Administrators.
  - C. Assign her the Custom privilege type and then define all the desired privileges you want her to have.
  - D. Assign her the Custom privilege type but ensure that the Edit MetaFrame Administrators permission has been disabled.
- A2: Both answers A and C ensure that the temporary administrator cannot modify the settings for other administrators. Answer A may be too restrictive, but it would still achieve the desired goal of limiting account access. Answer C satisfies this question simply because assigning anything other than the Full Administration privilege prevents the affected administrator from modifying other admin settings. There is no way to explicitly assign the modify administrator privilege without assigning the user full control.
- Answer B is incorrect because after you have assigned Full Administration privileges, you cannot modify individual user properties. This can be done only through the Custom type.
- Answer D is also incorrect because the permission Edit MetaFrame Administrators does not exist.
3. You have MetaFrame servers from the same farm deployed across three geographically disperse regions: North America, Europe, and Asia. You want to delegate administrative access to users in these different regions. Which of the following solutions would best accomplish what you are trying to do?

- A. Create subfolders under Servers corresponding to each of the regions you want managed. Place the corresponding servers into their correct region folder and then delegate the desired privileges to the administrators corresponding to the appropriate folder.
- 
- B. Create three separate server farms, one for each of the regions, and then delegate authority to the administrators in each farm.
- 
- C. Ensure that each region has a single zone within which all the servers in that region reside. For each zone, check the Enable Per-Zone Security setting. You then can delegate the desired permissions to the users in each zone.
- 
- D. Create subfolders under the MetaFrame Administrators node corresponding to each of the regions you want to manage. Group the administrators into the appropriate folders, and then assign them permissions to the servers that belong to their region.

A3: Answer A is correct. Conceptually, this is identical to the example discussed in which access was delegated based on the different zones in the farm. The concept of subfolders can be a very useful tool for segregating access between different applications or servers.

Answer B, while not technically incorrect, is not necessary to achieve the access delegation desired. Because the servers in the three regions are already in the same farm, it would not be desirable to divide them into different farms for this purpose. It would also mean that they could not all be managed through a single Management Console. You would need to run one for each region.

Answer C is incorrect because there is no such thing as the Enable Per-Zone Security setting. Zones themselves are not an integrated component of administrative delegation.

Answer D is also incorrect. You cannot create subfolders under the MetaFrame Administrators node. Only the Applications and Servers nodes allow you to create subfolders.

4. A client is attempting to connect to a published application in your server farm and keeps receiving an error message that says "You do not have the proper encryption level to access this Session." From the following list of options, which ones are valid reasons for the issue to exist? (Select all that apply.)

- A. The minimum required encryption setting for the published application is set higher than the encryption setting configured on the client.
- B. The minimum required encryption setting for the ICA connection is set higher than the encryption level configured on the client.
- C. A MetaFrame user policy applies to this client, and the minimum required encryption level is higher than the encryption level configured on the client.
- D. The minimum required encryption setting for the server farm is set higher than the encryption level configured on the client.

A4: Answers A, B, and C are correct. Each represents one area in the server farm that must be checked to ensure that the client has been configured properly with the minimum required encryption level. In most cases, if the user is receiving such an error message, it is likely that 128-bit encryption is being enforced and the client has been configured with the default Basic encryption level.

Answer D is incorrect. There is no such global encryption setting within the properties of the server farm.

5. Kerberos authentication is a new feature supported in MetaFrame Presentation Server 3.0. Select from the list the entry that best describes Kerberos client authentication. (Choose only one.)

- A. Kerberos allows you to encrypt communications between the MPS client and the MetaFrame server and is Citrix's replacement for SecureICA encryption.
- B. Kerberos is an industry-standard network authentication system that can be implemented in a MetaFrame environment to ensure that all MetaFrame servers are properly authenticated within the server farm. This protects against unauthorized MetaFrame servers being added to the server farm.
- C. Kerberos authentication is supported only within a Windows 2000 or 2003 domain, with version 8.x of the Win32 MPS client. Kerberos is an industry-standard network authentication system that protects against eavesdropping and man-in-the-middle attacks.

- D. Kerberos is an extension to the SecureICA encryption standard, providing secure authentication between the MetaFrame client and server. Kerberos is supported only on Windows 2000 or 2003 servers with version 8.x of the Win32 MPS client. With Kerberos, SecureICA is protected against eavesdropping and man-in-the-middle attacks.

A5: Answer C is correct. Answer A is incorrect because Kerberos does not encrypt the entire data stream, but instead manages securing only the authentication process. Kerberos is not a replacement for SecureICA.

Answer B is also incorrect. Kerberos has not been implemented to ensure authentication of the MetaFrame servers within the farm. Kerberos deals only with the authentication of the 8.x (or newer) Win32 client.

Answer D is incorrect because Kerberos is not an extension to SecureICA and does not integrate with Citrix's protocol encryption in any way. Kerberos deals with user authentication, while SecureICA is responsible for encrypting the data stream that runs between the client and server.

6. When you are using application sets (in Program Neighborhood) or the Program Neighborhood Agent and you want to employ Kerberos authentication, what must you use?

- A. Kerberos authentication without pass-through authentication
- 
- B. Kerberos authentication with pass-through authentication
- 
- C. ICA connection encryption
- 
- D. Windows Server 2003 servers only

A6: Answer B is correct. Program Neighborhood application sets and the Program Neighborhood agent do not support the use of Kerberos without pass-through authentication. Because of this, Answer A is incorrect.

Answer C is incorrect because ICA connection encryption has nothing to do with Kerberos authentication.

Answer D is incorrect. Kerberos authentication is supported on either Windows 2000 or Windows 2003.

7. Which of the following best describes the Citrix SSL Relay security component?



- A. Citrix SSL Relay enables users to connect to the MetaFrame server farm via a web page using the HTTPS secure protocol.



- B. Citrix SSL Relay provides full encryption for the server farm authentication process, ensuring that logon information cannot be intercepted via eavesdropping or man-in-the-middle attacks.



- C. Citrix SSL Relay provides encryption support for the ICA protocol. With SSL Relay, the ICA data is securely encrypted. The level of encryption used depends on the minimum required encryption setting found in the connection configuration, the published application configuration or the MetaFrame user policies.



- D. Citrix SSL Relay provides full encryption support for the ICA data stream between the MPS client and the MetaFrame Presentation Server. SSL Relay encapsulates the client data using the industrial standard SSL or TLS secure protocols.

A7: Answer D is correct. Citrix SSL Relay allows the MPS client to establish an SSL/TLS connection with the MetaFrame server, transmitting data fully encrypted and validated using security certificates. The full data stream is encrypted and authenticated, not just the logon credentials.

Answer A is incorrect. SSL Relay itself does not provide any form of web-based access to the MetaFrame server farm. This function is performed using the Web Interface, which in turn can have its data safely encrypted using SSL Relay.

Answer B is only partially correct, although more than just the session authentication is encrypted with SSL Relay.

Answer C is incorrect because SSL Relay does not provide the encryption support for ICA. ICA connection encryption and SSL/TLS connectivity are two different things. The ICA data stream is actually encapsulated and encrypted within the SSL/TLS session, but they do not directly interact in any way.

8. For a client to be able to employ SSL Relay, it must have a root certificate installed locally. What is the function of the root certificate?

- A. The root certificate provides the information required to validate the identity of the client to the server. When the client connects, the root certificate is passed to the MetaFrame server, where it is validated before allowing the client session to initiate.
- B. The root certificate provides the second half of the encryption key stored in the server certificate, which is installed on the MetaFrame server. When the client connects, the root certificate is combined with the server certificate and the full key is then used to establish the connection.
- C. The root certificate is required to activate the SSL Relay service in the Active Directory. Without the root certificate, this service cannot properly initialize because no certificate requests can be processed in the Active Directory.
- D. The root certificate is used to verify the certificate authority that signed the server certificate. If the root certificate exists on the client, the client is assumed to trust that CA, which in turn means that any server certificates issued by that CA are also trusted by the client.

A8: Answer D correctly describes the function of a root certificate. Many servers today maintain a large list of root certificates corresponding to trusted authorities who issue certificates that verify the identity of a server or person. Without a valid root certificate on the client, the client cannot trust that the host server is actually who it says it is. Only when a server certificate is issued from a less-known CA does a corresponding root certificate have to be installed on the server.

Answer A is incorrect. The root certificate does not contain validation information of the host it exists on. If a server required validation of a client's identity, a corresponding server certificate would be required, and the server would also be required to have the root certificate of the CA that issued the certificate to the client.

Answer B is incorrect. The server and root certificates do not represent a key that can be combined and then directly used to access the server.

9. The Citrix SSL Relay service listens on port \_\_\_\_\_ by default.

A. 80

B. 1494

C. 443

D. 8080

A9: Answer C is correct. The standard port for all SSL/TLS communications is TCP/IP port 443.

Answer A is incorrect. Port 80 is the standard HTTP port for unsecured web data. It is also the default port for the Citrix XML service.

Answer B is incorrect. Port 1494 is the ICA listening port when session reliability is not being used.

Answer D is also incorrect. Port 8080 is a common alternative HTTP port instead of port 80. No Citrix services employ port 8080.

10. You can add a server certificate to a MetaFrame server using either the IIS Web Server Certificate Wizard or the \_\_\_\_\_ if you are not running IIS on your MetaFrame server.

A. SSL Relay Certificate Import Wizard

B. The Certificates MMC snap-in

C. The SSL Relay Certificates MMC snap-in

D. The Import Certificates Tool

A10: Answer B is correct. SSL Relay leverages the certificates store built into Windows Server. Certificates are imported and managed using the Certificates MMC snap-in.

Answers A, C, and D are all incorrect. None of these tools actually exist.

 PREV

NEXT 

# 10. Application Integration

Terms you'll need to understand:

- Application Server mode
- change user /install
- change user /execute
- Packager
- Installer

Concepts you'll need to master:

- Understanding Install mode
- Understanding Execute mode
- Working with Application Compatibility Scripts

The power and beauty of MetaFrame Presentation Server has to be in the robust, intelligent, and centralized way by which it was designed to deliver applications to users. Just imagine an environment of 1,000 users requiring access to an accounting package. In a typical desktop environment, that application would have to be installed 1,000 times. You might say to yourself, "I'll just build an image and deploy it to all my desktops." That works with new computers or when you're doing an initial rollout, but what happens when you have existing desktops? Or better yet, what happens when a service pack for that application is released? You are probably saying, "Well, we can use some kind of remote deployment tool." Although that may be true, how efficient is that? And assuming it works great all the time with all issues, can you imagine what an administrative nightmare it would be to maintain 1,000 copies of an accounting package? Can you imagine what a support nightmare it would be for the helpdesk?

MetaFrame alleviates this problem by allowing you to install the application once on a server that is capable of supporting hundreds of users sometimes. In this scenario, you install the application once or on as many servers as you need to support the number of users you have; then you maintain the application's subsequent service pack or patch release on the servers only. Administration becomes easier, support becomes much easier, and from a helpdesk standpoint, the situation will not get any better. The environment is isolated and controlled, so you don't have to worry about what the user installed or did on his or her workstation that is rendering the application useless. You can concentrate on providing quality support for real issues.

In this chapter, we discuss how applications are installed and presented to the user.

# Preparing a Server for Application Installation

Terminal Servers or MetaFrame servers are delicate. You treat them right, and they will be very good to you; you treat them bad, and they will find a way to make your life miserable. For this reason, properly preparing a server for an application installation is very important. Installing an application on a MetaFrame server is a little different from installing it on a regular desktop for the simple reason that the install on the MetaFrame server would have to be primed and ready to service multiple simultaneous users on the same box.

## Enabling Terminal Server

First, make sure the server is in Application Server mode if you are using Windows 2000, or if you are using Windows Server 2003, make sure Terminal Server is enabled. This setting ensures that the server understands its role, which is to provide multiple simultaneous users access to applications on the server. This setting also allows users to log in to the server with their domain accounts. If this mode is not enabled, the server is configured in the Remote Administration mode, which allows only two simultaneous connections to the server. It allows these two connections only to members of the Administrators group.

## Install Versus Execute Mode

The second step in installing an application on a MetaFrame server is setting the mode in which the server is placed. You can choose one of two modes: Install or Execute. Because a MetaFrame server can host multiple users who may make changes to the same application running on it, you need to alert the server that it should monitor the installation of the application and record the settings and changes that it is making to the server. By doing so, you provide each user who logs in a certain privacy and the opportunity to make changes to an application without affecting other users.

You can tell the server to monitor all changes being made during the install of an application in two ways. You can select Add New Programs in Add or Remove Programs from the Control Panel to install the application. This method is the graphical user interface (GUI) equivalent of entering `change user /install` on the command line. If you decide to use the command line instead of the GUI, you need to complete a two-step process. First, put the server in Install mode, which tells it to monitor the changes by the application. Then install the application. After the installation is complete, switch back to Execute mode, which tells the server that it is ready to execute the application installed. To do this from a command line, you can type `change user /execute`. The advantage of using the GUI instead of the command line is that using the GUI from the Control Panel places the server in the Install mode automatically and, after the install is complete, switches the server back into Execute mode.

### Note

When you use the command line to set the server mode, it is very important to remember to put the server back in Execute mode after you install the application. You should not log off a server or reboot it before putting it back into Execute mode. Doing so tells the server to stop recording the application installation process. You should also know that after you log

off or reboot a server, it is automatically placed in Execute mode.

 PREV

NEXT 

## Application Compatibility Scripts

Many applications were not written for and were never intended to work in a multiuser environment. Installing them in their raw state may result in an inability to allow multiple users to take advantage of the application, thus defeating the purpose of the multiuser environment. Due to the success and popularity of MetaFrame and the need for many large and medium-sized companies to install certain applications on a MetaFrame server, the software developers created Application Compatibility Scripts. As their name implies, these scripts are dedicated to fixing or addressing certain issues in applications, making them multiuser enabled.

Application Compatibility Scripts are located in the Application Compatibility Scripts directory in the %SystemRoot% directory. These scripts should be run only against the applications they were intended for.

## Performing an Application Installation

Prior to installing an application on the server, you have to ensure that no sessions are currently running on the server and that no new connection can be established to the server while the application is being installed. Completing this step is imperative to ensure the proper running of the application for all users after the install is complete.

You can prevent new sessions from being established with the server in several ways. Select the easiest and most convenient for you. You can use the command line to disable access to the server by typing `change logon /disable`, which will disable new logons but will not log off existing sessions that are connected. You can then type `change logon /enable` later to reenable logons. You can disable logons to a server from the Management Console by expanding the Servers node, right-clicking the server, and choosing Properties. Select MetaFrame Settings from the left pane, and uncheck Enable Logons to this Server in the right pane, as shown in [Figure 10.1](#). You can also launch the Citrix Connection Configuration tool from the server where you want to disable logons, right-click the protocol, and choose Disable, as shown in [Figure 10.2](#).

Figure 10.1. Disable logons to the MPS server.

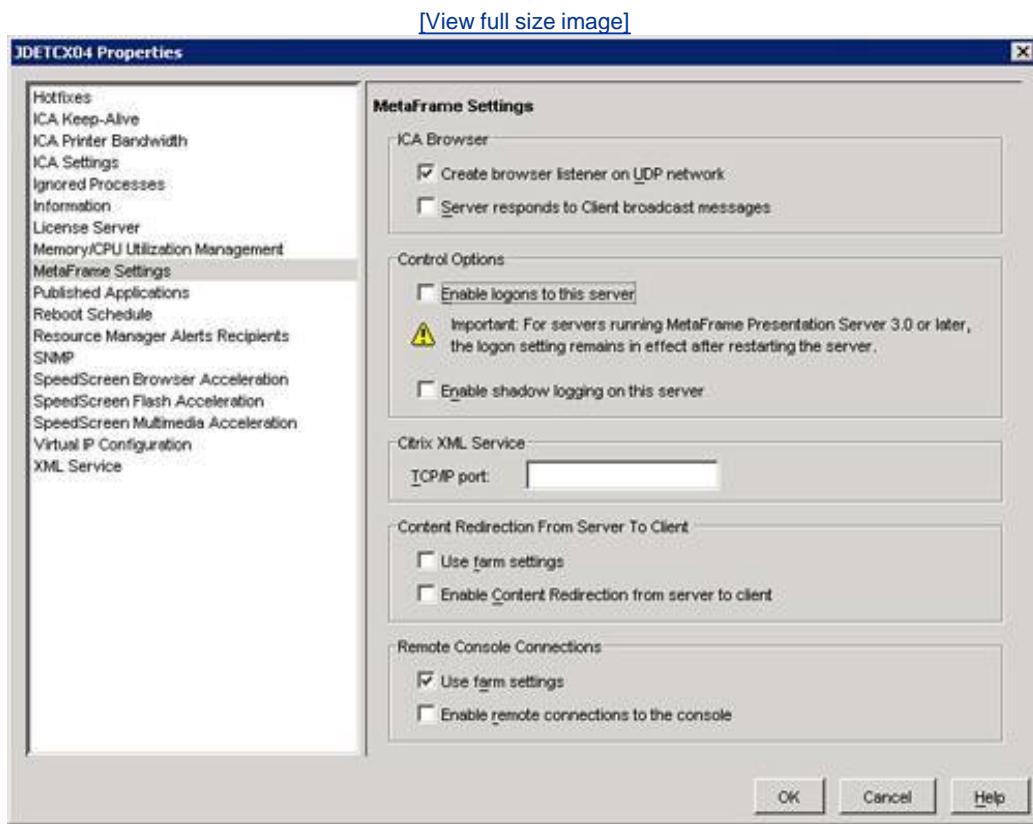
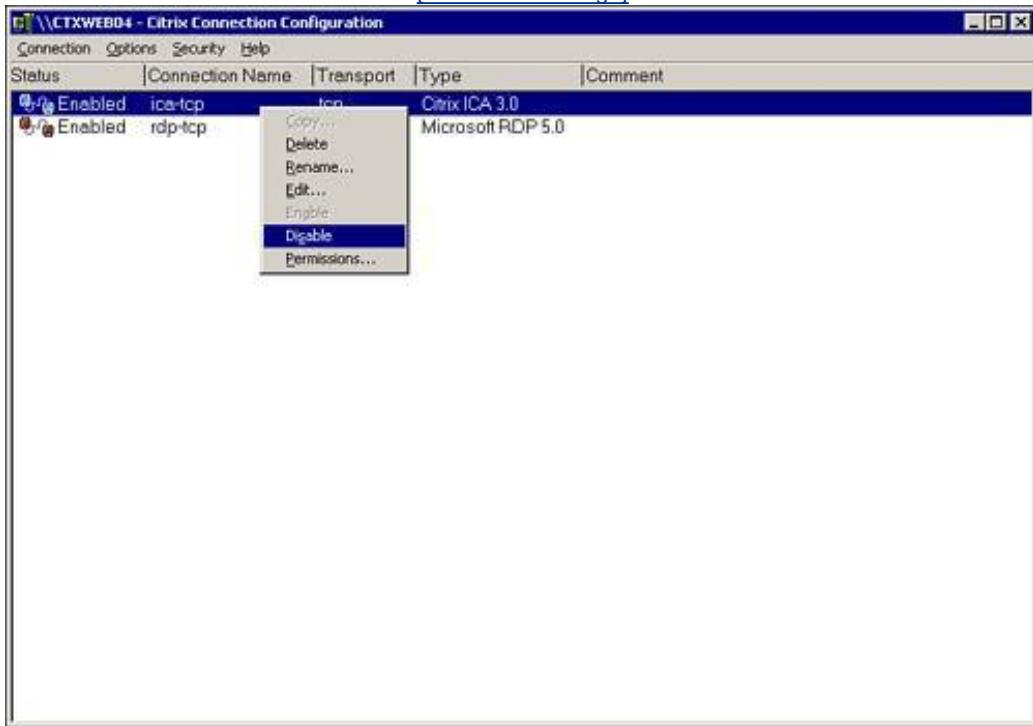


Figure 10.2. Disable the ICA-TCP protocol.

[\[View full size image\]](#)



The preceding steps take care of new connections but do not address currently connected sessions. You should always schedule your application install and announce to your users that this particular server will be unavailable on a particular date and time. The easiest way to view and log off users from a server is to use the Management Console. Expand the Server node and select the server in question. Click the Users tab in the right control pane. The tab displays a list of the users who are currently connected to the server. You can then select them all and right-click to log them off or reset their sessions.

## Installing an Application

After completing the preliminary steps and prerequisites to installing the application, you are ready to install it. If you decide to install using the command line, follow these steps:

1. Choose Start, Run, CMD and press Enter.
2. Type `change user /install`.
3. Run the setup program for the application from a CD, floppy disk, or network share.
4. After the install completes successfully, type `change user /execute` to switch back to Execute mode.

## Note

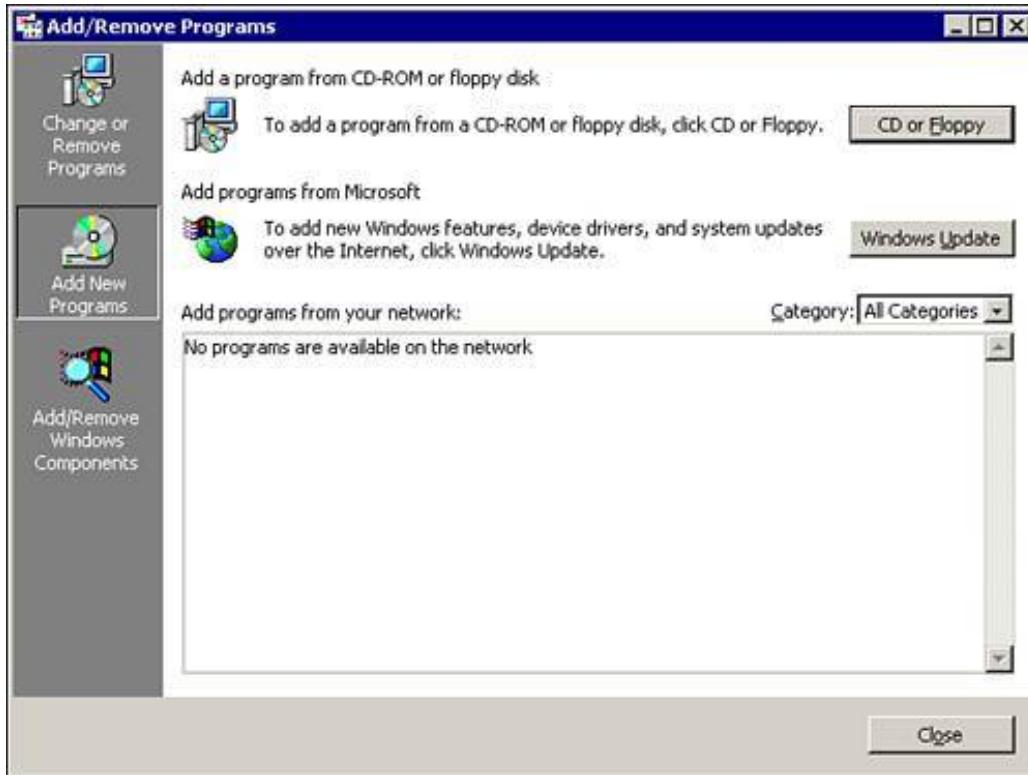
You can use `chgusr /install` and `chgusr /execute` as shortcuts to the full commands `change user /install` and `change user /execute`.

If you prefer to use the GUI to install an application, follow these steps:

1. Choose Start, Settings, Control Panel.
2. Double-click Add or Remove Programs and then click Add New Programs.
3. Click the CD or Floppy button, which launches a window that is the equivalent of the way Windows would have reacted had you typed `change user /install` manually from a command prompt.
4. Click Next. Then browse the CD, floppy, or network share and launch the setup program to run the installation of the application normally (see [Figure 10.3](#)).

Figure 10.3. Add New Programs Window.

[\[View full size image\]](#)



5. After the application finishes the installation successfully, you are then prompted to click Next and Finish to place the server back into Execute mode and save all the changes that were recorded by the server.
6. After the application is installed, you may need to run the appropriate Application Compatibility Scripts associated with that application for it run properly.

## Note

Many applications require you to reboot the server after their installation. It is important that you click Finish to ensure that all the changes the application made were properly recorded and saved.

**◀ PREV**

**NEXT ▶**

# Delivering the Application to the User

After installing the application, you are presented with the task of delivering it to the users. This task grants the users access to see and launch the published application or desktop. Again, you have to decide how to present this application to the user, whether you should use a published desktop or a published application. To be able to make a sound decision, you have to be familiar with each type.

## Full Desktops Versus Published Applications

When you are deciding which method to use to present the application to the users, there is no right or wrong, but rather the most appropriate and the most secure and convenient way of delivering the application. Several factors play a role in your decision.

A published desktop is ideal when the user needs to use multiple applications at the same time and those applications are all installed on the same server. Not only is it more convenient for the user to have one centralized desktop where all the applications are located, but it is also easier for the user to navigate and work within this desktop. A published desktop is also a performance enhancer for the server in that it does not launch several instances of the explore.exe process that is responsible for the GUI and is necessary for its operation. Therefore, if you are launching three applications separately, you are also launching a set of processes separately, among them an instance of explore.exe, for example, and putting strain on the server.

Published desktops, however, do have their drawbacks in that they are not as secure as published applications, and an administrator would have to spend a significant amount of time locking down such desktops via Group Policy to ensure that a user cannot accidentally shut down the server, for example, or run malicious code on the server.

Published desktops should be used when users need access to numerous applications that all reside on the same server.

Published applications, on the other hand, provide for tighter security and the feel of running applications as if they were being run locally on the computer. You can also deliver published applications to the users who reside on different servers. This fact is obviously seamless to the users.

## Publishing a Resource

To publish a resource, open the Management Console, right-click the Applications node, and then select Publish Application. This triggers the Application Publishing Wizard, which guides you through the process of publishing a resource in the farm.

### Welcome to the Application Publishing Wizard

The first wizard screen prompts you for a display name and an application description of the resource you are publishing. Fill in the necessary information.

## Specify What to Publish

The Application Publishing Wizard then prompts you to choose the application type. You can choose Application, Desktop, or Content. Based on your selection, you will have to provide either a path to the executable if you choose Application or the link to a resource such as a web page if you select Content. If you choose Desktop, you will not be prompted for more information. For the purpose of this example, we selected Application.

The configurable options are as follows:

- Command Line In this field, you specify the location of the application's executable.
- Working Directory In this field, you specify the directory where the application's executable is started from.
- Allow This Published Resource to Be Accessed Externally Through MetaFrame Secure Access Manager If checked, this option renders this application accessible to users from outside the network. Unchecking this box limits access to this application to users on the network. You can use this option as a secure measure to prevent access to certain critical applications such as a check-writing application from being accessed outside the network.

## Program Neighborhood Settings

The Program Neighborhood Settings screen allows you to control how the application is presented to the user (see [Figure 10.4](#)). The configurable options are as follows:

- Program Neighborhood Folder In this field, you specify a folder under which this application will appear within the Program Neighborhood interface.
- Application Shortcut Placement The options in this section allow you to place this application under the Program Neighborhood folder on the Start menu. This is applicable only to users of Win32 ICA clients. If your users have the Program Neighborhood Agent version of the ICA client, you can further customize where the published resources show up by creating a custom folder under the Programs menu of the Start menu. To do this, check the box next to Place Under Programs Folder: (Program Neighborhood Agent Only). In the Start Menu Folder text box, enter a name for the folder where you want to place this published resource under the Programs menu of the Start menu.
- Change Icon This option allows you to browse and select a different icon that will appear associated with this published resource.

Figure 10.4. Program Neighborhood Settings.

[\[View full size image\]](#)



## Specify Application Appearance

When the Specify Application Appearance window appears, you can customize how the application will look after the user launches it. The configurable options are as follows:

- **Session Window Size** This option allows you to select the dimension at which the application window will open. Your options are as follows: Standard resolution, which allows you to select from as low as 640x480 all the way up to 1600x1200; Custom, which allows you to manually specify the width and height of the window to be opened; Percent of Client Desktop, which allows you to select a percentage of the client desktop that the application window will cover when launched; and Full Screen, which covers the client's full screen when the application launches.
- **Colors** In this section, you can choose a color depth of one of the following: 16 colors, 256 colors, High Color (16bit), and True Color (24 bit).
- **Application Startup Settings** In this section, you can configure how the application will behave when initially launched. You have two options to choose from: Hide Application Title Bar allows you to hide the application title, which then prevents users from closing or minimizing an application using the X for example, at the top-right corner. This option prevents users from using this method to exit applications and places their sessions in a Disconnect mode when they intend to exit the application altogether. The other option, Maximize Application at Startup, starts the application maximized if selected.

## Specify Client Requirements

The Specify Client Requirements window opens next. The configurable options are as follows:

- Enable Legacy Audio This option enables audio support for applications that cannot take advantage of SpeedScreen Multimedia Acceleration. You can also choose to make this a minimum requirement whereby only clients that have audio support can launch this application. To do this, check the box next to Minimum Requirement.
- Enable SSL and TLS This option enables two security protocols: SSL (Secure Sockets Layer) and TLS (Transport Layer Security). If this option is enabled, the client and server would have to communicate over one of these two protocols.
- Encryption This option specifies the level of encryption used between the client and server. The options are as follows: Basic, which encrypts the packets with a non-RC5 algorithm; 128-Bit Login Only (RC5), which encrypt the packets exchanged between the client and server at logon time with 128-bit RC5 encryption and then uses Basic encryption for ongoing packet transfers; 40-Bit (RC5), 56-Bit (RC5), and 128-Bit (RC5), which constantly encrypt the data stream at the specified level. If you choose 40-Bit, it always encrypts the data packet at 40-bit RC5 and so on.
- Start This Application Without Waiting for Printers to Be Created Selecting this option actually improves the launch time of an application by allowing it to open and giving the user access to its graphical user interface before all the printers have had the chance to properly map within the session. The printers will continue to map; however, the idea here is that most likely the user will not launch an application and start printing immediately. Instead, the user will first input data. While he or she does this, the printers will have had ample time to be created and will be available to the user when needed.

## Specify Application Limits

The next wizard window, Specify Application Limits, allows you to specify how many instances of this application can run and the CPU prioritization it receives. The configurable options are as follows:

- Limit Concurrent Instances in Server Farm Checking this option enables you to set a maximum number of simultaneous instances to run in the server farm. You can set the number in the Maximum Instances text box.
- Allow Only One Concurrent Instance Per User This option allows every user to launch one instance of the application.
- CPU Priority Level This option allows you to set the CPU priority for this application. It can instruct the CPU on how to treat this application in terms of importance. Your options are Low, Below Normal, Normal, Above Normal, or High; the default is Normal.

## Specify Servers

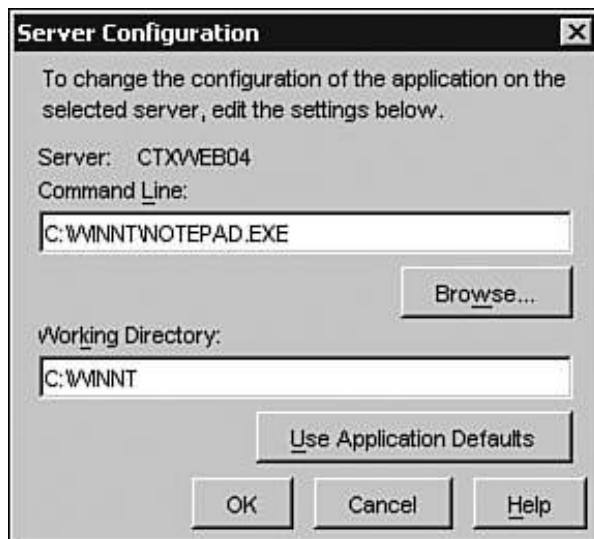
Next up is a wizard window that allows you to specify how many servers will service this application. One of the most powerful and most sought-after features of MetaFrame is the ability to load balance an application across several servers. This feature is a great way to spread user load and, from a redundancy standpoint, it allows you to eliminate single point of failure. So, in the event that you have configured two servers for this application, not only will MetaFrame load balance between them, but if one server fails, your users can still access the published resource because another server is configured with the same application. Keep in mind that this is not fault tolerance: If one of the servers goes down, the user sessions on that server are lost, but the user retains the ability to access that application because a second server hosts it.

You are presented with two lists here: the Available Servers list, which lists all the servers in the farm, and the Configured Servers list, which lists all the servers you have chosen to support this application. Obviously, the servers you select must have that application installed on them. Here, you can add and move servers back and forth between the Available Servers and Configured Servers lists.

This same window presents these three buttons:

- Filter Servers By This option allows you to limit the servers in the Available Servers dialog box based on the operating system they are running. The options to filter based on operating system are Windows NT 4.0 TSE, Windows 2000, and Windows Server 2003. You also can filter by whether the server has Installation Management capabilities.
- Refresh Available Servers This option forces a refresh of the Available Servers list.
- Edit Configuration You can select this option only after you have added a server to the Configured Servers list. It is a useful option when you are publishing an application that is installed in different locations on the MPS servers. For example, say you are publishing Notepad.exe and you want server 1 and server 2 to support this application. However, you have Notepad.exe installed in C:\Windows\system32 on server 1 and in D:\Apps on server 2. Using this option allows you to specify where the application resides on the MPS servers individually without having to republish the same application (see [Figure 10.5](#)).

Figure 10.5. Sever Configuration Window.



## Specify Users

At the next step in the Application Publishing Wizard, you can specify the users who have access to this published resource. The configurable options are as follows:

- Allow Anonymous Connections If you check this box, all users will have access to this application. They will get access to it without needing to authenticate; in other words, they will not need to provide a username, password, or domain.

## Note

For security reasons, on domain controllers that are acting as MPS servers as well, anonymous user accounts cannot be enabled.

- Add List of Names If you click this button, it allows you to paste or write several usernames separated by a semicolon. This capability is useful if you have the usernames in a text file. All you have to do is paste them, check the names against the directory, and the system will add them as users of this application.
- Look in This window allows you to set the scope where you will be searching for user accounts or groups. For example, it lists Active Directory domains, Windows NT domains, Novell Directory Services Trees, and local servers. You can browse any of these resources for a user account or group to add to the Configured Accounts section.
- Show Users When you are browsing account authorities, usually user accounts are not shown, just groups. To show all user accounts, you need to check this box.
- Configured Accounts This area lists the accounts that you have granted access to this published resource. It lists user accounts and groups.

## Note

It is highly recommended that you use groups as the preferred method of granting access to an application because using them simplifies the administration process tremendously.

## The Anonymous User Accounts

When you install MetaFrame Presentation Server, as part of the installation, 14 anonymous user accounts are created and added to the Users container of the local machine. These accounts are in the format of anon001 through anon014.

These accounts are used when you enable Allow Anonymous Connections for a published application.

When you install MPS on a domain controller, these accounts are not created primarily for security reasons; therefore, if you publish an application on a domain controller, you cannot enable anonymous connections to it.

## Specify File Type Associations

The next wizard screen shows off the strength and tight integration the MPS product now has with the local desktop. As you can see in [Figure 10.6](#), you have the option of associating this application with

file extensions or types. If you associate file extensions with this application, content redirection kicks in for this application, which will enable users to open files that reside locally on their computers with an application published on a MetaFrame Server.

Figure 10.6. File Type Association window.



Say you have Microsoft Word published on the server. Microsoft Word is not installed on the user's local machine, but Outlook is. The user receives an email with a Word attachment. After the user double-clicks the attached file, Microsoft Word is automatically launched from the MPS server and opens the file. This capability is very useful with more specialized applications that will most likely be installed on the MPS server and not locally on the user's desktop.

## Note

File associations will work only if the user is using the Program Neighborhood Agent as his or her ICA client.

# Published Application Properties

After you publish an application to the server farm, you can always go back into its properties and modify the settings you made during the Application Publishing Wizard process. You can also organize your published applications into folders for better and easier administration.

To accomplish these functions, launch the Management Console, right-click the Applications node, and select New Folder. You can then name that folder and just drag and drop applications into it.

To access the properties of a published application, right-click it and select Properties. The published application's properties window opens and offers you the following nodes to the left (see [Figure 10.7](#)):

- Application Appearance is the equivalent of the Specify Application Appearance step in the Application Publishing Wizard and offers the same settings.
- Application Limits is the equivalent of the Specify Application Limits step in the Application Publishing Wizard and offers the same settings.
- Application Location is the equivalent of the Specify What to Publish step in the Application Publishing Wizard and offers the same settings.
- Application Name allows you to set a display name and an application name. The display name can be the common name that your users are accustomed to calling the application, whereas the application name should be the real name of the application. You also can choose the Disable Application or Hide Disabled Application option (see [Figure 10.8](#)). If you disable the application, it will still show up in the user's list of available applications but will not work when the user tries to launch it. If you disable the application and then hide it, the icon for that application is completely hidden from the user. This capability can be useful in alleviating support calls from users complaining that they see the application but nothing happens when they click it.
- Client Options is the equivalent of the Specify Client Requirements step in the Application Publishing Wizard and offers the same settings.
- Content Redirection is the equivalent of the Specify File Type Associations step in the Application Publishing Wizard and offers the same settings.
- Program Neighborhood Settings is the equivalent of the Program Neighborhood Settings step in the Application Publishing Wizard and offers the same settings.
- Servers is the equivalent of the Specify Servers step in the Application Publishing Wizard and offers the same settings.
- Users is the equivalent of the Specify Users step in the Application Publishing Wizard and offers the same settings.

Figure 10.7. Published application's properties window.

[\[View full size image\]](#)

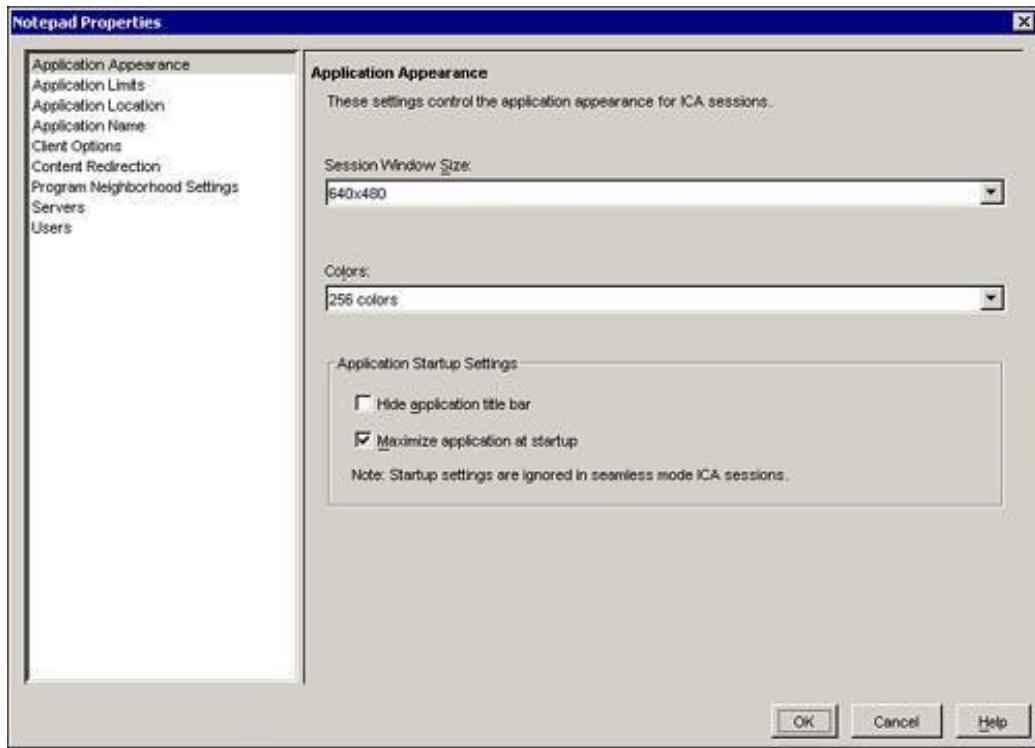
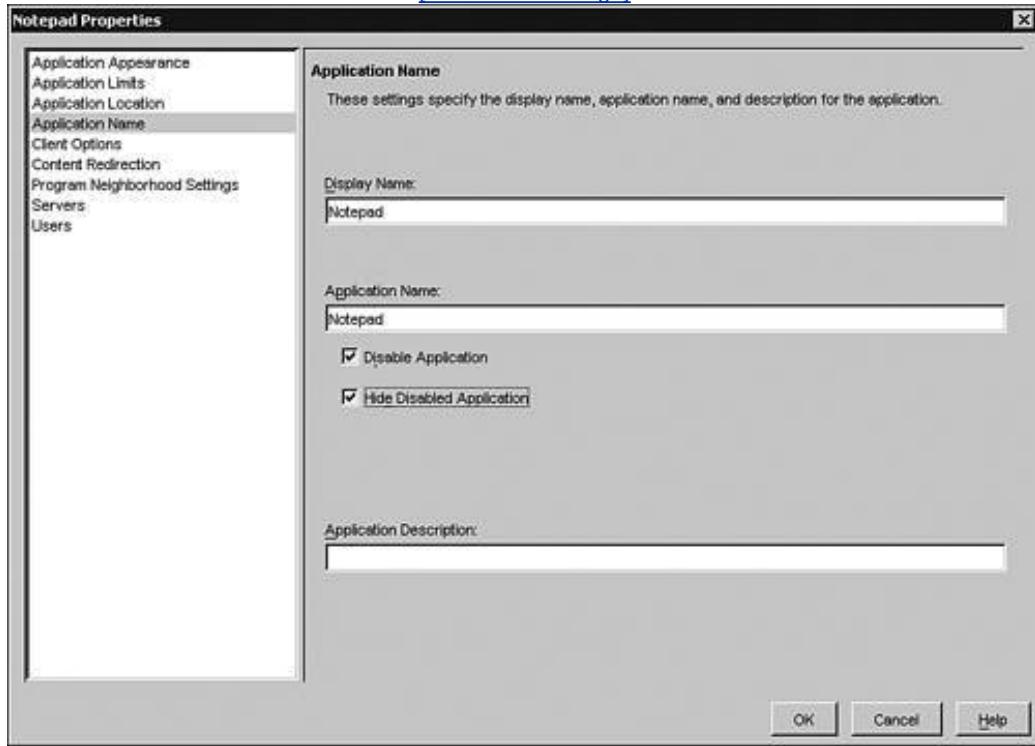


Figure 10.8. Application Name node.

[View full size image]



◀ PREV

NEXT ▶

## Installation Manager

The Enterprise Edition of MetaFrame Presentation Server 3.0 comes with a utility that allows you to package and distribute an application automatically to several servers. This utility is similar in concept to the Microsoft Systems Management Server (SMS). If you have 50 servers in your enterprise that host the same application, and the application vendor or in-house developers decide to release a service pack to address several issues, without this tool you would need to install the Service Pack 50 times.

Citrix Installation Manager alleviates this problem by allowing you to build a package known as an Application Deployment File (ADF). ADF is also the file extension of the packages that are built with Installation Manager. Also supported by Installation Manager are packages built as Microsoft Windows Installer (MSI) and Microsoft Windows Installer Patch (MSP) files. Installation Manager supports ADF, MSI and MSP packages.

Installation Manager consists of the following three components:

- Packager is the utility that builds the ADF file, schedules the deployment of packages, and monitors the installation of the packages. Packager can also roll out MSI and MSP packages.
- Installer is a service installed by default on all Enterprise Editions of MPS and is the component of Installation Manager that allows packages to be installed on the server by the packager.
- Network Share is a location on the network, typically a file server where the packages are stored. This network share would need to be accessible by the servers.

## Exam Prep Questions

1. Which of the following is the utility that automates the packaging and distribution of applications to MetaFrame Presentation Servers and is proprietary to Citrix?

- A. Systems Management Server
- B. Application Installer
- C. Installation Manager
- D. Rapid Deployment Manager

A1: Answer C is correct. The utility that is Citrix proprietary and that is used to deploy packages is Installation Manager. Answer A is a Microsoft application that can be used, but the question is about a Citrix proprietary application. Answers B and D are incorrect because they don't exist.

2. What is the correct method by which you should install applications on a MetaFrame Presentation Server to ensure that the server properly records these changes?

- A. Browse to the application executable and double-click it.
- B. From the Start menu, click Run and then launch the executable from a command line.
- C. Put the server in Execute mode.
- D. From Control Panel, run Add or Remove Programs and install the application.

A2: Answer D is correct. The proper way of installing an application on an MPS server is to either place the server in Install mode via the command `change user /install` or use Add or Remove Programs in Control Panel to run the install. Answers A, B, and C are incorrect because they are not the proper methods to install an application in MPS.

3. Which step in the Application Publishing Wizard allows you to specify the encryption level?

A. Program Neighborhood Settings

B. Specify Application Limits

C. Specify Client Requirements

D. Specify Servers

A3: Answer C is correct. In the Application Publishing Wizard, you can modify the encryption settings in the window called Specify Client Requirements. Answers A, B, and D are incorrect because they are not the proper place to make such changes.

4. Your organization has just deployed an accounting application called MoneyTracker and has installed this application on all 20 servers in the same location, D:\Apps\MoneyTracker. After a few months, you decide to hire an additional Citrix administrator, and one of his first tasks is to bring up the 21<sup>st</sup> Citrix server with MoneyTracker installed on it. He installs the application using its default path, C:\Program Files\MoneyTracker. How can you add this server to the list of configured servers that support this application without changing its path?

- A. In the Servers node of the published application's properties, add the server to the Configured Servers list, highlight it, and then click Edit Configuration and modify the path.
- 
- B. In the Application Location node of the published application's properties, add the server to the Configured Servers list, highlight it, and then click Edit Configuration and modify the path.
- 
- C. In the Application Name node of the published application's properties, add the server to the Configured Servers list, highlight it, and then click Edit Configuration and modify the path.
- 
- D. In the Client Options node of the published application's properties, add the server to the Configured Servers list, highlight it, and then click Edit Configuration and modify the path.

A4: Answer A is correct. If one or more servers are different from the others in terms of where the application was installed on the hard drive, you can make a modification on an individual server basis by going to the Servers node of the published application's properties, adding the server to the Configured Servers list, highlighting it, and then clicking on Edit Configuration and modifying the path. Answers B, C, and D are incorrect because they do not identify the correct nodes to make the changes required.

5. You have just published an application to your users, but your IT director has just emailed you asking you to place a shortcut directly to the user's desktop for easier and faster access to this application. How would you accomplish this?

- A. Visit each user's workstation and create a shortcut to the application.
- B. Use a remote access application to remotely access the user's desktop and create a shortcut.
- C. In the Program Neighborhood Settings node of the published application's properties, check the box next to Add Shortcut to the Client's Desktop.
- D. In the Client Options node of the published application's properties, check the box next to Add Shortcut to the Client's Desktop.

A5: Answer C is correct. You can add a shortcut to the user's desktop provided that the user is using the Program Neighborhood client on his or her workstation. To do this, you can check the box next to Add Shortcut to the Client's Desktop in the Program Neighborhood Settings node of the published application's properties. Answers A and B are incorrect because even though you can use these approaches, they are impractical and you would not be taking advantage of all the capabilities that MPS has to offer; plus, they simply reflect a lack of knowledge of the product. Answer D is incorrect because it is not the right location to make that change.

6. If you choose Allow Anonymous Connections in the Users node of the application's properties, which account is used for the anonymous user who is connecting?

- A. The built-in Guest account
- B. Anon001 through 014
- C. The CitrixAnon Service account
- D. Guest001 through 014

A6: Answer B is correct. When you install MPS, it creates 14 anonymous user accounts in the format of anon001 through 014, and those accounts are used to allow anonymous access when it is enabled. Answer A is incorrect because it does not use the built-in Guest account. Answer C is incorrect because there is no CitrixAnon service account. Answer D is incorrect because there are no Guest001 through Guest014 accounts.

7. What types of resources can you publish in a server farm? (Choose all that apply.)

A. Application

B. Desktop

C. Content

D. Video

A7: Answers A, B, and C are correct. The three available options to publish a resource in the Application Publishing Wizard are Application, Desktop, and Content. Answer D is incorrect because it is not one of the valid options you can choose.

8. If you are installing an application via Add or Remove Programs, and the installation completes successfully but is now asking for a reboot, what should you do?

A. Allow it to reboot and very quickly click the Finish button.

B. Allow the server to reboot to finish the installation.

C. Choose not to reboot, click Finish, and then manually reboot the server.

D. Choose not to reboot, do not click Finish, but manually reboot the server to allow it to finish the installation.

A8: Answer C is correct. You should choose not to allow it to reboot, click Finish to allow the

server to register all the changes that were made by the server, and then manually restart the server. Answer A is incorrect because it should never be a speeding contest. Answer B is incorrect because if you allow the server to reboot, you don't allow the server to properly register all the changes. Answer D is incorrect because, again, if you don't click Finish, the server does not register all the changes that were made by the application installation.

9. What file types can the Installation Manager support and distribute? (Choose all that apply.)

A. MSI

B. MSP

C. ADF

D. GHO

A9: Answers A, B, and C are correct. Installation Manager supports packages built on the Application Deployment File (ADF) and Microsoft Windows Installer (MSI) and Microsoft Windows Installer Patch (MSP). Answer D is incorrect because you can't deploy a GHO image. GHO is the file extension used by Symantec Ghost to create images.

10. What is the proper command to disable logons to a MetaFrame Presentation Server? (Choose all that apply.)

A. `change user /disable`

B. `chgusr /disable`

C. `change logon /disable`

D. `chglogn /disable`

A10: Answer C is correct. The proper command to disable new logons to a MetaFrame Presentation Server is `change logon /disable`. Choices A, B, and D are incorrect because no such commands exist.

 PREV

NEXT 

# 11. Deploying Applications Using Installation Manager

Terms you'll need to understand:

- Installation Manager (IM) packages
- MSI, MSP, and ADF packages
- Package management server
- Network share point server
- Package server
- Target server
- Installer and Packager services
- Server and package groups
- APPUTIL

Concepts you'll need to master:

- Identifying the components of Installation Manager and understanding the role they serve
- Identifying the default package source location and Windows authentication account
- Choosing the default Installation Manager options that best meet the needs of a particular deployment scenario
- Creating server and package groups
- Monitoring the status of a package deployment
- Scheduling the uninstall of package
- Deploying packages using application publishing

In [Chapter 10](#), "Application Integration," we reviewed application deployment and Citrix's concept of application and content publishing. While content typically resides in a central location where it is easily accessed from any server in the farm, an application must be installed on a MetaFrame server before it can be published.

To ease the task of deploying an application across multiple servers, Citrix provides Installation Manager as part of the Enterprise Edition of MPS. Installation Manager (IM) allows you to centrally manage the attended or unattended installation of applications and other software components (specific files, service packs, software patches, and so on) to the servers in your server farm. The

applications and other software components being deployed are referred to as *packages*. As the number of servers in the farm increases, the usefulness of IM becomes more and more apparent.

Installation Manager provides the following:

- It allows centralized, rapid deployment of application packages. Any MetaFrame server in the farm can be used to deploy packages, regardless of its location, connection speed, or hardware configuration.
- Applications can be installed, uninstalled, and repaired using Installation Manager.
- Application packages that have been created in IM can be published and automatically deployed to the target servers in the farm. You do this through the Application Publishing Wizard, which we discussed in [Chapter 10](#). Installation Manager adds the Installation Manager Package option to the list of application types that can be published. When an IM package is published, it is automatically installed and then published for the specified users.
- Packages can be deployed immediately or scheduled for a time that is appropriate for the environment. Application installation, removal, publishing, and even repair can be scheduled to run automatically without administrator intervention.

If necessary, a server restart can also be initiated immediately after the completion of the package deployment, ensuring that the application and the server environment are ready for use.

- Multiple packages can be managed as a single logical package through package groups. Within a package group, you can specify the installation sequence for all child packages, so when a single package group is deployed, all components are installed in the correct order. Package groups simplify the process of deploying multiple related packages to MetaFrame servers in the farm.

- IM supports the following three package formats:

- MSI These packages are based on the Microsoft Windows Installer Service. Many common software products such as Microsoft Office ship with MSI-based installation files, which can be used within IM to deploy the application. MSI files also support the use of transform files (usually with .mst extensions). Transform files modify the default behavior of the installation package and are most often used to tailor an MSI installation for a specific environment such as Terminal Services. IM supports the use of transform files with MSI packages.

MSI files can also be created using software deployment tools such as InstallShield. MetaFrame does not include tools for creating MSI packages.

- MSP MSP files are also based on the Microsoft Windows Installer Service and are typically used to patch or update an existing application deployed using an MSI package. MSP packages are usually provided by software manufacturers to patch their products and can also be created using software deployment tools. MetaFrame does not provide tools for creating MSP packages.
  - ADF Application Deployment File packages are created using the Packager application that is provided as part of Installation Manager. ADF packages are most often created when an application must be deployed and it does not already provide an MSI or MSP package. We review ADF package creation in the "[Creating ADF Packages Using the Packager Utility](#)" section later in this chapter.

- Installation Manager supports access delegation to MetaFrame administrators. Access to view

and edit the Installation Manager configuration is supported, as well as the delegation of rights to install and uninstall packages on servers within a server group. These install/uninstall access management rights were not available in MetaFrame versions prior to 3.0.

## Alert

Know that the install/uninstall access management rights are defined within a server group, and not within Installation Manager or a package group. View/edit rights apply to packages, whereas install/uninstall rights apply to servers.

- Citrix provides support for managing published applications from a command prompt using the **APPUTIL** utility. In addition, **APPUTIL** also allows you to manage the installation and removal of IM packages and entire package groups from servers in the farm. You can find a full summary of **APPUTIL'S** features as they pertain to Installation Manager in the "[Managing Packages from a Command Prompt](#)" section later in this chapter.

 PREV

NEXT 

# Components of Installation Manager

Installation Manager is made up of four components, whose configuration and deployment are based on the type of environment within which Installation Manager is intended to run. The four components are the package management server, network share point server, package server, and target servers.

## Package Management Server

One of the MetaFrame Presentation Server 3.0 Enterprise Edition servers in your farm is designated as the package management server and has both the Installation Manager component and the Management Console for MPS 3.0 installed. The package management server does not need to be run on a dedicated MetaFrame server in the farm. It can also be one of the target servers, which are described later. The package management server is used to configure and deploy the application packages via Installation Manager.

## Network Share Point Server

The application packages deployed through IM are not maintained within any kind of special MetaFrame repository, but are in fact stored on one or more file servers accessible from the Package Management Server. The network share point server can be any server in the environment that is accessible using the universal naming convention (UNC) name (\\\share name). This server is not required to be running MPS, and in fact is not even required to be running Windows. As long as the file server supports standard Windows file sharing access, it can be configured for use through Installation Manager. The package management server can be used as the network share point server, but a UNC name must still be used to access packages for deployment. IM does *not* allow you to define a drive-letterbased path to packages (c:\folder\packages, for example).

In addition to the UNC naming requirement, the network share point server has some additional basic system requirements:

- Sufficient disk space for the application packages and associated files must exist on the server.
- The server must be accessible to all target MetaFrame servers. It is not recommended that target servers be configured to access a network share point through a firewall. Instead, a network share point should be configured on the same local network as the target servers. Installation Manager supports the use of more than one network share point server, allowing servers to be positioned geographically close to the target servers.
- Two types of access privileges must be defined for the network share point and underlying folder:
  - A minimum of read and write access must be granted to an account to allow the copying of packages to the network share point server.
  - An account must have read access to the network share point (and administrative privileges on the target servers) to retrieve packages and install them on the target server. The

credentials for this account are entered and maintained as the default network credentials for Installation Manager. The configuration of IM is discussed further in the "[Installing and Configuring Installation Manager](#)" section of this chapter.

## Package Server

In an Installation Manager environment that also employs Citrix's Packager application to create custom ADF packages, a MetaFrame server must be designated as the package server. When a MetaFrame server is employed as the package server for IM, Citrix recommends that this server be dedicated to package creation, and not used for any other purpose, including MetaFrame client connections. Because the Packager "records" the installation steps for an application, it is important that the package server reflect as closely as possible the configuration of the production servers, right down to the operating system. Citrix recommends that the package server meet the following requirements:

- It should run a clean installation of Windows 2000 Server or Windows Server 2003, whichever is required for the target servers. Multiple package servers can be created if the target servers are a mix of Windows 2000 and 2003. Packages created on one operating system should not be used for deployment onto a different target operating system. The package server should not be tasked with any additional functions not found on the target servers (web page serving, file and printer sharing, and so on). The operating system should match what is found on the target servers as closely as possible.
- The partition on which the operating system is installed should not contain any additional applications or data not in use on the target servers.
- The Packager application should be installed on the same partition as the core MetaFrame files. The default location is the same partition as the operating system.

You can find details on the configuration and use of the Packager application on the package server in the "[Creating ADF Packages Using the Packager Utility](#)" section of this chapter.

### Alert

A package server is required only if you intend to create ADF packages for deployment. If your environment uses only MSI and MSP packages, a package server is not required.

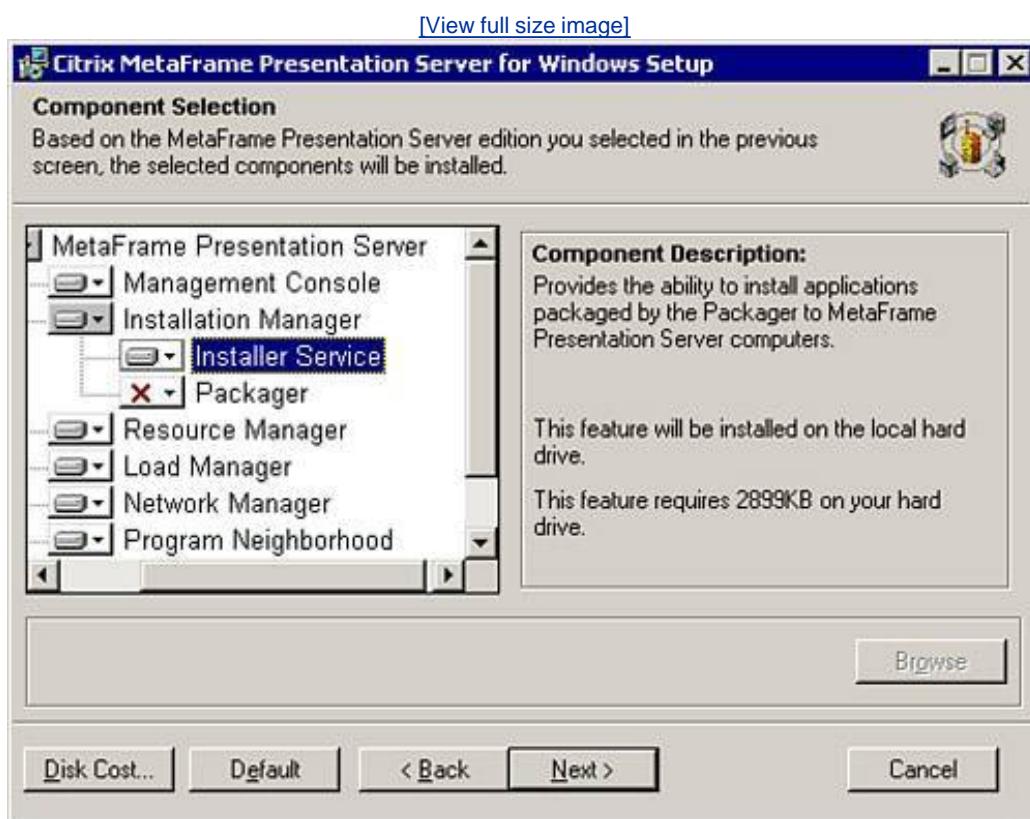
## Target Servers

All MetaFrame servers on which Installation Manager packages are deployed are known as target servers. To be a valid target server for IM, the server must be running MetaFrame Presentation Server Enterprise Edition and have the Installer service component (called ADF Installer Service) of IM running. The account used to perform package deployment must have administrative privileges on all target servers.

# Installing and Configuring Installation Manager

All components of Installation Manager are installed by default as part of the MetaFrame Presentation Server Enterprise Edition installation. During the installation, you select the specific components of Installation Manager that you want by verifying the Component Selection page, as shown in [Figure 11.1](#). In this example, only the Installer Service has been selected. If you do not require the Packager component, you must explicitly omit it from the installation; otherwise, it will automatically be included by default.

Figure 11.1. All components of the Installation Manager are installed by default along with MPS Enterprise Edition.



You can remove an existing Installation Manager configuration from a MetaFrame server by modifying the MetaFrame Presentation Server for Windows installation through Add/Remove Programs. On the Component Selection page, deselect Installation Manager.

## Note

After removing the Installation Manager component, be certain to reboot the server before you attempt to reinstall IM. A reboot ensures that the Installation Manager subsystem service (imsss.dll) has been properly deleted. If the reboot is not performed, it is likely that a new IM installation will be corrupted.

Before you deploy applications through Installation Manager, you need to configure some basic IM properties. You open the properties dialog box for IM by right-clicking Installation Manager in the Management Console for MPS 3.0 and selecting Properties from the context menu. The properties dialog box then opens, presenting you with three categories of options:

- About Installation Manager Provides name and version of IM.
- Network Account Settings Specify where you provide account credential and default share location information.
- Options Specify settings that dictate the general behavior of Installation Manager.

## Network Account Settings

Within this dialog box, you define the default network credentials used to retrieve packages from the network share point and install them on target servers. Installation Manager does not recognize the user-principal naming (UPN) format ([user@domain.com](mailto:user@domain.com)), so the username must be in the format domain\username. As mentioned earlier, the file share location must be a UNC path. IM does not allow you to specify a drive letter. This makes sense because all target servers use this information to locate the correct software package and a UNC path ensures that this can be done correctly.

### Alert

The default credentials and share location defined on this property page can be overridden within package groups. A review of package group creation and configuration is discussed later in this chapter.

## Options

On the Options property page, you define the general settings about the behavior of Installation Manager.

You can define the following settings:

- Days Before Jobs Expire and Are Removed By default, jobs never expire; they remain in the job list until they have successfully completed. This option allows you to specify an expiry date for jobs. At that point, they are automatically removed from the Installation Manager job list.
- Force Users to Log Off Before Installing When this option is enabled, new user logons are automatically disabled and users currently on the server are prompted to save their data and log off before their session is automatically reset. They receive three warnings at 5-minute intervals

before being logged off. After the third warning, any remaining user sessions are terminated and the installation starts. After the installation is complete, logons are re-enabled on the server. If a reboot is required, logons are re-enabled after the server has restarted.

- **Do Not Reboot Server If Any User Sessions Are Open** If this option is enabled, the reboot is aborted if there are active user sessions on the server. The reboot is not automatically performed after the last user logs off. Instead, an administrator must manually reboot. The Force Reboot After Install job setting overrides this default setting, forcing the server to reboot whether or not users are currently on the server.
- **Time Before Server Reboot** This setting allows you to adjust the default time after a package deployment completes before a server reboot is performed. The default interval is 15 minutes, but you can change it to one of 5, 10, 15, 30, or 60 minutes. You cannot specify your own custom time such as 25 minutes, however. This setting does not affect the time interval for sending warning messages if the Force Users to Log Off Before Installing option has been configured.
- **Send Reboot Message Every** By default, a message warning the users to save their data and log off before the server is restarted is sent every 5 minutes until the reboot wait time has been reached. You can change this value to 1, 3, 5, or 10 minutes. This setting does not affect the time interval between warnings if the Force Users to Log Off Before Installing option has been configured.
- **Add Custom Message to User Sessions** This simple setting allows you to define a personal message to send to users prior to the server rebooting. This message does not appear when users are forced off before installing a package.

 PREV

NEXT 

# Application Deployment Using Installation Manager

The actual process of application deployment using Installation Manager is quite straightforward. In this section, we review these steps while providing an example of how such a deployment could be performed using one of the most commonly used applications on MetaFrame, Microsoft Office 2003.

The following are the basic application deployment steps, which are reviewed in more detail in the following sections:

1. Verify Installation Manager configuration. Verify that the appropriate Installation Manager components have been configured as required and all the necessary permissions and administrative delegations have been assigned. This process was discussed in the "[Components of Installation Manager](#)" section earlier in this chapter.
2. Determine package format. If the application already provides an MSI or MSP installation package, you can use it; otherwise, you first need to package the installation using the Packager application. You can find details on this procedure in the section "[Creating ADF Packages Using the Packager Utility](#)" later in this chapter. For our example, we're going to use the MSI package provided with Microsoft Office 2003. Office 2003 Standard Edition provides the STD11.MSI package on the root of the installation media.
3. Copy packages to the network share point. An ADF package can either be manually copied or automatically copied when the package is being built. Microsoft recommends copying an MSI or MSP package to the share using the **MSIEXEC** command.

Use the **MSIEXEC** command with the **/a** (administrative installation option) parameter for MSI packages and the **/p** (apply an update) parameter for MSP packages. For example, using Office 2003 Standard Edition, from a command prompt, you would issue the following command, assuming that D: is your CD-ROM drive containing the Office installation media:

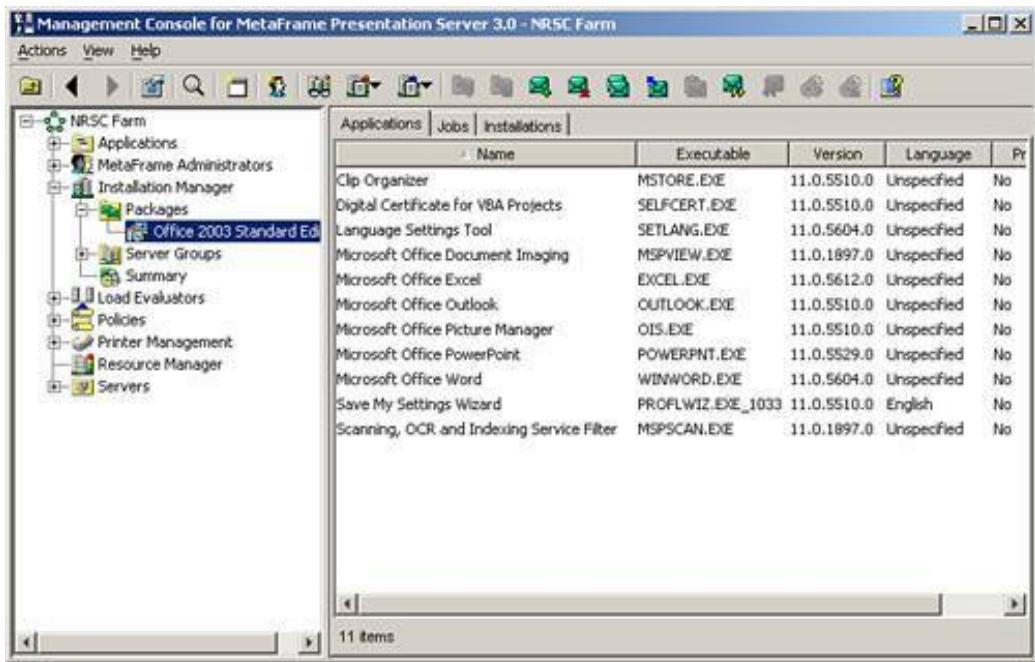
```
msiexec /a d:\std11.msi
```

Although it may appear that Office is actually being installed at this point, it is not. MSIEXEC is preparing Office in the designated share point so that a centralized, automatic installation can be performed.

4. Add the package to Installation Manager. The package must be added to Installation Manager before it can be deployed. An added package is listed under the Packages object in the Management Console, and clicking a specific package shows additional details about the applications available within the package, as shown in [Figure 11.2](#). You can easily add a package by right-clicking the Packages object, or selecting Installation Manager Packages from the Actions menu and then choosing Add Package.

Figure 11.2. Packages must be added to Installation Manager before they can be deployed to target servers.

[\[View full size image\]](#)



When you are adding or editing a package, the specific property information displayed depends on the type of package. For example, the properties for an MSI package allow you to specify one or more transform files, which customize the way the package installation will be performed. You can also define additional command-line options for the install and uninstall of the package. An ADF package does not have these additional configuration options available to it.

## Note

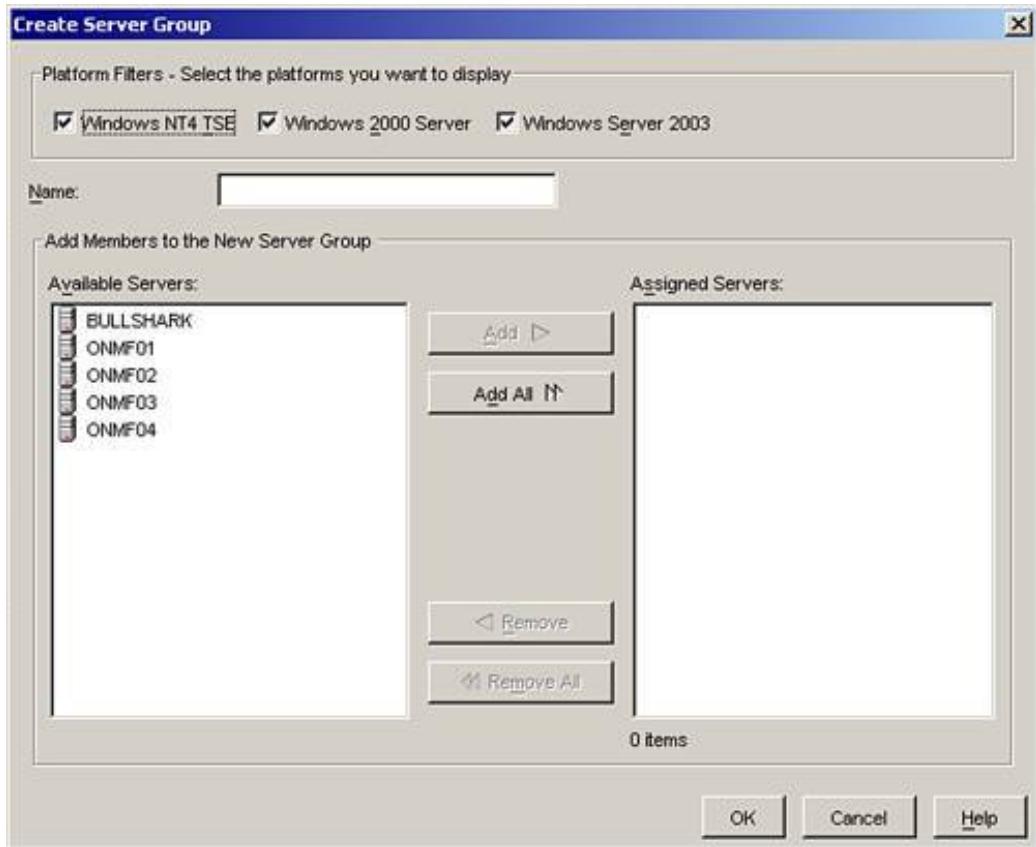
As part of its Office Resource Kit, Microsoft provides the Microsoft Office 2003 Custom Installation Wizard. This tool allows you to create a transform file for Office 2003, predefining a number of installation options that further streamline the installation of the Office 2003 package.

5. Create any required server groups. Server groups simplify deployments by allowing you to easily direct a package to multiple servers. A common server group configuration has all Windows 2003 Terminal Servers in one group and all Windows 2000 Terminal Servers in another. When grouped together, they are treated as a single entity for the purpose of application deployment.

When creating or editing a server group, you are presented with a dialog box that has all available servers matching the platform filters listed across the top, as shown in [Figure 11.3](#). Servers belonging to different platforms can reside in the same server group.

Figure 11.3. You manage the list of available servers that are displayed by selecting the desired platform filters.

[\[View full size image\]](#)



6. Create any required package groups. If the application you are deploying consists of multiple packages, you can group these packages into a single package group, assign an installation order for the packages, and then deploy it as a single object entity instead of having to schedule each package individually.

Right-clicking on the Packages object and selecting Create Package Group begins this process. Three tabs of information are available when you are creating or editing a package group.

On the Package Group tab, you select from the list of available packages to add to your package group. You can nest package groups within other package groups if desired. A package group can also consist of different package formats. You can quickly add packages to an existing package group simply by dragging and dropping them on top of the package group.

When more than one package belongs to a package group, you order the packages for deployment on the Install Sequence tab.

The final tab is Network Account. On this tab, you can override the default account and/or network share point that you defined when configuring Installation Manager.

7. Schedule the package deployment. The application is finally ready to be deployed to the target servers. Details on scheduling a package deployment are discussed in the next section of this chapter.
8. Monitor the status of a package deployment. Installation Manager allows you to monitor the status of a deployed application package. Details are reviewed in the "[Monitor the Status of a Package Deployment](#)" section of this chapter.
9. Schedule a package uninstall. After a package has been successfully installed, you then have the

option of creating an uninstall job to remove that program if desired.

By right-clicking an installed package or package group, you can select the Uninstall Package menu option. The Uninstall Job Scheduling Wizard is identical to the one you use to create a package installation (including scheduling options), except that the list of available servers shows only those servers that have the package installed. If a package is no longer installed on at least one server, the Uninstall option is automatically removed for the given package.

## Caution

If you have created an ADF package for an unattended installation using the Add Unattended Program option, you will not have the option to uninstall this program through Installation Manager.

Also, if an unattended Windows Installer (.MSI) installation is performed, uninstalling the package using Installation Manager does not remove application files (.dll, .ocx, and so on) stored in the SYSTEM32 folder.

Next, we look at the scheduling, monitoring, and deployment tasks in more detail.

## Note

You can view the packages that have been installed on a given server simply by highlighting the server in the Manager Console and selecting the Installed Packages tab from the right pane.

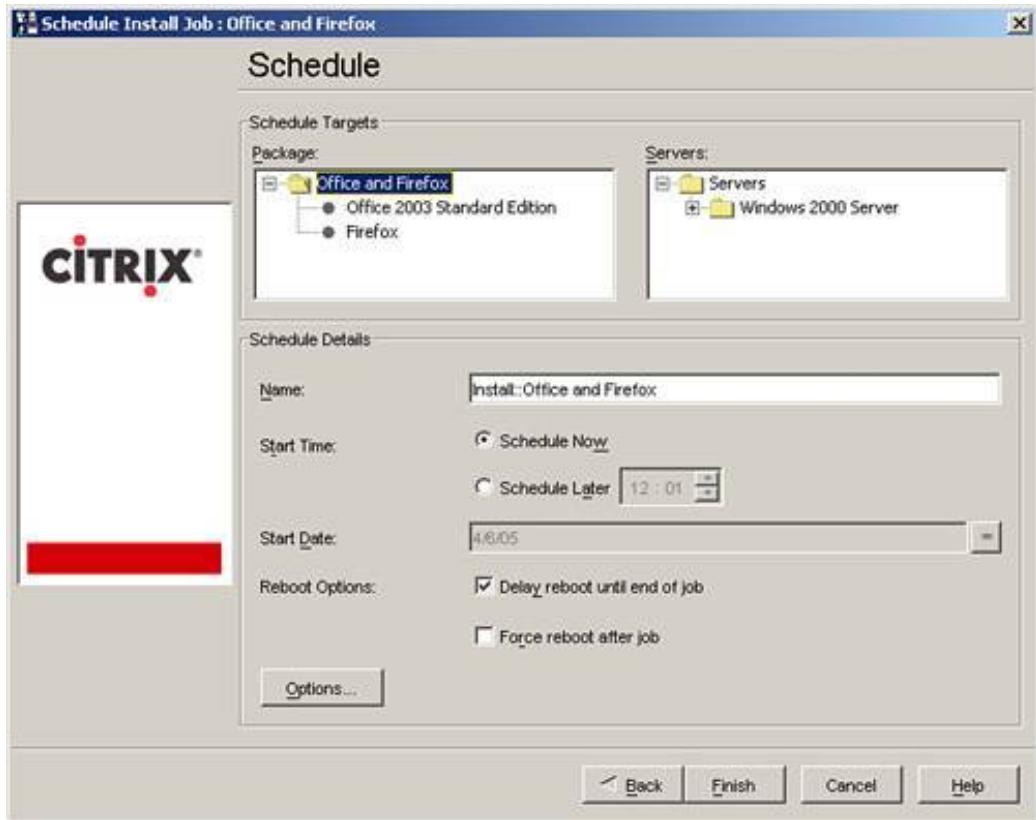
## Schedule the Package Deployment

To schedule package deployments, right-click the package or package group and select the Install option. Regardless of whether you've selected a package group or a package, the same Schedule Install Job Wizard appears. The steps to deploying a package are as follows:

1. Select the servers and/or server groups onto which the package (or package group) is going to be deployed.
2. Schedule the package or package group for deployment. The Schedule dialog box (see [Figure 11.4](#)) shows the packages you are scheduling and the target servers that will receive the packages. If you chose a server group, you can expand the server group folder to view individual servers.

Figure 11.4. Package deployments can be scheduled to begin immediately or at any time in the future.

[\[View full size image\]](#)



You can schedule a deployment immediately or for any date/time (time is in 24-hour format) in the future. If you are deploying a package group, you can select multiple calendar dates. Multiple dates can be chosen to accommodate the fact that a package group installation may be quite large and cannot be completed within a single maintenance window.

When a package group is being deployed, the Options button is visible. Clicking Options opens a small dialog box where you can define the installation window for the package. For example, you could define a window from 11 p.m. (23:00) to 4 a.m. (04:00) when a package group could be deployed. If all servers have not received the package group by the time the maintenance window closes, any deployments currently in progress will complete, but no new deployments of the package group will be started until the next deployment date is reached. If only a single date was selected for the deployment, the package group will not be deployed to all servers. If the package deployment begins again on another date, it will skip over any servers that already have received this version of the package and continue where the last maintenance window left off.

Two options are available for server reboots. When you are deploying a package group, the option labeled Delay Reboot Until End of Job is enabled and selected by default. When it is selected, Installation Manager prevents individual packages in the package group from initiating a reboot until the last package installation is complete.

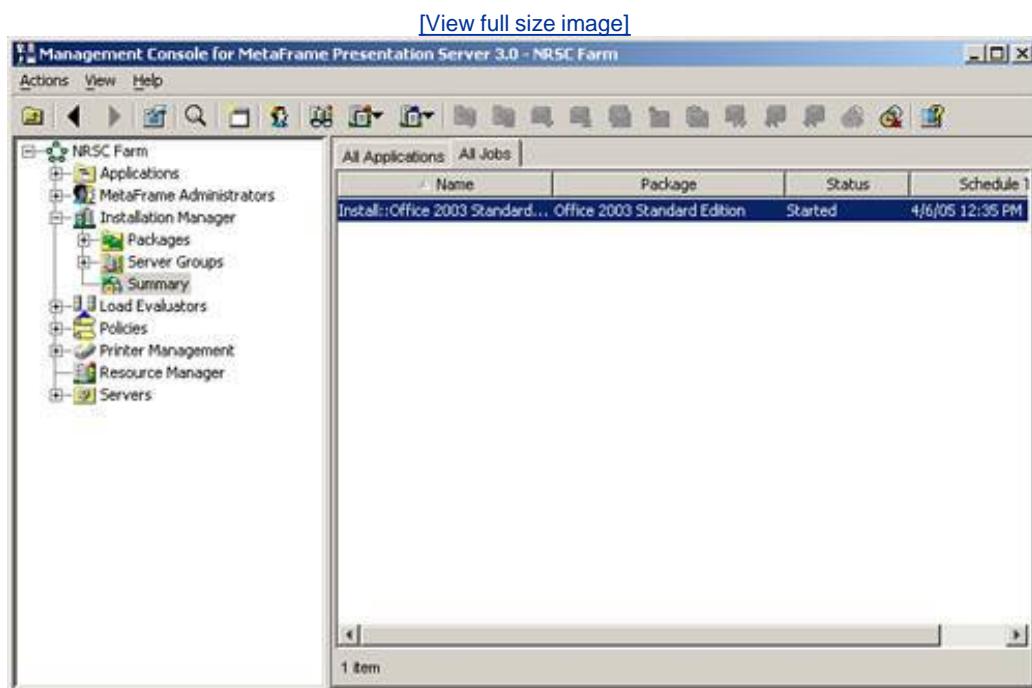
The Force Reboot After Job option is available whether a package or package group is being deployed. When it is selected, the target server is rebooted whether or not the package requires it. Citrix recommends that this option always be enabled to ensure a clean package deployment. If this option is not selected, the server will not reboot unless the package explicitly initiates it.

3. Click Finish to create the package installation job. If the job is scheduled to start immediately, it will; otherwise, it will be assigned a pending status until the deployment time and date are reached.

## Monitor the Status of a Package Deployment

You can view the current state of a deployment by clicking the Installation Manager Summary object. In the right pane, you can view the list of applications and jobs. [Figure 11.5](#) shows the current state for a deployment of the Office package.

Figure 11.5. The status of all jobs can be viewed under the Summary object.



Right-clicking the job allows you to edit the job settings, delete the job, or view and edit the properties for the job, including viewing more detailed information on the status of the deployment.

After the package installation is complete, the status will reflect either success or failure. By clicking the Job Details button, you can view the detailed log information for the package installation. This information can aid in determining what may have caused a package to fail.

The location of the log file on the target server depends on the package deployed. For an MSI package, the log file can be found by default in

<Citrix Install Dir>\Installer\Logs\Jobxxxx.log

<Citrix Install Dir> points to the location where MetaFrame Presentation Server is installed. By default, this is C:\Program Files\Citrix.

For an ADF package, the log file is located in

%SystemRoot%\Program Files\Citrix\Installer\against.log

## Tip

You can also access jobs for a specific package by selecting the package under the Packages object and then viewing the Jobs tab. Right-clicking a job allows you to access the same job details found under the Summary object.

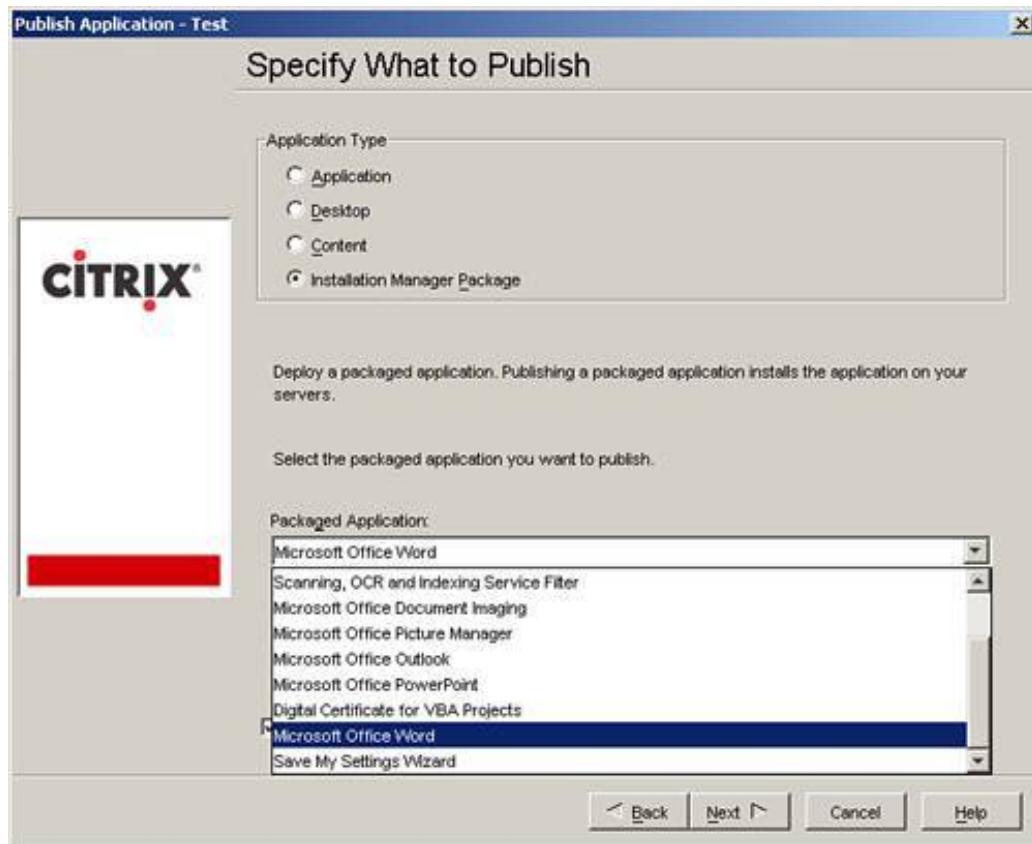
## Deploy a Packaged Application Using Application Publishing

Another method of scheduling the deployment of an application is through the Application Publishing Wizard. This approach combines the task of scheduling the deployment of a packaged application with the publishing of the application. Just as with standard application package deployment, before deploying a package through the Application Publishing Wizard, you must add it to Installation Manager. After you have added the package, you can deploy and publish the application as follows:

1. Within the Management Console, right-click the Applications object and select Publish Application, or choose New, Published Application from the Action menu.
2. When prompted for the application type, you need to choose Installation Manager Package and then choose the specific application from the Packaged Application drop-down list (see [Figure 11.6](#)). Notice that this matches the list of applications that exist within the MSI file for Office 2003 that we added to IM earlier in this chapter.

Figure 11.6. You can publish individual applications stored within application packages by using the Application Publishing Wizard.

[\[View full size image\]](#)



## Note

Applications packaged in ADF packages created using an unattended installation or a file copy do *not* appear in the Packaged Application list.

3. The remainder of the wizard prompts are identical to those for publishing a standard application, which was discussed in [Chapter 10](#). There is one thing you should note. When choosing the servers where you want to publish the application, do not specify the location where the application resides; instead, just leave this information blank. The application will automatically be located on the host server when requested by a user.
4. You will automatically go to the Schedule Install Job screen, where you specify when the job should be scheduled for deployment.

## Tip

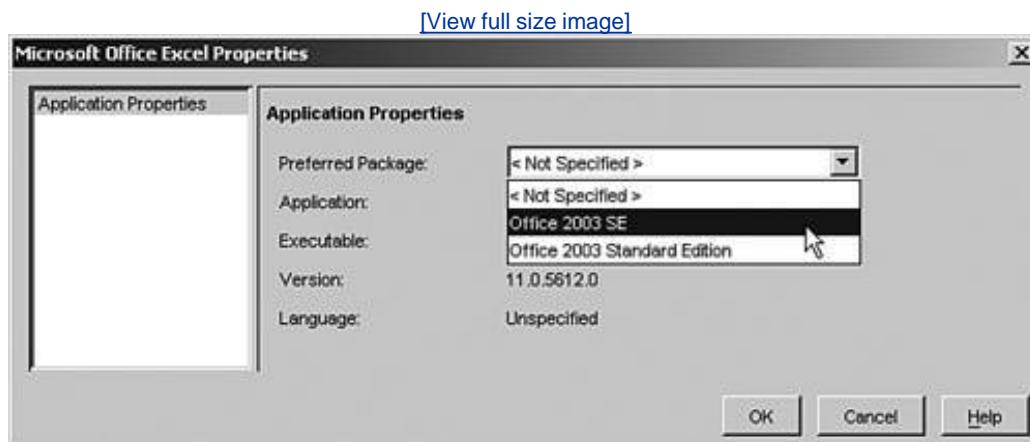
Until the application deployment is complete, the published application will *not* be available for use. You can enter query farm /app at a MetaFrame server's command prompt both before and after the deployment is complete to quickly confirm the availability of the published application.

## Assign a Preferred Application Package

Because an application can reside in multiple MSI, MSP, or ADF files, if you're going to be deploying applications using the Application Publishing Wizard, you should define the preferred package for that application so that IM knows what package to use when deploying the application to a given server.

You choose the preferred package by first selecting a package containing the appropriate application under the Packages object. Then, in the right pane, select the Applications tab, find the application, then right-click, and choose Properties. For the Preferred Package drop-down list box, choose the package that you would like to designate as the preferred package (see [Figure 11.7](#)). This package is then automatically used when a user selects the application, and it must be installed by Installation Manager.

Figure 11.7. Choose the preferred package for an application from the drop-down list box.



## Managing Packages from a Command Prompt

Besides the basic published application management tasks that can be performed using the [APPUTIL](#) command-line utility, this tool also allows an administrator to perform some simple package deployment tasks directly from a command prompt.

[APPUTIL](#) supports the following package deployment-related tasks:

- Add a server to the list of configured servers for a published application. If this application is publishing an Installation Manager application, the associated package is automatically installed on the MetaFrame server. The following command performs this task:

```
APPUTIL /i <app ID> <server name>
```

The app ID is not the friendly name for the application. You must run [APPUTIL /q](#) to find the app ID that corresponds to a given published application.

- Remove a server from the list of configured servers for a published application. [APPUTIL /u <app ID> <server name>](#) removes the server from the list, but it does *not* initiate the uninstall of the corresponding package from the server.
- Query the list of packages and package groups defined in the farm. Running the command

`APPUTIL /qp` returns the package ID, type, and description of the packages and package groups.

- Query the current state of a running job. You require the job ID for the given job in order to query its status. If a job was initiated from within the IM, there is no way of retrieving the associated job ID, but if you initiated a job from the command prompt, you can use the job ID output from that to query the current state. The syntax of the command is

```
APPUTIL /qj <job ID>
```

- Schedule the immediate installation of a package. The syntax is

```
APPUTIL /ip <package or package group ID> <server name> [REBOOT]
```

When the `REBOOT` parameter is included, the server is forced to reboot after the package or package group installation is complete.

This command does not allow you to access the scheduling features of Installation Manager. When a package deployment is initiated using this command, it begins immediately.

Schedule the *immediate* uninstall of a package. The syntax is nearly identical to the `/ip` parameter:

```
APPUTIL /up <package or package group ID> <server name> [REBOOT]
```

## Alert

Understand the syntax of the [APPUTIL](#) command and what tasks can and cannot be performed using this tool.

 PREV

NEXT 

# Creating ADF Packages Using the Packager Utility

The final task to review in this chapter is the creation of ADF packages. As we already mentioned, Citrix's Packager utility can be used to create packages for deployment when an MSI package does not already exist for an application. In this section, we use the increasingly popular Mozilla Firefox web browser to demonstrate how an ADF package can be created.

The Packager is a wizard-driven program that creates an ADF package by recording the changes made to a server when an application or software component is installed. This information and the necessary files are stored together within the ADF package for deployment to target servers. Any type of software that can be installed on a MetaFrame server can be deployed in an ADF package.

## Alert

The Packager creates only ADF packages. It does not create MSI or MSP packages.

## Packager Components and Terminology

You need to be able to identify and understand the function of the main components of the Packager application and ADF packages:

- Project Before you can build an ADF package, you must create an associated project that contains the intermediate files and information necessary to build the package. Details on what can be added to a project are discussed later in this section.

When a project is created, a subfolder is created underneath the Packager folder with the name of the project. The files and information for the project are maintained here. The default location for this is

`%ProgramFiles%\Citrix\IM\Packager\Projects\<Project Name>`

The following files are most commonly found in the project folder:

- Record log file This file, named `<Project Name>.ael`, contains the information captured during an application installation recording session. The data in this log is used to generate the ADF file. If the package was generated using something other than installation recording, this file will not exist.
- Project information file This binary file, named `<Project Name>.aep`, contains information on the properties of the project such as name, description, and target operating system.
- Project creation log file When the project is being analyzed and the ADF package created, a log file is generated. This file, named `<Project Name>_log.txt`, contains

information on the status of the creation process. This log file is stored in plain-text format.

- **ADF Package** After gathering all the necessary information for a project, you can build an ADF package. This package contains the information that allows Installation Manager to deploy and install the application on the target servers. The built package is located in the folder <Project Name>\PkgSrc. The type of package created dictates what information is found in this folder.
- **ADF File** As part of the package creation, an ADF file is generated. It contains all the Registry, environment variable, and file changes necessary to install the software. The final ADF file is built from the intermediate record log file (\*.ael) found in the project folder. The ADF file, named <Project Name>.wfs, is placed into the actual deployment folder for the package. This is typically the network share point for Installation Manager. This file is maintained in plain-text format.
- **Application Compatibility Scripts** Application compatibility scripts are used to ensure that legacy Windows-based applications function properly in a MetaFrame environment. Often these applications are designed as single-user applications and don't implicitly provide support for multiple concurrent user sessions. Citrix provides these compatibility scripts for many of the most commonly deployed legacy applications. The scripts available for inclusion can be found in the following folder:

%ProgramFiles%\Citrix\IM\Packager\appcompat

Note that application compatibility scripts are not required in all circumstances. Only when deploying a legacy application that does not natively understand a MetaFrame server configuration do you need to consider the use of these types of scripts.

## Preparing for ADF Package Creation

Before you begin the creation of an ADF package, you need to ensure the following:

- The Package Server meets the requirements outlined in the "[Components of Installation Manager](#)" section earlier in this chapter.
- No other applications are currently running, and only standard server services are currently active. You need to minimize the chances of information that is not directly related to the application installation from accidentally being captured during the installation recording.
- No other users (including administrators) are currently logged on to the server.
- You have all the required installation media for the application you want to package.
- You have defined the network share location and package management server. You can specify this information in the Packager, allowing it to directly build packages to the central network share and update the package management server with information of the new package's availability.

After verifying these points, you are ready to begin creating your ADF packages.

## Package Creation Using the Packaging Wizards

You either can create an ADF package using the various packaging wizards or create them manually. Let's first review the automated creation of packages using the wizards and then look briefly at the same process when performed manually.

Unlike other components of MetaFrame, which are all accessed through the Management Console, the Packager is a standalone application and is accessed through the Start menu under

Programs, Citrix MetaFrame Presentation Server, Installation Manager, Packager

Unless you have selected not to show the startup dialog box, every time you start the Packager, you are presented with the dialog box prompting you to open an existing package or create a new one using the Project Wizard. Selecting Create a New Project starts the Project Wizard. You can also start the Project Wizard from the File menu.

When the Project Wizard opens, you need to select the type of project you want to create. The three choices are

- Package an Installation Recording Choose this wizard when an application setup program prompts you for choices during the setup. Most programs that do not provide an MSI package fall into this category. The Firefox installation uses this wizard. The Packager runs in the background and records the application installation. After the installation is complete, the Packager will create the ADF package from the recorded information.

## Alert

An ADF package can contain only one installation recording. If you have multiple recordings, you need to package them independently and then deploy them as a package group through Installation Manager.

- Package an Unattended Program (Service Pack, and so on) Use this wizard when the application setup program does not prompt you for information (it performs a silent or unattended installation). Service packs and application updates are the most common applications to package with this wizard selection. When a package of this type is deployed through Installation Manager, an associated uninstall is not available.
- Package Selected Files Choose this wizard when you want to deploy specific files or folders. No application installation is performed; files are just delivered through the generated package. Configuration files and individual files that update a custom application are common examples that you would package using this wizard.

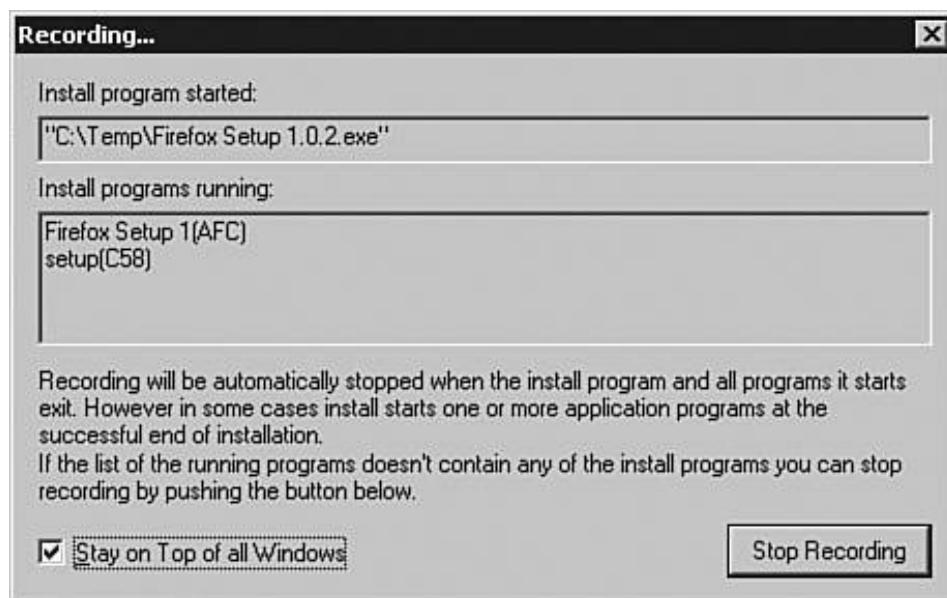
## Packaging Using the Installation Recording Wizard

Packaging an installation recording is one of the most common wizard tasks when creating ADF packages. We use the Firefox application to demonstrate how this type of package is created. The following steps summarize creation of a package using an installation recording:

1. Choose the Package an Installation Recording Wizard and provide a name for the new project when prompted.
2. Provide the full path to the installation program. This can be a UNC path or a path containing a Windows drive letter. If special command-line parameters are required, you can add them in the space provided on this screen.

3. (Optional) The step is necessary only if the application requires a special application compatibility script. If you choose to include a compatibility script, click the Find Script button to list all the scripts Citrix provides. Choose a script, if necessary, and click Next.
4. Choose a build location. This is the place where the completed package will be stored. If you want to automatically populate Installation Manager with your built package, make sure that you set the build location to correspond with the network share location; otherwise, you will have to manually copy the package to the network share.
5. Once recording begins and the installation program starts, the Recording window, shown in [Figure 11.8](#), appears with information on the installation programs currently running.

Figure 11.8. Once recording starts, the application setup program is run.



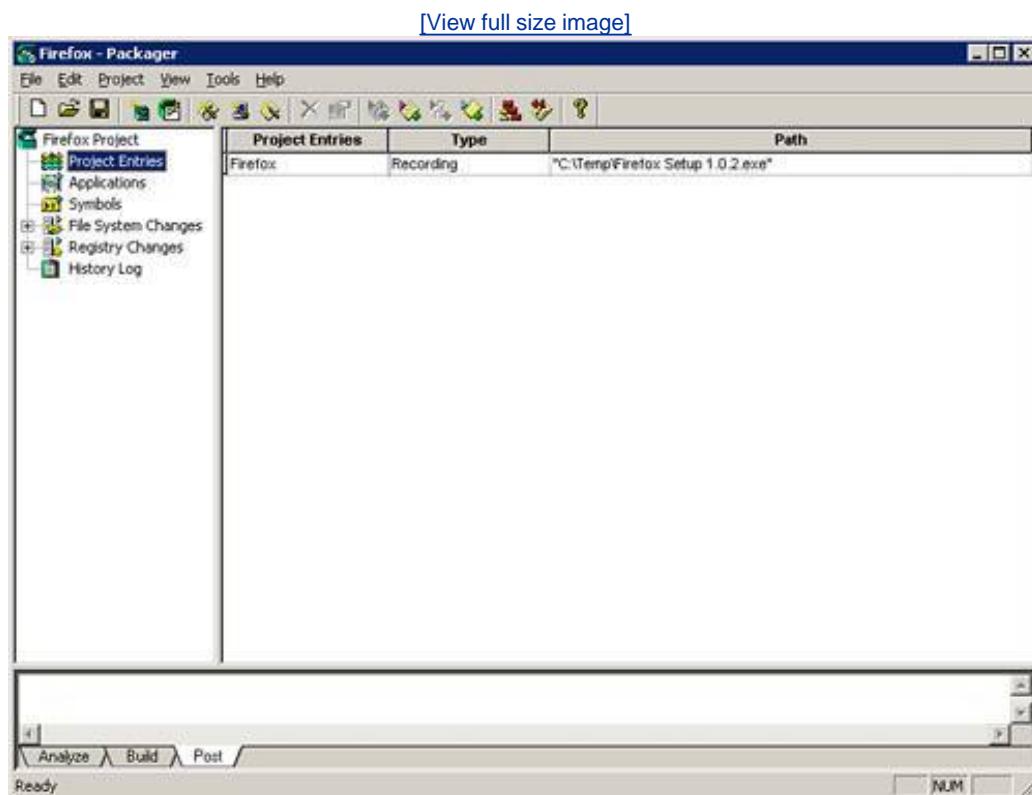
6. After the application installation is complete, click Done to stop the recording and continue.

If the application installation requests a restart, make sure that you have stopped the recording *before* you allow the restart to occur. The Packager recording will not continue after a restart.

7. After you complete the recording, the Packager analyzes the recording log and generates the ADF package for the application. If you defined the package management server during the configuration of the Packager, you will be prompted to select a Citrix server to post the package to. Clicking OK automatically updates Installation Manager with the availability of the new package. If the package already exists, then it will generate an error.

After the package build is complete, you are returned to the main window of the Packager, where you can review the new project information (see [Figure 11.9](#)). You can view any log information generated during the different stages of the package build by clicking the Analyze, Build, or Post tabs along the bottom of the window.

Figure 11.9. You can review the settings for the ADF package after the build is complete.



## Rolling Back Installation Recording Changes

After you have completed the recording of an application installation, Packager enables you to roll back those changes to preserve the initial state of the Package Server. The Rollback option is located under the Tools menu. When launched, it opens a dialog box listing the saved recording sessions. You have two options. You can either roll back the recording session, removing the installed application from the server, or you can delete the recording entry, accepting the installation as part of the new base configuration for the Package Server. After the recording information has been deleted, the application recording cannot be rolled back.

If you want to roll back multiple records, make certain that you perform the rollback in reverse order. That is, you roll back the newest entry first, followed by the second newest, and so on, until you reach the oldest entry remaining in the list.

### Note

Rolling back the changes or deleting the entry does not impact the saved project, nor the ADF package.

## Packaging Using the Package an Unattended Program Wizard

The Package an Unattended Program Wizard is similar to the Installation Recording Wizard except, as already discussed, this wizard is intended for use when an application can be deployed using a silent installation.

## Note

Batch scripts are also commonly deployed and executed using the Unattended Program Wizard. Registry changes can easily be scripted and deployed in this manner.

You package an unattended setup program as follows:

1. Launch Packager and start the Package an Unattended Program Wizard. Provide a name for the package when prompted and click Next.
2. Locate the installation file and provide any necessary command-line parameters to ensure that the program will install silently. For example, Windows 2000 Service Pack 4 can be deployed silently using the `/Q` parameter. Another parameter to use is `/Z`, which prevents the server from restarting after the service pack has been installed.
3. You define additional program options. One option allows you to enforce a reboot after the program installation completes. You can enforce the reboot here or when you deploy the application through Installation Manager. You also have the option of running the installation directly across the network from the source location, or you can configure the ADF package to copy the files into a temporary folder directly on the target server prior to beginning the installation. The default option is not to reboot and to copy the installation program locally. When files are copied locally, they are copied into the target server's temp directory and are not removed after the package deployment is complete.
4. The wizard completes with a request to set the build location and then asks for confirmation on the settings before the package is created. If a package management server has been configured for the Packager, you will be prompted to select a Citrix server to post the package to.

Unlike with the Installation Recording Wizard, the unattended installation program is not executed during the package build. The resulting ADF package is intended to deploy and launch the unintended installation program directly and not record specific installation information. It is for this reason that you are unable to generate an uninstall package for a package generated using the Unattended Program Wizard.

You can then deploy the resulting ADF package within Installation Manager, as discussed earlier in the chapter.

## Packaging Using the Package Selected Files Wizard

The final wizard-driven packaging option, Package Selected Files Wizard, allows you to create an ADF package containing selected files or folders that you want to deploy to the target servers. A common use for this type of package deployment is the upgrade of in-house or custom-developed applications. Often these types of application upgrades do not require the full installation of an application, but

involve simply updating one or more executables and associated DLLs. A package containing these files can be created and deployed quickly into the environment.

The Package Selected Files Wizard is straightforward, requiring only that you provide the files and/or folders to include in the package. It is extremely important to note that, by default, the source location from which the files/folders are retrieved is used as the target location for copying those files on the target servers.

For example, if you select a file called InventoryManager.exe, located in the \\onfp01\Home\ToddM\My Documents\Deploy folder, by default, the Packager defines the **TARGETDIR#** symbol to point to \\onfp01\Home (the share portion), while the target folder itself would be \ToddM\My Documents\Deploy. When a network source location is selected, a warning message is automatically generated, as shown in [Figure 11.10](#). This message reminds you to ensure the **TARGETDIR#** symbol is properly updated to avoid the situation in which the source files are copied back to the same network share.

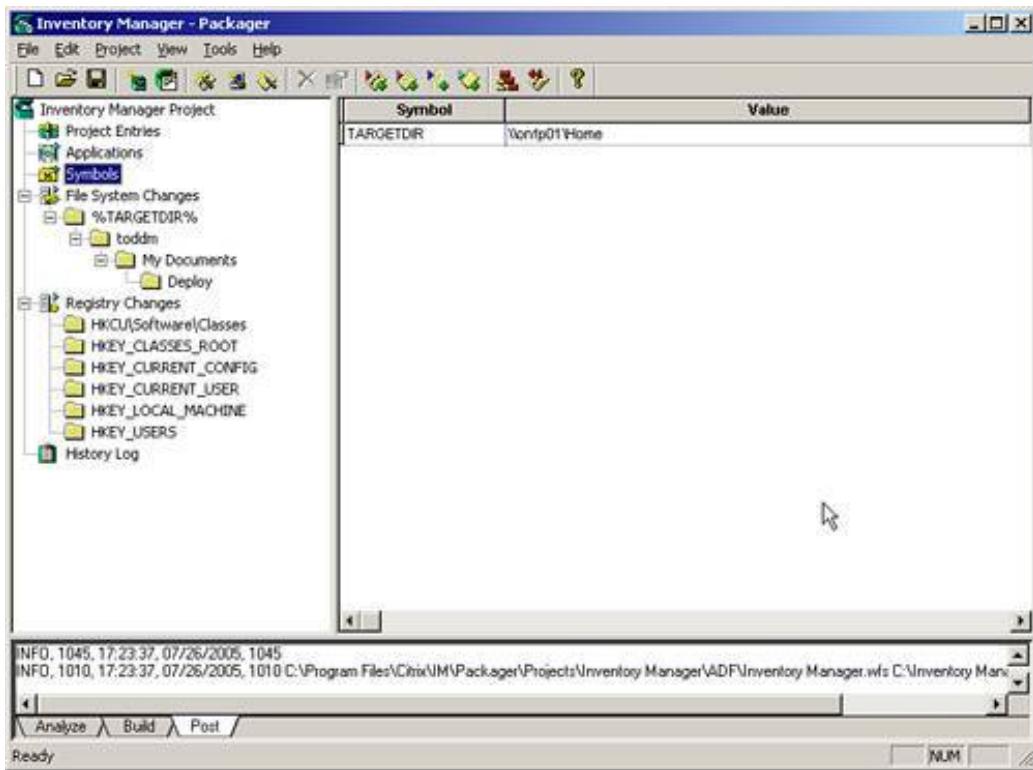
Figure 11.10. If the source location is on a network share, the Packager will generate a warning message reminding you to update the **TARGETDIR#** symbol.



You should either locate the files on the Packager server in the exact location where you would like them to be deployed on the target servers, or create the desired structure on the network and update the **TARGETDIR#** symbol after you have created the package. [Figure 11.11](#) shows where the **TARGETDIR#** symbol is found for the given package and the default value corresponding to the example described above.

Figure 11.11. The **TARGETDIR** symbol contains the path to the network share point when a network source location is being used.

[\[View full size image\]](#)



## Note

When configuring files for Package creation, I prefer to copy the desired files from a network share location into the exact folder that will be the destination folder on the client machines. The assumption is that any necessary testing should have been done with these files in the given location, ensuring that they will work as desired on the other MetaFrame servers. This is a personal preference, but one that has been reliable and consistent time and time again.

## ADF Package Review

Before you deploy an ADF package, it is a good idea to quickly review the File System Changes and Registry Changes (refer to [Figure 11.11](#)) to ensure that no other modifications (symbol or otherwise) should be made to the package.

## Manually Creating an ADF Package

You do not have to use the project wizards that Citrix provides to create an ADF package. Although you will find that the majority of the configuration steps are almost identical to those provided through the wizards, in some circumstances, there are additional advanced options available that you would otherwise not see when building a package using a wizard.

You create a package manually by selecting New Project from the File menu instead of Project Wizard. After you provide the name for the project, the basic project structure is generated and becomes visible. To this basic structure, you must add the desired package type, chosen from the Project menu.

You have four choices of information you can add to the project:

- Add Recording This option adds an installation recording to the project. You provide the name of the setup program to run and optionally include the specific hard drives to monitor from the Advanced settings. Local hard drives are included by default.

You also have the option to monitor only the Run Program and Programs It Starts. This controls to what extent the Packager monitors events in the system. When enabled the Packager monitors only the setup program and any child programs that are launched. When disabled the Packager will monitor everything running on the server. Under most circumstances, you do not need to deselect this setting unless a recording fails. Otherwise, you can enable it to see whether a component that was originally missed is required to build the package successfully.

After you click the Start button, the Recording dialog box appears, exactly the same as when you run the Installation Recording Wizard. The only difference is that the package is not automatically built. You must select Build Package from the Project menu to actually build the package.

- Add Compatibility Scripts This option opens a dialog box, allowing you to choose an application compatibility script to add to the current project.
- Add Unattended Program This option provides a single dialog box where the unattended program settings are defined. All the options available here are also found in the Unattended Program Wizard. When completed, the unattended program is added to the project, but the package itself is not created until you select Build Package from the Project menu.
- Add Files This selection allows you to provide a list of files and/or folders to add to the project, just as the Package Selected Files Wizard. As with the other options, the package itself must be manually built.

 PREV

NEXT 

## Exam Prep Questions

1. The components deployed using Installation Manager are referred to as \_\_\_\_\_.

A. target servers

B. network share points

C. installation software

D. packages

A1: Answer D is correct. The applications and other software components being deployed are referred to as packages. Answer A is incorrect. Target servers are the MetaFrame servers upon which packages are installed. Answer C is also incorrect. Installation software for an application is not necessarily in a format that could be deployed through Installation Manager. Answer B is incorrect because a network share point describes the location where software packages are stored after they are ready for deployment through IM.

2. Installation Manager supports three types of application packages. They are \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_. Citrix provides the Packager application, which allows you to create your own \_\_\_\_\_ packages for deployment.



A. MSI, MST, MSP, ADF



B. MSI, MSP, ADF, ADF



C. MSI, MSP, ADF, ADF



D. MSI, MST, ADF, MSP

- A2: Answer C is correct. Installation Manager allows you to deploy packages in the MSI, MSP, or ADF formats. You also can use the Packager application to create your own custom ADF packages. ADF is most often used to bundle programs or files that otherwise are not available in a supported format.

Answers A, B, and D are incorrect. Although IM supports the use of transform files (MST), they are used only in conjunction with MSI packages and alone cannot be used to deploy applications. The Packager program also supports only ADF package creation. Neither MSP nor MSI packages can be created with this tool.

3. One of the required components of Installation Manager is the \_\_\_\_\_. One of the tasks accomplished using this component is application deployment scheduling and execution.



A. Package Command Server



B. Package Management Server



C. Network Package Deployment Server



D. Target Server

- A3: Answer B is correct. Using the Package Management Server, an administrator can manage all aspects of Installation Manager, including application deployment scheduling and execution. Answers A and C represent fictitious component names, and D represents a valid component, just not the correct answer to the question.

4. Which options from the following list correctly describe a requirement for deploying Installation Manager? (Select all that apply.)

A. You must be running MetaFrame Presentation Server Enterprise Edition.

B. The desired Installation Manager components must be selected during the installation of MPS; otherwise, IM will not be available.

C. A MetaFrame Server running the required platform edition and the Management Console for MPS must be assigned the role of the package management server.

D. All MetaFrame servers that will be targets for deployed ADF packages must have the Packager component installed.

A4: Answers A and C are correct. Installation Manager is available only with the Enterprise Edition of MetaFrame, and to use Installation Manager, a server running the Enterprise Edition of MPS and the Management Console must also be assigned the package management server role. This does not exclude this server from also servicing regular user logon requests. This server can also be designated as a target server if desired.

Answers B and D are incorrect. When you install MPS 3.0 Enterprise Edition, all components of Installation Manager are installed by default. Also, target servers require only the Installer service and MPS Enterprise Edition to be a valid target server, regardless of the type of package being deployed. They do not require the Packager component, even though it is installed by default as part of the MPS Enterprise Edition.

5. The default network connection credentials and file sharing location defined for Installation Manager can be overridden in \_\_\_\_\_. (Select all that apply.)



A. server groups



B. application groups



C. package groups



D. user policies

- A5: Of the four choices, only answer C, package groups, is correct. When a package group is created, you can define alternate credentials and/or file share locations from which you can retrieve installation packages. The other three choices do not contain settings that pertain to the Installation Manager credentials or package locations.

You can modify the default connection credentials and file share location within the properties of the Installation Manager node in the Management Console.

6. An installation job that has been created requires a reboot to complete successfully. It was suggested that the Force Reboot After Install setting be chosen, but you want to ensure that the effects of this reboot have a minimal impact on the users. Choose the approach that would best achieve the desired goal.



A. Ensure that the Do Not Reboot Server If Any User Sessions Are Open option is enabled. This way, if users are on the server, a manual reboot can be performed.



B. Increase the Time Before Server Reboot option to the maximum value of 60 minutes and send reboot messages every 10 minutes.



C. Enable the Force Users to Log Off Before Installing option to ensure users are off the server before the reboot occurs.



D. Enable the Force Reboot After All Users Have Logged Off setting. This way, after the last user is off the server, it will automatically reboot before allowing new connections to the server.

A6: Of the four answers given, answer B most closely achieves the scenario you desire. It extends the reboot time to the maximum value of 60 minutes, giving users sufficient time to complete what they are doing and log off before the reboot occurs.

Answer A is incorrect because the Do Not Reboot Server If Any User Sessions Are Open setting does not override the Force Reboot After Install setting. Even with this option set, the server would still reboot once the time before reboot value had been reached, regardless of whether there were active users on the server.

Answer C is also incorrect. While forcing users off before the installation might help the install run more smoothly, because you cannot adjust the time interval before users are forced off, they are limited to the 15-minute window, which might not leave the users with enough time to complete their current tasks.

Answer D is incorrect because the option described does not exist.

7. Assuming that the configuration for Installation Manager is complete and the desired server groups already exist, which of the following best summarizes the tasks you would perform to deploy an individual MSI application package? (Select only one.)

- A. Copy the package to the network share point, add the package to Installation Manager, create the required package group, and schedule the package deployment.

- B. Copy the package to the network share point, add the package to Installation Manager, configure the account credentials and network share point for the package, and schedule the package deployment.

- C. Create the MSI package using the Packager utility, copy the package to the network share point, add the package to Installation Manager, create the required package group, and schedule the package deployment.

- D. Copy the package to the network share point, add the package to Installation Manager, and schedule the package deployment.

A7: Answer D is correct because it accurately describes the tasks you would perform to deploy an individual MSI package. Because you are interested only in deploying an individual package, you are not required to perform any package group configuration. This is why answer A, although technically not incorrect, is not the correct answer in this case.

Answer B is incorrect because you cannot define account credentials and a network share point for individual packages, only package groups.

Answer C is also incorrect because the Packager utility cannot create MSI packages, only ADF packages.

8. When copying an MSI or MSP installation package to a network share point, Microsoft recommends that you use the \_\_\_\_\_ command.

A. **MSIEXEC**

B. **MSIDEPLOY**

C. **MSIEXE**

D. **MSICOPY**

A8: Answer A is correct. **MSIEXEC** is actually the executable for the Windows installer and is used to configure the MSI package for a network installation. Answers B, C, and D are all incorrect. None of these choices represent valid executable names.

9. When you are scheduling the deployment of a package group, one of the available options allows you to define an installation window for the deployment. Choose the answer that best describes what happens if a package group deployment has not yet completed when the installation window end time is reached. (Select only one.)

A. The package group deployment that is currently in progress terminates and performs an automatic uninstall of all packages that make up that group. All servers with a completed deployment are not affected.

B. The package group deployment that is currently in progress completes. No new deployments are scheduled, and completed installations are not affected.

C. The package group deployment that is currently in progress terminates, and it and all the other servers that have completed their installation automatically roll back to their state prior to the start of the installation window. The deployment is not labeled a success unless all target servers are updated.

D. None of the above.

A9: Answer B is correct. If the maintenance window ends before the current installation is complete, it is allowed to finish, but no further deployments to any remaining target servers are initiated. These servers must either have a new deployment created for them, or additional schedule days need to be defined for the current job so that it can restart and complete the deployment. As a result, answer D is incorrect.

Answer A is incorrect because the in-progress deployment is allowed to complete and is not terminated. Similarly, Answer C is incorrect because completed package installations are never uninstalled by a package deployment unless specifically configured to do so.

10. You need to quickly retrieve a list of packages and package groups within a server farm. You open a command prompt and run the \_\_\_\_\_ command to retrieve this information.

A. `apputil /lp`

B. `apputil /qj`

C. `apputil /qp`

D. `apputil /q`

A10: Answer C is correct. The `/qp` (query package) parameter returns a list of all packages and package groups currently defined within Installation Manager. Answers A and D are both invalid commands, while Answer B (`/qj`) would return job information instead of package information.

11. Every ADF package has \_\_\_\_\_, which contains all the Registry, environment variable, and file change information required to deploy the package onto a target server. This file can be found in the network share point folder from which the ADF package is deployed to target servers. (Choose only one.)



A. an ADF file called <Project Name>.wfs



B. an ADF file called <Project Name>.ael



C. an ADF file called <Project Name>.aep



D. an ADF file called <Project Name>.adf

A11: Answer A is correct. In any ADF package folder on a network share point, you will find a file with a .wfs extension. This plain-text file contains the information required to deploy the package onto the target server.

Answer B is incorrect. Although there is a file with the .ael extension, it is the record log file and is located in the local package folder on the Packager server. This file is not found on the network share point.

Answer C is also incorrect. The file with the .aep extension is the binary project file that contains information about the package project that is editable from within the Packager application. This file is not part of the actual ADF package deployment.

Answer D is incorrect. There is no such thing as an .adf file created when generating an ADF package.

12. Which of the following are *not* valid project wizards in the Packager application? (Select all that apply.)



A. Package an Installation Recording



B. Package an MSI Recording



C. Package a Service Pack or Hotfix



D. Package Selected Files

A12: Answers B and C are correct. Neither are valid project wizards in the Packager application. MSI packages cannot be created using the ADF packager, and service packs or hotfixes can be packaged only using the Package an Unattended Program Wizard.

Answers A and D represent valid project wizards and so are not correct answers to this question.

13. When you are using the Package Selected Files Wizard, it is important to remember that the selected files \_\_\_\_\_. (Select all answers that would make this a truthful statement.)

- A. must not be MSI or MSP files.

- B. will be saved by default into the same folder path from which they were selected.

- C. will all be saved into the same location regardless of where they were selected from.

- D. should always be retrieved from a UNC path and not directly from a Windows drive letter.

A13: Of the four answers, only answer B creates a truthful statement. The path from which a file is selected is automatically used as the destination path on the target server.

Answer A is incorrect because MSI, MSP, or any other file type could be packaged and deployed using this wizard. The packaged file is not actually executed using this deployment method. It simply copies the file over the proper destination folder on the target server.

Answer C is incorrect. Files are not saved into the same folder unless they were in the same folder on the Package server.

D is incorrect. Files can be retrieved from either location. When using a network location as the source location you need to verify that the **TARGETDIR** symbol is pointing to the desired target location and is not going to accidentally overwrite the original source files.

 PREV

NEXT 

# 12. Printing

Terms you'll need to understand:

- Client printers
- Network printers
- Local printers
- MetaFrame universal printer driver
- Driver mappings
- Driver compatibility

Concepts and techniques you'll need to master:

- Replicating printer drivers
- Managing driver auto-replication
- Allowing only compatible printer drivers to be used in the farm
- Defining alternative driver mappings
- Troubleshooting client printer auto-creation issues
- Enabling and assigning a universal printer driver
- Importing network print servers
- Enforcing printer bandwidth restrictions
- Configuring network printer auto-creation

Because printing is such a critical part of most MetaFrame implementations, Citrix has put a large amount of effort into providing thorough support for all types of printing that may be found on a MetaFrame server. This support allows for the creation of an environment where the majority of users running applications on a MetaFrame server are able to print as seamlessly as they might through applications running on their local desktop computer. This chapter reviews the aspects of MetaFrame printer support that you need to understand in preparation for the exam.

# Supported Printer Types

The different types of printers supported by MetaFrame Presentation Server clients can be broken down into three main categories. They are client printers, network printers, and local printers.

## Client Printers

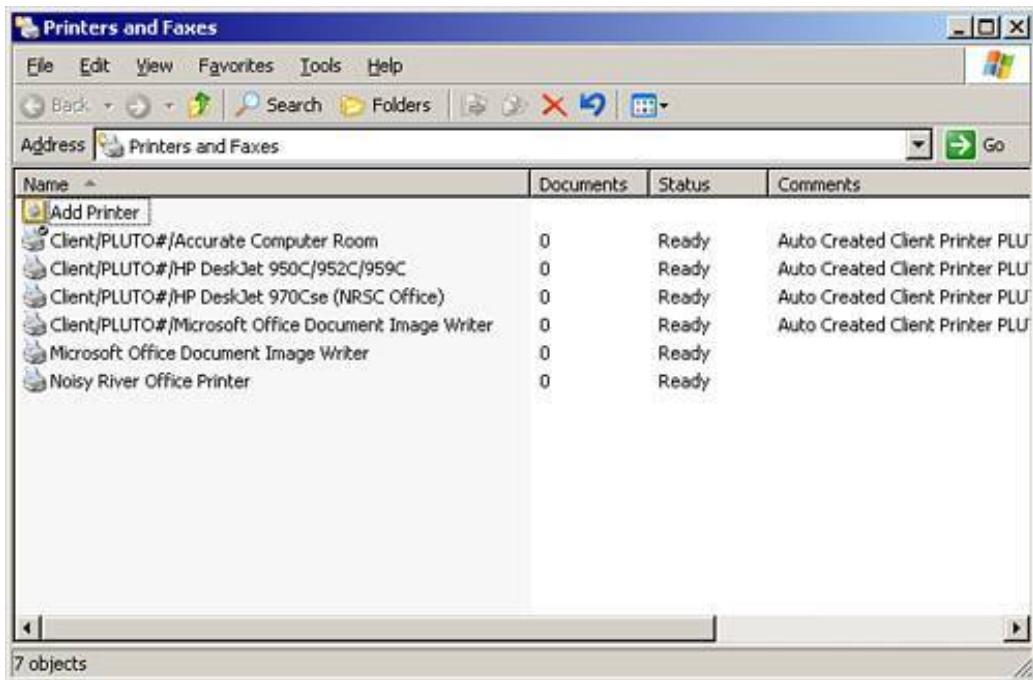
The *client printer* category represents any printer that is locally accessible from the client device. This includes

- Printers physically attached to a port on the client device. This is the only type of printer accessible through MetaFrame when using the DOS or Windows CE clients. Many thin-client devices also support locally attached printers through MetaFrame.
- Network-based printers accessed through a printer share or alternate means such as a TCP/IP printer port. When a network-based printer is set up on a local client device, it is considered to be a client printer.
- Virtual printers such as Adobe Acrobat, email, or fax printers. A virtual printer behaves like a printer, but the output is transparently directed to an alternative device or file instead of a printer. Note that not all types of virtual client printers are available within a MetaFrame client session.

A MetaFrame Presentation Server can be configured to automatically make client printers accessible from within a MetaFrame user session. When this is done, the client printer appears as a standard printer within the Printers folder in the MetaFrame session, as shown in [Figure 12.1](#).

Figure 12.1. MetaFrame can make client printers accessible from within a MetaFrame session.

[\[View full size image\]](#)



Names of client printers appear as follows:

Client/<clientname>/#<printername>

<clientname> represents the name of the MPS client, and <printername> is the name of the client printer. If the printer is a network-mapped printer, <printername> will include the name of the host print server and appear as follows:

Client/<clientname>#///<printservername>\<printername>

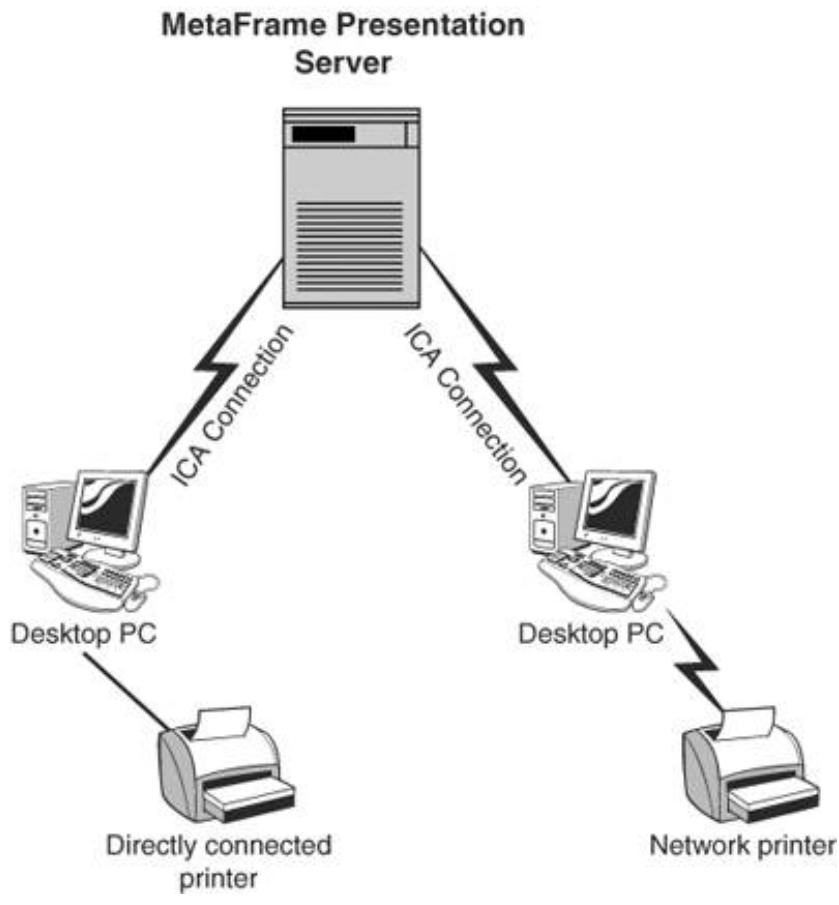
Also, note that the <clientname> is the MPS client name. Depending on how the client has been configured, this may or may not be the same as the hostname of the workstation. Having unique client names is important to ensuring that print jobs are directed to the correct client device.

## Caution

The MetaFrame Presentation Server Administrators Guide *incorrectly* states that client printers appear with the name #<clientname>/<printername>. In all versions of MetaFrame, client printers have always had the # added as a *suffix* to the client name.

[Figure 12.2](#) shows MPS clients with client printers in relation to a MetaFrame server. Both printers in this figure are considered to be client printers.

Figure 12.2. Any printer directly available on a MetaFrame client device is considered a client printer.



## Network Printers

A [network printer](#) is considered to be any printer that is connected to a print server and shared on a Windows network. Network printers are accessed within a MetaFrame session just as they would be from a local Windows desktop. A connection is made to the printer share, and jobs are sent to that queue for printing. As we discussed earlier, if a network printer is mapped on a local client device and then from a MetaFrame session, it is considered to be a client printer, not a network printer. Only when a shared network printer is mapped from within a MetaFrame session is it considered a network printer.

## Local Printers

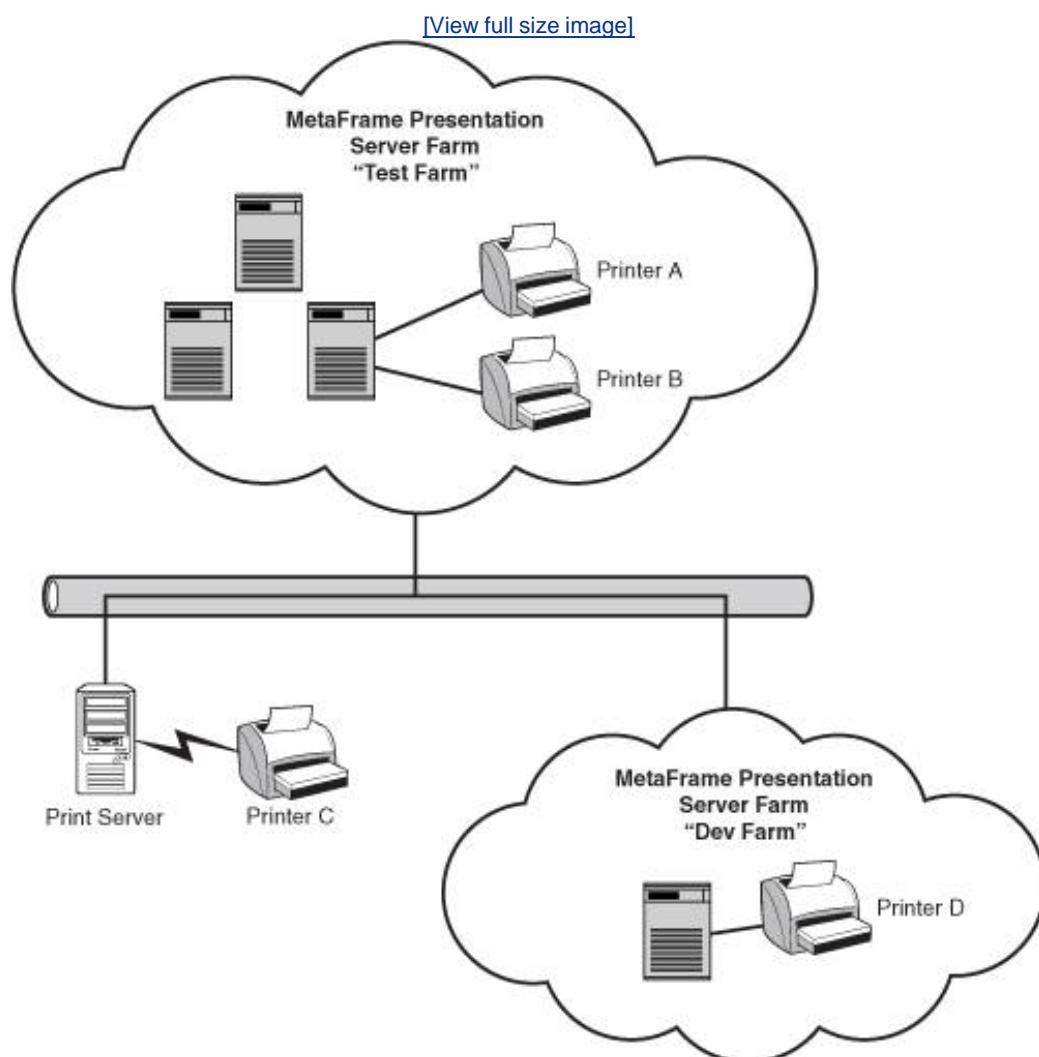
A printer falls into the [local printer](#) category when it is directly connected to any MetaFrame server within a server farm. *Locally connected* can mean one of two things:

- The printer is physically connected to a MetaFrame server through an LPT or USB port.
- A logical printer port has been configured to direct the print job to the remote queue for that printer. A TCP/IP printer port is one of the most common configurations, but third-party ports such as Lexmark or HP JetDirect can also be defined.

Referring to [Figure 12.3](#), the two printers (Printer A and Printer B) within the farm called Test Farm are considered local printers to that farm, and the printers connected to the print server (Printer C)

and the MPS server in the farm called Dev Farm (Printer D) would be considered network printers in relation to Test Farm. Similarly, Printer D would be a local printer to Dev Farm, and Printers A, B, and C would be network printers to Dev Farm.

Figure 12.3. A printer connected to any MetaFrame server within the same farm is considered a local printer.



Only printers connected to servers running MPS and belonging to the same farm fall into the local printer category.

### Alert

Understanding what differentiates a local printer from a network printer in an MPS 3.0 server farm is helpful. Only printers that are connected to MetaFrame servers in the same farm are considered to be local printers to that farm. All other printers are categorized as either network or client printers.

 PREV

NEXT 

# Printer Management Features in MetaFrame

Before reviewing how MetaFrame users configure and access the different categories of printers, we look at what printer-related management features are available.

As with most other areas of MPS, the management features for printing are located within the Management Console. Printer management options are actually available in two different parent nodes in the Management Console.

The first is the Printer Management node, found immediately under the root of the server farm. The second is found under the Servers node. When an individual server is selected in the Servers node, the right pane contains two printer-specific tabs: Printers and Printer Drivers.

## Note

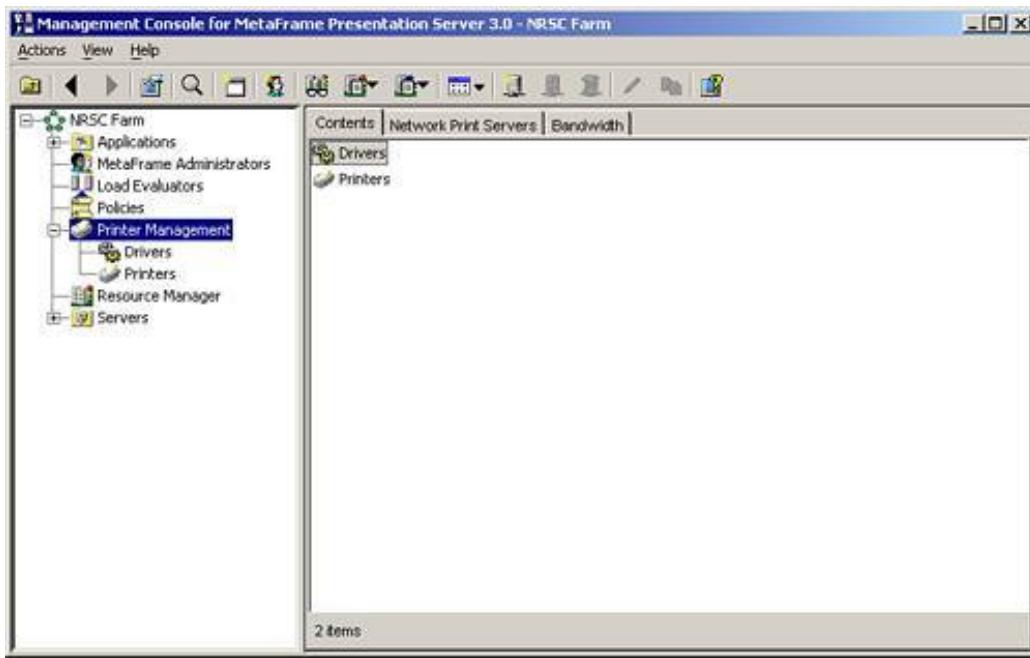
A number of printer management features can be administered through MetaFrame server policies. Details on policies were discussed in [Chapter 7](#), "MetaFrame Presentation Server Policy Management."

## The Printer Management Node

The Printer Management node enables you to control printer information for the entire farm. When the Printer Management node is selected, three tabs are available in the right pane: Contents, Network Print Servers, and Bandwidth (see [Figure 12.4](#)). Using these tabs, you can manage the various printer properties.

Figure 12.4. MetaFrame printer features are controlled within the Printer Management node.

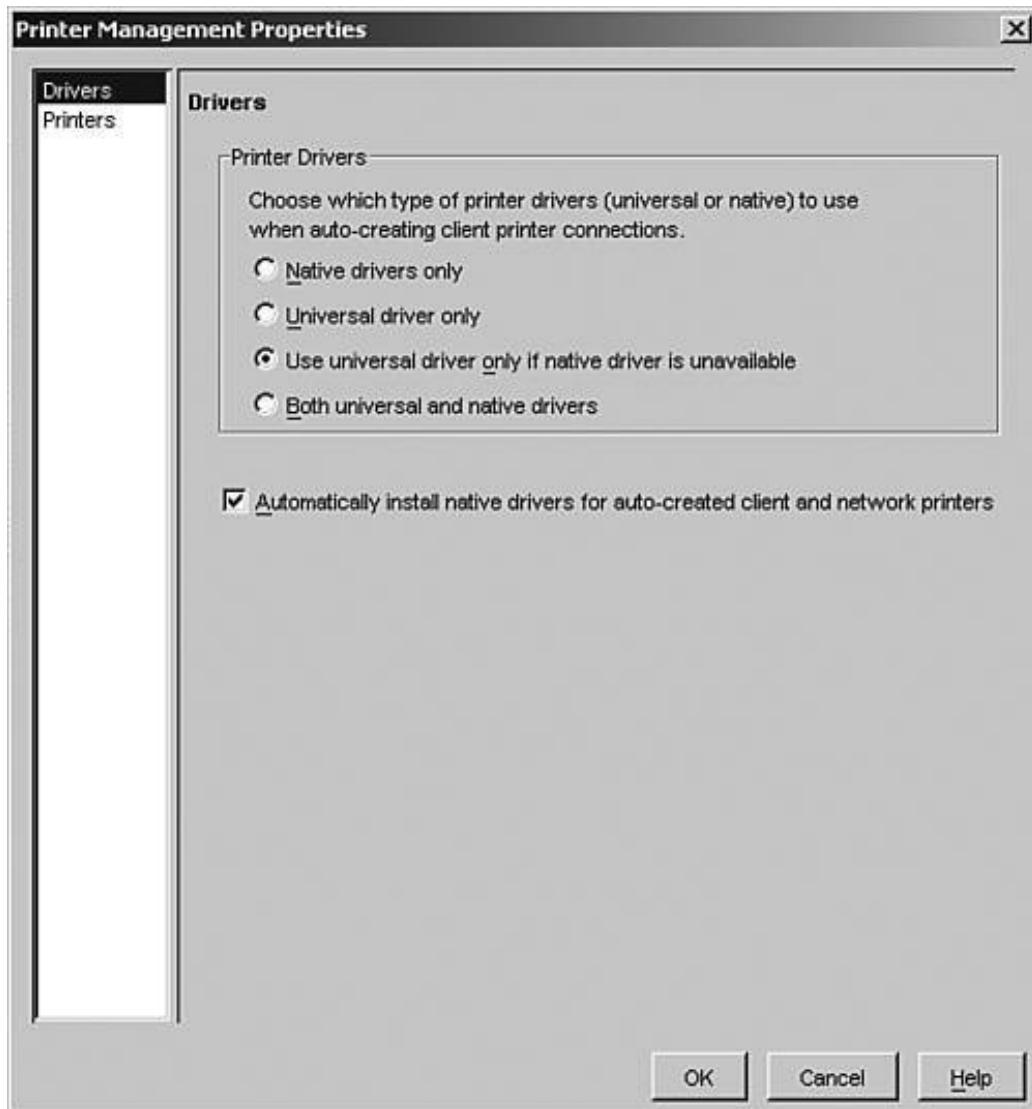
[\[View full size image\]](#)



You can also manipulate the properties for the Printer Management node. By selecting Properties from the Actions menu (or right-clicking on the Printer Management node and choosing Properties), you bring up the property page for Printer Management. Two settings of options are available: Drivers (shown in [Figure 12.5](#)) and Printers. The driver settings pertain to the way MetaFrame handles drivers for client printers, and the printer settings dictate how client and network printers are auto-created. Details on these settings are discussed later in this chapter. For now, we concentrate on reviewing the options for the three tabs pertaining to Printer Management.

Figure 12.5. The properties for Printer Management dictate the behavior of client printer drivers, client-mapped printers, and network-mapped printers.

[\[View full size image\]](#)



## Contents Tab

The Contents tab contains the same Drivers and Printers objects that are also visible when you expand the tree under the Printer Management node (refer to [Figure 12.4](#)). On the first of these, the Drivers node, you manage the printer drivers installed on any of the MetaFrame servers in the farm.

You can view the printer drivers available on any individual server in the farm or collectively for all servers simply by selecting the desired scope from the Server drop-down list box. You can also view the list of servers that have a particular driver installed simply by left-clicking on a driver name. All the servers with that driver appear in the far-right pane of the Management Console.

Note these four things about the Drivers node:

- Before a printer driver is visible in the Drivers node, it must be manually installed on at least one server in the farm. After installing it on one MetaFrame server, you can use driver replication to distribute it to all other servers in the farm. Driver installation and replication are discussed in the "[Printer Driver Management](#)" section later in this chapter.
- If a mixture of Windows 2000 and 2003 servers is running MPS in the same farm, the list of

available drivers is differentiated by platform version.

- MetaFrame automatically provides three generic universal printer drivers (UPD) that you can use instead of native printer drivers to provide client printing support. Normally, when a client connects, the server attempts to match the client printer driver with a server printer driver. If a matching native driver cannot be found, a suitable UPD is used instead. The three UPDs available support the Printer Control Language (PCL) 5c, PCL4, or PostScript (PS) printing languages. Specifically, the printer drivers are labeled

- HP Color LaserJet 4500 (MetaFrame PCL5c Universal Driver)
- HP Color LaserJet PS (MetaFrame PS Universal Driver)
- HP LaserJet Series II (MetaFrame PCL4 Universal Driver)

More specific details on the universal drivers and client printer mapping are given in the ["Printer Driver Management"](#) section of this chapter.

- Only printer drivers installed on MetaFrame servers in the farm can be viewed and managed through the Management Console. Printer drivers that have been installed on print servers not running MPS are not accessible.

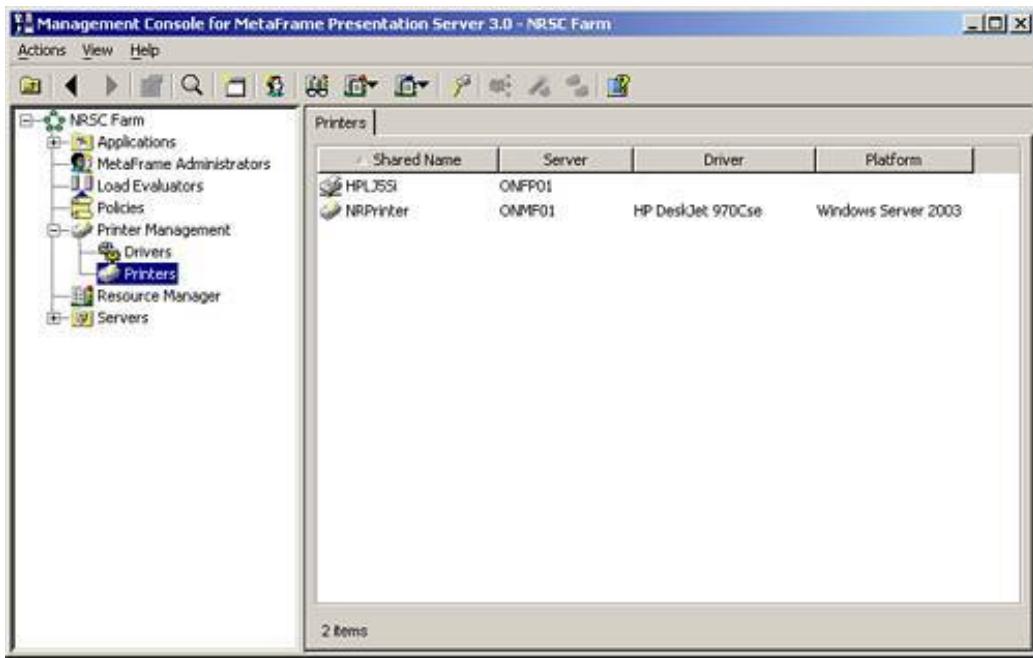
Besides the Drivers node, within the Contents tab, the Printers node is also accessible. When selected, this node displays all *printers* that can be configured in the server farm. Configuration tasks available include driver replication and defined auto-creation settings based on user credentials. Task details are discussed shortly. Before such tasks can be performed, printers must be added to the Printers node. Until printers have been added, this window appears empty. Configurable printers in the farm come from two possible sources:

- Any printers configured and shared on any MetaFrame server in the farm are automatically added to this node. These printers appear in the list showing the full printer name, host server name, driver name, and host operating system for the printer.
- Printers available on a standard Windows print server (not running MPS) can be added to the Printers node through the Network Print Servers tab (discussed in the next section). These printers appear in the list showing only the full printer name and host print server name.

[Figure 12.6](#) shows how printers appear coming from both of these sources. The first printer comes from the non-MetaFrame print server called ONFP01, and the second printer is shared off the MetaFrame server called ONMF01. Notice how driver and platform information is available only for the driver shared on ONMF01.

Figure 12.6. Any printers that can be configured in the server farm are listed in the Printers node.

[\[View full size image\]](#)



The specific configuration tasks available for these printers are dictated by the printer's source. To display the specific functions available, right-click a printer, or highlight it and choose Printer Management from the Actions menu.

Printers sourced from a MetaFrame server are fully configurable. You can choose these specific options:

- Replicate Drivers The printer driver can be replicated to any other MetaFrame server in the farm. This is an alternate method to replicating a driver from the Drivers tab. Either location performs the same function.
- Auto-creation Auto-creation allows the printer to be assigned automatically to a user when he or she logs on to a MetaFrame server in the farm.
- Copy Auto-creation Settings Auto-creation settings can be quickly replicated to other users or groups using this option.
- Client Printers When this option is defined, the printer is auto-created for DOS or CE-based users when they log on to a MetaFrame server.

A printer imported from a non-MPS print server supports all these options, with the exception of printer driver replication. A driver residing on a standard Windows print server cannot be directly replicated to a MetaFrame server. The driver must first be manually installed on at least one MetaFrame server before it can be replicated from the Drivers node, which we discussed earlier in this chapter.

Configuring printer auto-creation is discussed in the "[Printer Configuration](#)" section later in this chapter.

## Network Print Servers Tab

To access printers shared on non-MPS print servers, you must import these network print servers into the farm. You do this through the Network Print Servers tab. When you first create a server farm, this

tab is blank until you choose a print server to import. To import a print server, make sure the Printer Management node is selected and then choose Import Network Print Server from the Actions menu. The Import Network Print Server dialog box is then displayed.

You begin by providing the DNS name or IP address for the print server. Do not precede the name with the double backslash (\\\) commonly used to distinguish a NetBIOS name. For example, instead of entering \\ONFP01, simply enter **ONFP01**. The user credentials are optional, so you should enter them only if you want to retrieve printers for a certain type of user. When you omit the credentials, only those printers available to all users are imported.

After a print server has been imported, it appears in the Network Print Servers tab. Returning to the Printers node, you then see any printers that are accessible based on the credentials provided. Refer to [Figure 12.6](#) to see how an imported printer appears.

Besides the name of the print server, the Network Print Servers tab also displays the date that information was last updated from the server. This is an important point to note. The list of available printers from a network print server is not dynamically maintained in the Management Console. If any printer additions or deletions have been made on the print server, the changes will not be reflected in the Management Console until a *manual*/update is performed.

You initiate an update by highlighting the print server and choosing Update Network Print Server, either from the Actions menu or by right-clicking the print server and selecting from the context menu. The Last Updated time should change to reflect the latest information retrieval.

## Alert

Remember that changes to a network print server are not automatically reflected in the Management Console.

If you no longer want to manage printers on a particular print server, you can easily discard that server by highlighting it and choosing Discard Network Print Server from the Printer Management Actions menu. The print server and all associated printers from the Printers node are immediately removed from the Management Console.

## Bandwidth Tab

Bandwidth is the final tab in the Print Management node. Within this tab is a list of all MetaFrame servers in the farm and the current client printer bandwidth limit assigned to that server. This limit represents the maximum network bandwidth that will be assigned to *client* print jobs in each MPS connection.

It is very important to note that this bandwidth restriction applies *only* to client printers. Recall that client printers are printers that have been configured locally on an MPS client device and are made available to users through their MPS session. In other words, print jobs that must travel via ICA channels back to print queues on the client device are throttled through this bandwidth setting. The bandwidth setting has no effect on print jobs sent directly to other nonclient printers (network or local server) from within a MetaFrame session.

Bandwidth restrictions are applied on a per-server basis. You simply highlight the server within the Bandwidth tab and choose Edit from the Printer Management Actions menu. This opens the dialog box shown in [Figure 12.7](#). The default bandwidth is set to Unlimited, allowing print jobs to consume as

much bandwidth as is necessary to print the job as quickly as possible on the client device.

Figure 12.7. Unlimited bandwidth is allocated by default to all MetaFrame servers in the farm.



To limit the bandwidth, select the Limited radio button and enter the maximum bandwidth (in kilobits per second) that a print job can consume within a single MPS connection. You do not enter this value as a percentage, but as a hard value defining the upper limit on the connection. Contrary to what you may think, this value is enforced on a per-connection basis, not collectively for all users on the server.

It is very likely that you will need to test different values before you find the desired balance between user session performance and print job speed. Common starting values for testing are between 2 and 10 Kbps.

After defining bandwidth values on one MetaFrame server, you can quickly copy them to other servers in the farm simply by choosing Copy from the Printer Management Actions menu. When you do this, you are presented with a list of all servers in the farm. You simply choose one or more servers to be the target of the new bandwidth values.

## The Servers Node

Besides the Printer Management node, you can also view and manipulate printer information from within the Servers node. When the Servers node is highlighted, one of the four available tabs is labeled ICA Printer Bandwidth. This tab displays the exact same information as was found on the Bandwidth tab for the Printer Management node.

Selecting an individual server under the Servers node displays a large number of tabs, including the Printers and Printer Drivers tabs.

### Printers Tab

The Printers tab displays all the local printers that have been shared for that particular highlighted MetaFrame server. Only locally shared printers for the selected server are shown. If you right-click a printer or choose Printer Management from the Actions menu, you see that it displays the exact same configuration tasks available under the Printers node for Printer Management (discussed earlier in this chapter).

Although this Printers tab displays similar information to the Printer Management's Printers node, there are a couple of differences. First, only the locally shared printers for the currently highlighted server are visible. To view the printers belonging to another server, you must select that server. Second, you can view only network printers that have been imported from non-MPS print servers from the Print Management Printers node. These printers are not visible under the Servers node.

## Printer Drivers Tab

The Printer Drivers tab lists the printer drivers currently installed on the selected server. From this tab, you can also highlight a listed driver, and in the far-right pane, you will see a list of all other servers in the farm with that driver installed.

Unlike with the Printers tab, which shares the functionality available with the Printer Manager Printer node, the only task that you can perform from the Printer Drivers tab for a specific server is the replication of the driver to any other server in the farm. To carry out the other driver-related tasks such as auto-replication management or printer driver mappings, you must access the Drivers node under Printer Management. Printer driverrelated functions are discussed next.

 PREV

NEXT 

# Printer Driver Management

Even though MetaFrame supports what may at first appear to be a wide and confusing array of printing options for the end user, one common factor that does not change is the need to have a suitable printer driver available on a MetaFrame server before a user is able to send print jobs to the desired printer. MetaFrame supports a number of options for managing the replication and even substitution of printer drivers. In the following sections, we review all these management choices.

## Installing Printer Drivers

A couple of different methods exist for installing printer drivers on a MetaFrame server. The methods are summarized as follows:

- Install the printer driver using one of the standard Windows printer driver installation methods. This can include creating a local printer on a MetaFrame server using the familiar Add Printer Wizard. During the printer installation, the necessary driver is added to the MetaFrame server.

You can also manually add drivers to a server from the Drivers tab of the Print Server properties. Open Printers and Faxes on a Windows Server 2003 server (or Printers from a Windows 2000 server) and choose Server Properties from the File menu to access this dialog box. Here, you find the Drivers tab, where you can choose to add, delete, reinstall, or modify the driver properties.

- Use driver replication to deploy the driver to the desired MetaFrame server. When a printer driver has been installed on at least one MetaFrame server in the farm, you can use the driver replication feature to replicate the driver to any other MetaFrame server in the farm. This provides a fast and reliable method of adding printer drivers to all required MetaFrame servers without having to manually install the drivers on each server.

Automatically install a native printer driver during client or network printer auto-creation. MetaFrame supports the ability to automatically install a native Windows printer driver if a driver does not already exist for an automatically created client or network printer. This option is enabled by default and is found under the Drivers section of the Printer Management properties. It is important to note that this feature allows only the automatic installation of printer drivers that are natively supplied with Windows. Third-party or updated printer drivers must be manually installed and replicated. The automatic installation of native printer drivers is also performed only during the automatic creation of client or network printer connections. Printers that are mapped by other means such as logon scripts do not have native drivers automatically installed. Client and network auto-creation are discussed in the "[Printer Configuration](#)" section later in this chapter.

## Replicating Printer Drivers

To replicate a printer driver, highlight the desired driver from within the Management Console and choose Replicate Drivers from the Printer Management Actions menu (or from the context menu when right-clicking the driver). This opens the Replicate Driver dialog box, where you see the following information:

- Platform This is the version of Windows for which this printer driver is intended. Printer drivers are replicated only to servers running the matching platform version. This ensures driver compatibility.
- Server(s) This is the name of the server that will be the source for the driver replication. The driver information is taken from this server and used to replicate to the target MetaFrame servers. If the server choice Any was selected, it will appear here instead of a specific server name. Choosing Any causes MetaFrame to replicate the printer driver from any available server that has the driver installed.
- Driver This is the name of the printer driver that will be replicated.

In the middle of the Replicate Driver dialog box are two radio buttons from which you choose how the driver will be replicated. The default option is to replicate this printer driver to all other servers in the farm running the same Windows version and also to add this driver to the auto-replication list. Auto-replication is discussed in the next section.

The second option allows you to choose the desired target server for the replication. Only servers running the same platform version appear in the list. When specific servers are chosen as targets for replication, the operation is performed only once, and an auto-replication task is not created.

The final option on this screen is the check box that enables or disables overwriting existing drivers. By default, if a server already has a printer driver with the same name, it is not updated. Enabling this option forces the replacement of the printer driver, regardless of whether it exists or not. This option would normally be used if you were deploying an updated version of a printer driver or wanted to ensure a consistent driver version across all target MF servers.

## Auto-Replicating Printer Drivers

MPS allows you to configure the auto-replication of printer drivers to all MPS servers running the same Windows platform. Auto-replication ensures that all new servers added to the farm are automatically configured with the necessary drivers to support the end user's printing needs.

You manage auto-replication by highlighting the Drivers tab for Printer Management and choosing Auto-replication from the Actions menu. This opens the auto-replication dialog box, which shows all the drivers currently configured for replication (broken down by platform). From this dialog box, you are able to add or remove driver entries, but you are not able to directly edit an existing driver's settings. If you want to change the source server or the overwrite setting for a driver, you must delete and then re-add it.

You can set up a driver for auto-replication directly from this dialog box, or by choosing to replicate the driver either from the Drivers node for Print Management or the Printer Drivers tab for an individual server.

## Printer Driver Compatibility

Unfortunately, not all printer drivers are suitable (or desirable) for use in a MetaFrame environment. Some printer drivers can cause severe server issues such as a full system crash (blue screen of death STOP error), whereas others may just prove to be extremely slow or buggy. Whatever the reason, a mechanism must exist to ensure that these types of drivers can be prevented from operating on a MetaFrame server. This is why Citrix provided the Driver Compatibility feature, which allows an administrator to quickly control what printer drivers are and are not allowed to be used for auto-created client sessions.

You open the Driver Compatibility dialog box by selecting the Drivers node under Printer Management and selecting Compatibility from the Actions menu. By default, all printer drivers are permitted, but you can configure the farm to allow or restrict the use of specific drivers based on the options that you choose. These two options are available:

- Allow Only Drivers in the List This option blocks all client printer creation unless a client printer uses a driver that is specifically shown in the "allowed" list.
- Allow All Drivers Except Those in the List This is the default configuration, allowing all client printers to be automatically mapped unless the corresponding printer driver is included in the list.

To add a driver to the list, simply click the Add button and either type in the exact name of the client printer driver, or choose one from the list of drivers that have already been installed in the farm.

If the driver is currently not installed but you want to ensure that it will never be used, type in the exact driver name. Make sure that all spacing, punctuation, and capitalization match exactly; otherwise, MetaFrame cannot make a proper match. You can edit or delete an existing entry at any time by highlighting and clicking the appropriate button (Edit or Delete).

Whenever MetaFrame attempts to create a client printer, it first checks the include/exclude list and verifies the acceptance of the required driver before the client printer mapping is finalized.

## Note

The entries in the Driver Compatibility list have no impact on the auto-creation of network printers or the mapping of printers through logon scripts. If a network-based or local printer is causing server issues, it is advised that the auto-network mapping be terminated and the access to the offending printer's queue be restricted or eliminated to ensure users are not able to connect.

## Printer Driver Mapping

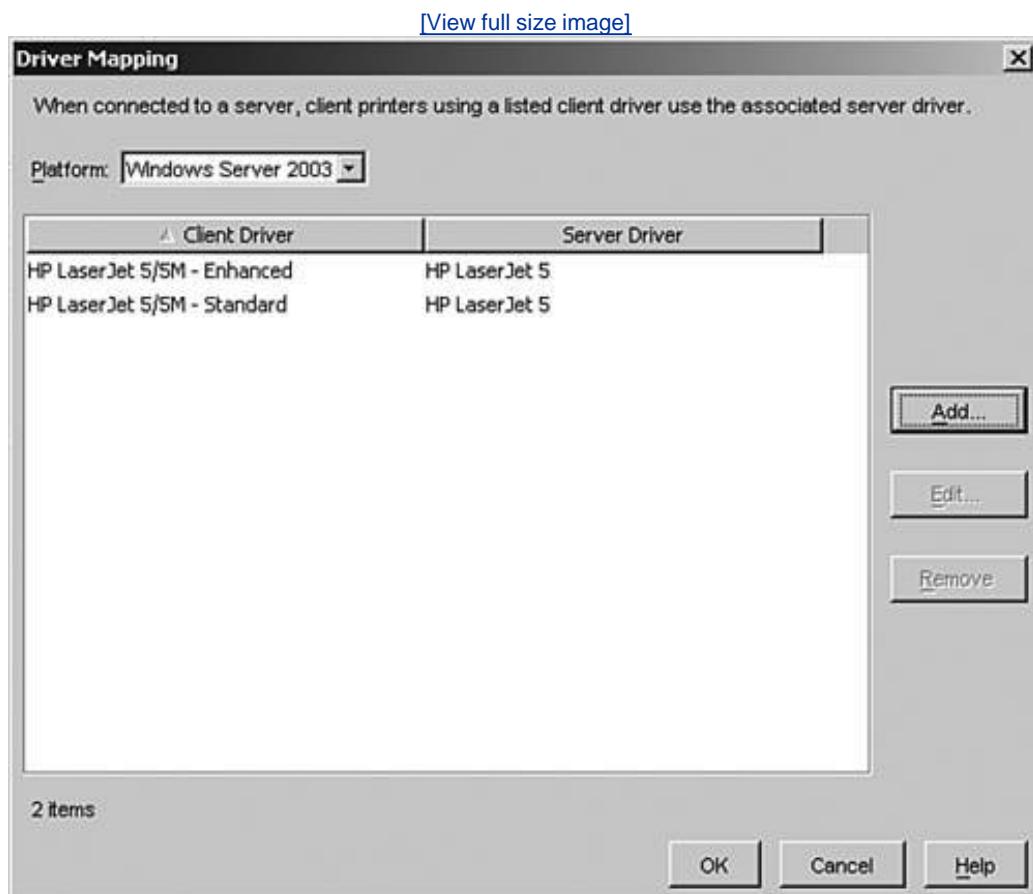
For you to be able to properly connect client printers within a MetaFrame session, the server needs a process by which it can identify and select the appropriate printer driver. This identification process involves comparing the name of the printer driver on the client with driver names on the server to find a match. If a name match is found, the printer is created within the user's MetaFrame session. If a match is not found, depending on the configuration of the server, either an attempt is made to use a MetaFrame universal printer driver, or the client printer mapping fails. Universal printer drivers are discussed in the next section.

This name matching process is reliable when the client and server are both running similar versions of the Windows software (Windows 2000 Professional and Windows 2000 Server or Windows XP and Windows Server 2003). In these situations, the same drivers are used on both the client and server, so the names almost always match each other. The matching process breaks down when the same printer has different driver names on the client and server. This is common when using an older Windows client such as Windows 95 or 98. Many Windows 9x printer drivers have slightly different names from the equivalent Windows 2000 Server or Windows Server 2003 printer driver.

To overcome this problem, Citrix created the driver mapping feature, which allows for the creation of an association between client and server driver names that do not match. You configure printer driver

mapping by selecting the Mapping action for the Drivers node under Printer Management. This opens the Driver Mapping dialog box shown in [Figure 12.8](#), which shows two existing printer driver mappings. When opened for the first time, the Driver Mapping dialog box is empty. Separate mappings for both Windows platforms are maintained to allow for discrepancies between Windows 2000 Server and Windows Server 2003 printer driver names.

Figure 12.8. The driver mapping feature allows you to match up client and server drivers that do not have matching driver names.



You create a driver mapping simply by choosing the desired platform, clicking the Add button, and then providing the name of the client and corresponding server driver names. If the server driver is already installed, you can select it from the drop-down list box. You are always required to type in the appropriate client driver name. You must ensure that the name matches exactly with the name of the driver on the workstation. All capitalization and punctuation must be identical; otherwise, the mapping will not be successful.

These steps summarize the printer driver identification process that MetaFrame follows when attempting to connect a client printer:

1. A user with client printer mapping enabled connects to a MetaFrame server.
2. The MetaFrame server retrieves the name of the local printer driver for example, a driver called HP LaserJet 5P/5MP (HP).
3. The server scans the driver mapping list for the appropriate platform, attempting to find a mapping for the client driver. If a mapping is found, the corresponding server driver is used to create the client printer.

If a driver mapping entry was created but the corresponding server driver does not exist, the mapping fails. MetaFrame does not attempt to continue by looking for an exact driver match.

4. If a mapping entry does not exist, the server searches through the printer drivers installed on the server, attempting to find a matching client driver name. If a match is found, the printer is created within the user's session using the matching printer driver.

If a match is not found, depending on the configuration of the server, either an attempt is made to use a MetaFrame universal printer driver or the client printer mapping fails.

## Note

Because MetaFrame consults the driver mapping table before it searches for locally installed drivers, you can use this to enforce an alternative driver be used for a particular client printer instead of the matching driver that may have already been installed on the server.

The driver mapping information is stored not only within the server farm's data store, but it is also stored locally on each server in a plain text file called **WTSPRNT.INF**. For a default Citrix MPS installation, you can find this file in the %ProgramFiles%\Citrix\System32 folder. For the mappings defined in [Figure 12.8](#), the corresponding entries in **WTSPRNT.INF** would look as follows:

```

;
;      WTSPRNT.INF    DO    NOT    CHANGE
;

;This file is supplied by Citrix as a reference and best guess for
;client printer selections. The file wtsuprn.inf is the user file
;for client printer mapping and takes precedence over this file.
;An example file, wtsuprn.txt is supplied as a template.
;

;This file is changed automatically when the admin makes changes to
;the farm wide driver mapping settings.
;This file may be overwritten during software upgrades!

[Identification]
OptionType=PRINTER
[ClientPrinters]
"HP LaserJet 5/5M - Enhanced"="HP LaserJet 5"
"HP LaserJet 5/5M - Standard"="HP LaserJet 5"

```

Do not modify this file directly because it will be overwritten the next time modifications are made to the driver mappings within the Management Console.

## Note

Changes made to the wtsuprn.inf file are implemented by the MetaFrame server; however, the mappings do not appear in the Management Console.

## MetaFrame Universal Printer Drivers

Since Feature Release 1 of MetaFrame XP, Citrix has provided the universal printer driver (UPD) as an alternative to maintaining drivers for many different printers in a large MetaFrame environment.

Three variations of the UPD are supported in MPS 3.0. One supports PostScript (PS) language, and the other two support different versions of the Printer Control Language (PCL5c and PCL4, respectively).

Instead of using a native printer driver, MetaFrame can be configured to employ one of these three universal drivers in its place. The generic driver is still responsible for creating the print data stream, spooling the job and directing it to the client. The client then renders the data stream using the corresponding interpreter for the UPD language (PS, PCL4, or PCL5c). Finally, the client redirects the data stream to the appropriate local printer for output.

## Alert

Two common misconceptions may trip you up on the exam. First, the UPD is employed only on the MetaFrame server and only for client-mapped printers. The UPD is *not* used at all by the client. Second, the UPD driver is not intended to be employed as an alternative driver for local MetaFrame printers or network printers (mapped manually or using logon scripts).

The use of universal printer drivers can reduce or eliminate the need to manually install and replicate native or custom printer drivers. Manual driver installation would be required only when an application required access to special printer-specific features not available through one of the UPDs.

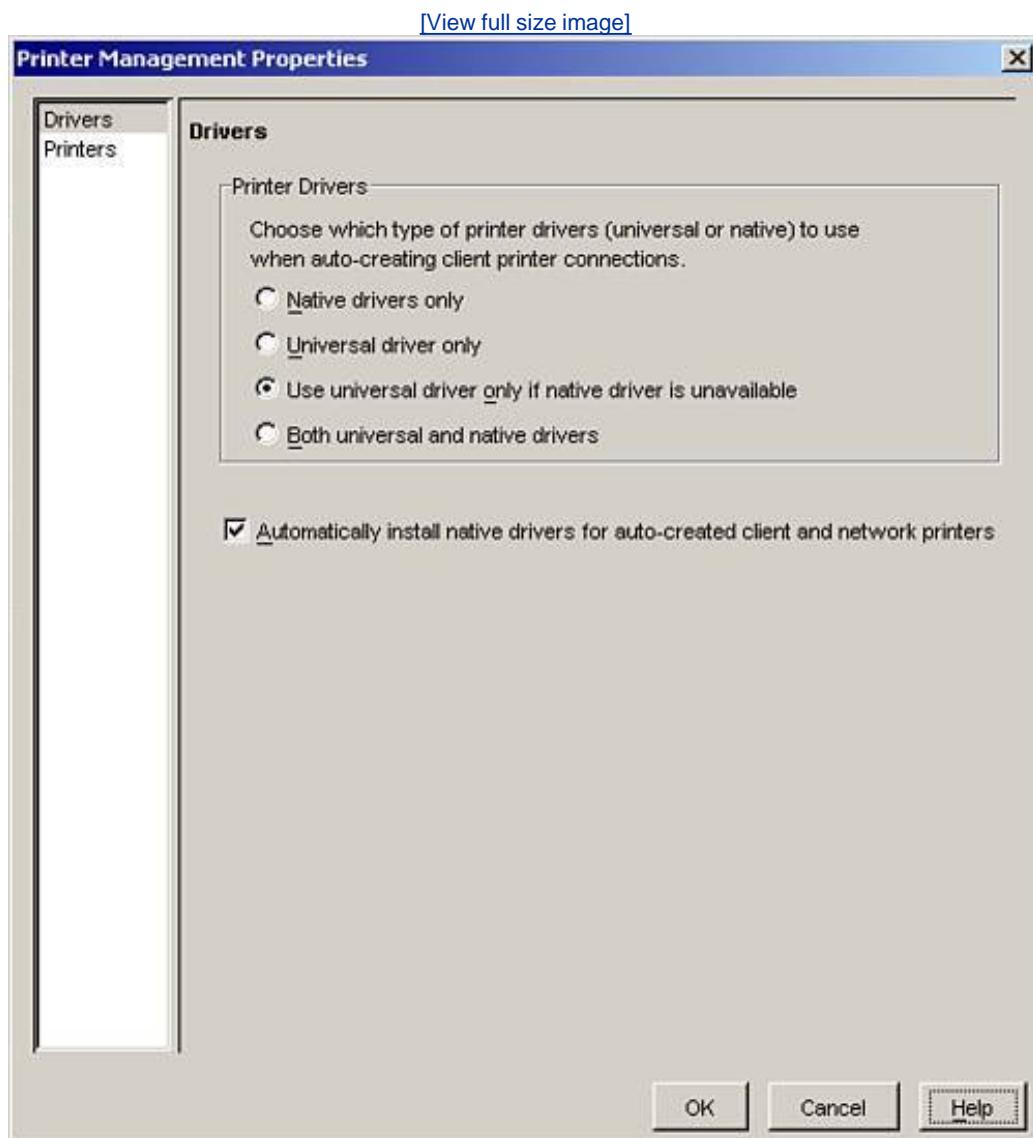
Besides simplifying driver maintenance in very large MetaFrame implementations, universal printer drivers can help to reduce the impact of certain native driver-related issues such as

- The transmission of large print job files generated by native drivers that do not employ advanced printer languages such as PCL or PS.
- Ill-behaved drivers in a MetaFrame environment causing failures of the print spooler service, which impact all users on the server. Although less common now compared to a few years ago, some third-party native printer drivers do not function well in multiuser environments such as MetaFrame.

You manage the use of universal printer drivers in client printer creation from within the properties of the Printer Management node. [Figure 12.9](#) shows the default driver settings within the Printer

Management properties.

Figure 12.9. The behavior of universal printer driver use is managed farmwide within the Printer Management node's properties.



The printer driver choices are

- Native Drivers Only This setting allows only native drivers to be selected when mapping client printers. If a native driver cannot be found, the printer is not connected.
- Universal Driver Only The opposite configuration always uses one of the universal drivers. When this setting is enabled, native drivers are never searched during the client printer connection process.
- Use Universal Driver Only If Native Driver Is Unavailable The default behavior attempts to fall back on using a universal driver only if a native driver cannot be found.

- Both Universal and Native Drivers When this choice is selected, it actually attempts to create two client printers, one using the native driver and the other using a universal driver. If the native driver does not exist or has been excluded using printer compatibility, only the UPD-based client printer will be created.

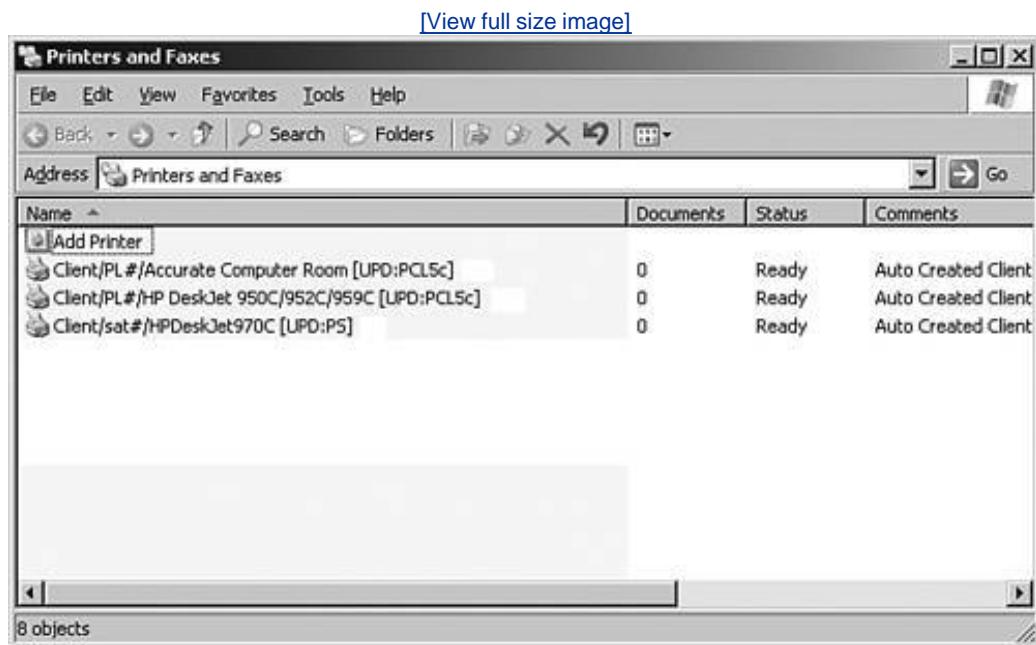
## Alert

You can override the printer choices for the farm with MetaFrame user policies. This allows you to define different driver requirements based on the class, type, or location of the users. Unexpected driver behavior usually indicates that a policy is involved.

The final option on this screen is used to control whether MetaFrame will attempt to install a native Windows driver when required during auto-creation of client and network printers. If you want to have complete control over the drivers added to a server or you are going to support only the UPDs, you should disable Automatically Install Native Drivers for Auto-Created Client and Network Printers.

You can quickly identify a client printer created using a UPD because the suffix [UPD:<driver type>] is added to the printer name. [Figure 12.10](#) shows how this name would appear. In this figure, you see two printers using the PCL5c universal printer driver, whereas the other uses the PS UPD.

**Figure 12.10.** Client-mapped printers that use a universal printer driver have [UPD:<driver type>] appended to the end of the printer name.



The universal driver that is employed depends on the client's version and Windows platform. The MetaFrame server automatically determines the highest UPD version supported by the client. The specific client versions compatible with the different UPDs are as follows:

- PCL5c The client must be running either the Macintosh or Win32 client at version 7.0 or higher to use this driver. The PCL5c driver supports both color and black-and-white printing up to 600 dots per inch (dpi).
- PCL4 Older versions of the ICA client utilize this driver. The PCL4 driver supports only black-and-white printing with a maximum resolution of 300 dpi.
- PS The PostScript driver is intended for use with version 7.0 or higher of the ICA client for UNIX.

 PREV

NEXT 

# Printer Configuration

Throughout the rest of this chapter, we look briefly at the actual steps required to configure the client, network, and local printers discussed at the beginning of this chapter.

## Client Printers

For users to be able to access their local client printers, a MetaFrame administrator must grant access. A number of different areas in the system contain settings that dictate when client printers are mapped, and certain settings override other settings. The following is a summary of the locations where client printer options can be found and their order of precedence, from highest to lowest. The higher-ranked settings take precedence over the lower settings:

1. MetaFrame User Policies In [Chapter 7](#), we discussed how to create custom policies to control many aspects of a user's connection. Some policy settings control the behavior of client devices, including the auto-creation of client printers. Client printer settings defined within a policy take precedence over settings made anywhere else in the system, including at the connection and user profile levels. Client printer policies are found under Client Devices\Resources\Local Printers.
2. Printer Management Properties When you open the property page for the Printer Management node and select Printers from the left pane, you see the settings shown in [Figure 12.11](#). The upper group box contains the settings that define the farmwide behavior for client-mapped printers. The Auto-Created Network Printers group box is discussed in the next section. The individual settings are as follows:
  - Auto-Create Client Printers When User Logs On Enabling this setting allows client printers to be created automatically. Even when this setting is disabled, users can still manually map back to their local client printer. This option is enabled by default.
  - Update Printer Properties at Each Logon When this setting is enabled, printer settings from the client are updated on the server printer at logon. When it is disabled, any changes made to the server printer are retained from logon to logon. This option is disabled by default.
  - Inherit Client Printer's Settings for Keeping Printed Documents If the client is configured to do so, the server printer will also retain the print jobs in the queue. This setting can result in a large consumption of disk space. It is enabled by default.
  - Delete Pending Print Jobs at Logout By default, auto-created printer print jobs are retained in the printer's queue when a user logs off so that the job can be processed the next time the user logs on. Enabling this option causes the jobs to be deleted when the user logs off, even if the printing is not yet finished. This setting applies only to auto-created client printers. Print jobs on print server queues are not deleted.
  - Always Create Client Network Printers as Client Printers By default, if a client device has a mapped network printer that is accessible by the MetaFrame server, the server will attempt to print directly to that printer instead of routing the job through the MetaFrame

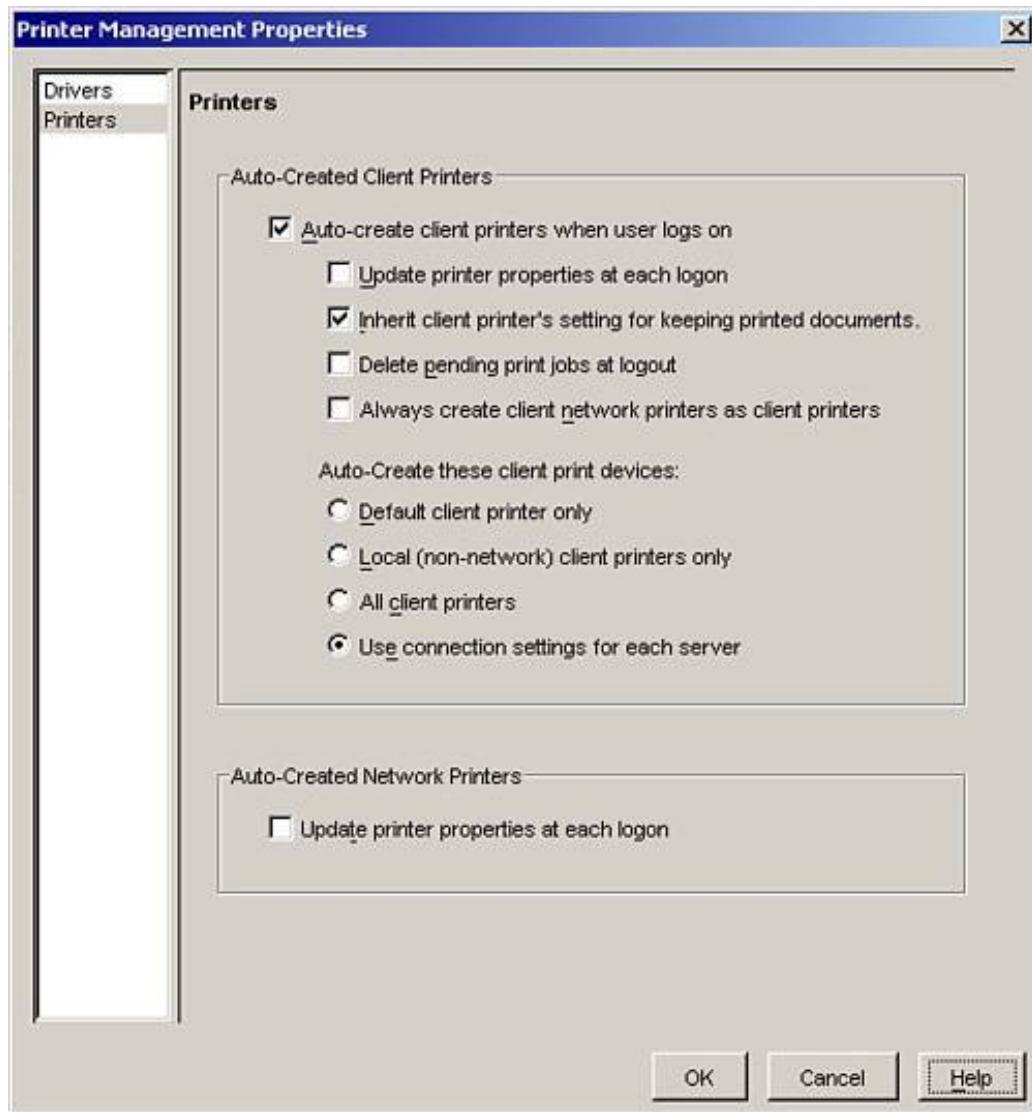
client. This can result in faster printing when the client and the MetaFrame server are on the same LAN. The setting is not foolproof though. If a printer with the same name exists on the client and server networks, the job can be routed to the wrong printer. Enabling this option forces the server to always direct the job through the client, regardless of whether the printer can be directly accessed. If the client is located across a WAN link, sending the job through the client can be faster because it is compressed before being sent. This option can also be set through a MetaFrame policy. The specific policy setting is found under

Client Devices\Resources\Network Printers\Print Job Routing

- Auto-Create These Client Print Devices Four choices exist for this option. The first, Default Client Printer Only, maps only the local client default printer. Any other client printers are ignored. The Local (Non-Network) Client Printers Only setting maps all printers that are local to the client and ignores any network-mapped printers. The third option maps all client printers, and the final option, which is the default, defers these settings to those defined at the connection level on each server. The connection settings have lower precedence with regard to client printer mapping.

Figure 12.11. The settings on the Printer Management property page dictate the defaults for the farm.

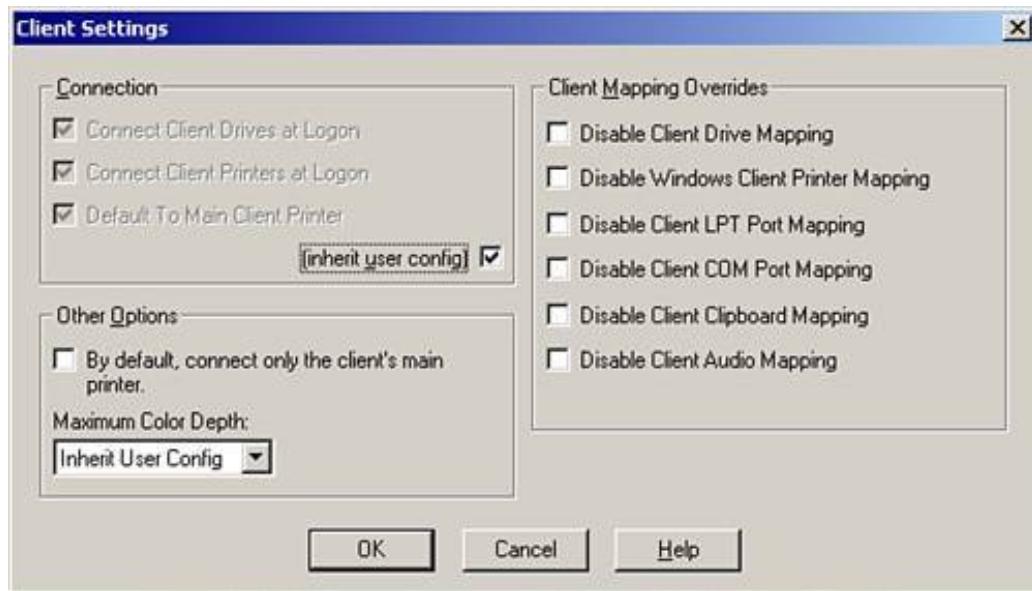
[\[View full size image\]](#)



3. ICA Connection Configuration The Citrix Connection Configuration tool and the Terminal Services Configuration tool both provide access to the ICA connection settings on a server. The client settings option for ICA connections in either tool display the same settings. [Figure 12.12](#) shows the client settings within the Citrix Connection Configuration tool. Here, you can define the same options available for the Auto-Create These Client Print Devices options at the farm level. The default configuration at the connection level is to defer these settings to the individual user's logon account.

Figure 12.12. Client printer mapping settings can also be defined at the connection level on a MetaFrame server.

[\[View full size image\]](#)



4. Environment Tab Within the individual user account (at the server or domain level), you will find the Environment tab, which has settings that control whether client printers are connected at logon and if the default is set to the main client printer. Both options are enabled by default, but disabling them works only if a higher precedence setting does not override the option.

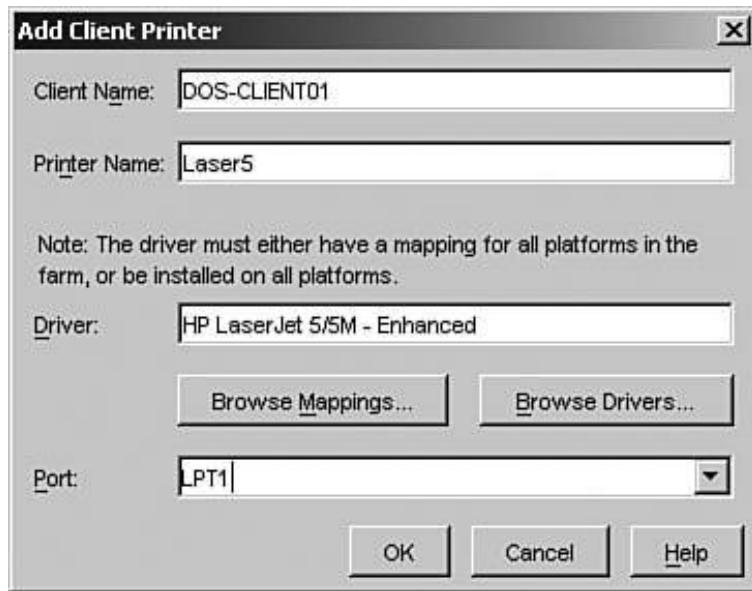
If client auto-creation is enabled, valid client printers are automatically created in the user's MetaFrame session. If the clients are running the DOS or Windows CE MetaFrame client, additional steps are required to ensure that the printers are automatically mapped.

## Auto-Client Printer Creation for DOS and the Windows CE Client

In MetaFrame 1.8, DOS and Windows CE clients would have to manually map their desired client printers using the ICA Client Printer Configuration tool. Although this tool is still included with MetaFrame, you are now able to define printer mappings for DOS and Windows CE clients so that they are automatically mapped when the client logs on.

To find these options, highlight the Printers node under Printer Management and choose Client Printers from the Actions menu. This opens the Client Printers dialog box, where you define the printer, driver, and port settings for a specific DOS or Windows CE client name. Clicking the Add button allows you to provide the appropriate settings. [Figure 12.13](#) shows the various inputs required. When choosing the server driver, you can either browse the list of drivers installed on the server or select from any driver mappings that you may have created.

Figure 12.13. DOS and Windows CE clients can have auto-created client printers if an administrator has created the appropriate client printer entry.



## Network Printers

Any shared network printer can be mapped using any of the following methods:

- Through a logon script The script can map the same printers for all users or map different printers based on group membership.
- Manually through the Add Printer Wizard Users can use the wizard to set up printers themselves if they know the name and location, or an administrator can assist the users in the mapping process.
- Auto-creation of network printers through MetaFrame MetaFrame also allows you to define the auto-creation of network-based printers. When a user logs on to a MetaFrame server, the assigned printers are automatically made available in the user's session. This is a powerful alternative to scripting, particularly when the administrator is not skilled in creating Windows scripts. Let's look briefly at network printer auto-creation.

You set up auto-creation of network printers from within the Printers node of Printer Management. Simply highlight the local or imported network printer in the right pane and then choose Auto-Creation from the Actions menu. In the simple dialog box that appears you define the individual users or groups associated with the printer as well as the basic printer preferences that will be enforced. Although the preferences are basic, this dialog box does allow you to define the paper size, copy count, print quality, and page orientation. These settings are usually sufficient when setting up a specific network printer. After the printer has been created, the user is able to access any advanced settings associated with the printer driver.

When a network printer is auto-created for a user, it appears in the Printers folder just as if it had been mapped through a logon script or added through the Add Printers Wizard.

Only two settings in Printer Management directly relate to the auto-creation of network printers, and both are found on the property page for Printer Management. The first, located on the Drivers screen, is Automatically Install Native Drivers for Auto-Created Client and Network Printers. If the necessary native driver is not installed for an auto-created network printer, enabling this feature will install the driver. Note that this pertains only to Windows native drivers, not third-party drivers that are not

shipped with Windows.

## Note

Auto-created network printers do *not* use universal printer drivers, but native printer drivers can be installed if necessary when mapping to the network printer.

The other option is located on the Printers screen in the Auto-Created Network Printers group box. This setting, labeled Update Printer Properties at Each Logon, is disabled by default. When it is enabled, the MetaFrame server automatically replaces any user-defined settings with the settings defined in the Management Console.

## Local Printers

A local MetaFrame printer is accessible in one of two ways. If the printer is defined on the same MetaFrame server that the user is logging on to, the printer will be visible in the Printers folder unless the printer's permissions have been defined to prevent this.

If the local printer exists on another MetaFrame server in the farm and is being shared, it can be accessed using the same methods described in the preceding "[Network Printers](#)" section.

 PREV

NEXT 

## Exam Prep Questions

1. MetaFrame supports three main categories of printer types. They are \_\_\_\_\_.

A. client printers, network printers, and local printers

B. client local printers, client network printers, and server local printers

C. client printers, server printers, and local printers

D. native printers, mapped printers, and universal printers

A1: Answer A is correct. The three categories of supported printers are client, network, and local printers.

Answer B is incorrect because both client local and client network printers are actually classified simply as client printers, and server local printers are equivalent to local printers. The actual network printers category is missing from this list.

Answer C is incorrect because server printers could represent either network or local printers.

Answer D is incorrect because it refers to printer driver properties, not supported printer types.

2. When a printer is shared off a MetaFrame server, it is considered to be a \_\_\_\_\_ printer to the farm. (Choose the answer that best completes the sentence.)

A. network

B. server

C. client

D. local

A2: Answer D is correct. When a printer is connected to a server running MPS, that printer is considered to be a local printer to the farm.

Answer A is incorrect. A network printer is a printer shared off a server that is not also running MetaFrame.

Answer B is incorrect because server printer is not one of the printer categories for MetaFrame.

Answer C is incorrect because a client printer is any printer that is configured on a client device, whether it is a printer directly attached to the client or a printer that is mapped to a share on the network.

3. Before a printer driver can be replicated to other servers in the farm, you must first \_\_\_\_\_. (Choose the answer that best completes the sentence.)

A. enable printer drive replication for the entire farm

B. install the driver on at least one MetaFrame server

C. create a client printer mapping entry for the server where the driver is installed

D. define the MetaFrame server that will act as the source for replicated printer drivers

A3: Answer B is correct. Before a driver can be replicated, it must exist on at least one server

in the farm. This driver can be installed on any server and replicated to any other server running the same Windows platform.

Answer A is incorrect because there is no single setting that must be toggled to enable or disable printer replication in the farm.

Answer C is incorrect because client printer mapping entries are created to allow a client running one type of printer driver to seamlessly be configured to use an alternative driver when logged in to the server. This setting dictates what association to make between the client and server printer drivers; it has no bearing on the function of driver replication.

Answer D is incorrect because no one server must be designated as the replication source.

4. When a printer is imported from a Windows print server that is not running MetaFrame, what printer management actions are not available? (Choose all that apply.)

A. Replicate drivers

B. Auto-creation

C. Copy auto-creation settings

D. Client printers

A4: Answer A is correct. When a printer is imported from a standard Windows print server, the Replicate Drivers action is not available. A printer driver must exist on at least one MetaFrame server before it can be replicated.

Answers B, C, and D are incorrect. All these printer management actions can still be performed, even if the printer was imported from a Windows print server that was not running MetaFrame.

5. The printer bandwidth limitations apply to what types of printers? (Choose all that apply.)

- A. local printers
- B. network printers
- C. client printers
- D. network printers mapped by scripts during MetaFrame server logon

A5: Only answer C is correct. The printer bandwidth limitations apply only to client-mapped printers. Local and network printers (answers A and B) are not throttled using this bandwidth setting. Answer D is also incorrect. Regardless of whether a network printer is mapped manually or through some automated scripting method, bandwidth restrictions are not imposed on that printer. As long as the printer is mapped back through the MPS client, printer bandwidth is controlled through the Bandwidth tab in Printer Management.

6. Which of the following tasks cannot be performed from the Printer Drivers tab for a MetaFrame server? (Choose all that apply.)

- A. Replicate the driver to other servers and add to the auto replication list.
- B. Manage the auto replication list for a driver.
- C. Control the printer drivers that can be used by client devices.
- D. Configure the associated driver to use when a client connects to the MetaFrame server.

A6: Answers B, C, and D are all tasks that cannot be performed from the Printer Drivers tab for a specific MetaFrame server. This must be performed from the Drivers node under Printer Management. One way to remember this is that each of these tasks involves settings that could affect all servers in the farm, not just one individual server.

Answer A is the only task that can be performed on an individual server's printer drivers and so is not the correct answer to this question.

7. A user named Marie connects to your MetaFrame server, but her local printer is not available when she logs on. Assuming that the printer is functioning properly on Marie's local device, which of the following are likely causes for the problem? (Choose all that apply.)

A. Marie's printer is not compatible with MetaFrame.

B. The appropriate driver is not installed on the MetaFrame server.

C. Her local printer driver name does not match a driver on the MetaFrame server.

D. Client printer mapping has been disabled.

A7: Answers B, C, and D are all valid reasons why Marie's printer may not be mapping properly. If no matching driver is installed on the server, her printer would not map if the universal printer driver was also disabled.

If her local printer driver name differs from the corresponding driver on the server, the printer would not map without a corresponding driver mapping definition.

It is also possible that client printer mapping has been disabled on the MetaFrame server, preventing Marie's client-based printer from appearing.

The only answer that is not valid is A. There is no such thing as a printer compatibility issue with MetaFrame. It is possible that a printer may not function properly on a Terminal Server, but this is a Windows issue, not a MetaFrame issue.

8. Where can the printer driver mapping information be found on each MetaFrame server in the farm?



- A. It is found in the WTSPRNT Registry value.
- 
- B. It is found in the **WTSPRNT.INF** file.
- 
- C. It is not stored on each server. It is stored only in the data store.
- 
- D. It is found in the local host cache file.

A8: Answer B is correct. Each server has a file called **WTSPRNT.INF** that contains the printer driver mapping information defined in the Management Console.

Answer C is incorrect. While printer driver mapping information is stored in the central data store for the farm, it is also stored in the **WTSPRNT.INF** file.

Answer A is incorrect. Printer driver mapping information has never been stored in the Registry. Similarly, answer D is also incorrect. Although the local host cache maintains a subset of the main data store information, it does not contain printer driver mapping information.

9. MetaFrame provides more than one type of universal printer driver. Select only the valid universal drivers from the following list.



A. PCL5



B. PCL5c



C. PS



D. PCL4c

A9: Answers B and C are the only two valid UPDs in the list. The third valid driver, called PCL4, is the only UPD not in this list. Neither answer A nor D represents a valid universal printer driver supplied with MPS 3.0. PCL4c is incorrect because the UPD driver is simply PCL4, without the c suffix.

10. Where would you go to configure the behavior of universal printer driver use in your MetaFrame server farm?

- 
- A. Properties of the Printer Management node
- 
- B. Properties of the Drivers node
- 
- C. Properties of the Printers node
- 
- D. Properties of the UPD within the Drivers node

A10: Answer A is correct. The options for using UPDs in client printer creation are managed within the properties of the Printer Management node. From here, you can dictate whether a native or universal driver will be used.

Although both answers B and C describe valid properties for the Drivers and Printers node, neither location manages information on the universal printer drivers.

The final answer, D, is incorrect because there are no such UPD properties within the Drivers node.

11. A universal printer driver can be used for which of the following printers? (Choose all that apply.)

- 
- A. auto-created client printers
- 
- B. printers manually mapped by a user
- 
- C. auto-created network printers
- 
- D. local printers

A11: Only answer A is correct. Universal printer drivers can be employed only for auto-created client printers. All other printer types depend on the availability of a suitable driver on the MetaFrame server, so answers B, C, and D are incorrect.

12. An order of precedence is followed when determining whether client auto-created printers are enabled and what settings are used. Choose the answer that correctly lists the order of precedence for these properties from highest to lowest.

- A. User account settings, Connection settings, Printer Management properties, User policies

- B. User policies, Connection settings, Printer Management properties, User account settings

- C. User policies, Printer Management properties, Connection settings, User account settings

- D. Printer Management properties, User policies, User account settings, Connection settings

A12: Answer C is correct. User policies always take precedence over other client printer auto-creation settings. Farm properties are the next highest, but by default they use the connection settings on the individual servers, which in turn look to individual user settings by default. Therefore, answers A, B, and D are incorrect.

13. Network printer auto-creation has been configured for a printer based on membership in the group called Printers. User Joe is complaining that he cannot see this printer within his MetaFrame session. What are possible reasons for his printer not being available? (Choose all that apply.)



A. He has not logged off and back on since the auto-creation was defined for that printer.



B. His local printer driver has a different name than the same driver on the server. A driver mapping is required.



C. He does not belong to the Printers group.



D. The print server upon which the printer is being shared has not been imported into the farm. You must import it into the farm before he can access it.

A13: Answers A and C are correct. If the auto-creation was configured but Joe has not logged off and back on, he cannot pick up the network printer mapping. He may also not be a part of the group, so he will not receive that mapping during logon.

Answer B is not correct in this case. Auto-created network printers do not rely on a client driver at all, so Joe would not be affected by any driver name mismatch that may exist.

Answer D is also incorrect. If the print server had not yet been imported, you would not have been able to configure the auto-creation of the network printer. The printer will appear in the Printer Management node only if it has been imported or it is being shared off a MetaFrame server in the farm.

 PREV

NEXT 

# 13. Citrix ICA Session and Client Configuration

Terms you'll need to understand:

- Presentation Server Client
- Citrix ICA Client
- Program Neighborhood
- Program Neighborhood Agent
- Citrix Web client
- Components CD
- Client Update Database
- Ica32Pkg client package
- Self-extracting executables
- Appsrv.ini and PN.ini
- ICA Client Distribution Wizard
- ICA Client Update Configuration
- ICAINST
- ICA pass-through client
- Remote Desktop Web Connection
- ICA browsing
- Citrix XML and ICA Browser Services
- Server location
- ICA dial-in
- Program Neighborhood Agent Console
- Workspace Control

Concepts and techniques you'll need to master:

- Selecting the appropriate deployment method for a given implementation scenario

- Creating installation floppy disks for a Win32 client installation
- Locating the appropriate client on the Components CD
- Identifying and configuring the different Win32 clients
- Customizing the MSI installer package and self-extracting executables
- Understanding the role of the Client Update Database and how one is created and managed
- Explaining the purpose of the ICA pass-through client
- Explaining the difference between the Citrix XML and ICA Browser services
- Identifying where in the environment a given configuration setting would be modified

For a user to be able to access content published on one or more Presentation Servers, he or she needs a Citrix MetaFrame Presentation Server client. Citrix provides client software for a wide variety of operating systems and devices. Currently, this list includes

- Windows 32-bit operating systems This includes Windows 95 and all later Windows desktop and server operating systems (Windows 9x/NT/2000/2003/XP). The Win32 client provides complete support for all the available client features. Client features are reviewed later in this chapter.
- Windows 16-bit operating systems Legacy support is available for Windows 3.1 and 3.11 environments. Only limited features are available with this client.
- Windows CE and PocketPC-based devices Clients exist for both Windows-based terminals and handheld devices that run these operating systems. Various processors are supported. Typically, if the processor supports Windows CE or PocketPC, an ICA client is available for that configuration.
- Apple Macintosh operating systems Both OS X and older versions (System 7.5.3 or later on PowerPC and System 7.1 or later on PowerPC or Motorola 68x processors) of the Macintosh operating system are supported with this client. An updated version of the OS X client was recently released.
- IBM OS/2 Warp operating system This is another legacy client that has not seen an update in a few years. Versions 3, 4, and 4.5 of IBM OS/2 Warp are supported. This client does not run on earlier versions of OS/2.
- DOS (16- or 32-bit clients) Both legacy clients provide similar capabilities, except for reduced conventional memory requirements and a few additional features such as bitmap caching available with the 32-bit client. Because of the use of extended memory, the 32-bit client requires at least an Intel (or compatible) 386 or later processor. Updates are no longer being made to the DOS clients.
- Linux and UNIX operating systems The increased popularity of Linux as an alternate business desktop operating system has not gone unnoticed by Citrix. Energy has been focused on ensuring that a current version of the Linux x86 and Solaris SPARC clients incorporate the majority of the features found in the Win32 client. The HP-UX and IBM AIX operating systems are the other two UNIX clients that are actively updated. The remaining UNIX-based clients (Solaris/x86, Sun OS, Compaq Tru64, SGI, and SCO) have not been updated in a few years and are maintained for legacy environments only.
- EPOC/Symbian devices A specialty client was developed for specific devices. The most recent

additions are still considered to be alpha products and should not be deployed in a production environment.

- Java applet client Another client actively updated by Citrix, this platform-independent client runs on any client device that has a web browser and a Java 2 Standard Edition 1.4.x environment or later. The client is actually a Java applet that resides on a web server and is downloaded and launched when a user navigates to the page containing the appropriate applet tab. To find more details on the configuration and use of the Java client within a web browser, see [Chapter 14](#), "Web Access to the MetaFrame Server Farm."

Although a few of these clients are no longer being actively updated (Win16, DOS, and IBM OS/2, for example), Citrix still maintains 100% backward compatibility with these clients in its latest Presentation Server product. A user running the Win16 client can just as easily access an MPS server as a MetaFrame 1.8 server. Many of the newer features such as session reliability or universal printer driver support are not available, but common features such as published application connectivity and client device mapping support are available.

## Alert

Ensure that you are able to readily identify what client platforms are and are not supported by Citrix Presentation Server.

Before going much further, we should discuss the various naming conventions of the Citrix client software. As Citrix has moved to change the name of the MetaFrame product to Presentation Server, so has it begun to update the naming of its clients from Citrix ICA Client to Citrix Presentation Server Client. Currently, the client documentation and the client software itself are in different states of transition, so you will likely see a combination of these names depending on the client that you are working with.

Regardless of the name used, it still references the same product. The Presentation Server Client for Linux and the ICA Client for Linux represent the same client software. You may encounter questions on the exam that reference either client name. You should not assume that a particular name refers to a particular version or type of client unless it is explicitly mentioned.

 PREV

NEXT 

## ICA Client Types

In addition to the different platforms supported, the exact method by which a user accesses published resources is dictated by the *type* of client used. Although many platforms support only a single type of client, others support multiple types that serve different client access and administrative requirements. Citrix supports four basic types of ICA clients:

- Program Neighborhood (PN) Program Neighborhood is the full Win32 client environment within which both application sets (groups of published resources available within a server farm) and specific connections (to published resources or directly to servers) can be configured and accessed. Although Program Neighborhood was once the main client used for Win32 desktop deployments, Citrix has since placed more emphasis on deploying the alternate Win32 client types because of their reduced desktop complexity and more centralized management features. Program Neighborhood is most often used by administrators who must manage access to a wide number of resources as well as more advanced users who require the ability to manage access to different servers or published applications. [Figure 13.1](#) shows the main PN window. NRSC Farm represents the Noisy River farm application set that has been configured on the client. The Find New Application Set icon accesses a wizard that allows you to connect to a server farm and create an associated application set. The final icon, labeled Custom ICA Connections, allows you to select specific servers or published applications to connect to. The PN client is described further later in this chapter.

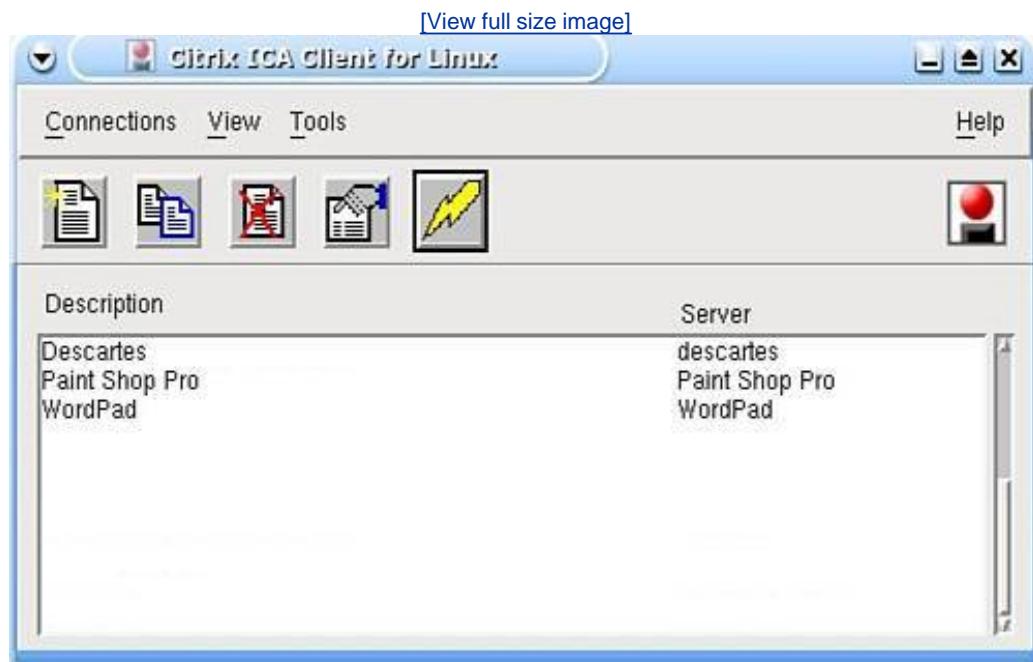
Figure 13.1. Program Neighborhood is available for Win32 operating systems only.

[View full size image]



- ICA Client Connections Depending on the client, this will either be the sole function of the client or a particular view within the client software. For example, the Program Neighborhood client supports a special view called Customer ICA Connections (see the icon in [Figure 13.1](#)), where you can create or manage connections to individual servers or published applications. This is also the default view when running other clients such as the ICA Client for Linux or Solaris SPARC. Other clients such as the Macintosh OS X client or the IBM AIX client support only this view. [Figure 13.2](#) shows the main connection view for the ICA Client for Linux. Note the list of available client connections. ICA Client Connections do not support the creation and use of application sets in the way presented in the PN client.

**Figure 13.2.** The ICA Client for Linux has a client view similar to the Custom ICA Connections view in the Program Neighborhood client.

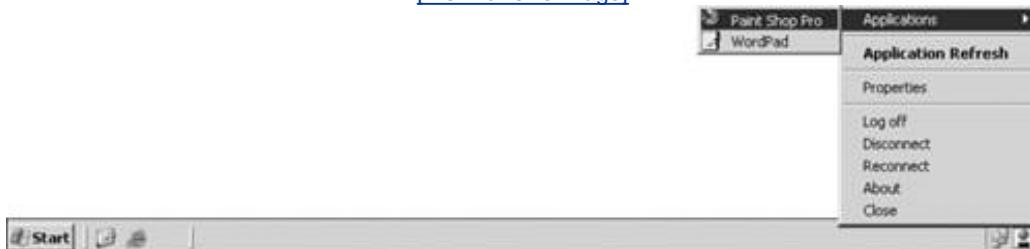


- [Program Neighborhood Agent \(PN Agent\)](#) The PN Agent works in conjunction with the Web Interface for Presentation Server (discussed in [Chapter 14](#)) and provides a seamless method of integrating published applications with the user's desktop. Within the PN Agent client, unlike the full PN client, only basic configuration options are managed directly. Instead, the majority of the client settings are controlled through the web-based Program Neighborhood Agent Console. There is a completely separate Win32 PN Agent client. It can be installed onto a Win32 desktop independent of the full PN client.

The only other clients that support the PN Agent interface are the Windows CE, Linux x86, and Solaris SPARC clients. These clients do not have separate PN Agent components, but instead offer a PN Agent view. This view can be configured to retrieve the necessary information from the Web Interface, just as the Win32 PN Agent client does. [Figure 13.3](#) shows the extent of the Win32 PN Agent interface visible to the user. The small icon on the system tray, which looks very similar to a lowercase /, allows access to menus that are completely configurable through the PN Agent Console. The published applications listed under the Applications menu can just as easily be configured to appear on the user's desktop or even the user's Start menu.

Figure 13.3. The PN Agent provides minimal visual overhead on the client device while providing full Win32 client functionality. An administrator's dream-come-true.

[View full size image]



- Web Client The fourth and final client type is the Web client, another Win32-only client that provides minimal overhead by allowing access to published resources directly from hyperlinks on a web page. The Web client is officially supported only with the Internet Explorer (5.0 or higher) or Netscape Navigator/Communicator (4.78, 6.2 or higher) web browser. Unlike other clients, the Web client does not have a distinct client-side interface component. Instead, all the published application access information is retrieved directly from the host website. To learn more about configuring Web client access, see [Chapter 14](#).

Actually, two different versions of the Web client are available. The first is the full-featured Web client, supported with both the Internet Explorer and Netscape browser. This client can be installed from a self-extracting executable or a compressed Microsoft cabinet (CAB) file. The second client, also known as the minimal Web client, is supported only with Internet Explorer, and sacrifices a number of client features to achieve its small footprint. This client is available only in a CAB file.

## Note

There is a common misconception that should be addressed. It is the mistaken thought that, to access published applications via a website (using the Web Interface for MPS, for example), you must use the Web client. This is not true. As long as the client device accessing the website has a valid ICA client installed, published applications will be accessible. For example, if you are running a Linux desktop and navigate to a Web Interface for MPS site, as long as the ICA Client for Linux is installed, you can click and launch applications directly from the browser. A special Web client for Linux is not required, and Web-based access is not limited to only the Win32 client platform.

## Alert

You should know the difference between the three Win32 clients and be able to describe the key benefits that they provide.

## Note

MPS 3.0 also introduced support for the Microsoft Remote Desktop (RDP) Web Connection software to access published content through the Web Interface. Use of the RDP Web client limits the features available when compared to an ICA client. You can find more details on the RDP Web client in [Chapter 14](#).

 PREV

NEXT 

# The Win32 Presentation Server Client

We now turn our attention specifically to the features and configuration of the Win32 Presentation Server Client. Currently, it is the most common client platform, so you should not be surprised that the more detailed client questions on the exam center on this client.

Fortunately for us, Citrix has maintained (as much as possible) commonality between the different clients, so when you are familiar with the configuration of one client (Win32, for example), you will have little difficulty configuring an ICA client for an alternate platform. When appropriate, we reference some of the other common client platforms such as Linux, Macintosh, and Java.

## Alert

The Java client is a popular choice for ICA client-related questions.

## Note

We encourage you to take every opportunity to expose yourself to as many different clients as possible. Viewing first-hand the behavior and support differences between the clients helps improve your overall understanding of the capabilities of the different clients.

# Client Deployment Methods

Before you deploy the client, it is recommended that you review the latest README file for the particular client version. You can find the README file for a particular client in the same location as the client binary files are found for download.

The various client deployment methods available are

- Installation using the Components CD The Components CD contains the installation files for all the client software available at the time of the Presentation Server release. The contents of this CD can be copied to a network share point (see later in this list) for remote access, or the CD can itself be used to install the desired Presentation Server client. Use of the Components CD to deploy the client directly to the end user is advised only in smaller environments and situations in which staff can quickly move from device to device to perform the installation.

## Note

Installation of the ICA client requires administrative privileges on the user's workstation.

- Installation with floppy disks Citrix still supports the installation of the Win32 client using floppy disks. Floppy-based deployments are practical only in small (single-site) companies or for remote users who cannot perform an installation using a CD-ROM drive.

An automated disk builder tool is provided with Windows 2000 Server, but not with Windows Server 2003. This Microsoft-developed tool is provided as part of the Windows operating system, not a utility that ships with Presentation Server. On a Windows 2000 Server, you can create disks by running the ICA Client Creator utility.

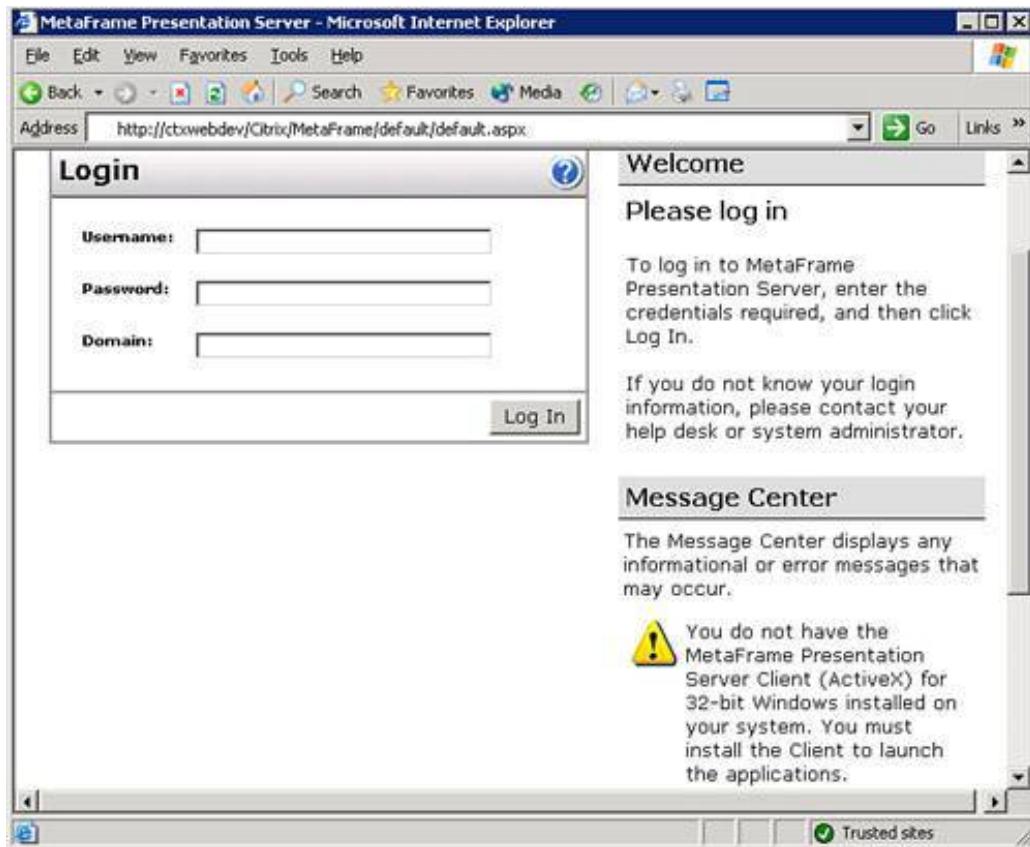
On a Windows Server 2003 machine, you must manually copy the disk images to preformatted floppies. The disk images can be found on the Components CD, under the folder \ICAINST\en\<client>\disks\. The supported disk-installable clients are Win16, Win32, and DOS. The corresponding folders are ICA16, ICA32, and DOS32, respectively.

- Client download from a network share point Creating a network share point containing the desired client installation files is an effective way to deploy the client to the end user. The network share point can be populated with the client files from a couple of different locations on the CD-ROM. The \ICAINST folder contains all the available client installation files, and the ICAWEB folder contains clients that can automatically be installed via the Web Interface. The ICAWEB folder contains multiple languages labeled *de*(German), *en*(English), *es*(Spanish), *fr*(French), or *ja*(Japanese). You can also populate a share location with client files downloaded directly from the Citrix website ([www.citrix.com](http://www.citrix.com)). Setup packages can be customized to ensure a consistent installation. This topic is discussed in the "Client Deployment Customization" section of this chapter.
- Web-based client installation Two methods of web-based client deployment are available. The first leverages the Web Interface for Presentation Server and its built-in capability to prompt a user for the desired client installation when necessary. The Web Interface is a convenient and reliable deployment method for organizations of any size (enterprise, application service provider, or small business).

Figure 13.4 demonstrates the client installation message displayed in the Message Center portion of the Web Interface logon screen. Client deployment settings are managed from within the Web Interface Console (WIC). Configuration of the Web Interface is discussed in Chapter 14 .

**Figure 13.4. The Web Interface informs the user that installation of the client is required before applications can be launched.**

[View full size image]



An alternate web-based deployment method involves the manual creation of a website that simply provides links to the appropriate client software to be downloaded and installed. Logistically, this is similar to the creation of a network share point for client installation.

- Active Directory (AD) or Microsoft Systems Management Server (SMS) Organizations that have the necessary Windows AD domain or SMS infrastructure available may want to leverage this deployment to push out the appropriate Win32 client to the desired target desktops. The Win32 MSI package can be configured and deployed using either one of these methods.
- Client Update Database For those devices that are already running a version of the ICA client, the Client Update Database can be used to completely automate the ICA Client upgrade process. If you want to use the Client Update Database, an older version of the ICA client must already be installed and must also understand remote update requests originating from the Client Update Database. The Client Update Database is described further in the "ICA Client Update Database" section of this chapter.

## Note

The one exception to the installation requirement is the Java client, which is completely contained within a Java applet. Although the applet must be downloaded to the client device, there is no installation process. The applet is simply downloaded and then executed by the client device's Java Virtual Machine. The Web Interface for Presentation Server can be configured to employ the Java client by default, as well as determine what client features such as audio or client drive mapping are enabled. Configuration and use of the Java client are discussed in Chapter 14 .

## Alert

Expect to identify the different client deployment options and understand what conditions must be satisfied to be able to use the Client Update Database.

## Choosing the Client Deployment Method

When you are deciding on the type of client deployment method (or methods) to use, be sure to take the following points into consideration:

- The client operating systems to be supported Each distinct operating system requires its own planning and preparation to ensure that it has been properly configured for the end users. Smaller environments with a more homogeneous client configuration are well suited for disk, CD-ROM, or the network share point deployment methods. In larger, heterogeneous client environments (enterprise or ASP configurations), it can be difficult or impossible to predict the client operating system being used. A web-based deployment is most effective in these situations.
- How users will access published applications How users will access the required published applications can dictate the deployment method employed. If the Web Interface is going to be used, client deployment naturally can be driven through this same web method. Clients using Program Neighborhood, Program Neighborhood Agent, or an alternate client may want to use a custom web page, network share point, or deployment tool such as SMS or other third-party product. In general, clients that do not rely on the Web Interface to provide configuration information (Web client or PN Agent) require customization before deployment. These clients are generally deployed using a network share point or pushed out using Active Directory, SMS, or another tool.

## Note

The type of published application can not only influence how users access the applications, but also the client that is used and ultimately deployed. When users are accessing individual applications, either the Web Interface or PN Agent clients are generally the recommended methods of remote access. On the other hand, when a full desktop is published, the PN Agent or even the full Program Neighborhood might be better suited. Typically, when users are required to access a full desktop session, it is better not to require them to open a web browser, provide their credentials, and then launch a connection to a full desktop session. It would be better if the full desktop session was initiated immediately after they log on or start up their client device.

- Ease-of-use requirements for the end user If users are required to perform their own client installation, you may need to customize the installation to hide the majority of the installation prompts that typically appear. More technically savvy users can be instructed on the required settings and expected to complete the setup successfully. The more typical user may have far less comfort with technology and, as a result, require a more foolproof method of client installation. Using customized client setup or automated deployment tools is suggested in this situation.

## Client Installation Files

Three types of client installation files can be used to deploy the MetaFrame Presentation Server Clients for 32-bit Windows:

- MSI Client Package Available on the Components CD or downloadable from the Citrix website, the Ica32Pkg.msi package contains the three Win32 clients (Program Neighborhood, Program Neighborhood Agent, and Web clients). Specific clients and client features can be configured for the package; these customization steps are reviewed in more detail in the next section of this chapter. As with all MSI packages, this package supports all the features provided by the Windows Installer technology, including the ability to install, uninstall, modify, repair, and upgrade client installations. MSI package installation requires Windows Installer Service 2.0 or later.
- Self-extracting executables For each of the available Win32 clients, an individual self-extracting executable is available and can be preconfigured before deployment, much like the MSI package. Configuring self-extracting executables is also discussed in the next section of this chapter. The available executables are
  - Ica32.exe Program Neighborhood; approximately 4MB in size.
  - Ica32a.exe Program Neighborhood Agent; approximately 3.55MB in size.
  - Ica32t.exe Web client; approximately 2.5MB in size.
- Cabinet files Citrix provides the following compressed Microsoft Cabinet installation files for the Web and Program Neighborhood clients. Cabinet files are most commonly used when performing a web-based client installation. Unlike MSI and executable installation files, the preconfiguration of settings before deployment is not supported with cabinet-based installation files.
  - Wfica.cab Program Neighborhood client; approximately 3.8MB in size.
  - Wficat.cab Full Web client; approximately 2.1MB in size.
  - Wficac.cab Minimal Web client; approximately 1.3MB in size.

### Alert

You should be able to identify the different clients that will be installed based on the executable or cabinet filename.

### Note

A fourth deployment method was recently introduced by Citrix: the Citrix Access Client MSI Package. The Citrix Access Client package is a single MSI installation package containing all Win32 client pieces for the Citrix Access Suite. This consolidated package can be downloaded from the Citrix website and is intended to ease the administrative task of deploying the multiple Access Suite components throughout the organization.

The Citrix Access Client Package contains all three of the Win32 Presentation Server clients (PN, PN Agent, and Web client), Citrix Access Gateway clients, and the Citrix Password Manager agent.

## Client Deployment Customization

Both the MSI installation package and the self-extracting executable allow you to customize the installation process, as well as preconfigure many of the client settings. The MSI package can be customized in any one of three ways:

- **MSI Client Packager** The client packager provides a wizard-based tool for customizing the behavior of the MSI package.
- **Command-line parameters** Command-line parameters can be fed to the MSI package file when executed to modify the default behavior of the installation.
- **MSI transform file** Custom transform files can be created to modify the default behavior of the installation. A third-party tool is required to create a transform file (MST). Products from Wise Solutions Inc. ([www.wise.com](http://www.wise.com)) or Macrovision Corporation ([www.installshield.com](http://www.installshield.com)) are just two examples of tools you can use.

### MSI Client Packager Wizard

The Client Packager Wizard provides an easy method of modifying the default behavior of the MSI installation package. The wizard is initiated by running the command

```
msiexec.exe /a <path to package>/ica32pkg.msi
```

where `<path to package>` is the full path to the ica32pkg.msi file if it is not in the current directory.

The `/a` parameter launches the installation package in administration mode. You know you have initiated the packager properly if you receive the message "Welcome to Client Packager Setup." The first input dialog box to appear prompts you to provide a location to store the generated client package image as well as how the package will be generated:

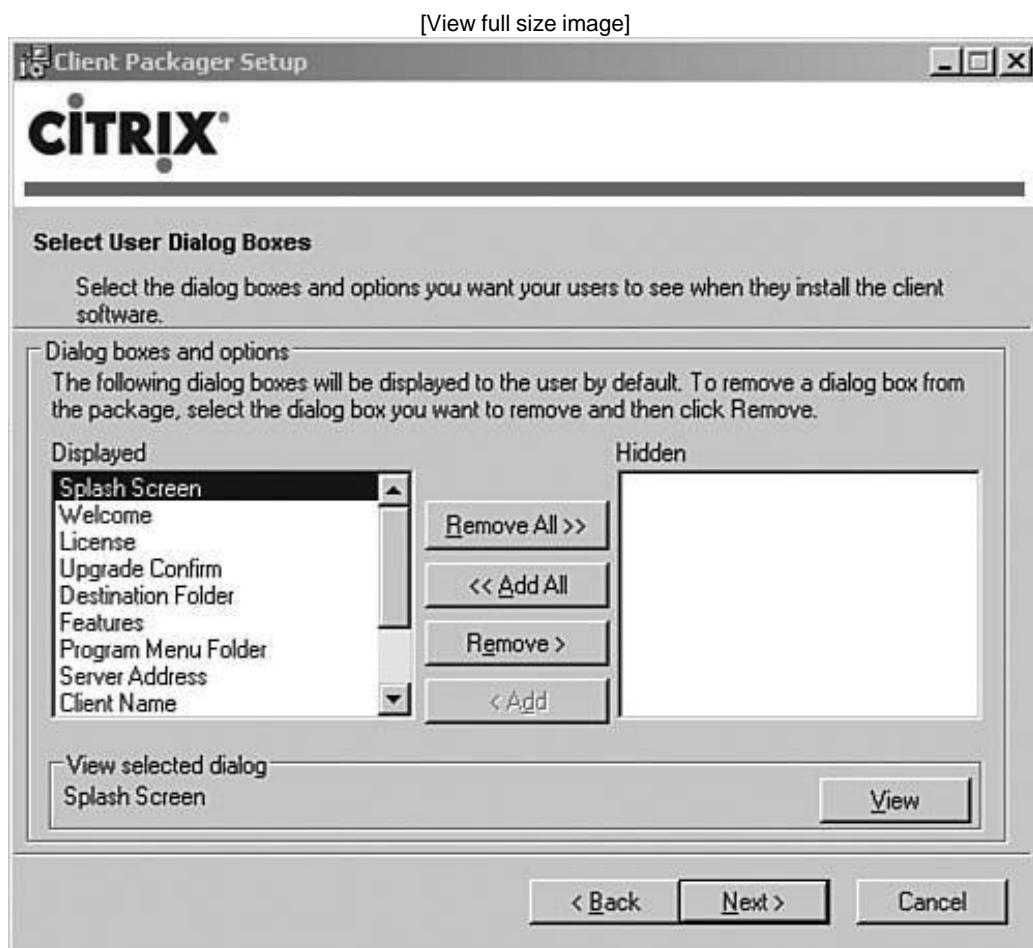
- **Uncompressed** All the deployment files are copied into the target folder.
- **Compressed** All the deployment files are compressed into a single cabinet file in the target folder.
- **Single Windows Installer file** All the deployment files are compressed into a single MSI installation package.

The Client Packager then prompts you to choose the specific clients that will be included in the custom installation (PN, PN Agent, Web). After you decide on the client(s) that will be installed, the remaining dialog boxes prompt you to provide defaults for the information that is usually prompted for during the installation. Some of the information requested is common to all clients, whereas other information is valid only for a specific client. For example, when deploying the PN Agent, you can provide the server URL where the client will retrieve configuration and application information.

In a dialog that appears near the end of the Package Configuration Wizard, you choose what installation dialog boxes will be presented to the end user during the client installation. Figure 13.5

shows how this dialog box would appear. Each of the dialog boxes in the left-hand list will appear during the installation. You can see how the dialog box would appear to the user by highlighting and clicking the View button. When a feature is hidden from the user, the default option defined within the package is automatically used.

Figure 13.5. In Select Users Dialog Boxes, you define the prompts that will appear during the customized client installation.



## MSI Client Command-line Parameters

As an alternative to creating a custom MSI package, you can also provide command-line parameters to the provided package, modifying the default behavior of the installation. The basic command-line syntax is as follows:

```
msiexec.exe /I <path to MSI package>\ica32pkg.msi [options]
```

The parameter `/i` (either upper or lowercase) initiates an install, and the additional `[options]` controls the behavior of the installation. Table 13.1 lists the supported options you can use. Note that all properties shown in uppercase must be provided with matching case; they are *case sensitive*. Using `allow_reboot` is not equivalent to using `ALLOW_REBOOT`.

/qn

Performs a silent installation.

/qb

Shows only progress and error messages during the installation. Otherwise, the installation is silent. The Cancel button is visible to the user.

/qb-!

Shows only progress and error messages during installation. This option also suppresses the display of the Cancel button to the user. Otherwise, the installation is silent.

/l\*v <LogFile>

Enables verbose logging to the provided log filename. The full path to the log file must be provided. You must also include quotation marks if the path contains spaces.

ALLOW\_REBOOT={ Yes|No}

Controls whether the client is allowed to reboot the device. The default is Yes.

CLIENT\_ALLOW\_DOWNGRADE={ Yes|No}

Enables or disables the overwriting of a newer client version with the current version. The default is No.

CLIENT\_NAME=<*ClientName*>

<*ClientName*> uniquely identifies the Presentation Server client. The default value is %COMPUTERNAME% .

CLIENT\_UPGRADE={ Yes|No}

Enables or disables the automatic upgrade of the client if an earlier version is installed. The default is Yes.

DEFAULT\_NDS\_CONTEXT=<Context1[, Context2,...]>

Allows you to define one or more default Novell Directory Services (NDS) contexts for the client. If more than a single context is being used, make sure to enclose the entire option within quotation marks for example "Context1,Context2" . Omitting quotation marks causes the parameter to fail.

ENABLE\_DYNAMIC\_CLIENT\_NAME={ Yes, No}

Enables or disables support for dynamically changing the MPS client name if the device name is changed.

ENABLE\_SSON={ Yes|No}

Enables or disables support for pass-through authentication. The default value is No. If this setting is enabled, a client restart is required.

INSTALLDIR=</*installation folder*>

Specifies the location where the client will be installed. The default location is "C:\Program Files\Citrix\ICA Client" .

PROGRAM\_FOLDER\_NAME= <Start menu folder name>

Allows you to specify the Start menu folder that will contain the client icons. This applies only to the PN and PN Agent clients. The default is "Citrix\MetaFrame Access Clients".

SERVER\_LOCATION= <Web server URL>

Applies only to the PN Agent client. Allows you to specify the URL of the Web Interface server that has the configuration file for PN Agent. You must prefix the server name with either http:// or https:// followed by the server name. If the default folder location is being used, you are not required to provide it. If you have changed the location of the configuration file, the full path must also be included in the URL.

**Table 13.1. Options for Command-Line Modification of the MSI Client Installation Package**

Option	Description
--------	-------------

## Alert

Given a list of options, you should be able to identify the resulting installation behavior.

## MSI Transform File

If you have created a custom transform file for the Win32 client package, you can employ this MST file by using similar syntax to that discussed for command-line parameters. The syntax is as follows:

```
[View full width]msiexec.exe /I <path to MSI package>\ica32pkg.msi TRANSFORMS=<full pa  
|\<transform file.mst>
```

The `/I` (upper or lowercase) and `ica32pkg.msi` parameters are required to use a transform file.

## Alert

You need to know only the syntax for employing a transform file, not the details on how one would be created.

## Customizing Self-Extracting Executables

Before you can modify the configuration of a self-extracting executable, the contents of the file must be extracted into a folder where the necessary configuration settings can then be updated. You can extract the contents by using a compression utility such as WinZip or by issuing the command

```
<exe name> -a -unpack:<target folder>
```

where `<exe name>` is the name of the self-extracting executable, and `<target folder>` is the location where the contents will be placed.

## Note

To repackage the contents into a new self-extracting executable, you must employ a third-party commercial package such as the WinZip Self-Extractor tool.

After the contents are extracted, the specific settings to modify vary depending on the Citrix client.

## Customizing the PN Agent Self-Extracting Executable

The installation settings for the PN Agent are managed through the install.ini file. The default contents of this file are listed here, and a summary of the options is shown in Table 13.2 . Any line that begins with a semicolon is considered to be a comment, so when you modify a setting in this file, be sure to remove the leading semicolon.

### ServerURL

The URL of the Web Interface server. The setting must be preceded by either `http://` for insecure or `https://` for secure SSL communications. If the configuration file is not located in the default location on the Web Interface server, this URL must include the full path to the file.

### SetMachineNameClientName

Setting this value to Yes enables use of the Windows machine name as the ICA client device name.

### Location

Installation location for PN Agent. Using the macro `<PROGRAM FILES>` automatically substitutes with the `%ProgramFiles%` environment variable. The default location is `C:\Program Files\Citrix\PNAgent`.

### StartMenu

This setting specifies the Start menu path where the PN Agent icons will be placed. The path entered here is appended to the Start menu's Programs folder.

### InstallSingleSignOn

Setting this value to Yes enables pass-through authentication. The default value is No.

### AcceptClientSideEULA

Setting this value to Yes automatically accepts the end-user license agreement for the client. The default is No.

Table 13.2. PN Agent Installation Settings

Option	Description
--------	-------------

```
[install]
;ServerURL=http://pnagent
;SetMachineNameClientName=DCN
;Location=<PROGRAM_FILES>\Citrix\PNAgent
;StartMenu=Citrix PN Agent
;InstallSingleSignOn=no
;AcceptClientSideEULA=no
```

## Customizing the Web Client Self-Extracting Executable

The configuration file for the Web client installation is called Ctxsetup.ini. When compared to the setup file for the PN Agent (install.ini), this file contains far more information, but only the first few lines should be modified. Anything that appears after the **Win32 Section** comment should not be changed. This is the editable information:

```
;
; INF file for use with CTXSETUP tool
;
; This INF file describes how to setup the Citrix 32-bit Web Client

[Setup]
Product=Citrix Web Client
InitialPrompt=1
TARGETDIR=%PROGRAMFILES%\Citrix\icaweb32
UninstFile=%TARGETDIR%\uninst.inf
DisplayLicenseDlg=1
AddUninstallLink=1
PromptForCopyingPlugins=0
DisplayStatusMsg=1

;If you want the user to be prompted when a netscape
;plugin is being copied to netscape plugins directory,
;then use the below line
;PromptForCopyingPlugins=1

; If you don't want license dialog to be displayed, then
; use the below line
;DisplayLicenseDlg=0
; If you don't want a completion message to appear when installation
; is finished use the below line
; WARNING: if installation fails the user will receive no error message
;DisplayStatusMsg=0
```

Table 13.3 summarizes the Web client setup options that can be modified.

### InitialPrompt

Setting this value to 0 hides the initial prompt. The default value is 1, which shows the prompt.

## TARGETDIR

The target location for the Web client files. Environment variables can be used to represent a target folder. The default is the Program Files\Citrix\Web folder.

## UninstFile

Location of the file that contains uninstall information. It is recommended that you not modify this setting.

## DisplayLicenseDlg

Setting this value to 0 suppresses display of the end-user license agreement for the client. The default is 1, which shows the EULA.

## AddUninstallLink

Setting this value to 0 prevents adding an uninstall link to the user's client device. The default value is 1, which enables creation of the link.

## PromptForCopyingPlugins

Setting this value to 1 prompts users when a Netscape plug-in is being copied to the Netscape plug-in folder. The default value is 0.

## DisplayStatusMsg

Setting this value to 0 suppresses display of the status message saying that the installation is complete. When suppressed, if an error in the installation has occurred, the user will not be notified.

**Table 13.3. Web Installation Settings**

Option	Description
--------	-------------

## Customizing the Program Neighborhood Self-Extracting Executable

Unlike the Web and PN Agent clients, the customization settings for Program Neighborhood modify the behavior of the client *after* it has been installed. The reason is that, unlike the Web and PN Agent clients, the PN client settings are all managed locally, not centrally through a website. These settings do not modify the default installation behavior of the full PN client.

The configuration settings are read from a set of INI files each time the client is started. The first time a user launches a PN client, the INI files are copied from the client installation location into the user's personal Windows profile. Specifically, the files go into the Application Data\ICAClient folder within the user's profile. Profiles are stored by default on a MetaFrame server under C:\Documents and Settings, with each user receiving a folder that matches his or her user ID.

The files that directly impact the configuration of the client are listed here in their order of precedence. The file listed at the top (wfclient.ini) is applied first, but if a matching setting is found in any of the other files, they take precedence in the listed order.

- wfclient.ini Contains initialization settings for the PN client.

- module.ini Provides information on the communication stack modules. This file resides in the application folder. Matching entries may be found in the appsrv.ini file. If so, they override settings in this file. The contents of this file should not be modified.
- pn.ini Contains information on all the defined application sets for the client. When a new application set is defined, the information is stored in this file.
- appsrv.ini Serves two functions. First, this file contains user interface configuration settings that apply to the client in general. Options such as keyboard macros are stored here. This INI file also contains the defaults for all new ICA custom connections as well as the specific properties defined for each custom connection that has been created.

Within the packaged PN setup executable, these INI files are actually stored with an .src extension instead of a .ini extension. Only the extension has changed; the files otherwise remain plain-text files.

The PN installation is customized by modifying these INI files and then repackaging them as part of the installation process. During installation, the modified INI files and other client binaries are copied into the application folder. As mentioned, first-time users then receive a copy of the INI files in their personal profile.

## Note

After a user has launched the PN client and received copies of the INI files, the client will never again attempt to retrieve files from the application folder, unless the files in the user's profile are moved or deleted.

If you upgrade an existing client with new custom INI files or modify the existing INI files for a PN installation, users will not necessarily pick up these changes. A method of forcing an update, such as scripting the removal of old INI files from the user's profile, would need to be performed before a user runs his or her PN client again.

The two INI files most often updated are the pn.ini and appsrv.ini files. These files can be modified in two different ways. The first involves copying the configuration files from an existing client installation into the folder containing the extracted setup files and replacing the existing SRC files with the modified INI files. The specific steps involved are as follows:

1.  
Extract the setup executable into a working folder.
2.  
Using either the extracted files or the self-extracting executable, install the client onto a test machine that is not used by regular users.
3.  
Launch the PN client and perform any desired customization. For example, you could define the default application set, create any required custom connections, or define the default server location for the client. Configure whatever settings you would like applied as the default when installed.
4.  
Traverse into the profile folder for the current user and copy all the INI files listed earlier from the Application Data\ICAClient folder into your installation working folder.
5.  
Rename (or delete) the existing SRC files in the working folder and then rename all new INI files to

have the .src extension instead of the .ini extension. The PN client now contains the default configuration settings that you defined. You can repackage the executable and deploy the custom client to the target client machines.

Another alternative is to directly modify the INI (or SRC) files using a text editor such as Notepad and manually configure the desired options. To do this, you need to be familiar with the various INI file parameters that are supported. Citrix has made available an Adobe Acrobat document titled "Citrix Presentation Server Program Neighborhood Client for 32-bit Windows Configuration Guide (.ini/.ica File Reference)." You can find this document at <http://support.citrix.com/docs>, under the ICA Clients option. This document contains a detailed listing of all supported parameters for the various .ini (and .ica for the Web Interface) files.

Instead of performing all the setting changes manually, most administrators make the majority of the changes to an installed client and then modify the updated INI files with the additional changes that they want implemented prior to repackaging the client executable.

Some commonly modified INI file parameters that cannot be directly manipulated via the GUI client interface are listed in Table 13.4. This is not a complete list. Refer to the Configuration Guide mentioned earlier for full details.

#### AddICAIconOff

When set to On, the option to add a new ICA Connection under Custom ICA Connections is hidden and not accessible to the user. This option can be used to prevent users from creating new connections.

#### ApplicationSetManagerIconOff

When set to On, the Application Set Manager icon is not available. This icon appears when you first open PN and allows you to manage application sets that have been defined as well as access Custom ICA Connections (if not the default).

#### CustomConnectionsIconOff

This option supports either an On or Off setting. When set to On, the Custom ICA Connections icon in the PN is hidden and not available to the users.

#### FindNewApplicationSetIconOff

When this option is set to On, users do not see the icon allowing them to find new application sets on the network. Removing this setting allows users to access only those application sets that you have already defined as part of the base installation.

**Table 13.4. Sample Program Neighborhood INI Settings**

Option	Description
--------	-------------

#### Alert

You need to know the methods in which the PN client can be customized for installation. You

are not required to know specific settings within the various configuration INI files.

## ICA Client Update Database

The ICA Client Update Database was created to provide a mechanism for automatically updating a supported client device with the latest available MetaFrame client software. It is intended to solve the problem of keeping a large number of clients up to date and properly configured with the latest MetaFrame client. The client update process itself is initiated when a user logs on to a MetaFrame Presentation Server that has been configured to point to a local or remote Client Update Database.

An administrator can fully manage how various clients are updated through the ICA Client Update Configuration utility. Settings that can be configured include whether the update is visible or transparent to the user and whether all clients or only those running an older version are updated.

### Alert

To be able to automatically deploy a client using the ICA Client Update Database, the target device must already have a supported client installed, and that client version must be 4.20.581 or higher. Earlier client versions do not support the automatic update feature.

The ICA Client Update Database has the following key characteristics:

- A new client version must be added to the Client Update Database before it is eligible for deployment. The Client Update Database is initially created and populated using the ICA Client Distribution Wizard. We review this tool shortly.
- Only newer versions of the *same* client product and model are updated. For example, Auto Update does not update a version of PN Agent with a newer version of Program Neighborhood.
- Auto Update works only if the client has been installed from a self-extracting executable. If the installation source was an MSI package, Client Update is not available.
- When version 4.20.581 or later of the ICA client is present, the Update Database automatically detects the version of the client currently installed and initiates an update if necessary.
- An Update Database can be maintained on each MetaFrame server or centrally managed through a database located on a network share point.
- The previous version is maintained in a folder called Backup within the ICA Client folder. This allows for the automatic restoration of the previous client version if necessary.
- When the need for an update is detected, the update process informs the user by default that a client upgrade is necessary. The user has the option to proceed or cancel. This default behavior can be modified to completely hide this option and perform a silent update to the device.
- The client update does not complete until users disconnect or log off their current session and completely close the client. When they log back in, the client update is complete. If users choose to wait for the download to complete, the update is performed automatically before they begin working. If they choose to continue working while it downloads in the background, the full client shutdown is required before they can access the new client version.

- Administrators can force users to wait for the update to complete before they are able to log on to the server.

## Alert

Remember that the Auto Update feature functions only for clients that have been installed using a self-extracting executable. MSI-based client installations cannot be updated using Auto Update.

## Note

Depending on the client device, a user may require administrative access to successfully update the client. For example, although the Linux client supports the automatic update feature, the update will fail unless the user performing the update is logged on with root privileges.

## Creating an Update Database

Although individual databases can be maintained on each server, it is typically best to configure a single database that updates client software for multiple servers. The ICA Client Update Database itself is created by running the ICA Client Distribution Wizard. This wizard automatically launches during the MetaFrame Presentation Server installation, so unless you skipped that portion of the installation, the database should already be configured by default on your MetaFrame server.

The ICA Client Distribution Wizard automatically creates the Update Database in the local folder %ProgramFiles%\Citrix\ICA\ClientDB on the MetaFrame server. A newly created database contains no client files. You must configure the desired clients for the Update Database before users will be able to receive automatic updates.

## Note

When you select a currently active database to be the default, ICUC prompts you to select any other MetaFrame servers in the farm that you would also like to have automatically updated to point to this new database by default. This setting allows you to quickly create and configure a central Client Update Database that is accessed by all desired MetaFrame servers.

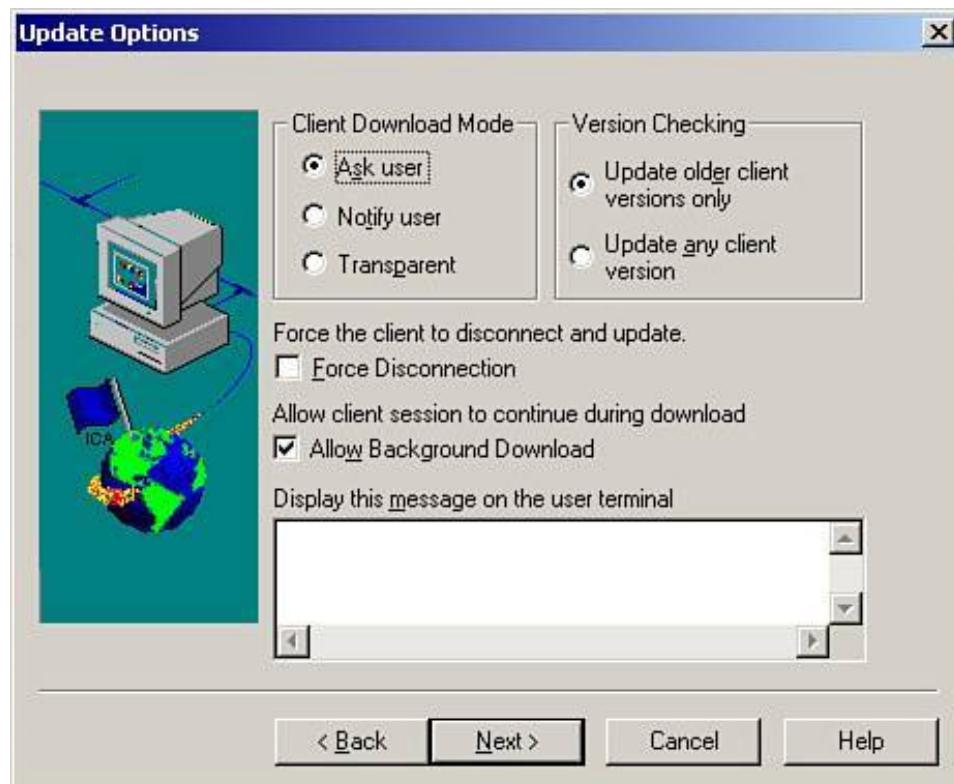
## Adding or Updating Clients in the Update Database

You can add or update supported clients by downloading them from the Citrix website ([www.citrix.com](http://www.citrix.com)) or by using an updated Components CD-ROM. The ICA Client Distribution (ICD) Wizard is used to populate the Update Database with either downloaded clients or the clients on a Components CD-ROM. The client files loaded by the ICD Wizard are found in the ICAINST folder on the

root of the Components CD-ROM drive.

The import of an individual client is performed directly within the ICA Client Update Configuration (ICUC) utility. Selecting New from the Client menu starts a wizard that directs you through selecting the individual Update.ini file associated with the client files. The Update.ini file contains information that describes the ICA Client Update capabilities for the client. The wizard also prompts you to provide the default settings shown in Figure 13.6 . If the client is already present in the database, the ICUC utility does not allow you to re-import that image, unless the existing one is first deleted.

Figure 13.6. The default settings for a new client image are defined while the client is being imported.



## Managing Database Properties in the Update Database

Table 13.5 summarizes the Update Database properties, which you access by choosing Properties from the Database menu.

### Database Path

This property shows the current database path where client information is retained. Auto-client update is active when the Enabled check box is selected.

### Client Download Mode

Three modes exist. The first is Ask User, which prompts the user to confirm whether he or she wants to update the client. Notify User simply tells the user that the client is going to be updated. The user has no option to terminate the update process. Transparent allows the update to be silently performed

on the client. The changes do not take effect until the next time the users log on.

### Version Checking

Update Older Client Versions Only. Updates only clients that are running an older client version than is available in the update database.

Update Any Client Version with This Client enforces not only updates of older clients, but also of newer clients as well. This is one way to force a rollback from a new version to an older version.

### Logging

Enabling the log options Log Downloaded Clients and/or Log Errors During Download creates associated log entries in the Application event log.

### Update Mode

This property dictates how the update is performed. Force Disconnection requires that users disconnect from their session to allow the completion of the client installation. The disconnect is automatically performed after the new client files have been downloaded. Allow Background Download allows users to keep working in their current session while the necessary client files are downloaded in the background. After the download is complete, the installation proceeds. If this setting is disabled, users must wait for the download to complete.

### Maximum Number of Simultaneous Updates on the Server

This property dictates how many users can simultaneously update their client files from the Update Database. When the maximum number is reached, any new update attempts are ignored until the load drops below the maximum. The automatic update is initiated only during the logon process, so only new connections are updated. Any existing ones that were skipped would have to log off and back on to attempt a new update. This is the only setting that cannot be overridden with per-client property settings.

**Table 13.5. Update Database Properties**

Property	Description
----------	-------------

## Managing Client Properties in the Update Database

When a new client is added to the database, it is assigned the default settings defined for the database. You can override these settings when creating the entry or at any time by opening the client's properties. Client properties have four tabs:

- Description This tab provides information on the client version, product number, and in some cases, variant. You can enable or disable updating of this specific client from this tab. If the entire database has been disabled, enabling the client here has no effect.
- Update Options The same client download mode and version checking options found in database properties are also found on this tab. From this tab, you can also define a message that will be displayed to users if they click the More Info button during the client update.

- Event Logging This tab displays the same logging information discussed in Table 13.5 . These settings override the database defaults.
- Client Files This tab displays a list of all client files that make up this MetaFrame client.

## The ICA Pass-through Client

We previously mentioned the ICA pass-through client and how the option to update or install the pass-through client appears when you run the ICA Client Distribution Wizard. The ICA pass-through client is simply an alternate name for running either the full Program Neighborhood or the PN Agent directly off a MetaFrame server. Running such a client on the server allows you to provide PN-based features to clients that do not directly support running the Program Neighborhood or PN Agent.

For example, you might have PN installation on a server and published as an application. A group of Macintosh users could access PN as a published application and have access to application sets that they otherwise would not be able to directly access. Running a pass-through client also allows you to quickly test client connectivity without having to use a separate client device.

Here are a couple of points to note about applications launched through the pass-through client:

- Seamless window support Applications can run in a seamless window within a MetaFrame desktop session.
- Local device support Even though the client is running on the MetaFrame server, it "knows" that it is acting as a pass-through client, so it still allows you to access supported devices directly on the client (printer, drive, COM port, and so on).

## Win32 Client Features

The complete list of available MetaFrame Presentation Server features is supported by the Win32 client. Subsets of these features are then supported by the other client types currently available. Some, such as the Linux client, support nearly all the features found in the Win32 client. Others, such as the Mac OS X client, support only the most common feature subset.

For a breakdown of the features supported by the various clients, we recommend that you review the Citrix Feature Matrix, a Microsoft Excel spreadsheet that is downloadable from the Citrix website at

[http://download2.citrix.com/files/client\\_feature.xls](http://download2.citrix.com/files/client_feature.xls)

This file summarizes all the client features available and identifies which features are supported in each of the different clients. [Table 13.6](#) summarizes all the features available, along with brief descriptions of what each feature provides.

Table 13.6. Supported Win32 Client Features

Feature	Description
Core functionality	Core features supported by all ICA clients are:  1280x1024 resolution  24-bit color depth  Memory and persistent (disk) cache  TCP/HTTP server browsing  Disconnect/reconnect support  Encryption up to 128 bits  International keyboard support
Seamless windows	A published application appears as if it is running locally on the client's desktop.
Text Entry Prediction	SpeedScreen feature that provides the user with instant feedback to text entry regardless of whether the data transmission from the server is complete.
Panning	A client window can be set larger than the actual client desktop size. Panning allows the user to scroll the desktop view around to see different portions at one time.
Scaling	A larger client session can be shrunk to display within a smaller client device desktop size.

Feature	Description
Browser Acceleration	SpeedScreen feature that enhances processing of graphics in a web browser (Internet Explorer 5.5 or later) or email (Outlook or Outlook Express).
Multimedia Acceleration	SpeedScreen audio and video acceleration. Multimedia files are sent compressed to the client, and client-side resources decompress and play the content. This feature requires Enterprise or Advanced Editions of Presentation Server.
Image Acceleration	SpeedScreen feature. Images are compressed before sending them to the client.
Flash Acceleration	SpeedScreen feature. Macromedia Flash animation is rendered in a low-quality mode and sent to the client. This feature requires Enterprise or Advanced Editions of Presentation Server.
Dynamic Session Resizing	A desktop session can be dynamically resized by the user on the fly.
Client Device Mapping	This feature allows access to the local client device from within the MetaFrame session. The supported devices include drives, printers, COM ports, audio (client to server and server to client), and the Clipboard.
Auto Client Reconnect	If a client is disconnected due to a network or device failure, the client automatically attempts to reconnect to the server.
Roaming User Reconnect	If a user moves from one device to another, the user's session (active or disconnected) is automatically transferred from one location to the other when the user logs on.
Auto Client Update	This feature automatically updates the client based on settings in the Client Update Database.
Extended Parameter Passing	This feature allows the association of a local file type with a published application. It requires configuration on both the client and server to function properly. This feature provides functionality equivalent to client/server content redirection, a feature available only with PN Agent.
Content Publishing	This feature supports accessing content besides applications. Published content can include any type of file including documents, web links, or media files.
Content Redirection (Client to Server)	This feature enables integrated support only through PN Agent and requires Enterprise or Advanced Edition of Presentation Server. It allows local file associations to open applications published in the farm.
Content Redirection (Server to Client)	Server-based file associations can open applications that run locally on the client device. For example, a web link could be opened using a local Internet Explorer instead of the browser on the server.
Auto Printer Detection	This feature automatically detects and maps client printers in the MetaFrame session.
Universal Printer Driver	This feature substitutes a Citrix universal printer driver for the native driver associated with a client printer.

Feature	Description
Session Reliability	A feature that shields users from connection interruptions by setting the cursor to an hourglass and displaying an image of the user's session while it automatically attempts to re-establish a connection with the server.
SmartCard support	This feature allows authentication using a SmartCard and PIN.
NDS support	This feature allows authentication using Novell Directory Services.
SSL/TLS	This feature provides Presentation Server connectivity through the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) security protocols.
SOCKS 4/5 proxy support	This feature provides client connectivity through a SOCKS version 4 or 5 proxy server.
Auto Proxy Discovery	The ICA client attempts to retrieve the proxy settings from the default web browser for the device.  If the default browser is IE and is configured to automatically detect settings, the Win32 client ignores these settings and attempts a direct connection.
Secure Proxy	This feature supports connectivity through a Secure Proxy server. A secure proxy server uses SSL tunneling.
NTLM Proxy Authentication	When a proxy server supports NTLMv2 authentication, a Win32 client can provide the necessary credentials. Otherwise, only basic proxy authentication is supported.
Pass-through Authentication	This feature supports the use of local user credentials to automatically authenticate and access resources on the server.
Time Zone Support	The local time zone of the client device can be detected and used to display the appropriate local time for the user on the server.
Enhanced Unicode Keyboard Support	Enhanced keyboard support allows for input of text using alternate methods such as handwritten text entry or Microsoft Input Method Editors (IMEs), which allow input of foreign language characters such as Japanese characters on a standard keyboard.
Multiple Server Farm Support	The Web Interface and Program Neighborhood Agent support simultaneous access to applications within different server farms.
End-user Change Password	User password change support is provided from within the Web Interface.

## Alert

Although you are not expected to identify all supported options for each different client, you are expected to know all the features available to the Win32 client.

 PREV

NEXT 

# Program Neighborhood Client Configuration

In the following sections, we briefly review the configuration features for the Program Neighborhood client. We highly recommend that you take the time to familiarize yourself with the corresponding interface for each client. Hands-on practice with the configuration of each client will go a long way in preparing for the exam. As we've already mentioned, unlike the PN Agent and Web clients, the full Program Neighborhood client is not centrally managed. All configuration options must be set directly on the client, either through the interface or within the appropriate INI file before (or after) deployment.

## ICA Browser Settings

An extremely important concept to understand when it comes to the ICA client is that of ICA browsing. [ICA browsing](#) is the term used to describe the process that a client follows to discover MetaFrame servers on the network and gather information about published applications and the associated server farm.

### Alert

The Web and PN Agent clients do not perform ICA browsing. The task of discovering servers and accessing published application information is handled by the Web Interface and its direct communication link with servers in the server farm.

In the process of browsing, the client communicates with one of two services running on the MetaFrame server. The choice in service is dictated by the protocol chosen for use by the client:

- Citrix XML Service Provides published application information to either clients or the Web Interface, transmitting XML data using the HTTP protocol. For a client to communicate with the Citrix XML Service, it must be configured with the name of at least one MetaFrame server in the farm. If a valid server name is not provided, the client will fail to locate a server or server farm. The Citrix XML Service cannot be contacted using network broadcasts.
- [ICA Browser Service](#) Listens on User Datagram Protocol (UDP) port 1604 for published application or server requests from a client. Clients can communicate with the ICA Browser service either through directed or broadcast UDP requests. When sending a UDP broadcast, the client and server must reside on the same network for the client request to be received successfully by the server. After a client has successfully located a MetaFrame server, further communications occur through directed UDP requests to the ICA Browser service.

### Alert

Presentation Servers always respond to directed UDP client requests, but broadcast requests are acknowledged only when the server farm is operating in mixed (interoperability) mode.

ICA browsing is initiated in the following situations:

- A user attempts to view a list of servers or published applications when creating or editing a custom ICA connection.
- A user views the Application Set list when running the Find New Application Set Wizard.
- A user launches a published application. As part of the launching process, the client communicates with the farm to request a server on which to launch the application.

## Network Protocol Connection Options

PN allows you to specify the network protocol used to communicate with the server farm. The supported options available are

- TCP/IP+HTTP Published content is accessed using ICA over TCP/IP and ICA browsing is performed by transmitting XML data encapsulated in HTTP packets to the Citrix XML Service.
- SSL/TLS+HTTPS Published content is accessed using ICA encapsulated in SSL/TLS over TCP/IP. ICA browsing is performed by transmitting XML data encapsulated in HTTPS packets to the Citrix XML Service via the SSL Relay service. This combination provides strong encryption of ICA traffic combined with server authentication.
- TCP/IP Published content is accessed using ICA over TCP/IP. ICA browsing is performed by sending UDP packets (either broadcast or directed) to the ICA Browser service running on the MetaFrame servers.
- IPX/SPX and NetBIOS Windows 2000 Terminal Servers support client communications via IPX/SPX or NetBIOS. ICA browsing for all three protocols is done using the ICA Browser Service. Windows Server 2003 allows only TCP/IP-based Terminal Services client connections.

The network protocol to use is first set when a new application set or custom ICA connection is created and can be changed any time by editing the properties. Be certain that you are choosing the protocol supported by your target server farm. The client cannot detect during creation of the connection or application set whether the chosen protocol will be supported by the server.

### Alert

The full Program Neighborhood client is the only Win32 client to support protocols other than TCP/IP. The Web and PN Agent clients support only TCP/IP communications with the server farm.

## Global Program Neighborhood Client Properties

PN maintains a set of properties that are global to the client, whether you are using custom ICA connections or an application set to access published resources. On the Tools menu, you will find the three options that can be configured:

- ICA Settings The first and most detailed settings are found here. Four tabs contain global settings that you can configure. The first is the General tab, containing a variety of settings. Of note are the following settings:
  - Client Name The name defaults to the choice made during installation, which is usually set to dynamically match the client name.
  - Allow Automatic Client Updates Disabling this setting prevents client updates regardless of the Update Database settings.
  - Pass-through Authentication This option can be changed only if the user has administrative privileges. Pass-through support must have been selected during the client installation for the user to be able to use this setting.
  - Use Local Credentials to Log On This setting is enabled only if pass-through authentication has been enabled.

Next is the Bitmap Cache tab, which manages settings for the disk-based bitmap cache. The cache size can be altered, but the default value is the recommended setting of 10MB. The default cache location is within the user's Windows profile. The minimum sized bitmap to cache is 8KB by default.

The Hotkeys tab specifies the alternate key combinations to use to mimic the typical Windows hotkey behavior. For example, instead of pressing Ctrl+Alt+Del to bring up the Security window, you could define Ctrl+F1 as the alternate key combination within a MetaFrame session.

The Event Logging tab controls the plaintext log file settings for the client. The file is stored in the Application Data\ICAClient folder within the user's profile and is called wfcwin32.log. The log is automatically overwritten every time a new connection is established.

- Modems The second menu option under Tools simply opens the Windows Phone and Modem Options dialog box.
- Serial Devices For a serial device to be available to the PN and in turn accessible from within the MetaFrame session, the device needs to be added from within the Serial Devices dialog box. After adding a serial device, you can modify the standard serial properties such as communications speed, data bits, parity, and stop bits.

## Default Custom Configuration Settings

When you open the Custom ICA Connections view in Program Neighborhood, you manage the default options for custom connections by selecting Custom Connections Settings from the File menu.

Two tabs exist in the Custom Connections Settings: Connection and Default Options.

### Connection Tab

On the Connection tab, you define the global default server location settings, which are applied by

default to all custom connections that have not explicitly defined alternate settings. By adjusting the server location setting, you define how ICA browsing is performed for each of the available protocols. ICA Browsing was reviewed in the "[ICA Browser Settings](#)" section earlier in this chapter.

The available network protocols have been grouped together as HTTP/HTTPS, TCP/IP, IPX/SPX, and NetBIOS. Each protocol group maintains its own independent server list. When a custom ICA connection is created, the network protocol chosen for that connection dictates the corresponding server list that is assigned. For each protocol, up to three groups of five unique server addresses can be defined (Primary, Backup1, and Backup2). If no servers in the first group respond, the servers in the next group are contacted. If that fails, group three is used.

The default entry for TCP/IP, IPX/SPX, and NetBIOS is (Auto-Locate). This entry configures the associated protocol to attempt a UDP broadcast for the ICA Browser service. The default entry for the HTTP/HTTPS entry is "ica". Unless this entry is replaced with the name of a valid Presentation Server, the client will attempt to resolve the name "ica" to a valid IP address and use that to request farm information.

## Alert

Given a connection protocol and a configuration scenario, you should be able to identify whether the client will be able to successfully locate the desired server farm.

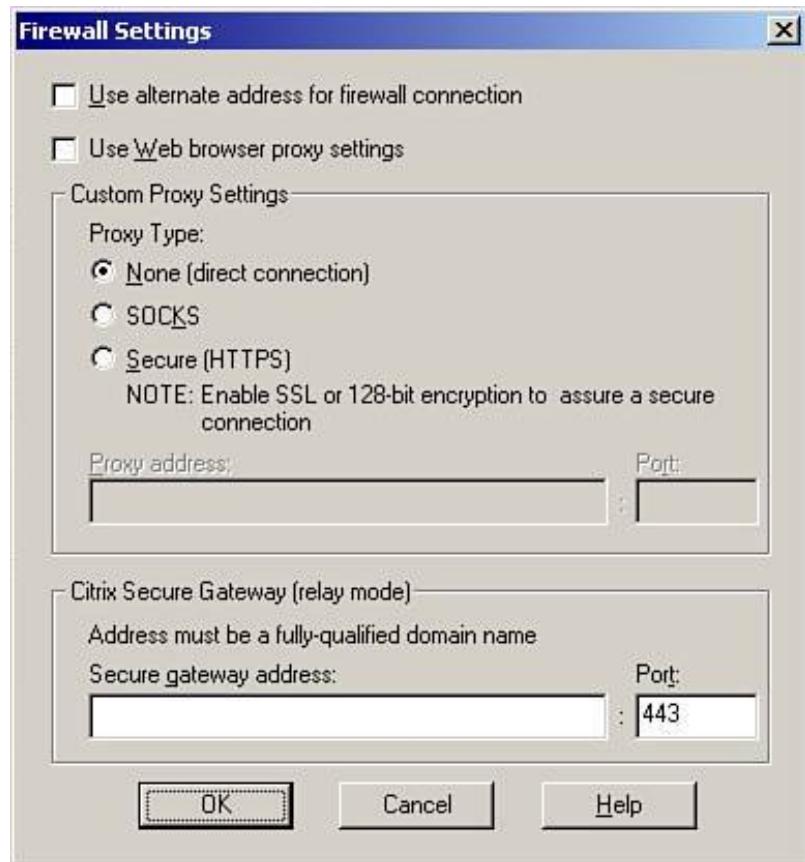
## Note

If you're not going to provide explicit server names in the server location list, Citrix suggests that you consider creating one or more DNS records for the "ica" name that point to valid MetaFrame servers instead of naming a server "ica". This way, you can leverage DNS round-robin to provide redundancy in the ICA browsing process.

When implementing MetaFrame connections using SSL/TLS+HTTPS, you must provide the fully qualified domain name (FQDN) for all MetaFrame servers that have been properly configured with a digital certificate using the SSL Relay Configuration Tool. The SSL Relay Configuration Tool is discussed in the next chapter.

On the Connections tab, look for the Firewalls button in the lower-right corner. This button brings up the Firewall Settings dialog box (see [Figure 13.7](#)).

**Figure 13.7.** Default firewall settings are applied to all custom connections.



The options in the Firewall Settings dialog box include

- Use Alternate Address for Firewall Connection When this option is selected, the client requests the MetaFrame server's alternate TCP/IP address. This setting is required when the PN client is directly accessing published resources located behind a firewall and network address translation (NAT) is being used to map an external address to an internal MetaFrame server address. By default, ICA browsing returns the true address of the MetaFrame server, which is not desired in an NAT scenario. Instead, the associated external address can be returned by the ICA Browser if this option is selected. The server must be configured with an alternate address for this to work properly. Configuration of the alternate address and firewall traversal are discussed in [Chapter 14](#).

This option is not required when you are using the Web Interface or if you are accessing a server directly using an external NAT address and not accessing a published application.

- Use Web Browser Proxy Settings This option uses the proxy settings defined for your default web browser to access the Presentation Server environment. If the default browser is Internet Explorer and it is configured to automatically detect settings, Program Neighborhood does *not* assign proxy settings but instead assumes no proxy settings are defined and attempts a direct connection.
- Custom Proxy Settings The PN client allows you to assign custom default proxy settings if proxy traversal is required to reach the MetaFrame server. If SOCKS or Secure (HTTPS) is chosen, you need to provide the address and port number for the associated proxy server.
- Citrix Secure Gateway Only if you will be accessing a MetaFrame environment through a Citrix Secure Gateway running in relay mode do you need to modify these settings. Provide the fully

qualified domain name of the Secure Gateway along with the port. The default port is 443. Version 2.0 or later of the Secure Gateway does not support operation in relay mode.

## Default Options Tab

Any of the settings configured on the Default Options tab apply to all custom ICA connections, unless the Use Custom Default check box is deselected.

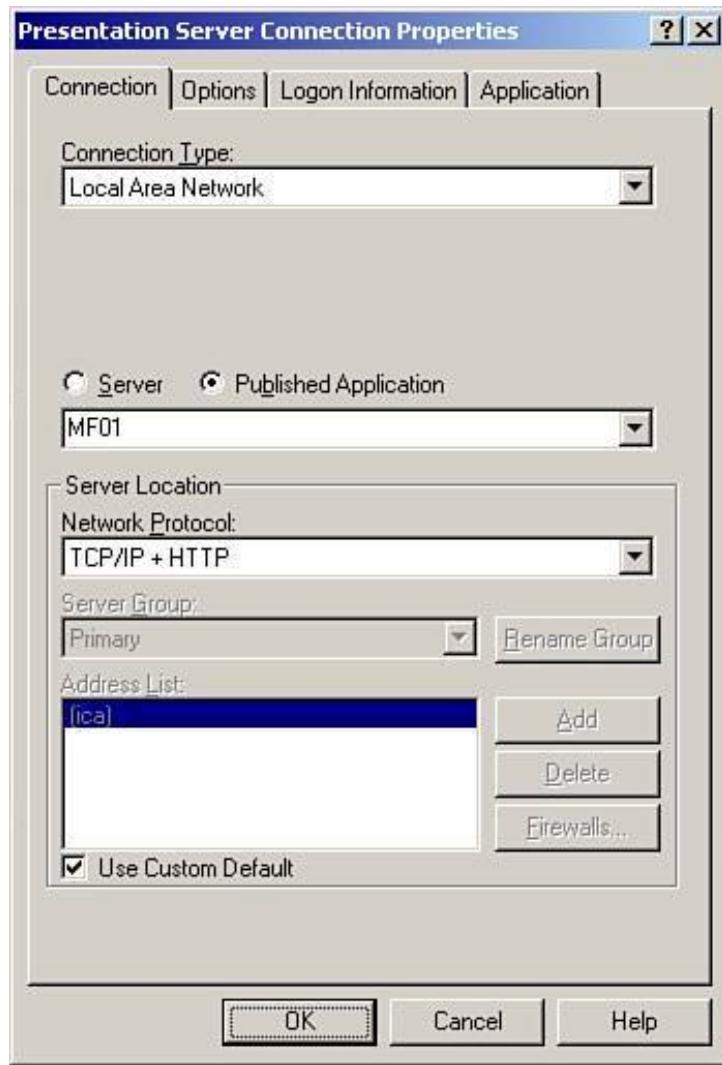
These settings include

- **Enable Sound** Enabling this option allows published applications to play sounds on the local client. The client must be equipped with a compatible sound card. The default sound quality assigned depends on the type of connection created. A LAN connection has sound defaulting to medium quality, whereas a WAN or dial-up connection has low-quality sound as the default.
- **Encryption Level** This setting assigns the default ICA encryption for all custom connections. It is recommended that 128-bit encryption be employed in all situations, even if data is completely contained on a local area network.
- **Window Colors** Four color options are available: 16 colors, 256 colors, high color (16 bit), and true color (24 bit).
- **Window Size** This setting is ignored if the published application is configured to run in seamless window mode. The options are fixed size, custom size, and percentage of the screen size (75%, for example), or you can choose to run the session in full-screen mode, completely hiding the local desktop, including the Start bar.

## Custom Configuration Connection Settings

To create a new custom connection, you need to use the Add ICA Connection Wizard. [Figure 13.8](#) shows the first of four tabs containing configuration information for a custom connection.

Figure 13.8. Custom ICA connections are created using the Add ICA Connection Wizard.



## Connection Tab

The Connection tab shows connection-specific information. The first option, the Connection Type setting, dictates what information appears on this tab as well as what settings are enabled by default under the Options tab. There are four connection types to choose from:

- Local Area Network Only the Use Data Compression Option is enabled.
- Wide Area Network When this setting is selected, both the Use Data Compression and Use Disk Cache for Bitmaps options are selected.
- Dial-Up Networking (PPP/RAS) If the client must be dialed into a private Microsoft network before being able to launch the MetaFrame session, you can select this option. A dial-up networking connection must already have been configured on the client before this option can be selected. Besides your having to choose a dial-up networking connection, all other options on this tab are the same as for a LAN or WAN connection. The same default options as the WAN connection are also enabled when you choose a dial-up networking connection.
- ICA Dial-In If the client will be directly dialing into the MetaFrame server, you should choose this option. When you do so, the standard settings are hidden, and you are then required to

select a configured modem on the client. After choosing a valid modem, you need to provide the phone number to dial to reach the host MetaFrame server.

Options such as the Server or Published Application setting and network protocol are not available when choosing dial-in. None of these settings are necessary as you are dialing directly into a MetaFrame server and not establishing any type of network-based connection.

The next option (unless you're using dial-in) allows you to select either a Server or Published Application as the connection target. If you know the name or IP address of the server, you can directly enter that information instead of selecting from the drop-down list. The population of the drop-down list depends on the Server Location settings.

## Options Tab

On the Options tab, you configure the "behavior" of the connection. The settings that you can manage here are

- Use Data Compression This setting is always enabled by default.
- Use Disk Cache for Bitmaps Over slower connections, this setting is enabled, allowing bitmaps to be cached to the local disk. The client maintains an in-memory cache, but larger and more images can be cached when the disk is enabled. WAN and dial-up connections enable this setting by default.
- Queue Mouse Movements and Keystrokes This setting is an older latency reduction feature of the Citrix client. It remains disabled for all clients. When it is enabled, mouse and keyboard updates are set less frequently, reducing the "chatty" tendency of ICA data. Bundling more data can improve performance over low-speed connections. This setting should normally remain disabled to improve responsiveness.
- Enable Session Reliability This setting is enabled by default, but is not available when you are performing an ICA dial-in connection. Session reliability is enabled by default for all other connection types.
- Enable Sound If you want to use high sound quality, you have to override the Use Custom Default and explicitly select High. High consumes substantially more network bandwidth. Medium is adequate for most LAN environments.
- Encryption Level This setting uses the custom default unless overridden.
- [SpeedScreen Latency Reduction](#) The client-side portion of the SpeedScreen Latency Reduction Manager, discussed in [Chapter 6](#), "Configuring and Administering MetaFrame Presentation Server" is configured on a per-connection basis, and the Auto setting is enabled by default, meaning that PN enables or disables SpeedScreen Latency Reduction based on the estimated network slowness. The Mouse Click Feedback option always defaults to being enabled, whereas Local Text Echo is always disabled by default.

### Note

Enabling or disabling SpeedScreen Latency Reduction on the client does not affect the other SpeedScreen optimization settings (also discussed in [Chapter 6](#)), such as SpeedScreen Browser or Multimedia Acceleration.

- Window Colors and Window Size This setting manages the size and color depth of the session. When connecting to a server, you have the Window Size settings that were discussed earlier when looking at window size defaults. If the connection is to a published application, an additional entry, Seamless Window, is added to the drop-down list box.

## Logon Information Tab

On the third tab, Logon Information, the logon configuration for the ICA connection is maintained. You must choose one of three configurations:

- Local User Select this setting to ensure users are prompted for logon information. If pass-through authentication has been enabled, the associated check box can be selected, eliminating the need for users to provide their credentials every time they log on to the server or published application.
- SmartCard This setting configures the client to require a SmartCard and associated PIN to authenticate against the server. The pass-through configuration is identical to the configuration that would be used when Local User was selected.
- User-specified Credentials PN can authenticate using the credentials that you provide here. If the Save Password option has not been disabled, you can cache the credentials for future use. If the farm is performing authentication using Novell Directory Services (NDS), the User Name field should be used for the NDS distinguished name, the password should be provided normally, and the Windows domain name field should be omitted.

## Application Tab

From the Application tab, you see one of two possible dialog boxes. When a *serverconnection* has been established you have the option of populating the Application field with the full path to an executable that resides on the server along with an associated Working Directory. This information is used to automatically launch the application after logging on to the server. This option provides legacy support for application launching but is not recommended as a substitute for using a published application. You also can modify the default icon if desired.

If the custom connection is a *published application* instead of a server, this tab provides a read-only view of the published application name. You still have the option to change the icon if you want.

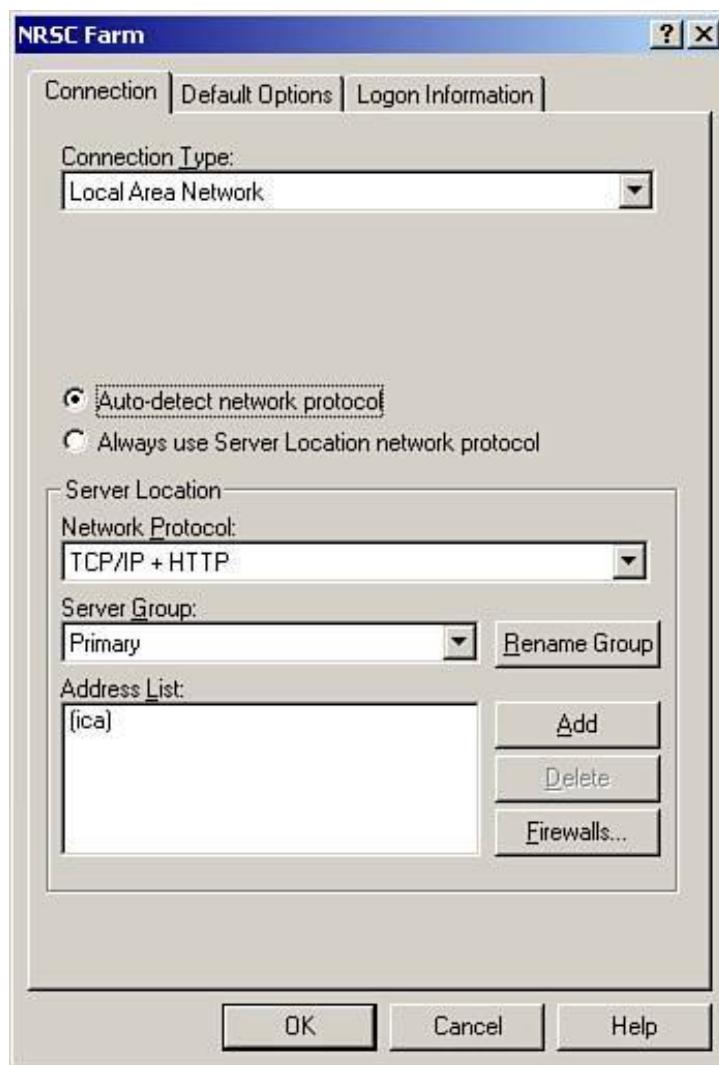
## Application Set Settings

Application sets and custom ICA connections share the same ICA Settings defaults, but application sets themselves do not have an additional set of global defaults. Each application set that is created must be configured with the necessary settings to be able to function.

You add application sets to PN by running the Find New Application Set Wizard. When finding an application set, you are defining the parameters required to find the associated server farm and retrieve the applications for users based on the logon credentials they provide. With an application set, unlike a custom ICA connection, you are not creating a shortcut to a specific server or published application. Instead, all the published application shortcuts available to you are automatically created based on your user credentials.

[Figure 13.9](#) shows the properties for an application set. When comparing properties for an application set and a custom ICA connection, you will find that these settings are nearly identical.

Figure 13.9. Application set properties are nearly identical to those belonging to a custom connection.



The properties that differ are as follows:

- The Connection tab supports a setting called Auto-Detect Network Protocol. This setting allows PN to attempt to auto-detect the appropriate protocol to use to find the application set.
- Under the firewall settings, the option to connect through a Citrix Secure Gateway operating in relay mode is not supported for an application set.
- Under the Options tab is a setting called Turn Off Desktop Integration for This Application Set. It disables the creation of desktop or Start menu shortcuts for applications in this application set, overriding the options defined within a published application.

- ICA dial-up connections are not available for use with application sets.

Multiple application sets can be created for a PN client, but a single application set can consist of applications drawn from only *one* server farm. You cannot have applications from different farms appear within one application set.

## Caution

Do not mix MetaFrame servers from different farms in the server location list. This produces unpredictable results when you are querying for applications.

 PREV

NEXT 

# Program Neighborhood Agent Client Configuration

There are two methods of client configuration for the Program Neighborhood Agent. The main location for PN Agent configuration is the Program Neighborhood Agent Console located on a server running the Web Interface. Details on the configuration of this portion of the client are discussed in [Chapter 14](#). The other configuration location is on the client where the PN Agent is running. Depending on the options defined on the Console, certain local features are available for configuration.

 PREV

NEXT 

## Web Client Configuration

The Web client itself has no user configuration component, and what few options can be configured are handled entirely through the Web Interface Console (see [Chapter 14](#)).

 PREV

NEXT 

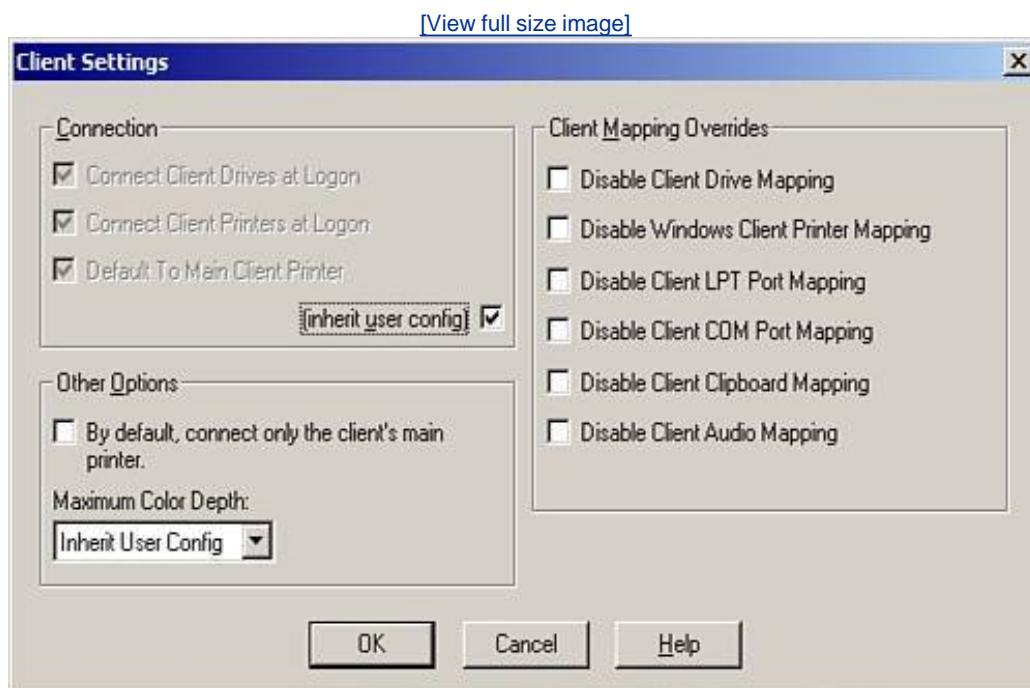
# Server-side ICA Connection and Session Configuration

The following sections summarize the server-side configuration options that impact the behavior of the client environment. Earlier in this book, we reviewed the specifics on how these options are configured, so here we simply provide the general feature and the location in the other chapters where you can find this information if you have not already covered it in the study material.

## Citrix Connection Configuration

The venerable Citrix Connection Configuration utility provides access to managing the core connection settings for the MetaFrame server. Similar options can be managed through the Terminal Services Configuration utility, but some settings are accessible only through the Citrix Connection Configuration utility. This utility is found in the Administrative Tools folder under the Citrix program group in the Start menu. [Figure 13.10](#) demonstrates some of the client settings that can be managed at the connection level. The use of this utility is discussed in [Chapter 6](#).

Figure 13.10. Citrix Connection Configuration is used to configure the base connection settings for the server.



## User Account Settings

Options can be defined within an individual user account that may take effect depending on the ICA

connection settings. Settings such as mapping of client drives or printers can be managed on a per-user basis in this way. Although the use of MetaFrame Policies is preferred, this option is still supported; see [Chapter 6](#).

## MetaFrame Presentation Server Policies

MetaFrame user policies allow an administrator to apply certain MetaFrame server settings to users based on their connection criteria and, hence, tailor the computing experience differently for different users.

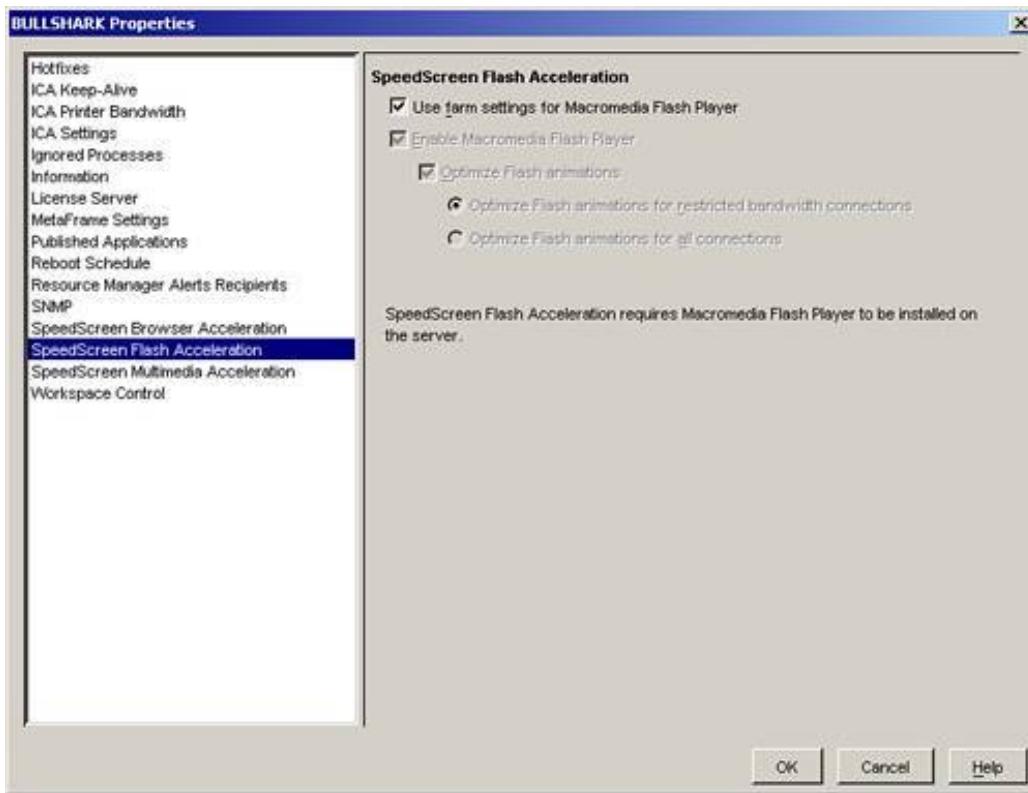
Options such as automatic client update and SpeedScreen settings can be managed through policies. The use of policies to perform client and user session configuration was discussed in [Chapter 7](#), "MetaFrame Presentation Server Policy Management."

## SpeedScreen Performance Enhancements

Citrix provides a number of SpeedScreen performance enhancements that are intended to improve the users' computing experience, particularly over lower bandwidth connections. Some of the SpeedScreen-related settings are managed within MetaFrame policies, whereas others are defined at the server farm and optionally at the server level. Unless overridden, all servers in a MetaFrame server farm use SpeedScreen acceleration settings defined at the farm level. Details on configuring the properties of servers and server farms was also discussed in [Chapter 6](#). [Figure 13.11](#) shows the SpeedScreen properties for a specific MetaFrame server. Notice how it defaults to using the farm settings.

Figure 13.11. Many of the SpeedScreen acceleration features are managed at the server farm or individual server level.

[\[View full size image\]](#)



◀ PREV

NEXT ▶

## Exam Prep Questions

1. Choose from the following list all clients that do not support running a MetaFrame Presentation Server client. (Choose all that apply).

A. Palm3 handheld PC

B. OS/2 Warp

C. FreeBSD

D. HP-UX

A1: Answers A and C are correct. Citrix does not currently have a Palm or a FreeBSD client. OS/2 Warp and HP-UX clients are both available for download from the Citrix site, so answers B and D are incorrect.

2. Which of the following statements is not true about MetaFrame Presentation Server clients?

A. Accessing published content via the Web Interface requires that the user run one of the Web clients.

B. The Presentation Server maintains basic connectivity support for older ICA client versions.

C. The ICA Client for Linux supports client printer mapping.

- D. The Client Update Database supports the automatic update of clients on multiple different platforms.
- A2: Answer A is correct. Of the four responses, this is the only false statement. Published content is accessible from any client that can run an ICA client and has a browser supported by the Web Interface. This includes client operating systems such as Macintosh and Linux.

Older clients can still connect even to the latest MetaFrame server version. The Linux client does support client printer mapping, and the Client Update Database automatically updates clients running on a number of different platforms. Therefore, answers B, C, and D are incorrect.

3. The latest version of the ICA Client can automatically be deployed using \_\_\_\_\_.
- 
- A. the Update Management Console
- 
- B. the Components CD-ROM
- 
- C. the Client Update Database
- 
- D. the Management Console for Presentation Server

- A3: Answer C is correct. The Client Update Database allows you to store the latest client images and automatically deploy them to users as they connect to servers in your farm.

Answer A is incorrect. It is not a valid name for a Citrix tool.

Answer B is also incorrect. Although the Components CD-ROM may contain the latest client image, it does not provide a mechanism for automating that deployment.

Answer D is incorrect because the Management Console for Presentation Server does not support the configuration and deployment of updated client images.

4. The Win32 MSI Client installation package is called \_\_\_\_\_.



A. ICA32.msi



B. Win32Pkg.msi



C. Win32Ica.msi



D. Ica32Pkg.msi

A4: Answer D is correct. Ica32Pkg.msi is the name of the Win32 MSI installation package that contains all three of the Win32 clients (Program Neighborhood, Program Neighborhood Agent, and the Web client). Therefore, answers A, B, and C are incorrect.

5. What is the name of the Program Neighborhood Agent self-extracting executable installation file?



A. A. Ica32.exe



B. Ica32p.exe



C. Ica32t.exe



D. Ica32a.exe

A5: Answer D is correct. Ica32a.exe is the self-extracting executable that installs the PN Agent client. Ica32.exe is the full PN client, Ica32t.exe is the Web client, and Ica32p.exe is not a valid Win32 client installation file. Therefore, answers A, B, and C are incorrect.

6. The installation steps for the Program Neighborhood Agent self-extracting executable are managed by what INI file?



A. install.ini



B. setup.ini



C. ctxsetup.ini



D. appsrv.ini

A6: Answer A is correct. When the contents of the PN Agent self-extracting executable are expanded, the install.ini file is edited to customize the client installation.

Answer B is not a valid setup filename. Answer C, ctxsetup.ini, is the install file for the Web client, and answer D, appsrv.ini, contains the configuration information for the full Program Neighborhood client.

7. You have received an updated Components CD-ROM and would like to place the latest clients into your Client Update Database. What utility can you run to automate this process?



A. ICA Client Update Configuration utility



B. ICA Client Migration utility



C. ICA Client Distribution Wizard utility



D. Management Console for Presentation Server

A7: Answer C is correct. The ICA Client Distribution Wizard can be used to load the client images off a Components CD into the Update Database.

Answer A is incorrect. Although the ICA Client Update Configuration utility is used to manage the Update Database and load in individual client images, it is not used to load the files directly off a Components CD-ROM.

Answer B is not a valid tool and so is incorrect.

Answer D is also incorrect. The Management Console does not contain any utilities for importing or managing the Update Database.

8. Which of the following answers best describe why you would want to install a pass-through client on your Presentation Server? (Choose all that apply.)

A. Your client device cannot run an ICA client, and you want the device to be able to connect to the MetaFrame server.

B. You want to be able to quickly test the configuration of your MetaFrame server.

C. You have a heterogeneous client environment, and you want to provide all users with access to the full Program Neighborhood client.

D. You want your clients to be able to pass application data seamlessly from their client device to the server.

A8: Answers B and C would best explain why you would want to install the pass-through client on your MetaFrame Presentation Server. From the server console, you could quickly launch the client to verify that the environment was configured the way you want. You can also use the pass-through client to provide users of non-Win32 client devices with access to the full Program Neighborhood client.

Answers A and D are incorrect. If a client cannot locally run an ICA client, it has no way of establishing an ICA connection to the MetaFrame server. The pass-through client is so named because it allows applications run on the server to transparently communicate with local resources such as printers and drives. It has nothing to do with allowing the passing of application data from the client to the server.

9. Which of the following are true concerning Presentation Server and ICA browsing? (Choose all that apply.)

A. A Presentation Server will never respond to UDP broadcasts.

B. The Citrix XML Service is installed on a Presentation Server by default.

C. The ICA Browser Service listens on port 1604 by default.

D. The Citrix XML Service listens on port 80 by default.

A9: Answer B is correct. The XML Service is a standard part of every Presentation Server installation.

Answer C is correct. The virtual ICA Browser Service listens on port 1604 for UDP ICA Browser requests.

Answer D also is correct. The XML Service listens on port 80 by default.

Answer A is incorrect. A Presentation Server responds to UDP broadcasts if it is running in interoperability mode. Only when it is running in native mode will it not respond to broadcasts. It will respond to directed UDP requests when running in either mode.

10. You are creating a new custom ICA connection and have selected the TCP/IP+HTTP network protocol combination. Which of the following options, if implemented, would allow successful browsing for the list of published applications? (Choose all that apply.)

A. Leaving the default server location address as (Auto-Locate) but ensuring that the farm is running in mixed mode.

B. Creating a DNS entry that resolves the ica hostname to a valid MetaFrame server name.

C. Assigning one or more MetaFrame servers to the server location list.

D. Ensuring the client is on the same subnet as at least one MetaFrame server.

A10: Answers B and C are correct. When you select TCP/IP+HTTP, the default server location address is the "ica" hostname. If a DNS record exists for that name and it resolves to a MetaFrame server, the client can successfully retrieve a list of published applications. If one or more servers are added to the server list, the client also can retrieve the published application list.

Answer A is incorrect. The default server location for TCP/IP+HTTP is not (Auto-Locate).

Answer D is incorrect because even if the client and server were on the same subnet, TCP/IP+HTTP does not perform any broadcasting. Within a valid hostname in the server location, the client will fail to retrieve a published application list.

11. From the following list of options, select all that can be configured as defaults for all custom ICA connections in the full Program Neighborhood client. (Choose all that apply.)

A. Primary address list for the TCP/IP network protocol

B. Enable sound and set the default sound quality to high

C. Set the minimum support color depth for the client connection to 16-bit (High color)

D. Enable the disk cache for bitmaps

A11: Answers A and C are valid options that can be defined as the default for all custom ICA connections.

Answer B is incorrect because even though you can enable sound by default, you are not able to set the minimum default sound quality to high. You must change the quality on a connection-by-connection basis.

Answer D is incorrect as well. You cannot set the disk cache status as a global property for all Custom ICA Connections.

12. Which of the following statements are true about application sets in the full Program Neighborhood client? Choose all that apply.

- A. Application sets share the same default ICA Settings as custom ICA Connections.
  - B. The applications available within an application set are dictated by the logon credentials used to authenticate against the farm.
  - C. Applications from different farms can be combined within a single application set view as long as they are not published with the same name and at least one server from each farm is listed in the Server Location properties for the application set.
  - D. An application set can be centrally managed through the Program Neighborhood Agent Console if the Use Program Neighborhood Agent Properties option is enabled within the application set properties.
- A12: Of the four choices, only Answers A and B are correct. Both Custom ICA Connections and Application Sets share the same default ICA Settings. The list of applications that appear within an Application Set are also dictated by the credentials with which the user logs on to the farm.
- Answer C is incorrect because applications from different farms cannot be combined within a single PN application set. Mixing servers from different farms in the server location list is not recommended. Applications from multiple farms can be combined into a single view using either the PN Agent client or the Web Interface.
- Answer D is incorrect because the full PN client cannot leverage the central management features found in the PN Agent client. The two are completely distinct. There is no Use Program Neighborhood Agent Properties option in the PN client.
13. A desktop support technician calls you and asks you how he can modify the configuration of a user's ICA Web client so that he can enable sound. Choose the appropriate answer for the support technician. (Choose one.)

- A. The Web Client settings can be modified within the APPSRV.INI file located in the user's profile folder.
- B. The Web Client settings are modified within the ICAWEB.INI file located in the user's profile folder.
- C. The Web Client settings are modified within the TEMPLATE.ICA file located in the user's profile folder.
- D. The Web Client settings are managed through the Web Interface Console and cannot be modified from the user's client.

A13: Answer D is correct. The Web Client has no client-side configuration options available. All settings are done through the Web Interface Console. Hence, answers A, B, and C are all incorrect.

The APPSRV.INI file is used by the full Program Neighborhood client, there is no such configuration file called ICAWEB.INI, and although the TEMPLATE.ICA file contains the client options that are read by the Web Client, these settings are defined on the web server and passed down. They cannot be modified on the client prior to being interpreted by the Web Client.

 PREV

NEXT 

# 14. Web Access to the MetaFrame Server Farm

Terms you'll need to understand:

- Web Interface
- Citrix XML Service
- ICA template file
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- Secure Gateway
- Session ticketing
- Client-side proxy
- WebInterface.conf
- Network address translation (NAT)
- Citrix SSL Relay
- Secure Ticket Authority (STA)
- Secure Gateway Proxy
- Double-hop demilitarized zone (DMZ)

Concepts and techniques you'll need to master:

- Identifying components of the Web Interface
- Identifying steps in the authenticating and launching of client applications through the Web Interface
- Understanding and identifying features of the Web Interface
- Identifying security features of the Web Interface
- Configuring the Web Interface
- Managing network address translation with the Web Interface
- Identifying Secure Gateway Components
- Choosing appropriate deployment configuration given a specific scenario

Citrix's Web Interface provides users with access to the suite of applications to which they have been assigned. The Web Interface itself is made up of three components (as depicted in [Figure 14.1](#)):

- One or more server farms The Web Interface acts as a form of the Program Neighborhood interface to collect and display application set information for a user. Unlike the full PN client, the Web Interface can query multiple server farms using the provided user credentials and create a consolidated view of applications from these farms in a single application set dynamically displayed in an HTML page.

The Web Interface communicates with the servers in the different server farms via the Citrix XML Service. The Web Interface must be able to communicate with a minimum of one server running the XML Service in each farm from which it is required to retrieve application set information.

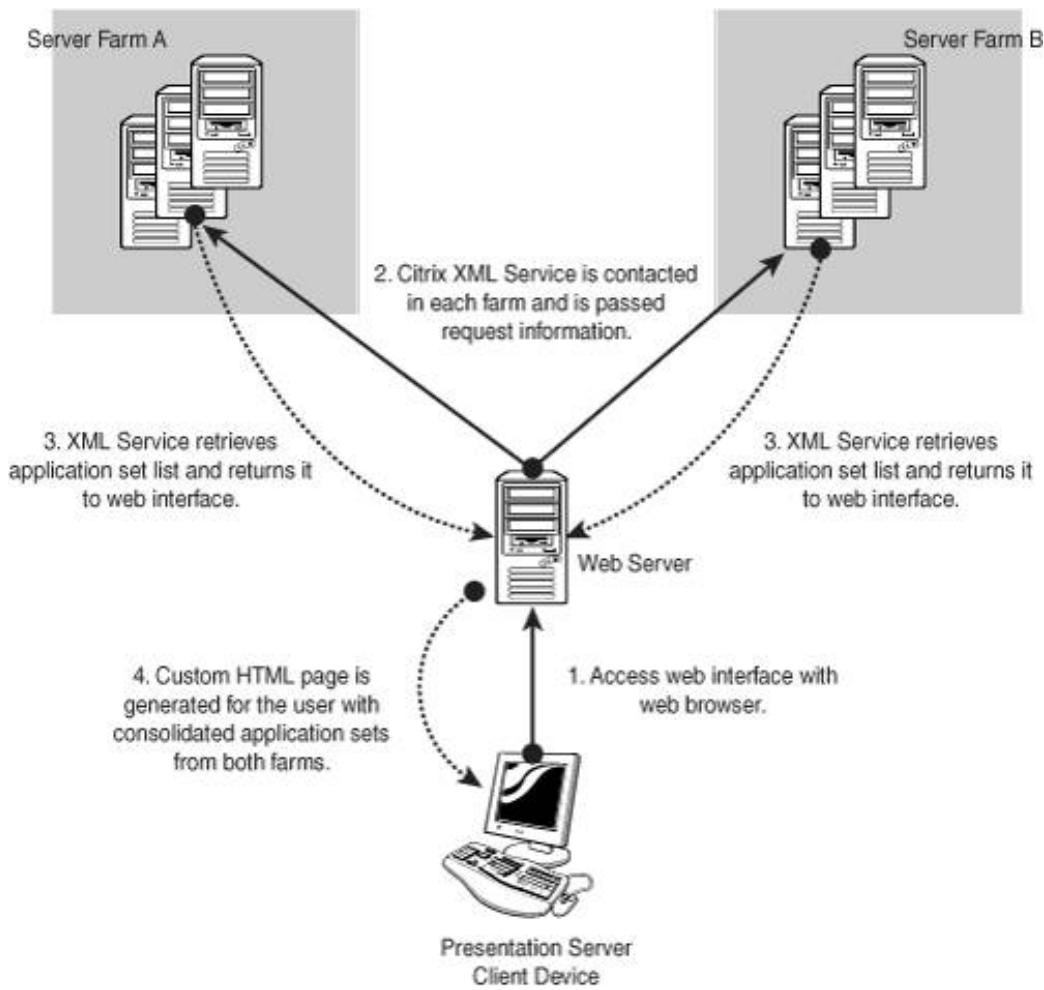
- A web server The Web Interface itself is installed on a web server. Although the web server can run Presentation Server, it is not required to do so, and a dedicated web server is recommended in most production implementations.

The Web Interface can operate as a standalone website dedicated for application access or can be integrated into a new or existing corporate web portal.

- [\*\*Presentation Server client\*\*](#) device Any device that can support a Presentation Server client and web browser can be used with the Web Interface. The browser and client work in tandem to provide users with application access. The web browser requests user credentials and displays the corresponding list of applications the user can access. When an application hyperlink is clicked, the Presentation Server client comes into play, providing the mechanism for actually connecting to the published application.

Figure 14.1. A Web Interface deployment requires three network components.

[\[View full size image\]](#)



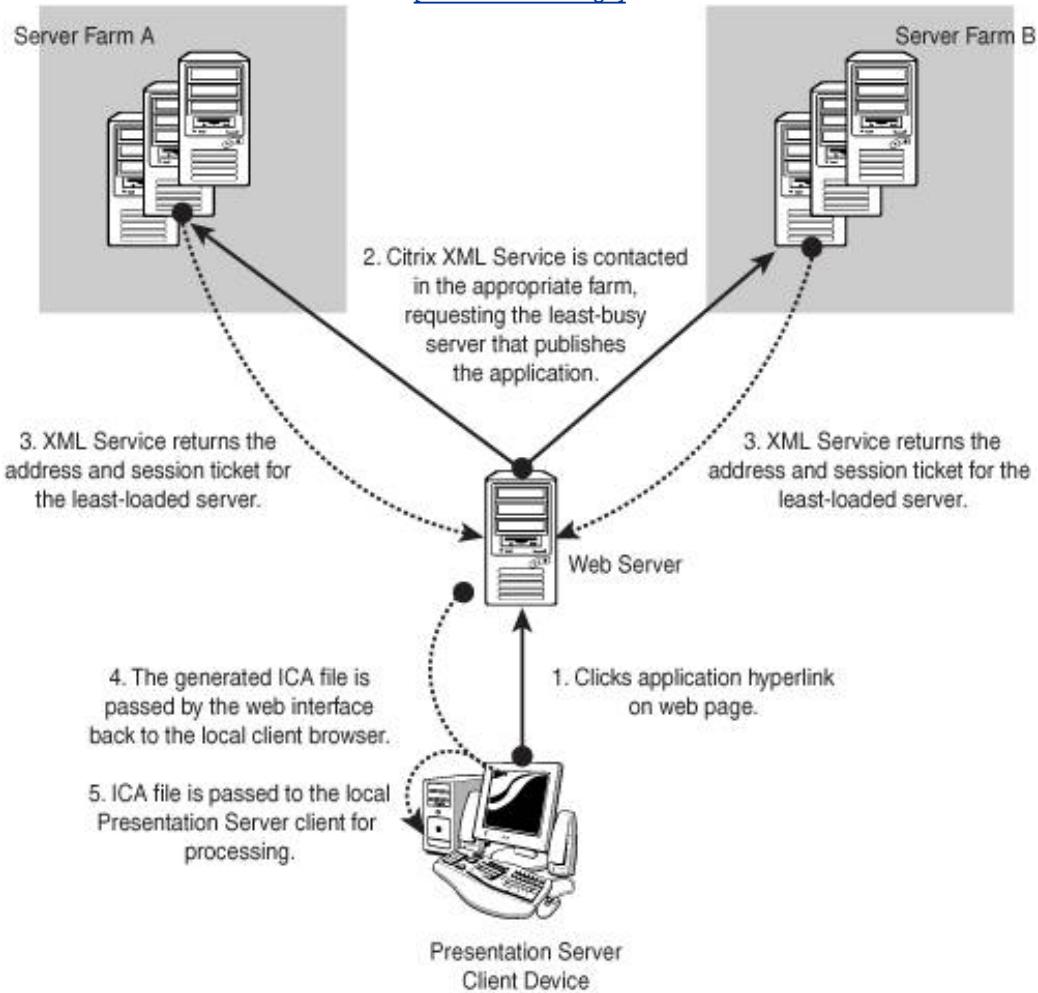
[Figure 14.1](#) also summarizes the steps involved in generating an application set for a user. The steps are as follows:

1. The user accesses the Web Interface and provides the requested credentials. The information is passed from the client to the Web Interface.
2. The Web Interface receives the user's credentials and forwards this information to a Citrix XML Service in each of the defined server farms.
3. The XML Service then builds the application set for the user based on the information it receives from the IMA and Program Neighborhood services. Once generated, the application set information is returned to the Web Interface.
4. Based on this application set information, the Web Interface then generates an HTML page containing links to each of these applications.

The next stage of interaction between the client, the Web Interface, and the server farm occurs when a user clicks an application link. [Figure 14.2](#) demonstrates the steps followed to launch the application requested by the user.

Figure 14.2. The client, Web Interface, and specific servers in the server farm interact when a user clicks an application hyperlink.

[View full size image]



The specific steps are as follows:

1. Clicking an application hyperlink initiates a request on the web server to retrieve an ICA file specific for that application. The ICA file contains all of the information required for the client to establish a connection to the specified published application.

The Web Interface does not maintain a list of hard-coded ICA files for each published application. Instead, it has access to a template ICA file, which contains special fields called *substitution tags*. The special Java classes in the Web Interface replace these substitution tags with information specific to the application before passing it to the client.

2. The Citrix XML Service is contacted in the appropriate server farm to retrieve the connection information for the least-busy server that publishes the requested application. A session ticket is then retrieved from this MetaFrame server for the user's application request.
3. The application, server address, and session ticket information are then passed by the XML Service back to the Web Interface.
4. The Web Interface does not maintain a list of hard-coded ICA files for each published application. Instead, it has access to a template ICA file, which contains special fields called *substitution tags*. The special Java classes in the Web Interface replace these substitution tags with information specific to the application before passing it to the client. The Web Interface completes the replacement of the substitution tags in the template.ica file with the information received by the XML Service. This file is then passed back to the client's web browser.
5. The web browser then passes the ICA file to the Presentation Server client, typically through a file association, and the PS client then uses the information within the ICA file to launch the actual MetaFrame published application connection.

## Alert

Having the opportunity to perform some hands-on work and launch applications via the Web Interface will help in understanding these steps.

You should clearly understand the steps involved when a user initiates a connection with the Web Interface, logs on to the environment, and selects a valid application hyperlink.

[Listing 14.1](#) demonstrates a small portion of a typical template.ica file. This file, along with guest and wide area network templates, can be found on the Web Interface server in the Citrix\MetaFrame\conf folder under the Web root.

### Listing 14.1. Portion of the Default template.ica File

```
[Encoding]
InputEncoding=[NFuse_Template_Encoding]

[WFCClient]
Version=2
ClientName=[NFuse_ClientName]
[NFuse_TransportReconnect]
RemoveICAFfile=yes
```

```
[NFuse_ProxySettings]
ProxyTimeout=30000

[NFuse_COMPortMappingSetting]
[NFuse_ClientPrintingSetting]

[ApplicationServers]
[NFuse_AppName]=

[[NFuse_AppName]]
Address=[NFuse_AppServerAddress]
InitialProgram=#[NFuse_AppName]
LongCommandLine=[NFuse_AppCommandLine]
DesiredColor=[NFuse_WindowColors]
Launcher=WI
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
[NFuse_ClientLogon]
[NFuse_ProxySettings]
ProxyTimeout=30000
```

All entries in the file that have the prefix **NFuse\_** and are contained within the square brackets **[ ]** represent the substitution tags.

In the following sections, we discuss the configuration of the Web Interface and how many of these settings can influence the way the ICA file is generated for the client.

 PREV

NEXT 

# The Web Interface 3.0 Feature Summary

[Table 14.1](#) summarizes the key features of the Web Interface for MetaFrame Presentation Server 3.0.

Table 14.1. Web Interface Feature Summary

Feature	Description
Active Directory and Novell Directory Services (NDS) support	User authentication is integrated with Microsoft Active Directory or NDS. User Principal Names (UPN) can also be used when providing user credentials on the Web Interface authentication page. A UPN typically appears as <i>name@domain.com</i> . NDS authentication is supported only when running the Web Interface on IIS.
ActiveX client deployment control	The Web Interface allows you to define the specific version and class ID of the Web Client and Remote Desktop Connection ActiveX controls that you want to deploy to the end user.
Anonymous user logon	Users can log on to the farm using an anonymous account (an account requiring no user ID and password), providing support for kiosk-type implementations using the Web Interface.
Application and content publishing support	Published applications and content can be accessed through the Web Interface. Configuration options for published content and applications are managed through the ICA template files.
Improved address translation support	Address translation options can be created within the Web Interface. These options are based on the client subnet address and subnet mask rules that you define. When users connect from a given subnet, the associated address translation rules can be automatically applied, ensuring that users are always connecting to the proper servers.
Multiple site support with IIS	When an IIS server is hosting more than one website, you can specify the target site where the Web Interface will be hosted. Multiple instances of the Web Interface can be deployed on different sites on the same server.

Feature	Description
Personal Digital Assistant/Windows-based Terminal Support	Citrix supports accessing the Web Interface on a limited range of PDA and WBT devices, including those running PocketPC 2002 or later.
Presentation Server client deployment	The Web Interface allows you to control deployment of Presentation Server clients to any device with a web browser. The Web Interface can detect the client and browser type, presenting the user with the appropriate client for installation. Only the presence of the 16- and 32-bit clients can be detected and the installation request shown or hidden as required. For all other client types, the option to install the client is always shown.
Presentation Server/IIS Server integration	Citrix supports the integration of Presentation Server and IIS running on the same server and sharing port 80 between IIS and the Citrix XML Service. This is made possible by the Internet Server Application Program Interface (ISAPI) extension that is part of the Citrix XML Service.
Presentation Server load balancing and failover support	The Web Interface allows you to define references to multiple servers hosting the XML Service. This ensures applications remain accessible even if the primary reference is unavailable. References can be load-balanced, which is the default, or accessed sequentially, failing over to the next server if the previous one was unavailable.
Program Neighborhood Agent Integration	The Web Interface also integrates with the Program Neighborhood Agent. The PN Agent allows access to published applications through the Web Interface without requiring the use of a web browser. For more details on the Web Interface, see the section titled " <a href="#">The Program Neighborhood Agent</a> " later in this chapter.
Remote Desktop Connection support	Microsoft's ActiveX client for RDP is natively supported in the Web Interface, but with limited features compared to the Citrix clients. See the section " <a href="#">Remote Desktop Web Connection Software</a> " for more information on this client support.
Secure Gateway for Presentation Server	The Secure Gateway, included as part of Presentation Server, provides a single point of secured access into your server farm. Specifically created to secure access to the farm from untrusted networks (such as the Internet), the Secure Gateway is discussed in the " <a href="#">Securing Server Access with the Secure Gateway</a> " section of this chapter.
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) support	SSL/TLS is supported for securing communications between the Web Interface

Feature	Description
	server and the XML Service on MetaFrame servers in the farm. On the Windows platform, SSL and TLS support is provided by Microsoft's Secure Channel (SChannel) security package.
Session authentication tickets	Instead of user credentials being passed within a generated template ICA file, the Web Interface employs special authentication tickets that are used to validate a user's access to published content. Once used, or if the expiry date has passed, the ticket can no longer be used for authentication. To support ticketing, the Citrix XML Service must be running on all servers in the farm and listening on the same port. By default, the XML Service is installed as part of Presentation Server and listens on port 80.
Support for multiple server farms	As we already mentioned, application sets can be retrieved from multiple server farms and displayed to the user. Server farms must be in trusted domains in order to share one set of user credentials.
Unicode support for ICA template files	You can configure the Web Interface to generate a Unicode-based ICA template file when a user clicks an application link in the web browser. Unicode is a 16-bit encoding scheme (compared to 8-bit for ASCII), allowing the combination of character sets from different languages (European, Japanese, Chinese, and so on) to be represented in a single character set. Encoding the ICA template files in Unicode greatly expands the usability of the Web Interface in non-European countries.
Workspace Control	Workspace Control allows a user to quickly connect, disconnect, or log out of all running applications. Workspace Control can allow users to quickly access applications, even if they have been left connected at another terminal.

## Note

Certain Web Interface features are available only when a given Presentation Server and client version are used. For example, the Workspace Control feature requires MetaFrame Presentation Server 3.0 and ICA Client version 8.0 or higher. A complete list can be found in Citrix's "Web Interface Administrator's Guide." All the features discussed are available when using the latest version of Presentation Server and ICA client.

 PREV

NEXT 

# Web Interface Installation Requirements

Some general installation requirements exist for the Web Interface itself. They are broken down into the three categories discussed earlier: the MetaFrame Server, web server, and Presentation Server client device.

## MetaFrame Server Requirements

[Table 14.2](#) lists the MetaFrame versions supported by the Web Interface. As noted already, not all Web Interface features are available with all versions of Presentation Server.

Table 14.2. MetaFrame Versions Supported by the Web Interface

Citrix Platform	Windows 2000 Server	Windows Server 2003	Windows NT 4.0, Terminal Server Edition	UNIX
MetaFrame Presentation Server 3.0	X	X		
MetaFrame XP for Windows with SP2			X	
MetaFrame XP for Windows with SP3	X	X		
MetaFrame 1.8 for Windows with FR1 and SP3	X		X	
MetaFrame Presentation Server for UNIX				X
MetaFrame for UNIX version 1.1 with FR1				X

## Web Server Requirements

The Web Interface can run on either the Windows or UNIX platform. On the Windows platform, the Web Interface runs on either of the following:

- Internet Information Services (IIS) 6.0 on Windows Server 2003
- IIS 5.0 on Windows 2000 Server with SP4

Prior to installing the Web Interface, you must also install the following software components:

- .NET Framework 1.1 (Windows 2000 Server only) Install IIS on the server prior to installing the .NET Framework. This ensures that ASP.NET is also installed.
- ASP.NET ASP.NET is installed with the .NET Framework on Windows 2000 Servers as noted in the preceding point. On a Windows Server 2003 server, ASP.NET is installed if you enable IIS as part of the Windows installation, or you must explicitly select it if IIS is installed after Windows has been installed.
- Visual J# .NET 1.1 This and the .NET Framework 1.1 are both included in the Support folder on the MPS CD-ROM.

## Presentation Server Client Device Requirements

To access and log on to the Web Interface, you need a web browser. Although many different web browsers can be used to perform this function, Citrix officially supports only specific operating system/web browser combinations. The latest available list can be found on the Citrix website. If a browser does not appear in the list, it does not mean that a particular web browser cannot function with the Web Interface. It means only that the browser has not been tested and approved by Citrix.

All ICA client versions that ship on the Components CD-ROM and run on an operating system that supports a compatible web browser are compliant with the Web Interface.

Citrix recommends that you run the latest available client version to ensure that the latest features and capabilities are available to users.

 PREV

NEXT 

# Installing the Web Interface

On either platform, it is highly recommended that you follow all web server security guidelines. On a Windows server, you must ensure that the file system is running NTFS and not FAT. Access to the Web Interface Console, where configuration changes are managed, relies on NTFS security. On a FAT file system, no authentication is performed, allowing nonadministrators to manage the Web Interface.

The installation process on either platform is straightforward. Here are some general notes regarding the Web Interface installation:

- During the installation, you are prompted to provide the TCP/IP port number that the XML Service is listening on. By default, this service listens on port 80. From within the Management Console for Presentation Server, you can view the current XML port setting by opening the properties for the specific server.
- You are also prompted to install the ICA Client images onto the web server. These images are used to deploy the ICA client to any device that connects to the Web Interface. You can provide client images from the Components CD or from files downloaded from the Citrix website. Client installation images are copied under the following folder:

*<Web root>/Citrix/ICAWEB/<language>/<clientplatform>*

*<Web root>* is the root of the web server structure, *<language>* is the two-character language code (en is used for English, for example), and *<clientplatform>* is the folder that contains the client files specific to that platform. If you decide to add client images manually, make sure you create the proper folder structure.

After the Web Interface has been installed, it is immediately ready for use, although you will likely want to perform additional configuration or customization tasks.

You can test the Web Interface by navigating to the site using a supported web browser. If the Web Interface is configured as the default page, it opens when you provide the URL for the server; otherwise, you need to provide the full URL:

`http://<servername>/Citrix/MetaFrame`

# Configuring the Web Interface

The two methods for configuring the Web Interface are as follows:

- **Web Interface Console** Available only when the Web Interface is run on a Windows IIS web server (it is not supported on a UNIX web server), the Web Interface Console is a Web-based graphical interface, within which you can quickly perform common administrative tasks. Many of the settings within the Web Interface configuration file can be directly modified using the Web Interface Console. The Web Interface Console is accessible from any client running Internet Explorer 5.5 or later. Non-Microsoft Web browsers are not currently supported.
- **Web Interface configuration file** The configuration method available on both Windows and UNIX systems, the specific file, called `WebInterface.conf`, is a plain-text file that you can edit to modify many of the Web Interface properties. On Windows, this file is located by default in the following folder:

`<WebRoot>\Citrix\MetaFrame\conf`

On UNIX, it is in the following folder:

`<WebRoot>/Citrix/WEB-INF`

In both cases, `<WebRoot>` represents the path to the appropriate root web folder of the web server. Before any changes made to the configuration file take effect, you must stop and restart the web server service. A full summary of all supported commands is provided in the "Web Interface Administrator's Guide."

## Alert

Web Interface configuration focuses on the use of the Web Interface Console and the features it can manage instead of the fields that can be edited in the `WebInterface.conf` file.

## Note

You can also write custom web server scripts or Java servlets to customize the Web Interface site. Citrix provides a special guide called "Customizing the Web Interface" that provides information on how this can be achieved.

As mentioned, the Web Interface Console is available only when you run the Web Interface on Microsoft IIS. The URL to access the Console is

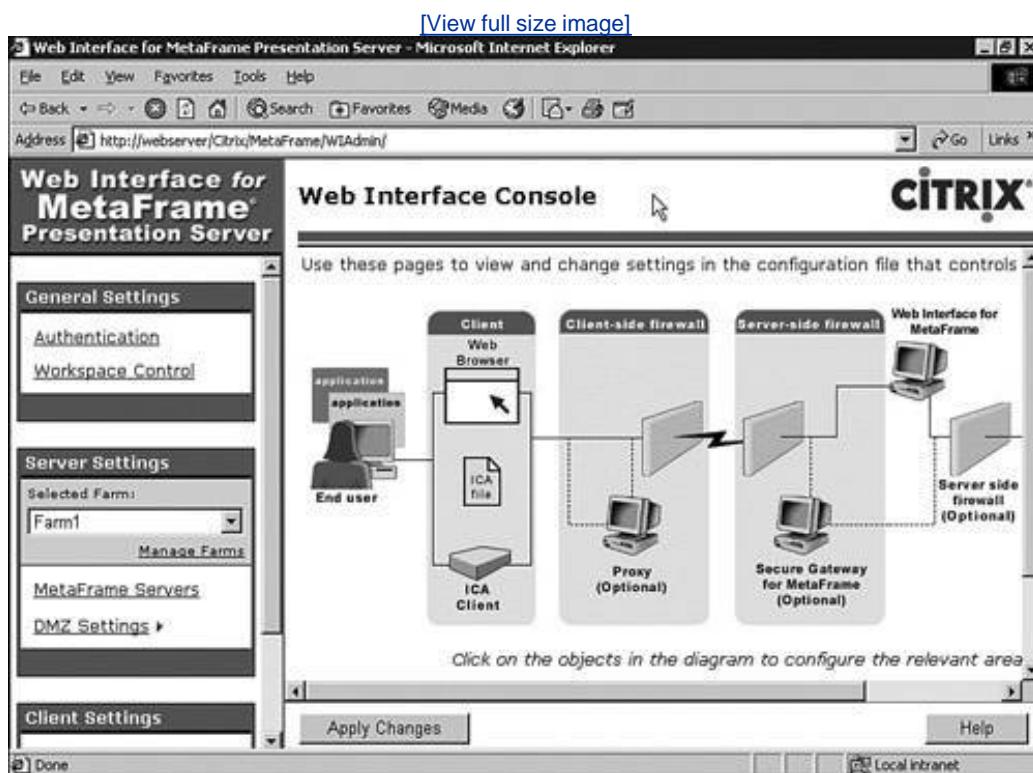
`http://<servername>/Citrix/MetaFrame/WIAdmin`

where <servername> is the server running the Web Interface.

To be authorized to access the Console, you must belong to the *Local*/Administrators group on the server. If the Console cannot automatically authenticate you, you are prompted to provide the necessary credentials.

After you are authenticated, the main Web Interface Console page appears (see [Figure 14.3](#)). The page is laid out to represent all the possible components that could make up a Web Interface environment. On this main page, you see the Apply Changes button. Until this button is clicked, any changes made on the individual configuration pages will not take effect until the web server is restarted. Clicking this button immediately applies the changes to the live system.

Figure 14.3. The main Web Interface Console page gives a graphical view of the managed environment.



You manage configuration settings either by clicking an image in the component diagram or by choosing one of the links down the left side of the page. For example, clicking the Authentication link takes you to the same settings as clicking the "Web Interface for MetaFrame" image.

[Table 14.3](#). cross-references the link names with the images in the component diagram.

Table 14.3. Setting Link and Component Diagram Image Cross-Reference

Link Setting	Diagram Component
Authentication	Web Interface for MetaFrame
Workspace Control	End User
Selected Farm	(no equivalent)
Manage Farms	"(Multiple MetaFrame Farms can be added)" text
MetaFrame Servers	"Servers" icon under MetaFrame Farm
DMZ Settings	
Network Address Translation	Server-side firewall
Secure Gateway Support	Secure Gateway for MetaFrame
Client-side Proxy	Proxy
Client Deployment	Web Browser
Client Customization	ICA Client

## General and Client-Side Settings

In this section, we review the configuration settings of the Web Interface.

### Authentication

Authentication allows the configuration of the authentication methods available when logging on through the Web Interface. Citrix strongly recommends that you enable only those authentication methods required by your users. Any changes to the authentication for the Web Interface require any active users to close and restart their web browser; otherwise, error messages may appear. The following authentication methods are available:

- **Anonymous** A user can access the server without providing a user ID or password. The use of anonymous authentication is not recommended with the Secure Gateway for MetaFrame because it can allow a user to still receive Secure Gateway tickets.
- **SmartCard** A user authenticates by inserting a SmartCard into a SmartCard reader attached to the client device. The user is requested to enter a PIN to complete authentication. SmartCard with Single Sign-on eliminates the user's having to enter a PIN again to log on to the farm. SmartCard authentication is not available when running the Web Interface on UNIX. SSL must also be enabled on the IIS server for SmartCard authentication to function properly.
- **Single Sign-on** The user credentials used when logging on to the Windows desktop are used to automatically authenticate within the Web Interface. Single Sign-on should be used only over a secured connection.
- **Explicit Login** The default setting, this requires the user to provide a user ID and password to log on to the Web Interface. You can choose either Windows domain or Novell NDS authentication. Three general settings apply to either Windows domain or NDS settings. You can allow users to change their passwords. You can also configure two-factor authentication using

RSA SecurID or Safeword. The Time To Live value specifies how long a ticket used for explicit authentication is valid before it expires. The default is 200 seconds, but you can adjust this value.

## Note

For security reasons, when two-factor authentication is enabled, the PN Agent cannot be used to access applications via the Web Interface.

Here's one issue to note if you decide to enable the changing of passwords through the Web Interface. If you have multiple server farms defined for the Web Interface and the farms are in separate domains, some farms do not support password changes, or a farm contains a mixture of UNIX and Windows servers, Citrix recommends that you not enable support for the changing of passwords. When you make a password change, the Web Interface contacts each server farm in the order specified until the change request is honored by a farm. At that point, the change password request completes.

## Note

When multiple farms reside in different domains and are accessed through the Web Interface, a two-way trust must exist between these domains in order for the application enumeration and access to function properly.

## Workspace Control

Workspace Control options are managed within this setting. As we mentioned earlier in this chapter, Workspace Control allows a user to quickly disconnect all running applications, log completely out of all running applications, or reconnect to all of the user's applications, whether disconnected or active at another client device. Workspace Control does require version 8.x or higher of the ICA client.

If users are given the option to override the setting choices you've made on this screen, they see reconnect settings to the Web Interface.

## Client-Side Proxy

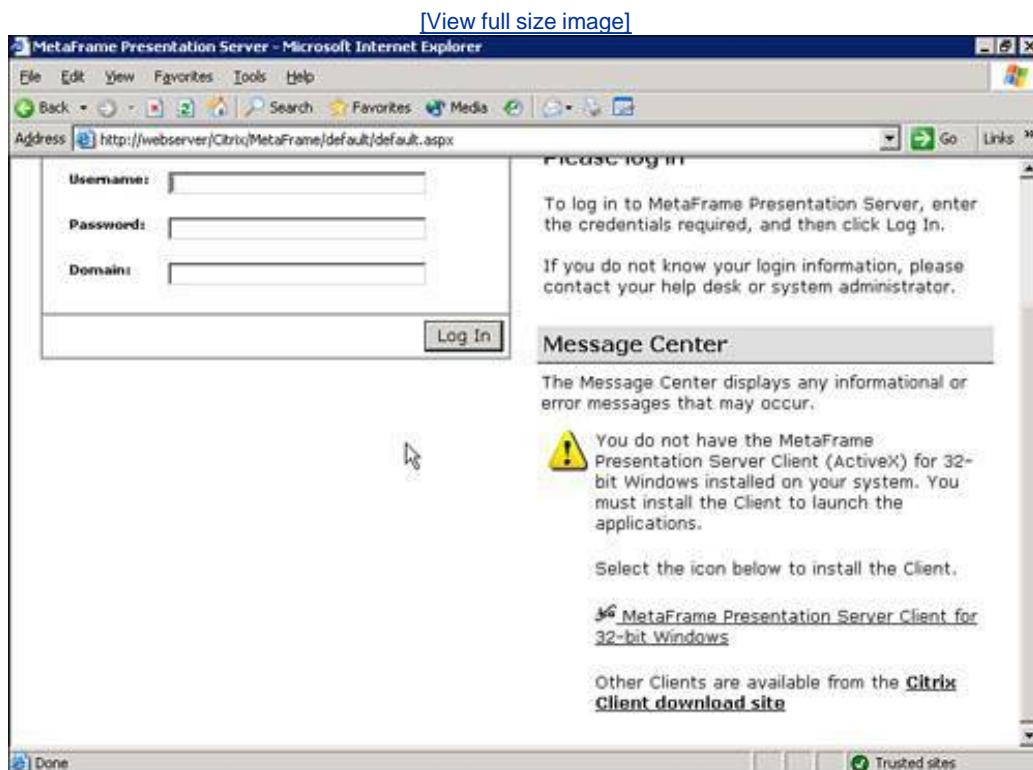
When a proxy server is employed on the client-side of the Web Interface, you can define settings here that dictate whether the Presentation Server client must communicate through the proxy server when connecting to a MetaFrame server.

## Client Deployment

The deployment of Presentation Server clients is managed through the client deployment settings page. The client deployment feature provides a powerful and convenient mechanism for ensuring that

your end users have the appropriate client installed. Client installations are advertised in the Web Interface through installation captions in the Message Center portion of the logon page. [Figure 14.4](#) shows what an installation caption looks like in the Message Center.

Figure 14.4. Installation captions prompt the user to install the appropriate client if necessary.



Near the bottom of the client deployment settings page is the Display Client Installation Caption option. It allows you to force captions on or off, or allow them to be auto-detected. When this option is set to Yes, the caption is always displayed, even on Windows machines where the client has been detected. No means the caption is never displayed, and Auto (the default) means the caption is always displayed to non-Windows clients and displayed to Windows clients only if a valid client is not detected.

You can also customize the message displayed by directly modifying the WebInterface.conf file. The specific value to modify is `OverrideClientInstallCaption`. The same custom message appears regardless of the client choices offered by the Web Interface.

A number of options within the Web Interface Console are configurable for client deployment. Most of the options are specific to the Launch Settings. These settings dictate what client is used to establish a connection with a MetaFrame server when a user clicks an application hyperlink. The information on this page includes

- Default client Here, you choose the default client that should be used on the client to access published content. The default option is Local Client, which refers to the standard local client corresponding to the client operating system. Other options include the embedded client (ActiveX or Netscape plug-in), the Client for Java, or Embedded Remote Desktop Connection software. If an alternate option is set as the default, note that it is valid only on platforms where the client is

supported. For example, the Remote Desktop Connection client is valid only on a Windows 32-bit OS with IE 5.5 or higher.

- **Web Client Settings** This box contains settings specific to the ActiveX clients. The default entry corresponds to the Win32 Web client. If you want to deploy the minimal Web client, you can substitute the given cabinet name (wficat.cab) with the name wficac.cab. If you want to deploy the Program Neighborhood or the Program Neighborhood Agent instead of the Web client, you need to manually modify the WebInterface.conf file and edit the Win32Client entry to point to the alternate installation file instead of the default.

When the Auto-deploy Web Client at Logon option is enabled, the appropriate client is downloaded and installed the first time the user logs on. These settings, along with the Remote Desktop Connection ActiveX settings, are enabled only if the Web client is selected as the default or selected as a possible alternate client. When the Web client has not been chosen as a possible client for installation, these options are grayed out.

- **Client for Java** These options allow you to choose the components included with the Java applet. Selecting only the packages required minimizes the size of the data downloaded. One option to note is the Use a Private Root Certificate setting. If you are implementing Secure Gateway for MetaFrame or SSL Relay (both discussed later in this chapter) and have used certificates that require a root certificate not already available on a client, you can use this option to deliver that certificate to the client. The certificate must be placed into the same folder as the Java client packages on the web server.

The Java client is ideal for environments where client installation files cannot be downloaded and installed.

- **Legacy Support** This setting dictates whether Unicode ICA files are generated by the Web Interface. Legacy clients do not understand Unicode ICA files.

## **Client Customization**

Client Customization allows you to define what options a client can override. The three options are window size, window color, and audio quality.

## **Server Settings**

Within the Server Settings, you manage the server farms, associated servers, and DMZ settings.

### **Manage Farms**

The Web Interface supports the creation of an application set based on information gathered from one or more server farms. All the available applications from each farm are retrieved and then displayed within the same interface. If applications in different farms have the same name, the user appears to have duplicate application entries. Applications should have unique names if they will be displayed within the Web Interface to reduce user confusion.

When you define the single MetaFrame server during the Web Interface installation, the default farm named "Farm1" is created, and that MetaFrame server is assigned to that farm. The farm name within the Web Interface is an arbitrary name used only to distinguish the different server lists. These names are *not* used to validate with the actual server farms. Although you can call these farms whatever you like, you should name them to match your farm names. Farms are easily added, deleted, and

arranged. Farms have a priority because the Web Interface contacts each farm to acquire applications. When all information is retrieved from one farm, the Web Interface then moves on to the next. If contact with a farm is slow, it affects the speed with which the applications are displayed.

## MetaFrame Servers

Each farm that is created is assigned its own list of servers. All the listed servers must be running the Citrix XML service. Each listed server is eligible to be used by the Web Interface to communicate with the appropriate server farm. When a new server is added, it is added to the bottom of the list. The ordering of the servers is relevant only when employing fault tolerance. By default, the server list is used for load balancing, which distributes connections among all the available servers. If connectivity to a server fails, it is removed from the list for the default of 60 minutes, a setting that can be edited. If the load balancing option is disabled, the Web Interface treats the list as a fault tolerance list. Requests are all processed by the highest priority server unless it fails, at which point it does not attempt to contact that server again for the default of 60 minutes. If all servers fail under either scenario, the Web Interface tries to reconnect every 10 seconds.

All three transport types are available for use. HTTP, the default choice, transmits information to and from the XML Service in plain text. HTTPS is valid only when IIS is also running on the MetaFrame server and the XML Service is configured to share the port with IIS. IIS must also be configured to support HTTPS (SSL or TLS). The final choice is SSL Relay, a listening service that can be configured on each MetaFrame server that you want to communicate securely with the Web Interface server.

## Network Address Translation

Network address translation (NAT) allows a local area network to use a set of IP addresses internally, while a separate set of addresses is used for external, usually Internet, traffic. Typically, a hardware- or software-based firewall exists between the two networks and is responsible for managing the translation of addresses from the external to the internal, and vice versa.

When a user accesses the Web Interface from an external address, you need to ensure that you have properly configured network address translation to ensure the Web Interface returns the appropriate external address for a Presentation Server. If NAT is not configured, the Web Interface returns the default or internal address to the external user. The user is unable to connect to the server because that address is invalid on the external network.

The default address translation settings are applied to all users connecting to the Web Interface, unless you have defined a specific address translation setting. When configuring specific address translation settings, you define the subnet address and mask and then configure the appropriate translation behavior. When the Web Interface matches these settings to a client's network, the specific settings are used instead of the default settings.

Both the default and specific settings share common options:

- Normal address This is the default behavior. The actual address of the Presentation Server is returned to the client.
- Alternate address The alternate address defined on the MetaFrame server is returned to the client. You configure alternate addresses on a MetaFrame server using the ALTADDR command-line utility.
- Translated address The Web Interface consults the server address translation map (at the bottom of the page) to determine the translated address to return to the client. When creating a

translation entry, you specify the internal address and port for the server. You then specify the equivalent translated (external) address with the associated translated port number. This translation map is a convenient alternative to defining alternate addresses directly on each server. The use of fully qualified domain names (FQDNs) or IP addresses for the server address is dictated by the [AddressResolutionType](#) value in the WebInterface.conf configuration file. If the value is set to DNS-port or DNS, the server address must be a FQDN. If the value is IPv4-port or IPv4, it must be an IP address. The default resolution type is IPv4-port.

- Secure Gateway Server When the Secure Gateway Server is employed, this option must be selected along with the corresponding translation type. Choosing a translation type for the Secure Gateway determines how Presentation Server addresses are translated when the Secure Gateway attempts to communicate with a server. A translation option is required only if NAT is employed on a firewall between the Secure Gateway and the MetaFrame server farm. If the translated address option was chosen, you do not populate the address translation map on this page. Instead, you need to populate similar settings on the Secure Gateway Support page. Secure Gateway configuration for the Web Interface is reviewed in the next section of this chapter.

## Alert

Remember that specific address translation settings are used as exceptions to the default settings. When both external and internal users are using the Web Interface, it is best to define the default configuration for external users and then define exceptions for users on the internal network.

## Secure Gateway Support

If you have deployed Secure Gateway in your environment, you need to configure the Web Interface to work with the Secure Gateway. Configuring the Secure Gateway is discussed in the "[Securing Server Access with the Secure Gateway](#)" section of this chapter.

With the Secure Gateway, clients no longer connect directly to the appropriate MetaFrame server in the farm. Instead, the client is directed to the Secure Gateway, through which the connection is created and managed. All traffic to and from the Presentation Server is directed through the Secure Gateway.

On the Secure Gateway Support page, you configure the following options:

- Secure Gateway Server You provide the fully qualified domain name for the Secure Gateway Server. This address is passed to the client so that it can connect to the Secure Gateway. This name must match the certificate installed on the Secure Gateway. The default port number is 443, but this can be changed if necessary.

You also provide the full URL to one or more servers running the Secure Ticket Authority (STA). The STA is responsible for generating tickets, which are passed to the client, then to the Secure Gateway, and eventually back to the STA in exchange for the information necessary to launch the application requested by the client. Tickets generated by the STA are different from those generated by the Web Interface without the Secure Gateway. Web Interface tickets replace the use of user credentials in the generated ICA file. STA tickets replace not only the user credentials, but also the specific MetaFrame server and published application information.

Multiple STAs can be provided, and by default, they load balance exactly the same way that the Web Interface load-balances access to the Citrix XML Service. If an STA server is unavailable, it is removed from the list for the same period of time defined on the MetaFrame Servers property page (60 minutes by default).

## Note

Citrix does not recommend the use of third-party load balancers for managing access to multiple STA servers.

- Internal firewall address translation map If you have configured the NAT property page to use the Secure Gateway with translated addresses, then it is here that you actually define the list of server and translated addresses. You are required to configure translated or alternate addresses with the Secure Gateway only if a firewall exists between the Secure Gateway and the Presentation Servers, and that firewall is employing NAT to access the Presentation Servers. NAT is not required when the only firewall that exists is the one between the Secure Gateway and the client device.

## Disabling Error Messages

On the Windows platform, you have the option to disable the custom Web Interface error messages and display more informative messages. You do this by editing the web.config file. The file is located in

*<WebRoot>/Citrix/MetaFrame/WIAdmin*

Change the default setting of

```
<customErrors mode="On" defaultRedirect="html/serverError.html" />
```

to

```
<customErrors mode="Off" defaultRedirect="html/serverError.html" />
```

The custom message simply says "An internal error occurred" if a server error is encountered.

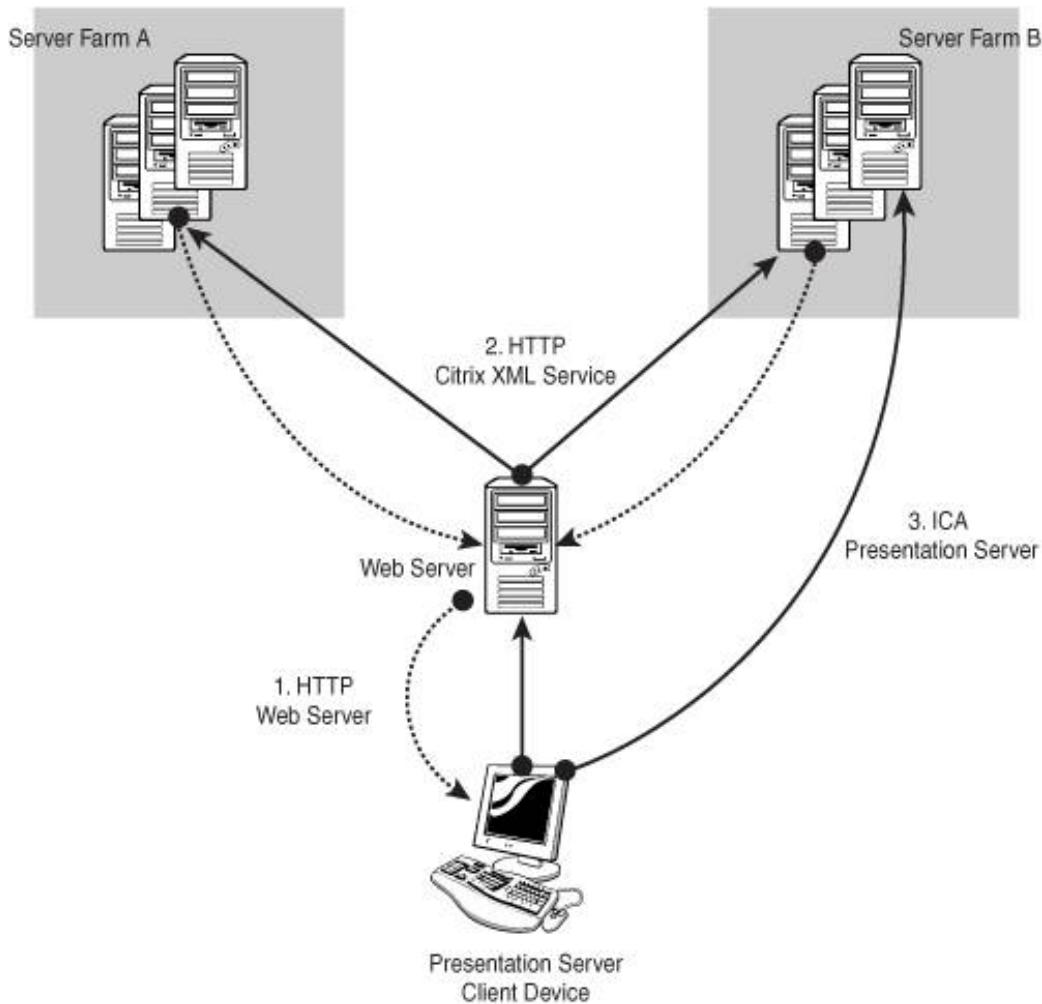
 PREV

NEXT 

## Securing the Web Interface

Figure 14.5 shows the familiar standard Web Interface configuration, but this time you can see the specific protocols the services use to communicate.

Figure 14.5. Three different communication channels should be secured in a Web Interface implementation.



There are three distinct communication scenarios:

- Client <-> Web Interface Data is transmitted between the client web browser and the Web Interface via standard HTML. User credentials, the generated ICA file for application connections, and a session cookie are all information that could potentially be intercepted or accessed unless communications are secured. Communications can be secured by requiring HTTPS (secure)

HTTP). You need only to configure the web server hosting the Web Interface to require secured (SSL/TLS) connectivity. This requires that an authentication ticket be stored on the web server. SSL/TLS provides server authentication, data encryption, and message integrity validation.

The use of single sign-on can also create a potential security issue. If the user were to receive an ICA file from an attacker, it could potentially transmit the user credentials to an unauthorized or counterfeit server. Disabling single sign-on eliminates this risk and provides a more secure environment.

- **Web Interface <-> Presentation Server** The Web Interface and Presentation Server transmit user credentials and application set information via the Citrix XML Service. All Citrix XML data is transmitted in plain text, except for passwords, which are scrambled using a trivial algorithm.

Transmissions between these two servers can be secured by employing Citrix SSL Relay. SSL Relay is installed with Presentation Server and allows you to employ SSL to secure the Citrix XML data transmission. To use SSL Relay, you must install a separate certificate on each Presentation Server. SSL Relay uses the Microsoft SSL implementation, known as SChannel and shares the same Registry-based certificate store as Windows and IIS. This allows certificates imported through IIS (when running on the Presentation Server) or the Microsoft Management Console (MMC) Certificate snap-in to be used by SSL Relay. SSL Relay is configured for the Web Interface either through the MetaFrame Server settings or by editing the WebInterface.conf file. Within the file, locate the line beginning with

`SessionField.NFuse_<Farm Name>`

where `<Farm Name>` is the farm that you are editing. If you have only the default farm, it is called "Farm1". Modify the Transport entry so it says Transport:SSL. Then modify the SSLRelayPort entry so it says SSLRelayPort:443 or an alternate port if SSL Relay is not listening on port 443. Remember to stop and start the web server for the changes to take effect.

If you are not able to employ SSL Relay, you can eliminate the risk of unsecured Citrix XML Service transmissions by running the Web Interface directly on a Presentation Server. The Web Interface can then be configured to communicate with the local XML Service, eliminating network traversal of the XML data.

- **Client <-> Presentation Server** The final communication channel to secure involves the client and the Presentation Server. This actually occurs when the user launches a published application. Three options exist for securing client session communications:
  - **ICA Encryption** Also known as SecureICA, ICA Encryption was discussed in [Chapter 9](#), "MetaFrame Security." ICA Encryption does not provide server authentication, making it susceptible to man-in-the-middle attacks. Citrix recommends that you employ an alternate method of securing session transmissions when clients are connecting over an unsecured network such as the Internet.
  - **SSL/TLS** Presentation Server supports users connecting to the server using SSL/TLS. This connection is managed through the SSL Relay service, just as secured connections to the Presentation Server from the Web Interface are managed. After SSL Relay has been configured, clients can connect to the server using SSL/TLS. SSL/TLS provides the server validation component not found in ICA Encryption.
  - **Secure Gateway** The Secure Gateway allows for the securing of client/server communications by creating an SSL/TLS-based gateway between the ICA clients and the Presentation Server farm. Instead of users connecting directly to a server via name or IP address, clients connect to the server farm through the Secure Gateway, which proxies all communications between the client and the server.

All communication channels must be secured to ensure a fully secure environment.

 PREV

NEXT 

# Program Neighborhood Agent Console

The Program Neighborhood Agent is a Win32 client that allows users to access applications via the Web Interface without requiring that they access the environment via a web browser. The PN Agent can display application shortcuts directly on the users' desktop.

The Program Neighborhood Agent Console is installed as part of the Web Interface, and the PN Agent Management Console is accessed using the following URL:

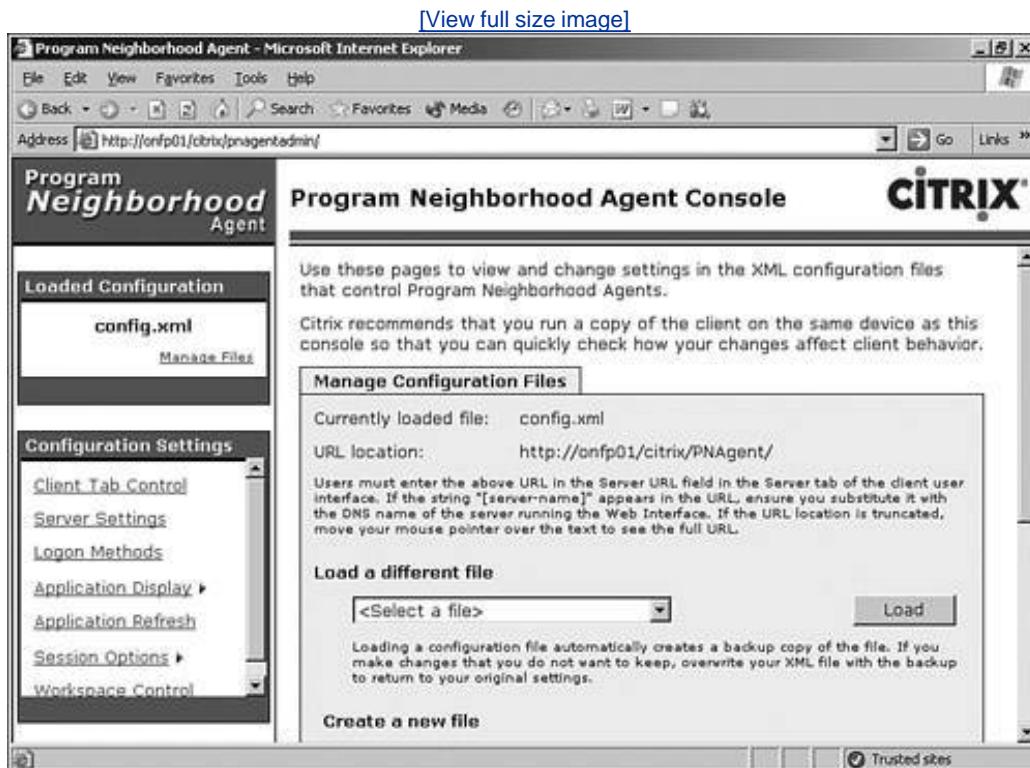
<Web Root>/Citrix/PNAgentAdmin

You can also directly modify the configuration files used by the PN Agent. The default configuration file is called Config.xml and is accessed using the following URL:

<Web Root>/Citrix/PNAgent

[Figure 14.6](#) shows the main PN Agent Console page.

Figure 14.6. The PN Agent Console provides extensive configuration options for the PN Agent client.



All configuration settings managed through the Console and processed by the client are stored in XML-formatted files on the Web Interface server. The default file, Config.xml, is the file loaded both by the

Console and by the client unless modified by an administrator. All configuration files for PN Agent are stored in the folder <*Web root*>\Citrix\PNAGent on the Web Interface server.

You are able to maintain as many different configuration files as you want (with any name) and need to assign the PN Agent client only to point to a specific configuration file to load those settings. All users who load the same configuration file receive the same settings. You cannot create user- or group-specific settings within a specific XML file.

## Manage Files

When the Console loads, it defaults to showing the Manage Configuration Files page, which shows the name of the current configuration file on the left side. As the name implies, this page enables you to manage the configuration or deletion of existing files as well as the creation of new configuration files.

Here's one thing that you should note: You cannot choose a file for deletion if it is currently being edited. This prevents you from deleting the default config.xml file unless another file has been created to replace it.

### Alert

When a configuration file is loaded, a backup copy of the file is created in the same folder with the same name but with the extension .bak. You can roll back from the most recent changes by deleting your XML file and replacing it with the BAK file.

## Client Tab Control

The Client Tab Control page manages what options are visible on the properties page of the PN Agent client and editable by the end user. When an option is hidden, it cannot be edited locally. These tabs can be hidden:

- Server You can change the source server for the XML configuration file and select the desired logon mode. Four logon modes exist: prompt user, single sign-on authentication, smartcard logon, and smartcard with single sign-on authentication.
- Application Display This tab controls where the application shortcuts are displayed.
- Application Refresh This tab is hidden from the user by default. It controls when the PN Agent refreshes the application list with the Web Interface. By default, it refreshes the list when the PN Agent starts and again every six hours.
- Session Options You can set the desired window size, color depth, and audio settings.
- Workspace Control The corresponding tab in the PN Agent is actually called Reconnect Options.

After you modify any of these settings, make sure that you click the Save button to update the configuration file.

## Server Settings

On the Server Settings page, you control configuration file behavior and whether communications between the client and server are secured. When this page opens, you see the full path to the current XML configuration file as an HTTP or HTTPS URL.

The refresh interval for the client configuration is set here. When an interval is defined, the client automatically contacts the Web Interface and retrieves the available configuration settings.

## Logon Methods

The Logon Methods page allows you to control the logon methods available to your users, as well as the default method the PN Agent will use. Even though a logon method may be selected on this page, unless it is also configured within the Web Interface, the option is not available to the user. When a logon option is enabled, it appears in the logon list under the Server tab for the PN Agent properties.

At the bottom of the page, you choose the default option that is automatically used when the PN Agent first loads. Enabling the check box Only Allow Users to Log On Using the Default Logon Method prevents the user from selecting any other available method. This option is automatically enabled if the Server tab has been configured to be hidden from the end user.

## Application Display

The Application Display configuration setting actually consists of four subcomponents that deal with various aspects of the application display:

- Shortcut Removal This setting controls when shortcuts created by PN Agent are removed. Normally, shortcuts created by PN Agent are removed only if that application is no longer published or if a user's access to that application has been eliminated. You can configure PN Agent to remove icons every time users log off or if the PN Agent client is closed.

Users are also able to create their own shortcuts that point to those created by PN Agent. By default, these shortcuts are removed only if the application itself is no longer available (same as the default behavior for PN Agent-created shortcuts). You can also select to have these user shortcuts removed every time users close or log off PN Agent. This discourages the use of personal shortcuts instead of the ones created by PN Agent.

- Start Menu This page controls how the shortcuts are displayed on the users' Start menus.

User customization can be granted or denied from this page, unless you have chosen to hide the Application Display tab. In this case, the option to customize these settings is automatically disabled.

And finally, custom Start menu settings can also be defined in the Presentation Server Console. On the Start Menu page, you can specify if these Presentation Server Console settings will override the PN Agent Console settings, be ignored for the PN Agent settings, or both utilized. If both are used, they can create duplicate shortcuts appearing in different Start menu folders.

- Desktop Similar to the Start menu settings, Desktop settings control how shortcuts appear on the client device's desktop. The Presentation Server Console settings can be used, merged, or ignored, just as they were for the Start menu settings.

- System Tray The final Application Display setting is the place where you configure whether application shortcuts appear under the Applications context menu for the PN Agent system tray icon. As with the other settings, if the Application Display tab is hidden, you cannot dictate whether users can modify this setting. It is automatically disabled.

## Application Refresh

From the Application Refresh page, you can centrally manage how the PN Agent client refreshes the list of available published resources. By default, an automatic refresh is configured to occur when the client first starts up and then every six hours.

## Session Options

The Session Options configuration consists of four subcomponents, all related to the configuration of the users' sessions and the options available to users:

- Window Size Using this page, you control whether users have the ability to select their own MetaFrame session window size.
- Color Depth Similar to the window size, if you want to allow users to select their preferred color depth, you must enable this option and choose the colors you want to have available.
- Audio Quality As with the others, this page allows you to decide whether to allow users to modify the audio settings for their PN Agent client.
- Template File The final session option component allows you to select the ICA template file used when a client accesses a published resource. Template files have the .ica extension and are created in the Citrix\PNAGent folder under the web root.

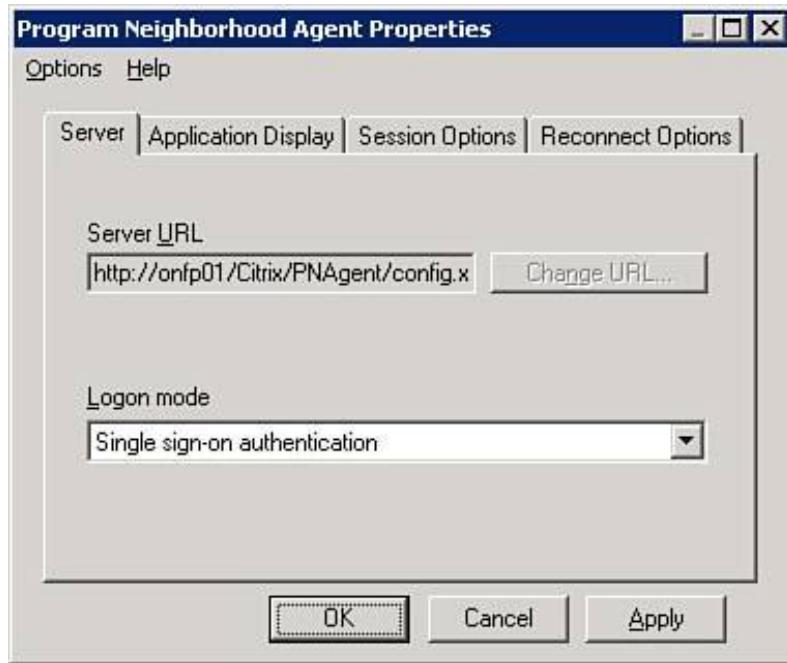
## Workspace Control

The final configuration setting deals with the automatic reconnect options of Workspace Control. From this page, you enable or disable automatic session reconnect and whether it applies to only disconnected sessions or to an active session on another client as well.

## Program Neighborhood Agent Client Configuration

[Figure 14.7](#) shows the properties for the PN Agent client. You display this dialog box by right-clicking on the "i" icon on the system tray and selecting Properties from the context menu.

Figure 14.7. The properties available for the PN Agent client are managed through the PN Agent Console.



As we just discussed, the visible tabs and options that can be managed on them are completely managed through the PN Agent Console.

### Note

A common strategy is to allow some client-side management of the properties during testing, but when everything is verified to be working properly, access to manage settings locally is disabled from within the PN Agent Console.

## Remote Desktop Web Connection Software

Another feature introduced with MPS 3.0 is support for the use of the Microsoft Remote Desktop (RDP) Web Connection software to access published content through the Web Interface. When configured, the Web Interface deploys the Web Connection ActiveX control just as it would the other ICA Web clients. The Remote Desktop Web Connection software is supported only on Windows 98 or later, running Internet Explorer 5.5 or later. The use of the RDP Web client does limit the features that are available when compared to an ICA client. Only two Presentation Server features are fully supported with the RDP client, and the third is only partially supported:

- Dynamic session reconfiguration. This feature allows dynamic updating of the display settings based on the capabilities of the client device.
- Zone preference and failover. If a MetaFrame policy has been created containing zone preference and failover settings, Citrix can use this information to direct the RDP Web client to the appropriate farm.
- Improved user logon support. Only the server-side information displayed during logon is

available. Client-side messages displayed by the ICA client are not available with the RDP Web client. When logging on to a MetaFrame server using the latest ICA client, you will notice that a number of messages appear while the connection is established. Messages such as "Preparing to connect...," "Connection in progress...," and "Connection established... Negotiating capabilities..." are all examples of the client-side messages not available when using the RDP Web client. Any messages that originate from the server are still displayed to the RDP client.

Citrix also provides only limited pass-through authentication support for the RDP Web client. Anonymous applications are accessible without requiring any explicit authentication, just as they would be with an ICA client.

Access for applications that require explicit user credentials are another story. The following list summarizes the access available to an RPD Web client based on the user authentication from the Web Interface:

- Guest access Any applications that require explicit user credentials are not available. Users do not receive the option to provide explicit credentials. Anonymous applications are available.
- Explicit user logon No further credentials are required to access explicitly published applications.
- Desktop pass-through authentication Users are still required to provide an ID and password to access explicit applications. Credentials are not cached for automatic authentication.
- SmartCard authentication SmartCard authentication is available with the RDP Web client only on a Windows 2003 Terminal Server. Explicitly published applications require users to provide their PIN. Credentials are not cached for automatic authentication.

 PREV

NEXT 

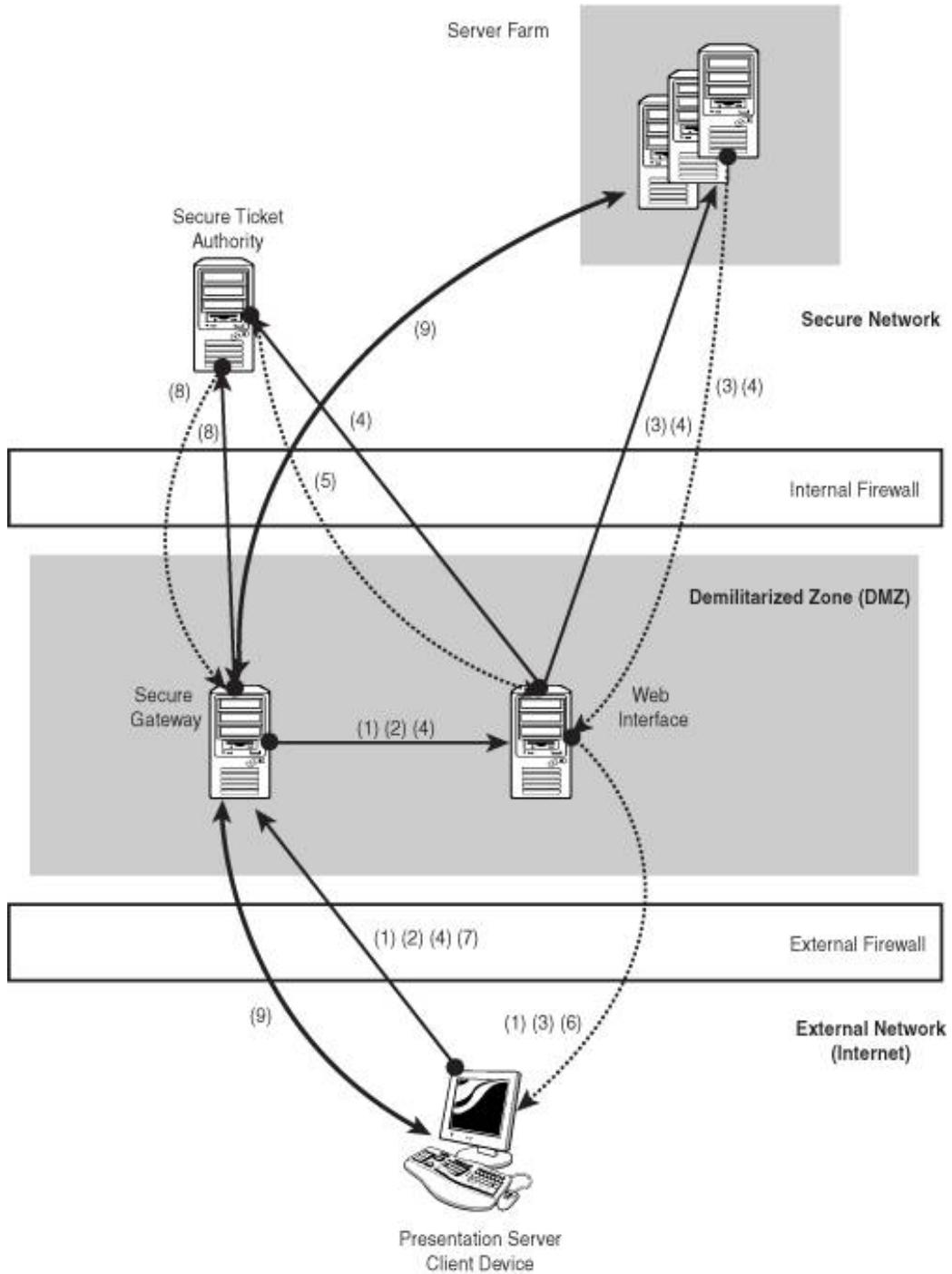
## Securing Server Access with the Secure Gateway

The Secure Gateway for Presentation Server is a component of Citrix's Access Suite infrastructure and is used to secure access to server farms and access centers. Communication with the servers is both authenticated and encrypted, ensuring maximum security for the environment.

The Secure Gateway also eases firewall traversal by eliminating the need for users to establish connections to specific MetaFrame servers via port 1494. With the Secure Gateway, all communications take place through port 443 (SSL/TLS port), a commonly used port open on most firewalls. [Figure 14.8](#) demonstrates a simple implementation of the Secure Gateway with the Web Interface, securing access to published resources in one or more server farms. The different communication paths are illustrated in this figure. Notice that the client device has only one point of entry into that environment. That is through the Secure Gateway.

Figure 14.8. Typical Web Interface implementation with Secure Gateway.

[View full size image]



## Alert

The Secure Gateway can be used to secure either a MetaFrame server farm or an environment running the MetaFrame Secure Access Manager. This exam focuses only on securing a MetaFrame Server farm using the Secure Gateway.

The behavior of a Web Interface environment when Secure Gateway has been deployed differs from running the Web Interface on its own. The following steps illustrate how a user would access an

application set and launch a published application when the Secure Gateway and Web Interface are deployed together to secure access to a server farm:

1. The user enters the address of the Secure Gateway in his or her web browser, not the address of the Web Interface. The Secure Gateway receives the request and then forwards it onto the Web Interface, which in turn presents the user with the logon page.
2. The user enters his or her credentials, and the information is routed through the Secure Gateway to the Web Interface.
3. The Web Interface contacts the Citrix XML Service on one of the servers in the farm and retrieves the application set for that user. The generated page is passed back through the Web Interface to the user.
4. After the user clicks an application link, the Web Interface retrieves a server IP address and port from the XML Service. It then passes this information to the Secure Ticket Authority (STA), requesting a session ticket.
5. The STA stores the server address information and issues an associated ticket to the Web Interface.
6. The Web Interface includes this ticket in the ICA file generated for the client. This file also contains the server name of the Secure Gateway. It does not contain the name of the MetaFrame Server associated with that ticket. In a Secure Gateway deployment, the specific server name is never revealed to the Presentation Server client.
7. The Presentation Server connection is initiated on the client using the generated ICA file. The client contacts the Secure Gateway and presents the session ticket.
8. The Secure Gateway then contacts the STA and presents the ticket for validation. If the ticket is valid, the corresponding server address is returned to the Secure Gateway. If it is invalid, an error message is returned to the client.
9. After receiving a valid server address, the Gateway establishes a connection with the Presentation Server and then brokers the flow of data between that server and the client.

The following components interact in this scenario:

- **Secure Gateway** This is the single point of user access to the server farm. Every client request for a MetaFrame server is brokered through the Secure Gateway. The Secure Gateway can run on the same server as the Web Interface, or it can be deployed on its own dedicated server. For maximum security, it should run on its own server. Secure communications require that the Secure Gateway has a server certificate installed.
- **Web Interface** The Web Interface is deployed in the DMZ along with the Secure Gateway. The Web Interface must be configured to function with the Secure Gateway as described earlier in this chapter.
- **Secure Ticket Authority (STA)** Residing in the secure network, the STA is responsible for creating and issuing *session tickets*. Session tickets are created when a user requests access to a published resource. A ticket is passed through the Web Interface to the client, which in turn passes the ticket to the Secure Gateway. The Secure Gateway returns the ticket to the STA in

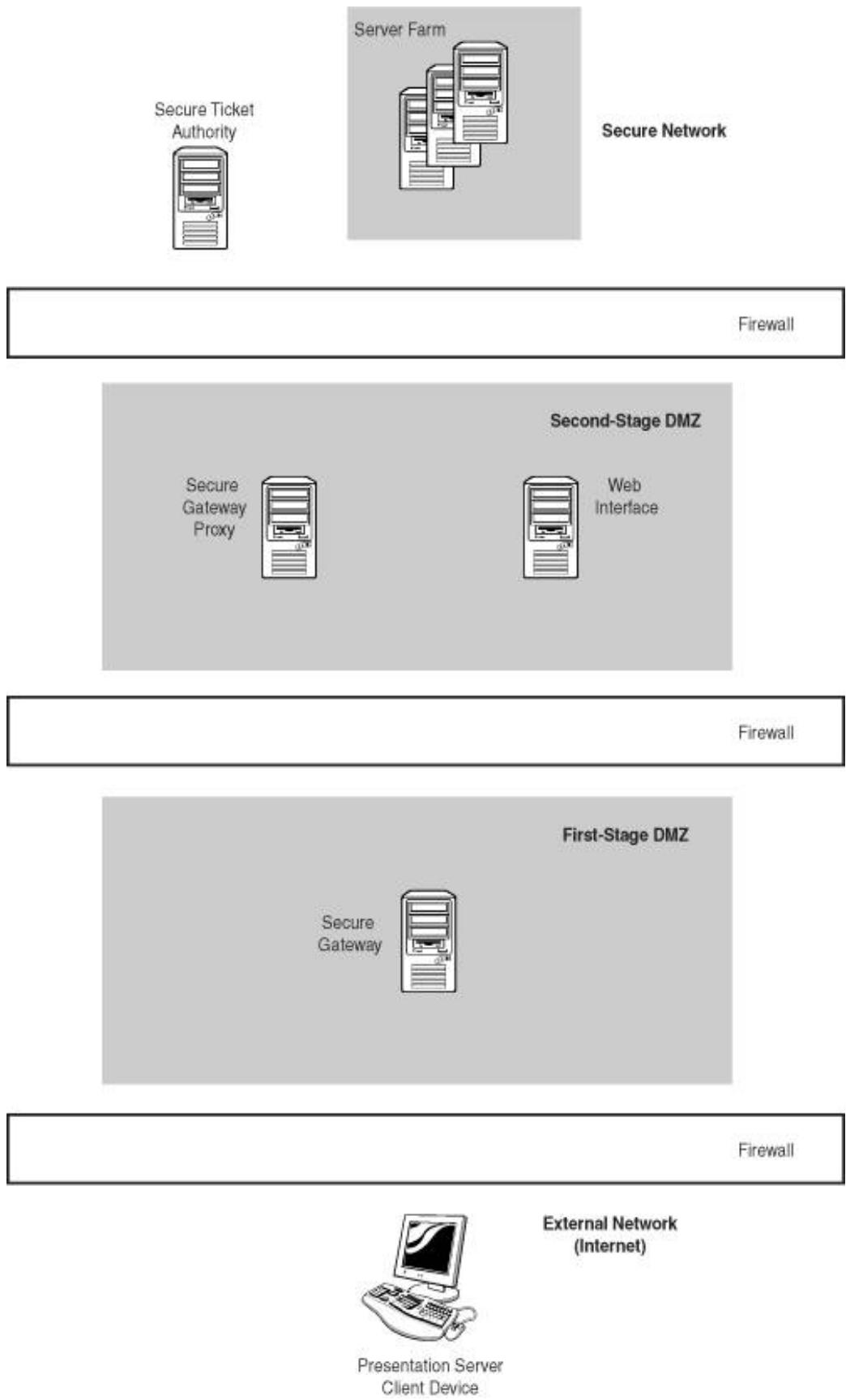
exchange for the appropriate server and application information, which is then used to establish the actual connection with the published application. Tickets themselves contain no server or user authentication information. To ensure secured communications, the STA must have a server certificate installed.

- **Citrix XML Service** The Web Interface contacts the server farm via the Citrix XML Service running on a MetaFrame server. Communications to the Citrix XML Service are secured using SSL Relay.

You can also deploy the Secure Gateway in a *double-hop DMZ*. [Figure 14.9](#) shows a simplified diagram illustrating how this would appear. The illustration is almost identical to that shown in [Figure 14.8](#), except that an additional firewall and the Secure Gateway Proxy machine have been added. The Secure Gateway Proxy is responsible for directing traffic to and from the Secure Gateway and the secured internal network. In this configuration, the Web Interface must be located in the second-stage DMZ. This allows it to communicate directly with the internal MetaFrame servers as required.

Figure 14.9. Secure Gateway deployed in a double-hop DMZ.

[\[View full size image\]](#)



## Installing the Secure Gateway

Before you begin the actual installation of the Secure Gateway components, note the following:

- The Secure Gateway or Secure Gateway Proxy servers require the minimum Windows 2000 Server (latest service pack) or Windows Server 2003 (latest service pack) configuration in addition to having at least 512MB RAM. The Secure Gateway components do *not* require IIS to be installed on the server to be able to function properly.
- The Secure Ticket Authority server should meet the minimum requirements for running Windows 2000 Server or Windows Server 2003. It should have a minimum of 256MB RAM. IIS must also be installed to be able to use the STA.
- In addition to the certificate requirements discussed earlier for securing a Web Interface environment, the Secure Gateway, Secure Gateway Proxy (if used), and the STA all require digital certificates to allow for the use of SSL.
- Citrix provides the Secure Gateway Pre-installation Checklist PDF with the other documents on the Presentation Server CD-ROM. It is highly recommended that this document be printed and completed prior to beginning the installation. It simply ensures that the necessary information is readily available prior to your starting the different component installations.

When you are installing the various components of the Secure Gateway, Citrix recommends the following sequence. It is important that you follow this sequence to ensure that everything is detected and validated properly. If a component cannot be validated, the Secure Gateway may fail to start.

1. Install components of the internal (secure) network first. This means that Presentation Server should be installed first, followed by the Secure Ticket Authority.

During the STA installation, the one piece of information required from the checklist is the location where the STA will be stored. It needs to go into the < /netPub>\Scripts folder, so if your website is located somewhere other than the default location, you may need to update this setting. You should also double-check to ensure that a server certificate is installed on the server running STA. This is required for authentication during communications.

2. The next set of components to install resides in the DMZ (or the second-stage DMZ in double-hop DMZ deployments). This would be the Web Interface and either the Secure Gateway or the Secure Gateway Proxy. The Web Interface is installed exactly as described earlier in this chapter. Make certain that the Web Interface has a root certificate installed that corresponds to the server certificate installed on the STA. This is required to ensure that the Web Interface can validate the STA's certificate when required.
3. The next component to install is the Secure Gateway Proxy, if you are implementing a double-hop DMZ, and finally the Secure Gateway component itself. The same installation package installs either product. You make the choice of proxy or service during the installation.

## Installing the Secure Ticket Authority

The STA is installed from the Components CD that accompanies the Presentation Server software. If you are performing the installation through the Autorun feature, you can find the STA installation under the Secure Gateway option. You can also initiate the installation by directly launching the MSI file located in the Secure Gateway\Windows\ folder. This file is called CSG\_STA.msi.

When the appropriate path to the Scripts folder has been provided, the STA components are copied to the server, and the Configuration Wizard starts immediately. Basic configuration options are allowed at

this time. Namely, you can specify STA ID, ticket timeout (the default is 100 seconds), and the maximum number of tickets to generate.

You need to restart the web service for the STA service to start.

## Installing the Secure Gateway

The Secure Gateway is also installed from the Components CD and is found in the same location as the Secure Ticket Authority. The Secure Gateway MSI file is called CSG\_GWY.msi.

### Note

Prior to beginning the Secure Gateway installation, you should have the required server certificate installed on the server.

When the installation begins, the first pair of choices is whether this is the Secure Gateway Service or the Secure Gateway Proxy, followed by the version of Presentation Server that is being secured. No Presentation Server 3.0 option is explicitly listed, so you must choose the MetaFrame XP Server Only option.

During the advanced installation of the Secure Gateway, which prompts for all parameter values, you are asked the following:

- **Server Certificate** All server certificates found on the server are listed, and you are asked to select the certificate that the Secure Gateway will use when requested for authentication.
- **Secure Protocol** You choose whether to support TSL only or SSL and TSL. Unless your organization specifically requires one or the other, selecting both protocols provides the widest available support for different clients.
- **Cipher Suite** This setting asks you to choose GOV, COM, or ALL. COM represents commercial-strength cipher suites, and GOV represents government-strength cipher suites. When ALL is selected, both suites are available, with preference given to the highest encryption strength.
- **Inbound Client Connections** This setting allows you to define the IP addresses and ports to monitor for client traffic. The default is all addresses and port 443.
- **Outbound Connections** This setting represents outbound connections from the Secure Gateway to servers within the DMZ or the secure network. There are three choices. No Outbound Traffic Restrictions allows the Secure Gateway to connect with any server in the DMZ or secure network. Use the Secure Gateway Proxy forces the Gateway to communicate through the Secure Gateway Proxy. You are required to provide the fully qualified domain name and port of the proxy. The Secured check box forces communications to be encrypted between the two servers. The final choice on the page is Use an Access Control List (ACL). The use of ACL limits the Secure Gateway to accessing only servers at the specified addresses. An ACL increases security by limiting the destination of the host.
- **STA Details** You must provide one or more STAs that the Secure Gateway can communicate with. For each STA you define, you specify the FQDN and whether to secure communications with HTTPS. After you have provided the required information and click OK, the Secure Gateway

attempts to establish a connection with the STA and verify the ID. If successful, the STA is added to the list along with the valid identifier. After all STAs have been added, you can continue.

- **Connection Parameters** This setting allows you to specify the connection timeout settings as well as whether limits should exist on the maximum number of connections. While the default is unlimited, Citrix highly recommends that you define a realistic limit on connections based on your environment. When a maximum number of connections has been defined, the connection resume value is automatically set to 90% of that. This setting dictates when the Secure Gateway should resume allowing connections after new connections have been temporarily disabled.
- **Logging Exclusions** You define any network devices that should be ignored when generating event logs. This setting is included to allow network load balancers or other monitoring software to "ping" the gateway without filling its logs with extraneous information.
- **Logging Parameters** Here, you choose the level of logging detail. All noninformational events are logged by default.
- **Web Interface Details** Here, you indicate where the Web Interface is running. If it is installed locally, this option is selected by default. If it is located on an alternate server, you need to provide the FQDN along with port address and whether to secure with HTTPS.

After you have provided the Web Interface information, the Secure Gateway validates that port 443 is available upon which to listen and then completes the installation. A reboot is required to complete the Secure Gateway installation.

## Configuring and Managing the Secure Gateway

After completing the installation, you're ready to configure and manage your Secure Gateway environment. The three applications that have been installed along with the Secure Gateway are used to perform these tasks. We conclude this chapter with a brief review of each tool and what common tasks can be performed with each.

### Secure Gateway Service Configuration

When executed, the Secure Gateway Service Configuration tool presents the same wizard that appeared when the Gateway was initially installed. You can modify any of the settings that you defined earlier, such as certificate to use, desired cipher suites, and so on.

### Secure Gateway Diagnostics

Secure Gateway Diagnostics is a handy utility for quickly viewing configuration settings and validating other components of the Secure Gateway. [Figure 14.10](#) shows a sample diagnostic report from a Secure Gateway running on the same server as the Web Interface. Issues with access to the Web Interface or the STAs are easily identified through this tool.

Figure 14.10. Secure Gateway Diagnostics quickly summarizes the state of the Secure Gateway environment.

[\[View full size image\]](#)



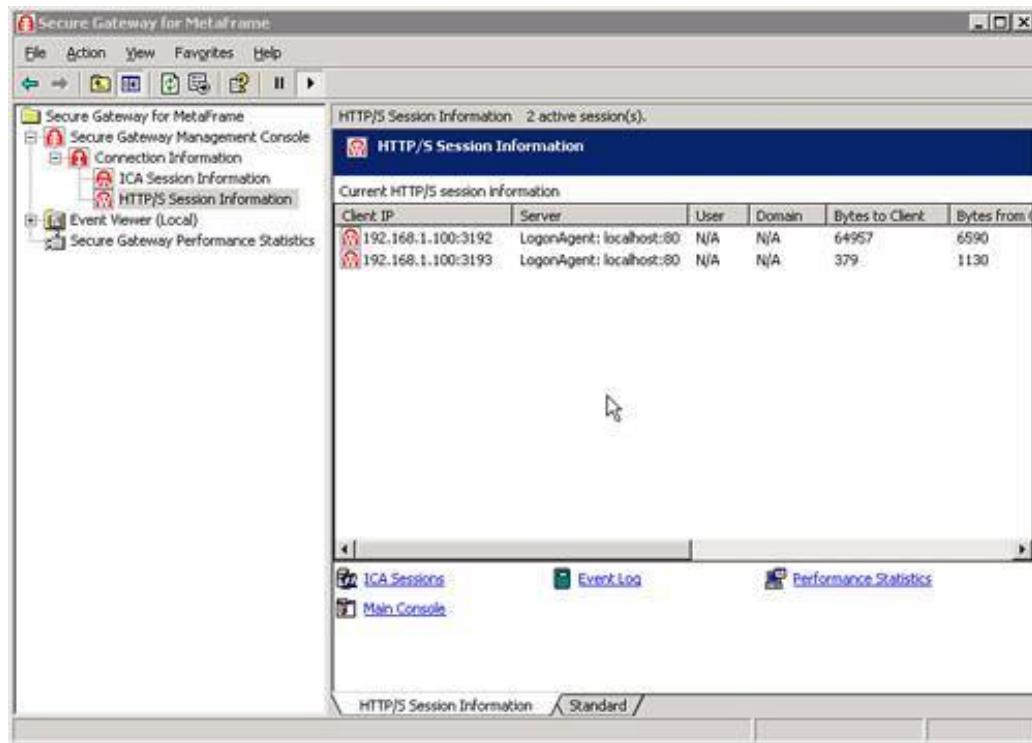
## Secure Gateway Management Console

The Secure Gateway Management Console is an MMC snap-in that provides some basic management capabilities for the Gateway. Within this console, you can perform the following tasks:

- Launch Configuration and Diagnostics tools You can access both tools directly from within the Management Console by selecting the Secure Gateway Management Console icon and choosing the desired utility from the All Tasks menu.
- Manage the Secure Gateway Service From the same All Tasks menu, you are able to start, stop, pause, resume, or restart the Secure Gateway Service.
- View connection information You can view both current ICA and HTTPS session information. [Figure 14.11](#) shows an example of the current HTTPS session information displayed.

Figure 14.11. Current ICA and HTTPS session information is available in the Management Console.

[\[View full size image\]](#)



- Use Windows Event view You can quickly view the Windows Event logs from within the Console. Event log information is *not* filtered specifically for Secure Gateway events, although the Secure Gateway event log node is accessible.
- Check Secure Gateway performance statistics There is also direct access to the Windows Performance tool, although the tool is not prepopulated with Secure Gateway-specific performance counters. The desired counters must be added manually. From the available Secure Gateway performance object, you can add specific counters and quickly assess the load on the gateway.

After it is installed and configured properly, the Secure Gateway provides an effective method of properly securing client access to a Presentation Server farm.

**PREV**

**NEXT**

## Exam Prep Questions

1. Which of the following is not a valid Web Interface component?

A. Presentation Server Farm

B. ICA Client for Linux

C. Web Interface Server

D. SSL Server

A1: Answer D is not a valid Web Interface component. Although the Web Interface communicates via the SSL Relay Service, it is not specifically an SSL Server.

Answer A is a valid component. At least one server farm is required.

Answer B is also valid. A Presentation Server Client is necessary to access the Presentation Server.

Answer C is valid as well. The Web Interface itself is, of course, a necessary component.

2. The entry of user credentials is secured in the Web Interface by using \_\_\_\_\_.

- A. HTTPS
- 
- B. SSL Relay
- 
- C. SecureICA
- 
- D. Program Neighborhood Agent

A2: Answer A is correct. If the Web Interface server is configured to require SSL encryption, users must access the server via HTTPS, ensuring that user credential information is securely transmitted to the web server.

Answer B is incorrect. SSL Relay secures communications between the Web Interface and the Citrix XML Service. It does not secure the entry of user credentials.

Answer C is incorrect. SecureICA is the Citrix mechanism for securing ICA data traffic. The ICA protocol is not used when entering credentials on the web page.

Answer D is incorrect. Although the Program Neighborhood Agent is an alternative method of accessing Web Interface data, it alone does not secure the entry of user credentials.

3. The template.ica file contains \_\_\_\_\_, which are updated with information specific to the application by the Web Interface.

- 
- A. placeholders
- 
- B. hard-coded references
- 
- C. substitution tags
- 
- D. XML tags

A3: Answer C is correct. The template.ica file contains substitution tags, which are updated by the Web Interface when users launch an application.

Answers A, B, and D are incorrect. None of these are valid answers.

4. User credentials are passed to the server when an application is launched as \_\_\_\_\_.

A. a substitution tag

B. a session ticket

C. plain text

D. an SSL certificate

A4: Answer B is correct. A session ticket is generated and placed within the generated ICA file instead of the user credentials. The ticket has an expiry date and can be used only once to log on to a Presentation Server.

Answer A is incorrect. The session ticket field is a substitution tag in the template.ica file, but not in the generated file that is sent to the client.

Answer C is incorrect. User credentials are never placed into the generated ICA file as plain text.

Answer D is incorrect. An SSL certificate is not used to store user credentials in the ICA file.

5. SSL/TLS can be used to secure communications between what Web Interface component?

A. Web Interface and the SSL Relay Service

B. Web Interface and the Presentation Server Client

C. Presentation Server Client and the Presentation Server

D. All of the above

A5: Answer D is correct. All the components can employ SSL/TLS to secure communications with their respective components.

6. On a Windows IIS server with the Web Interface installed, the Web Interface configuration file is called \_\_\_\_\_.

A. WebInterface.cfg

B. WebConfig.inf

C. WebConfig.conf

D. WebInterface.conf

A6: Answer D is correct. The configuration file on both Windows and UNIX is called WebInterface.conf, although it is located in a different subfolder on each platform.

Answers A, B, and C are all invalid names.

7. Your friend has a UNIX server configured with the Web Interface but doesn't know how to access the Web Interface Console. Where should he go to find it?



A. `http://<servername>/Citrix/MetaFrame/WIAdmin`



B. `http://<servername>/Citrix/WebInterface/Admin`



C. `http://<servername>/Citrix/MetaFrame/WebAdmin`



D. None of the above

A7: Answer D is correct. The Web Interface Console is not available when running on a UNIX web server. The console is available only on a Microsoft IIS server.

Answer A is incorrect. Although this is the valid location on an IIS server, it is incorrect on a UNIX server.

Answers B and C are both incorrect because they point to fictitious locations.

8. When servers are listed in the MetaFrame Settings page for the Web Interface, load balancing is enabled by default. If a server fails, the default behavior of the Web Interface is



A. retry once every 10 seconds until the server becomes available or 60 attempts have been made.



B. drop the server from the list but try once every 10 seconds until the server becomes available.



C. drop the server from the list for 60 minutes before trying again.



D. drop the server from the list for 60 minutes or until the Presentation Server is restarted.

A8: Answer C is correct. If a server is determined not to be available, it is dropped from the list for 60 minutes before the Web Interface will again try to contact it.

Answers A, B, and D are all incorrect. The Web Interface will attempt to reconnect once every 10 seconds only when all listed MetaFrame Servers have failed to respond to a Web Interface request.

9. You want to create a new Program Neighborhood Agent configuration file for your accounting department. What tool would you use to make this change?

A. Management Console for MetaFrame Presentation Server

B. Web Interface Console

C. Program Neighborhood Agent Console

D. Program Neighborhood Agent

A9: Answer C is correct. Using the PN Agent Console, you can copy an existing configuration file and then modify the properties. Unless the accounting department was already configured to use a unique configuration file, it would have to be manually updated to point to this new file.

Answer A is incorrect because the Management Console is used to perform server and server farm configuration. Although the Management Console can be used to configure how shortcuts appear on the user's desktop and Start menu, it does not provide any configuration file management capabilities.

Answer B is incorrect. Even though the PN Agent depends on the existence of the Web Interface, the Web Interface Console does not have PN Agent management features integrated in.

Answer D is incorrect. Although the PN Agent properties can be modified to point the client to an alternative configuration file, you cannot use the client to create or modify the file.

10. Which of the following tasks *cannot* be performed using the Program Neighborhood Agent Console? (Select all that apply.)



A. Hide tabs in the PN Agent property dialog box.



B. Manage the list of supported logon methods.



C. Push out the PN Agent client to selected users.



D. Configure the list of available server farms.

A10: Answer C is correct. The PN Agent Console does not provide support for client deployment.

Answer D is also correct. The list of supported server farms is managed through the Web Interface Console, not the PN Agent Console.

Answer A is incorrect. The PN Agent Console does allow you to hide the property tabs for the PN Agent.

Answer B is also incorrect. The PN Agent Console does allow the selection of the desired logon methods to support.

11. What is the name of the default configuration file loaded by the Program Neighborhood Agent?



A. config.pna



B. pnagent.xml



C. config.xml



D. config.ica

A11: Answer C is correct. The default configuration file used by PN Agent is config.xml. Answers A and B do not represent valid filenames. Answer D has the .ica extension, which is the default extension used for ICA template files. An ICA template file is used to establish the connection with the published resource.

12. What Program Neighborhood Agent Console setting is modified to hide the Property tabs in the Program Neighborhood Agent client?

A. Property Tab Control

B. Client Property Control

C. Session Options

D. Client Tab Control

A12: Answer D is correct. The Client Tab Control configuration setting is the place where the various property tabs for the PN Agent can be shown or hidden.

Answers A and B are incorrect. They do not represent valid configuration setting names.

Answer C is incorrect because the Session Options configuration setting is the place where settings such as window size, color depth, and audio quality are configured.

13. The Secure Gateway secures a MetaFrame Server farm by \_\_\_\_\_. (Choose all that apply.)

- A. forcing all communications with the server farm to go through the Secure Gateway, reducing the number of open ports on the external firewall
- B. providing authentication and encryption support for MetaFrame connections
- C. doubling the encryption strength of the ICA protocol to 2,048 bits
- D. allowing only users who are running the special Secure Gateway client to properly log on to the environment

A13: Answers A and B are correct. Both of these statements are true. By forcing all connections through one carefully guarded access point, you greatly reduce the attack surface available to would-be intruders. The combined authentication and encryption support provided to MetaFrame connections through SSL ensures that not only is the information secure against eavesdropping, but it is also protected from modification by a third-party attempting to perform a man-in-the-middle attack.

Answer C is incorrect. The Secure Gateway does not directly modify the ICA security in any way.

Answer D is incorrect. There is no such thing as the Secure Gateway client. One of the benefits of the Secure Gateway is that it employs standards for Web security that require no special client software like a VPN connection might.

14. In a Secure Gateway deployment, the Secure Ticket Authority is responsible for \_\_\_\_\_. (Choose all that apply.)

- A. issuing tickets to the Web Interface in response to server access requests
- B. reconciling tickets received from the Secure Gateway and providing the associated server information
- C. verifying that a session ticket has not expired
- D. providing user credentials to the Presentation Server for processing

A14: Answers A, B, and C are correct. When the Web Interface receives a request to access a published application, the server that will execute the program is passed to the STA by the web server. A corresponding session ticket is received and is then used to verify that the user should be logging on to that server. If the ticket is invalid or has expired, the STA denies the application launch request.

Answer D is incorrect. The STA is not responsible for passing user authentication information to a MetaFrame server for processing.

 PREV

NEXT 

# 15. Managing and Monitoring Using Resource Manager

Terms you'll need to understand:

- Cost Centers
- Fee Profiles
- Metrics
- Summary Data
- Summary Database
- Farm Metric Server
- Database Connection Server

Concepts you'll need to master:

- Identifying and describing the components of Resource Manager
- Properly upgrading an existing Resource Manager environment
- Understanding the role and requirements of the Summary Database
- Assigning and monitoring metrics on servers and applications
- Monitoring metric values in real time
- Running both current and historical data reports
- Configuring and generating billing reports

# Resource Manager Overview

As with any enterprise-level system, resource monitoring is an integral part of maintaining optimal performance and determining expansion needs and growth. Resource monitoring is one of your most useful tools when you need to justify hardware upgrades and expansion.

Resource Manager is a Citrix Presentation Server Enterprise Edition component that is designed to monitor resources such as CPU and memory on a Presentation Server. It allows you to generate detailed reports that provide you with information about how a server is performing during certain times of the day. It is also a very useful tool because of its historical data retention option, which allows you to run a report to determine the server's resource usage at any give date and time.

Resource Manager uses *metrics* to determine a resource's current load. Metrics are evaluation agents or performance-measuring units based on the operating system's performance counters. Metrics can be attached to a resource to measure its current load and report it back to Resource Manager. These metrics can be configured to alert the Citrix administrator when certain thresholds are reached so that steps can be taken to address any concerns.

## Alert

Expect to see more questions on Resource Manager in the 223 exam compared to the 256 exam. You should have a basic understanding of the technology for both, but Citrix is currently working to develop a more thorough (and separate) exam to cover Resource Manager and its use in a production Presentation Server environment.

# Resource Manager Components

Resource Manager relies on the following three components to gather, manage, and maintain data:

- **Farm Metric Server** The farm metric server is responsible for collecting and interpreting farm-wide metric information from the zone data collector and reporting alerts or alarms if metric thresholds are exceeded. By default, this is the first server where you install Resource Manager. The second server on which you install Resource Manager is designated as the backup Farm Metric Server.

Because Farm Metric Servers retrieve updates from the zone data collector every 15 seconds, Citrix highly recommends that the zone data collector also be designated as the Farm Metric Server.

- **Database Connection Server** You select and configure this server to receive summary information once a day from each of the Presentation Servers in the farm. This information is then written by the Database Connection Server into the Summary Database. It is recommended that the Database Connection Server be configured on an MPS server with relatively low load to ensure optimal performance.

The storage of historical metric information is an optional component of Resource Manager. If historical data is not going to be maintained, the Database Connection Server is not required.

- **Summary Database** When historical data is retained for Resource Manager, it is stored in the Summary Database. Unlike the Data Store for the Citrix Presentation Server farm, the Summary Database for Resource Manager must be deployed on either a Microsoft SQL Server or an Oracle database.

## Alert

You are expected to be able to identify the components of Resource Manager and understand their function.

## Resource Manager Installation

As with other components of the Enterprise Edition of Presentation Server, unless a valid Enterprise Edition license exists on the Access Suite License Server, the component can be installed but will not function. To install Resource Manager, you follow the normal procedures for installing MPS as detailed in [Chapter 5](#), "Installing MetaFrame Presentation Server 3.0." Check the option to install Resource Manager from the Components Selection screen, as shown in [Figure 15.1](#).

Figure 15.1. Select Resource Manager from the Components Selection screen of the Presentation Server installation.



## Resource Manager Upgrade

When upgrading an existing version of Presentation Server with Resource Manager installed, you need to upgrade your servers in the following order:

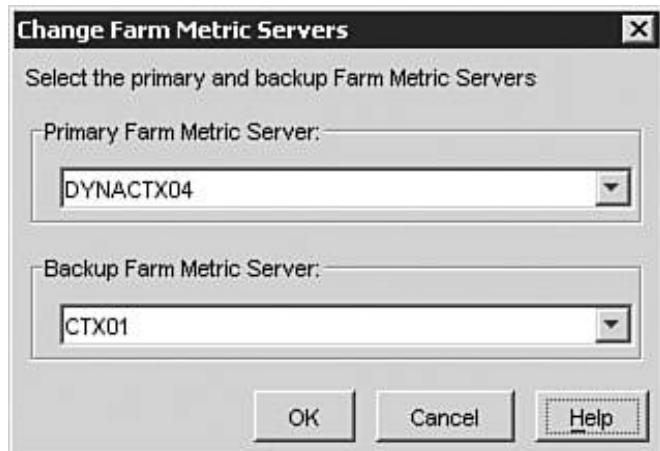
- Database Connection Server (if implemented)
- Primary Farm Metric server
- Backup Farm Metric server
- All other servers in the farm

Upgrading these servers out of order may introduce problems because a new version of Presentation Server may send metric information to a metric server or the Database Connection server that an older version of Resource Manager would not understand, resulting in unpredictable behavior and possible Resource Manager issues.

## Selecting the Farm Metric Server

As mentioned before, the Farm Metric server is, by default, the first server where Resource Manager is installed. In the event that you need to change the Primary or Backup Metric server, simply click the Resource Manager node in the Management Console and then select the Farm Metric Server tab in the far-right side. Click on the Change Farm Metric Servers button. In the Change Farm Metric Servers window, shown in [Figure 15.2](#), you can select any MPS server to be the Primary Metric server and a Backup Metric server.

Figure 15.2. Change Farm Metric Servers window.



## Implementing a Summary Database

To be able to produce historical or billing reports, you require a Summary Database within which to retain this historical data. In addition to the Summary Database, you also require the Database Connection server. This is the only server that communicates directly with the Summary Database. No other servers in the farm, including the Farm Metric servers, talk directly to the Summary Database.

The Summary Database must be installed on a database management system (DBMS) running either

- Microsoft SQL Server 7 or 2000

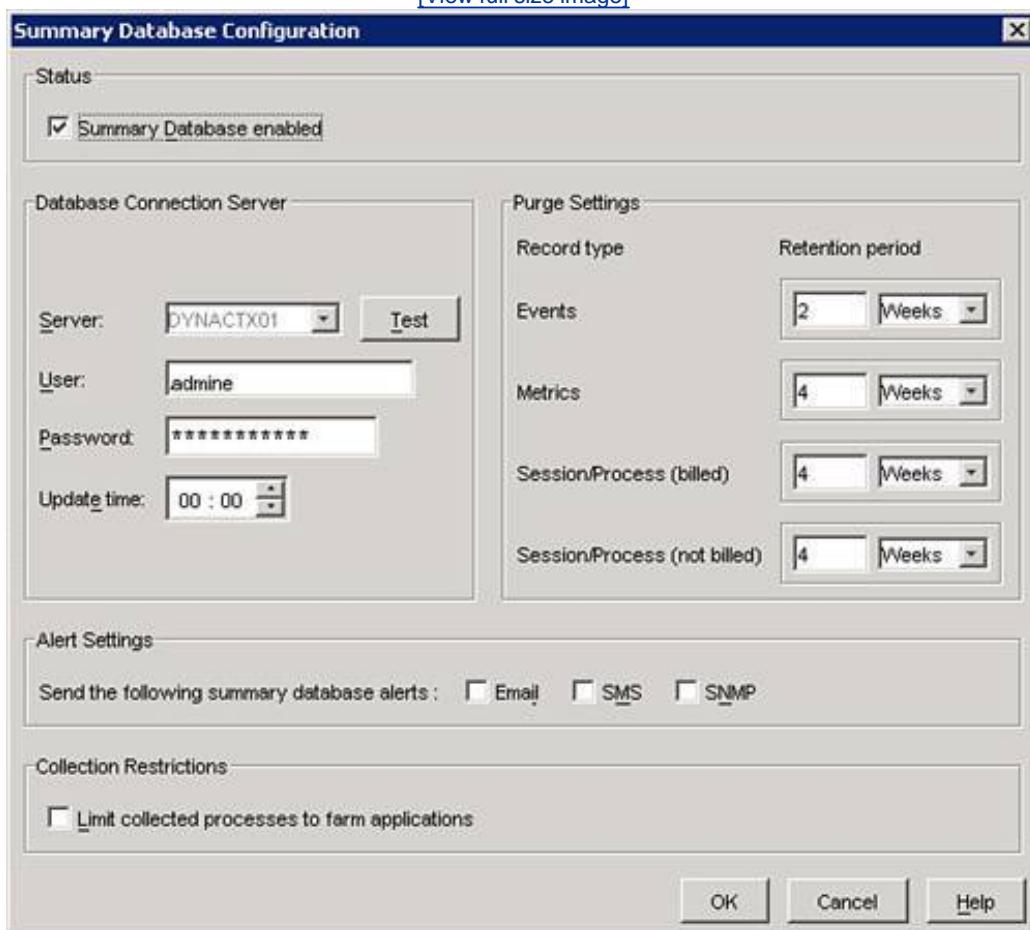
- Oracle Database version 8i or 9i

After choosing the DBMS, you configure the Summary Database as follows:

1. Create a database in the DBMS to store the summary data.
2. Create a system data source name (DSN) on the designated Database Connection Server.
3. Within the Management Console for Presentation Server, click on the Resource Manager node, select the Summary Database tab, and then click the Configure button. You may need to resize the Management Console window to be able to see this button, which is located along the bottom of the tab. A screen similar to the one shown in [Figure 15.3](#) appears, where you configure the Summary Database.

Figure 15.3. Summary Database Configuration window.

[View full size image]



◀ PREV

NEXT ▶

## Using Resource Manager

After you have installed and configured Resource Manager, you can begin using it to monitor your resources farmwide. You can monitor resources in many different ways in the Management Console, depending on the type of information you are looking to gather. For example, you can select the Applications node in the left pane of the Management Console and then select the Resource Manager tab in the right pane to display a summary of the application metrics that are being monitored (see [Figure 15.4](#)). You can further limit your view by expanding the Applications node, selecting a particular application, and then clicking the Resource Manager tab in the right pane again to display the Resource Manager information for just this application.

Figure 15.4. Metrics information is accessed through the Resource Manager tab.

[View full size image]

The screenshot shows the Management Console interface for MetaFrame Presentation Server 4.0. The title bar reads "Management Console for MetaFrame Presentation Server 4.0". The menu bar includes "Actions", "View", "Help", and standard toolbar icons. The left pane displays a tree view under "GPP" with nodes like "Applications", "MetaFrame Administrators", "Installation Manager", "Isolation Environments", "Load Evaluators", "Policies", "Printer Management", "Resource Manager", and "Servers". The "Applications" node is currently selected. The right pane has three tabs: "Contents", "Content Redirection", and "Resource Manager". The "Resource Manager" tab is active, showing a table with columns: Status, Applications, Error, Warning, Not config, Idle, Unknown, and Metric C. The table lists various applications with their status and metric values. For example, "IT Tools" is listed as "Not configured" with 0 errors, 0 warnings, 0 not configured, 0 idle, 0 unknown, and 0 metric C. Other applications listed include Maryland Apps, Market Research, Makers Apps, Dyna Apps, ProSystem Fx, Hyperion, Treasury Manager, Notes, Heat, JDE Apps, MicroMain, Human Capital Desktop, Angus, LeaseMaker Desktop, CRM Desktop, Citrix MetaFrame Confe..., Citrix Conference Room, and TeleCommuter Desktop.

Status	Applications	Error	Warning	Not config	Idle	Unknown	Metric C
Not configured	IT Tools	0	0	0	0	0	0
Not configured	Maryland Apps	0	0	0	0	0	0
Not configured	Market Research	0	0	0	0	0	0
Not configured	Makers Apps	0	0	0	0	0	0
Not configured	Dyna Apps	0	0	0	0	0	0
Not configured	ProSystem Fx	0	0	0	0	0	0
Not configured	Hyperion	0	0	0	0	0	0
Not configured	Treasury Manager	0	0	0	0	0	0
Not configured	Notes	0	0	0	0	0	0
Not configured	Heat	0	0	0	0	0	0
Not configured	JDE Apps	0	0	0	0	0	0
Not configured	MicroMain	0	0	0	0	0	0
Not configured	Human Capital Desktop	0	0	0	0	0	0
Not configured	Angus	0	0	0	0	0	0
Not configured	LeaseMaker Desktop	0	0	0	0	0	0
Not configured	CRM Desktop	0	0	0	0	0	0
Not configured	Citrix MetaFrame Confe...	0	0	0	0	0	0
Not configured	Citrix Conference Room	0	0	0	0	0	0
Not configured	TeleCommuter Desktop	0	0	0	0	0	0

Another way of looking at Resource Manager data is by server. You can select the Servers node in the Management Console and then choose the Resource Manager tab in the right pane to get a summary of all the servers and their status. Alternatively, you can further limit your view by expanding the Servers node and selecting a particular server to query for data again by selecting the Resource Manager node in the right pane.

The third method by which you can monitor server and application loads is by using the Resource

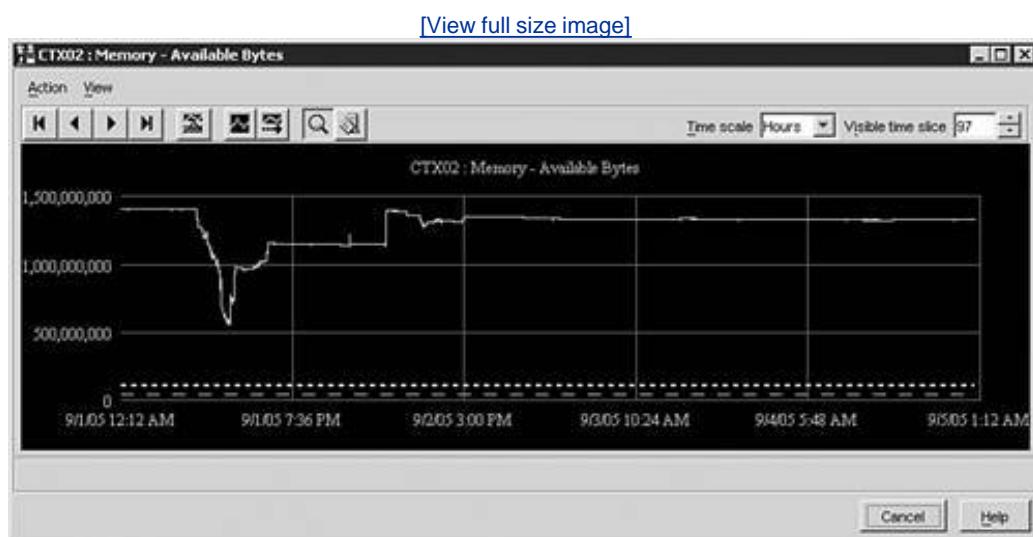
Manager node in the left pane of the Management Console. Selecting the Resource Manager node gives you access to the following tabs in the right pane:

- Watcher displays a list of all MPS servers in the farm that are reporting an alert.
- Reports allows you to run reports such as Current Process, Current User Activity, Server Snapshot (which shows the status), Process Summary, User Summary, and Server Summary. Until a Summary Database is available, the associated reports are grayed out.
- Billing allows you to generate billing reports based on resource usage. A Summary Database must exist before billing reports can be generated.
- Summary Database allows you to configure the Summary Database.
- SMS allows you to configure Short Message Service (SMS) as a method by which alerts are delivered to your mobile device.
- SNMP allows you to configure SNMP traps as a method by which alerts are delivered to you.
- Email allows you to configure email as a method by which alerts are delivered to you.
- Farm Metric Server allows you to assign the Primary and Backup Farm Metric servers and also see their status.

## Real-time Application and Server Monitoring

Often you will be interested in knowing the current activity on a server. This is where real-time application and server monitoring comes in handy. This feature allows you to see the status of an application or server *now*. To get access to view real-time monitoring, expand the Servers node in the Management Console and select a server. In the right pane, choose the Resource Manager tab and double-click the object you want to view in real-time. You are presented with a graph similar to the one shown in [Figure 15.5](#).

Figure 15.5. Real-time monitoring.



## Maintaining Historical Data

Every MPS server in the farm maintains Resource Monitoring data on itself, known as *summary data*. This data is stored locally as files in the following temporary location: \Program Files\Citrix\Citrix Resource Manager\SummaryFiles. Every hour the server updates and adds to these files. The Database Connection server then collects the summary data on a daily basis from every MPS server and writes it to the Summary Database. Once written to the Summary Database, the files are overwritten with new information.

Maintaining historical data is important and necessary, but you should also be selective of what type of data you are storing in the Summary Database. You need to know how long it will be stored and what the purpose of the storage is. Failing to do so results in a database that is incredibly large and that will keep getting larger. For example, if you are using the billing features and you want to bill users for the amount of memory they use, it is a good idea to maintain memory logs. If you need to justify hardware upgrades to management, you can choose to monitor certain processes that can be beneficial, such as the CPU utilization.

In addition to determining the type of data to store, you need to decide how long you need to store this information. This decision also impacts the size of the dataset.

## Reporting

The main reason to use Resource Manager is reporting; it is the mechanism by which you can receive reports that summarize what is going on or what went on a server at a specific time. It is also a great tool for analyzing, forecasting, and comparing server and application loads. Two types of reports can be run using Resource Manager:

- Current All current reports use the information that Resource Manager stores on the local MPS server to generate reports. This is where you get real-time snapshots, and the server records the information every 15 seconds.
- Summary All summary reports use information stored in the Summary Database to generate its reports. Summary reports, even though less detailed than current reports, can be generated against any time period for which data was recorded in the Summary Database; thus, they provide a source for historical data.

Both the Current and Summary reports can be generated on a per-server basis or against multiple servers.

You can generate reports from the Management Console by selecting the Resource Manager node in the left pane and then selecting the Reports tab in the right control pane. The Reports Center in the Access Suite Console gives you access to a bigger variety of reports that can be generated.

## Alert

Be able to identify the supported reporting types and the associated server farm requirements needed to access a particular reporting type. For example, Summary reporting is only available if a Summary Database exists and contains historical data.

## Usage Billing

In many organizations, users are billed or charged for the resources they use. This billing is useful in cases in which your infrastructure is limited and you want to make sure users don't waste resources unnecessarily. It can also be used as a means for expanding the infrastructure by having other departments in the organization pay for the expansion as they use the system more and more. It is a way of putting a dollar amount on the resource usage.

Resource Manager allows you to do this type of billing by using information stored in the Summary Database against a *fee profile* that you set up. A fee profile is basically a structure whereby you say that the price of using memory or CPU time is X. You can also specify the currency that you want to use.

You can also create a *cost center*. This allows you to group your users and apply a fee profile to them. Usually, cost centers are created for every department in your organization, which makes user management easier. Reports can then be generated against cost centers and billed to the respective departments.

To configure fee profiles or cost centers, or to run billing reports, launch the Management Console and select Resource Manager in the left pane. Then choose the Billing tab in the right pane, as shown in [Figure 15.6](#).

Figure 15.6. Billing usage.

[View full size image]



**◀ PREV**

**NEXT ▶**

## Exam Prep Questions

1. Which license level of MetaFrame Presentation Server do you need to run Resource Manager?

- 
- A. Advanced
- 
- B. Standard
- 
- C. Enterprise
- 
- D. Custom

A1: Answer C is correct. To activate and use Resource Manager, you need the Enterprise Edition of MetaFrame Presentation Server running. Answers A and B are incorrect because these editions of MPS server do not offer the Resource Manager component. Answer D is incorrect because there is no Custom version of the MPS server.

2. How often is data collected from the MPS servers in the farm written to the Summary Database?

- 
- A. every 60 minutes
- 
- B. every 24 hours
- 
- C. every 12 hours
- 
- D. every 6 hours

A2: Answer B is correct. Data is collected from all the MPS servers and written to the Summary Database on a daily basis. Answers A, C, and D are incorrect because they are not the correct interval at which data is written to the Summary Database.

3. Every MPS server in the farm temporarily stores Resource Manager data locally. What is that data called?

A. Summary data

B. Summary Database

C. TempRMDData

D. RMData

A3: Answer A is correct. The temporary data stored locally on each MPS server is known as the summary data. Answer B is incorrect because the Summary Database is the place where the RM data is stored for longer periods of time; it is not a temporary location and is not stored locally on each MPS server. Answers C and D are incorrect because no such filenames or data names exist.

4. How often does the Farm Metric Server access the zone data collector to retrieve farmwide application and server metrics?

A. 15 seconds

B. 15 minutes

C. 60 minutes

D. 24 hours

A4: Answer A is correct. The Farm Metric Server queries the zone data collector every 15 seconds, which is why Citrix recommends that the two functions be combined on the same server. Because of this, answers B, C, and D are incorrect.

5. You want to quickly check to see whether any servers in your farm are generating alerts. Where in the Management Console would you go to perform this task?

A. The Servers tab in the Resource Manager node

B. The Watcher tab in the Servers node

C. The Watcher tab in the Resource Manager node

D. The Summary tab in the Resource Manager node

A5: Answer C is correct. The Watcher tab in the Resource Manager node lists all servers in the farm that have generated alerts. Answers A, B, and D are all incorrect because these nodes do not exist. Another location where you could view alert information is the Resource Manager tab under the Servers node.

6. Where do MPS servers locally store the Summary Data files?

A. \Program Files\Citrix\Citrix Resource Manager\SummaryFiles

B. \Program Files\Citrix\Citrix Resource Manager\SummaryData

C. \Program Files\Citrix\Citrix Resource Manager\SummaryDataFiles

D. \Program Files\Citrix\Citrix Resource Manager\SummaryDBFiles

A6: Answer A is correct. The correct path to store the temporary files on each MPS server is \Program Files\Citrix\Citrix Resource Manager\SummaryFiles. Answers B, C, and D are incorrect because the paths are incorrect.

7. How often is the real-time data refreshed on an MPS server?

A. every 1 second

B. every 15 seconds

C. every 30 seconds

D. every 60 seconds

A7: Answer B is correct. When you are viewing real-time graphs, the data is refreshed every 15 seconds. Answers A, C, and D are incorrect because they are not the correct interval.

8. Choose the two types of report categories to which you have access from the Resource Manager node in the Management Console?

A. Reports from Local Database

B. Reports from Historical Database

C. Reports from Real-time Database

D. Reports from Summary Database

A8: Answers A and D are correct. The two reporting categories that you have access to from the Resource Manager node in the Management Console are Local Database and Summary Database. Answers B and C are incorrect because no such categories exist.

9. What are the communications methods by which Resource Manager can alert an administrator of an issue on an MPS server? (Choose all that apply.)

A. Email

B. SMS

C. Bluetooth

D. Pager

E. SNMP

A9: Answers A, B, and E are correct. Email, SMS, and SNMP are the only three communications methods Resource Manager can use to send alerts. Answer C is incorrect because Bluetooth is not a supported communications medium. Answer D is incorrect because Pager is not a supported communications medium.

10. When using the billing features of Resource Manager, how do you group users to apply a fee-based profile on them and run reports against them?

A. group users in cost centers

B. group users in billing centers

C. group users in domain groups

D. group users in organizational units

A10: Answer A is correct. Cost centers are used to group users and apply a fee-based profile on them. Cost centers are also used to run reports against. Answers B, C, and D are incorrect because there is no such thing as billing centers, you can't group users and apply fee-based profiles on domain groups directly, and you can't take advantage of user groupings in organizational units to apply fee-based profiles or run reports.

 PREV

NEXT 

# 16. What's New in MetaFrame Presentation Server 4.0

Terms you'll need to understand:

- CPU Utilization Management
- Virtual Memory Optimization
- CPU Shares and Reservations
- Application Isolation Environment
- Virtual IP Support
- Citrix Universal Printer
- TWAIN Redirection
- PDA-USB Synchronization

Techniques you'll need to master:

- Managing CPU usage for multiple users
- Managing virtual memory usage and excluding applications from the memory optimization process
- Recognizing the new management enhancements to the MetaFrame Access Suite Console
- Understanding the benefits of application isolation and how applications are managed within an isolation environment
- Understanding the benefits of virtual IP and loopback address support
- Recognizing the new policies introduced with MPS 4.0
- Familiarizing yourself with enhancements to printing
- Familiarizing yourself with enhancements to Citrix ICA Session and Client Configuration
- Familiarizing yourself with enhancements to the Web Interface and web access to MetaFrame server farms

In this chapter, we focus on the new features of Citrix Presentation Server 4.0 that are covered in the associated Citrix Presentation Server 4.0: Administration exam 256. Much of the environment remains unchanged from MPS 3.0 and therefore is still relevant in the new exam. To clearly illustrate the areas of the environment that have changed, we have broken down this chapter into sections that are directly associated with the earlier chapters in this book. In each of the relevant sections, we then

summarize the changes or additions found in 4.0 versus 3.0. We hope this format allows you to quickly assimilate the 4.0 changes and helps you to prepare properly for the 256 exam. The following list summarizes the 4.0 changes as they relate to the subject matter of the chapters in this book (chapter numbers indicated in parentheses):

- MetaFrame Presentation Server Architecture (2) The core Presentation Server architecture itself remains unchanged. Components such as the MetaFrame Access Suite License Server, the Data Store, zone data collectors, and the Local Host Cache are all still used, and common TCP/IP listening ports remain unchanged. A number of farm, server, and application changes have been introduced, particularly in the area of application performance. One significant change is the elimination of mixed mode farm support with MetaFrame 1.8. Environments that require a migration path from MetaFrame 1.8 must use MPS 3.0 and then upgrade from MPS 3.0 to 4.0. MPS 4.0 also now includes installation media for Presentation Server for UNIX as well as Citrix Conference Manager.
- Installation Prerequisites (3) No changes have been made in the recommended hardware based on the operating system used. MPS still supports Windows 2000 Server, Windows Server 2003, and Novell Directory Services (NDS) for user authentication. Both Microsoft and Citrix licensing remains unchanged. The only difference relates to the Presentation Server Management Console, which now recommends the minimum Java Runtime Environment (JRE) version 1.2.4\_06 instead of 1.2.4\_04. With the removal of support for mixed mode operation, deployment planning involving MF 1.8 farm names is also no longer applicable.
- MetaFrame Access Suite Licensing (4) The new MetaFrame Access Suite Licensing (MASL) model introduced with MPS 3.0 remains unchanged in MPS 4.0. Two additions have been made to this product. The License Management Console now runs on an Apache web server. Citrix also now officially supports running the MASL server in a two-node Microsoft cluster in an Active/Passive configuration.
- Installing MetaFrame Presentation Server (5) The installation process and tasks remain unchanged in the new version. The recommended migration process from MetaFrame 1.x has been updated for MPS 4.0.
- Configuring and Administering MetaFrame Presentation Server (6) Citrix has introduced a new node and settings to the Management Console and has greatly expanded the functionality of the Access Suite Management Console. Both areas are reviewed in this section of the chapter.
- MetaFrame Presentation Server Policy Management (7) The policy creation and management processes remain unchanged, but some additional policy settings have been introduced. These settings are briefly reviewed in this section.
- Citrix Load Management (8) There are no changes in Load Management in MPS 4.0.
- MetaFrame Security (9) Some new security enhancements have been introduced in 4.0 including additional Smart Card support and support for RSA SecurID and SafeWord running on UNIX instead of just on Windows.
- Application Integration (10) The process of publishing applications and content remains unchanged, but Citrix has introduced the new isolation environment, memory optimization, and virtual IP address features that directly relate to running applications on a Presentation Server. These three features are reviewed in this section.
- Deploying Applications Using Installation Manager (11) Installation Manager now supports the installation of packages directly into an isolation environment. All other components of this module remain unchanged.

- Printing (12) A number of enhancements have been made to both client and network printing in MPS 4.0. These new features include a new universal printer driver, client support for print job viewing, and support for a generic Citrix Universal Printer.
- [Citrix ICA Client](#) Configuration (13) MPS 4.0 brings with it the 9.x release of the Win32 ICA client. A number of new client-related features have been added, such as client-device support for TWAIN and USB ActiveSync support for personal digital assistant (PDA) devices.
- Web Connectivity to the MetaFrame Server Farm (14) Conceptually, the Web Interface remains unchanged, but MPS 4.0 introduces both a new way of managing the environment and additional management features. Instead of the web-based Web Interface Console and the PN Agent Console, both components are now managed through the Access Suite Console (ASC).
- Resource Manager (15) The components of Resource Manager are unchanged in MPS 4.0.

Throughout the remainder of this chapter, we review in detail those areas that have seen modifications in MPS 4.0.

 PREV

NEXT 

# MetaFrame Presentation Server Architecture

The core Presentation Server architecture (License server, Data Store, Data Collectors, and so on) discussed in [Chapter 2](#) remains unchanged in MPS 4.0. Three architectural changes to note are

- Elimination of mixed mode (interoperability mode) support for the MetaFrame 1.8 farm migration
- CPU utilization management
- Memory utilization management

## Elimination of MetaFrame 1.8 Interoperability

One significant change in MPS 4.0 is the elimination of mixed mode farm support with MetaFrame 1.8. Companies that want to migrate from their existing MF 1.8 environment have two choices:

- Upgrade their environment in stages using interoperability support with MPS 3.0. After migrating all servers to MPS 3.0, they can perform an in-place upgrade to MPS 4.0. Citrix fully supports the upgrade path from 3.0 to 4.0.
- Implement a new MPS 4.0 environment in parallel to the existing MF 1.8 environment and migrate users gradually from one farm to the other. If users must access applications in both environments, Citrix recommends using the Web Interface for MPS to access applications from both the new MPS 4.0 farm and the legacy 1.8 farm. Authentication tickets must be disabled for the 1.8 farm; otherwise, users will be unable to access these applications, instead receiving a message stating an error occurred while trying to connect to the published resource.

As a result, all associated interoperability settings are no longer available in the latest Management Console. You *can* still enable Data Collectors to respond to legacy ICA Browser UDP broadcasts within the properties for the server farm.

### Alert

Note the supported migration methods from MF 1.8 to MPS 4.0 and remember that interoperability mode is no longer supported.

## CPU Utilization Management

A significant new feature available only with the Enterprise Edition of MPS 4.0 is CPU utilization management. When enabled, this setting modifies Windows's default job priority scheduling in an attempt to ensure all users have "fair" access to an equal share of the CPU resources. Through this change, the normal CPU consumption of each user is brought within a predictable range (what Citrix

refers to as *normalizing*). In doing so, typical application performance spikes are reduced, increasing the available CPU to handle additional processing tasks.

CPU utilization management also throttles CPU-intensive applications, restricting them to a fixed number of CPU cycles and protecting the entire environment from being impacted by such applications.

CPU utilization can be controlled at the farm level or at an individual server level. When this feature is enabled, two special services called Citrix CPU Utilization Mgmt/Resource Mgmt and Citrix CPU Utilization Mgmt/User-Session Sync are started. Together, these services work to calculate the load for all processes associated with a user and adjust CPU priority of these processes accordingly.

Citrix has introduced new Performance Monitor counters, allowing you to track the effectiveness of the CPU utilization configuration. The object labeled Citrix CPU Utilization Mgmt User contains the counters CPU Entitlement, CPU Reservations, CPU Shares, CPU Usage, and Long Term CPU Usage.

MPS users are granted an equal number of CPU *shares*, representing a relative percentage of CPU cycles. The default value assigned to each user is 8, but this value can be adjusted on a per-user basis by modifying the Registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CTXCPU\Policy
```

Specific users can be assigned different shares by adding an entry with the format

```
<userID>,cpu.shares=<x>
```

where **<userID>** is the user ID preceded with the domain for example, NOISY\toddm. Currently, only individual users can be added. Windows groups are not supported. The **<x>** represents the number of shares assigned to the user. If you assign 10 to user A, then relative to user B who is assigned 8, user A would get 20% more of the CPU.

Within the CTXCPU key, you can also reserve a specific percentage of the CPU for one or more users. In the Policy key, you would add an entry with the format

```
<userID>, cpu.reservation=<y>
```

where **<userID>** is the same as the preceding description and **<y>** is the percentage of CPU in thousands. The default entry found here is

```
NT AUTHORITY\SYSTEM,cpu.reservation=20000
```

meaning that the **SYSTEM** process automatically reserves 20% of the CPU, leaving the other 80% to be divided among all active users.

In certain instances, you may want to allocate a differential share or reservation of the CPU to given users. Any changes should be monitored carefully using the appropriate Performance Monitor objects.

You can find the setting to enable CPU utilization management under the new Memory/CPU Utilization Management setting in properties of the farm node or an individual server in the Management Console.

## Alert

You should understand the concept of *CPU shares and CPU reservation* and how these settings could be customized for a specific user ID.

## Virtual Memory Optimization

An associated optimization feature for virtual memory has also been introduced in the Enterprise Edition of MPS 4.0. Memory optimization allows you to improve speed, performance, and scalability for a farm or individual servers. Memory management increases the number of users a server can support by optimizing the use of DLLs stored in virtual memory. When this feature is enabled, the Citrix Virtual Memory Optimization service is started. This service is responsible for monitoring application loads and recording any DLL access collisions that occur. These collisions are recorded to a file called Repair.SFO that is read at scheduled intervals (and on bootup) by the CtxBace.exe program. This program is responsible for optimizing the loading of the executables and DLLs listed in the Repair.SFO file. A list of all optimized DLLs and the associated memory savings are recorded to an XML file called Bind####.SFO. All associated files for virtual memory optimization are located in the Server Resource Management\Memory Optimization Management folder under the Presentation Server installation folder.

When enabled, memory optimization is applied to all executables and the associated DLLs by default. Predefined sets of applications (processes) and DLLs (components) that are excluded are listed in the following Registry keys:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SFO\ComponentExclusionList

and

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SFO\ProcessExclusionList

Within the Memory/CPU Utilization Management property of the farm or server node, this setting is enabled or disabled. In the Memory Optimization property (found only within the farm node), you define the actual optimization schedule and manage the list of applications and components excluded from the memory optimization process.

## Note

Part of Citrix's optimization process involves taking the original executable or DLL and rewriting it to the file system with updated memory reference information. This updated information loads DLLs in alternate base memory locations, avoiding conflicts with other DLLs and increasing its reusability with multiple processes. Changing the base memory location is known as *rebasing*. Associated executables that use these DLLs are rewritten to include this alternate base address information and the addresses of the exported functions within the DLL. This greatly increases the startup time of the EXE because querying for this information on startup is not required. The updated EXE and DLL files are stored in alternate streams in the file system. They are hidden from programs such as Windows Explorer but accessed when the program is launched.

This process is not without limitations. Programs that validate their executable or associated DLLs at runtime (such as antivirus programs) fail with this optimization. Digitally signed programs can also fail if checked by the application. These types of programs must be

excluded when memory optimization has been enabled in order to run properly.

## Tip

Sometimes application files are stored on a remote file server and require special access permissions for instance, domain administrator permissions. If this is the case, clear the Use Local System Account check box. Enter the appropriate account and password that have permissions to access the remote files.

 PREV

NEXT 

## Installation Prerequisites

No changes have been made in the recommended hardware or supported operating systems in MPS 4.0. The Presentation Server Management Console now requires a minimum of JRE 1.2.4\_06, and interoperability support for MetaFrame 1.8 is no longer available. See the section "[MetaFrame Presentation Server Architecture](#)" for more information.

## MetaFrame Access Suite Licensing

The new MetaFrame Access Suite Licensing (MASL) model introduced in MPS 3.0 and discussed at length in [Chapter 4](#) has not changed in MPS 4.0. All of the installation requirements are still valid. A couple of enhancements to MASL improve functionality:

- Apache Web Server Support The License Management Console now runs on an Apache web server instead of just on Microsoft IIS. Apache is supported only on the Windows operating system. MASL cannot be deployed on a non-Windows operating system.
- Two-node Microsoft Cluster Support Citrix provides support for MASL operating in an active/passive cluster configuration with a shared drive. To install MASL on a clustered server, you must launch the installation from a command prompt, providing special command-line switches to the MSI installer. When generating the license file for the cluster, you must provide the full name of the cluster, not the name of an individual license server. Full details on the two-node cluster configuration are found in the latest MetaFrame Access Suite Licensing Guide.

## Installing MetaFrame Presentation Server

The installation process remains unchanged in MPS 4.0. The only exception is the change in the MF 1.8 to MPS migration path. See the section "[MetaFrame Presentation Server Architecture](#)" for details.

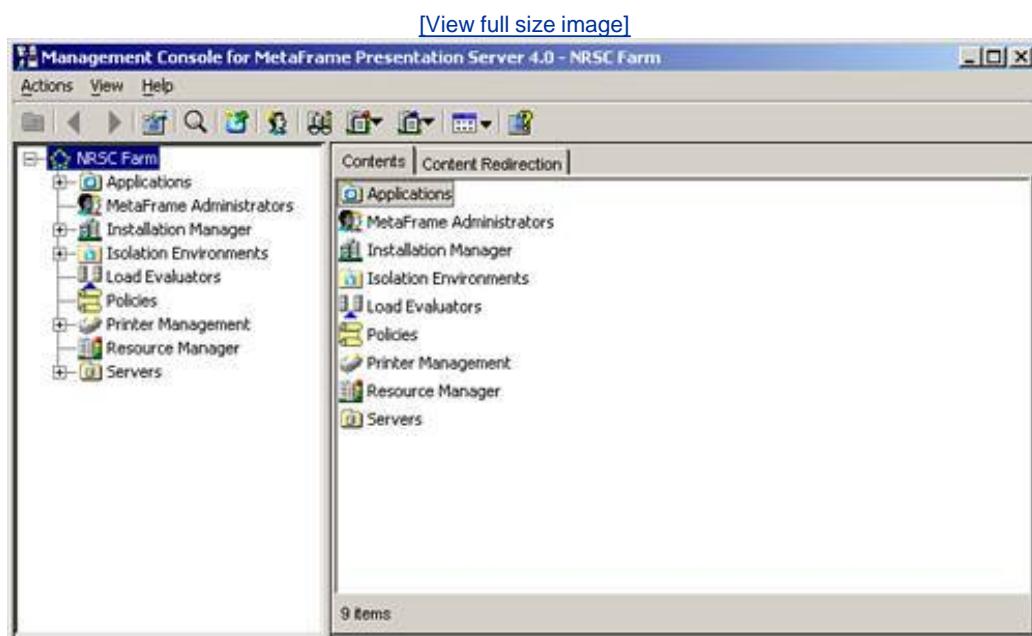
# Configuring and Administering MetaFrame Presentation Server

With MPS 4.0 has come new settings in the Management Console for Presentation Server and the Access Suite Console for Presentation Server. As you recall from [Chapter 6](#), the Access Suite Console operates as a Microsoft Management Console (MMC) snap-in and provides tools for overall performance, configuration, and maintenance of all of your Citrix Access Suite products. The Presentation Server Management Console is a Java-based application designed specifically to manage your Presentation Server farm.

## Changes and Additions to the Presentation Server Management Console

[Figure 16.1](#) shows the default view of the new Management Console for the Enterprise Edition of MPS 4.0. In the next few sections, we provide an overview of the new features and changes in each of the main management modules.

Figure 16.1. The Presentation Server Console for MPS 4.0.

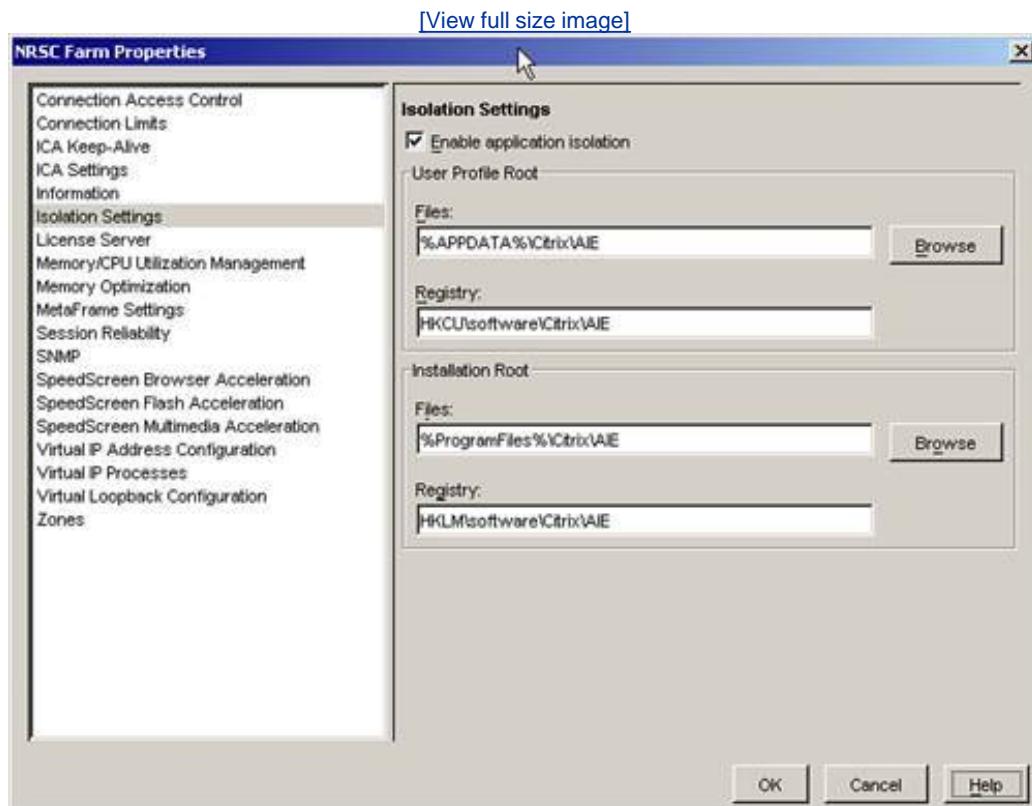


### Server Farm Node

The property page for the Server Farm node has the following changes and additions:

- Connection Access Control This setting allows you to restrict how users can access published content in the farm. By default, connections from any client are accepted. There is also the option to restrict access to only those clients coming through the Web Interface (including PN Agent) or through the Secure Access Manager product. Direct client access to the farm is restricted. The third option restricts access to only those clients coming through the Secure Access Manager.
- Interoperability This setting has been removed.
- Isolation Settings The new Isolation Settings feature (see [Figure 16.2](#)), which we review in the "[Application Integration](#)" section of this chapter, provides an environment within which you can run applications that traditionally would not function well (or at all) in a Terminal Services or MetaFrame environment. This settings page provides a single location where the isolation environment can be enabled or disabled for the entire farm; in addition, it specifies the location where the Application Isolation Environment (AIE) Registry and file system information are maintained. Note that although you can enable or disable support for isolation environments at the farm or individual servers, the default isolation locations shown here are still read by individual servers. You can override these settings within an individual isolation environment. Support for application isolation is enabled by default for all servers in the farm.

Figure 16.2. Application isolation is a new feature of MPS 4.0.



- Memory/CPU Utilization Management and Memory Optimization These two options manipulate the CPU and memory optimization settings that we discussed in the "[MetaFrame Presentation Server Architecture](#)" section earlier in this chapter.
- MetaFrame Settings One new option has been added to this property page: the setting labeled Enable Merging of Shadowers in Multiple Shadowing Policies. This setting overrides the default

policy behavior that applies only the highest priority policy containing shadower settings. Any lower-priority policies that also contain shadower properties are ignored. When this setting is enabled, all policies that have shadower settings are merged together, and all are considered valid. Refer to [Chapter 7](#) for details on policy behavior and the shadower policies.

- **Virtual IP Address Configuration** This setting allows applications to run with their own virtual IP address. Computer telephony applications commonly fall into this category. On this screen, you must first define a range of addresses that will be available for assignment. You then assign either all or a subset of the addresses in that range to one or more Presentation Servers. These addresses are then available to be used by the specified applications (processes) on that server. Virtual IP assignment will not take effect until the server is restarted. After virtual IPs have been assigned to a server, you can assign the associated processes that may require access to one of these addresses. This is done in the Virtual IP Processes, discussed next.
- **Virtual IP Processes** In this setting, you associate processes with either the Virtual IP Address or the Virtual Loopback Address settings. You must know the name of the application's main process (Winword.exe, for example) and manually add it to the appropriate section. You cannot browse the system for this information.
- **Virtual Loopback Configuration** This setting is similar to the Virtual IP Address configuration, but instead allows servers to provide virtual loopback address support. The loopback address is 127.0.0.1 and is also accessible as the *localhost* hostname.

## Applications

Published applications in the Applications node have a couple of additions:

- **Access Control** This setting allows you to configure whether the application is available through the MetaFrame Secure Access Manager (4.0 or later). Either it is enabled for all connections, or it can be restricted to specific Secure Access Manager farms and filters. You can restrict this application to have access only through Secure Access Manager by deselecting the Allow All Other Connections option at the bottom of the dialog box.
- **Application Location** When you are publishing an application (this setting does not apply to desktops or content), this property page displays the Isolate Application setting. Isolation environments are discussed next in the "[Isolation Environments](#)" section.

## Isolation Environments

One of the most-discussed new features of MPS 4.0 is the addition of isolation environments. Created to address the issue of running certain legacy and nonWindows-compliant applications, isolation environments allow you to run an application within a virtual Windows environment, protecting the operating system, other applications, and itself from interacting with each other.

Isolation environments allow you to safely host applications that are otherwise unable to coexist on a single server (for instance, different versions of an application), or software that isn't designed for use by multiple simultaneous users and that exhibits compatibility issues in a multiuser environment.

Isolation environments are also good for hosting legacy applications such as MS-DOS or 16-bit Windows applications.

## Note

Do not install an application into an isolation environment unless that application would otherwise not run correctly on the Presentation Server.

Applications are either installed directly into an isolation environment or can be placed there after installation. Typically, if it is determined that an application requires isolation, Citrix recommends that it be uninstalled and then reinstalled directly into an isolation environment. Once within this environment, the application is transparently provided access to copies of system and user-specific resources that it can then access and modify without affecting the originals, accessed by all other processes that run outside the isolation environment.

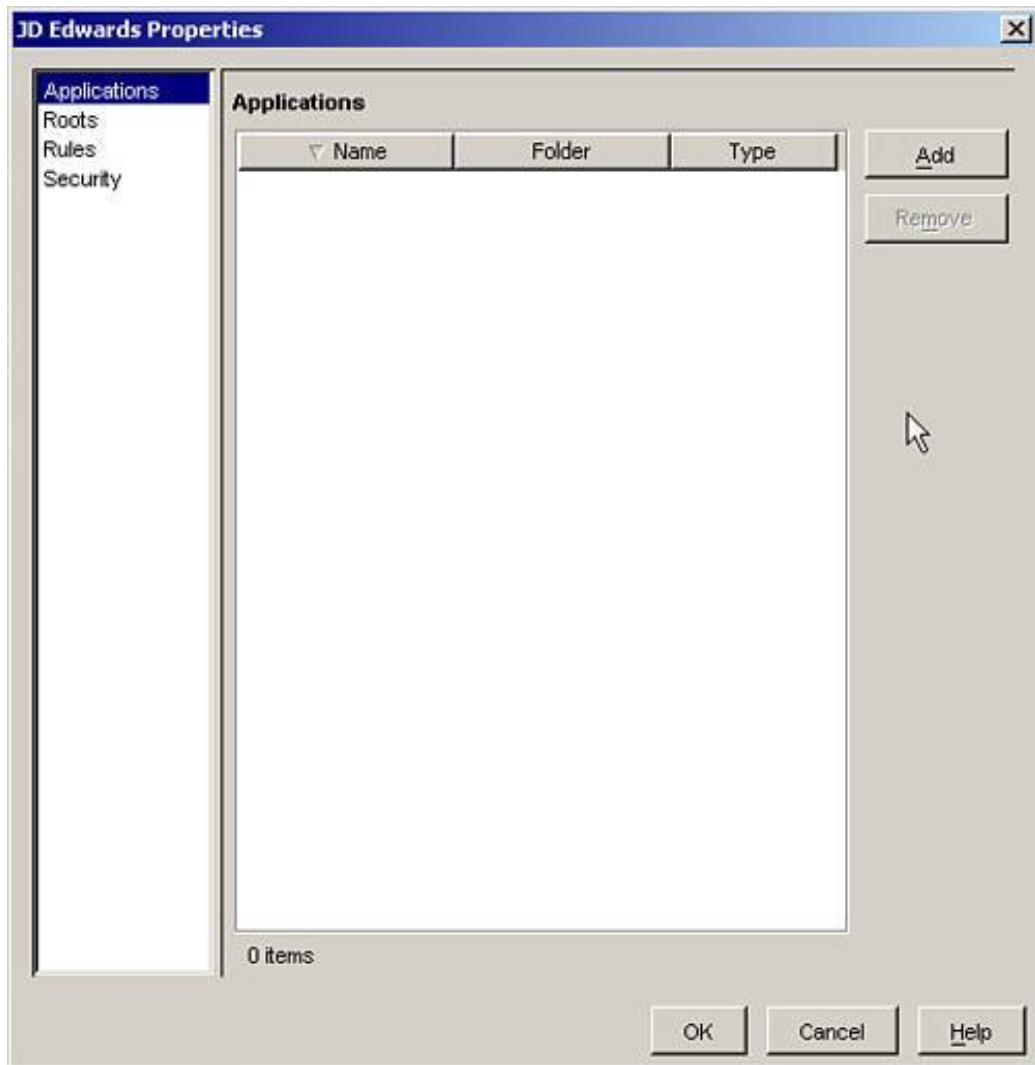
## Alert

Understand the circumstances within which you would benefit from adding an application to an isolation environment.

Within the isolation environment, specific rules are defined that dictate exactly how this application will behave within the environment. After creating a new isolation environment by right-clicking on the Isolation Environments node and selecting New Isolation Environment, you can then modify the environment's properties shown in [Figure 16.3](#).

Figure 16.3. Each isolation environment maintains its own properties.

[\[View full size image\]](#)



With an isolation environment, you can define the following options:

- Applications You add or remove existing published applications from within this setting. Applications can belong to only one isolation environment at a time. If you add an application to another environment, it is automatically removed from the one it currently belongs to.
- Roots From here, you define the root Registry and folder locations. You can use the existing farm defaults or define settings for individual servers.
- Rules This advanced setting allows you to manage the behavior of the isolation environment as it pertains to system and Registry settings. In this advanced configuration, only administrators with thorough knowledge of the Windows system architecture should make changes. Modifying the existing settings without proper knowledge can produce unexpected results.
- Security This setting determines whether to allow the execution of programs within the user's profile root. Windows security settings always take precedence over this setting.

In the "[Application Integration](#)" section of this chapter, we review the steps to installing an application directly into an application isolation environment.

## Policies

The creation, priority, and assignment of MetaFrame policies remain unchanged from the information described in [Chapter 7](#). Citrix has added a number of new policy settings. We briefly review these policy settings in the "[MetaFrame Presentation Server Policies](#)" section of this chapter.

## Printer Management

A number of new printer enhancements have been introduced with MPS 4.0. Specific details on these changes are discussed in the "[Printing](#)" section of this chapter. Within the Printer Management node, you need to be aware of two main changes:

- New Universal Printer Driver When clicking on the Drivers node, you see another UPD in the right pane labeled simply Citrix Universal Printer. It represents the new Citrix UPD that enables Presentation Servers to use Microsoft's Windows Enhanced MetaFile Format (EMF) to transfer print jobs from the server to the client. This is the same format Windows uses to transfer print jobs to a printer spooler for printing. This new UPD is available only to Windows-based clients. Linux-based clients still use the PS UPD. You will find a noticeable improvement in printer performance with this new printer driver. You will also have access to additional advanced printing features such as alternate printer trays.
- Network Printer Auto-Creation In MPS 3.0, Citrix provided access to a network printer auto-creation feature from the Printer Management node. This feature allowed an administrator to assign users and/or groups to one or more printers. When users logged on to a MetaFrame server, the printer was automatically mapped for them. There was no need to manage printer mappings through logon or other scripts.

MPS 4.0 has removed this feature from the Printer Management node. Right-clicking on a printer within the Printers node no longer shows the Auto-Creation option. Instead, this mapping feature has been moved to a MetaFrame Policy. See the "[MetaFrame Presentation Server Policies](#)" section for more information.

All other functionality in the Printer Management node remains unchanged from MPS 3.0.

## Servers

When a server within the Servers node is selected, the same tabs visible in MPS 3.0 are displayed in MPS 4.0. Within the properties for a server, the following additions have been made:

- Isolation Settings This setting accompanies the corresponding server farm setting and dictates whether the server inherits the farm settings for the isolation environments or whether it is explicitly enabled or disabled on its own. No per-server root information is maintained here. You can define per-server settings directly within the properties of an existing isolation environment. See "[Isolation Environments](#)" earlier in this chapter.
- Memory/CPU Utilization Management This setting defines whether memory and CPU utilization settings are inherited from the farm or explicitly set for the application. The processes that are excluded from memory optimization are defined only at the farm level and cannot be managed on a per-server basis.
- Virtual IP Configuration Unless you have defined an IP address range and assigned the server within the properties of the server farm node, the Enable Virtual IP for This Server setting is

grayed out and not editable. After it has been configured at the farm level, you can disable or enable the option. It is enabled by default if set in the farm node. The Enable Virtual Loopback for This Server setting is disabled by default but can be enabled per server without any farm settings required.

## Alert

You are expected to identify what new features of Presentation Server are managed at the farm level and what associated settings can be managed on a per-server level.

## Changes and Additions to the MetaFrame Access Suite Console

This MMC snap-in has been updated to include support for managing the Web Interface. Through the Access Suite Console, you now create and manage all of your Web Interface for Presentation Server and Program Neighborhood sites. We look at this topic in more detail in the "[Web Connectivity to the MetaFrame Server Farm](#)" section of this chapter.

## Note

Because the Access Suite Console is now used to manage the Web Interface, it *must* be installed on each web server that will host a Presentation Server Web Interface. The Web Interface will not install without it being present.

Aside from the addition of the web components and some minor changes to the look of the interface, the remaining options available in this console are the same as those found in the MPS 3.0 Access Suite Console.

 PREV

NEXT 

## MetaFrame Presentation Server Policy Management

The creation and management of MetaFrame policies remains unchanged from MPS 3.0 and the information provided in [Chapter 7](#). Citrix has made some minor changes in the order in which policy folders appear, however, and provided some additional policies that we review in [Table 16.1](#).

Table 16.1. MPS 4.0 Policy Additions

Policy Path	Settings	Comments
Bandwidth/Session Limits/TWAIN Redirection	Limit (Kb/sec)	This policy is added as part of the new support for mapping TWAIN client devices. The maximum bandwidth available to clients for TWAIN redirection is provided here.
Client Devices/Resources/Drives/Optimize/Asynchronous writes	Turn on asynchronous writes to client disks.	This policy is designed to improve drive access and folder browsing through client-mapped drives. This policy enables the asynchronous writing of data from server to client drive but should be enabled only when users are accessing over a high-bandwidth connection and experiencing high latency. Citrix recommends enabling this option only when users will be able to restart any file transfer that is interrupted due to a failure.
Client Devices/Resources/Ports/Turn off COM ports	Turn off client COM ports.	This feature is not new, but disabling COM port mapping prevents USB-connected PDAs on the client device from being accessible in MetaFrame.
Client Devices/Resources/PDA Devices/Turn on virtual COM port mapping	Turn on virtual COM port mapping.	Enabling this option allows USB-connected PDA client devices to synchronize via Microsoft ActiveSync with

Policy Path	Settings	Comments
		software on the MetaFrame server. Virtual COM port mapping also requires that the Turn Off Client COM ports policy be "Not Configured" or "Disabled."
Client Devices/Resources/Other/Configure TWAIN Redirection	Do not allow TWAIN redirection.  Allow TWAIN redirection.	When this policy is enabled, you can configure whether to enable lossy compression. This feature increases performance of the image transmission by reducing the quality of the image. Citrix does not recommend using this setting with optical character recognition (OCR) software.
Printing		This entire node is new in MPS 4.0. The printer settings previously found under Resources in MPS 3.0 have been moved here along with a few new settings.
Printing/Client Printers/Legacy Client Printers	Create dynamic session-private printers.  Create old-style client printers.	The creation of session-private printers generates client-mapped printers that are private to each user session and have a naming standard similar to client printers in Terminal Services alone. The format is <name> from <client> in session x. Old-style client printers can be shared between sessions; they use the old Citrix client printer naming standard.
Printing/Client Printers/Printer property retention	Printer properties should be:  Saved on the Client only.  Retained in user profile only.  Held in profile only if not saved on client.	This policy controls how user printer settings are retained.  Saved on the Client Only is suitable for situations in which users have mandatory profiles or roaming profiles that are not saved. This setting is supported only on MPS 4.0 or later and the Citrix client

Policy Path	Settings	Comments
		9.0 or later. Retained in User Profile Only preserves the settings in the Terminal Server profile. There is no attempt to write information to the client. This option is supported with MPS 3.0 and the MPS client 8.x or earlier. Held in Profile Only If Not Saved on Client is enabled by default, and it instructs the MPS server to try to maintain client settings if supported; otherwise, they are retained on the server. This setting is compatible with MPS 3.0 and the MPS client 8.x or earlier.
Printing/Drivers/Native printer driver auto-install	<p>Install Windows native drivers as needed.</p> <p>Do not automatically install drivers.</p>	By enabling this option and setting Install Windows Native Drivers as Needed, you instruct the MetaFrame Server to install native Windows drivers if necessary when a client connects with a new client-mapped printer. Only drivers present in the driver.cab file are installed. This CAB file contains those printer drivers signed by Microsoft as being compatible. When Do Not Automatically Install Drivers is selected, a native driver is not available for a client printer unless explicitly installed by an administrator. Citrix warns that a large number of native drivers could be installed if users are connecting from a variety of different clients with different printers available.
Printing/Drivers/Universal driver	<p>Use universal driver only if requested driver is unavailable.</p> <p>Use only printer model specific</p>	This rule replaces the MPS 3.0 rule in Resources/Local Printers/Drivers. The functionality is identical.

Policy Path	Settings	Comments
	drivers.  Use universal driver only.	
Printing/Session printers	Network printers to connect at logon.  Choose client's default printer.  Do not adjust the user's default printer.  Set default printer to the client's main printer.	This policy combines the MPS 3.0 policy found in Resources/Local Printers/Default with the Network Printer Auto-Creation feature that was available in the Printer Management node. Within this policy, you can select any number of available network printers in the farm and assign them to the policy recipients. You also have the option of whether to remap the default printer to match the local client default printer.
User Workspace		Aside from moving the option for MetaFrame Password Manager to the bottom of the list, all policies under here remain unchanged.

 PREV

NEXT 

# MetaFrame Security

Citrix has introduced a number of more subtle security enhancements in MPS 4.0. Users who use the existing technology will find these changes beneficial to the operation of the environment. The changes include

- Smart Card Recognition Support Smart Card support is now accessible by applications within Presentation Server without the need to run the **SCCONFIG** command-line utility. In previous versions of MetaFrame, only the Winlogon.exe and LSASS.exe processes used for Smart Card logon had access. Other applications would not "see" the Smart Card unless they had been configured using the **SCCONFIG** tool.
- Smart Card Authentication Pass-through User credentials generated using a Smart Card can now be passed through to new sessions on different servers. Users can now access nonSmart Card-enabled servers using credentials generated from their initial Smart Card logon.
- Common Access Card Support In combination with the Win32 client for Presentation Server, Citrix now fully supports the use of the Common Access Card. Common Access Cards provide a mechanism for both authentication and identity validation. Common Access Cards typically are used as a means of digitally signing content such as emails.
- HP ProtectTools Support Citrix has added support for HP ProtectTools through the Win32 clients or the Web Interface. ProtectTools is an HP-developed product that provides access security using products such as Smart Cards, embedded security chips, and USB tokens.
- RSA SecurID and SafeWord on UNIX Support Support for user authentication to the Web Interface using either of these products has been extended from Windows to include UNIX operating systems.
- "Safe for Scripting" Property Addition to the Web Client The Web client now contains the necessary property settings that flag it as being "safe for scripting." When an ActiveX control is marked "safe for scripting," this tells the web browser that is loading the object (such as Internet Explorer) that it contains the necessary precautions to ensure that any web page script attempting to access it cannot violate any of the security mechanisms of the client environment. Without such a mechanism, the control may not load and execute properly, depending on the security settings of the browser.

## Alert

Make certain you can identify and list the security enhancements in MPS 4.0.

# Application Integration

The application and content publishing features of MetaFrame remain unchanged in MPS 4.0. Citrix has introduced new features to better utilize the available resources for application use. All of these options have already been discussed in this chapter. In the following sections, we look at some specific configuration options in more detail. The new features are

- [Application Isolation Environments](#) This feature was discussed in the "[Isolation Environments](#)" section of this chapter. In this section, we review how to install and uninstall an application from an isolation environment.
- [Memory Optimization](#) This feature was discussed in the "[MetaFrame Presentation Server Architecture](#)" section of this chapter.
- Virtual IP Address Support This feature was also introduced earlier in this chapter. In this section, we review the circumstances under which these settings may need to be implemented.
- Virtual IP Loopback Address Support This feature was discussed earlier.
- Client IP Address Pass-through A new feature not prominently mentioned is MetaFrame's capability to pass the client IP address through to a server application. This feature is intended only to satisfy those applications that require a unique IP address for identification purposes. This address cannot be used for any form of binding or addressing. We describe the configuration process in this section as well.

## Installing Applications within an Isolation Environment

There are two ways of isolating an application in your MetaFrame environment. The first is to associate the published application with an isolation environment either when the application is first published or after the fact by modifying the isolated application setting for that published application.

The other way to isolate an application is to install it into the desired isolation environment. When an application appears to be a candidate for isolation, this is the configuration Citrix recommends because it ensures everything related to that application is isolated. Even if the isolation environment fails to correct an application that is associated with the environment, installing the application into that environment may correct the issues. If necessary, an application should be uninstalled and then reinstalled directly into an isolation environment. Citrix supports installing applications into an isolation environment in one of three ways:

- Using Installation Manager. Installation Manager includes a new option allowing you to choose to install a package into a specified isolation environment.
- Using a third-party product such as Microsoft SMS.
- Using the AIESetup.exe utility.

Citrix does not support application installations into an isolation environment through a Microsoft RDP connection.

## Note

MPS 4.0 does not support the isolation of services. Citrix silently disables any services that are installed as part of an isolated application install.

AIESetup is a command-line tool that allows you to perform an application installation into an existing isolation environment. It is recommended that each isolated application run within its own isolation environment. This minimizes conflicts and simplifies the process of removing the application at a later date.

The AIESetup utility has the following syntax:

```
aiesetup [/d] [/n] [/q] [/w] <Isolation Env. Name> <Installer Name> [app parameters]
```

**/d** Disables the automatic application discovery process that otherwise initiates when the application installation completes. The application discovery process is intended to assist in the publishing of the application by searching the server for any installation-created shortcuts and extracting the application startup information and writing to the Data Store. When publishing the application, you then have the option of using this information when adding the application to the isolation environment. If you omit **/d**, you are prompted at the end of installation as to whether you want to run this process.

**/n** Disables automatically placing the server into install mode prior to installing the application. If this setting is not specified, AIESetup performs the equivalent of a `change user /install` command.

**/q** Installs in quit mode. All AIESetup prompts are suppressed.

**/w** Waits for the setup program to complete before continuing. This is most often used when launching AIESetup from a script and you want to proceed only after the application installation is complete.

**<Isolation Env. Name>** Indicates the name of the isolation environment into which this application is being installed. Include quotes around the name if spaces exist.

**<Installer Name>** Indicates the name of the installation program.

**app parameters** Specifies optional installation parameters for the installer program. If the installer program is a Microsoft Installer binary (.MSI), you should use `msiexec.exe /i <installer .MSI>` followed by the MSI parameters.

To install an application using AIESetup, you must have the following rights:

- Administrative access on the MetaFrame server
- Rights to manage isolation environments in the farm
- Rights to publish and edit applications in the farm

After installing the application into the isolation environment, you need to go into the Management Console and publish the application. When publishing the application, choose to isolate the application and then select the option specifying the application has already been installed in the environment. Choose the installed application from the list, verify any application parameters, and then continue to

complete the setup.

## Alert

You are expected to know and understand the process of installing an application into an isolation environment, including permissions using AIESetup. You should also know the different methods of installing an application into an isolation environment.

## Uninstalling an Application from an Isolation Environment

An application that has been installed into an application isolation environment cannot be removed using Add/Remove Programs. Instead, a manual process is required to ensure that all of the associated application binary and Registry additions have been successfully removed.

The simplest way to remove an application is to remove all of the file and Registry root folders created for the isolation environment. This is one reason why it is recommended that only a single application be installed into an isolation environment.

You remove all applications from an isolation environment as follows:

1. Remove the published application.
2. Locate the installation root folder for the isolation environment. The default is C:\Program Files\Citrix\AIE\<Isolation Env. name>.
3. Open the Registry. Remember all of the warnings regarding incorrect use of the Registry. Locate the Registry root folder for the isolation environment. The default is HKLM\Software\Citrix\AIE\<Isolation Env. name>.

## Caution

If you completely remove the isolation environment, you also delete any user-specific information stored in the per-user profile root. Make sure that all necessary data is backed up before removing an isolation environment.

## Virtual IP Addressing

You can provide a unique IP address for those applications that

- Have a dependency on the use of Windows sockets for communications
- Require a unique IP address per application instance or must use a specific fixed TCP port number

When these conditions are met, you need to enable the assignment of virtual IP addresses for multiple instances running on the same server to function properly.

Virtual IP addresses are defined in the Virtual IP Address Configuration property of the server farm. See the earlier section "[Changes and Additions to the Presentation Server Management Console](#)" for details on this and other IP address configuration choices.

When determining the number of IP addresses to assign to each server, you must take into consideration the maximum number of concurrent users who will be logged on to the server at any given time. When virtual IP addresses are assigned, they are assigned to each user session, regardless of whether they run an application that requires a virtual IP. If insufficient addresses are available, a user may receive an error message stating that no virtual IP addresses are available for the session. Failure to acquire a virtual IP does not prevent the user from logging on to the server or running any of his or her published applications. It will likely cause any applications dependent on the virtual IP address to fail.

After defining the IP address range, you can assign processes to use the assigned virtual address within the farm properties. You cannot make these changes within the individual server properties. The only IP address options supported at the server level are

- Enable or disable the use of virtual IP address assignment.
- Use the farm settings for logging or define them for the server.
- Enable virtual loopback assignment. We discuss this setting next.

When logging is enabled at the farm or server level, the assignment and release of the IP address are logged for each user session within the Application log.

## Alert

Remember that a unique IP address is assigned to every user session on a server that is providing virtual addresses, not just those user sessions running applications that require a virtual IP.

## Virtual Loopback Addressing

The use of a virtual loopback address is required if an application

- Requires access to the Windows loopback address (localhost or 127.0.0.1)
- Uses a specific TCP port number on this address

In this case, multiple instances of such an application conflict when they attempt to run unless loopback address virtualization is enabled. To enable this setting, you can either designate the desired servers in the farm within the server farm's Virtual Loopback Configuration properties or select Enable Virtual Loopback for This Server within the Virtual IP Configuration properties. When this setting is enabled, the server is automatically added to the list maintained at the farm level. Unlike virtual IP addresses, there is no possibility of a session being unable to receive a virtual loopback address.

## Client IP Address Pass-through

For those applications that require access to a unique IP address for identification or validation, the capability to pass through the IP address of the client device has been included in MPS 4.0. When the application queries for an IP address, the server automatically provides the associated address of the client. Client IP address pass-through should not be used if any of the following are true:

- The client is connecting using a protocol other than TCP/IP.
- The clients disconnect active sessions and then reconnect to those sessions from another client. The reconnected session returns an IP address that does not match the current client's address.
- A client is accessing the application through a pass-through client. The IP address returned is the address of the server on which the pass-through is occurring, not the local client IP address. This results in the application receiving a nonunique address if multiple pass-through clients are accessing the same application.

This setting must be enabled through the Registry. Being sure to follow all precautions regarding Registry use, you need to create the following Registry key (if it doesn't exist):

HKLM\Software\Citrix\VIP\

Next, you need to create the following two values:

`UseClientIP:REG_DWORD:0` (disabled) or `1` (enabled)

`HookProcessClientIP:REG_MULTI_SZ:<list of executable names that require client IP access>`

You must restart the server for the changes to take effect.

 PREV

NEXT 

## Deploying Applications Using Installation Manager

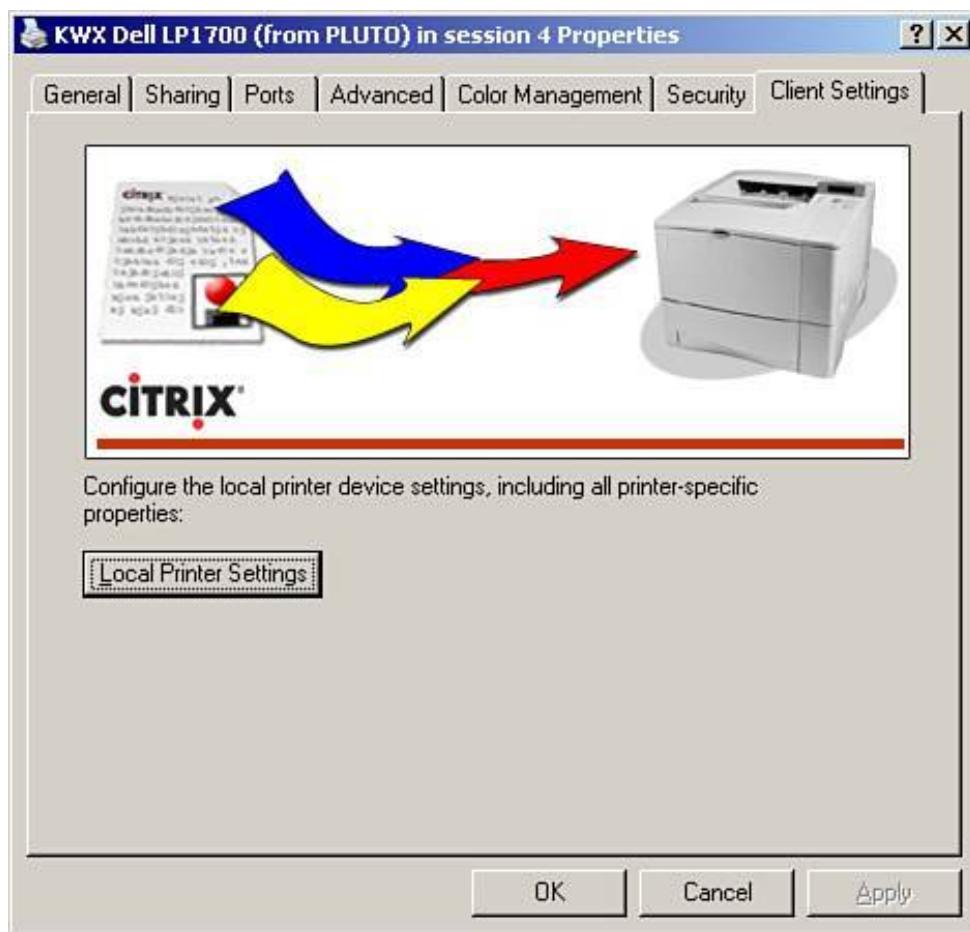
The use of Installation Manager remains unchanged from MPS 3.0, but one new option has been added to the Schedule Install Job dialog box for a package deployment. When deploying an application, you now have the option to specify that the application should be installed into an application isolation environment. When the Install into Isolation Environment check box is selected, the Settings button is enabled, and clicking provides the option to select an existing environment or to create a new one.

## Printing

In the "[MetaFrame Presentation Server Policy Management](#)" section of this chapter, we discussed the addition of the new Printing folder and the associated printer-related policy additions and changes. One of the other printing-related features in MPS 4.0 is the new version of the universal printer driver allowing MPS to use Microsoft's Windows Enhanced MetaFile Format (EMF) for transferring print job information from server to client. Through the use of EMF, users will notice a significant improvement in the time to print, as well as the addition of enhanced printer property management, including multiple tray selections and page collation. To take advantage of this feature, you must be running version 9.0 or higher of the Win32 Presentation Server client. When you are using an older ICA client, the alternate PCL or PS universal printer driver and print mechanism are used.

When the new UPD is being used, you see the driver named Citrix Universal Printer. You also see the Client Settings tab, as shown in [Figure 16.4](#). Clicking the Local Printer Settings button opens the settings page for the associated printer on the local client. You can then make the desired changes to the local printer before sending the print job to the client.

Figure 16.4. The new Citrix universal printer driver provides easy access to the local client settings.



The new Win32 9.x clients also support the viewing of client redirected print jobs within a local print job viewer application. Two different viewers are included:

- PCL2BMP.EXE This is the helper application for PCL and PS data. All print jobs using PCL or PS are directed through this helper application before being viewed or printed.
- CPVI EWER.EXE This application is responsible for processing EMF print job data from the MetaFrame server.

In conjunction with these clients and their viewers, you can now enable a generic Citrix Universal Printer on the MetaFrame server. This printer is not physically associated with any client printer and has no knowledge of their specific capabilities. When this printer is enabled, it is created along with any other client-mapped printers. For those users who require only basic printing capabilities, you can simplify management by disabling client-mapped printers and leaving them only with this generic printer and reduce the overhead of creating multiple locally mapped printers that are not required.

To enable this generic printer, you must modify the Registry. If it does not already exist, create the Registry key HKLM\Software\Citrix\Print. Within this key, create the following value:

**DefaultPrnFlags : REG\_DWORD**

If a value already exists, sum the existing value with the hex value 0x00000020. If the value does not exist, create the **DWORD** entry and assign it this value. A restart is *not* required. The next time a user logs on, he or she will see a printer labeled Citrix Universal Printer assigned as the default. The properties for the printer appear as they would for any other general Windows printer, but the Local Printer Settings button on the Client Settings tab appears disabled.

When a print job is sent to this printer, it automatically appears on the client's local PC within the Citrix EMF Viewer. Choosing Print from within this application opens the local printers, from which the user can then choose a desired target printer.

## Alert

Understand the role of the new print viewers and how to enable the new Citrix Universal Printer.

 PREV

NEXT 

# Citrix ICA Client Configuration

MPS 4.0 ships with Version 9.x of the ICA client. The client runs on Windows 9x, Windows NT 4.0, Windows 2000, Windows 2003, and Windows XP. Not only does the new client offer many new features and performance improvements, but it is also fully backward compatible with earlier versions of Windows and MetaFrame. The following list summarizes the new client-related features supported by version 9.x and MPS 4.0:

- **TWAIN Client Device Redirection** MPS can now transparently redirect locally attached imaging devices, such as scanners, from the client to the server. When these devices are connected, the user can capture an image when running software on the MetaFrame server that supports image acquisition via TWAIN devices. TWAIN redirection is managed through MetaFrame policies discussed earlier in this chapter. This feature requires the Advanced or Enterprise Editions of MPS.
- **Client-based PDA Synchronization** MPS now supports USB-tethered PDA synchronization with Microsoft Windows-powered PDAs and Microsoft ActiveSync synchronization agent. PDA synchronization is controlled through MPS policies and is dependent on the ability to map client COM ports.
- **Client Printer Improvements** The new and enhanced features were discussed in the "[Printing](#)" section of this chapter.
- **Smart Card Roaming** Support The Program Neighborhood Agent now supports the automatic logon and logoff of users when a Smart Card is inserted or removed from a client's associated card reader. The existing WorkSpace Control features can be implemented to further enhance this feature. WorkSpace Control is discussed in [Chapter 13](#).

**File Access and Folder Browsing Improvements** Citrix has implemented improvements in the speed at which files and folders are accessed over high-latency connections. Asynchronous writes to a client drive can be enabled through the associated MetaFrame policy.

## Note

Citrix commonly refers to features related to the integration of the client and the Presentation Server as *SmoothRoaming* features.

- **Quick Launch Bar Addition for Program Neighborhood** The PN client now includes a Quick Launch address bar where you can simply type in the name or address of a server and establish a connection without having to create a new custom ICA connection first. You manage properties for the Quick Launch Bar by clicking the Options button located at the far-right side of the client window. Most of the default options for custom ICA connections are used unless overridden by these options.
- **Operating System File Locking Support** Client drive mapping now supports and respects operating system file-locking rules. The remote file system driver locks an opened file on both the server and client sides. This prevents possible versioning conflicts that might otherwise occur.

when multiple clients simultaneously use a file.

- Improved Multimonitor Support MetaFrame Presentation Server has enhanced support for multimonitor user environments. Users can connect seamlessly to published applications without having to modify primary monitor settings (previous versions required you to set the top leftmost monitor as the primary monitor). Application menus now appear in the correct locations, instead of showing up only on the primary monitor. The client device needs a compatible video card. Plus, the client operating system needs to detect all the monitors. Each monitor should appear separately on the Settings tab in the Display Properties dialog box.

To configure properties, right-click on the server in the Presentation Server Console and choose Properties and then ICA Settings. Set the maximum memory to use for each session's graphics setting high enough that it will include the client's entire virtual desktop; otherwise, the application will be restricted to the subset of the monitors that fit within the size specified.

- Windows Keyboard Shortcut Pass-through MPS 4.0 supports the pass-through of typical Windows keyboard shortcuts to the Presentation Server desktop. With this long-overdue feature, you can now capture typical Windows keyboard combinations such as Alt-Tab within a full Presentation Server desktop instead of requiring users to use an alternate combination such as Alt-+. This feature is supported on a number of different clients, including all of the Win32 clients and the latest ICA Client for Linux.

 PREV

NEXT 

# Web Connectivity to the MetaFrame Server Farm

Conceptually, the behavior of the Web Interface remains unchanged from MPS 3.0, but Citrix has introduced a number of new features that change how the Web Interface and the Program Neighborhood Agent are managed. The following list is a summary of the new web features in MPS 4.0. Where noted, we provide more detailed information on the specific feature:

- **Web Server Requirements** The web server requirements outlined in [Chapter 14](#) still apply with one addition. Prior to installing the Web Interface, you must first install the Access Suite Console. The installation MSI for this application can be found on the MPS 4.0 installation CD-ROM in the \Administration\Access Suite Console folder. After all of the prerequisites have been met, the Web Interface can be installed.
- **Web Interface Installation** The installation process has changed since MPS 3.0. Multiple different languages are now supported (German, English, Spanish, French, and Japanese). The installation now prompts only for the location of the client installation files. You are no longer prompted for any MetaFrame server information. All farm-related configuration is now done after the installation has completed.
- **The Web Interface, Program Neighborhood Agent, and the MetaFrame Access Suite Consoles** Management of the Web Interface and the Program Neighborhood Agent are no longer performed through their respective web-based consoles. They are now managed from within the Access Suite Console. We look at the features and functionality of the console later in this chapter.
- **Remote Configuration** Remote Configuration allows the Web Interface configuration file (WebInterface.conf) and/or the PN Agent configuration file (config.xml) to be stored in the farm's Data Store instead of locally on the web server if desired. We discuss Remote Configuration in more detail shortly.
- **Multiple Site Support** Multiple Presentation Server, PN Agent, and Conference Manager sites can co-exist on the same Web Interface server. The Access Suite Console makes it easy to manage all of the required tasks for these sites.
- **Web Interface Site Grouping** Sites from multiple Web Interface servers can be logically grouped and managed as a single entity, all sharing the same common Web Interface configuration file. When this file is updated within the Access Suite Console, all load-balanced sites in the group are automatically updated.
- **Web Interface Customization Wizard** The general appearance of the Web Interface can easily be modified without requiring any Web coding. A simple wizard allows you to change a number of site features such as text, logos, colors, and icons. We discuss this feature further when we review the new management features of the Web Interface.
- **UNIX Web Interface Support for RSA SecurID and Secure Computing SafeWord** for Citrix Both two-factor authentication configurations are supported via the RADIUS authentication protocol in UNIX. The Web Interface on Windows continues to provide native support for these products.
- **Novell NDS Authentication Support** NDS authentication is now supported directly via LDAP and no longer requires the Novell client to be installed on the Web Interface server. NDS

authentication is *not* available within the UNIX Web Interface.

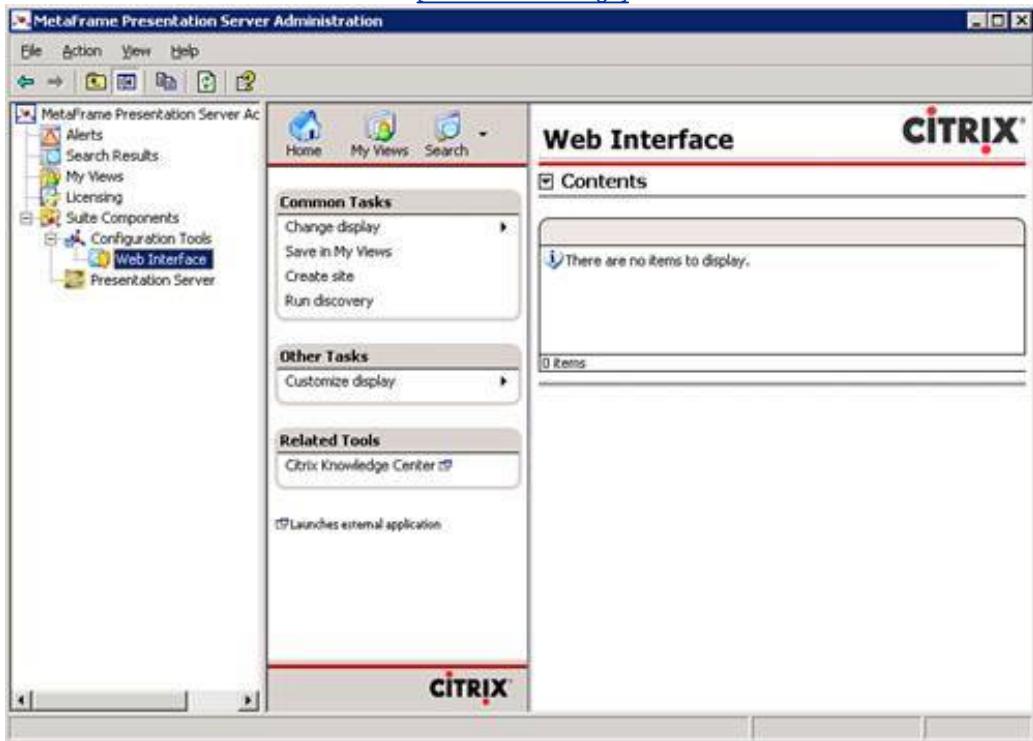
- Improved Error Reporting from the Citrix XML Service The Citrix XML Service on an MPS 4.0 server now returns the IMA error code to the Web Interface instead of the generic "Unspecified error" reported in previous versions of MPS.
- template.ica Replacement The template.ica file, which was used in previous versions of the Web Interface to generate specific ICA files for published application access, has been replaced in the MPS 4.0 Web Interface. Now, the specific ICA file sent to the client is generated completely from within the Web Interface Java classes. If the default output file must be modified, special ICA override files can be created. The Web Interface reads these files as it generates the ICA file for the published application. When a site is generated, the override files can be found in the <site root>/conf folder, the same location as the Web Interface configuration files.
- End-User Changes In addition to the changes that have been introduced to the Web Interface on the server-side, some improvements have also been made to the user interface and how the WI interacts with the user. The user-specific features are
  - Multiple Language Support The Web Interface provides built-in support for displaying information in any one of five languages (English, German, Spanish, French, or Japanese). The WI attempts to detect the web browser's locale and display the appropriate language. You can also select the desired language from within the interface.
  - Bandwidth Tuning The Web Interface now allows users to provide bandwidth information during logon, which in turn allows the WI to provide the appropriate tuning settings within the generated ICA file for the client.
  - User Interface Configuration Settings Users now can customize different aspects of the Web Interface display. An administrator controls the configurable areas through the Access Suite Management Console.
  - Java Client Fallback Support The Java client can now be configured to act as an automatic fallback client if a user connects to the Web Interface without having the proper Win32 client installed. With no Win32 client detected, the WI automatically delivers the Java client as a substitute.
- Secure Gateway Modifications MPS 4.0 introduces some modifications to the Secure Gateway configuration. See the "[Secure Gateway Configuration in an MPS 4.0 Environment](#)" section for more information.

## Managing the Web Interface with the Access Suite Console

Unlike the Web Interface in MPS 3.0, which was useable immediately after installation, the 4.0 Web Interface requires that you first create a site with the Access Suite Console (ASC). The first time you launch the ASC, it prompts you to discover the available products and components. This includes both the Web Interface and any associated Presentation Servers. Whereas the Presentation Server choice is optional, you must select the Web Interface option. After discovery has completed, you can select the Web Interface module (see [Figure 16.5](#)) and then select the Create Site task to begin creation of the first site.

Figure 16.5. You must create a new Web Interface site before you can begin to use the Web Interface.

[\[View full size image\]](#)



During the setup, you are given the choice of creating one of three site types:

- MetaFrame Presentation Server This site allows users to access the Presentation Server farm through the Web Interface.
- Program Neighborhood Agent Services This site allows the PN Agent client to connect and retrieve the config.xml file.
- Conferencing Manager Guest Attendee This site allows guest users to log in to Conference Manager.

You are then able to choose whether to make this the default page for the IIS site. You are also asked to choose either a local or central configuration file. Details on Remote Configuration are discussed in the next section of this chapter.

During the installation, you are prompted to provide both a reference name for the farm and the name of at least one Presentation Server within that farm that you want to make accessible through the Web Interface. After the site has been created, it appears as an object underneath the Web Interface icon in the Access Suite Console. When it is selected, you see the list of both the common and other tasks for the Presentation Server Web Interface site.

Quickly viewing the list of tasks, you will see that many of them are similar to those found within the Web Interface for MPS 3.0 (see [Chapter 14](#).) The interface and location of the settings have changed, but the most of the options that can be configured in the environment have not changed much at all. This list summarizes the tasks and their purpose:

- Manage Server Farms This task opens a dialog box that combines the settings found under Manage Farms and MetaFrame Servers in the MPS 3.0 Web Interface Console. From here, you

can add multiple server farms to the WI and assign the order in which applications are queried and change password attempts are processed.

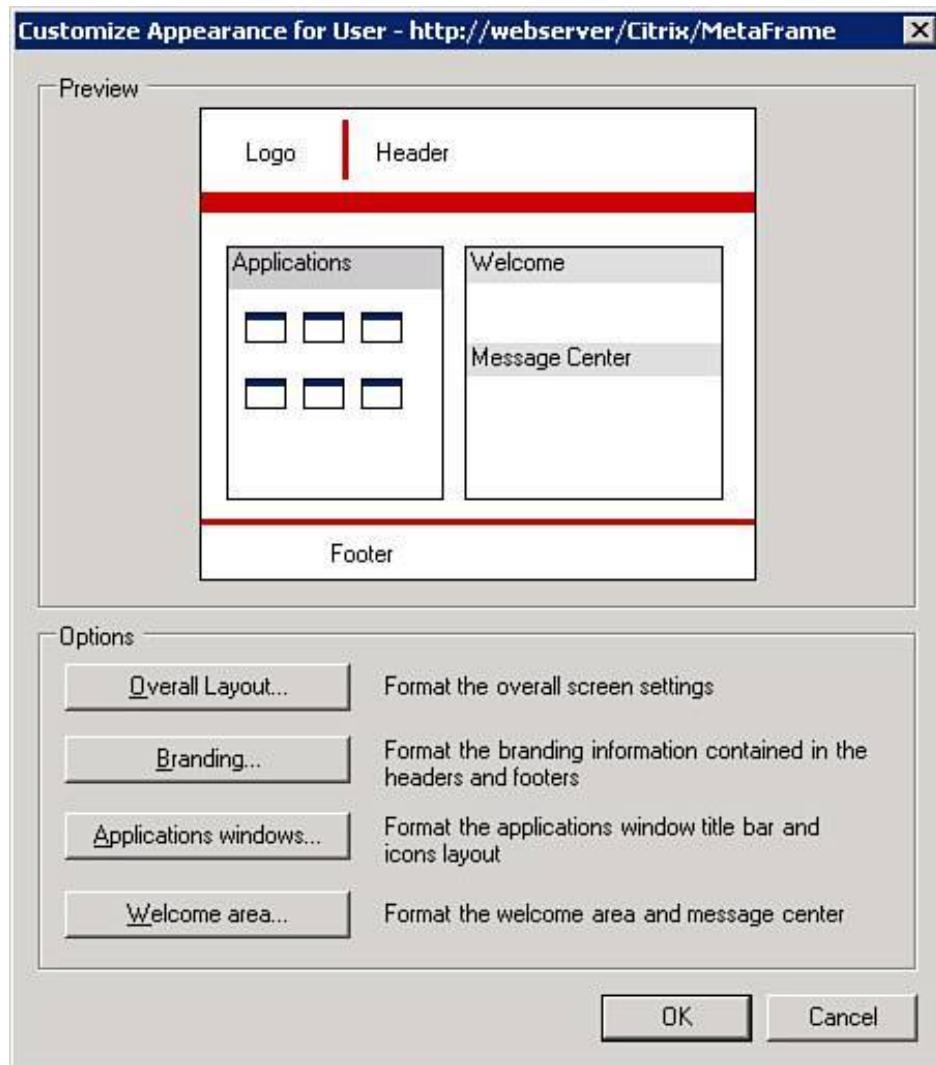
For each server farm, you also define the servers that the WI can contact to query application information. If load balancing is disabled, the order in which the servers are listed determines the failover order. Failed servers are bypassed for 60 minutes, a setting that you can edit. The transport type used to contact the XML service also remains the same. You still have three choices: HTTP, HTTPS, and SSL Relay.

The ICA Authentication Ticket setting found under the Authentication tab in MPS 3.0 has been moved here. Ticketing is enabled by default and still has a time to live (TTL) value of 200 seconds.

An Advanced button on this dialog box provides you with access to enable or disable the pooling of socket connections between the WI site and the XML service. Enabled by default, this option helps to improve performance but in rare circumstances may cause instability. Disabling this option improves stability but reduces performance. XML socket time and retry options can also be modified from here. Citrix does not recommend changing these default values. Socket pooling should be disabled when the WI is contacting one or more MetaFrame Presentation Server for UNIX servers.

- Configure Authentication Method The single Authentication setting in the WI for MPS 3.0 has been replaced with the Configure Authentication Methods Wizard. The Authentication methods are as follows:
  - Anonymous This setting is unchanged from 3.0.
  - Smart Card Smart Card authentication is now supported with MetaFrame Presentation Server for UNIX; otherwise, it is unchanged from MPS 3.0.
  - Pass-through This setting was called Single Sign-On in MPS 3.0. It now has the option to enable Kerberos authentication.
  - Pass-through with Smart Card Pass-through authentication support is also now available with Smart Cards.
  - Explicit As in MPS 3.0, you can enable two-factor authentication with either RSA SecurID or SafeWord. You can select Windows (or NIS on UNIX) or Novell NDS authentication on the next screen in the wizard. Domain and UPN customization options are available when you choose Windows. Similarly, context restrictions and contextless authentication options are available when you choose NDS.
- Customize Appearance for Users This new feature to MPS 4.0 allows an administrator to quickly and easily customize the appearance of the Web Interface without having to do any scripting or custom Web development. [Figure 16.6](#) shows the main customization dialog box. Four buttons allow you to customize various components of the WI:

**Figure 16.6.** MPS 4.0 allows you to easily customize the appearance of the Web Interface.



- Overall Layout Changes the overall layout of the Web page. Your choices are Auto, Compact, or Full Display; the default is Auto. Users can modify the overall layout, but this setting is not enabled by default.
- Branding Enables or disables display of headers or footers for the site. You can also change the general branding color from the default of red, specify a header and logo image source location, and make the corporate logo a hyperlink.
- Application Windows Dictates how the application icons are displayed for an authenticated user. The configurable options are background color and image, text color for the title bar, and the number of icons per row that are displayed. By default, the user can configure these settings.
- Welcome Area Allows you to create a welcome area for the environment. The default and additional language messages can be in English, French, Japanese, French, or German.
- Manage Secure Client Access Within this task, you define the appropriate security settings for your Web Interface environment. The four options listed here are equivalent to the similarly named settings in the MPS 3.0 Web Interface environment:
  - Edit DMZ Settings Here, you specify how the IP address of the MetaFrame server is presented to the end user. The options provided here are the same as those found in MPS

3.0 but have been organized to provide a more intuitive interface. The default option is still Direct, meaning that the client receives the real IP address of the MetaFrame server, and it is able to successfully connect to that address. You define the appropriate rules for each of the different networks from which users can connect to the environment. The order in which these rules are set dictates the order in which they are processed. For each of the access methods, there is also an equivalent Secure Gateway option that is defined when users are accessing the environment through the Secure Gateway.

- Edit Secure Gateway Settings When users access the Web Interface via the Secure Gateway, you provide the SG information on this screen. The FQDN to the Secure Gateway is defined here. Session reliability can be enabled, an option not available with MPS 3.0. One or more Secure Ticket Authorities are added here. Remember that the STA component is now integrated into the XML Service in MPS 4.0. Load-balancing and failover rules mimic those for the server farm and servers. STA servers now maintain their own failover time intervals.

## Alert

Session reliability support via the Secure Gateway is an important difference between the MPS 3.0 and MPS 4.0 Web Interfaces.

- Edit Address Translations Any address translation mappings are defined here for any defined client routes, Secure Gateway routes, or both. Multiple mapping entries can be maintained if desired. This consolidates the translation mappings that were managed independently in MPS 3.0.
- Display Settings These settings provide a visual display of the configured client access methods defined in the Edit DMZ Settings section. Unused settings appear grayed out.
- Manage Client Deployment This task launches the Client Deployment Wizard, which allows you to configure options similar to those found in the Client Deployment settings page in the MPS 3.0 Web Interface. The first screen prompts you to select the clients that will be available for installation. Local Client, Native Embedded Client, and Client for Java are enabled by default. Embedded Remote Desktop Connection is disabled by default.

The second dialog box contains settings that enable the automatic update of the Web client, whether the installation caption is displayed, and whether Unicode is supported. To support Unicode, you must select Support Version 8 or Later of the Clients. One new option on this screen is the ability to automatically fall back to the Java client if a native or embedded client is not detected. This can simplify user access when a local client is not available for use.

In the next dialog box, you can make any desired changes to the default Web client CAB file used for installation.

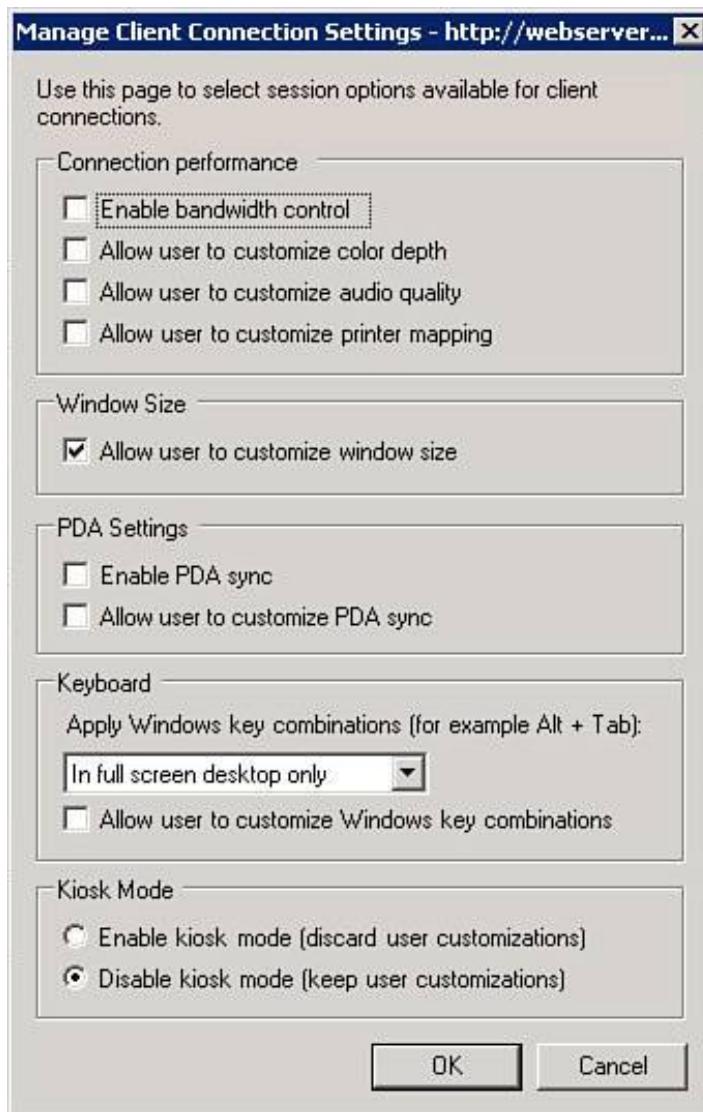
You then choose the Java packages that will be deployed with the client on the Client for Java dialog box. The fewer packages you select, the smaller the client download. Choose only those packages that are relevant to your environment. The packages available here are the same as those in the MPS 3.0 Web Interface, including the option to include a private root certificate with the Java package.

- Edit Client-side Proxy When a proxy server is employed on the client side of the Web Interface, you can define settings here that dictate whether the Presentation Server client must communicate through the proxy server when connecting to a MetaFrame server. These options

are the same as those found in the MPS 3.0 Web Interface console.

- Manage Client Connection Settings [Figure 16.7](#) shows the dialog box containing the client connection settings you can modify. These options have all been discussed either in the appropriate chapters of the book or earlier in this chapter when they pertain to MPS 4.0. For example, we reviewed the new client PDA device access and Windows key combination support earlier in this chapter. Most of these options have to do with whether a user has access to customize areas of the interface. One of the new options, Kiosk Mode, prevents users from saving any of their personal customizations.

Figure 16.7. By default, users have access to modify some of their personal Web Interface properties.



- Manage Workspace Control This task gives you access to configure the Workspace Control features for Web Interface users. All of the common settings related to Workspace Control are modified here. The requirements and usage of Workspace Control have not been modified since MPS 3.0.
- Control Diagnostic Logging Here, you can configure both diagnostic logging options for the

Web Interface as well as customize the URL used for error callback.

- Local Site Tasks Here, you manage general settings for the Web Interface site. You can modify the source of the configuration file for the site and modify the IIS hosting options, where you could specify the default page for the IIS site. You can also repair and uninstall a site.
- Import and Export Configuration This task enables you to export the configuration from one server and import it into another.

## Managing the Program Neighborhood Agent with the Access Suite Console

To create Program Neighborhood Agent configuration sites, choose the option Create Site and then select Program Neighborhood Agent Services. During the creation, you are requested to provide a server farm as well as at least one MetaFrame server within that farm. After these sites are created, you can create a new configuration file at the PN Agent site level or manage global options such as the server farms or client-side proxy settings.

When you select a specific configuration file, you then have access to configure the common features for the PN Agent environment. Many of these features are similar to those options already discussed for the Web Interface for Presentation Server, and much of this information is the same as that found within the old PN Agent Management Console. The available tasks for the PN Agent are

- Configure Authentication Methods Allows you to define the default authentication for the PN Agent clients. This task is almost identical to the Web Interface settings, with the exception of two-phase authentication.
- Change Session Options Opens a dialog box with three tabs. Here, you specify the desired session sizes, client resources (including color depth, Windows key combinations, and audio options), and the Workspace Control settings.
- Manage Application Shortcuts Provides access to all of the shortcut-related settings for the PN Agent. This includes shortcut creation on the desktop, the Start menu, and the notification area on the system tray. You also can access the shortcut removals option here, allowing you to dictate how shortcuts are deleted from the client device.
- Manage Server Settings Allows you to specify that SSL is to be used for client-to-site communications, whether the user can customize the server URL where the XML configuration file is read, and how the configuration is read from the file.
- Manage Application Refresh Specifies how often the application list for an authenticated user is retrieved from all configured farms. These settings are unchanged from MPS 3.0.
- Duplicate Client Configuration Duplicates the current configuration XML file, creating it with the same name with an *x* appended, where *x* is an integer that is incremented as necessary. For example, the file config.xml would be duplicated, and the new file would be called config\_1.xml.
- Export Client Configuration Allows you to export the file to whatever location you want and with whatever name you want.

## Remote Configuration

The Web Interface now supports a feature called Remote Configuration. This feature allows the Web

Interface for Presentation Server configuration file (WebInterface.conf) and/or the PN Agent configuration file (config.xml) to be stored in the farm's Data Store instead of locally on the Web Interface server. When configured to use a remote configuration file, the Web Interface retrieves the desired file from the Data Store (via an XML proxy called the Configuration Proxy, hosted either by IIS or the XML Service) when it starts up.

The Configuration Proxy communicates with a DCOM application called the Configuration Manager that is always installed with Presentation Server 4.0 but is activated only when it receives a request from a Web Interface server. The Access Suite Console loads a special .NET assembly to communicate with the Configuration Proxy. This assembly is called the Configuration Object Library (COL). To access the Configuration Proxy, the administrator running the Access Suite Console must be delegated a Presentation Server administrator with the access Log On to the Web Interface Console. With these permissions, the Configuration Manager can be successfully started on the Presentation Server, initiating the required communications to store and retrieve the remote configuration information.

## Alert

Only a server running MetaFrame Presentation Server 4.0 can act as a Web Interface Configuration Server.

Because Remote Configuration requires access privileges on the Presentation Server, you cannot use Remote Configuration on a Web Interface server configured in a workgroup or standalone server outside a Windows domain. This effectively limits the Remote Configuration feature to only those Web Interface environments that run the web servers as part of a domain that can interact with Presentation Servers in the same (or another) domain.

## Secure Gateway Configuration in an MPS 4.0 Environment

As we mentioned earlier, two of the major changes to the Secure Gateway with the latest Web Interface are

- Integration of the Secure Ticket Authority (STA) feature into the Citrix XML Service in MPS 4.0
- Support for Session Reliability in conjunction with the 9.x client and the latest Web Interface

Aside from these features, the Secure Gateway discussion in the "[Securing Server Access with the Secure Gateway](#)" section of [Chapter 14](#) remains unchanged. Diagrams showing the STA can now have that component rolled up and into the production Presentation Servers, or running on its own MPS 4.0 server that is not simultaneously processing user logons. References to the STA installation can be omitted, but other components are installed in the same order and have the same installation process.

Modifications to the Web Interface to support the Secure Gateway are now done through the Access Suite Console. See the earlier section on the Access Suite Console and the Web Interface Console for details on the Secure Gatewayrelated settings and where they are located.

## Exam Prep Questions

1. You are implementing solutions for IT initiatives to cut costs and improve performance through server consolidation. You also want to increase the number of users who are supported on each server and are determining whether to enable CPU utilization management. Under what circumstances would it not be advisable to enable CPU utilization management for all users?

- A. When user demand exceeds available CPU resources and causes farm performance to degrade

- B. When the server allocates an equal share of the CPU to each user

- C. On farms or servers that host CPU-intensive applications that may require a user to have a share of the CPU greater than that allocated to fellow users

- D. For individual servers within the farm

A1: Answer C is correct. CPU utilization management allocates an equal share of the CPU to each user. If you have special users who require a greater share of the CPU, either you must not enable CPU optimization on these farms or servers, or you must explicitly allocate these users a greater share of CPU resources. Depending on the needs of the application, this may produce undesirable performance restrictions on these users.

Answers A, B, and D are all incorrect. Answers A and B are both good reasons to enable CPU utilization, and D is not a reason not to enable this option.

2. An application fails to run properly after you upgrade a server to Presentation Server 4.0. The Virtual Memory Optimization feature is enabled. You notice the following behavior: The application was working properly in Presentation Server 3.0. The application works properly when the IMA Service is stopped. The application fails at the server console when the IMA Service is running. What should you do to get the application to run?

- A. Nothing. The application is incompatible with Presentation Server 4.0.
  - B. Disable the Virtual Memory Optimization feature.
  - C. Stop the IMA service.
  - D. Add the application to the exclusion list.
- A2: Answer D is correct. If an application is not functioning correctly after being optimized by the Virtual Memory Optimization feature, it can be placed on the application exclusion list. The exclusion list is located in the Presentation Server Console under the farm properties in the Memory Optimization section.
- Answers A, B, and C are incorrect. The application is simply not compatible with the new memory optimization feature of MPS 4.0. Although disabling Virtual Memory Optimization will correct the problem, it will eliminate any benefits that could be gained from the optimization performed with other applications. Stopping the IMA service is not an option because it will impair the behavior of the Presentation Server in the farm.

3. When the Citrix Virtual Memory Optimization service is started, it is responsible for monitoring applications as they load and recording any DLL access collisions that occur. These collisions are recorded to what file? (Choose one.)

- A. Collisions.SFO
- B. Repair.SFO
- C. Bind####.SFO
- D. VMem.SFO
- E. Exclude.SFO

A3: Answer B is correct. Collisions are recorded in the Repair.SFO file, which is then read at scheduled intervals and during bootup in order to optimize the conflicting programs.

Answers A, D, and E are incorrect because they represent files that are not part of the Virtual Memory Optimization feature. Answer C is incorrect because the Bind####.SFO file contains the list of optimized DLLs and their associated memory savings.

4. Where is the list of processes and components excluded from memory optimization managed? (Choose all that apply.)

A. In the server farm node

B. In the server node

C. In the published application node

D. In the Registry

A4: Answers A and D are correct. The list of processes and components to exclude from memory optimization is managed only within the server farm node and within the Registry. Citrix recommends that all changes be made in the farm node and not directly in the Registry.

Answers B and C are incorrect. You can enable or disable memory optimization in the server node, but you cannot modify the individual applications that are excluded. The published application node contains no memory optimization settings.

5. You are customizing options for the Web Interface for a Presentation Server installation in a medical clinic. Users frequently need to move between a variety of client devices and quickly disconnect and reconnect running applications. You have just upgraded from a legacy MetaFrame 1.8 environment to a completely new MPS 4.0 environment and have set up Workspace Control. However, it is not working. What should you do?

- A. Turn off interoperability mode.
- B. Upgrade all ICA clients to version 8 or higher.
- C. Implement SmoothRoaming with Smart Cards.
- D. Configure connection settings in the Presentation Server Console.

A5: Answer B is correct. Workspace Control cannot be used with the ICA Client for Windows CE, the Win32 client prior to version 8, and Remote Desktop Connection software. Additionally, this feature works only with servers running MetaFrame Presentation Server version 3.0 or later.

Answer A is incorrect because interoperability mode does not even exist in MPS 4.0. Answers C and D are also incorrect because SmoothRoaming with Smart Cards is not a requirement for Workspace Control.

6. Many of the users in your organization have PDAs. You want to use the new PDA synchronization support feature in MetaFrame Presentation Server. Which of the following statements about PDA synchronization support are true? (Choose all that apply.)

- A. ActiveSync must be used as the synchronization agent.
- B. It does not work for pass-through ICA connections and reconnection to disconnected sessions.
- C. It is supported in all editions of Presentation Server 4.0.
- D. It offers full Plug and Play (PnP) support for USB-tethered Windows CEbased PDAs.
- E. All of the features of ActiveSync are supported.

A6: Answers A, D, and E are correct. PDA synchronization requires that ActiveSync be used as the synchronization agent, and all of the features of ActiveSync are supported. It offers full Plug and Play (PnP) support for USB-tethered Windows CEbased PDAs.

Answer B is incorrect. The restrictions on pass-through ICA connection support and reconnecting to disconnected sessions are limitations of local IP address redirection, not PDA synchronization. Answer C is incorrect because PDA synchronization is available only in the Advanced and Enterprise Editions of MetaFrame Presentation Server.

7. Which of the following statements concerning new features and changes in MetaFrame Presentation Server 4.0 is NOT true?

A. UNIX and Windows licenses can now be shared in the Enterprise Edition.

B. MetaFrame 1.8 interoperability mode is now supported.

C. MPS 4.0 now includes UNIX Presentation Server.

D. Conferencing Manager is now included as a component of Presentation Server.

A7: Answer B is correct. MetaFrame 1.8 interoperability mode is no longer supported in 4.0.

Answers A, C, and D are all true statements about MPS 4.0.

8. Certain users in your organization have locally attached scanners. You want these devices to be transparently redirected so that they can be controlled and accessed from applications running on the Presentation Server. What should you do?

A. Enable Windows key pass-through.

B. Enable Workspace Control.

C. Enable TWAIN redirection.

D. Enable application isolation.

A8: Answer C is correct. TWAIN redirection enables you to transparently redirect locally attached imaging devices, such as scanners, from the client to the server. Users can thus control client-attached imaging devices from applications that run on the server. The application can detect and use the imaging device from within the session, just like a client-based application.

Answers A, B, and D are incorrect. None of these features are associated with the redirection of local client devices such as scanners.

9.

You want to run an application on your Presentation Server that requires a unique IP address for each user. You have assigned a total of 10 IP addresses because you have only 10 users who run this application. Occasionally, you get phone calls from these users saying they are receiving a message stating that an IP address is not available. When this happens, the users cannot run their application. What is the most likely cause of this issue? (Choose one.)

A. A user is disconnecting and reconnecting from a different workstation, consuming additional licenses.

B. The application is crashing and not freeing up a virtual IP address.

C. The application does not support the use of virtual IP addresses.

D. More than 10 users are connecting to the server.

E. A and B.

- A9: Answer D is correct. Each user who connects to a server with virtual IP addressing enabled will receive a virtual IP address from the pool, regardless of whether that user actually uses an application that requires that address. If all available IP addresses are exhausted, users will receive a message stating that no more addresses are available for use.

Answers A, B, C, and E are all incorrect. Virtual IP address assignment is not affected by disconnecting and reconnecting (you keep the same IP). Because the IP is associated with the session, the application crashing has no effect on this. Even if an application does not support the use of virtual IP addresses, it does not cause this error to occur.

10. Many of the users in your organization have PDAs. You want to use the new PDA synchronization support feature in MetaFrame Presentation Server. How do you enable PDA synchronization?

A. Enable the rule Client Devices/Resources/PDA Devices/Turn on automatic virtual COM port mapping.

B. Disable the rule Client Devices/Resources/PDA Devices/Turn on automatic virtual COM port mapping.

C. Enable the rule Client Devices/Resources/Ports/Turn off COM ports (or set it to Not Configured).

D. Disable the rule Client Devices/Resources/Ports/Turn off COM ports (or set it to Not Configured).

E. B and C

F. A and D

- A10: Answer F is correct. To enable PDA synchronization, you need to configure a policy. The PDA Devices policy rule is disabled by default.

Answer A alone is incorrect because PDA devices do not connect if the COM port redirection has been turned off.

Answer B is incorrect because you want to enable this rule, not disable it.

Answers C and D are incorrect on their own because enabling or disabling the COM port option does not enable PDA redirection unless the PDA Devices rule is also enabled properly.

Answer E is incorrect because it does not set the proper policies correctly.

 PREV

NEXT 

# 17. Practice Exam 1

You've now reached that point where it is time to put all the knowledge you've learned to the test. This is the first of two practice exams (additional exams and study content can be found on the accompanying CD-ROM) that will test you on a wide variety of the topics covered in this book. We suggest that you write your answers on a separate sheet of paper so that you can quickly compare them to the answers, which are listed in [Chapter 18](#). This will also make it easier to go back and work through the exam again without having slightly faded pencil marks reminding you of what you chose last time. We also recommend that you work through all the questions in this exam, review the areas where you may be weak, and then take the second exam in [Chapter 19](#). Make sure you note carefully the areas where you may need to study further. Avoid the temptation to simply repeat the exam a couple of times, memorizing the answers to these questions. Repeat the exams enough and you'll eventually get 100%, but that won't help you nearly as much as properly reviewing the material and scoring 90%+ on the second (or maybe even the first) time through. After you've worked through these practice exams a couple of times, you'll be ready to move on to the test exams available on the accompanying CD-ROM.

Have fun and good luck!

## Practice Exam

1. Choose the two types of content redirection supported with Presentation Server.

A. Server-to-client

B. Server-to-application

C. Application-to-server

D. Client-to-server

2. As a Citrix administrator, you want to configure the AutoLogon feature for all ICA connections. Where would you do that in the Citrix Connection Configuration tool?

A. AutoLogon Settings tab

B. Client Settings

C. Advanced Connection Settings

D. ICA Settings

3. In Resource Manager, metrics can be directly written by a Presentation Server to what location(s)? (Choose all that apply.)

- A. Summary database
  - B. Local Host Cache
  - C. Event log
  - D. Local temporary summary files
  - E. Zone data collector
4. As a Citrix administrator, you can use which feature of the Printer Management node to make sure only certain printer drivers can be used for printing in your environment?
- A. Driver Compatibility
  - B. Auto-Replication
  - C. Printer Driver Security
  - D. Driver Mapping
5. Which of the following information is stored in the Data Store database? (Choose all that apply.)

- A. MetaFrame Administrators
  - B. Trust Relationships
  - C. Printer Configuration
  - D. Farm configuration information
  - E. Server configuration information
  - F. Published Application information
6. Each zone in a farm contains one server that is designated as the zone data collector. From the following list, choose only the information that is stored within the zone data collector. (Choose all that apply.)
- A. All available published applications
  - B. The real-time farmwide application metric information
  - C. The current server loads
  - D. A list of the active user sessions
  - E. A backup copy of the total license count for the farm
7. From the following list, choose the database that contains a portion of the information

found in the Data Store database.

- A. MF20.DSN
- B. Local Host Cache
- C. Management Console for MetaFrame Presentation Server
- D. Local Database Cache
- E. Summary database

8. As a Citrix administrator, you can use the Citrix Connection Configuration tool to perform which of the following tasks? (Choose all that apply.)

- A. Configure advanced ICA protocol settings
- B. Configure client settings
- C. Set security permissions on the ICA protocol
- D. Modify user group memberships
- E. Enable and disable ICA connections
- F. Configure ICA settings

9. How would you rename a zone after the installation of MetaFrame Presentation Server?

- A. In the Presentation Server Console, right-click the farm node, choose Properties, and then select Zones. Select the zone to rename and click Rename Zone.

- B. In the Presentation Server Console, expand the server farm node, expand the Zones folder, right-click the zone to rename and select Rename Zone from the menu.

- C. A zone can't be renamed after the installation of MPS. If you must rename a zone, you need to reinstall MPS.

- D. In the Presentation Server Console, expand the Zones node, right-click the zone to rename, and select Rename Zone from the menu.

10. As a Citrix administrator, you can apply Citrix policies to which of the following? (Choose three.)

- A. Client IP addresses

- B. Windows users and groups

- C. Servers

- D. Novell users

- E. UNIX users

11. The default load evaluator reports a full user session load when the server exceeds what number of users?

A. 1,000

B. 100

C. 10,000

D. 99

12. Which of the following are truthful statements about Citrix Presentation Server when it is installed on Windows Server 2003? (Choose all that apply.)

A. It supports only TCP/IP-based user connections.

B. The Terminal Services Licensing service must be installed on the same server as the Citrix data store.

C. Unless the Terminal Services component is installed on the Windows Server 2003 server, only a maximum of two Presentation Server clients can be concurrently connected to the server at one time.

D. The Restrict Each User to One Session feature is enabled by default.

E. Users must be members of the Remote Desktop Users group to be able to connect through Terminal Services.

13. As a Citrix administrator, you are able to generate which two types of reports from the License Management Console?

- A. Summary Report
  - B. Usage Report
  - C. License Report
  - D. Product Report
14. MetaFrame Presentation Server does not allow you to share License Servers across multiple server farms.
- A. True
  - B. False
15. The Web Interface supports which of the following authentication methods? (Choose all that apply.)
- A. SmartCard
  - B. Explicit Logon
  - C. Anonymous Login
  - D. Finger Printer authentication

E. SmartCard with Single Sign-on

F. Single Sign-on

G. Basic Authentication

16. When multiple load evaluators are configured to a server and its published applications, which load evaluator determines the server load?

A. The load evaluator with the lowest load

B. The load evaluator assigned to the server

C. The load evaluator with the highest load

D. The load evaluator assigned to the application

17. Which of the following are not supported database types for the Data Store? (Choose all that apply.)



A. IBM DB2



B. Microsoft SQL Server Desktop Engine (MSDE)



C. Microsoft SQL Server



D. Sybase Adaptive Server Enterprise



E. Oracle



F. Microsoft Access

**18.** How would you, as a Citrix administrator, configure the election preference of a data collector?



A. In the Presentation Server Console, right-click the Servers node and select Properties. In the left pane, select Zones. Then in the right pane, choose the desired server and then select the election preference for that server.



B. In the Presentation Server Console, right-click the Zones node and select Properties. In the left pane, choose Election Preferences, and then in the right pane, highlight the server you want to configure and set the election preference for that server.



C. In the Presentation Server Console, expand the Zones node, right-click the server, and select Properties. In left pane, choose Election Preference, and then in the right pane, set as desired for the server.



D. In the Presentation Server Console, right-click the Farm node and select Properties. In the left pane, select Zones, and then in the right pane, highlight the desired server and click the Set Election Preference button. Set election

preferences as desired.

19. Choose the load rules that make up the Advanced Load Evaluator. (Choose three.)

A. CPU

B. Application User Load

C. Server User Load

D. Bandwidth

E. Page Swap

F. Disk I/O

G. Memory

20. From the following list, choose all answers that describe a function of the Citrix XML Service.

- A. Passes user credentials from the client to the server
  - B. Supplies the Web Interface and Program Neighborhood with the list of published applications available in the server farm
  - C. Supplies the ICA Client device the names of the Citrix servers that are available
  - D. Manages ICA session reliability and stability
21. How could you, as a Citrix administrator, go about changing the settings of a published application? (Choose all that apply.)
- A. In the Presentation Server Console, expand the Applications node, right-click a published application, and choose Properties.
  - B. In the Presentation Server Console, expand the Servers node, right-click on a server, and choose Properties. In the left pane, choose Published Applications, right-click the desired published application, and then choose Properties.
  - C. In the Access Suite Console, expand the Servers node, right-click on a server, and choose Properties. In the left pane, choose Published Applications.
  - D. In the Access Suite Console, expand the Applications node, right-click a published application, and choose Properties.
22. Which TCP port is used for server-to-server IMA communication in MPS?

A. 1494

B. 2513

C. 1604

D. 80

E. 2512

F. 443

23. Which of the following are components of the Access Suite Licensing server? (Choose all that apply.)

A. License file

B. MyCitrix.com website

C. Terminal Services Licensing Service

D. License Management Console

E. Citrix Licensing service

24. As a Citrix administrator, you can use which of the following tools to create a new update database?

- A. ICA Client Distribution Wizard
- B. ICA Client Creator
- C. ICA Client Update Configuration
- D. ICA Client Update Database

25. Citrix Installation Manager supports which three package types?

- A. .EXE
- B. .ADF
- C. .MST
- D. .MSI
- E. .MSP

26. What are the two methods by which a Citrix administrator can place an MPS server into install mode?

- A. Change Mode /Install
  - B. Change User /Install
  - C. Add/Remove Programs in Control Panel
  - D. Change Logon /Install
27. As a Citrix administrator, you can configure Resource Manager to send you alerts by which of the following methods? (Choose three.)
- A. SMS to a mobile phone
  - B. Microsoft Active Directory
  - C. Email
  - D. SNMP
  - E. Messenger Service
28. Select the load rule that would limit the number of users allowed to connect to a published application.

- A. Server User Load
- 
- B. Connections Load
- 
- C. Published Application Load
- 
- D. Application User Load
- 
- E. Application Server Load

29. What is the default ICA Keep-Alive time-out value?

- A. 30 seconds
- 
- B. 60 seconds
- 
- C. 90 seconds
- 
- D. 120 seconds
- 
- E. 180 seconds

30. Where would you, as a Citrix administrator, configure the database connection server and the summary database for Resource Manager to work properly?

- A. Presentation Server Console
  - B. Access Suite Console
  - C. Data Sources in Administrative Tools
  - D. Citrix Connection Configuration
  - E. Resource Manager Console
31. Where would you, as a Citrix administrator, go about enabling or disabling SpeedScreen Browser Acceleration, SpeedScreen Flash Acceleration, and SpeedScreen Multimedia Acceleration?
- A. Using the SpeedScreen Latency Reduction Manager
  - B. In the Presentation Server Console, right-click the Farm node and choose Properties
  - C. In the Advanced button in Citrix Connection Configuration
  - D. Via MetaFrame Presentation Server policies
32. What are the three privileges that can be granted to a new MetaFrame Administrator account?

A. View only

B. Servers only

C. Full administration

D. Published applications only

E. Server Operator

F. Modify

G. Custom

33. Where is the printer drivers' information stored?

A. System32 directory in Windows

B. Local Host Cache

C. Data Collector

D. Data Store

E. Member Server

34. Which of the following situations is ideal for server-to-client content redirection?

- A. A user clicks a URL link from an email message within Outlook, which is running as a published application.

- B. A user clicks a URL from a web page using Internet Explorer on the local machine.

- C. A user double-clicks a Microsoft Word document on his or her local machine.

- D. A user saves an attachment from an email message using Mozilla Thunderbird as a published application.

35. How long do Citrix Policy rules remain in effect?

- A. As long as the policy is available

- B. As long as the ICA session is active

- C. Until the Citrix administrator disables it

- D. Until the MPS server restarts

36. Choose the statement that best describes the pass-through client.

- A. An instance of Program Neighborhood or Program Neighborhood Agent running as a published application on a Presentation Server. Non-Win32 clients can then access the features available in these clients that are not available with their native ICA client. Users get the benefits of PN or PN Agent without even having it installed locally on their client device.
- B. A component of the Secure Gateway for Presentation Server. The pass-through client seamlessly brokers ICA traffic between the client and the server through the gateway. Communications are fully secured, using industry-standard SSL/TLS technology. The Secure Gateway can be implemented without the pass-through client, but traffic is secured only through ICA encryption.
- C. Another term for the Win32 Web client, the pass-through client passes ICA traffic via standard HTTP to and from the Presentation Server. Published content appears seamlessly within the web browser. The pass-through client allows ICA traffic to traverse over the standard HTTP port 80, ensuring it will not be blocked by most firewalls and routers.
- D. A Presentation Server client that has been configured to pass the user's local credentials through to the MetaFrame server to automatically log the user on to the server. This reduces the number of times a user must enter a password, improving his or her computing experience.

37. Which tool would you, as a Citrix administrator, use to create ICA connections for different transport protocols?

- A. My Network Places
- B. Presentation Server Console
- C. Citrix Server Administration
- D. Citrix Connection Configuration

38. How would you, as a Citrix administrator, create reports of a farm's performance using the Access Suite Console?

A. Dashboard

B. Performance Monitor

C. Resource Monitor

D. Event Viewer

E. Report Center

39. You have restricted the ability for users to install printer drivers on all of the MetaFrame servers in your farm. To ensure users have no issues printing, you have also created a common set of printer drivers that you want to ensure are available across all servers in the farm. How would you go about ensuring that these printers are available on all of your Presentation Servers?

A. Enable the Universal Print Driver on each server.

B. Enable Printer Driver Mapping and configure all servers to share a common mapping.

C. Use Printer Driver Replication to deploy the drivers to all servers.

D. Use the Printer Driver Compatibility List to define all of the servers that will receive a copy of the printer drivers.

40. On which layer of the OSI model would you place the ICA protocol?

A. Session layer

B. Transport layer

C. Application layer

D. Presentation layer

E. Network layer

 PREV

NEXT 

 PREV

NEXT 

# 18. Answer Key 1

[Answer Key](#)

 PREV

NEXT 

# Answer Key

1. A, D

2. C

3. D

4. A

5. A, B, C, D, E,  
F

6. A, C, E

7. B

8. A, B, C, E, F

9. A

10. A, B, C

11. B

12. A, D, E

13. A, D

14. B

15. A, B, C, E, F

16. C

17. D

18. D

19. A, E, G

20. B, C

21. A

22. E

23. A, D, E

24. C

25. B, D, E

26. B, C

27. A, C, D

28. D

29. B

30. A

31. B

32. A, C, G

33. D

34. A

35. B

36. A

37. D

38. E

39. C

40. D

## Question 1

Answers A and D are correct. The two types of supported content redirection are client-to-server and server-to-client. These refer to the direction in which applications and content can be accessed. Client-to-server content redirection is supported only with the Program Neighborhood Agent Win32 client and requires the Advanced or Enterprise Editions of Presentation Server. This type of redirection opens local files that are associated with published applications running in the farm. Server-to-client content redirection refers to the opening of URLs encountered within applications running on a Presentation Server and redirecting the opening of those URLs to a local web browser or multimedia player running on the local client device. Server-to-client redirection is supported only with the Win32 and Linux clients for Presentation Server. Answers B and C are incorrect because these redirection types do not exist.

## Question 2

Answer C is correct. You would click the Advanced button of the Citrix Connection Configuration (CCC) tool and configure the AutoLogon settings within the Advanced Connection Settings dialog box. Settings here affect all users who connect using the configured network protocol.

Answer A is incorrect because there is no such option within the Connection Configuration tool.

Answers B and D are incorrect because even though they are valid CCC tool properties, they do not contain the Autologon options.

## Question 3

Answer D is correct. On an hourly basis, a Presentation Server writes summary information to local temporary Summary Database files. Once per day, this information is collected by the Database Connection Server for storage in the Summary Database.

Answer A is incorrect because the only source that can write information directly into the datastore is the Database Connection Server. No Presentation Server is able to directly write metric information into the Summary Database. Answers B and C are incorrect simply because Resource Manager does not write information to either of these locations. The Local Host Cache is used to maintain a subset of the data found in the server farm's Data Store. Resource Manager metrics are not maintained here. The same goes for the Event log. This is a source for event information, not for data storage.

Answer E is also incorrect. The Presentation Server communicates with the zone data collector to continuously send updates to the Farm Metric Server, but it does not write metric information to the zone data collector.

## Question 4

Answer A is correct. The Driver Compatibility list is the place where you would allow the use of certain print drivers or would deny the use of certain print drivers in your environment.

Answer B is incorrect because auto-replication controls the replication of drivers from one server to another. It does not restrict the use of additional drivers on one or more servers. Answer C is incorrect because this option does not exist, and D is incorrect because Driver Mapping dictates an alternate driver when a particular client driver is encountered. Using driver mapping, you could reduce the likelihood of a bad printer driver being used, but this option alone does not eliminate the chances of this happening.

## Question 5

Answers A through F are correct. MetaFrame Administrators, Trust Relationship, Printer Configuration, Farm configuration information, Server configuration, and Published application configuration are all examples of information that is stored in the Data Store. The Trust Relationships information is added to the Data Store by each server in the farm during the trust query cycle. All trusted domains are recorded for each server and are available to any requesting server in the farm. Access to this trust list is requested by an application that has been selected to perform an operation on a server that it does not trust. An attempt is made to contact a Presentation Server that has an existing trust relationship with the target and to use that to complete the desired operation.

## Question 6

Answers A, C, and E are correct. The zone data collector maintains real-time information for all servers in the zone, providing quick access to information, such as what server currently has the least load for a given published application.

Answer B is incorrect. Real-time farmwide application metric information is stored in the Farm Metric

server. The zone data collector stores only the name of the Farm Metric server. Even if both functions are combined on one server, the ZDC does not directly maintain such information.

Answer E is incorrect. A backup copy of the full license count for the farm is maintained on each MetaFrame server, not the zone data collector.

## Question 7

Answer B is correct. The Local Host Cache is the database that resides on every MPS server and that contains a portion of the Data Store that would allow the server to function in the event that the Data Store should go down for any reason.

Answer A is incorrect. The MF20.DSN is the data source file containing connection information for the Data Store. If the MetaFrame server has a local data source or is accessing a DBMS such as SQL Server, this file is populated with the necessary information. If the server is connecting indirectly through another server, this file is ignored.

Answer C is incorrect. The Management Console contains no data itself. It is used only to manage the environment. Answer D is not a real database, so this answer too is incorrect. Answer E is incorrect because the Summary Database contains only historical Resource Manager metric information. It contains no Data Store information.

## Question 8

Answers A, B, C, E, and F are correct. The Citrix Connection Configuration tool allows you to enable/disable logons, configure client settings, set security permissions on the ICA protocol, configure advanced ICA protocol settings, and configure ICA settings. Answer D is incorrect because you can't modify user group memberships from this tool.

## Question 9

Answer A is correct. To rename a zone after the installation of MPS, in the Presentation Server Console, right-click the farm node, choose Properties, and select Zones. Select the zone to rename and click Rename Zone.

Answers B, C, and D are all incorrect because the options described do not exist in the Management Console for Presentation Server.

## Question 10

Answers A, B, and C are correct. Citrix policies can be applied to client IP addresses, Windows users and groups, and servers. Answers D and E are incorrect because you can't apply Citrix policies to UNIX users or Novell users.

## Question 11

Answer B is correct. The MPS server will report a full user load when the number of users is 100. Answers A, C, and D are incorrect because they do not reflect the default value at which the server will

report a full load.

## Question 12

Answers A, D, and E are correct. Windows Server 2003 supports Terminal Services (and hence Presentation Server) connections only via TCP/IP. Users are also restricted to one session by default. This setting can be modified within Terminal Services Configuration. Users must also belong to the local Remote Desktop Users group; otherwise, they cannot log on to the server using either Terminal Services or Presentation Server. Administrators are not restricted by this feature.

Answers B and C are incorrect. The Terminal Services Licensing service is a component of Terminal Services and is completely independent from Presentation Server. Presentation Server does not even install on Windows Server 2003 or Windows 2000 Server unless the Terminal Services component has been installed (application server mode in Windows 2000). Terminal Services Remote Administration is not a valid operating environment for Presentation Server.

## Question 13

Answers A and D are correct. The two types of reports an administrator can generate using the License Management Console are a Summary Report and a Product Report. A Summary Report compares license usage across all products, and a Product Report is specific to a product type.

Answers B and C are incorrect. There is neither a Usage nor a License report available in MetaFrame Access Suite Licensing. Don't confuse Usage Report with the Usage Logs option within the Historical Usage screen. Using the Usage Logs option, you select the desired usage log file from which to generate Summary Reports or Product Reports.

## Question 14

Answer B is correct. You can share a license server among more than one server farm provided that you point both server farms to the same license server.

## Question 15

Answers A, B, C, E, and F are correct. The Web Interface supports authentication via SmartCard, Explicit Logon, Anonymous Login, SmartCard with Single Sign-on, and Single Sign-on. Answers D and G are incorrect because the Web Interface does not support either of these authentication methods.

## Question 16

Answer C is correct. The load evaluator with the highest load is used to determine the current load, regardless of whether it is a server or an application. The total load for an evaluator is determined by the rules within the evaluator. When all rules in an evaluator report full load or exceed their defined threshold, the server is removed from the list of available servers.

Answers A, B, and D are incorrect because they do not represent the correct load evaluator calculation for Load Manager.

## **Question 17**

Answer D is correct. Sybase Adaptive Server Enterprise is the only database management system listed that Citrix does not support as a possible source for the server farm Data Store.

Answers A, B, C, E, and F all represent databases supported by Citrix to host the Data Store.

## **Question 18**

Answer D is correct. To manipulate the election criteria of a Data Collector, you launch the Presentation Server Console, right-click the Farm node, and select Properties. In the left pane, select Zones, and then in the right pane, select the desired server and click the Set Election Preference button to configure the settings for that server. Answers A, B, and C are incorrect because they do not provide the proper location to edit the election preference of a zone. No Zones property exists for the Servers node. There is also no Zones node in the Presentation Server Management console.

## **Question 19**

Answers A, E, and G are correct. The rules that make up the advanced load evaluator are the CPU, the memory, and the page swap. Answers B, C, D, and F are incorrect because they do not make up the default rules available in the advanced load evaluator.

## **Question 20**

Answers B and C are correct. The Citrix XML Service is responsible for supplying the Web Interface and Program Neighborhood with the list of published applications available in the server farm for a given user account. The Citrix XML Service also provides the ICA Client with a list of servers or published applications if a client such as the Program Neighborhood or ICA Client for Linux has been configured to use HTTP or HTTPS browsing.

Answers A and D are incorrect. Credentials are not passed directly from the client to a server using the XML Service. Credentials may be provided via the Web Interface, but ICA clients never transmit this information through the XML Service. The XML Service is also not responsible for ICA session reliability and stability. Session reliability is handled directly by the IMA service when ICA traffic is tunneled inside the session reliability protocol on port 2598. This ICA traffic tunneling is performed automatically when the Presentation Server has session reliability enabled and a client that supports session reliability attempts to connect to the server.

## **Question 21**

Answer A is correct. The correct method to edit a published application's properties is to launch the Presentation Server Console, expand the Applications node, right-click on the application in question, and go to Properties. Answers B, C, and D are incorrect because they are not the proper way to edit a published application's properties.

## **Question 22**

Answer E is correct. The correct TCP port for server-to-server IMA communication between MPS servers is TCP port 2512. Answers A, B, C, D, and F are all incorrect. Port 1494 is used for client-to-server ICA communications when not using session reliability. Port 2513 is reserved for Management ConsoletoIMA server communications. Port 1604 provides legacy support for broadcast (when configured) or directed UDP requests from legacy clients. Port 80 is the common listening port for the Citrix XML Service, and port 443 is the listening port for the SSL Relay Service.

## Question 23

Answers A, D, and E are correct. License files contain the encoded licensing information that the License Server uses to verify the product and concurrent user count for which you are authorized. The License Management Console is the main management tool for the license server, and the Citrix Licensing service is one of the services that runs on the license server, providing Access Suite Licensing capabilities.

Answers B and C are incorrect. The MyCitrix.com website is the place where you retrieve license files, but it is not integrated into the Access Suite Licensing server. Although Terminal Server Client Access Licenses are required for user access, they are not integrated in any way with the Citrix Licensing server.

## Question 24

Answer C is correct. The ICA Client Update Configuration is the tool that a Citrix administrator would use to create a new update database. Answers A, B, and D are incorrect. The ICA Client Distribution Wizard can be used to update the client images in an existing update database, but it cannot be used to create a new database. The ICA Client Creator, a tool found on Windows 2000 Servers, allows you to create installation diskettes for common clients. There is no such tool called the ICA Client Update Database.

## Question 25

Answers B, D, and E are correct. Citrix Installation Manager uses three kinds of packages: .ADF, .MSP, and .MSI. Answers A and C are incorrect because they are unsupported file types.

## Question 26

Answers B and C are correct. The two methods by which an MPS server can be placed into install mode are Change User /Install and Add/Remove Programs in Control Panel. Answers A and D are incorrect. Neither answer represents a valid Terminal Server command.

## Question 27

Answers A, C, and D are correct. The three methods by which an administrator can be notified of Resource Manager alerts are email, SMS, and SNMP. Answers B and E are incorrect because they are not communications means supported by Resource Manager.

## **Question 28**

Answer D is correct. The load evaluator that would limit the number of users connecting to a published application is Application User Load. Answers A, B, C, and E are incorrect because they do not limit user load to published applications.

## **Question 29**

Answer B is correct. The default ICA Keep-Alive value is 60 seconds. Answers A, C, D, and E are incorrect because they do not indicate the correct default value for ICA Keep-Alive.

## **Question 30**

Answer A is correct. You would configure the database connection server and the Summary Database in the Presentation Server Console. Answers B, C, D and E are incorrect because they are not the right tools to configure the database connection server or the Summary Database. The Access Suite Console currently has no plug-ins that directly support the management of Resource Manager. Data Sources is the place where you define data source names for database connections. They contain no configuration settings for either Resource Manager component. The Citrix Connection Configuration tool manages only the ICA and RDP connection settings on the MetaFrame Server. There is no such tool called the Resource Manager Console.

## **Question 31**

Answer B is correct. In the Presentation Server Console, right-click the Farm node and click Properties. Answers A, C, and D are incorrect because none of these options allow you to modify the listed SpeedScreen features. The SpeedScreen Latency Reduction Manager can be used only to configure the mouse click feedback and local text echo features. Connection Configuration has no SpeedScreen features, and the only SpeedScreen option currently managed through MetaFrame policies is image acceleration using lossy compression.

## **Question 32**

Answers A, C, and G are correct. The three privileges that can be granted to a new Citrix administrator account are View Only, Full Administration, and Custom. Answers B, D, E, and F are incorrect because they are not privilege answers available for selection when creating a new MetaFrame administrator.

## **Question 33**

Answer D is correct. The printer driver information for each server in the farm is stored in the Data Store. Answers A, B, C, and E are incorrect because they are not the right location to store the printer drivers.

## **Question 34**

Answer A is correct. Server-to-client redirection allows for the association of a server-side file with an application running on the user's local desktop. The situation described in answer A fits this description. When the user clicks the URL link in the email message, the link can be redirected and opened using a web browser running on the local client. Answer B is incorrect because the user is already running on the local machine and the URL is being opened within a web browser already. Answer C is incorrect for a slightly different reason. Although this scenario is a candidate for redirection, it represents client-to-server redirection because the Word document is being opened locally. Answer D is incorrect because the action of saving a file does not trigger the launching of an associated application.

## Question 35

Answer B is correct. The Citrix Policies remain in effect as long as a user's ICA session is active. Only after a user logs completely off a server and logs back on will he or she pick up any changes that have been made by an administrator. Answers A and C are incorrect because even after a change has been made, the updates are not applied to the user's session until he or she logs off and back on to the system. Answer D is incorrect. Even though rebooting a server would force all users off and in effect ensure that any changes were applied during the next logon, a reboot is not required to have changes in a policy rule take effect.

## Question 36

Answer A is correct. The pass-through client refers to the PN or PN Agent clients being published for users running non-Win32 operating systems. These users then have access to the features of these clients even though they are not installed locally.

Answers B and C are both incorrect. The pass-through client does not refer to the Secure Gateway or any component of the Web Interface. It also has nothing to do with any communications protocol. Answer D is also incorrect. When user credentials are automatically passed through to the server, that is known as pass-through authentication, not pass-through client.

## Question 37

Answer D is correct. The tool that should be used to create a different transport protocol for ICA is the Citrix Connection Configuration. Answers A, B, and C are incorrect because you can't create a new transport protocol for ICA using them.

## Question 38

Answer E is correct. You would use the Report Center to generate performance reports. Answers A, B, C, and D are incorrect because they can't be used to generate reports of farm performance.

## Question 39

Answer C is correct. Printer Driver Replication is the tool that you would use to replicate print drivers across all the MPS servers in the farm. Answers A, B, and D all describe valid Printer Management features, but none of them can be used to perform printer driver replication.

## Question 40

Answer D is correct. The ICA protocol is a Presentation layer protocol on the OSI model. Answers A, B,

 PREV

NEXT 

 PREV

NEXT 

# 19. Practice Exam 2

Welcome to the second of two practice exams included in this book. We hope you've come through the first exam no worse for wear and are ready to tackle the next round of questions.

Good luck!

 PREV

NEXT 

## Practice Exam

1. The \_\_\_\_\_ protocol is a presentation layer protocol and is the engine by which Presentation Server and its clients communicate.
- A. TCP/IP
- B. Independent Computing Architecture
- C. Independent Management Architecture
- D. Virtual channel
2. Which of the following statements are true about administrative delegation in the Management Console? (Choose three.)
- A. The user account provided during the MPS installation is granted full access privileges to manage the new farm.
- B. Only administrators with full administrative authority are able to add, modify, or delete other administrative accounts in the farm.
- C. Access can be delegated to administrators for subfolders created within the Servers and/or Applications nodes.
- D. The local administrator of the Presentation Server is always granted access to log on to the Management Console.

- E. When an administrator is delegating privileges, the three choices available are Read Only, Full Control, and Modified.
3. When a printer is shared directly off a Presentation Server, it is considered to be a \_\_\_\_\_ printer to the farm.
- A. direct
- B. network
- C. local
- D. client
- E. server
4. What are two of the published application types accessible through the Web client?
- A. application
- B. seamless
- C. server
- D. Installation Manager Package
5. When an application link is clicked within the Web Interface for Presentation Server, the

following is downloaded to the client and used to launch the connection to the appropriate published application.

- A. template.ini
- B. appsrv.ini
- C. appsrv.ica
- D. template.ica
- E. <app name>.ica, where <app name> is the name of the published application to connect to

6. Which three items are valid nodes of the Management Console for MetaFrame Presentation Server 3.0?

- A. Applications
- B. Licensing
- C. Load Balancing Manager
- D. Installation Manager
- E. Printer Management

7. Which of the following items are valid Presentation Server, Advanced Edition components? (Choose four.)

A. MetaFrame Access Suite Licensing

B. Web Interface for MetaFrame Presentation Server

C. Resource Manager

D. Management Console for MetaFrame Presentation Server

E. Load Manager

8. From the following list, select all that are valid states for a rule within a MetaFrame policy. (Choose all that apply).

A. Lower

B. Disabled

C. Higher

D. Enabled

E. Not Configured

9. Presentation Server supports the ability for an administrator to connect directly to a Windows Server 2003 server's console simply by right-clicking on the server in the Management Console and choosing Connect to Server's Console under the Launch ICA Session context menu. Which of the following tasks would enable this option in the Management Console? (Choose all that apply.)

- A. Nothing is required. This option is enabled by default on Windows Server 2003.
  - B. Open the properties for the Server Farm node, select ICA Settings, and enable the option Enable Remote Connections to the Console.
  - C. Open the Server node, open the properties for the desired server, select MetaFrame Settings, and then enable the option Enable Remote Connections to the Console.
  - D. Open the properties for the Server Farm node, select MetaFrame Settings, and enable the option Enable Remote Connections to the Console.
10. Which statements are true about published applications? (Choose all that apply.)
- A. When necessary, application logic is transferred to the client, where it is processed locally and returned to the server for rendering.
  - B. Available to both explicit and anonymous user sessions.
  - C. Centrally managed and controlled through the Management Console for Presentation Server.
  - D. Available only to Win32 clients unless running on the Advanced or Enterprise Editions of Presentation Server.
  - E. Requires Load Manager in order to be published with the same application name across multiple servers.
11. Which of the following are not found in the Presentation Server 3.0 Data Store? (Choose all that apply.)

A. Load Manager information

B. Printer driver information

C. Pooled license information

D. User profiles

E. Logon scripts

12. Policy assignment is dictated by \_\_\_\_\_, which determine who (or what) is affected by a policy.

A. rules

B. policies

C. priorities

D. filters

13. What is the metric used by the Default load evaluator to calculate a server's current load?

A. CPU Utilization

B. Memory Usage

C. Page Swaps

D. Server User Load

E. Application User Load

14. What must be installed on a Presentation Server for it to be a Target server for Installation Manager?

A. Packager component

B. Installer component

C. Management Console for Presentation Server

D. Target component

15. How are zone-based administrative privileges delegated?

- A. From within the MetaFrame Administrators node, define the zone privileges within the properties for the corresponding administrator.
  - 
  - B. From within the properties of the Server Farm node, choose Zones and then set the desired administrative privileges for each of the displayed zones.
  - 
  - C. Within the properties of the Servers node, choose Zones and then set the desired administrative privileges for each of the displayed zones.
  - 
  - D. None of the above.
- 16. MetaFrame Presentation Server 3.0 provides backward compatibility with MetaFrame 1.8 when operating in interoperability mode. You enable interoperability mode by \_\_\_\_\_\_. (Complete the sentence.)

  - 
  - A. opening the Management Console for Presentation Server, opening the property page for the server farm node, choosing Interoperability, and then selecting the check box Work with MetaFrame 1.8 Servers in the Farm.
  - 
  - B. opening the Management Console for Presentation Server, opening the property page for the Zone Data Collectors node, choosing Interoperability, and then selecting the check box Work with MetaFrame 1.8 Servers in this Zone.
  - 
  - C. opening the Management Console for Presentation Server, opening the property page for a server in the farm, choosing Interoperability, and then selecting the check box Work with MetaFrame 1.8 Servers.
  - 
  - D. selecting the Work with MetaFrame 1.8 Servers option during the installation of the first Presentation Server in your farm.
- 17. MetaFrame Presentation Server can be installed on which operating systems? (Choose all that apply.)

A. Windows XP Professional

B. Windows Server 2003, Enterprise Edition

C. Windows NT 4.0, Terminal Server Edition with SP6

D. Windows 2000 Server with SP4

E. Windows Server 2003, Terminal Server Edition

18. The Management Console for Presentation Server can be installed on which operating systems? (Choose all that apply.)

A. Windows XP Professional

B. Windows Server 2003, Enterprise Edition

C. Windows NT 4.0, Terminal Server Edition with SP6

D. Windows 2000 Professional with SP4

E. Windows Server 2003, Terminal Server Edition

19. Which of the following statements are true about a Farm Metric Server? (Choose all that apply.)

- A. The Primary and Backup Farm Metric Servers can be changed from within the properties of the Server Farm node.
- B. The first server upon which you install Resource Manager becomes the Primary Farm Metric Server.
- C. The second server upon which you install Resource Manager becomes the Backup Farm Metric Server.
- D. The server processes the metrics that apply to the entire server farm and generates alerts when required.
- E. Citrix recommends that the Farm Metric Server not be the same server as the Zone Data Collector.

20. To use Kerberos client authentication, the following must be true. (Choose all that apply.)

- A. All MetaFrame servers must belong to the same (or trusted) Windows 2000 or 2003 domains.
- B. Server certificates must be installed on each server.
- C. All Presentation Servers must be configured Trusted for Delegation.
- D. The server farm setting Enable XML Service DNS Address Resolution is enabled.
- E. ICA Encryption in the Citrix Connection Configuration tool must be set to Kerberos.

21. What is session reliability?



- A. It allows users to continue to see a published application's window even when the connection to the application is broken. The mouse pointer changes to an hourglass, but the session remains visible until the connection is restored or times out.



- B. It allows users to continue to work with a published application even if the connection to the application is broken. Mouse and keyboard information is stored and then pushed to the server when the connection is restored, providing users with a seamless working experience.



- C. It provides a redundant connection, increasing the reliability of the user's session to remain up. If one connection is broken, the other immediately becomes active, allowing the user to continue working without interruption.



- D. It provides session redundancy, allowing a copy of the user's current session to be cached on another Presentation Server in the farm. If the user's current connection is lost, session reliability immediately switches to this alternate server, allowing the user to continue working without interruption.

22. You are planning a large Presentation Server deployment. As part of the implementation, you want to allow a group of users to run their email client locally, while having any attachments that they open within the mail client redirected to the Presentation Server, where they are opened for viewing. This configuration requires client-to-server content redirection. Which of the following are required to implement this solution? (Choose all that apply.)

- A. Enable client drive mapping for those users.
  - B. Deploy the Web Interface for Presentation Server.
  - C. Publish the server-side application and associate it with the necessary file types.
  - D. Deploy Program Neighborhood to these users.
23. Citrix employs \_\_\_\_\_ licensing for its MetaFrame Presentation Server product.
- A. per-device
  - B. concurrent-user
  - C. per-user
  - D. none of the above

24. Ursula User has been configured by her Presentation Server administrator to connect to a group of published applications that are divided between Customer Service, Sales, and Marketing server farms. Customer Service and Sales belong to the same farm, but Marketing is in its own farm. Each farm has its own licensing server.

At one point during the day, Ursula is connected to three applications in Customer Service, two applications in Sales, and one application in Marketing. How many Client Access Licenses is she consuming?

- A. 6
- B. 5
- C. 4
- D. 3
- E. 2
25. To ensure that a user's client drives are mapped to drive C: and D:, you have decided to remap the Presentation Server drives to X: and Y:. When does Citrix recommend that you perform this drive remapping task?
- A. Prior to the installation of Presentation Server
- B. During the installation of Presentation Server, when prompted
- C. Immediately after the installation of Presentation Server
- D. After you have installed Presentation Server and all desired applications on the server
26. During the installation of Presentation Server, unless you specify a zone name, the server will \_\_\_\_\_

- A. be assigned to a zone named "Default."
  - 
  - B. be assigned to a zone matching the server farm name.
  - 
  - C. be assigned to a zone matching the subnet of the server.
  - 
  - D. be assigned to a zone matching the IP address of the server.
27. By default, server-to-server IMA communications are exchanged over port \_\_\_\_\_, while the Management Console uses port \_\_\_\_\_ to communicate with the IMA service.
- - A. 1494, 1604
  - 
  - B. 80, 443
  - 
  - C. 2512, 2513
  - 
  - D. 1494, 2598
  - 
  - E. 27000, 27000
28. You want to create an ADF package from an installation recording using the Packager component of Installation Manager. Which of the following tasks must be completed when creating this package? (Choose all that apply.)

- A. None. You cannot create ADF packages using the Packager Wizard.
  - B. Ensure no other applications are running and that no other users are logged on the server where you will run the Packager.
  - C. Make sure that the Presentation Server has been placed into install mode before starting the installation recording.
  - D. If a reboot is required to complete the installation, make certain that the recording is stopped once the restart is complete.
29. A Presentation Server client has been configured to use TCP/IP+HTTP. When contacting the server farm for published application information, what service will respond to these client requests?
- A. ICA Browser
  - B. IMA Service
  - C. Program Neighborhood Service
  - D. Citrix XML Service
  - E. Kerberos
30. What is the maximum number of load evaluators that can be assigned to a server or published application at any one time?

A. Unlimited

B. The total number of servers in the farm

C. 2000

D. 2

E. 1

31. The company that you are working for wants to publish an application in its server farm with the following requirements. It must be available only to users on the internal network, and it must be available only between 8 a.m. and 6 p.m. At all other times, the application must not be accessible. This application currently has a custom load evaluator called PubApp assigned to it. Which of the following steps provide the best solution to this issue? (Choose two.)

A. In the domain, set the allowed logon hours for those users from 8 a.m. to 6 p.m.

B. Create a new server farm for the internal subnet and grant access only to those internal users who require it.

C. Modify the PubApp load evaluator and define an IP range rule containing the internal network addresses.

D. Modify the PubApp load evaluator and define a schedule rule restricting access between 8 a.m. and 6 p.m.



- E. Create a domain group containing only those authorized users and assign that group to the list of users able to access the published application.

32. Before a printer driver can be replicated to other servers in the farm, you must first do what?



- A. Create a driver mapping for the correct Windows platform.



- B. Install the printer driver on at least one Presentation Server in the farm.



- C. Import all required network print servers.



- D. Designate a master replication server for printer drivers.

33. You have been brought in to help troubleshoot a Presentation Server installation problem. You want to shadow a remote user but realize that during the installation of Presentation Server, the option Prohibit Shadowing of User Sessions on This Server was selected. What must you do to enable shadowing so that you can save the day?



- A. Within the Management Console, open the properties for the server and select Enable Shadowing under MetaFrame Settings.



- B. Within Add/Remove Programs, modify the Presentation Server installation to enable shadowing of user sessions on the server.



- C. Within Citrix Connection Configuration, change the properties for ICA connections to enable shadowing.



- D. Reinstall MetaFrame Presentation Server.

34. An ICA packet is composed of optional and required packets. Which of the following packets are optional? (Choose all that apply.)

A. Encryption

B. Compression

C. Frame Head and Frame Tail

D. Data

E. Command

35. Which of the following are truthful statements about the SpeedScreen Flash Acceleration feature of Presentation Server? (Choose all that apply.)

A. It reduces the amount of data downloaded by reducing the quality of the Flash animation.

B. It buffers the Flash animation to the client, where a local Flash player renders the information, reducing the CPU load on the Presentation Server.

C. SpeedScreen Flash Acceleration requires that the Macromedia Flash Player be installed on the Presentation Server.

D. The displaying of Flash content can be completely disabled by disabling the Flash Acceleration option.

36. Which of the following are MetaFrame Access Suite Licensing (MASL) features? (Choose four.)

- A. Permission delegation
  - B. Mixed-mode license support with MetaFrame 1.8
  - C. Alert configuration
  - D. License server load balancing
  - E. Web-based management
37. What version of the Novell client is required for Presentation Server to be able to access Novell Directory Services?
- A. 3.1
  - B. 4.0
  - C. 4.8
  - D. 5.1
  - E. A client is not required. Support is integrated in with Presentation Server 3.0.
38. When supporting end users, you have the option of initiating shadowing through the Management Console or by using the Shadow Taskbar utility. Which of the following are valid differences between shadowing through the Management Console and shadowing with the Shadow Taskbar? (Choose all that apply.)

- A. The Management Console allows shadowing of multiple simultaneous users, whereas the Shadow Taskbar allows shadowing of only one user at a time.
- B. When shadow logging has been enabled on the server, only shadowing attempts performed through the Management Console are written to the system log. Shadow Taskbar attempts are logged only to a file.
- C. Through the Management Console, you are able to shadow a user who is logged directly onto a server console. This option is not available with the Shadow Taskbar.
- D. The Management Console allows shadowing of only one user at a time, whereas the Shadow Taskbar allows shadowing of multiple simultaneous users.

39. Which of the following client platforms are not supported by Citrix? (Choose two.)

- A. IBM OS/2 2.0
- B. Linux x86
- C. Palm
- D. Pocket PC 2003
- E. DOS

40. Which Independent Management Architecture (IMA) component is responsible for storing session information?

A. Local Host Cache

B. Data Store

C. Zone Data Collector

D. Management Console

41. A desktop support rep has called you saying that he is having problems configuring the Program Neighborhood client to connect to the published desktop in your server farm. He is receiving an error saying that the ICA browser did not return any server names. Assuming you are running a native-mode server farm and the client will be using TCP/IP+HTTP to communicate with the farm, which of the following options, if implemented, would allow the user to successfully connect to the farm? (Choose all that apply.)

A. Create a DNS entry that resolves the hostname ima to a valid server in your server farm.

B. Instruct the rep to assign one or more servers to the server location list for the HTTP/HTTPS protocol.

C. Switch the server farm to operate in mixed mode.

D. Set the ICA Browser service to automatically start so that broadcasts from the client will be detected.

42. Which of the following statements are true about a Presentation Server environment with an Access database as the Data Store? (Choose all that apply.)

- A. It is recommended for environments of up to 50 Presentation Servers.
- B. It is installed on the first Presentation Server that is set up in a new farm.
- C. It supports only direct Data Store connections.
- D. It must be set up to replicate to each Zone Data Collector in the farm to ensure Data Store access.
- E. It must be running Advanced and Enterprise Editions of Presentation Server.

43. Which of the following are valid IMA subsystems? (Choose four.)

- A. ICA Browser
- B. Application Management
- C. Static Storage
- D. User Management
- E. Printer Management

44. Every zone holds \_\_\_\_\_ elections to determine which Presentation Server is to become the Zone Data Collector.

- A. master browser
  - B. TCP
  - C. UDP
  - D. SMTP
45. An associate has asked you to tell her about server-to-client redirection in Presentation Server. Which of the following would you tell her? (Choose all that apply.)
- A. It is supported only with the Win32 client.
  - B. Only embedded URLs are redirected to the local client.
  - C. If the client fails to connect to a URL, the URL is redirected back to the server.
  - D. Server-to-client redirection requires the Advanced or Enterprise Editions of Presentation Server.
46. When you are scheduling the deployment of a package group, one of the available options allows you to define an installation window for the deployment. Choose the answer that best describes what happens if a package group deployment has not yet completed when the installation window end time is reached. (Select only one.)

- A. The package group deployment that is currently in progress terminates and performs an automatic uninstall of all packages that make up that group. All servers with a completed deployment are not affected.
  - B. The package group deployment continues until completed. Any deployments not yet started are immediately started. Once a package group deployment begins, it will process 100%, even if the installation window end time is reached.
  - C. The package group deployment currently in progress terminates, and it and all the other servers that have completed their installation automatically roll back to their state prior to the start of the installation window. The deployment is not labeled a success unless all target servers are updated.
  - D. None of the above.
- 47.** Which of the following statements are true about the Program Neighborhood Agent Console? (Choose all that apply.)
- A. The default configuration file is called config.xml and is located in the *<Web Root>/Citrix/MetaFrame/PNAgent* folder.
  - B. Centralized management of PN Agent is performed using the Program Neighborhood Agent Console, which is located in *<Web Root>/Citrix/PNAgentAdmin*.
  - C. When the PN Agent Console is accessed, a backup copy of the file is maintained with the same name and the extension .bak.
  - D. You can fully manage the location where application icons are displayed on the client. The specific settings are managed within the subcomponents of the Application Display settings.

- E. The Program Neighborhood Agent Console is integrated into the Client Update Database, allowing you to centrally manage the deployment of the PN Agent client out to the end users.

48. You have enabled the SecureICA Encryption rule for a MetaFrame policy that is being applied to all servers in the farm. This rule enforces 56-bit (RC5) encryption for all user connections. You also have a published application with a required encryption set to 128-bit (RC5). When a user connects to the published application, which setting will take priority?

- A. Neither, it depends on the encryption level of the client.

- B. Neither, it depends on the encryption level of the ICA connection.

- C. 128-bit (RC5)

- D. 56-bit (RC5)

49. The Local Host Cache is responsible for \_\_\_\_\_.

- A. storing session information

- B. maintaining a subset of the Data Collector

- C. maintaining a subset of the Data Store

- D. maintaining session information for the server



E. maintaining session information for the farm

50. MetaFrame Policies can be filtered on which of the following criteria? (Choose four.)



A. Client time zone



B. Client IP address



C. Client name



D. Username or group name



E. MetaFrame server name

51. How many application metrics does Resource Manager monitor?



A. 1



B. 5



C. 10



D. 13

52. It is recommended that communications between the Web Interface and the Citrix XML Service be secured. What component of Presentation Server must be configured to secure this connection?

- A. Client-side proxy settings
  - B. ICA encryption
  - C. Secure Gateway for Presentation Server
  - D. Citrix SSL Relay
53. What components of a Presentation Server deployment can communicate securely with a Presentation Server using SSL? (Choose all that apply.)
- A. Presentation Server Client
  - B. Web Interface
  - C. Secure Ticket Authority
  - D. Secure Gateway
  - E. Program Neighborhood Agent Console
54. You have been asked to configure an unattended installation of Presentation Server. Where on the MPS CD-ROM will you find the sample answer file provided by Citrix?

- A. \Unattended\Install\UnattendedTemplate.txt
  - B. \UnattendedTemplate.txt
  - C. \Support\Install\UnattendedTemplate.txt
  - D. \MPS\Install\Unattended.txt
55. Choose from the following list the valid universal printer drivers included with MPS 3.0. (Choose three.)
- A. HP Color LaserJet 4500 (MetaFrame PCL5 Universal Driver)
  - B. HP LaserJet Series II (MetaFrame PCL4 Universal Driver)
  - C. HP Color LaserJet 4500 (MetaFrame PCL5c Universal Driver)
  - D. HP Color LaserJet PS (MetaFrame PS Universal Driver)
  - E. HP Color LaserJet PS (MetaFrame PSc Universal Driver)
56. Summary data is kept in special temporary summary files on each server that is running Resource Manager. \_\_\_\_\_ information is updated in these summary files and then \_\_\_\_\_ the information is collected and stored in the \_\_\_\_\_, which in turn updates the \_\_\_\_\_. (Choose the answer that properly fills in the blank fields.)

- A. Hourly, daily, Data Connection Server, Summary Database
  - B. Every 15 minutes, hourly, Data Connection Server, Summary Database
  - C. Hourly, daily, Summary Database, Data Store
  - D. Hourly, daily, Farm Metric Server, Summary Database
  - E. Every 15 minutes, hourly, Farm Metric Server, Summary Database
57. You have an existing MetaFrame 1.8 environment that you want to upgrade to MPS 3.0. Which of the following are necessary steps in performing this migration? (Choose all that apply.)
- A. Install MPS 3.0 on a MetaFrame 1.8 server that is currently the Master ICA Browser.
  - B. Assign the new server farm the same name as the existing MetaFrame 1.8 server farm.
  - C. Configure the MPS 3.0 server to function in interoperability mode.
  - D. Stop the ICA Browser service on all MetaFrame 1.8 servers.
58. An administrator has defined a MetaFrame user policy with a filter that applies it to all users who belong to the Sales group. This policy has been assigned a priority number of 3, with the total number of policies in the ranking being 4. When she logs on as a member of this group, the defined rules are not being applied as expected. Why might the policy rules not be applied properly? (Choose all that apply.)

- A. The policy with a priority level of 4 has disabled these particular rules.
  - B. The policy with a priority level of 1 or 2 has disabled these particular rules.
  - C. The policy is currently disabled.
  - D. The Presentation Server that she is logging on to has not yet received the replicated policy information.
59. When a user clicks an application link in the Web Interface, how is the user authenticated by the server when the application is launched?
- A. A substitution tag in the template.ica file is replaced with the user's ID and password, encrypted using SecureICA and RC5 (128-bit) encryption.
  - B. A substitution tag in the template.ica file is populated with the session ticket information from the Web Interface. The session ticket contains the information necessary to perform authentication.
  - C. A substitution tag in the template.ica file is populated with the user's ID and password in plain text. This is why SSL should be used to secure communications between the client and the Web Interface.
  - D. A substitution tag in the template.ica file is replaced with an SSL certificate, which is used to verify the user's identity on the MetaFrame Server.
60. Which of the following statements about published content are true? (Choose all that apply.)

- A. Published content can be configured to be opened with applications on the server or the local client device.
  - B. Accessing published content will consume a Presentation Server license regardless of whether it is opened on the server or the client device.
  - C. For the user to open published content with a server-based application, the application must also be published and accessible by the end user.
  - D. You can view published content only through the Web Interface, Program Neighborhood Agent, or Program Neighborhood application sets. You cannot create a custom connection to published content.
  - E. Published content is available only to Windows-based clients.
61. You have been asked to change the zone election settings for a Presentation Server from Most Preferred to Default Preference. Where in the Management Console can this be performed?
- A. Zones setting within the properties of the Server Farm node
  - B. Zone settings within the properties of the Servers node
  - C. Zone Election settings within the properties of the Servers node
  - D. Zone Election settings within the properties of the Zones node
62. Installation Manager supports what types of application packages? (Choose all that apply.)

A. MSI

B. MST

C. MSP

D. ADF

E. ADP

63. What database management systems are supported for storing the Resource Manager Summary Database? (Choose all that apply.)

A. Microsoft Access

B. Microsoft SQL Server 2000 Desktop Engine (MSDE)

C. Microsoft SQL Server 7 and 2000

D. Oracle 7, 8i, and 9i

E. IBM DB2

64. What does the Registry value InitialClientDrive in the Registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\do?

- A. Defines the starting drive letter for use with client drive mappings. If a client drive cannot be mapped to its "matching" server drive letter, the system searches forward toward Z from this drive letter until the first available drive is found.
- B. Defines the starting drive letter for use with client drive mappings. If a client drive cannot be mapped to its "matching" server drive letter, the system searches backward toward A from this drive letter until the first available drive is found.
- C. Defines the starting drive letter for use with client drive mappings. Instead of attempting to use the matching server drive letter, the system begins assigning drives starting here and working forward toward Z.
- D. Defines the starting drive letter for use with client drive mappings. Instead of attempting to use the matching server drive letter, the system begins assigning drives starting here and working backward toward A.

65. How is the Printers node under the Printer Management node populated? (Choose all that apply.)

- A. Printers installed and shared off any Presentation Server in the farm are automatically added to the Printers node. The full printer name, host server name, driver, and host operating system are all displayed.
- B. When a user with client printer mapping enabled connects to the server and its printers are successfully mapped, they appear in the Printers node. Only the full printer name and client name are displayed.
- C. Any printers available on a standard print server (not running MPS) can be added to the node if imported from the Network Print Servers tab. Only the full printer name and host print server name appear for these printers.

- D. When a user logs on to the server and has network drives mapped using a logon script, they are automatically added to the Printers node. They appear with only the full printer name and host print server name.
66. You have taken over support for a Presentation Server farm consisting of six servers all in the same zone. Users are accessing Microsoft Office, which is published on all six servers, via the Web Interface. One of your co-workers runs in saying that a server has just caught on fire and melted into the floor. What must you tell him to do to ensure that users can still access Microsoft Office?
- A. Move the remaining five servers to a new zone.
- B. Restart the IMA service on all the remaining servers.
- C. Stop publishing Microsoft Office on the downed server.
- D. None of the above.
67. By default, Presentation Server enables a feature where the client's local time is used instead of the server time to time-stamp applications. For ICA client versions earlier than 6.x, the server must estimate the client's local time. How is time estimation performed in these earlier clients?

- A. The virtual channel responsible for client drive mappings is used to read the time information in the client's Registry.
  - B. The client sends the local time of the device to the server. The server uses this to estimate the time zone for the client.
  - C. The client sends the local time zone information only. The server must then estimate the local time based on this.
  - D. The server uses the IP address of the client to estimate what time zone the client resides in. This is then used to estimate the local time of the client.
- 68.** Which of the following statements are true about MetaFrame Access Suite Licensing? (Choose all that apply.)
- A. All license server management can be performed using the License Management Console.
  - B. License server files are associated with the fully qualified domain name (FQDN) of the license server.
  - C. The license server allocates temporary Client Access Licenses (CALs), which are good for 30 days if all available CALs are currently checked out.
  - D. The Citrix Vendor Daemon randomly selects a listening port every time it is restarted.
  - E. When configured for interoperability mode, the license server can store and allocate licenses for MetaFrame XP servers, but only if they are in the same farm as the MPS 3.0 servers.

69. Select the answer which best lists the order in which the components of the Secure Gateway should be installed and configured.

- A. Secure Ticket Authority, Secure Gateway, Web Interface, MetaFrame Presentation Server

- B. Secure Gateway, Web Interface, Secure Ticket Authority, MetaFrame Presentation Server

- C. MetaFrame Presentation Server, Secure Ticket Authority, Web Interface, Secure Gateway

- D. MetaFrame Presentation Server, Web Interface, Secure Gateway, Secure Ticket Authority

70. Where in the system would you go to view the list of load evaluators associated with the servers and published applications in the farm?

- A. Within the Servers node, select the Load Manage Monitor tab for a server.

- B. Within the Applications node, select the Load Manage Application menu option after right-clicking on an application.

- C. Within the Load Evaluator node, select the Contents tab from the right-hand pane.

- D. Within the Load Evaluator node, select the Usage Reports tab from the right-hand pane.

 PREV

NEXT 

 PREV

NEXT 

## 20. Answer Key 2

[Answer Key](#)

 PREV

NEXT 

# Answer Key

1. B
2. A, B, C
3. C
4. A, D
5. D
6. A, D, E
7. A, B, D,  
E
8. B, D, E
9. C, D
10. B, C, E
11. C, D, E
12. D
13. D
14. B
15. D
16. A
17. B, D
18. A, B, C,  
D
19. B, C, D
20. A, C, D
21. A
22. A, B, C
23. B

24. E  
25. A  
26. C  
27. C  
28. B  
29. D  
30. E  
31. C, D  
32. B  
33. D  
34. A, B, C  
35. A, C, D  
36. A, C, E  
37. C  
38. D  
39. A, C  
40. C  
41. B  
42. A, B  
43. A, B, D,  
E  
44. B  
45. B, C  
46. D  
47. B, C, D  
48. C  
49. C  
50. B, C, D,  
E

51. A

52. D

53. A, B, C,  
D

54. C

55. B, C, D

56. A

57. B, C

58. B, C

59. B

60. A, C, D

61. A

62. A, C, D

63. C, D

64. B

65. A, C

66. D

67. B

68. A, D

69. C

70. D

## Question 1

Answer B is correct. Citrix designed the Independent Computing Architecture (ICA) protocol to be a powerful multichannel protocol that can exchange data over network bandwidth as low as 10 to 20Kbps. Answer A is incorrect. TCP/IP is not correct because this is a networking protocol, not a presentation protocol. Answer C is also incorrect. The Independent Management Architecture is a protocol used for communications between Presentation Servers, not for client-server interaction. Likewise, Answer D is incorrect. Virtual channels are a mechanism for extending the functionality of the ICA protocol, not a communications protocol itself.

## Question 2

Answers A, B, and C are correct. During the installation of the first Presentation Server in a new farm, you are prompted to provide the name and domain of a user who will be the initial administrator of the farm. This user is granted full access rights to the farm. Through this account, you can grant and delegate privileges to other users. Only an administrator with full privileges can modify other administrative accounts. These account privileges cannot be delegated. By creating subfolders under Applications or Servers, you can assign granular access rights to specific users or groups. Answer D is incorrect. Unless the local administrator has been granted access, even she cannot log on to and administer the farm. Answer E is also incorrect. The three categories of privilege types are View Only, Full Administration, and Custom. The options listed for this choice do not even exist.

## Question 3

Answer C is correct. When a printer is directly connected to a server running MPS, that printer is considered to be a local printer to the farm. Answer A is incorrect because this is not the correct term to describe the printer. Answer B is also incorrect. A network printer is a printer shared off a server that is *not* running Presentation Server. Answer D is incorrect because a client printer is any printer that is configured on a client device, whether it is a printer directly attached to the client or a printer that is mapped to a share on the network. Answer E is incorrect because server printer is not one of the printer categories for MetaFrame.

## Question 4

Answers A and D are correct. The two valid published application types in this list are application and Installation Manager Package. The other two types not listed are Desktop and Content. Answers B and C are incorrect because they are not valid published application types. Seamless is a method by which a published application is displayed, not the type being deployed. Server also is not a published application type, but is directly accessible using a full client such as the Linux client or the full Program Neighborhood client.

## Question 5

Answer D is correct. When a user clicks an application link, the Web Interface replaces the substitution tags with the appropriate information and then sends the template.ica file to the client, where the local ICA client then processes the file and establishes the connection to the published application on the corresponding server. The same process is used to launch applications through the PN Agent Console.

Answers A and C are incorrect because these filenames do not exist. Answer B is incorrect because appsrv.ini is the local per-user configuration file used with the full Win32 Program Neighborhood client. Answer E is incorrect because the Web Interface does not generate an ICA file with the name of the application.

## Question 6

Answers A, D, and E are correct. The Applications node is where published applications and content are managed. Installation Manager is where application packages are grouped and deployed. Printer Management is where all printer-related functions of the farm are managed. Answer B is incorrect. Licensing has been moved out of the Management Console and into the MetaFrame Access Suite Licensing server. Answer C is also incorrect. Load management is defined within the Load Evaluators

node and then assigned to specific servers or published applications within the Applications or Servers nodes. There is no such node named Load Balancing Manager.

## Question 7

Answers A, B, D, and E are correct. The Advanced Edition of Presentation Server provides access to all these components with the exception of Resource Manager, which, along with Installation Manager, is a component available only with the Enterprise Edition of Presentation Server. Therefore, answer C is incorrect.

## Question 8

Answers B, D, and E are correct. A rule within a MetaFrame Policy can be in one of three states: Not Configured, Enabled, or Disabled. Higher and lower refer to the position of a policy relative to other priorities when discussing the order of precedence for policies. It has nothing to do with the state of a rule. This is why answers A and C are incorrect.

## Question 9

Answers C and D are correct. To be able to launch an ICA session directly to the server's console, you must first enable this option under the MetaFrame Settings for the entire farm or for the specific server in question. The option is found in the same location within the properties of the farm or the individual server. Answer A is incorrect. Although direct console logon requires Windows Server 2003, it is not enabled within Presentation Server by default. Answer B is incorrect because the setting in question is not found in the ICA Settings for the farm.

## Question 10

Answers B, C, and E are correct. Anonymous or explicit user sessions can be configured to access a published application. All aspects of the published application's configuration are managed within the Applications node of the Management Console. To be published with the same name across multiple servers, Load Manager must be available. When published in this fashion, it is automatically configured for load balancing, meaning that client connections are distributed across all servers that are published that application. Answer A is incorrect. No portion of the application logic is sent to the client for processing. Only application input and output are transmitted between the server and client device. Answer D is also incorrect. All versions of Presentation Server can publish applications, and these applications are available to any supported ICA client device.

## Question 11

Answers C, D, and E are correct. None of these settings are found in the Data Store. Pooled license information is now maintained in the MetaFrame Access Suite License server, where it is accessible by Presentation Server and other Access Suite products. User profiles and logon scripts are both features of Windows and not specific to Presentation Server. The two components, Load Manager information and printer driver information, are both maintained within the Data Store. Therefore, answers A and B are incorrect.

## **Question 12**

Answer D is correct. Policies are assigned based on filters, which are created to narrow down the objects that are affected by one or more policies. Answer A is incorrect. A rule is an individual setting within a policy. Answer B is also incorrect. A policy does not contain any information that dictates who is affected. Answer C is incorrect as well. Priorities dictate the order in which multiple policies are applied, but they do not dictate who receives the policy.

## **Question 13**

Answer D is correct. The Default load evaluator, one of two evaluators included with Presentation Server, bases its load calculations for a server on the number of connected users on the server. Answers A, B, C, and E are all valid load evaluator metrics but are not used by the Default evaluator.

## **Question 14**

Answer B is correct. To be a valid target server for Installation Manager, the Installer component must be installed on the Presentation Server. This component is part of the Enterprise Edition of Presentation Server. Answers A, C, and D are incorrect. The Packager component is required only on a server that is going to be used to build custom Installation Manager Packages. The Management Console is needed to configure and manage Installation Manager, but it is not required for a server to be a valid target server. Answer D is incorrect because there is no such component labeled Target component.

## **Question 15**

Answer D is correct. None of the steps listed correctly configure zone-based administrative privileges. To define zone-based privileges, you need to create a subfolder within the Server node corresponding to each zone. The appropriate servers are then placed within each folder, and the desired administrative privileges are delegated to each folder. There is no true way of tying privileges to a zone. Answer A is incorrect because an option to configure zone privileges does not exist. Answer B is incorrect because within the Zones setting for the Server Farm node, there is no option to set privileges. Answer C is incorrect because there is no properties page available for the Servers node.

## **Question 16**

Answer A is correct. Interoperability mode is enabled in an MPS 3.0 server farm by selecting the check box Work with MetaFrame 1.8 Servers in the Farm in the Interoperability option for the farm. Answers B, C, and D are all incorrect. They refer to settings that do not actually exist in Presentation Server. There is no Zone Data Collector node, interoperability is not set on a per-server basis, and it is not an option available during the installation of Presentation Server.

## **Question 17**

Answers B and D are correct. MetaFrame Presentation Server is supported on all versions of Windows 2000 Server with SP4 and Windows Server 2003. Answers A and C are incorrect. MPS cannot be installed on any desktop Windows operating system and will not install on NT 4.0, Terminal Server

Edition. Answer E is incorrect because there is no such version of Windows Server 2003 called Terminal Server Edition.

## Question 18

Answers A, B, C, and D are correct. Unlike Presentation Server, which you can install only on server operating systems, you can install the Management Console on Windows NT 4.0 or higher server or desktop operating systems. In addition to one of these 32-bit operating systems, you also require the Sun Java Runtime Environment (JRE) 1.4.1 or higher. Answer E is incorrect because there is no such version of Windows Server 2003 available.

## Question 19

Answers B, C, and D are correct. The first two servers upon which Resource Manager is installed are designated as the Primary and Backup Farm Metric Servers, respectively. These servers are then responsible for collecting and processing metric data for the farm and generating alerts when appropriate. Answer A is incorrect because the Primary and Backup Metric Servers are managed through the Resource Manager node, not the Server Farm node. Answer E is incorrect because Citrix actually does recommend that you deploy the Primary and Backup Metric Servers on the same servers that are the Zone Data Collectors.

## Question 20

Answers A, C, and D are correct. Kerberos is an integrated component of Windows 2000 Server and Windows Server 2003, and requires one of these operating systems to function properly. The Trusted for Delegation setting allows any services running with the local system account to request services from other (external) servers. The option Enable XML Service DNS Address Resolution allows the server to return the fully qualified domain name (FQDN) to the clients. This FQDN is required for Kerberos authentication. Answer B is incorrect. Server certificates are not required for Kerberos authentication. Answer E is also incorrect. There is no ICA Encryption setting called Kerberos.

## Question 21

Answer A is correct. Session reliability allows a user's published application to remain visible even if the connection to the server has been lost. The session remains active, and the reconnection attempts continue until a timeout value is reached. The default timeout is 3 minutes. If the session is reestablished within that time, the connection is automatically reconnected without requiring the entry of user credentials, and the user can continue working without any sense that the session was actually lost. Answers B, C, and D all describe false scenarios that are not supported. Mouse and keyboard input is not available when the connection has been lost. To the user, the application appears to be "busy." Session reliability also does not maintain redundant connection or session information. It is not a fail-over solution.

## Question 22

Answers A, B, and C are correct. To implement client-to-server redirection, the users must have client drive mapping enabled. Client-to-server redirection requires that users run the Program Neighborhood Agent client, which requires the Web Interface. When the application is published, the final screen of

the Application Publishing Wizard allows you to define file types that are associated with the published application. These file types are used by the PN Agent to update the Win32 Registry with the necessary server-side application references. Answer D is incorrect because the users require the PN Agent client, not the full Program Neighborhood client.

## Question 23

Answer B is correct. Presentation Server licensing is based on concurrent users. If you have purchased 30 Client Access Licenses, you can have up to 30 concurrent users connected at any one time, regardless of where they are connecting from. Two hundred users could all have the Presentation Server client installed, but only 30 out of that 200 can be connected simultaneously. Answers A, C, and D are incorrect. Per-device or per-user licensing is required for Terminal Services licensing.

## Question 24

Answer E is correct. Regardless of the number of applications open, only one Client Access License is consumed per license server. So even though Ursula is connected to applications in both the Customer Service and Sales server farms, because they share a license server, she consumes only one license. The second license is consumed by accessing the one application in Marketing, which uses its own license server. Because of this, answers A, B, C, and D are all incorrect.

## Question 25

Answer A is correct. Citrix strongly recommends that if you decide to remap server drive letters, you do so prior to the installation of any applications, including MPS 3.0, on the server. Answer B is incorrect. The Presentation Server installation process no longer prompts for this drive remapping change. Older versions of MetaFrame did integrate this function as part of the standard installation wizard. Answer C is incorrect. Even though it is possible to perform the drive remapping after the MPS installation has completed, Citrix does not recommend doing so. Answer D is also incorrect. Waiting until after MetaFrame and all the other applications have been installed almost guarantees that certain applications will not function properly. The drive remap process cannot be relied upon to properly remap all application associates that may exist with the C: and D: drives prior to the remap occurring.

## Question 26

Answer C is correct. By default, unless you specify the name of the zone to create or join, a newly installed Presentation Server is assigned to the zone with the name matching the subnet of the server. For example, if the server has an IP address of 192.168.1.25, the zone name is set to 192.168.1.0. Answers A, B, and D are all incorrect.

## Question 27

Answer C is correct. Servers communicate on port 2512, while the Management Console connects to the IMA service on port 2513. Although all the other answers represent valid Presentation Server-related ports, they are not correct answers to the question. Port 1494 is used for standard ICA client-to-server connections. Port 1604 is the UDP port used for either client-to-server or server-to-server communications when mixed-mode interoperability is enabled. Port 80 and 443 are used for insecure and secure communications with the Web Interface, Citrix XML Service, and Secure Gateway.

Port 2598 is used to support the session reliability feature. Port 27000 is the default listening port for the MetaFrame Access Suite Licensing server.

## Question 28

Answer B is correct. Of the four choices, the only one that is a valid task is B. If you want to ensure an accurate installation recording, there should be no other applications running and no other users logged on to the MetaFrame server. Answer A is incorrect because the Packager does create ADF packages. It cannot create MSI or MSP packages. Answer C is also incorrect. You are not required to place the server into install mode when performing a package recording. Answer D is also incorrect. When the recorded program requires a restart, you must ensure the recording has been stopped *before* you allow the restart to occur.

## Question 29

Answer D is correct. The Citrix XML service is responsible for servicing all HTTP/HTTPS requests for farm information. Answer A is incorrect because the client is using HTTP. Only if the client was using UDP broadcasts would the ICA Browser service possibly respond. Answer B is incorrect. The IMA Service does not directly respond to client requests, except for Management Console connection. Answer C is also incorrect. The PN Service is integrated with the IMA Service and does not directly process client requests. Likewise, answer E is incorrect. Kerberos is an authentication architecture, not a Citrix connection service.

## Question 30

Answer E is correct. Only one load evaluator can be assigned to a published application or a server at any one time. If an evaluator is assigned to both, when a user launches the published application on the server, the evaluator with the highest threshold settings is used. Therefore, answers A, B, C, and D are incorrect.

## Question 31

Answers C and D are correct. Both requirements can be met using the Boolean type rules for the Load Manager that place restrictions on access based on the IP address of the client and the time of day the connection is attempted. If either criterion is not met, the load is returned as 100%, and the application is unavailable to the user. Answer A is incorrect because specifying a logon time frame would prevent the users from accessing any other applications outside that window. Answer B is incorrect as well. The creation of a separate farm itself would not guarantee that users could not access the environment from an alternate address. In fact, an internal user could access the server from an external location. Answer E is also incorrect. Even though it would restrict access to only the authorized users, it would neither prevent one of those users from accessing the program from a different network, nor would it restrict access to the application only within the desired time frame.

## Question 32

Answer B is correct. Before a driver can be replicated, it must exist on at least one server in the farm. This driver can be installed on any server and replicated to any other server running the same Windows platform. Answer A is incorrect. Driver mappings are not required to replicate printer drivers.

Answer C is incorrect because driver replication is not dependent on imported network print servers. Answer D is incorrect because there is no such thing as a master printer driver replication server.

## Question 33

Answer D is correct. Unfortunately, after shadowing has been prohibited on a Presentation Server, it can be enabled only by reinstalling the software. This security feature prevents shadowing from "accidentally" being reenabled. Answers A, B, and C are all incorrect. No option within the server properties nor Add/Remove programs allows shadowing to be reenabled, and the settings in the Citrix Connection Configuration tool allow you to manipulate shadowing only if it was enabled during installation.

## Question 34

Answers A, B, and C are correct. The only required component of an ICA packet is the Command byte, which is why E is an incorrect answer to this question. Answer D is also incorrect because there is no such component labeled Data in the ICA packet. Encryption is present only when the data is encrypted between the client and server. Similarly, Compression is included only when data compression has been configured. The Frame Head and Frame Tail are included in transmissions only when a streaming transmission protocol such as TCP/IP is being used.

## Question 35

Answers A, C, and D are correct. By default, Flash animation attempts to render in the highest quality, resulting in excessive CPU processing and a high quantity of data transmitted to the client with each animation frame. Flash Acceleration reduces the default quality of the Flash animation, resulting in a reduction in both CPU usage and data being transmitted. If you want to employ Flash Acceleration, the Macromedia Flash player must be installed on each Presentation Server. By disabling Flash Acceleration, you disable the playing of Flash animation on servers in the farm. Answer B is incorrect. It is the SpeedScreen Multimedia Acceleration feature that attempts to stream multimedia content to the local PC, not the Flash Acceleration feature. Flash content is rendered and transmitted from the server to the client.

## Question 36

Answers A, C, and E are correct. MetaFrame Access Suite Licensing supports permission delegation, alert configuration, and web-based management. MASL is not able to manage licenses for older versions of MetaFrame XP or MetaFrame 1.8. These legacy environments must continue to use their existing license configuration. MASL also does not provide native support for load balancing the licensing data although it does simplify the data backup process, allowing for much quicker recovery than in previous environments.

## Question 37

Answer C is correct. You require version 4.8 of the Novell client to access NDS on Novell servers. Answers A, B, D, and E are all incorrect because they contain incorrect client versions. MPS 3.0 does not include integrated support for accessing NDS. It still relies on the Novell client for communications.

## **Question 38**

Answer D is correct. You can initiate multiple simultaneous shadowing sessions through the Shadow Taskbar, whereas shadowing within the Management Console is restricted to one user at a time. Answers A, B, and C are all incorrect. A is incorrect because it is the opposite of what is stated in answer D. Answer B is incorrect because as long as shadow logging has been enabled on the server where the user is being shadowed, it is captured in the event log, whether it is initiated through the Management Console or the Shadow Taskbar. Shadow Taskbar does allow writing to a log, but this is not mutually exclusive to the event log entries. Answer C is incorrect because users logged on to the local console of the server cannot be shadowed, regardless of the method used.

## **Question 39**

Answers A and C are correct. Citrix provides support for OS/2 Warp, but only versions 3.0 and later. Palm is the only other OS in this list that is currently not supported by Citrix. Answers B, D, and E are incorrect because Citrix provides clients for all these versions.

## **Question 40**

Answer C is correct. Zone Data Collectors are responsible for storing frequently changing information for servers in their zone. This information includes server user load, and active and disconnected sessions. Answer A is incorrect because the Local Host Cache (LHC) maintains a subset of Data Store information, quickly accessible by the server on which the LHC resides. This information provides redundancy in the event that the Data Store connectivity is broken. It does not store active session information. The Data Store itself contains configuration information about the entire farm. It does not maintain a list of active session information. Therefore, answer B is incorrect. Answer C, the Management Console, is incorrect because this tool provides access to viewing and configuring the Presentation Server farm; it does not store any farm or zone information itself.

## **Question 41**

Answer B is correct. Out of the four choices, only B is correct. If the user defines one or more valid MetaFrame servers in the server location list for HTTP/HTTPS, the client will know with which server to query for farm information. Answer A is incorrect because the default hostname on all ICA clients is ica, not ima. Creating a DNS entry for ica would allow the client to resolve at least one hostname. Answer C is incorrect because even in mixed mode, the client would still be attempting to contact with TCP/IP+HTTP. The client would also need to be switched to use TCP/IP and be on the same subnet as the server to successfully broadcast for farm information. Answer D is incorrect. You cannot manually start the ICA Browser service, but even if you could, the client does not broadcast at all when using TCP/IP+HTTP.

## **Question 42**

Answers A and B are correct. Citrix recommends that the Access database be used only in environments of up to 50 Presentation Servers. When selected, the Access Data Store is installed on the first Presentation Server that is set up for a new server farm. Answer C is incorrect. Actually, when you are using an Access Data Store, only indirect connections are supported. This means that additional Presentation Servers must communicate with the IMA service on the server hosting the

Data Store, which in turn retrieves or updates the appropriate farm information, instead of the servers communicating directly with the Data Store. Direct connections are supported only with SQL Server, Oracle, and DB2 databases. Answer D is incorrect because no replication is required for any Data Store that is employed. Answer E is incorrect because all host platforms for the Data Store are supported regardless of the platform edition of Presentation Server that is deployed.

## Question 43

Answers A, B, D, and E are correct. ICA Browser, Application Management, User Management, and Printer Management are all valid IMA subsystems. Answer C is incorrect. Static storage is not a valid subsystem component. Persistent Storage is a valid subsystem, responsible for updating the Local Host Cache on each server in the farm.

## Question 44

Answer B is correct. Zone Data Collector elections require the TCP protocol. UDP is supported only for legacy ICA browsing requirements, whereas the SMTP protocol is used for email delivery. Therefore, answers C and D are incorrect. Data Collector elections are not master browser elections. MetaFrame XP maintained an ICA browser master, which required an election process very similar to the Data Collector elections to determine what server would behave as the master browser. This is why answer A is incorrect.

## Question 45

Answers B and C are correct. Server-to-client redirection supports only URL redirection, using the local browser and support multimedia applications to process certain web content. If, for whatever reason, the URL cannot be processed by the client, it is redirected back to the server for processing. Answer A is incorrect. The Linux client also supports server-to-client redirection. Answer D is also incorrect; server-to-client redirection is supported in all versions of Presentation Server. It is client-to-server redirection that is available only in the Advanced and Enterprise Editions.

## Question 46

Answer D is correct. None of the other answers given to this question are correct. If the maintenance window ends before the current installation is complete, it is allowed to finish, but no further deployments to any remaining target servers are initiated. Any outstanding deployments do not complete unless a new deployment is created for them, or additional scheduled days are defined for the current job so that it can restart and complete the deployment. Because of this, answers, A, B, and C are all incorrect. In-progress deployments are allowed to complete, queued deployments are not allowed to begin after the window has ended, and installed packages are never uninstalled unless specifically configured to do so.

## Question 47

Answers B, C, and D are correct. The PN Agent Console allows you to centrally manage the PN Agent client and is accessed within the Citrix/PNAgentAdmin folder under the root of the web server. The PN Agent Console does automatically keep a backup of the configuration file prior to the latest changes. If an undesirable change was made, you can revert back simply by overwriting the latest file with this

backed-up version. Within the Application Display settings, you are able to fully manage how the PN Agent client pushes out the icons to the end user's desktop. Answer A is incorrect because the wrong location for the config.xml file was given. The filename itself is correct, however. Answer E is also incorrect. The PN Agent client is not automatically pushed out, and the console is not integrated into the Client Update Database. The client must either be manually deployed or deployed using an alternate distribution method.

## Question 48

Answer C is correct. MetaFrame policies override all other settings in the environment, with the exception of encryption, if the policy would enable a lower encryption level than is set elsewhere in the system. The other exception is with shadowing. A policy overrides other shadow settings, unless the other settings are more restrictive. For these reasons, answers A, B, and D are all incorrect.

## Question 49

Answer C is correct. The Local Host Cache maintains a subset of the Data Store information. This speeds up processing of information by the Presentation Server and allows it to function independently in the event that connectivity to the Data Store fails. Answers A, D, and E are all incorrect because the LHC is not responsible for maintaining any session information. That is the responsibility of the Zone Data Collector, which is why answer B is also incorrect.

## Question 50

Answers B, C, D, and E are correct. You can filter on the client IP address (individual, range, or all addresses that connect to a server), client name (use WI\_\* to filter Web Interface clients), username or group name, and the MetaFrame server name. You cannot define filter criteria based on the client's time zone information; therefore, answer A is incorrect.

## Question 51

Answer A is correct. Resource Manager monitors one application metric, and it is the application count. This reflects the number of application instances currently running in the farm. Resource Manager can alert you if this count exceeds a predefined value, and is specifically created to provide license management capabilities. Answers B, C, and D are all incorrect because Resource Manager can monitor only one application metric.

## Question 52

Answer D is correct. The Citrix SSL Relay is responsible for providing SSL/TSL communications support from both the Web Interface and Presentation Server clients that have been configured to connect in this fashion. The Citrix SSL Relay Configuration tool is used to enable SSL relay, including selection of the certificate to use for authentication and encryption, as well as the encryption standard (SSL v3 or TLS v1) and the ciphersuites to use. Answer A is incorrect. Client-side proxy is a setting in the Web Interface used to configure how client connections to the MetaFrame farm should be directed. Answer B is incorrect because ICA encryption is the encryption strength used to secure ICA communications between the client and the Presentation Server. Answer C is also incorrect because the Secure Gateway is responsible for securing communications between the client and the Presentation Server,

not the Web Interface and Presentation Server.

## Question 53

Answers A, B, C, and D are correct. The client can use SSL/TLS+HTTPS to connect to the Presentation Server via SSL Relay. The Web Interface, Secure Ticket Authority, and Secure Gateway all communicate securely with the servers in the farm through the same SSL Relay. Answer E is the only incorrect choice because the Program Neighborhood Agent Console does not communicate with any of the Presentation Servers. Instead, the administrator's web browser and console communicate, with the console directly updating the configuration files locally on the web server.

## Question 54

Answer C is correct. The sample unattended installation file is called UnattendedTemplate.txt and is found in the \Support\Install folder on the main Presentation Server installation CD-ROM. Answers A, B, and D all list invalid file locations, and as such are incorrect answers.

## Question 55

Answers B, C, and D are correct. Citrix provides three universal printer drivers: two for PCL (black-and-white and color) and one color PostScript driver. Answer A is incorrect because the driver should be a PCL5c driver, not a PCL driver. Answer E is incorrect because the driver should be a PS driver, not a PSc driver.

## Question 56

Answer A is correct. Once every hour, information from all Resource Manager servers in the farm is updated in the local summary files. Daily this information is then transmitted to the Data Connection Server, where it is finally sent to the Summary Database. After it has been successfully updated in the Summary Database, the local summary files are cleared and new data collection begins. Answer B is incorrect because the time intervals are wrong. Answer C is wrong because the Data Store does not receive or store Resource Manager information. Answer D is wrong because the Farm Metric Server is responsible for storing farm-wide metrics, which it in turn sends off to the same Data Connection Server and then the Summary Database. Answer E is wrong because both the components and the time intervals are incorrect.

## Question 57

Answers B and C are correct. When installing the first MPS 3.0 server in an existing MF 1.8 server farm, you must create the new Data Storebased farm with the exact same name as the existing farm. You then must enable interoperability (mixed) mode, allowing the MPS server to provide legacy support for the farm. Answer A is incorrect. You should actually install MPS on a 1.8 server that is *not* currently the master browser. Answer D is also incorrect. Stopping the ICA Browser service on the 1.8 servers effectively removes them from operating in the farm, causing issues with user connectivity.

## Question 58

Answers B and C are correct. If a policy with a higher priority (in this case 1 or 2) explicitly disables these policies, the net result is that the policy is canceled out and the configuration change is not applied to the user's session. It is also possible that the policy itself has a status set to Disabled. In this case, the policy is completely ignored and no rules are applied. Answer A is incorrect because a lower-priority policy rule (in this case 4) takes precedence only if a higher-priority rule is set to Not Configured. Answer D is incorrect because policy information is not replicated to all servers. It is stored in the Data Store and retrieved by the MetaFrame servers when required during user logon.

## Question 59

Answer B is correct. User credentials are not passed between the client and server. Instead, the session ticket is used to verify the identity of the user to the server, allowing the user to launch the appropriate published application. Answers A and C are both incorrect because the user's ID and password are never placed into the template.ica file. Answer D is also incorrect because SSL certificates are not used to perform user authentication on a Presentation Server. They are used strictly to secure communications between the various components of the Web Interface environment.

## Question 60

Answers A, C, and D are correct. You can configure the environment to open published content locally on the client device or through an application published on the server. The user must have access to that application to open content on the server. If the user does not have access to the published application, MetaFrame attempts to open the content locally on the client. Published content is not accessible through a custom ICA connection. It is visible only through the Web Interface, PN Agent, or Program Neighborhood application set. Answer B is incorrect. If content is opened locally on the client, no license is consumed. Answer E is also incorrect. Any Presentation Server client can access published content through the Web Interface.

## Question 61

Answer A is correct. The zone settings are found within the properties of the Server Farm node. Answers B, C, and D are all incorrect. There are no properties for the Servers node, and no Zones node exists within the Management Console.

## Question 62

Answers A, C, and D are correct. Installation Manager supports the MSI, MSP, and ADF packages for deployment. Answer B is incorrect. The MST package is an MSI transform and can be used to modify an MSI deployment but cannot itself be deployed. Answer E is also incorrect. ADP is not a valid package format.

## Question 63

Answers C and D are correct. Unlike the server farm Data Store, which supports all the listed database management systems, the Summary Database is currently supported only on Microsoft SQL Server (7 or 2000) or Oracle (7, 8i, 9i). Answers A, B, and E all list DBMSs that are not supported, so they are wrong.

## **Question 64**

Answer B is correct. When performing a client drive mapping, the server always attempts to first match the client drive (for example, C) to the matching drive letter on the server. If this match cannot be performed, the server starts at drive V: and works backward toward A: looking for the first available drive to assign to the client drive. By configuring this Registry value, you can set the starting value for client drive mappings. Instead of V:, the server starts at this alternate drive letter and works back toward A:. Answer A is incorrect because the server is moving in the wrong direction assigning drives. Answers C and D are both incorrect because they are not attempting to map to the matching drive letter before processing this starting drive.

## **Question 65**

Answers A and C are correct. Printers shared off MetaFrame servers are automatically added to the Printers node and are fully manageable. Printers on non-MetaFrame print servers can be manually imported, although options such as driver replication are not available for these printers. Answers B and D are both incorrect. Client printers, whether mapped through client printer mapping or logon scripts, are not automatically added to the Printers node. They appear only under the Windows Printers folder.

## **Question 66**

Answer D is correct. In fact, you would tell your co-worker to do nothing. Presentation Server load balancing automatically redirects any users connecting to a Microsoft Office product to one of the servers that is still available.

Answers A, B, and C are incorrect. Moving these servers to a new zone does not have any effect on users being able to access the applications. If you stop and restart the IMA service on the available servers, that only makes them temporarily unavailable as they are removed and re-added to the list of balanced servers. Removing the downed server from the list of available servers hosting Office also does not affect accessibility to the available servers. It only makes Office unavailable on that server when it does come back up.

## **Question 67**

Answer B is correct. The Presentation Server calculates the proper client time based on the client's time zone setting, not necessarily the actual time setting of the client. Version 6.x and later of the ICA client send the proper time zone information of the client to the server, where the proper time is calculated based on the server's time zone and the current time. Versions of the client prior to 6.x are able to transmit only the local time of the client. This is not necessarily reliable. The user may have set the time correctly on her PC but may have the wrong time zone set for her device. In this case, the server attempts to determine the time zone based on the local time compared to the server's time. This can easily result in the wrong time zone being used. Answer A is incorrect. The server does not perform any local Registry queries via this channel. Answer C is incorrect. This is actually how newer clients transmit the proper time information. Answer D is also incorrect because the server performs no estimates using client networking settings.

## Question 68

Answers A and D are correct. The web-based License Management Console can be used to manage the configuration of the license server. The Citrix Vendor Daemon component of MASL randomly selects a port to listen on every time it is restarted. The License Manager Daemon, which always listens on port 27000, informs any connecting Presentation Server what port must be used to contact the Citrix Vendor Daemon. Answer B is incorrect. The license server files are associated with the license server's hostname, not the fully qualified domain name. Answer C is incorrect because MASL does not allocate temporary licenses. If all existing licenses are in use, any new users are rejected. Answer E is incorrect. MASL is incompatible with previous versions of MetaFrame. If a mixed environment of servers is supported, license environments corresponding to the MetaFrame version must also be supported.

## Question 69

Answer C is correct. Citrix recommends that the components of the Secure Gateway be configured from the secure network outward. This means that when the MetaFrame Presentation Server environment is working properly, the Secure Ticket Authority is installed and validated. Next, the Web Interface is configured, and communications directly via the Web Interface can be secured. Finally, the Secure Gateway itself is deployed, and from it, you can validate whether all the other components are available and functioning properly. Answers A, B, and D are all incorrect because they list the components in the incorrect order.

## Question 70

Answer D is correct. The Usage Reports tab for the Load Evaluators node allows you to view the list of applications and servers and their associated load evaluators. You have the choice of three different views: either by applications, by servers, or by evaluators. When viewing the list by evaluator, you see the evaluators, applications, and servers all listed in one table. Answer A is incorrect because the Load Manage Monitor tab displays only the total load count and the load for each of the evaluators.

 PREV

NEXT 

# A. CD Contents and Installation Instructions

The CD features an innovative practice test engine powered by MeasureUp, giving you yet another effective tool to assess your readiness for the exam. The CD also includes a helpful "[Need to Know More?](#)" appendix that will break down by chapter extra resources you can visit if some of the topics in this book are still unclear to you.

# Multiple Test Modes

MeasureUp practice tests are available in Study, Certification, Custom, Adaptive, Missed Question, and Non-Duplicate question modes.

## Study Mode

Tests administered in Study Mode allow you to request the correct answer(s) and explanation for each question during the test. These tests are not timed. You can modify the testing environment *during* the test by clicking the Options button.

## Certification Mode

Tests administered in Certification Mode closely simulate the actual testing environment you will encounter when taking a certification exam. These tests do not allow you to request the answer(s) or explanation for each question until after the exam.

## Custom Mode

Custom Mode allows you to specify your preferred testing environment. Use this mode to specify the objectives you want to include in your test, the timer length, and other test properties. You can also modify the testing environment *during* the test by clicking the Options button.

## Adaptive Mode

Tests administered in Adaptive Mode closely simulate the actual testing environment you will encounter when taking an adaptive exam. After answering a question, you are not allowed to go back; you are only allowed to move forward during the exam.

## Missed Question Mode

Missed Question Mode allows you to take a test containing only the questions you missed previously.

## Non-Duplicate Mode

Non-Duplicate Mode allows you to take a test containing only questions not displayed previously.

 PREV

NEXT 

## Question Types

The practice question types simulate the real exam experience.

 PREV

NEXT 

 PREV

NEXT 

## Random Questions and Order of Answers

This feature helps you learn the material without memorizing questions and answers. Each time you take a practice test, the questions and answers appear in a different randomized order.

 PREV

NEXT 

 PREV

NEXT 

## Detailed Explanations of Correct and Incorrect Answers

You'll receive automatic feedback on all correct and incorrect answers. The detailed answer explanations are a superb learning tool in their own right.

 PREV

NEXT 

## Attention to Exam Objectives

MeasureUp practice tests are designed to appropriately balance the questions over each technical area covered by a specific exam.

# Installing the CD

The minimum system requirements for the CD-ROM are as listed here:

- Windows 95, 98, ME, NT4, 2000, or XP
- 7MB disk space for testing engine
- An average of 1MB disk space for each test

## Note

If you need technical support, please contact MeasureUp at 678-356-5050 or email [support@measureup.com](mailto:support@measureup.com). Additionally, you'll find Frequently Asked Questions (FAQs) at [www.measureup.com](http://www.measureup.com).

To install the CD-ROM, follow these instructions:

1. Close all applications before beginning this installation.
2. Insert the CD into your CD-ROM drive. If the setup starts automatically, go to step 6. If the setup does not start automatically, continue with step 3.
3. From the Start menu, select Run.
4. Click Browse to locate the MeasureUp CD. In the Browse dialog box, from the Look In drop-down list, select the CD-ROM drive.
5. In the Browse dialog box, double-click on **Setup.exe**. In the Run dialog box, click OK to begin the installation.
6. On the Welcome Screen, click Next.
7. To agree to the Software License Agreement, click Yes.
8. On the Choose Destination Location screen, click Next to install the software to **C:\Program Files\MeasureUp Practice Tests\Launch**.

## Note

If you cannot locate MeasureUp Practice Tests through the Start menu, see the section

later in this appendix titled "[Creating a Shortcut to the MeasureUp Practice Tests](#)."

9. On the Setup Type screen, select Individual Typical Setup. Click Next to continue.
10. On the Select Features screen, click the check box next to the test(s) you purchased. After you have checked your test(s), click Next.
11. On the Enter Text screen, type the password provided in this receipt and click Next. Repeat this step for any additional tests.
12. On the Select Program Folder screen, verify that the Program Folder is set to MeasureUp Practice Tests, and click Next.
13. After the installation is complete, verify that Yes, I Want to Restart My Computer Now is selected. If you select No, I Will Restart My Computer Later, you will not be able to use the program until you restart your computer.
14. Click Finish.
15. After restarting your computer, choose Start, Programs, MeasureUp Practice Tests, Launch.
16. On the MeasureUp welcome screen, click Create User Profile.
17. In the User Profile dialog box, complete the mandatory fields and click Create Profile.
18. Select the practice test you want to access and click Start Test.

## **Creating a Shortcut to the MeasureUp Practice Tests**

To create a shortcut to the MeasureUp Practice Tests, follow these steps:

1. Right-click on your desktop.
2. From the shortcut menu, select New, Shortcut.
3. Browse to `C:\Program Files\MeasureUp Practice Tests` and select the `MeasureUpCertification.exe` or `Localware.exe` file.
4. Click OK.
5. Click Next.
6. Rename the shortcut MeasureUp.
7. Click Finish.

After you have completed step 7, use the MeasureUp shortcut on your desktop to access the MeasureUp products you ordered.

**◀ PREV**

**NEXT ▶**

## Technical Support

If you encounter problems with the MeasureUp test engine on the CD-ROM, you can contact MeasureUp at 678-356-5050 or email [support@measureup.com](mailto:support@measureup.com). Technical support hours are from 8 a.m. to 5 p.m. EST Monday through Friday. Additionally, you'll find Frequently Asked Questions (FAQs) at [www.measureup.com](http://www.measureup.com).

If you'd like to purchase additional MeasureUp products, telephone 678-356-5050 or 800-649-1MUP (1687), or visit [www.measureup.com](http://www.measureup.com).

## B. Need to Know More?

Citrix provides an extensive set of PDF-based documents that can be found both on the MetaFrame Presentation Server CD-ROM installation media and downloaded from its website at <http://support.citrix.com>. All documentation found online can be referenced by the Citrix Knowledgebase Article number, a unique number that is prefixed by the letters CTX. From the <http://support.citrix.com> URL, there is a search box within which you can enter the appropriate CTX reference number and quickly retrieve the associated document. Because Citrix may change the exact URL that loads a particular document, this reference appendix lists the relevant documents and provides the corresponding CTX number instead of a full URL to the download location. This way, you will be able to find the appropriate document regardless of where Citrix may actually store it on its website.

# Chapter 1



Citrix Systems, "Getting Started with MetaFrame Presentation Server 3.0." Available from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Getting Started with MetaFrame Presentation Server 4.0." Available online with KB article number CTX106301 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 2



Citrix Systems, "Getting Started with MetaFrame Presentation Server 3.0." Available from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Getting Started with MetaFrame Presentation Server 4.0." Available online with KB article number CTX106301 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 3



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Migration and Upgrade GuideMetaFrame Presentation Server 3.0." Available online with KB article number CTX104486.

## Chapter 4



Citrix Systems, "MetaFrame Access Suite Licensing Guide." Available online with KB article number CTX102833 and from the documentation provided with the MetaFrame Presentation Server 3.0/4.0 installation CD-ROM.



Citrix Systems, "MetaFrame Access Suite License Server Customizations." Available online with KB article number CTX103955.



Citrix Systems, "Citrix Access Suite Licensing Guide." Available online with KB article number CTX106282.



Citrix Systems, "MetaFrame Access Suite License Server 4.0 Readme EN." Available online with KB article number CTX105718.

## Chapter 5



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Pre-Installation Checklist" (checklist.html). Available online with KB article number CTX103879 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Installation Checklist" (checklist.html). Available online with KB article number CTX105728 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 6



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Advanced Concepts Guide MetaFrame Presentation Server for Windows Version 3.0." Available online with KB article number CTX104144.



Citrix Systems, "Advanced Concepts Guide." Available online with KB article number CTX107059.

## Chapter 7



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Extended Policies FAQ." Available online with KB article number CTX103793.

## Chapter 8



Citrix Systems, "Administrator's GuideLoad Manager for MetaFrame Presentation Server 3.0." Available online with KB article number CTX103744 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Load Manager Administrator's Guide." Available online with KB article number CTX106452 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 9



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Citrix MetaFrame Presentation Server 3.0 Security Standards and Deployment Scenarios." Available online with KB article number CTX105749.

## Chapter 10



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 11



Citrix Systems, "Installation Manager Administrator's Guide." Available online with KB article number CTX103718 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Installation Manager Administrator's Guide." Available online with KB article number CTX106469, and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Installation Manager Application Compatibility Guide." Available online with KB article number CTX106516.

## Chapter 12



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

## Chapter 13



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Client for 32-bit Windows Administrator's GuideVersion 8.x." Available online with KB article number CTX103754 and from the documentation provided with the MetaFrame Presentation Server 3.0 Components CD-ROM.



Citrix Systems, "Client for 32-bit Windows Administrator's GuideVersion 9.0." Available online with KB article number CTX106223 and from the documentation provided with the MetaFrame Presentation Server 4.0 Components CD-ROM.



Citrix Systems, "Presentation Server Program Neighborhood Client for 32-bit Windows Configuration Guide (INI File Reference), version 9." Available online with KB article number CTX 107102.

## Chapter 14



Citrix Systems, "Web Interface Administrator's Guide." Available online with KB article number CTX103761 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Web Interface Administrator's Guide." Available online with KB article number CTX106472 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Secure Gateway for Windows Administrator's Guide." Available online with KB article number CTX103759 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Secure Gateway 3.0 for Windows Pre-installation Checklist." Available online with KB article number 106311 and from the documentation provided with the MetaFrame Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "Secure Gateway 3.0 for Windows Administrator's Guide." Available online with KB article number CTX106300 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 3.0 for Windows Administrator's Guide." Available online with KB article number CTX103723 and from the documentation provided with the MetaFrame

Presentation Server 3.0 installation CD-ROM.



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

PREV

NEXT

 PREV

NEXT 

## Chapter 15



Citrix Systems, "Resource Manager Administrator's Guide." Available online with KB article number CTX106471 and from the documentation provided with the MetaFrame Presentation Server 3.0/4.0 installation CD-ROM.

 PREV

NEXT 

## Chapter 16



Citrix Systems, "MetaFrame Presentation Server 4.0 Administrator's Guide." Available online with KB article number CTX106319 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Installation Manager Administrator's Guide." Available online with KB article number CTX106469 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Web Interface Administrator's Guide." Available online with KB article number CTX106472 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.



Citrix Systems, "Secure Gateway 3.0 for Windows Administrator's Guide." Available online with KB article number CTX106300 and from the documentation provided with the MetaFrame Presentation Server 4.0 installation CD-ROM.

# Glossary

## ACS

See [\*Application Compatibility Script\*](#).

## ADF packages

Packages created using the Packager application included as part of Installation Manager.

See also [\*Installation Manager packages\*](#).

## administrative delegation

The process of assigning server farm administrative and management privileges to users or groups from Microsoft Active Directory or Novell Directory Services. Custom privileges can be assigned to different nodes in the Management Console, or the generic Full authority or View-only authority privileges can be assigned. The first administrator created when the farm is created is assigned Full authority privileges.

## alert threshold

A user-defined value at which an event, typically a user notification, occurs. Event thresholds can be defined within both the License Management Console and the Resource Manager. Within the License Management Console, thresholds can be set for license usage, subscription advantage date, and license expiration date. Within the Resource Manager, an alert threshold can be defined for change in metric state.

## allow access

A policy filter state that applies the policy to all objects that meet the filter criteria.

## Application Compatibility Script (ACS)

A script used to ensure that legacy Windows-based applications function properly in a MetaFrame environment. Often these applications are designed as single-user applications and don't implicitly provide support for multiple concurrent user sessions. An ACS can be executed when the application is installed and/or whenever the application is launched. Scripts are initiated by the USRLOGON.CMD batch script.

## Application Isolation

The segregation of an application into a virtual execution environment on a Presentation Server. Within this virtual execution environment, the application is isolated from other applications and components on the server, protecting both the application and other processes in the environment from undesirable interaction.

Isolation is achieved through the virtualization of the *file system*, *Registry* and *named objects*, all of which are key operating system resources.

## Application Server mode

Server mode that places the Windows server into the multiuser access mode required for running MetaFrame Presentation Server or Terminal Services by itself. The number of concurrent user sessions allowed on the server is limited only by the number of Client Access Licenses available and the limit configured on the server.

When the Terminal Services component is installed on a Windows 2000 Server, you are given the choice to configure either Application Server mode or Remote Administration mode. When the Terminal Services component is installed on a Windows Server 2003 server, it automatically places the server into Application Server mode. The Remote Administration mode is available by default on all Windows Server 2003 servers.

See also [Remote Administration mode](#).

## appsrv.ini

The main configuration file for Program Neighborhood. All connection and client configuration settings for PN are stored in this file, which is copied from the main program folder the first time a user executes the PN and is stored in the Application Data\ICAClient folder of the user's profile. This file can be customized prior to the PN installation to define common settings and configure certain components of the user interface. Prior to installation, the file is called appsrv.src.

See also [pn.ini](#).

## APPUTIL

A command-line utility that allows you to perform basic published application and application deployment tasks.

## asynchronous writes

Presentation Server policy rule designed to enhance the performance of disk write operations from a MetaFrame server to a client-mapped drive. The asynchronous writes rule is designed for high bandwidth and *high latency* client/server connections and is not appropriate for users who are not operating in a high latency environment. This rule is new in MPS 4.0.

See also [MetaFrame user policy](#).

authentication ticket

See [session ticketing](#).

auto client reconnect

Automatic attempt to reconnect to the server if a client is disconnected due to a network or device failure.

auto client update

Automatic update of a client based on settings in the Client Update Database.

auto proxy discovery

An ICA client feature that can be configured to attempt to retrieve the proxy settings from the default web browser for the device.

If the default browser is Internet Explorer and it is configured to automatically detect settings, the Win32 client ignores these settings and attempts a direct connection.

automatic printer detection

Automatic detection and mapping of client printers in a Presentation Server session.

billing report

A report generated by Resource Manager giving an associated cost with a particular resource's usage. Two types of billing reports can be generated. The first is a Cost Center report, typically created to bill a cost center for usage. At least one fee profile and cost center must be defined in Resource Manager before this report can be generated.

The other billing report is a Domain Users report. This report is used to generate resource usage bills to individual users or groups. The generation of this report requires only one fee profile.

See also [cost center](#), [fee profile](#).

browser acceleration

SpeedScreen feature that enhances a web browser when running Internet Explorer 5.5 or later.

CAL

See [Client Access License](#).

CAS

See [Citrix Activation System](#).

CCC

See [Citrix Connection Configuration](#).

certificate

See [digital certificate](#).

certificate authority (CA)

A trusted source that issues digital certificates to requestors. A CA can be a third-party organization, or it can be internal to an organization, employing certificate-generating software such as Microsoft Certificate Services. One advantage of using a third-party organization such as VeriSign is that most operating systems (Windows, Mac, Linux, for example) include root certificates that verify the identity of these organizations and imply a trust relationship in the validity of certificates they issue. Root certificates generated by internal certificate services are not distributed by default, requiring you to ensure these certificates are distributed to the appropriate clients as required.

Citrix Activation System (CAS)

Citrix's Web application for configuring and downloading the license file for your MetaFrame Access Suite License server. It is accessed through the MyCitrix.com web portal.

Citrix Connection Configuration (CCC)

Citrix's utility for managing the configuration of ICA and RDP connections on a Presentation Server. It provides certain ICA-specific settings not found in the Terminal Services Configuration utility.

Citrix connection license

A valid license that must be available for check out on the Access Suite License Server for each concurrent user who logs on to a Presentation Server. This file remains locked for the duration of the user's active connection(s) in the farm. After the user is logged out, the license is returned to the license server, where it is available for use by other users. The appropriate number of connection licenses is downloaded within a license file from the MyCitrix.com web portal.

## Citrix ICA Client

See [\*Presentation Server client\*](#).

## Citrix server farm

Presentation Servers grouped in a logical management unit, all sharing a common database of information called a Data Store.

## Citrix SSL Relay

A service available by default on MetaFrame Presentation Server that allows for the creation of a secure SSL-based communication link between the client and a Presentation Server. SSL Relay can provide secure access to the Citrix XML Service for retrieving server farm information and processing authentication requests. SSL Relay can also be used to establish a secured and authenticated connection with a Presentation Server client or the Secure Gateway for the MetaFrame Access Suite.

## Citrix startup license

A special product license automatically added to the Access Suite License Server after it has been installed. When a Presentation Server first starts, it attempts to contact the License Server to request a valid startup license. Once acquired, the license entitles the Presentation Server to communicate and request Citrix connection licenses whenever a user accesses published content on the server.

## Citrix universal printer driver (UPD)

A Citrix printer driver that can substitute for the native driver associated with a client printer. The UPD allows support for printers that may not have a driver that can run on Presentation Server or simply to reduce the number of unique drivers that must be installed on the server. A UPD can be substituted only for client-mapped printers. It is not used on the local client, nor is it available as a substitute driver for printer mappings created directly within a Presentation Server session.

## Citrix Web client

The smallest of the Win32 clients. The Web client is available in two types. One is the *full Win32 Web client*, which is also the default client deployed to all Win32 users connecting to the Web Interface without already having a local client. The other Web client, commonly referred to as the *minimal Web client*, has a number of components stripped out in order to make it the minimal size possible for download and execution.

## Citrix XML Service

The service responsible for providing server farm information to various requesting systems, such as the Presentation Server clients or the Web Interface for Presentation Server. Unlike the legacy ICA Browser, this service transmits information using TCP, not UDP. The default port for the XML Service is port 80.

## Client Access License (CAL)

The individual user license that is required to connect to a computer system. Both Citrix Presentation Server and Microsoft Terminal Server require their own unique client access licenses in order for users to be legally able to connect to a server. Citrix supports concurrent user licensing, allowing you to purchase only the licenses required for the maximum number of users on the server at any one time. Microsoft, on the other hand, requires per-user or per-device licenses. This means that a license is required for every user or device that will connect to a Terminal Server, regardless of how many of them are connecting concurrently. Terminal Server CALs are required even when you are running Presentation Server.

See also [\*Citrix connection license\*](#).

## client device mapping

A Presentation Server feature that allows access to the local client device from within the MetaFrame session. The supported devices include drives, printers, COM ports, audio (client-to-server and server-to-client), and the Clipboard. MPS 4.0 also includes support for client-side TWAIN devices such as scanners and Microsoft-powered PDA devices connected to a client via USB and supporting ActiveSync synchronization software.

## client printer

Any printer that is locally accessible from the client device. This includes printers physically attached to the client; network-based printers accessible through a printer share or alternate means such as TCP/IP port; and virtual printers such as Adobe Acrobat, email, or fax printers.

See also [\*local printer\*](#), [\*network printer\*](#).

## client-side proxy

A settings page in the Web Interface console. Settings are configured on this page when you have remote clients that have local proxy servers between themselves and your server. Through these settings, you are able to define whether client connections to the Presentation Servers must go through those client-side proxy servers. By defining these settings on the Web Interface, you can manipulate their ICA client settings, ensuring that they can successfully connect to the Presentation Server.

## Client Update Database

A database that can be configured centrally among a number of Presentation Servers or can be

maintained separately on each one. This database contains client installation images that can be pushed out to the client when it detects a newer version of the product for installation. An ICA client must already exist on the client machine to perform an automatic update. The Client Update Database is a client update tool. It cannot be used to configure deployment of a Presentation Server client to new client devices.

## Components CD

The companion CD-ROM available as part of the Presentation Server installation package. The Components CD contains installation sources for a number of nonPresentation Server products such as Presentation Server client installation files, Secure Gateway installation components, MetaFrame Conferencing Manager, and the Document Center. As part of the Web Interface installation, the Components CD is one option from which to retrieve the client installation images.

## content publishing

A feature that supports accessing content similar to accessing published applications. Published content can include any type of file such as a document, web link, or media file.

## content redirection (client-to-server)

Integrated support available only through PN Agent; it requires the Enterprise or Advanced Edition of Presentation Server. It allows local file associations to open applications published in the farm.

See also [extended parameter passing](#).

## content redirection (server-to-client)

Server-based file association that can open applications running locally on the client device. For example, a web link could be opened using a local Internet Explorer instead of the browser on the server.

## cost center

Individual users or groups defined within Resource Manager to group resource usage and generate cost center billing reports.

See also [billing report](#), [fee profile](#).

## CPU utilization management

A Presentation Server 4.0 farmwide or per-server setting intended to improve the server's ability to manage CPU resources. By modifying the normal priority scheduling for processes in the system, Citrix is able to reduce both the frequency of application processing spikes and the

resources reserved for coping with these spikes.

This feature is available only in the Enterprise Edition of MPS 4.0. To enable or disable it, simply check the option in the Memory/CPU Utilization Management property for the server farm node or the node of an individual server.

See also [memory optimization](#).

## cross-farm license sharing

A configuration in which two distinct server farms both share licenses from one common MetaFrame Access Suite License server.

## database connection server

A component of Resource Manager that is responsible for collecting summary data information from all Presentation Servers, including the farm metric server, and writing this information to the Summary database.

See also [farm metric server](#), [Summary database](#).

## data collector

See [zone data collector](#).

## Data Store

The central ODBC-compliant database for a server farm where persistent farm information such as published applications and printer information is maintained. The supported database management systems are Microsoft Access, Microsoft SQL Server 2000 Desktop Engine, Microsoft SQL Server, Oracle, and IBM DB2.

## demilitarized zone (DMZ)

A subnetwork situated between a trusted internal network and an untrusted external network such as the Internet. This subnetwork is usually located between an external and an internal firewall, but it can also be located off a single external network. Servers are placed into this DMZ and can be accessed by clients on the untrusted network. This zone is created with the intention of segregating these servers so that if one is compromised, it does not allow unconstrained access to the internal network.

See also [double-hop DMZ](#), [single-hop DMZ](#).

## deny access

A policy filter state that does *not* apply the policy to all objects that meet the filter criteria.

## digital certificate

An electronic document that is presented by users or computers to verify they are who they say they are. The certificate can also contain a public encryption key that is then used to send encrypted messages back to the certificate presenter. Digital certificates are issued by trusted sources known as certificate authorities (CAs).

## double-hop DMZ

A setup that provides additional security by requiring traffic from the Internet to pass through two DMZs before accessing systems on the internal network. Servers placed in the first stage have no direct access into the internal network but are configured to have limited access to specific machines within the second DMZ. Only systems in the second DMZ are configured with access to servers on the internal network.

See also [demilitarized zone](#), [single-hop DMZ](#).

## driver compatibility

A Presentation Server feature that enables you to configure the farm to allow or restrict specific printer drivers from being installed on servers in the farm. By default, all printer drivers are permitted. This setting affects only client-mapped printers. It has no effect on the mapping of network printers from within Presentation Server.

## driver auto-replication

See [printer driver auto-replication](#).

## driver mapping

See [printer driver mapping](#).

## dynamic session resizing

The ability of a user to resize a desktop session dynamically. For example, user can change a 1024x768 session to 1280x1024 on the fly. The size can also be reduced if desired. Desktop contents are adjusted as required to fit within the new display size.

## extended parameter passing

The capability to associate a local file type with a published application. This requires configuration on both the client and server to function properly. This feature provides functionality equivalent to client/server content redirection, a feature available only with PN

Agent.

See also [content redirection \(client-to-server\)](#).

## farm metric server

By default, the first server upon which Resource Manager is installed in a server farm. The farm metric server is responsible for gathering metric information from other Presentation Servers, interpreting the results, and raising alerts if necessary.

## fee profile

A report that contains a cross-reference of rates to charge for resource usage. It associates a cost with resource usage and is used by Resource Manager when generating a billing report. Multiple fee profiles can be defined and used to calculate resource usage costs.

See also [billing report](#).

## Flash acceleration

See [SpeedScreen Flash Acceleration](#).

## Ica32Pkg client package

A consolidated installation bundle in which all three Win32 clients are available. This Ica32Pkg.msi package can also be used to create customized installations containing only the desired Win32 clients.

## ICA asynchronous connection

A type of dial-in connection that allows clients to directly dial in to a MetaFrame Presentation Server without the additional overhead or configuration requirements of Microsoft's Remote Access Services (RAS). Direct dial-in requires that one or more modems be directly connected to a Presentation Server and properly configured for dial-in access. Asynchronous connections are configurable only on Windows 2000 Terminal Servers. Windows Server 2003 and hence Presentation Server does not support asynchronous client connections.

## ICA browsing

The process of discovering Presentation Servers or published content in a server farm. The Citrix XML Service provides HTTP-based browsing services via port 80 by default on all Presentation Servers. Legacy ICA browsing support is provided for MetaFrame 1.8 users via directed UDP or broadcast UDP connections on port 1604. Directed UDP browsing is supported by default in Presentation Server, but UDP broadcast listening is not enabled by default. The Broadcast Response setting must be enabled in the Management Console before this functionality is enabled.

See also [Interoperability mode](#).

## ICA Browser Service

A service that manages legacy ICA browsing support via UDP on port 1604. In MetaFrame 1.8, this was an actual Windows service called ICA Browser. Now, the IMA Service provides integrated support by listening on port 1604.

## ICA Client Creator

A utility available only on Windows 2000 Server systems that allows you to create client installation diskettes for the Win32, Win16, DOS, and Web clients.

## ICA Client Distribution Wizard

A wizard provided with Presentation Server that allows you to install or update the ICA client images on a MetaFrame server and in the Client Update Database, as well as install or update the ICA Pass-Through client. The ICA Client Distribution Wizard is automatically run during Presentation Server installation.

## ICA Client Printer Configuration

Legacy MetaFrame tool used to manually map client printers from within a MetaFrame session. This tool can still be used to map any available client printers, but it was created primarily to allow DOS and Windows CE clients to map printers because they could not automatically be created. The tool is no longer required for DOS or Windows CE clients. The desired client printer mappings can be defined within the farm and automatically applied when the DOS or WinCE clients connect.

## ICA Client Update Configuration

A utility used to manage the Client Update Database.

## ICA Dial-In

See [ICA asynchronous connection](#).

## ICA encryption

Citrix's native encryption support for the ICA protocol, also known as SecureICA. ICA traffic can be secured using different key strengths up to 128-bit. Encrypting ICA traffic makes it more difficult for someone to intercept and view session transmissions. ICA encryption does not provide server authentication, making it susceptible to man-in-the-middle attacks. Citrix does

not recommend the use of ICA encryption for securing communications over an insecure network (Internet). Instead, Citrix recommends that you use the SSL support provided with the Presentation Server clients and the SSL Relay service. This provides strong encryption as well as the server authentication features not found in the ICA protocol.

## ICA file

A plain-text file (usually with an .ica extension), containing information on a published application. The file contents, organized in Windows INI file format, can be loaded and interpreted by Presentation Server clients. ICA files are passed by the Web Interface to a client session, allowing the client to parse the file and extract the necessary information to establish the connection with the specified server, running the specified application.

## ICA keep-alive

A property of the server farm that configures the servers in the farm to periodically send packets to the client to verify that the connection is still active. If the client fails to respond, the server places the client into the disconnect state. This property is commonly used when clients lose their connection to the server, but their session remains in the active state and does not disconnect properly.

## ICA Pass-Through client

Either the Program Neighborhood or Program Neighborhood Agent client, which can be installed on a server and used to provide users of non-Windows client devices with access to run PN or PN Agent as a published application. This allows them to take advantage of the features of these clients regardless of their local device's operating system or configuration.

## ICA shadowing

A technique that allows remote viewing or controlling of another user's ICA server session; it is referred to as *remote control* when describing a similar technique using the Microsoft RDP. Depending on the server configuration, the shadower can either passively view the shadowed user's session or can interact with mouse and keyboard input. Shadowing is a powerful support and training tool because it provides an administrator with the ability to interact with another user regardless of physical location. Leveraging the functionality of the ICA protocol ensures that the overhead of shadowing is minimal, allowing the user to operate normally while the administrator assists in the issue at hand. Shadowing is also commonly used to provide remote training and coaching for users.

## ICA template file

A special type of ICA file containing substitution tags instead of hard-coded connection settings. These tags are replaced with the appropriate values by the Web Interface when generating a custom ICA file. The default template file used with the Web Interface is called template.ica.

See also [ICA file](#).

## ICA Toolbar

A simple management toolbar that appears, by default, down the right side of the desktop for any administrator who logs on to a Presentation Server. It provides a means of quickly launching the commonly used Citrix utilities. The toolbar can be customized or disabled if desired.

## IMA

See [\*Independent Management Architecture\*](#).

## image acceleration

A SpeedScreen feature by which images are compressed before being sent to the client.

## Independent Computing Architecture (ICA) protocol

Citrix's Presentation Services protocol that allows a client to establish a session with a MetaFrame server and access server-based applications and content as if they were available locally on the client. ICA is platform independent, allowing access to a Presentation Server from almost any client platform. The functionality supported via the ICA protocol is extensible by way of virtual channels. A single ICA protocol packet is broken down into seven components, six of which are optional based on the data being transmitted. The seven components are

- Frame Head (optional)
- Reliable (optional)
- Encryption (optional)
- Compression (optional)
- Command
- Command Data (optional)
- Frame Tail (optional)

## Independent Management Architecture (IMA)

The management architecture foundation for the Presentation Server farm but also the name of the associated protocol that is employed for the server-to-server management communications. The ability to centrally manage any number of Presentation Servers, regardless of their location, is made possible by IMA. The IMA protocol is UDP-based, communicating from server to server via port 2512. Connections from the Management Console for Presentation Server are serviced on port 2513.

## Installation Manager packages

Collectively, any applications or other software components to be deployed within Installation Manager. Installation Manager supports three types of package formats: Microsoft Windows Installer packages (MSI), Microsoft Windows Installer patch files (MSP), and ADF packages. ADF packages are created using the Packager application provided with Presentation Server, Enterprise Edition. Packages can contain installation recordings, unattended installations, as well as individual folders or files.

## Interoperability mode

Mode of operation that provides backward compatibility with MetaFrame 1.8, allowing for the transparent introduction of new Presentation Servers into an existing 1.8 server farm. It is also referred to as *mixed mode*. Interoperability mode is not supported in MPS 4.0. If this support is required for migration from a MetaFrame 1.8 environment, MPS 3.0 is required.

## Kerberos client authentication

Alternate method of user authentication that does not send the user's password across the network. Kerberos is an industry-standard network authentication system that allows machines communicating over networks to prove their identity to each other. Kerberos authentication requires that both the server and the clients belong to the same or trusted Windows 2000 or 2003 domains. Version 8.x or higher of the Win32 MPS client supports the use of Kerberos authentication.

## LHC

See [Local Host Cache](#).

## License Management Console

A web-based application that must be installed and run on the same server as the MASL component. It provides a GUI front end to manage licenses in the farm.

## license server failure grace period

A period of time in which the MetaFrame server farm will allow user connections even without the availability of an Access Suite License Server before user access is suspended. If a MetaFrame server loses connectivity to a license server due to a license server failure, network issues or some other problem, the MetaFrame server immediately begins operating in a fail-over mode, which has a separate grace period of operation before the license server must once again be available. The time frame for the "fail-over" grace period is 30 days. For the fail-over grace period to be valid, the license server must have a valid license file installed. A license server with no valid license file does not allow a MetaFrame server to function in "fail-over" mode.

See also [start-up grace period](#).

## load evaluator

A set of rules that define how the load for a server is calculated by the Load Manager. The calculated value is used to determine the least-loaded server available in a farm for a given published application.

## Load Manager

A utility available in the Advanced and Enterprise Editions that allows published applications to be load-balanced across multiple Presentation Servers. When users connect to a published application, they are directed by the Load Manager to the least-loaded server.

## Local Host Cache (LHC)

A special access database in which a subset of the Data Store is maintained on each server in the farm. This cache exists to provide Presentation Servers with quick access to Data Store information, as well as redundancy of Data Store information in the event that the server hosting the Data Store is unavailable. By default, the LHC can be found in %ProgramFiles%\Citrix\Independent Management Architecture\IMALHC.MDB.

When changes are made to the Data Store, each Presentation Server in the farm is notified of the change, which in turn causes it to refresh its Local Host Cache.

Presentation Servers also periodically query the Data Store for changes and update their Local Host Cache if required. The default query interval is 30 minutes, but this period can be adjusted by modifying the Registry on each server.

## local printer

A printer that is directly connected to any MetaFrame server within a server farm. *Directly connected* can mean one of two things: Either the printer is physically connected to a MetaFrame server through an LPT or USB port, or a logical printer port has been configured that directs the print job to the remote queue for that printer. A TCP/IP printer port is one of the most common configurations, but third-party ports such as Lexmark or HP JetDirect can also be defined.

See also [client printer](#), [network printer](#).

## Management Console for MetaFrame Presentation Server

The main management tool for Presentation Server server farms.

## management nodes

The different nodes within the Management Console that provide access to server farm management and configuration features. The available nodes are

- Applications
- MetaFrame Administrators
- Installation Manager
- Isolation Environments (MPS 4.0 only)
- Load Evaluators
- Policies
- Printer Management
- Resource Manager
- Servers

## memory optimization

A Presentation Server 4.0 farmwide or per-server setting intended to reduce the overall virtual memory usage on a server by optimizing the load order of the DLLs for an application. Proper DLL load optimization can greatly reduce the amount of memory required to run an application, freeing up server resources and improving server stability and performance.

The optimization of virtual memory is scheduled through the Memory Optimization properties for the farm or an individual server. Citrix recommends that optimization tasks be performed when user load on the server is low. When enabled, memory optimization is performed daily at 3 a.m. by default. Applications that are adversely affected by the optimization can be explicitly excluded from this process.

Memory optimization is available only in the Enterprise Edition of MPS 4.0.

See also [CPU utilization management](#).

## MetaFrame Access Suite Licensing (MASL)

Citrix's integrated licensing infrastructure that relies on a central server that performs all license management for the various Access Suite products. This server is responsible for storing and issuing licenses when requested. Unlike earlier versions of MetaFrame that required the entry of license and activation codes directly within the Management Console, a license file is downloaded and stored directly on the license server. The information contained within this file is used by the license server to determine characteristics such as the types of licenses and the quantity available for use.

## MetaFrame platform solution

The three different Presentation Server categories available. They are Standard Edition,

Advanced Edition, and Enterprise Edition.

## MetaFrame universal printer driver

See [Citrix universal printer driver](#).

## MetaFrame user policy

A policy that allows an administrator to apply certain MetaFrame server settings to users based on their connection criteria and, hence, tailor the computing experience differently for different users. MetaFrame user policies are managed under the Policies node located in the Management Console for MetaFrame Presentation Server.

See also [management nodes](#).

## metrics

Performance-measuring units based on the operating system's performance counters; they are used by Resource Manager to determine a resource's current load. Thresholds in Resource Manager are set to trigger when a certain metric value is met or exceeded.

See also [alert threshold](#).

## minimum required encryption level

Configuration setting for published applications that sets the minimum encryption level setting that must be defined on the client to be able to launch the application. By enforcing a minimum encryption level, you control what type of ICA encryption is being used. This setting does not affect the use of SSL for client connections.

## mixed mode

See [Interoperability mode](#).

## MSI packages

Packages based on the Microsoft Windows Installer Service. They can be deployed using Installation Manager. Installation Manager cannot create MSI packages.

See also [Installation Manager packages](#).

## MSP packages

Patch packages based on the Microsoft Windows Installer Service. They can be deployed using

Installation Manager but, like MSI files, cannot be created with Installation Manager.

See also [Installation Manager packages](#).

## Multimedia Acceleration

See [SpeedScreen Multimedia Acceleration](#).

## MultiWin

The technology developed by Citrix to allow multiple users to simultaneously share resources and run applications on a central server. Each user operates in a session isolated from other sessions on the server. Microsoft has licensed the MultiWin technology from Citrix and incorporated it into Windows to produce Terminal Services.

## MyCitrix.com

Citrix's customer Web portal where you manage subscription advantage membership and license activations, as well as download media and access support options. With your subscription advantage membership, you receive access to a wide variety of features in your personal MyCitrix portal.

## network address translation (NAT)

A process that allows computer systems on private networks to access resources on the Internet without requiring a public Internet address. With NAT, networks can use one set of "internal" addresses for their computers and have the return address of packets originating from those internal machines automatically changed to a valid external address when they pass onto the Internet. Return packets are automatically changed so that their destination points back to the appropriate internal system. This address translation process is transparently managed on an external router or firewall without any configuration required on the client.

## network printer

Any printer that is connected to a print server and shared on a Windows network. This type of printer is accessible directly within a Presentation Server session just as it would be from a local Windows desktop. If a network printer is mapped on a local client device, from a MetaFrame session, it is considered to be a client printer, not a network printer. Only when a shared network printer is mapped from within a MetaFrame session is it considered a network printer.

See also [client printer](#), [local printer](#).

## Network Share Point Server

A standard Windows network drive share on the network where Installation Manager packages are stored and retrieved for distribution.

## Package Management Server

A Presentation Server in the farm assigned the role of configuring and deploying application packages via Installation Manager, a component of the Management Console. The Presentation Server does not have to be dedicated hardware.

## Package Server

The role assigned to a Presentation Server chosen as the source for ADF package creation. ADF packages are created using the Citrix Packager application and deployed using Installation Manager. Citrix recommends that a server with a configuration identical to other production servers but with no (or very limited) user sessions be dedicated as the Package Server for Installation Manager.

## panning

The action of scrolling around the desktop view to see different portions at one time when the Presentation Server window size is larger than the actual client desktop size.

See also [scaling](#).

## pass-through authentication

The use of local user credentials to automatically authenticate and access resources on the server.

## Pass-Through client

See [ICA Pass-Through client](#).

## pn.ini

The companion file to appsrv.ini for Program Neighborhood. This file contains the properties for all defined application sets in the client. A copy resides in the same location as appsrv.ini for each user who has run PN. Prior to installation, this file is called pn.src.

See also [appsrv.ini](#).

## PN

See [Program Neighborhood](#).

## PN Agent

See [Program Neighborhood Agent](#).

## policy filter

Criteria created to enforce one or more policies on a set of users, client devices, and/or servers. Filters can be created on any combination of client IP address, client name, username or group name, and Presentation Server name.

## policy priorities

Priority rankings given to MetaFrame policies, starting at 1, the highest, and lowering in priority as the value increases. The closer the priority number to 1, the higher the ranking compared to other policies. If two policies define the same policy rule, the policy with the higher ranking takes precedence.

## policy rule

A directive that dictates the configuration of a specific setting within a MetaFrame policy. A MetaFrame policy is made up of one or more rules. A rule can be in one of three states: not configured, disabled, or enabled. When the same rule is defined in more than one policy, an order of precedence is applied to determine the final state of the rule.

See also [policy priorities](#).

## preferred package

A package that you define as being the default from which Installation Manager retrieves the source files for a publish application deployment. An application can reside within multiple packages. When deploying an application via application publishing, you should define a preferred package for that application so that Installation Manager knows from what package to draw the application during the installation.

## Presentation Server client

Any device capable of establishing a client session with a Presentation Server. The device must understand the Citrix ICA protocol. Currently, Citrix maintains a mixture of names for clients on different platforms. For example, Win32 clients are now called Clients for Presentation Server, whereas Linux clients are still called ICA Clients for Linux. Regardless of the name, they are both considered Presentation Server clients.

## printer driver auto-replication

Process by which printer drivers (files and associated Registry keys) for a given platform are

automatically copied to all servers in the farm. You access printer driver auto-replication by right-clicking on the Drivers node under Printer Management in the Management Console for MetaFrame Presentation Server. Printers listed for a given platform are automatically replicated from the given source to all other servers running the same platform in the farm. Drivers from a Windows Server 2003 server will not replicate to a Windows 2000 Server and vice versa.

## printer driver mapping

A cross-reference mapping between a client printer driver name and the corresponding server printer driver name. Because Presentation Server matches client printer drivers to server printer drivers based on the driver name, if the client and server names do not match then a mapping cannot take place. By creating a printer driver mapping, you provide Presentation Server with a means of associating the client printer driver with a server driver, ensuring the client printer connection is created. This problem is most common with legacy clients such as Windows 95. You can also use printer driver mappings to substitute a more generic and stable driver for one that may be known to have issues in Presentation Server.

## Program Neighborhood (PN)

One of the three Win32 clients. Program Neighborhood is considered to be the "full" Presentation Server client. It provides support for accessing application sets within individual farms and presenting the corresponding icons based on the credentials provided by the end user. PN also allows you to create individual connection shortcuts to published applications or specific server names. PN is recommended only for power users or administrators because this client does not provide centralized management capabilities. Once it is deployed, if changes must be made to the configuration, they must be made on the desktop, either from within the PN GUI or by directly manipulating the user's personal configuration files. The two main configuration files for PN are appsrv.ini and pn.ini.

## Program Neighborhood Agent (PN Agent)

One of two Win32 clients that reads configuration information from a central location and is managed through a web-based management console on the Web Interface. PN Agent is managed using the Program Neighborhood Management Console. It has a very small footprint on the client desktop, appearing only as an icon in the System Tray. The options that can be configured locally are dictated by settings defined in the PN Agent Management Console. Icons for application set information retrieved by PN Agent can be displayed in a number of different locations including the client's desktop, the Start menu and within the System Tray icon.

## Program Neighborhood Agent Console

The Web-based management console for the Program Neighborhood Agent client. The PN Agent Console is included as part of the Web Interface and is accessed with the following URL: <Web Server>/Citrix/PNAgentAdmin.

## Remote Administration mode

One of two modes of operation available when the Terminal Services component is installed on a Windows 2000 Server; the other is Application Server mode. When Windows 2000 Server is configured to run in Remote Administration mode, it allows a maximum of two concurrent Remote Desktop Protocol connections to the server. They are considered administration connections and do not require any additional licenses. When operating in Remote Administration mode, the server does not attempt to contact a Terminal Services Licensing service.

On a Windows Server 2003 server, Remote Administration mode is available by default. You are not required to install the Terminal Services component. The only thing required to enable Remote Administration mode is to enable Remote Desktop access from under the properties of My Computer.

See also [\*Application Server mode\*](#).

## Remote Desktop Protocol (RDP)

Microsoft's equivalent of Citrix's ICA protocol. RDP allows clients to establish a session on a Terminal Server and access server-based applications. Currently, RDP provides only a subset of the functionality available with the ICA protocol. Features such as seamless windows are not yet available. RDP is not a platform-dependent protocol, but Microsoft provides clients only for Windows 32-bit desktops and Apple Macintosh OS X. Some third-party and open source clients do exist for Unix- and Linux-based desktops.

## Remote Desktop Web Connection

An ActiveX client from Microsoft that uses the Microsoft RDP protocol instead of Citrix's ICA protocol to connect to a Terminal Server. Presentation Server provides basic support for the Remote Desktop Web Connection via the Web Interface, but most features that would be available to an ICA client are not available with this client.

## Report Center

A system management tool available through the Access Suite Console that provides extended reporting capabilities for Resource Manager.

## Resultant policy

The final set of policy rules applied to a given IP address, client name, user, user group, or server. It is determined by providing all the necessary information so that the final policy rule set can be determined.

## roaming user reconnect

See [\*Workspace Control\*](#).

## Root certificate

A special digital certificate used in conjunction with the certificate issued by a certificate authority (CA). By comparing the information in the root certificate with the data in the server certificate, the client can electronically verify the signature in the certificate. Assuming that the client trusts the root certificate, it can trust the information in the server certificate to be accurate.

## scaling

Shrinking a larger client session window to fit within a smaller client device desktop size.

## seamless windows

A feature that allows a published application to appear as if it is running locally on the client's desktop.

## Secure Gateway

A component of the MetaFrame Access Suite that provides the capability to secure access to Presentation Server and Secure Access Manager. Acting as single point of entry into the secured network, Secure Gateway minimizes the attack surface of the environment while ensuring that all the necessary Presentation Server functionality is available to users, regardless of where they are connecting from. Secure Gateway employs SSL to ensure data integrity and security.

## Secure Gateway Management Console

An MMC snap-in that allows basic management of the Secure Gateway. This tool is installed locally on the Secure Gateway server.

## Secure Gateway Proxy

The Secure Gateway component employed in a double-hop DMZ to act as a conduit of data transmissions between the Secure Gateway and the secure internal network.

See also [demilitarized zone](#), [double-hop DMZ](#), [single-hop DMZ](#).

## Secure CA

See [ICA encryption](#).

## Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Nonproprietary industry-standard security architectures that provide server authentication, data

encryption, and message integrity. TLS is a standardized version of SSL, renamed by the Internet Engineering Taskforce (IETF), which is responsible for developing an open-standard version of SSL. TLS 1.0 and SSL 3.0 have very few technical differences, hence the reason for the common use of SSL/TLS in combination.

## Secure Ticket Authority (STA)

A component of the Secure Gateway for the MetaFrame Access Suite that is responsible for issuing session tickets, which are used by the Secure Gateway to securely launch published applications on a given Presentation Server. The STA deployed with MPS 3.0 requires a server running IIS and must be manually installed. The STA deployed with MPS 4.0 no longer requires IIS and is now an integrated component of the Presentation Server installation.

## self-extracting executable

An executable that, when launched, automatically initiates the installation of a Win32 Presentation Server client. A self-extracting executable installation is available for each of the Win32 clients. The executable names are ica32.exe for the Program Neighborhood client, ica32t.exe for the full Web client, and ica32a.exe for the Program Neighborhood Agent.

## Server certificate

See [\*digital certificate\*](#).

## server drive remapping

Changing the server driver letter(s) from the standard C:, D:, and so on, to any alternate drive letter sequence that you desire prior to installing Presentation Server by using a utility on the installation CD-ROM. For example, you could remap drives C: and D: on a server to be X: and Y:. Then, for example, when booting up the server, you would go into the folder X:\Windows\System32 to access the core Windows executables.

Server drive remapping is provided to allow you to select server drive letters that will not conflict with client-drive mappings. When attempting to map a user's client drives, Presentation Server first tries to map C: to C:, D: to D:, and so on. If these drive letters are in use on the server, Presentation Server uses alternate drives starting at V: and works backward. Often this type of alternate mapping can be confusing to users, particularly when running seamless published applications that allow for drive access.

## server farm

See [\*Citrix server farm\*](#).

## server groups

Subfolders created under the Servers node in the Management Console for Presentation Server.

They are typically created to allow the assignment of privileges based on specific server groupings.

## Server Location

The Presentation Server client property that dictates how the client performs ICA browsing. The configuration of the Server Location dictates the network protocol and method (HTTP, TCP or UDP) of browsing employed. Server Location settings for the Web, PN Agent, and Java clients are actually managed by the Web Interface, which is responsible for retrieving the desired application and server information. None of these clients directly query the Citrix XML or ICA Browser services.

See also [\*ICA browsing\*](#).

## Session Printers

A MetaFrame policy within which network printers can be configured to automatically map within a user's session. Session Printers is a policy new to MPS 4.0. It provides an alternative way of assigning network printers to users without requiring logon scripts.

Session Printers in MPS 4.0 replaces the network printer auto-creation feature found in MPS 3.0, which was accessed by right-clicking on a printer in the Printers node. This auto-creation option does not exist in MPS 4.0.

## session reliability

A Presentation Server feature that attempts to hide brief server disconnects by showing an hourglass mouse pointer and the current session window until the connection is reestablished and the user is automatically logged back on to the session. The user will notice that the system has become unresponsive but will not be aware that connectivity was actually lost unless access to the server is not restored.

## session shadowing

See [\*ICA shadowing\*](#).

## session ticketing

A feature employed by the Web Interface and Secure Gateway to enhance authentication security. Instead of passing user credentials (ID and password) between servers and clients, a session ticket is issued to the client during application launching, which in turn is presented when requested to validate the user's right to access the application. Once used, a ticket expires and is no longer valid. It will also expire if not used within a certain time period.

## shadowing

See [ICA shadowing](#).

## Shadow Taskbar

A Citrix administration tool installed with Presentation Server that allows an administrator to simultaneously manage the shadowing of multiple different users.

## single-hop DMZ

A typical demilitarized zone (DMZ) situated between two firewalls.

See also [demilitarized zone](#), [double-hop DMZ](#).

## smart card roaming

A feature of MPS 4.0 allowing a user to log on and off Presentation Server simply by inserting or removing a smart card from a properly configured terminal. Inserting the card automatically initiates the logon to the farm and retrieval of the user's applications. Removing the card automatically logs the user off the farm.

## SpeedScreen

The collective set of technologies Citrix developed to improve the responsiveness and speed of published content access, particularly over low-bandwidth/high-latency communication links. The following SpeedScreen enhancements are available:

- SpeedScreen Browser Acceleration
- SpeedScreen Flash Acceleration
- SpeedScreen Image Acceleration
- SpeedScreen Latency Reduction
- SpeedScreen Multimedia Acceleration

## SpeedScreen Browser Acceleration (SBA)

SpeedScreen technology that provides two features specifically designed to improve the responsiveness of graphically rich web pages and email. SBA provides performance improvements only in published versions of Internet Explorer, Microsoft Outlook, and Microsoft Outlook Express. Other web browsers and email clients cannot take advantage of SBA. This is an important point to note, as people often assume, particularly with the image compression feature, that it affects all browser or application versions on the server. SBA provides two enhancements. The first allows the user to scroll the pages and access the Back and Stop buttons while any images download in the background. The second allows for the compression of JPEG images, sacrificing image quality for a faster load of the image through the reduction in

size of the image being transmitted to the client. Image compression introduces a minor increase in load on both the server and client.

SpeedScreen Browser Acceleration is enabled by default for the entire farm.

### SpeedScreen Flash Acceleration

SpeedScreen technology that improves Flash rendering by forcing it to operate in low-quality mode by default. When Macromedia Flash animation is rendered on the server, image quality is processed in high quality by default. This results in large bandwidth consumption and poor animation quality on the client. While SpeedScreen Flash Acceleration reduces the quality of the animation, it also reduces both bandwidth and processing requirements to display that animation.

SpeedScreen Flash Acceleration is enabled by default for the entire farm.

### SpeedScreen Image Acceleration

SpeedScreen technology that employs a special compression technique known as lossy compression to reduce image file size, resulting in a smaller amount of bandwidth traversing the wire to be rendered on the client. The SpeedScreen Image Acceleration compression technique is so named because redundant or unnecessary information is removed from the image as part of the compression process. The resulting image does not retain the exact same quality as the original, but in most cases the differences are so small that they are not readily noticeable. The processing of large image files on a Presentation Server itself negatively affects the client by consuming large amounts of bandwidth.

Unlike SpeedScreen Browser Acceleration, which affects images available only through Internet Explorer, Microsoft Outlook, or Outlook Express, SpeedScreen Image Acceleration is available to all images on the server that might be displayed. SpeedScreen Image Acceleration is enabled by default but can be managed via MetaFrame policies to more granularly control who has access to what level of image quality if desired.

### SpeedScreen Latency Reduction

SpeedScreen technology made up of two features, mouse-click feedback and local text echo, both of which are designed to improve the perceived responsiveness of the server to the client. Mouse-click feedback, enabled by default, changes the mouse pointer from an arrow to busy (usually the hourglass) immediately after the user clicks on a link. The user interprets this as the server processing the request, which in turn reduces the user's tendency to repeatedly click the link when it doesn't appear to immediately respond.

When enabled, local text echo uses local client fonts to immediately display text as the user enters it, while simultaneously sending the information to the server where it is processed, updated on the remote display, and transmitted back to the client. Local text echo is intended to eliminate the delay of text entry and visual response. Local text echo does not work under all circumstances. Applications that use nonstandard text controls or employ non-Windows API calls to update text information do not function properly with local text echo.

## SpeedScreen Latency Reduction Manager

SpeedScreen technology used specifically to define the thresholds at which MetaFrame's SpeedScreen latency reduction features are automatically enabled or disabled. In addition to these thresholds, you can also set the default behavior for text echoing and mouse-click feedback on a per-server basis.

## SpeedScreen Multimedia Acceleration (SMA)

SpeedScreen technology that can stream multimedia content (audio and video) directly to the client, where it is then decompressed and rendered locally. Traditionally, multimedia content was rendered on the server and then transmitted to the client in the uncompressed format, consuming extra bandwidth on the network and processing on the server. To achieve this, the following requirements must be met:

- Multimedia playback is supported only through published instances of Internet Explorer, Windows Media Player, or RealOne Player.
- Only media files compressed using algorithms adhering to Microsoft's DirectShow standard can be optimized using SMA.
- The client must have software installed that can process the multimedia stream being sent. If this software is not present, the audio/video stream cannot be processed.

SpeedScreen Multimedia Acceleration is enabled farmwide by default.

## SSL

See [Secure Sockets Layer \(SSL\)/Transport Layer Security \(TLS\)](#).

## SSL Relay

See [Citrix SSL Relay](#).

## STA

See [Secure Ticket Authority](#).

## start-up grace period

Period in which a license server operates until a license file has been downloaded and applied. During this grace period, the MASL server issues a maximum of two Client Access Licenses to nonadministrators. These licenses allow access to the MetaFrame server for a maximum of 96 hours (four days). After that, the users cannot log on until a valid product license file is downloaded and installed on the license server. This 96-hour grace period does not apply to an administrator, who is granted access to the product indefinitely.

See also [\*license server failure grace period\*](#).

## Summary database

An optional component of Resource Manager that is housed on either a Microsoft SQL Server or Oracle server and maintains all historical data gathered by the Presentation Servers and the farm metric servers. A Summary database is required if you want to run reports on any historical performance data for the farm or generate billing reports.

## Target Server

Any Presentation Server within a farm chosen to receive packages deployed via Installation Manager.

## template.ica

See [\*ICA template file\*](#).

## Terminal Services Licensing

The Microsoft licensing required for users connecting to a server running MetaFrame Presentation Server. Even though users may not be connecting using the Microsoft Remote Desktop Connection client, you are still required to purchase the appropriate number of Terminal Services Client Access Licenses (TSCALs). A CAL is required for a user to be able to log on to a server and access Terminal Services resources. The only exception occurs when the server is running in the standard mode, also known as Remote Administration. When the server is operating in this mode, two connection licenses are automatically included with Windows. Specific TSCALs are not required to perform the remote administration tasks on the server.

Terminal Services Licensing requires a server running the TS Licensing service. This service is managed using the Terminal Services Licensing Manager.

## text entry prediction

A SpeedScreen latency reduction feature that provides the user with instant feedback to text entry regardless of whether the data transmission from the server is complete.

## ticketing

See [\*session ticketing\*](#).

## time zone support

A feature that allows the local time zone of the client device to be detected and used to display

the appropriate local time for the user on the server. This feature allows users from different time zones to simultaneously log on to the same server and see an accurate representation of their local time. Limited support exists for detecting the time on legacy clients.

## Transport Layer Security(TLS)

See [Secure Sockets Layer \(SSL\)/Transport Layer Security \(TLS\).](#)

## TWAIN Device

An image acquisition device (scanner, camera, and so on) that adheres to the public standard for application and image acquisition device interaction called TWAIN. MPS 4.0 includes support for accessing TWAIN-compliant devices connected to a client from within a Presentation Server session. The TWAIN Working Group is available at [www.twain.org](http://www.twain.org).

## universal printer driver (UPD)

See [Citrix universal printer driver.](#)

## User Principal Name (UPN)

A Windows Active Directory username in the familiar email address format *username@domain*. Windows 2000 Server and Windows Server 2003 support the entry of usernames in this format.

## USRLOGON.CMD

Legacy batch script used to launch application compatibility scripts and provide root drive support, a process required with Windows NT 4.0, Terminal Services Edition, to overcome the NT4 inability to map directly to a user's home share folder.

## virtual channel

A bidirectional connection that can be used to exchange data between a Presentation Server and an ICA client. The ICA protocol supports these special extensions. Virtual channels allow for the expansion of functionality of the client by Citrix or third-party vendors. A number of ICA-supported functions such as Clipboard or client printer mapping leverage different virtual channels to transmit information between the client and server.

## virtual IP address

A per-session option within MPS 4.0, allowing an application to operate with its own IP address instead of depending on the IP address of the MetaFrame server. This setting is intended to assist in running applications on a Presentation Server that depend on having a unique IP address and/or a specific hard-coded local TCP port number in order to function properly.

The virtual IP address feature is enabled farmwide or on a per-server basis. Specific executables are then flagged as requiring the virtual IP address option.

See also [virtual loopback address](#).

## virtual loopback address

A per-session option within MPS 4.0, allowing each session to access its own loopback address. The loopback address is the TCP/IP address 127.0.0.1, also commonly referred to as *localhost*. The virtual loopback address setting is required only when an application has a hard-coded reference to the localhost address *and* a specific hard-coded TCP port number. Applications that use dynamic port addressing with the localhost address do not require a virtual loopback address.

The virtual loopback address option can be defined for the entire farm or on a per-server basis. Specific executables are then flagged as requiring the virtual loopback address option.

See also [virtual IP address](#).

## Web Interface (WI)

A utility that provides users with access to their published applications and content directly from a web browser. Clicking an application link creates a connection to the Presentation Server publishing the desired application.

## WebInterface.conf

The Web Interface configuration file, which contains all the settings that drive the Web Interface's functionality. The Web Interface Console provides a web-based front end to the contents of this file. When changes are directly made to this file, you must stop and restart the web server to apply the changes.

## Windows Enhanced MetaFile Format (EMF)

An extension to the Windows MetaFiles Format, the EMF format is the format used by the Windows spooler to store and process print jobs. An EMF-formatted print job is smaller than the raw print job, reducing the network bandwidth requirements when sent across the network.

Citrix's latest Universal Printer Driver (UPD) that ships with MPS 4.0 uses this format to transfer print jobs from server to client, speeding up the processing of client printing when compared to previous versions of MetaFrame.

## Workspace Control

A feature that enables users to quickly disconnect or log off all applications or to reconnect to all applications. It facilitates moving quickly between client devices and gaining access to all their applications when they log on. When this feature is configured, users can immediately pull up all

their applications, even if they are active in another location. Workspace Control is available only when users access applications through the Web Interface (including with the PN Agent client).

## wtsprnt.inf

A plain-text file found in the %ProgramFiles%\Citrix\System32 folder on all Presentation Servers. It contains a copy of the printer driver mapping information found in the farm's Data Store.

See also [\*printer driver mapping\*](#).

## zone

A logical grouping of Presentation Servers. Typically, these servers are geographically close to each other, but this is not a strict requirement. All servers within the same zone communicate with a single server in the zone elected to be the zone data collector. When a farm contains multiple zones, only the zone data collectors (ZDCs) communicate with each other, reducing the amount of intra-zone communications and enhancing performance.

Unlike earlier versions of MetaFrame, starting with MPS 3.0, load information is not automatically shared between zones. Each ZDC maintains the load information for only its own zone. When a user attempts to connect to a published application, the ZDC in each zone is consulted to determine what server in the farm is publishing the application and currently has the least load. This can result in users crossing a WAN link to access a published application instead of accessing a local server.

Zone preference and fail-over rules are managed through MetaFrame policies, allowing you to define default and failover zones for users. This way, users access a published application in the zone "closest" to them, even if the load is higher in that zone compared to another zone. Zone preference and fail-over support are available only when users are connecting to the farm using the Web Interface or the Program Neighborhood Agent client.

## zone data collector (ZDC)

A single Presentation Server responsible for keeping zone-specific information gathered from all the Presentation Servers within the same zone. Information that changes frequently is maintained in the ZDC, such as server user load and active and disconnected sessions. A Presentation Server in each zone is chosen to become the zone data collector through an election. Each server can be assigned an election priority, which influences the likelihood that it will be elected the data collector for a zone.

## zone preference and failover

A policy rule allowing you to define both default and failover zones where users access published content. Through the definition of one or more Presentation Server policies, you can define preferred zones where users will attempt to launch applications. This allows for the establishing of preferred and failover zones, and is recommended by Citrix when you are deploying a farm with multiple zones located in geographically dispersed areas. For a user to benefit from zone preference and failover settings, the user must access published content through the Web

Interface or the Program Neighborhood Agent. When you are editing the properties for a policy, you can find the zone preference and failover policy rule under User Workspace Connections.

 PREV

NEXT 

 PREV

NEXT 

# Index

[SYMBOL] [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Z](#)

 PREV

NEXT 

# Index

[[SYMBOL](#)] [[A](#)] [[B](#)] [[C](#)] [[D](#)] [[E](#)] [[F](#)] [[G](#)] [[H](#)] [[I](#)] [[J](#)] [[K](#)] [[L](#)] [[M](#)] [[N](#)] [[O](#)] [[P](#)] [[Q](#)] [[R](#)] [[S](#)] [[T](#)] [[U](#)] [[V](#)] [[W](#)] [[X](#)] [[Z](#)]

128-bit encryption

[ISA Connection Encryption 2nd 3rd](#)

128-bit encryption for logon only configuration

[ISA Connection Encryption 2nd 3rd](#)

40-bit encryption

[ISA Connection Encryption 2nd 3rd](#)

56-bit encryption

[ISA Connection Encryption 2nd 3rd](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

Access Control Suite

[managing Program Neighborhood Agent](#) 2nd 3rd

access management rights

packages

[Installation Manager](#)

[Access Suite Console](#)

Web Interface

[managing](#) 2nd

[access suite console \(MPS 4.0\)](#) 2nd

[access suite licensing \(MPS 4.0\)](#) 2nd

accessing

[client printers](#) 2nd 3rd

activating

license servers (MASL)

[central management of](#) 2nd

Active Directory

[Web Interface support](#)

Active Directory (AD)

Win32 Presentation Server Client

[installation method](#)

Active session (ICA)

[IMA protocol](#)

ActiveX

client deployment control

[Web Interface support](#)

ActiveX controls

safe for scripting marking

[MPS 4.0 security](#)

Add MetaFrame Administrator Wizard

privileges

[delegating](#) 2nd 3rd 4th 5th

[ADF File \(Packager utility\)](#)

[ADF Package \(Packager utility\)](#)

ADF package format

[Installation Manager](#)

ADF packages

[creating \(Packager utility\)](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th

[manual creation of](#) 2nd

[Project Wizard creation steps \(Packager utility\)](#) 2nd

[requirements for creation \(Packager utility\)](#)

administering

users

[License Management Console \(LMC\)](#) 2nd

[administration commands \(MASL\)](#)

[lmdiag](#)

[lmdown](#)

[Imhostid](#)  
[Imremove](#)  
[Imreread](#)  
[Imstat](#)  
[Imswitchr](#)

[administrative delegation](#) 2nd  
  [exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th  
  [examples of](#) 2nd 3rd

external tool access  
  [managing](#) 2nd

[license servers \(MASL\)](#)

Management Console  
  [access limitations](#) 2nd  
  [modifying](#) 2nd  
  [zone-based](#) 2nd

administrative tools (MPS/EE)  
  [Citrix Connection Configuration \(CCC\) tool](#)  
  [ICA Client Distribution Wizard](#)  
  [ICA Client Printer Configuration](#)  
  [ICA Client Update Configuration](#)  
  [ICA Toolbar](#)  
  [Shadow Taskbar](#)  
  [SpeedScreen Latency Manager](#)  
  [SSL Relay Configuration tool](#)

administrators  
  [creating \(Management Console\)](#) 2nd 3rd

external tool access  
  [managing](#) 2nd

package rights  
  [Installation Manager](#)

privileges  
  [Custom category](#)  
  [modifying](#) 2nd  
  [zone-based](#) 2nd

server farms  
  [selecting \(MPS installations\)](#)

Administrators node (Management Console)  
  administrators  
    [creating](#) 2nd 3rd

Advanced evaluator  
  [Citrix Load Manager](#) 2nd

Advanced rule evaluator  
  [user sessions](#) 2nd

Advanced tab  
  [Citrix Connection Configuration \(CCC\)](#) 2nd 3rd 4th

alert thresholds  
  [License Management Console \(LMC\)](#) 2nd

Allow access filter  
  [user policies](#)

anonymous authentication  
  [Web Interface](#)

[anonymous user accounts](#)

anonymous user logons  
  [Web Interface support](#)

anonymous users  
  [Users filter \(user policies\)](#)

[Application Compatibility Scripts](#) 2nd

[\(Packager utility\)](#) 2nd

[Application Deployment File \(ADF\)](#)

application licenses

[MPS 3.0](#)

Application Publishing Wizard

applications

[deployment process](#) 2nd 3rd 4th

packages

[preferred application assignment](#) 2nd

[Program Neighborhood Settings screen](#) 2nd

resources

[publishing](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th

[Specify Application Appearance window](#) 2nd

[Specify Application Limits window](#) 2nd

[Specify Client Requirements window](#) 2nd

[Specify File Type Association window](#) 2nd

[Specify Servers window](#) 2nd

[Specify Users window](#) 2nd

application sets

[generating for users \(Web Interface\)](#) 2nd 3rd 4th

[Program Neighborhood \(PN\) client](#) 2nd

Application tab tab

Program Neighborhood (PN) client

[custom configuration connection setting](#) 2nd

Application User Load rule evaluator

[user sessions](#)

applications

[adding \(SpeedScreen Latency Reduction Manager\)](#) 2nd

[Application Compatibility Scripts](#) 2nd

client IP addresses pass-through

[applying](#) 2nd

delivery methods

[published applications](#)

[published desktops](#) 2nd

deployment

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th

deployment of

[MPS 4.0 features](#)

deployment process

[Application Publishing Wizard](#) 2nd 3rd 4th

[APPUTIL command-line utility](#) 2nd

[Installation Manager](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

hardware size requirements (MPS)

[resource allocation](#) 2nd

Installation Manager

[ADF package format](#)

[Application Deployment File \(ADF\)](#)

[function of](#) 2nd 3rd

[MSI package format](#)

[MSP package format](#)

[installation preparations](#)

[Execute mode](#) 2nd

[Install mode](#) 2nd

[Terminal Server activation](#)

installations

[command line method](#) 2nd  
[disabling new sessions](#) 2nd  
[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th  
[executing](#) 2nd  
[GUI method](#) 2nd

integration of  
  [MPS 4.0 features](#) 2nd

isolation environments  
  [installing](#) 2nd 3rd  
  [uninstalling](#) 2nd

Management Console node  
  [administrator privileges](#)

Program Neighborhood Agent Console  
  [display options](#) 2nd

properties  
  [replicating to other servers in farm \(SpeedScreen Latency Reduction Manager\)](#)  
  [setting \(SpeedScreen Latency Reduction Manager\)](#) 2nd 3rd 4th

published  
  [properties, accessing](#) 2nd  
  [properties, setting](#) 2nd

publishing  
  [Web Interface support](#)  
  [publishing \(Citrix Secure Gateway\)](#) 2nd 3rd  
  [publishing \(MPS Web Interface\)](#) 2nd  
  [real-time monitoring \(Resource Manager\)](#)

remote desktops  
  [publishing \(Remote Desktop Protocol\)](#) 2nd 3rd

resources  
  [publishing \(Application Publishing Wizard\)](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th

virtual IP addresses  
  [applying](#) 2nd

virtual loopback addresses  
  [applying](#) 2nd

Applications node  
  [Management Console](#)  
  Management Console (MPS 4.0)  
    [configuring](#)  
    [Management Console for MetaFrame Presentation Server](#)

APPLUTIL utility  
  [package deployment tasks](#) 2nd

appsrv.ini file  
  [Program Neighborhood \(PN\)](#)

APPUTIL command-line utility  
  applications  
    [deployment management](#) 2nd

APPUTIL utility  
  Installation Manager  
    [package controls](#)

architecture  
  [MASL](#) 2nd  
    [concurrent user licensing](#) 2nd  
    [failover grace periods](#)  
    [startup grace periods](#) 2nd 3rd  
    [system requirements](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

[MPS 4.0 changes](#)  
  [access suite console](#) 2nd

[access suite licensing](#) 2nd  
[application deployment](#)  
[application integration](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th  
[configuration of](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th  
[CPU utilization management](#) 2nd 3rd  
[elimination of MetaFrame 1.8 interoperability](#) 2nd  
[ICA client configuration](#) 2nd  
[installation prerequisites](#)  
[installation process](#)  
[policy management](#) 2nd 3rd 4th 5th  
[printing enhancements](#) 2nd 3rd  
[security enhancements](#) 2nd  
[virtual memory optimization](#) 2nd 3rd  
[web connectivity](#) 2nd 3rd 4th

assigning

[load evaluators](#) 2nd

server licenses

[License Management Console \(LMC\)](#) 2nd

user policies

[via filters](#)

audio virtual channel

[ICA protocol](#)

auditing

shadowed sessions

[IMA protocol \(MetaFrame Presentation Server\)](#) 2nd

authentication

Kerberos Client Authentication

[enabling](#) 2nd 3rd

Microsoft Remote Desktop Web Authentication

[configuring \(MPS installations\)](#) 2nd 3rd

session tickets

[Web Interface support](#)

Web Interface

[anonymous](#)

[explicit login](#)

[single sign-on](#)

[SmartCard](#)

auto-replicating

[printer drivers](#) 2nd

availability (server farms)

[load balancing](#) 2nd

[redundant hardware](#) 2nd

 PREV

NEXT 

# Index

[[SYMBOL](#)] [[A](#)] [[B](#)] [[C](#)] [[D](#)] [[E](#)] [[F](#)] [[G](#)] [[H](#)] [[I](#)] [[J](#)] [[K](#)] [[L](#)] [[M](#)] [[N](#)] [[O](#)] [[P](#)] [[Q](#)] [[R](#)] [[S](#)] [[T](#)] [[U](#)] [[V](#)] [[W](#)] [[X](#)] [[Z](#)]

backup servers

[necessity of for license servers \(MASL\)](#)

[Baltimore Technologies certificate authority](#)

bandwidth

    hardware size requirements (MPS)

[performance criteria 2nd](#)

[MASL system requirements](#)

[Bandwidth policy rule \(user policy\) 2nd 3rd](#)

basic encryption

[ISA Connection Encryption 2nd 3rd](#)

billing reports

[Citrix Resource Manager](#)

[Boolean rule evaluator category](#)

Boson.com

[practice exams](#)

[Browser Acceleration \(SpeedScreen\) 2nd](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

cabinet files

Win32 Presentation Server Client installation files

[Wfica.cab 2nd](#)

[Wficac.cab 2nd](#)

[Wficat.cab 2nd](#)

candidates

[prior Microsoft certifications 2nd](#)

[technical knowledge 2nd](#)

CD-ROM

[PDF support documentation 2nd 3rd 4th 5th 6th 7th 8th](#)

certificate authorities (CAs)

[Baltimore Technologies](#)

server certificates

[issuance of](#)

[VeriSign](#)

certificate signing requests (CSRs)

[generating 2nd 3rd](#)

certification tracks

[Citrix Certification Administrator \(CCA\) 2nd](#)

[eLearning course requirements](#)

[Exam 220](#)

[Exam 221](#)

[Exam 222](#)

[Citrix Certification Enterprise Administrator \(CCEA\) 2nd 3rd 4th](#)

[elective requirements 2nd](#)

[Exam 223](#)

[Exam 913](#)

[Exam 962](#)

[Exam 992](#)

Citrix Certified Administrator (CCA)

[candidate qualifications 2nd](#)

[Citrix Certified Enterprise Administrator \(CCEA\)](#)

[Citrix Certified Instructor \(CCI\) 2nd 3rd](#)

[certification requirements 2nd](#)

[Citrix Certified Integration Architect \(CCIA\) 2nd 3rd 4th 5th](#)

[Exam 223](#)

[Exam 610](#)

[Exam 611](#)

[Microsoft design exam requirements 2nd](#)

[Citrix Certified Sales Professional \(CCSP\) 2nd 3rd 4th](#)

[eLearning course requirements 2nd](#)

[exam requirements](#)

remaining requirements

[viewing on Citrix website 2nd](#)

cipher suites

[Secure Gateway installations](#)

Citrix XML Service

MetaFrame Presentation Server (MPS)

[installing 2nd](#)

Citrix

certification tracks

[Citrix Certified Administrator \(CCA\) 2nd 3rd 4th 5th](#)

[Citrix Certified Enterprise Administrator \(CCEA\) 2nd 3rd 4th 5th](#)

[Citrix Certified Instructor \(CCI\) 2nd 3rd](#)

[Citrix Certified Integration Architect \(CCIA\) 2nd 3rd 4th 5th](#)

[Citrix Certified Sales Professional \(CCSP\) 2nd 3rd 4th](#)

Citrix Activation System (CAS)

[license activation functions](#)

[Citrix Certification Administrator \(CCA\) 2nd](#)

[eLearning course requirements](#)

[Exam 220](#)

[Exam 221](#)

[Exam 222](#)

[Citrix Certification Enterprise Administrator \(CCEA\) 2nd 3rd 4th](#)

[elective requirements 2nd](#)

[Exam 223](#)

[Exam 913](#)

[Exam 962](#)

[Exam 992](#)

Citrix Certified Administrator (CCA)

[candidate qualifications 2nd](#)

[Citrix Certified Enterprise Administrator \(CCEA\)](#)

[Citrix Certified Instructor \(CCI\) 2nd 3rd](#)

[application form downloads](#)

[certification requirements 2nd](#)

[Citrix Certified Integration Architect \(CCIA\) 2nd 3rd 4th 5th](#)

[Exam 223](#)

[Exam 610](#)

[Exam 611](#)

[Microsoft design exam requirements 2nd](#)

[Citrix Certified Sales Professional \(CCSP\) 2nd 3rd 4th](#)

[eLearning course requirements 2nd](#)

[exam requirements](#)

[Citrix Connection Configuration \(CCC\) tool](#)

Citrix Connection Configuration (CCC) utility

[Advanced tab 2nd 3rd 4th](#)

[Client Settings tab 2nd 3rd](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[function of 2nd](#)

[ICA protocol configuration 2nd](#)

[ICA Settings tab 2nd](#)

[launching](#)

Citrix Connection Configuration utility

[server core connections 2nd](#)

Citrix Feature Matrix

[downloadable spreadsheet 2nd 3rd 4th 5th 6th](#)

[Citrix Load Manager](#)

[Advanced evaluator 2nd](#)

[compatibility issues](#)

[Default evaluator](#)

[Citrix Resource Manager \(MPS\)](#)

[billing reports](#)

[real-time monitoring](#)

[report generation](#)

[server metrics 2nd](#)

Citrix Secure Gateway

published applications

[accessing 2nd 3rd](#)

[versus Web Interface 2nd 3rd](#)

[Citrix Universal Printer \(MPS 4.0\) 2nd 3rd](#)

Citrix Vendor Daemon

listening ports

[modifying \(MASL\) 2nd](#)

[Citrix Vendor Daemon \(CITRIX.EXE\) service](#)

Citrix website

MetaFrame Presentation Server

[documentation resources](#)

[MetaFrame Presentation Server home page](#)

[Citrix XML Service](#)

Citrix.com

[CCI \(Citrix Certified Instructor\) application form](#)

[class information](#)

[documentation resources](#)

exams listing

[life cycle dates](#)

[PDF online documentation 2nd 3rd 4th 5th 6th 7th 8th](#)

remaining certification requirements

[tracking 2nd](#)

[user policy resources](#)

client

communication scenarios

[with Presentation Server 2nd](#)

[Client Access Licenses \(CALs\)](#)

client deployment

Web Interface

[configuring 2nd 3rd](#)

[Client Devices policy rule \(user policy\) 2nd 3rd 4th](#)

Client IP Address filter

[user policies](#)

client IP address pass-through

applications

[applying 2nd](#)

client licenses

MPS 3.0

[application licenses](#)

[connection licenses 2nd 3rd](#)

[migration licenses](#)

[upgrade licenses](#)

[Windows 2000 Server Client Access License \(CALs\)](#)

[Windows 2000 Terminal Server Client Access License \(CALs\)](#)

[Windows Server 2003 Client Access License \(CALs\)](#)

[Windows Server 2003 Terminal Client Access License \(TSCALs\)](#)

Client Name filter

[user policies 2nd](#)

client names

user policies

[filtering criteria](#)

client printers

[accessibility of 2nd](#) [3rd](#)

[configuring](#)

[environmental settings](#)

[for DOS clients 2nd](#)

[for Windows CE clients 2nd](#)

[ICA connection](#)

[management properties 2nd](#)

[user policies](#)

[names of](#)

Client Settings tab

[Citrix Connection Configuration \(CCC\) 2nd](#) [3rd](#)

Client Update Database

[characteristics 2nd](#)

clients

[adding/updating 2nd](#)

[properties 2nd](#)

databases

[creating 2nd](#)

properties

[managing 2nd](#) [3rd](#)

Win32 Presentation Server Client

[installation method 2nd](#)

client-side proxy servers

Web Interface

[configuring](#)

clients

[exam prep questions 2nd](#) [3rd](#) [4th](#) [5th](#) [6th](#) [7th](#) [8th](#)

ICA

[ICA Client Connections 2nd](#)

[keyboard shortcut pass-through](#)

[multimonitor support 2nd](#)

[new MPS 4.0 features 2nd](#)

[operating systems file-locking support](#)

[PDA synchronization](#)

[Program Neighborhood \(PN\) 2nd](#)

[Program Neighborhood \(PN\); application set settings 2nd](#)

[Program Neighborhood \(PN\); browser settings 2nd](#) [3rd](#)

[Program Neighborhood \(PN\); custom configuration connection settings 2nd](#) [3rd](#) [4th](#) [5th](#) [6th](#) [7th](#) [8th](#) [9th](#) [10th](#)

[Program Neighborhood \(PN\); default custom configuration settings 2nd](#) [3rd](#) [4th](#) [5th](#) [6th](#)

[Program Neighborhood \(PN\); global properties 2nd](#) [3rd](#) [4th](#)

[Program Neighborhood \(PN\); protocol connection options 2nd](#)

[Program Neighborhood Agent \(PN Agent\) 2nd](#)

[Quick Launch Bar](#)

[smart card roaming support](#)

[TWAIN client device redirection](#)

[Web Client 2nd](#) [3rd](#)

Pass-Through

[enabling \(MPS installations\) 2nd](#)

Program Neighborhood Agent Console

[configuration options 2nd](#)

[management options 2nd](#)

software

[naming conventions 2nd](#)

supported operating systems

[backward compatibility](#)

[DOS](#)

[EPOC/Symbian](#)  
[IBM OS/2](#)  
[Java applet](#)  
[Linux](#)  
[Mac OS X](#)  
[UNIX](#)  
[Windows 16-bit](#)  
[Windows 32-bit 2nd](#)  
[Windows CE](#)  
[Windows PocketPC](#)

web browsers  
    [communication scenarios with Web Interface 2nd](#)  
[Win32 Presentation Server Client 2nd](#)  
        [Citrix Feature Matrix website 2nd 3rd 4th 5th 6th](#)  
        [deployment selection criteria 2nd](#)  
        [downloading from network share points 2nd](#)  
        [ICA Client Update Database 2nd 3rd](#)  
        [ICA Client Update Database, additions/updates 2nd](#)  
        [ICA Client Update Database, database creation 2nd](#)  
        [ICA Client Update Database, properties 2nd](#)  
        [ICA Client Update Database, property management 2nd 3rd](#)  
        [ICA Pass-through Client 2nd](#)  
        [installation files, cabinet-based 2nd](#)  
        [installation files, MSI Client Package 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th 21st 22nd](#)  
        [installation files, self-extracting executables](#)  
        [installing via Active Directory \(AD\)](#)  
        [installing via Client Update Database 2nd](#)  
        [installing via Components CD](#)  
        [installing via floppy disks 2nd](#)  
        [installing via Systems Management Server \(SMS\)](#)  
        [README file](#)  
        [web-based deployments 2nd](#)

Clipboard mapping virtual channel  
    [ICA protocol](#)

clustering  
    server farms  
        [MPS distribution option](#)

command line

applications  
    [installing from 2nd](#)

Common Access Cards  
    [MPS 4.0 security](#)

communication  
    clients  
        [with Presentation Server 2nd](#)

Web Interface  
    [with client web browser 2nd](#)  
    [with Presentation Server 2nd](#)

Components Selection screen  
    [Install Resource Manager option 2nd](#)

components  
    MetaFrame Presentation Server (MPS)  
        [selecting for installation 2nd 3rd](#)  
    [MPS/EE environment](#)

Components CD  
    Win32 Presentation Server Client

[installation method](#)

compression byte

[ICA protocol](#)

configuring

[client printers](#)

[environmental settings](#)

[for DOS clients](#) 2nd

[for Windows CE clients](#) 2nd

[management properties](#) 2nd 3rd

[user policies](#)

[Installation Manager](#) 2nd

[network account settings](#) 2nd

[Options property settings](#) 2nd

[Management Console \(MPS 4.0\)](#) 2nd

[Applications node](#)

[isolation environments](#) 2nd 3rd

[printer management](#) 2nd

[Server Farm node](#) 2nd 3rd

[server management](#) 2nd

Microsoft Remote Desktop Web Authentication

[MetaFrame Server \(MPS\) installations](#) 2nd 3rd

[network printers](#) 2nd 3rd

Resource Manager

[Summary Database Server](#) 2nd

Secure Gateway

[Diagnostics utility](#)

[Management Console](#) 2nd

[Service Configuration tool](#)

[Web Interface](#)

[anonymous authentication](#)

[authentication password changes](#)

[client deployment options](#) 2nd 3rd

[client-side proxy server options](#)

[explicit login authentication](#)

[Server Settings, network address translation \(NAT\)](#) 2nd 3rd

[Server Settings, Secure Gateway support](#) 2nd

[Server Settings, server farm management](#) 2nd

[Server Settings, server load balancing](#) 2nd

[Server Settings, server ordering](#) 2nd

[single sign-on authentication](#)

[SmartCard authentication](#)

[via Web Interface configuration file](#) 2nd

[via Web Interface Console](#) 2nd 3rd 4th 5th

[Workspace Control options](#)

Conn session (ICA)

[IMA protocol](#)

Connect option

User Sessions Management node

[Management Console](#)

connection licenses

[MPS 3.0](#) 2nd 3rd

Connection Limits option

[Farm node \(Management Console\)](#)

Connection tab

Program Neighborhood (PN) client

[custom configuration connection setting](#) 2nd 3rd

[default](#) [custom configuration setting](#) 2nd 3rd 4th

connections

[Secure Gateway installations](#)

[Connections policy rule \(user policy\)](#) 2nd

ConnQ session (ICA)

[IMA protocol](#)

[Content Redirection policy rule \(user policy\)](#)

[Contents tab \(Printer Management node\)](#) 2nd 3rd

Context Switches rule evaluator

[user sessions](#)

copying

[load evaluators](#)

cost centers

[usage billing \(Resource Manager\)](#)

CPU Utilization rule evaluator

[user sessions](#)

CPUs

[reservations](#)

[shares](#)

[utilization management \(MPS 4.0\)](#) 2nd 3rd

[CPVIEWER.EXE print viewer](#)

cross-farm license sharing

[license servers \(MASL\)](#) 2nd

CTX-1223AI class

[exam preparations](#)

current reports

[generating \(Resource Manager\)](#) 2nd

Custom category

[administrator privileges](#) 2nd 3rd

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

Data Collectors (DCs)

IMA protocol

[MetaFrame Presentation Server](#) 2nd

[zone elections](#) 2nd 3rd

Data Store

IMA protocol

[MetaFrame Presentation Server](#)

Data Store (IMA protocol)

[evolution of](#)

[licensing information](#)

[print environment information](#) 2nd

[published application information](#) 2nd

[server configuration information](#) 2nd

[user configuration information](#) 2nd

[Database Connection Server \(Resource Manager\)](#)

databases

ICA Client Update Database

[creation of](#) 2nd

IMA Data Store

[direct connections](#) 2nd

[indirect connections](#) 2nd

IMA Data Store software support

[IBM DB/2](#)

[Microsoft Access](#) 2nd

[Microsoft SQL Server](#)

[Microsoft SQL Server Desktop Engine \(MSDE\)](#)

[Oracle](#)

dedicated license servers

[MASL deployment](#) 2nd 3rd 4th

Default evaluator

[Citrix Load Manager](#)

Default Options tab

Program Neighborhood (PN) client

[default custom configuration setting](#) 2nd

Default rule evaluator

[user sessions](#) 2nd

deleting

[load evaluators](#) 2nd

delivering

applications

[published application method](#)

[published desktop method](#) 2nd

[demilitarized zone \(DMZ\)](#)

Deny access filter

[user policies](#) 2nd

deploying

applications

[Application Publishing Wizard](#) 2nd 3rd 4th

[APPUTIL command-line utility](#) 2nd

[Installation Manager](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

applications via Installation Manager ([MPS 4.0](#))

license servers ([MASL](#)) 2nd

[MASL](#)

[dedicated versus shared server implementation](#) 2nd 3rd 4th

[host server guidelines](#) 2nd

[multiple server farms](#)

devices

[demilitarized zone \(DMZ\)](#)

[Diffie-Hellman encryption algorithm](#)

direct connections

[IMA Data Store \(MPS\) support](#) 2nd

disabled state

[user policy rules](#) 2nd 3rd

disabling

error messages

[Web Interface](#) 2nd

Disc session (ICA)

[IMA protocol](#)

Disconnect option

User Sessions Management node

[Management Console](#)

discontinued exams

[life cycle stage](#) 2nd

Disk Data I/O rule evaluator

[user sessions](#)

Disk Operations rule evaluator

[user sessions](#)

disk space

[MASL system requirements](#) 2nd

distributed databases

server farms

[MPS distribution option](#)

documentation

Citrix.com

[PDF-based online support](#) 2nd 3rd 4th 5th 6th 7th 8th

DOS

client printers

[configuring](#) 2nd

[DOS client](#)

double-hop DMZ

[Secure Gateway deployment](#) 2nd

Down session (ICA)

[IMA protocol](#)

downloading

[Citrix Feature Matrix](#) 2nd 3rd 4th 5th 6th

license files

[License Management Console \(LMC\)](#) 2nd 3rd

drive letters

servers

[remapping \(DriveRemap.exe utility\)](#) 2nd

drive mapping virtual channel

[ICA protocol](#)

[Driver Compatibility dialog box 2nd](#)

DriveRemap.exe utility

server driver letters

[remapping 2nd](#)

drivers

printers

[auto-replicating 2nd](#)

[compatibility, ensuring 2nd](#)

[installing 2nd](#)

[listing of \(Printer Drivers tab\)](#)

[management of \(Drivers node\) 2nd 3rd](#)

[mapping 2nd 3rd 4th](#)

[replicating 2nd](#)

[universal 2nd 3rd 4th 5th](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

editing

[load evaluators 2nd](#)

eLearning

Citrix Certification Administrator (CCA)

[course requirements](#)

Citrix Certified Sales Professional (CCSP)

[course requirements 2nd](#)

elections

Data Collectors (DCs) zones

[priorities 2nd 3rd](#)

elective tracks

[Citrix Certification Enterprise Administrator \(CCEA\) 2nd](#)

enabled state

[user policy rules 2nd](#)

enabling

Pass-Through clients

[MetaFrame Server \(MPS\) installations 2nd](#)

encryption

[Diffie-Hellman algorithm](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[RC5 algorithm](#)

[SSL Relay 2nd](#)

[client requirements 2nd 3rd](#)

[configuring 2nd](#)

[root certificates, obtaining 2nd 3rd](#)

[server certificates, installing 2nd](#)

[server certificates, obtaining 2nd 3rd](#)

[server requirements](#)

[symmetric-key](#)

encryption byte

[ICA protocol](#)

Enhanced MetaFile Format (EMF)

[universal print driver \(MPS 4.0\)](#)

entitlements

server licenses

[License Management Console \(LMC\) 2nd 3rd](#)

environmental settings

client printers

[configuring](#)

[EPOC/Symbian client](#)

error messages

[disabling \(Web Interface\) 2nd](#)

exam

[allowable/disallowable materials](#)

[answering strategies 2nd](#)

[arrival times](#)

[cancellation charges](#)

[identification requirements](#)

[login process](#)

[pass/fail scores](#)

practice exam #1

[answer key 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th](#)

[questions 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th](#)

practice exam #2

[answer key 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th](#)

[questions 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th 21st 22nd 23rd 24th 25th 26th 27th](#)

28th 29th

prep questions

[administrative delegation 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[application deployment 2nd 3rd 4th 5th 6th 7th](#)

[application installations 2nd 3rd 4th 5th 6th 7th 8th](#)

[Citrix Connection Configuration \(CCC\) 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[clients 2nd 3rd 4th 5th 6th 7th 8th](#)

[encryption 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[Installation Manager 2nd 3rd 4th 5th 6th 7th](#)

[Load Manager 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[Management Console 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[MASL 2nd 3rd 4th 5th 6th 7th 8th 9th 10th](#)

[MetaFrame Presentation Server 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th](#)

[MetaFrame Presentation Server, installations 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th](#)

[MPS 4.0 2nd 3rd 4th 5th 6th 7th 8th](#)

[printers 2nd 3rd 4th 5th 6th 7th](#)

[Resource Manager 2nd 3rd 4th 5th](#)

[security 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[Shadow Taskbar 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[SpeedScreen Latency Reduction Manager 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[user policies 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th](#)

[Web Interface 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[Win32 Presentation Server Client 2nd 3rd 4th 5th 6th 7th 8th](#)

[preparations](#)

[authorized classroom training](#)

[Citrix website documentation](#)

[ExamCram2.com website documentation](#)

[MetaFrame Presentation Server 3.0 Enterprise Edition installation media package](#)

[self-study courseware](#)

questions

[formats 2nd](#)

[number of](#)

readiness

[assessing 2nd](#)

registration procedures

[via phone](#)

[via website](#)

resources

[overview](#)

[scoring strategies 2nd](#)

[self-assessment](#)

[candidate qualifications 2nd](#)

[practice testing 2nd](#)

test dates

[viewing \(Prometric.com\)](#)

time limits

[native English-speaking](#)  
[non-native English-speaking](#)  
[typical cost](#)

[Exam 220 \(Citrix Certification Administrator\)](#)  
[Exam 221 \(Citrix Certification Administrator\)](#)  
[Exam 222 \(Citrix Certification Administrator\)](#)  
[Exam 223 \(Citrix Certification Enterprise Administrator\)](#)  
[Exam 223 \(Citrix Certified Integration Architect\)](#)  
[Exam 610 \(Citrix Certified Integration Architect\)](#)  
[Exam 611 \(Citrix Certified Integration Architect\)](#)  
[Exam 913 \(Citrix Certification Enterprise Administrator\)](#)  
[Exam 962 \(Citrix Certification Enterprise Administrator\)](#)  
[Exam 992 \(Citrix Certification Enterprise Administrator\)](#)

ExamCram2.com

[exam resources](#)

exams

life cycles

[Citrix.com dates schedule](#)  
[discontinued stage 2nd](#)  
[release stage 2nd](#)  
[retired stage 2nd](#)

MeasureUp

[creating shortcuts 2nd](#)  
[installing 2nd 3rd](#)  
[multiple test modes 2nd](#)  
[troubleshooting](#)

practice

[Boson.com](#)  
[LearnCitrix.com](#)

[rescheduling](#)

exceptions

user policies  
[defining 2nd](#)

Execute mode

[setting for application installations 2nd](#)

explicit login authentication

[Web Interface](#)

external tools

administrators  
[access management 2nd](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

failover grace periods

[MASL licensing](#)

failovers

[Web Interface support](#)

failover grace periods

[MASL server fault tolerance 2nd](#)

[Farm Metric Server \(Resource Manager\)](#)

[selecting](#)

Farm node

[Management Console 2nd 3rd](#)

[Connection Limits option](#)

[ICA Keep-Alive option](#)

[ICA Settings option 2nd 3rd](#)

[Information option](#)

[Interoperability option](#)

[License Server option](#)

[MetaFrame Settings option 2nd](#)

[Session Reliability option 2nd](#)

[SNMP 2nd](#)

[SpeedScreen Browser Acceleration 2nd](#)

[SpeedScreen Flash Acceleration](#)

[SpeedScreen Multimedia Acceleration](#)

[Zones option 2nd 3rd](#)

farms

[\(servers\) 2nd](#)

MetaFrame Presentation Server

[availability options, load balancing 2nd](#)

[availability options, redundant hardware 2nd](#)

[distribution options 2nd](#)

[distribution options, clustering option](#)

[distribution options, distributed database method](#)

[distribution options, multiple farm method](#)

fault tolerance

MASL

[failover grace periods 2nd](#)

[Microsoft Clustering 2nd](#)

fee profiles

[usage billing \(Resource Manager\)](#)

files

Program Neighborhood Agent Console

[management options 2nd](#)

Filter Table option

User Sessions Management node

[Management Console](#)

filters

[user policies 2nd](#)

[Allow access](#)  
[assigning via](#)  
[by client IP addresses](#)  
[by client names](#)  
[by server names](#)  
[by usernames](#)  
[Client IP Address](#)  
[Client Name](#) 2nd  
[Deny access](#) 2nd  
[Server](#) 2nd  
[Users](#)  
[Users, accounts](#)  
[Users, anonymous](#)  
[Users, groups](#)  
[Users, nonanonymous](#)

firewalls

port configuration  
[MPS environments](#) 2nd

[Flash Acceleration \(SpeedScreen\)](#)

floppy disks

Win32 Presentation Server Client  
[installation method](#) 2nd

font and keyboard layout virtual channel

[ICA protocol](#)

frame head byte

[ICA protocol](#) 2nd

frame trail byte

[ICA protocol](#)

Full Administration category

[administrator privileges](#) 2nd

 PREV

NEXT 

# Index

[[SYMBOL](#)] [[A](#)] [[B](#)] [[C](#)] [[D](#)] [[E](#)] [[F](#)] [[G](#)] [[H](#)] [[I](#)] [[J](#)] [[K](#)] [[L](#)] [[M](#)] [[N](#)] [[O](#)] [[P](#)] [[Q](#)] [[R](#)] [[S](#)] [[T](#)] [[U](#)] [[V](#)] [[W](#)] [[X](#)] [[Z](#)]

generating

current reports

[Resource Manager 2nd](#)

summary reports

[Resource Manager 2nd](#)

GUI

applications

[installing from 2nd](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

hard disks

[MASL system size requirements 2nd](#)

hardware

redundancies

[server farm availability 2nd](#)

size requirements for MPS 3.0

[application types 2nd](#)

[ICA clients](#)

[performance criteria 2nd](#)

[user loads, power user category 2nd](#)

[user loads, typical user category 2nd](#)

[Windows 2000 Datacenter Server platform](#)

[Windows 2000 Server platform 2nd](#)

[Windows Server 2003 Datacenter Edition platform](#)

[Windows Server 2003 Enterprise Edition platform](#)

[Windows Server 2003 Standard Edition platform](#)

workstations

[Management Console \(MPS\) requirements 2nd](#)

help

Citrix.com

[PDF online support documentation 2nd 3rd 4th 5th 6th 7th 8th](#)

help desk

administrative delegation

[access limitations 2nd](#)

historical data

[storing \(Resource Manager\) 2nd](#)

historical usage

[License Management Console \(LMC\) 2nd](#)

host servers

MASL

[deployment guidelines 2nd](#)

Hotfixes option

Servers mode

[Management Console](#)

HP ProtectTools

[MPS 4.0 security](#)

HTTPS

[Web Interface \(MPS\)](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

IBM DB/2

[IMA Data Store \(MPS\) support](#)

[IBM OS/2 client](#)

ICA

server connections

[logs, viewing \(Load Manager\) 2nd](#)

ICA browsing

[Program Neighborhood \(PN\) client 2nd 3rd](#)

ICA client

[keyboard shortcut pass-through](#)

[multimonitor support 2nd](#)

[new MPS 4.0 features 2nd](#)

[operating systems file-locking support](#)

[PDA synchronization](#)

[Quick Launch Bar](#)

[smart cards roaming support](#)

[TWAIN client device redirection](#)

[ICA Client Connections 2nd](#)

ICA Client Distribution (ICD) Wizard

clients

[populating 2nd](#)

[ICA Client Distribution Wizard](#)

[ICA Client Printer Configuration](#)

[ICA Client Update Configuration](#)

[ICA Client Update Database](#)

[characteristics 2nd](#)

clients

[adding/updating 2nd](#)

[properties 2nd](#)

databases

[creating 2nd](#)

properties

[managing 2nd 3rd](#)

ICA clients

[ICA Client Connections 2nd](#)

MPS 3.0

[hardware size requirements](#)

[Program Neighborhood \(PN\) 2nd](#)

[application set settings 2nd](#)

[browser settings 2nd 3rd](#)

[custom configuration connection settings 2nd 3rd 4th 5th 6th 7th 8th 9th 10th](#)

[default custom configuration settings 2nd 3rd 4th 5th 6th](#)

[global properties 2nd 3rd 4th](#)

[protocol connection options 2nd](#)

[Program Neighborhood Agent \(PN Agent\) 2nd](#)

[Web Client 2nd 3rd](#)

ICA connection

client printers

[configuring](#)

## [ICA Connection Encryption](#)

configuration

[128-bit 2nd 3rd](#)

[128-bit encryption for logon only 2nd 3rd](#)

[40-bit 2nd 3rd](#)

[56-bit 2nd 3rd](#)

[basic 2nd 3rd](#)

[limitations of 2nd](#)

ICA display virtual channel

[ICA protocol](#)

ICA Encryption

[session communications](#)

ICA Keep-Alive option

[Farm node \(Management Console\)](#)

Servers mode

[Management Console](#)

## [ICA Pass-through Client 2nd](#)

ICA Printer Bandwidth option

Servers mode

[Management Console](#)

ICA protocol

[\(Independent Computing Architecture\)](#)

[bandwidth ranges](#)

[client component](#)

[configuring via Citrix Connection Configuration \(CCC\)](#)

[network component](#)

[packets](#)

[command data byte](#)

[compression byte](#)

[encryption byte](#)

[frame head byte 2nd](#)

[frame trail byte](#)

[presentation layer \(OSI\)](#)

[server component](#)

[virtual channels](#)

[audio](#)

[Clipboard mapping](#)

[drive mapping](#)

[font and keyboard layout](#)

[ICA display](#)

[parallel port managing](#)

[printer spooling](#)

[serial port managing](#)

[SpeedScreen control](#)

ICA sessions

IMA protocol

[MetaFrame Presentation Server 2nd](#)

ICA Settings option

[Farm node \(Management Console\) 2nd 3rd](#)

Servers mode

[Management Console](#)

ICA Settings tab

[Citrix Connection Configuration \(CCC\) 2nd](#)

## [ICA Toolbar](#)

Ica32.exe

[Win32 Presentation Server Client self-extracting installation files](#)

Ica32a.exe

[Win32 Presentation Server Client self-extracting installation files](#)

Ica32t.exe

[Win32 Presentation Server Client self-extracting installation files](#)

idle session (ICA)

[IMA protocol](#)

idle sessions

IMA protocol

[MetaFrame Presentation Server 2nd 3rd](#)

IIS

multiple sites

[Web Interface support](#)

IMA Data Store (MPS)

[direct connections 2nd 3rd 4th](#)

software support

[IBM DB/2](#)

[Microsoft Access 2nd](#)

[Microsoft SQL Server](#)

[Microsoft SQL Server Desktop Engine \(MSDE\)](#)

[Oracle](#)

IMA protocol

[\(Independent Management Architecture\)](#)

[centralized administration 2nd](#)

[Data Collectors \(DCs\) 2nd](#)

[zone elections 2nd 3rd](#)

[Data Store 2nd 3rd 4th](#)

[ICA sessions 2nd](#)

[idle sessions 2nd 3rd](#)

[listener ports 2nd](#)

[Local Host Cache \(LHC\) 2nd](#)

published applications

[discovery process 2nd](#)

shadowed sessions

[auditing 2nd](#)

[SNMP monitoring](#)

[subsystems management 2nd](#)

[zones](#)

importing

[print servers to server farms \(Printer Management mode\) 2nd 3rd 4th](#)

inbound client connections

[Secure Gateway installations](#)

[Incremental rule evaluator category](#)

Independent Computing Architecture (ICA)

protocols

[connection configurations 2nd](#)

Independent Computing Architecture protocol, [See [ICA protocol](#)]

Independent Management Architecture, [See [IMA protocol](#)]

indirect connections

[IMA Data Store \(MPS\) support 2nd](#)

Information option

[Farm node \(Management Console\)](#)

Servers mode

[Management Console](#)

## INI files

### [Program Neighborhood \(PN\)](#)

[appsrv.ini](#)  
[effect of modification on installation process 2nd 3rd 4th](#)  
[module.ini](#)  
[pn.ini](#)  
[settings options 2nd](#)  
[wfclient.ini](#)

### Init session (ICA)

#### [IMA protocol](#)

### Install mode

#### [setting for application installations 2nd](#)

### installation

[MeasureUp 2nd 3rd](#)  
[creating shortcuts 2nd](#)  
[troubleshooting](#)

### Installation Manager

#### access controls

[administrators](#)

#### application deployment

[package group creation](#)  
[server group creation](#)

#### [Application Deployment File \(ADF\)](#)

#### applications

[deployment process 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th](#)

### APPUTIL utility

[package controls](#)

### configuring 2nd

[network account settings 2nd](#)  
[Options property settings 2nd](#)

### function of 2nd 3rd

### Installer service

### installing 2nd

### [Network Share component](#)

### [network share point server 2nd](#)

### [package management server](#)

### [package server 2nd](#)

### [Packager utility](#)

### packages

[adding to](#)  
[ADF format](#)  
[monitoring deployment status of 2nd](#)  
[MSI format](#)  
[MSP format](#)  
[scheduling deployments 2nd 3rd 4th](#)

### target server

### [Installation Manager \(MPS\)](#)

[Network Share Point Server component](#)  
[Package Server component 2nd](#)  
[Packet Management Server component](#)  
[Target Server component](#)

### Installation Manager node

[Management Console](#)  
[Management Console for MetaFrame Presentation Server](#)

### installation recordings

[packaging \(Packager utility\) 2nd](#)

[rolling back changes \(Packager utility\) 2nd](#)

installations

[prerequisites \(MPS 4.0\)](#)

[process \(MPS 4.0\)](#)

Installer Manager

[exam prep questions 2nd 3rd 4th 5th 6th 7th](#)

[Installer service \(Installation Manager\)](#)

installing

applications

[command line method 2nd](#)

[disabling new sessions 2nd](#)

[GUI method 2nd](#)

[in isolation environments 2nd 3rd](#)

[server preparations](#)

[server preparations, Execute mode 2nd](#)

[server preparations, Install mode 2nd](#)

[server preparations, Terminal Server activation](#)

[Installation Manager 2nd](#)

[license servers \(MASL\)](#)

[MASL 2nd 3rd 4th](#)

[server fault tolerance 2nd 3rd 4th](#)

[MetaFrame Presentation Server \(MPS\) 2nd](#)

[components selection 2nd 3rd](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th](#)

[final step 2nd](#)

[license agreement acceptance](#)

[License Server identification 2nd](#)

[License Server option](#)

[Microsoft Remote Desktop Web Authentication, configuring 2nd 3rd](#)

[Pass-Through clients, enabling 2nd](#)

[product editions selection](#)

[server farms, administrator selection](#)

[server farms, creating 2nd](#)

[server farms, joining 2nd](#)

[shadowing, configuring 2nd](#)

[unattended support 2nd](#)

[XML Service options 2nd](#)

[printer drivers 2nd](#)

[Resource Manager 2nd](#)

[Secure Gateway 2nd 3rd 4th 5th 6th 7th 8th](#)

[Secure Ticket Authority \(STA\) 2nd](#)

[server certificates 2nd](#)

Web Interface

[general guidelines 2nd](#)

[MetaFrame Server requirements 2nd](#)

[Presentation Server client device requirements 2nd](#)

[testing](#)

[web server requirements 2nd](#)

Win32 Presentation Server Client

[cabinet-based installation file 2nd](#)

[downloads from network share points 2nd](#)

[method selection criteria 2nd](#)

[MSI Client Package installation file](#)

[MSI Client Package installation file, custom deployments 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th](#)

19th 20th 21st

[self-extracting executable installation files](#)

[via Active Directory \(AD\)](#)  
[via Client Update Database 2nd](#)  
[via Components CD](#)  
[via floppy disks 2nd](#)  
[via Systems Management Server \(SMS\)](#)  
[web-based deployments 2nd](#)

Internet Information Services (IIS)

[License Management Console \(LMC\)](#)

interoperability mode

[MetaFrame 1.8 legacy server farm support 2nd 3rd 4th 5th](#)

Interoperability option

[Farm node \(Management Console\)](#)

IP addresses

network address translation (NAT)

[Web Interface, Server Settings 2nd 3rd](#)

translation of

[Web Interface support](#)

user policies

[filtering criteria](#)

IP Range rule evaluator

[user sessions](#)

IPX/SPX protocol

[program Neighborhood \(PN\) 2nd](#)

isolation environments

applications

[installing 2nd 3rd](#)

[uninstalling 2nd](#)

Management Console (MPS 4.0)

[configuring 2nd 3rd](#)

 PREV

NEXT 

# Index

[\[SYMBOL\]](#) [\[A\]](#) [\[B\]](#) [\[C\]](#) [\[D\]](#) [\[E\]](#) [\[F\]](#) [\[G\]](#) [\[H\]](#) [\[I\]](#) [\[J\]](#) [\[K\]](#) [\[L\]](#) [\[M\]](#) [\[N\]](#) [\[O\]](#) [\[P\]](#) [\[Q\]](#) [\[R\]](#) [\[S\]](#) [\[T\]](#) [\[U\]](#) [\[V\]](#) [\[W\]](#) [\[X\]](#) [\[Z\]](#)

[Java applet client](#)

joining

server farms

[MetaFrame Presentation Server \(MPS\) installations 2nd](#)

[◀ PREV](#)[NEXT ▶](#)

# Index

[\[SYMBOL\]](#) [\[A\]](#) [\[B\]](#) [\[C\]](#) [\[D\]](#) [\[E\]](#) [\[F\]](#) [\[G\]](#) [\[H\]](#) [\[I\]](#) [\[J\]](#) [\[K\]](#) [\[L\]](#) [\[M\]](#) [\[N\]](#) [\[O\]](#) [\[P\]](#) [\[Q\]](#) [\[R\]](#) [\[S\]](#) [\[T\]](#) [\[U\]](#) [\[V\]](#) [\[W\]](#) [\[X\]](#) [\[Z\]](#)

[Kerberos Client Authentication](#)

[enabling 2nd 3rd](#)

keyboards

shortcut pass-through

[MPS 4.0 support](#)

[◀ PREV](#)[NEXT ▶](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

Latency Reduction (SpeedScreen)

[Local Text Echo](#) 2nd

[Mouse Click Feedback](#) 2nd

LearnCitrix.com

[practice exams](#)

[License Management Console \(LMC\)](#) 2nd 3rd 4th

[Configure License Server option](#)

[Generate Historical Reports option](#)

[Historical Usage option](#) 2nd

[license alert thresholds](#) 2nd

[license assignments](#) 2nd

[entitlements](#) 2nd 3rd

license files

[downloading](#) 2nd 3rd

license usage

[monitoring](#) 2nd

[system requirements](#) 2nd

[User Administration option](#) 2nd 3rd

[View Current Usage Data option](#) 2nd 3rd 4th 5th

[License Management Console \(LMC\);](#) 2nd 3rd 4th

License Manager Daemon

listening ports

[modifying \(MASL\)](#) 2nd

[License Manager Daemon \(LMGRD.EXE\) service](#)

License Server

MetaFrame Presentation Server (MPS)

[identification of](#) 2nd

[installation options](#)

License Server option

[Farm node \(Management Console\)](#)

Servers mode

[Management Console](#)

license servers (MASL)

[administrative delegation](#)

[centralized management of](#) 2nd 3rd 4th

[cross-farm license sharing](#) 2nd

[deploying](#) 2nd

[installation recommendations](#)

[necessity of backup servers](#)

[nonadministrative user grace periods](#) 2nd

[time-based licensing format](#)

License Threshold rule evaluator

[user sessions](#) 2nd

licenses

administrative privileges

[License Management Console \(LMC\)](#) 2nd

alert thresholds

[License Management Console \(LMC\)](#) 2nd

historical usage

[License Management Console \(LMC\)](#) 2nd

MetaFrame Presentation Server (MPS)

[acceptance of agreement](#)

licensing

[access suite console \(MPS 4.0\)](#) 2nd

[access suite model \(MPS 4.0\)](#) 2nd

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th

[implementation process](#)

[initial connection phase](#) 2nd

[retrieval phase](#) 2nd 3rd

MASL

[activation of](#)

[administration commands](#) 2nd 3rd 4th 5th 6th 7th 8th

[architecture](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th

[backwards compatibility limitations](#)

[deployment considerations](#) 2nd 3rd 4th 5th 6th

[failover grace periods](#)

[function of](#)

[installations](#) 2nd 3rd 4th

[introduction of](#)

[License Management Console \(LMC\)](#) 2nd

[License Management Console \(LMC\), system requirements](#) 2nd

[management](#)

[management of](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

[MetaFrame Client Access Licenses \(CAL\)](#) 2nd

[migrating to new servers](#) 2nd

[server fault tolerance](#) 2nd 3rd 4th

[server file locations](#) 2nd

[startup grace periods](#) 2nd 3rd

[uninstallations](#) 2nd 3rd

[MetaFrame Access Suite Licensing \(MASL\)](#)

[administrative delegation](#)

[centralized license management](#) 2nd

[cross-farm license sharing](#) 2nd

[exam coverage](#)

[installation recommendations](#)

[issuance of](#)

[license server management](#) 2nd

[necessity of backup servers](#)

[nonadministrative user grace periods](#) 2nd

[shared/dedicated server deployment](#) 2nd

[time-based](#)

licensing requirements

[MetaFrame Presentation Server](#)

[Windows 2000 Server](#) 2nd 3rd

[Windows Server 2003](#)

[Linux client](#)

Listen session (ICA)

[IMA protocol](#)

listener ports

IMA protocol

[MetaFrame Presentation Server](#) 2nd

listening ports

MASL

[Citrix Vendor Daemon modification](#) 2nd

[License Manager Daemon modification](#) 2nd

listings

[Portion of the Default template.ica File \(14.1\)](#) 2nd

[Imdiag command \(MASL\)](#)

[Imdown command \(MASL\)](#)

[Imhostid command \(MASL\)](#)

[Imremove command \(MASL\)](#)

[Imreread command \(MASL\)](#)

[Imstat command \(MASL\)](#)

[Imswitchr command \(MASL\)](#)

load balancing

[process example](#)

[server farm availability](#) 2nd

[Web Interface support](#)

load evaluators

[assigning](#) 2nd

[copying](#)

[creating](#) 2nd

[deleting](#) 2nd

[editing](#) 2nd

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

rules categories

[Boolean](#)

[Incremental](#)

[Moving Average](#)

[Moving Average Compared to High Value](#)

[rules collection](#) 2nd

[Advanced type](#) 2nd

[Application User Load type](#)

[Context Switches type](#)

[CPU Utilization type](#)

[Default type](#) 2nd

[Disk Data I/O type](#)

[Disk Operations type](#)

[IP Range type](#)

[License Threshold type](#) 2nd

[Memory Usage type](#)

[Page Fault type](#)

[Page Swap type](#)

[Scheduling type](#)

[Server User Load type](#)

updates

[changing frequency of \(Load Manager\)](#) 2nd

usage reports

[viewing \(Load Manager\)](#) 2nd

Load Evaluators node

[Management Console](#)

[Management Console for MetaFrame Presentation Server](#)

Load Manager

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[function of](#) 2nd

information updates

[frequency of](#) 2nd

load balancing

[process example](#)

load evaluators

[assigning 2nd](#)  
[copying](#)  
[creating 2nd](#)  
[deleting 2nd](#)  
[editing 2nd](#)

[rules categories, Boolean](#)  
[rules categories, Incremental](#)  
[rules categories, Moving Average](#)  
[rules categories, Moving Average Compared to High Value](#)  
[rules collection 2nd](#)  
[rules collection, Advanced type 2nd](#)  
[rules collection, Application User Load type](#)  
[rules collection, Context Switches type](#)  
[rules collection, CPU Utilization type](#)  
[rules collection, Default type 2nd](#)  
[rules collection, Disk Data I/O type](#)  
[rules collection, Disk Operations type](#)  
[rules collection, IP Range type](#)  
[rules collection, License Threshold type 2nd](#)  
[rules collection, Memory Usage type](#)  
[rules collection, Page Fault type](#)  
[rules collection, Page Swap type](#)  
[rules collection, Scheduling type](#)  
[rules collection, Server User Load type](#)

logs

[ICA connections to server 2nd](#)

monitoring activities

[launching 2nd](#)

[overview of 2nd](#)

system requirements

[proper functioning of 2nd](#)

[uninstalling 2nd](#)

usage reports

[viewing 2nd](#)

Local Host Cache (LHC)

IMA protocol

[MetaFrame Presentation Server 2nd](#)

local printers

[connection classification 2nd](#)

[versus network printers](#)

Local Text Echo

[SpeedScreen Latency Reduction 2nd](#)

logging exclusions

[Secure Gateway installations](#)

Logoff Selected Session option

User Sessions Management node

[Management Console](#)

Logon Information tab tab

Program Neighborhood (PN) client

[custom configuration connection setting 2nd](#)

logons

Program Neighborhood Agent Console

[configuration options 2nd](#)

[Web Intergace \(MPS\) 2nd](#)

logs

Load Manager

[ICA connections to server 2nd](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

[Mac OS X client](#)

Macrovision Corporation website

[MSI transform file creator](#)

Management Console

administrative delegation

[access limitations](#) 2nd

administrator privileges

[application permissions](#)

Administrators node

[access to external tools](#) 2nd

[administrators, creating](#) 2nd 3rd

[privilege modifications](#) 2nd

[Applications node](#)

[Resource Manager metrics](#)

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

Farm node 2nd 3rd

[Connection Limits option](#)

[ICA Keep-Alive option](#)

[ICA Settings option](#) 2nd 3rd

[Information option](#)

[Interoperability option](#)

[License Server option](#)

[MetaFrame Settings option](#) 2nd

[Session Reliability option](#) 2nd

[SNMP option](#) 2nd

[SpeedScreen Browser Acceleration option](#) 2nd

[SpeedScreen Flash Acceleration option](#)

[SpeedScreen Multimedia Acceleration option](#)

[Zones option](#) 2nd 3rd

[function of](#) 2nd

[Installation Manager node](#)

load evaluators

[assigning](#) 2nd

[copying](#)

[creating](#) 2nd

[deleting](#) 2nd

[editing](#) 2nd

[Load Evaluators node](#)

[MetaFrame Administrators node](#) 2nd 3rd 4th

[Policies node](#)

[Printer Management node](#)

printers 2nd

[Printer Management node](#) 2nd

[Printer Management node; Contents tab](#) 2nd 3rd

[Printer Management node; Network Print Servers tab](#) 2nd 3rd 4th

[Servers node](#)

[Servers node; Printer Drivers tab](#)

[Servers node; Printers tab](#)

[Resource Manager node](#)

[Billing tab](#)

[Email tab](#)

[Farm Metric Server tab](#)

[Reports tab](#)

[SMS tab](#)

[SNMP tab](#)

[Summary Database tab](#)

[Watcher tab](#)

[Servers node 2nd](#)

[Hotfixes option](#)

[ICA Keep-Alive option](#)

[ICA Printer Bandwidth option](#)

[ICA Settings option](#)

[Information option](#)

[License Server option](#)

[MetaFrame Settings option 2nd](#)

[Published Applications option](#)

[Resource Manager metrics](#)

[Workspace Control option](#)

[Shadow Taskbar](#)

[Applications window](#)

[benefits](#)

[launching](#)

[Servers window](#)

[Users window](#)

[user policies](#)

[creation of 2nd](#)

[managing](#)

[User Session Management node](#)

[Connect option](#)

[Disconnect option](#)

[Filter Table option](#)

[Logoff Selected Session option](#)

[Reset option](#)

[Send Message option](#)

[Session Information option](#)

[Shadow option](#)

[Sort Table option](#)

[Status option](#)

[Management Console \(MPS 4.0\)](#)

[configuration of 2nd](#)

[Applications node](#)

[isolation environments 2nd 3rd](#)

[printer management 2nd](#)

[Server Farm node 2nd 3rd](#)

[Servers node 2nd](#)

[Management Console \(MPS\)](#)

[workstation support requirements 2nd](#)

[Management Console for MetaFrame Presentation Server](#)

[Applications node](#)

[Installation Manager node](#)

[Load Evaluators node](#)

[MetaFrame Administrators node](#)

[parent server farm node](#)

[Policies node](#) 2nd

[Printer Management node](#)

[Resource Manager node](#)

[Servers node](#) 2nd

management tools (MPS/EE)

[Access Suite Console](#)

[Management Console for MetaFrame Presentation Server](#)

[Applications node](#)

[Installation Manager node](#)

[Load Evaluators node](#)

[MetaFrame Administrators node](#)

[parent server farm node](#)

[Policies node](#) 2nd

[Printer Management node](#)

[Resource Manager node](#)

[Servers node](#) 2nd

managing

[MASL](#)

[License Management Console \(LMC\)](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

printers

[Management Console](#) 2nd

[Management Console, Printer Management node](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[Management Console, Servers node](#) 2nd 3rd

[manual package creation](#) 2nd

mapping

[printer drivers](#) 2nd 3rd 4th

MASL

[\(MetaFrame Access Suite Licensing\)](#)

activation of

[administration commands](#)

[Imdiag](#)

[Imdown](#)

[Imhostid](#)

[Imremove](#)

[Imreread](#)

[Imstat](#)

[Imswitchr](#)

architecture 2nd

[Citrix Vendor Daemon \(CITRIX.EXE\) service](#)

[concurrent user licensing](#) 2nd

[failover grace periods](#)

[License Management Console \(LMC\)](#) 2nd

[License Manager Daemon \(LMGRD.EXE\) service](#)

[licensing process, initial connection phase](#) 2nd

[licensing process, retrieval phase](#) 2nd 3rd

[startup grace periods](#) 2nd 3rd

[system requirements](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

[backwards compatibility limitations](#)

[concurrent user licensing format](#)

[deployment considerations](#)

[dedicated versus shared server](#) 2nd 3rd 4th

[multiple server farms](#)

[function of](#)

[host server guidelines](#) 2nd

[installations](#) 2nd 3rd 4th

[server fault tolerance](#) 2nd 3rd 4th

[introduction of](#)

licenses

[migrating to new servers](#) 2nd

[licensing implementation process](#)

[initial connection process](#) 2nd

[retrieval process](#) 2nd 3rd

listening ports

[Citrix Vendor Daemon modification](#) 2nd

[License Manager Daemon modification](#) 2nd

[management](#)

[management of](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

[MetaFrame Client Access Licenses \(CAL\)](#) 2nd

[server file locations](#) 2nd

[uninstallations](#) 2nd 3rd

[MeasureUp](#)

[creating shortcuts](#) 2nd

[installing](#) 2nd 3rd

[multiple test modes](#) 2nd

[troubleshooting](#)

memory

base location

[rebasing](#)

[MASL system requirements](#) 2nd

Memory Usage rule evaluator

[user sessions](#)

MetaFrame 1.8

[elimination of mixed mode farm support from MPS 4.0](#) 2nd

[legacy server farm support in MPS 3.0](#)

[interoperability mode](#) 2nd 3rd 4th 5th

[mixed mode](#) 2nd 3rd 4th 5th

[native mode](#)

MetaFrame 1.8 Server

[migrating to MetaFrame Presentation Server](#) 2nd

[MetaFrame Access Suite Licensing \(MASL\)](#)

[administrative delegation](#)

[centralized license management](#) 2nd

[cross-farm license sharing](#) 2nd

[exam coverage](#)

[installation recommendations](#)

[issuance of licenses](#)

[license server management](#) 2nd

[necessity of backup servers](#)

[nonadministrative user grace periods](#) 2nd

[shared/dedicated server deployment](#) 2nd

[time-based](#)

MetaFrame Access Suite Licensing, [See [MASL](#)]

MetaFrame Administrators node

[Management Console](#) 2nd 3rd 4th

[Management Console for MetaFrame Presentation Server](#)

[MetaFrame Conferencing Manager \(MCM\)](#) 2nd

[MetaFrame Password Manager policy rule \(user policy\)](#) 2nd

MetaFrame Presentation Server

Citrix.com

[documentation resources](#)

firewalls

[port configuration 2nd](#)

hardware size requirements

[application types 2nd](#)

[bandwidth performance criteria 2nd](#)

[ICA clients](#)

[user loads, power user category 2nd](#)

[user loads, typical user category 2nd](#)

[Windows 2000 Datacenter Server](#)

[Windows 2000 Server 2nd](#)

[Windows Server 2003 Datacenter Edition](#)

[Windows Server 2003 Enterprise Edition](#)

[Windows Server 2003 Standard Edition](#)

IMA Data Store

[direct connections 2nd](#)

[indirect connections 2nd](#)

IMA Data Store software support

[IBM DB/2](#)

[Microsoft Access 2nd](#)

[Microsoft SQL Server](#)

[Microsoft SQL Server Desktop Engine \(MSDE\)](#)

[Oracle](#)

licenses

[application licenses](#)

[connection licenses 2nd 3rd](#)

[migration licenses](#)

[upgrade licenses](#)

[licensing requirements](#)

[Server](#)

[Windows 2000 Server 2nd](#)

[Windows Server 2003](#)

Management Console

[workstation support requirements 2nd](#)

server farm availability

[load balancing 2nd](#)

[redundant hardware 2nd](#)

[server farm distribution 2nd](#)

[clustering option](#)

[distributed database method](#)

[multiple farm method](#)

software requirements

[TCP/IP 2nd](#)

[Terminal Services, enabling 2nd 3rd 4th](#)

[Terminal Services, licensing 2nd](#)

Metaframe Presentation Server

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th](#)

MetaFrame Presentation Server (MPS)

installations

[components, selecting 2nd 3rd](#)

[final step 2nd](#)

[license agreement acceptance](#)

[License Server identification 2nd](#)

[License Server options](#)

[Microsoft Remote Desktop Web Authentication, configuring 2nd 3rd](#)

[Pass-Through clients, enabling 2nd](#)

[product editions selection](#)

[server farms, administrator selection](#)

[server farms, creating](#) 2nd

[server farms, joining](#) 2nd

[shadowing, configuring](#) 2nd

[standard overview](#) 2nd

[unattended support](#) 2nd

[XML Service options](#) 2nd

[MetaFrame 1.8 Server migrations](#) 2nd

[uninstalling](#) 2nd

Metaframe Presentation Server (MPS)

installation process

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

MetaFrame Presentation Server 3.0 Enterprise Edition

installation media package

[familiarity with for exam preparations](#)

[MetaFrame Presentation Server 3.0, Advanced Edition \(MPS/AE\)](#)

MetaFrame Presentation Server 3.0, Enterprise Edition, [See [MPS/EE](#)] [See [MPS/EE](#)]

[MetaFrame Presentation Server 3.0, Standard Edition \(MPS/SE\)](#)

MetaFrame Presentation Server 4.0, [See [MPS 4.0](#)]

MetaFrame Presentation Server Architecture

ICA protocol

[client component](#)

[network component](#)

[packet bytes](#)

[packet bytes, command data](#)

[packet bytes, compression](#)

[packet bytes, encryption](#)

[packet bytes, frame head](#)

[packet bytes, frame trail](#)

[packet bytes, reliable](#)

[presentation layer \(OSI\)](#)

[server component](#)

[virtual channels](#)

[virtual channels, audio](#)

[virtual channels, Clipboard mapping](#)

[virtual channels, drive mapping](#)

[virtual channels, font and keyboard layout](#)

[virtual channels, ICA display](#)

[virtual channels, parallel port managing](#)

[virtual channels, printer spooling](#)

[virtual channels, serial port managing](#)

[virtual channels, SpeedScreen control](#)

[IMA protocol](#)

[auditing shadowed sessions](#) 2nd

[centralized administration](#) 2nd

[Data Collectors \(DCs\)](#) 2nd

[Data Collectors \(DCs\), zone elections](#) 2nd 3rd

[Data Store](#) 2nd 3rd 4th

[ICA sessions](#) 2nd

[idle sessions](#) 2nd 3rd

[listener ports](#) 2nd

[Local Host Cache \(LHC\)](#) 2nd

[published applications discovery process](#) 2nd

[subsystems](#) 2nd

[zones](#)

[SNMP monitoring](#)

MetaFrame Server

Web Interface  
    [installation requirements](#) 2nd

MetaFrame server  
    core connections  
        [configuring \(Citrix Connection Configuration utility\)](#) 2nd

    policies  
        [setting](#) 2nd

    SpeedScreen properties  
        [setting](#)

MetaFrame Settings option  
    [Farm node \(Management Console\)](#) 2nd

    Servers mode  
        [Management Console](#) 2nd

metrics  
    [Resource Manager](#) 2nd  
        [viewing](#) 2nd 3rd

Microsoft Access  
    [IMA Data Store \(MPS\) support](#) 2nd

Microsoft Clustering  
    [MASL server fault tolerance](#) 2nd

Microsoft design exam series  
    [Citrix Certified Integration Architect \(CCIA\) requirements](#) 2nd

[Microsoft Remote Desktop \(RDP\)](#)

Microsoft Remote Desktop Web Authentication  
    MetaFrame Presentation Server (MPS)  
        [configuring](#) 2nd 3rd

Microsoft SQL Server  
    [IMA Data Store \(MPS\) support](#)

Microsoft SQL Server Desktop Engine (MSDE)  
    [IMA Data Store \(MPS\) support](#)

Microsoft Web Server Certificate Wizard  
    certificate signing requests (CSRs)  
        [generating](#) 2nd 3rd

migrating  
    licenses  
        [to new servers \(MASL\)](#) 2nd

MetaFrame 1.8 Server  
    [to MetaFrame Presentation Server \(MPS\)](#) 2nd

migration licenses  
    [MPS 3.0](#)

mixed mode  
    [MetaFrame 1.8 legacy server farm support](#) 2nd 3rd 4th 5th

modifying  
    [administrator privileges](#) 2nd

module.ini file  
    [Program Neighborhood \(PN\)](#)

monitoring  
    Load Manager  
        [server activities](#) 2nd

package deployments  
    [Installation Manager](#) 2nd

server license usage  
    [License Management Console \(LMC\)](#) 2nd

monitors  
    multiuser settings  
        [MPS 4.0 support](#) 2nd

Mouse Click Feedback

[SpeedScreen Latency Reduction](#) 2nd

moving

licenses

[to new servers \(MASL\)](#) 2nd

[Moving Average Compared to High Value rule evaluator category](#)

[Moving Average rule evaluator category](#)

MPS

[user policy rules](#)

[Bandwidth](#) 2nd 3rd

[Client Devices](#) 2nd 3rd 4th

[Connections](#) 2nd

[Content Redirection](#)

[MetaFrame Password Manager](#) 2nd

[Security](#) 2nd

[Shadowing](#) 2nd

[Time Zones](#) 2nd

[Workspace](#)

[MPS 4.0](#)

[access suite console](#) 2nd

[access suite licensing](#) 2nd

ActiveX controls

[safe for scripting](#)

[application deployment](#)

[application integration](#) 2nd 3rd 4th 5th 6th 7th

[client IP addressing pass-through](#) 2nd

applications

[virtual IP addressing](#) 2nd

[virtual loopback addressing](#) 2nd

changes from 3.0 version

[application deployment](#) 2nd

[application integration](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th

[client configuration](#)

[configuration](#)

[ICA client configuration](#) 2nd

[installation prerequisites](#)

[installation process](#)

[licensing](#)

[load management](#)

[policy management](#) 2nd 3rd 4th 5th 6th

[Presentation Server architecture](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th 21st 22nd

23rd 24th 25th 26th 27th 28th 29th

[printing enhancements](#) 2nd 3rd 4th

[security enhancements](#) 2nd 3rd

[web connectivity](#) 2nd 3rd 4th 5th

[configuration of](#) 2nd

[Applications node](#)

[isolation environments](#) 2nd 3rd

[printer management](#) 2nd

[Server Farm node](#) 2nd 3rd

[Servers node](#) 2nd

[CPU utilization management](#) 2nd 3rd

[elimination of MetaFrame 1.8 interoperability](#) 2nd

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th

[ICA client configuration](#) 2nd

[installation prerequisites](#)

[installation process](#)

[policy additions](#) 2nd 3rd 4th 5th

printers

[Enhanced MetaFile Format \(EMF\)](#)

[enhancements](#) 2nd 3rd

[viewer applications](#)

[security enhancements](#)

[virtual memory optimization](#) 2nd 3rd

[web connectivity enhancements](#) 2nd 3rd 4th

Web Interface

[Configure Authentication Methods task](#) 2nd

[Control Diagnostic Logging task](#)

[Customize Appearance for Users task](#) 2nd

[Manage Client Connection Settings task](#)

[Manage Client Deployment task](#) 2nd

[Manage Client-side Proxy task](#)

[Manage Secure Client Access task](#) 2nd

[Manage Server Farms task](#) 2nd

[Manage Workspace Control task](#)

[Remote Configuration feature](#) 2nd

[Secure Gateway feature](#) 2nd

MPS/EE

[\(MetFrame Presentation Server 3.0, Enterprise Edition\)](#) 2nd

[Access Suite Console](#)

[Citrix Connection Configuration \(CCC\) tool](#)

[Citrix Load Manager](#)

[Advanced evaluator](#) 2nd

[compatibility issues](#)

[Default evaluator](#)

[Citrix Resource Manager](#)

[billing reports](#)

[real-time monitoring](#)

[report generation](#)

[server metrics](#) 2nd

Citrix Secure Gateway

[versus Web Interface](#) 2nd 3rd

[component view of environment](#)

exam

[prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th

[ICA Client Distribution Wizard](#)

[ICA Client Printer Configuration tool](#)

[ICA Client Update Configuration tool](#)

[ICA Toolbar](#)

[Installation Manager](#)

[Network Share Point Server component](#)

[Package Server component](#) 2nd

[Packet Management Server component](#)

[Target Server component](#)

legacy MetaFrame 1.8 server farm support

[interoperability mode](#) 2nd 3rd 4th 5th

[mixed mode](#) 2nd 3rd 4th 5th

[native mode](#)

[native node](#)

[Management Console for MetaFrame Presentation Server](#)

[Applications node](#)

[Installation Manager node](#)

[Load Evaluators node](#)  
[MetaFrame Administrators node](#)  
[parent server farm node](#)  
[Policies node 2nd](#)  
[Printer Management node](#)  
[Resource Manager node](#)  
[Servers node 2nd](#)

[MetaFrame Access Suite Licensing \(MASL\)](#)

[administrative delegation](#)  
[centralized license management 2nd](#)  
[cross-farm license sharing 2nd](#)  
[exam coverage](#)  
[installation recommendations](#)  
[issuance of licenses](#)  
[license server management 2nd](#)  
[necessity of backup servers](#)  
[nonadministrative user grace periods 2nd](#)  
[shared/dedicated deployment 2nd](#)  
[timed-based](#)

[Shadow Taskbar](#)  
[SpeedScreen Latency Reduction Manager](#)  
[SSL Relay Configuration tool](#)

Web Interface

[logons 2nd](#)  
[PNAgent \(Program Neighborhood Agent\)](#)  
[website resources](#)

MSI Client command-line parameters

Win32 Presentation Server Client installation files

[custom deployments 2nd 3rd](#)  
[options 2nd 3rd](#)

MSI Client Package

[Win32 Presentation Server Client installation files](#)  
[custom deployments 2nd 3rd 4th](#)

MSI Client Packager Wizard

[launching 2nd](#)  
[package generation options](#)

MSI package format

[Installation Manager](#)

MSI transform files

creation tools

[Macrovision Corporation](#)  
[Wise Solutions](#)

Win32 Presentation Server Client installation files

[custom deployments 2nd](#)

MSP package format

[Installation Manager](#)

multiple server farms

[Web Interface support](#)

[Multimedia Acceleration \(SpeedScreen\)](#)

multimonitor user environments

[MPS 4.0 support 2nd](#)

multiple server farms

[MASL deployment](#)  
[MPS distribution option](#)

[multiple test modes \(MeasureUp\) 2nd](#)

MultiWin

[Terminal Server concept](#)

MyCitrix.com

Citrix Activation System (CAS)

[license activation functions](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

native mode

[MetaFrame 1.8 legacy server farm support](#)

native node

[MetaFrame 1.8 legacy server farm support](#)

network accounts

Installation Manager settings

[configuring 2nd](#)

network address translation (NAT)

Web Interface

[Server Settings 2nd 3rd](#)

Network Print Servers tab (Printer Management node)

printer servers

[importing to server farms 2nd 3rd 4th](#)

network printers

[configuring 2nd 3rd](#)

[versus local printers](#)

[Network Share component \(Installation Manager\)](#)

Network Share Point Server

[Installation Server \(MPS\)](#)

network share point server

packages

[copying to \(Installation Manager\)](#)

[network share point server \(Installation Manager\) 2nd](#)

network share points

Win32 Presentation Server Client

[client installation method 2nd](#)

networks

[MASL system bandwidth requirements](#)

screen updates

[session acceleration \(SpeedScreen technology\) 2nd](#)

nonadministrative users

grace periods

[license servers \(MASL\) 2nd](#)

nonanonymous users

[Users filter \(user policies\)](#)

not configured state

[user policy rules 2nd](#)

Novell Directory Services (NDS)

[Web Interface support](#)

# Index

[[SYMBOL](#)] [[A](#)] [[B](#)] [[C](#)] [[D](#)] [[E](#)] [[F](#)] [[G](#)] [[H](#)] [[I](#)] [[J](#)] [[K](#)] [[L](#)] [[M](#)] [[N](#)] [[O](#)] [[P](#)] [[Q](#)] [[R](#)] [[S](#)] [[T](#)] [[U](#)] [[V](#)] [[W](#)] [[X](#)] [[Z](#)]

operating systems

client software support

[backward compatibility](#)

[DOS](#)

[EPOC/Symbian](#)

[IBM OS/2](#)

[Java applet](#)

[Linux](#)

[Mac OS X](#)

[UNIX](#)

[Windows 16-bit](#)

[Windows 32-bit 2nd](#)

[Windows CE](#)

[Windows PocketPC](#)

[file-locking support \(MPS 4.0\)](#)

[MASL platform support requirements](#)

Options property

Installation Manager settings

[configuring 2nd](#)

Options tab

Program Neighborhood (PN) client

[custom configuration connection setting 2nd 3rd](#)

Oracle

[IMA Data Store \(MPS\) support](#)

OSI model

presentation layer

[ICA protocol](#)

outbound connections

[Secure Gateway installations](#)

overriding

user policies

[exceptions to 2nd 3rd](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

package groups

    application deployment

[creating \(Installation Manager\)](#)

package management server (Installation Manager)

Package Server

[Installation Server \(MPS\) 2nd](#)

package server (Installation Manager) 2nd

Packager utility

[ADF File](#)

[ADF Package](#)

    ADF packages

[creating 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th](#)

[Project Wizard creation steps 2nd](#)

[requirements for creation](#)

[application compatibility scripts 2nd](#)

[Project folder](#)

[project creation log file](#)

[project log file](#)

[record log file](#)

Packager utility (Installation Manager)

packages

[adding to Installation Manager](#)

ADF

[creating \(Packager utility\) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th](#)

[manual creation of 2nd](#)

[Project Wizard creation steps \(Packager utility\) 2nd](#)

[requirements for creation \(Packager utility\)](#)

command prompt

[managing \(APPUTIL utility\) 2nd](#)

copying to network share point

[deployment of \(Installation Manager\)](#)

deployments

[monitoring status of \(Installation Manager\) 2nd](#)

[scheduling \(Installation Manager\) 2nd 3rd 4th](#)

format determination

[deployment of \(Installation Manager\)](#)

Installation Manager

[ADF format](#)

[function of 2nd](#)

[MSI format](#)

[MSP format](#)

Installation Recording

[creating 2nd](#)

[rolling back changes 2nd](#)

[management of \(APPUTIL utility\)](#)

selected files

[creating 2nd](#)  
unattended programs  
[creating 2nd](#)

Packet Management Server  
[Installation Server \(MPS\)](#)

Page Fault rule evaluator  
[user sessions](#)

Page Swap rule evaluator  
[user sessions](#)

parallel port managing virtual channel  
[ICA protocol](#)

parent server farm node  
[Management Console for MetaFrame Presentation Server](#)

[Pass-through Client 2nd](#)

Pass-Through clients  
MetaFrame Presentation Server (MPS)  
[enabling 2nd](#)

passthrough authentication  
[Remote Desktop Protocol \(RDP\) 2nd](#)

passwords  
authentication  
[changing \(Web Interface\)](#)

[PCL2BMP.EXE print viewer](#)

PCL4 (Printer Control Language)  
[universal printer drivers \(UPDs\)](#)

PCL5c (Printer Control Language)  
[universal printer drivers \(UPDs\)](#)

PDAs  
[synchronization of \(MPS 4.0\)](#)  
[Web Interface support](#)

performance  
hardware size requirements (MPS)  
[network bandwidth issues 2nd](#)

permissions  
administrator privileges  
[Management Console](#)

platforms  
[MASL system requirements](#)  
[MetaFrame Presentation Server solutions](#)

pn.ini file  
[Program Neighborhood \(PN\)](#)

PNAgent  
[\(Program Neighborhood Agent\)](#)

published applications  
[accessing 2nd](#)

policies  
MetaFrame servers  
[setting 2nd](#)

MPS 4.0  
[new additions 2nd 3rd 4th 5th](#)

Policies node  
[Management Console](#)  
[Management Console for MetaFrame Presentation Server 2nd](#)

ports  
firewalls  
[configuring \(MPS\) 2nd](#)

power users

hardware size requirements (MPS)

[resource allocation](#) 2nd

practice exam #1

[answer key](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th

[questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th

practice exam #2

[answer key](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th

[questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th 21st 22nd 23rd 24th 25th 26th 27th 28th

29th

practice exams

[assessing progress for actual exams](#) 2nd

[Boson.com](#)

[LearnCitrix.com](#)

[MeasureUp](#)

[creating shortcuts](#) 2nd

[installing](#) 2nd 3rd

[multiple test modes](#) 2nd

[troubleshooting](#)

precedence rules

[user policy overrides](#) 2nd 3rd

prep questions

[administrative delegation](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[application deployment](#) 2nd 3rd 4th 5th 6th 7th

[application installations](#) 2nd 3rd 4th 5th 6th 7th 8th

[Citrix Connection Configuration \(CCC\)](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[encryption](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[Installation Manager](#) 2nd 3rd 4th 5th 6th 7th

[Load Manager](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[Management Console](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[MASL](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th

[MetaFrame Presentation Server](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th

[installation of](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th

[security](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[Shadow Taskbar](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[SpeedScreen Latency Reduction Manager](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[user policies](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th

prep questions (exam)

[clients](#) 2nd 3rd 4th 5th 6th 7th 8th

[MPS 4.0](#) 2nd 3rd 4th 5th 6th 7th 8th

[printers](#) 2nd 3rd 4th 5th 6th 7th

[Resource Manager](#) 2nd 3rd 4th 5th

[Web Interface](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[Win32 Presentation Server Client](#) 2nd 3rd 4th 5th 6th 7th 8th

preparations (exam)

[authorized classroom training](#)

[Citrix website documentation](#)

[ExamCram2.com website documentation](#)

[MetaFrame Presentation Server 3.0 Enterprise Edition installation media package](#)

[self-study courseware](#)

presentation layer (OSI)

[ICA protocol](#)

Presentation Server

client deployment

[Web Interface support](#)

client devices

[Web Interface installation requirements](#) 2nd  
[communication scenarios with clients](#) 2nd  
[communication scenarios with Web Interface](#) 2nd  
load balancing and failovers  
    [Web Interface support](#)  
Secure Gateway  
    [Web Interface support](#)  
print servers  
    [importing to server farms \(Printer Management node\)](#) 2nd 3rd 4th  
[Printer Drivers tab \(Servers node\)](#)  
Printer Management node  
    [Management Console](#)  
    Management Console (MPS 4.0)  
        [configuring](#) 2nd  
    [Management Console for MetaFrame Presentation Server](#)  
universal printer drivers (UPDs)  
    [managing](#) 2nd  
Printer Management node (Management Console)  
    [Contents tab](#) 2nd 3rd  
    [Network Print Servers tab](#) 2nd 3rd 4th  
    [properties](#) 2nd  
printer spooling virtual channel  
    [ICA protocol](#)  
printers  
    [Citrix Universal Printer \(MPS 4.0\)](#) 2nd 3rd  
client type  
    [accessibility of](#) 2nd 3rd  
    [configuring](#)  
    [configuring environmental settings](#)  
    [configuring for DOS clients](#) 2nd  
    [configuring for Windows CE clients](#) 2nd  
    [configuring ICA connection](#)  
    [configuring management properties](#) 2nd  
    [configuring user policies](#)  
    [names of](#)  
drivers  
    [auto-replicating](#) 2nd  
    [compatibility, ensuring](#) 2nd  
    [installing](#) 2nd  
    [listing of \(Printer Drivers tab\)](#)  
    [management of \(Drivers node\)](#) 2nd 3rd  
    [mapping](#) 2nd 3rd 4th  
    [replicating](#) 2nd  
    [universal](#) 2nd 3rd 4th 5th  
[Enhanced MetaFile Format \(EMF\)](#)  
[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th  
local type  
    [connection classification](#) 2nd  
    [versus network type](#)  
[Management Console](#) 2nd  
    [Printer Management node](#) 2nd  
    [Printer Management node, Contents tab](#) 2nd 3rd  
    [Printer Management node, Network Print Servers tab](#) 2nd 3rd 4th  
    [Servers node](#)  
    [Servers node, Printer Drivers tab](#)  
    [Servers node, Printers tab](#)

[network type](#)  
[configuring 2nd 3rd](#)  
[versus local type](#)  
[new MPS 4.0 features 2nd 3rd](#)

viewer applications  
[CPVIEWER.EXE](#)  
[PCL2BMP.EXE](#)

[Printers tab \(Servers node\)](#)

priorities  
user policies  
[number values 2nd 3rd 4th](#)

privileges

administrators  
[Custom category 2nd 3rd](#)  
[Full Administration category 2nd](#)  
[modifying 2nd](#)  
[setting 2nd 3rd](#)  
[View Only category 2nd](#)  
[zone-based 2nd](#)

processors  
[MASL system requirements 2nd](#)

product editions  
MetaFrame Presentation Server (MPS)  
[selecting](#)

Program Neighborhood (PN)

[application set settings 2nd](#)  
browser settings  
[configuring 2nd 3rd](#)  
[custom configuration connection settings 2nd 3rd 4th 5th 6th 7th 8th 9th 10th](#)  
[default custom configuration settings 2nd 3rd 4th 5th 6th](#)

global properties

[ICA Settings 2nd](#)  
[Modems](#)  
[Serial Devices](#)

network protocols

[connection options 2nd](#)  
self-extracting executables  
[installation settings 2nd 3rd 4th 5th](#)

[Win32 client type 2nd](#)

Program Neighborhood Agent

[managing via Access Control Suite 2nd 3rd](#)  
[managing via Access Suite Console \(MPS 4.0\)](#)  
[new MPS 4.0 features 2nd 3rd 4th 5th 6th 7th](#)

site tasks

[Change Session Options \(MPS 4.0\)](#)  
[Configure Authentication Methods \(MPS 4.0\)](#)  
[Duplicate Client Configuration \(MPS 4.0\)](#)  
[Export Client Configuration \(MPS 4.0\)](#)  
[Manage Application Refresh \(MPS 4.0\)](#)  
[Manage Application Shortcuts \(MPS 4.0\)](#)  
[Manage Server Settings \(MPS 4.0\)](#)

Program Neighborhood Agent (PN Agent)

[installation settings 2nd](#)  
[Web Interface support](#)  
[Win32 client type 2nd](#)

Program Neighborhood Agent Console

[accessing](#)  
[Application Display page](#) 2nd  
[client configuration](#) 2nd  
[Client Tab Control page](#) 2nd  
[configuration options](#)  
[features](#)  
[Logon Methods page](#) 2nd  
[Manage Configuration Files page](#) 2nd  
[page appearance](#)  
[Remote Desktop \(RDP\) Web Connection software](#) 2nd 3rd  
[Session Options page](#) 2nd  
[Workspace Control page](#)

Program Neighborhood Settings screen  
[Application Publishing Wizard](#) 2nd

[Project folder \(Packager utility\)](#)  
[project creation log file](#)  
[project log file](#)  
[record log file](#)

Project Wizard  
project options  
[Package an Installation Recording](#) 2nd 3rd  
[Package an Unattended Program](#) 2nd 3rd  
[Package Selected Files](#) 2nd 3rd

Project wizard  
ADF packages  
[creating](#) 2nd

projects  
[Add Files option](#)  
[Add Recording option](#) 2nd  
[Add Unattended Program option](#)  
[manual package creation](#) 2nd

Prometric.com  
[exam test dates](#)

properties  
applications  
[replicating to other servers in farm\(SpeedScreen Latency Reduction Manager\)](#)  
[SpeedScreen Latency Reduction Manager](#) 2nd 3rd 4th

client printers  
[configuring](#) 2nd

ICA Client Update Databases  
[managing](#) 2nd 3rd

Program Neighborhood (PN) client  
[ICA Settings](#) 2nd  
[Modems](#)  
[Serial Devices](#)

protocols  
ICA  
[configuring via Citrix Connection Configuration \(CCC\)](#) 2nd

Program Neighborhood (PN) client  
[IPX/SPX](#) 2nd  
[SSL/TLS+HTTPS](#) 2nd  
[TCP/IP](#) 2nd  
[TCP/IP+HTTP](#) 2nd  
[Secure Gateway installations](#)

TCP/IP  
[default installations by Windows 2000/2003 Server](#) 2nd

PS (PostScript)

[universal printer drivers \(UPDs\)](#)

published applications

applications

[delivery method to users](#)

discovery process

[IMA protocol \(MetaFrame Presentation Server\) 2nd](#)

properties

[accessing 2nd](#)

[setting 2nd](#)

Published Applications option

Servers mode

[Management Console](#)

published content

[eligible on MPS servers 2nd](#)

published desktops

applications

[delivery method to users 2nd](#)

publishing

applications

[Citrix Secure Gateway \(MPS\) 2nd 3rd](#)

[Web Interface \(MPS\) 2nd](#)

resources

[Application Publishing Wizard 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th](#)

 PREV

NEXT 

# Index

[\[SYMBOL\]](#) [\[A\]](#) [\[B\]](#) [\[C\]](#) [\[D\]](#) [\[E\]](#) [\[F\]](#) [\[G\]](#) [\[H\]](#) [\[I\]](#) [\[J\]](#) [\[K\]](#) [\[L\]](#) [\[M\]](#) [\[N\]](#) [\[O\]](#) [\[P\]](#) [\[Q\]](#) [\[R\]](#) [\[S\]](#) [\[T\]](#) [\[U\]](#) [\[V\]](#) [\[W\]](#) [\[X\]](#) [\[Z\]](#)

questions (exam)

[formats 2nd](#)

[number of](#)

Quick Launch Bar

[Program Neighborhood \(MPS 4.0\)](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

[RC5 encryption algorithm](#)

README file

[Win32 Presentation Server Client](#)

real-time monitoring

applications

[Resource Manager](#)

[Citrix Resource Manager](#)

servers

[Resource Manager](#)

rebasing

[memory base location](#)

redundant hardware

[server farm availability 2nd](#)

registering

exams

[via phone](#)

[via website](#)

released exams

[life cycle stage 2nd](#)

reliable byte

[ICA protocol](#)

remapping

server drive letters

[DriveRemap.exe utility 2nd](#)

Remote Configuration feature

[Web Interface \(MPS 4.0\) 2nd](#)

Remote Desktop (RDP)

Program Neighborhood Agent Console

[Web Connection software 2nd 3rd](#)

[Web Interface support](#)

Remote Desktop Protocol (RDP)

applications

[publishing 2nd 3rd](#)

[passthrough authentication 2nd](#)

Remote Desktop Web Authentication (Microsoft)

MetaFrame Presentation Server (MPS)

[configuring 2nd 3rd](#)

remote sessions

user-shadowing

[configuring \(MPS\) 2nd](#)

Replicate Driver dialog box

[Driver tab 2nd](#)

[Platform tab 2nd](#)

[Servers tab 2nd](#)

replicating

[printer drivers 2nd](#)

[SpeedScreen Latency Reduction Manager settings](#)

reports

[generation of \(Citrix Resource Manager\)](#)

Resource Manager

[current type 2nd](#)

[current type, generating 2nd](#)

[summary type 2nd](#)

[summary type, generating 2nd](#)

Reset option

User Sessions Management node

[Management Console](#)

Resource Manager

applications

[real-time monitoring](#)

[Database Connection Server](#)

[exam prep questions 2nd 3rd 4th 5th](#)

[Farm Metric Server](#)

[selecting](#)

[function of 2nd](#)

historical data

[storing 2nd](#)

[installation of 2nd](#)

Management Console

[Billing tab](#)

[Email tab](#)

[Farm Metric Server tab" "Resource Manager; metrics; viewing" "metrics; Resource Manager; viewing" "viewing;metrics;Resource Manager"](#)

[Reports tab](#)

[SMS tab](#)

[SNMP tab](#)

[Summary Database tab](#)

[Watcher tab](#)

[metrics 2nd](#)

[viewing 2nd 3rd](#)

reports

[current type 2nd](#)

[summary type 2nd](#)

servers

[real-time monitoring](#)

[Summary Database Server](#)

[configuring 2nd](#)

upgrading

[component order](#)

usage billing

[cost centers](#)

[fee profiles](#)

Resource Manager node

[Management Console](#)

[Management Console for MetaFrame Presentation Server](#)

resources

Citrix.com

[PDF online documentation 2nd 3rd 4th 5th 6th 7th 8th](#)

[publishing \(Application Publishing Wizard\) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th](#)

types

[eligible for publishing 2nd](#)

resources (exam)

[overview](#)

resultant sets

user policies

[searching by 2nd 3rd](#)

retired exams

[life cycle stage 2nd](#)

rolling back

[installation recording packages 2nd](#)

root certificates

SSL Relay service

[obtaining 2nd 3rd](#)

RSA SecurID on UNIX

[MPS 4.0 security](#)

rules

[load evaluators 2nd](#)

[Advanced type 2nd](#)

[Application User Load type](#)

[Boolean category](#)

[Context Switches type](#)

[CPU Utilization type](#)

[Default type 2nd](#)

[Disk Data I/O type](#)

[Disk Operations type](#)

[Incremental category](#)

[IP Range type](#)

[License Threshold type 2nd](#)

[Memory Usage type](#)

[Moving Average category](#)

[Moving Average Compared to High Value category](#)

[Page Fault type](#)

[Page Swap type](#)

[Scheduling type](#)

[Server User Load type](#)

user policies 2nd

[Bandwidth 2nd 3rd](#)

[Client Devices 2nd 3rd 4th](#)

[Connections 2nd](#)

[Content Redirection](#)

[disabled state 2nd 3rd](#)

[enabled state 2nd](#)

[MetaFrame Password Manager 2nd](#)

[not configured state 2nd](#)

[overriding 2nd 3rd](#)

[Security 2nd](#)

[Shadowing 2nd](#)

[Time Zones 2nd](#)

[User Workspace](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

SafeWord on UNIX

[MPS 4.0 security](#)

scheduling

package deployments

[Installation Manager 2nd 3rd 4th](#)

Scheduling rule evaluator

[user sessions](#)

screen updates

[session acceleration \(SpeedScreen technology\) 2nd](#)

Secure Gateway

[cipher suites](#)

[connection parameters](#)

[Diagnostics utility](#)

[double-hop DMZ deployment 2nd](#)

inbound client connections

[installing 2nd 3rd 4th 5th 6th 7th 8th](#)

[logging exclusions](#)

[Management Console 2nd](#)

[outbound connections](#)

Presentation Server

[Web Interface support](#)

[protocol selection](#)

[Secure Ticket Authority \(STA\)](#)

[adding](#)

[server certificates](#)

server farm access

[Web Interface implementation 2nd 3rd 4th](#)

[Service Configuration tool](#)

Web Interface

[configuring 2nd](#)

Secure Gateway feature

[Web Interface \(MPS 4.0\) 2nd](#)

[Secure Ticket Authority \(STA\)](#)

[installing 2nd](#)

[Secure Gateway installations](#)

security

[administrative delegation 2nd](#)

[examples of 2nd 3rd](#)

[Management Console, access limitations 2nd](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

firewalls

[port configuration \(MPS\) 2nd](#)

[ICA Connection Encryption](#)

[128-bit encryption configuration 2nd 3rd](#)

[128-bit encryption for logon only configuration 2nd 3rd](#)

[40-bit encryption configuration 2nd 3rd](#)

[56-bit encryption configuration](#) 2nd 3rd

[basic encryption configuration](#) 2nd 3rd

[limitations of 2nd](#)

[Kerberos Client Authentication](#)

[enabling](#) 2nd 3rd

MPS 4.0

[common access card support](#)

[HP ProtectTools](#)

[RSA SecurID on Unix Support](#)

[SafeWord on Unix Support](#)

[smart card authentication pass-through](#)

[smart card recognition support](#)

server farms

[access infrastructure \(Secure Gateway\)](#) 2nd 3rd 4th

[SSL Relay](#) 2nd 3rd

[client requirements](#) 2nd 3rd

[configuring](#) 2nd

[root certificates, obtaining](#) 2nd 3rd

[server certificates, installing](#) 2nd

[server certificates, obtaining](#) 2nd 3rd

[server requirements](#)

Security Gateway

[session communications](#)

[Security policy rule \(user policy\)](#) 2nd

selected files

[packaging \(Packager utility\)](#) 2nd

selecting

Resource Manager

[Farm Metric Server](#)

[self-assessment \(exam\)](#)

[candidate qualifications](#) 2nd

[practice testing](#) 2nd

self-extracting executables

Win32 Presentation Server Client installation files

[custom deployments](#) 2nd

[custom deployments, PN Agent](#) 2nd

[custom deployments, Program Neighborhood \(PN\)](#) 2nd 3rd 4th 5th

[custom deployments, Web client](#) 2nd 3rd

[Ica32.exe](#)

[Ica32a.exe](#)

[Ica32t.exe](#)

Send Message option

User Sessions Management node

[Management Console](#)

serial port managing virtual channel

[ICA protocol](#)

server architecture

[MPS 4.0 changes](#)

[access suite console](#) 2nd

[access suite licensing](#) 2nd

[application deployment](#)

[application integration](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th

[configuration of](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th

[CPU utilization management](#) 2nd 3rd

[elimination of MetaFrame 1.8 interoperability](#) 2nd

[ICA client configuration](#) 2nd

[installation prerequisites](#)

[installation process](#)

[policy management](#) 2nd 3rd 4th 5th

[printing enhancements](#) 2nd 3rd

[security enhancements](#) 2nd

[virtual memory optimization](#) 2nd 3rd

[web connectivity](#) 2nd 3rd 4th

server certificates

certificate authorities (CAs)

[issuance of](#)

certificate signing requests (CSRs)

[generating](#) 2nd 3rd

[Secure Gateway installations](#)

SSL Relay service

[installing](#) 2nd

[obtaining](#) 2nd 3rd

Server Farm node

Management Console (MPS 4.0)

[configuring](#) 2nd 3rd

server farms

[access security through Secure Gateway](#) 2nd 3rd 4th

[administrative delegation](#) 2nd

[examples of](#) 2nd 3rd

[external tool access](#) 2nd

[Management Console, access limitations](#) 2nd

[modifying](#) 2nd

[zone-based](#) 2nd

administrator privileges

[delegating](#) 2nd 3rd 4th 5th

Kerberos Client Authentication

[enabling](#) 2nd 3rd

[managing \(Web Interface\)](#) 2nd

MetaFrame Presentation Server (MPS)

[administrator selection](#)

[creating](#) 2nd

[joining](#) 2nd

multiple

[Web Interface support](#)

[Web Interface](#)

Server filter

[user policies](#) 2nd

server groups

application deployment

[creating \(Installation Manager\)](#)

server licenses

MPS 3.0

[Windows 2000 Server platforms](#) 2nd

[Windows Server 2003 platforms](#) 2nd

server metrics

[Citrix Resource Manager](#) 2nd

server names

user policies

[filtering criteria](#)

Server Settings (Web Interface)

server farms

[managing](#) 2nd

servers  
  [load balancing](#) 2nd  
  [ordering for farm use](#) 2nd

Server User Load rule evaluator  
  [user sessions](#)

servers  
  applications  
    [installation preparations](#)  
    [installation preparations, Execute mode](#) 2nd  
    [installation preparations, Install mode](#) 2nd  
    [installation preparations, Terminal Server activation](#)

drive letters  
  [remapping \(DriveRemap.exe utility\)](#) 2nd

MASL  
  [fault tolerance](#) 2nd 3rd 4th  
  [real-time monitoring \(Resource Manager\)](#)

Servers node  
  [Management Console](#) 2nd  
    Hotfixes option  
    ICA Keep-Alive option  
    ICA Printer Bandwidth option  
    ICA Settings option  
    Information option  
    License Server option  
    MetaFrame Settings option 2nd  
    Published Applications option  
    Workspace Control option

Management Console (MPS 4.0)  
  [configuring](#) 2nd  
  [Management Console for MetaFrame Presentation Server](#) 2nd

Servers node (Management Console)  
  [Printer Drivers tab](#)  
  [Printers tab](#)

session authentication tickets  
  [Web Interface support](#)

session communications  
  clients  
    [with Presentation Server](#) 2nd

  security options  
    [ICA Encryption](#)  
    [Security Gateway](#)  
    [SSL/TLS](#)

  Web Interface  
    [with client web browser](#) 2nd  
    [with Presentation Server](#) 2nd

Session Information option  
  User Sessions Management node  
    [Management Console](#)

Session Reliability option  
  [Farm node \(Management Console\)](#) 2nd

session tickets  
  [Secure Ticket Authority \(STA\)](#)

sessions  
  [disabling during new application installations](#) 2nd

Program Neighborhood Agent Console  
  [configuration options](#) 2nd

screen updates  
[accelerating \(SpeedScreen technology\) 2nd](#)

Shadow option

User Sessions Management node

[Management Console](#)

Shadow session (ICA)

[IMA protocol](#)

shadow sessions

[auditing \(IMA protocol\) 2nd](#)

Shadow Taskbar

[\(Management Console\)](#)

[Applications window](#)

[benefits](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

[launching](#)

[Servers window](#)

[Users window](#)

shadowing

MetaFrame Presentation Server (MPS)

[configuring 2nd](#)

[Shadowing policy rule \(user policy\) 2nd](#)

shared license servers

[MASL deployment 2nd 3rd 4th](#)

shortcuts

[MeasureUp 2nd](#)

Simple Network Management Protocol, [See [SNMP](#)]

single sign-on authentication

[Web Interface](#)

site tasks (Web Interface)

[Configure Authentication Methods \(MPS 4.0\) 2nd](#)

[Control Diagnostic Logging \(MPS 4.0\)](#)

[Customize Appearance for Users \(MPS 4.0\) 2nd](#)

[Manage Client Connection Settings \(MPS 4.0\)](#)

[Manage Client Deployment \(MPS 4.0\) 2nd](#)

[Manage Client-side Proxy \(MPS 4.0\)](#)

[Manage Secure Client Access \(MPS 4.0\) 2nd](#)

[Manage Server Farms \(MPS 4.0\) 2nd](#)

[Manage Workspace Control \(MPS 4.0\)](#)

smart cards

authentication pass-through

[MPS 4.0 security](#)

recognition support

[MPS 4.0 security](#)

[roaming support](#)

SmartCard authentication

[Web Interface](#)

SNMP

[\(Simple Network Management Protocol\)](#)

[monitoring functions on MetaFrame Presentation Server](#)

SNMP option

[Farm node \(Management Console\) 2nd](#)

software

clients

[naming conventions 2nd](#)

MPS 3.0 requirements

[TCP/IP 2nd](#)

[Terminal Services, enabling](#) 2nd 3rd 4th

[Terminal Services, licensing](#) 2nd

software (MPS/EE)

administrative tools

[Citrix Connection Configuration \(CCC\) tool](#)

[ICA Client Distribution Wizard](#)

[ICA Client Printer Configuration](#)

[ICA Client Update Configuration](#)

[ICA Toolbar](#)

[Shadow Taskbar](#)

[SpeedScreen Latency Manager](#)

[SSL Relay Configuration tool](#)

management tools

[Access Suite Console](#)

[Management Console for MetaFrame Presentation Server](#)

Sort Table option

User Sessions Management node

[Management Console](#)

Specify Application Appearance window

[Application Publishing Wizard](#) 2nd

Specify Application Limits window

[Application Publishing Wizard](#) 2nd

Specify Clients Requirements window

[Application Publishing Wizard](#) 2nd

Specify File Type Association window

[Application Publishing Wizard](#) 2nd

Specify Servers window

[Application Publishing Wizard](#) 2nd

Specify Users window

[Application Publishing Wizard](#) 2nd

SpeedScreen

[Browser Acceleration](#) 2nd

[Flash Acceleration](#)

Latency Reduction

[Local Text Echo](#) 2nd

[Mouse Click Feedback](#) 2nd

MetaFrame servers

[setting](#)

[Multimedia Acceleration](#)

screen updates

[performance features](#) 2nd

SpeedScreen Browser Acceleration option

[Farm node \(Management Console\)](#) 2nd

SpeedScreen control virtual channel

[ICA protocol](#)

SpeedScreen Flash Acceleration option

[Farm node \(Management Console\)](#)

[SpeedScreen Latency Manager](#)

SpeedScreen Latency Reduction Manager

applications

[adding](#) 2nd

[properties, setting](#) 2nd 3rd 4th

[benefits of](#)

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th

[function of](#)

[launching](#)

settings

[replicating to other servers in farm](#)

SpeedScreen Multimedia Acceleration option

[Farm node \(Management Console\)](#)

SSL

[Web Interface support](#)

[SSL Relay 2nd 3rd](#)

[client requirements 2nd 3rd](#)

[configuring 2nd](#)

root certificates

[obtaining 2nd 3rd](#)

server certificates

[installing 2nd](#)

[obtaining 2nd 3rd](#)

[server requirements](#)

[SSL Relay Configuration tool](#)

SSL/TLS

[session communications](#)

SSL/TLS+HTTPS protocol

[program Neighborhood \(PN\) 2nd](#)

[startup grace periods](#)

[MASL licensing 2nd 3rd](#)

Status option

User Sessions Management node

[Management Console](#)

storing

historical data

[Summary Database Server \(Resource Manager\) 2nd](#)

subsystems management

IMA protocol

[MetaFrame Presentation Server 2nd](#)

summary data

[storing \(Resource Manager\) 2nd](#)

[Summary Database Server \(Resource Manager\)](#)

[configuring 2nd](#)

historical data

[storing 2nd](#)

summary reports

[generating \(Resource Manager\) 2nd](#)

Sun Java Runtime Environment (JRE)

[License Management Console \(LMC\)](#)

[symmetric-key encryption](#)

system requirements

MASL

[disk space 2nd](#)

[memory 2nd](#)

[network bandwidth](#)

[processors 2nd](#)

[supported platforms](#)

Systems Management Server (SMS)

Win32 Presentation Server Client

[installation method](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

Target Server

[Installation Server \(MPS\)](#)

[target server \(Installation Manager\)](#)

TCP/IP

[default installations by Windows Server 2000/2003 2nd](#)

TCP/IP protocol

[program Neighborhood \(PN\) 2nd](#)

TCP/IP+HTTP protocol

[program Neighborhood \(PN\) 2nd](#)

Terminal Server

[enabling for application installations](#)

[MultiWin technology](#)

[Terminal Server Client Access Licenses \(TSCALs\)](#)

testing

[MeasureUp](#)

[creating shortcuts 2nd](#)

[installing 2nd 3rd](#)

[multiple test modes 2nd](#)

[troubleshooting](#)

Thomson Prometric

[exam administration](#)

[Time Zones policy rule \(user policy\) 2nd](#)

time-based licensing

[license servers \(MASL\)](#)

TLS

[Web Interface support](#)

Tomcat servlet engine

[License Management Console \(LMC\)](#)

tools

administrators

[access management 2nd](#)

tracking

remaining certification requirements

[Citrix.com 2nd](#)

troubleshooting

[MeasureUp](#)

TWAIN client devices

[redirection of](#)

typical users

hardware size requirements (MPS)

[resource allocation 2nd](#)

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

unattended installations

  MetaFrame Presentation Server

    executing 2nd

unattended programs

  packaging (Packager utility) 2nd

Unicode

  template files

    Web Interface support

uninstalling

  applications

    in isolation environments 2nd

    Load Manager 2nd

    MASL 2nd 3rd

    MetaFrame Presentation Server (MPS) 2nd

universal printer drivers (UPDs) 2nd 3rd 4th

  client versions

    PCL4 (Printer Control Language)

    PCL5c (Printer Control Language)

    PS (PostScript)

    managing 2nd

UNIX client

updates

  frequency of

    changing (Load Manager) 2nd

upgrade licenses

  MPS 3.0

upgrading

  Resource Manager

    component order

usage billing

  Resource Manager

    cost centers

    fee profiles

usage reports

  viewing (Load Manager) 2nd

user accounts

  Users filter (user policies)

user groups

  Users filter (user policies)

user loads

  hardware size requirements (MPS)

    application types 2nd

    power user category 2nd

    typical user category 2nd

user policies

  assigning via filters

[characteristics](#) 2nd 3rd 4th 5th 6th 7th 8th

[Citrix.com resources](#)

client printers

[configuring](#)

[conflicting](#)

[creation of 2nd](#)

effectiveness

[determination of 2nd 3rd](#)

[exam prep questions](#) 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th

exceptions

[defining 2nd](#)

[filters 2nd](#)

[Allow access](#)

[by client IP addresses](#)

[by client names](#)

[by server names](#)

[by usernames](#)

[Client IP Address](#)

[Client Name](#) 2nd

[Deny access](#) 2nd

[Server 2nd](#)

[Users](#)

[Users, accounts](#)

[Users, anonymous](#)

[Users, groups](#)

[Users, nonanonymous](#)

[function of](#)

[managing \(Management Console\)](#)

[override exceptions](#) 2nd 3rd

[priority numbers](#) 2nd 3rd 4th

resultant sets

[searching by](#) 2nd 3rd

[rules 2nd](#)

[Bandwidth](#) 2nd 3rd

[Client Devices](#) 2nd 3rd 4th

[Connections](#) 2nd

[Content Redirection](#)

[disabled state](#) 2nd 3rd

[enabled state](#) 2nd

[MetaFrame Password Manager](#) 2nd

[not configured state](#) 2nd

[Security](#) 2nd

[Shadowing](#) 2nd

[Time Zones](#) 2nd

[User Workspace](#)

User Session Management node

[Management Console](#)

[Connect option](#)

[Disconnect option](#)

[Filter Table option](#)

[Logoff Selected Session option](#)

[Reset option](#)

[Send Message option](#)

[Session Information option](#)

[Shadow option](#)

[Sort Table option](#)

## Status option

user sessions

- [Advanced rule evaluator 2nd](#)
- [Application User Load rule evaluator](#)
- [Context Switches rule evaluator](#)
- [CPU Utilization rule evaluator](#)
- [Default rule evaluator 2nd](#)
- [Disk Data I/O rule evaluator](#)
- [Disk Operations rule evaluator](#)
- [IP Range rule evaluator](#)
- [License Threshold rule evaluator 2nd](#)
- [Memory Usage rule evaluator](#)
- [Page Fault rule evaluator](#)
- [Page Swap rule evaluator](#)
- [Scheduling rule evaluator](#)
- [Server User Load rule evaluator](#)

[User Workspace policy rule \(user policy\)](#)

usernames

- user policies
  - [filtering criteria](#)

users

[anonymous user accounts](#)

application sets

[generating \(Web Interface\) 2nd 3rd 4th](#)

[shadowing \(Shadow Taskbar\)](#)

Users filter

- [user policies](#)
  - [accounts](#)
  - [anonymous](#)
  - [groups](#)
  - [nonanonymous](#)

 PREV

NEXT 

# Index

[SYMBOL] [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Z](#)

[VeriSign certificate authority](#)

View Only category

[administrator privileges](#) 2nd

viewing

    Load Manager logs

[ICA connections to server](#) 2nd

metrics

[Resource Manager](#) 2nd 3rd

virtual channels

[ICA protocol](#)

[audio](#)

[Clipboard mapping](#)

[drive mapping](#)

[font and keyboard layout](#)

[ICA display](#)

[parallel port mapping](#)

[printer spooling](#)

[serial port mapping](#)

[SpeedScreen control](#)

virtual IP addresses

applications

[applying](#) 2nd

virtual loopback addresses

applications

[applying](#) 2nd

virtual memory

[optimization \(MPS 4.0\)](#) 2nd 3rd

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

web browsers

[License Management Console \(LMC\) 2nd](#)

Web Client

[Win32 client type 2nd 3rd](#)

Web client

self-extracting executables

[installation settings 2nd 3rd](#)

Web Interface

application sets

[generating for users 2nd 3rd 4th](#)

[authentication methods](#)

[anonymous](#)

[explicit login](#)

[password changes](#)

[single sign-on](#)

[SmartCard](#)

[bandwidth tuning \(MPS 4.0\)](#)

[Citrix XML Service error reporting \(MPS 4.0\)](#)

client deployment

[configuring 2nd 3rd](#)

client-side proxy server options

[configuring](#)

communication scenarios

[with client web browsers 2nd](#)

[with Presentation Server 2nd](#)

[components 2nd](#)

configuration methods

[Web Interface configuration file 2nd](#)

[Web Interface Console 2nd 3rd 4th 5th 5th](#)

[Customization Wizard \(MPS 4.0\)](#)

[end-user changes \(MPS 4.0\)](#)

error messages

[disabling 2nd](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th 9th](#)

features summary

[Active Directory support](#)

[ActiveX client deployment control](#)

[address translation support](#)

[anonymous user logons](#)

[application publishing support](#)

[IIS multiple site support](#)

[load balancing and failover support](#)

[multiple server farm support](#)

[Novell Directory Services \(NDS\) support](#)

[PDA support](#)

[Presentation Server client deployment support](#)

[Program Neighborhood Agent \(PN Agent\)](#)  
[Remote Desktop \(RDP\) support](#)  
[Secure Gateway for Presentation Server](#)  
[session authentication tickets](#)  
[SSL/TLS support](#)  
[Unicode support for template files](#)  
[Windows-based Terminal Support \(WBT\) support](#)  
[Workspace Control](#)

[installation of](#)  
installation process  
    [general guidelines](#) 2nd  
    [testing](#)

installation requirements  
    [MetaFrame Server](#) 2nd  
    [Presentation Server client devices](#) 2nd  
    [web servers](#) 2nd  
[Java client fallback support \(MPS 4.0\)](#)

listings  
    [Portion of the Default template.ica File \(14.1\)](#) 2nd  
[managing via Access Suite Console \(MPS 4.0\)](#) 2nd 3rd  
[multi-language support \(MPS 4.0\)](#)  
[multiple site support \(MPS 4.0\)](#)  
[new MPS 4.0 features](#) 2nd 3rd 4th  
[Novell NDS authentication support \(MPS 4.0\)](#)

Program Neighborhood Agent Console  
    [accessing](#)  
    [Application Display page](#) 2nd  
    [client configuration](#) 2nd  
    [Client Tab Control page](#) 2nd  
    [configuration options](#)  
    [features](#)  
    [Logon Methods page](#) 2nd  
    [Manage Configuration File page](#) 2nd  
    [page appearance](#)  
    [Remote Desktop \(RDP\) Web Connection software](#) 2nd 3rd  
    [Session Options page](#) 2nd  
    [Workspace Control page](#)  
[Remote Configuration feature \(MPS 4.0\)](#) 2nd  
[Remote Configuration tool \(MPS 4.0\)](#)

Secure Gateway  
    [server farm access](#) 2nd 3rd 4th  
[Secure Gateway feature \(MPS 4.0\)](#) 2nd

Server Settings  
    [network address translation \(NAT\)](#) 2nd 3rd  
    [Secure Gateway support](#) 2nd  
    [server farm management](#) 2nd  
    [server load balancing](#) 2nd  
    [server ordering](#) 2nd  
[site grouping \(MPS 4.0\)](#)

site tasks  
    [Configure Authentication Methods \(MPS 4.0\)](#) 2nd  
    [Control Diagnostic Logging \(MPS 4.0\)](#)  
    [Customize Appearance for Users \(MPS 4.0\)](#) 2nd  
    [Manage Client Connection Settings \(MPS 4.0\)](#)  
    [Manage Client Deployment \(MPS 4.0\)](#) 2nd  
    [Manage Client-side Proxy \(MPS 4.0\)](#)

[Manage Secure Client Access \(MPS 4.0\) 2nd](#)

[Manage Server Farms \(MPS 4.0\) 2nd](#)

[Manage Workspace Control \(MPS 4.0\)](#)

site types

[Conferencing Manager Guest Attendee 2nd](#)

[MetaFrame Presentation Server 2nd](#)

[Program Neighborhood Agent Services 2nd](#)

Workspace Control

[configuring](#)

Web Interface (MPS)

[HTTPS](#)

[logons 2nd](#)

[PNAgent \(Program Neighborhood Agent\)](#)

[versus Citrix Secure Gateway 2nd 3rd](#)

Web Interface Console

[accessing URL 2nd](#)

[component diagram/link settings 2nd](#)

[page appearance](#)

Web Interface for Presentation Server

Win32 Presentation Server Client

[client installation method 2nd](#)

web servers

Web Interface

[installation requirements 2nd](#)

web sites

Citrix.com

[user policy resources](#)

web-based console

license servers (MASL)

[administering 2nd](#)

websites

certificate authorities (CAs)

[Baltimore Technologies](#)

[VeriSign](#)

Citrix

[MetaFrame Presentation Server documentation resources](#)

[MetaFrame Presentation Server home page](#)

Citrix.com

[CCI \(Citrix Certified Instructor\) applications](#)

[class information](#)

[documentation resources](#)

[exam life cycle dates](#)

[Feature Matrix spreadsheet 2nd 3rd 4th 5th 6th](#)

[PDF online documentation 2nd 3rd 4th 5th 6th 7th 8th](#)

[remaining certification requirements, tracking 2nd](#)

ExamCram2.com

[exam resources](#)

Macrovision Corporation

[MSI transform file creator](#)

Prometric.com

[exam test dates](#)

Wise Solutions

[MSI transform file creator](#)

wfclient.ini file

[Program Neighborhood \(PN\)](#)

Wfica.cab

[Win32 Presentation Server Client cabinet-based installation file 2nd](#)

Wficac.cab

[Win32 Presentation Server Client cabinet-based installation file 2nd](#)

Wfcat.cab

[Win32 Presentation Server Client cabinet-based installation file 2nd](#)

Win32 Presentation Server Client 2nd 3rd 4th

[Citrix Feature Matrix website 2nd 3rd 4th 5th 6th](#)

deployment methods

[downloading from network share points 2nd](#)

[installing via Active Directory \(AD\)](#)

[installing via Client Update Database 2nd](#)

[installing via Components CD](#)

[installing via floppy disks 2nd](#)

[installing via System Management Server \(SMS\)](#)

[selection criteria 2nd](#)

[web-based 2nd](#)

[exam prep questions 2nd 3rd 4th 5th 6th 7th 8th](#)

[ICA Client Update Database](#)

[characteristics 2nd](#)

[client additions/updates 2nd](#)

[client properties 2nd](#)

[databases, creating 2nd](#)

[properties, managing 2nd 3rd](#)

[ICA Pass-through Client 2nd](#)

installation files

[cabinet-based files 2nd](#)

[MSI Client Package](#)

[MSI Client Package, custom deployments 2nd 3rd 4th 5th 6th 7th 8th 9th 10th 11th 12th 13th 14th 15th 16th 17th 18th 19th 20th 21st](#)

[self-extracting executables](#)

[README file](#)

[Windows 16-bit client](#)

Windows 2000 Datacenter Server

MPS 3.0

[hardware size requirements](#)

Windows 2000 Server

[licensing requirements for MPS 3.0 2nd 3rd](#)

MetaFrame Presentation Server (MPS)

[installation of 2nd](#)

MPS

[TCP/IP default installation 2nd](#)

MPS 3.0

[hardware size requirements 2nd](#)

Terminal Services

[enabling for MPS 3.0 2nd 3rd 4th](#)

[licensing for MPS 3.0 2nd](#)

Windows CE

client printers

[configuring 2nd](#)

[Windows CE client](#)

[Windows PocketPC client](#)

Windows Server 2003

[licensing requirements for MPS 3.0](#)

MetaFrame Presentation Server (MPS)

[installation of 2nd](#)

MPS

[TCP/IP default installation 2nd](#)

Terminal Services

[enabling for MPS 3.0 2nd 3rd 4th](#)

[licensing for MPS 3.0 2nd](#)

Windows Server 2003 Datacenter Edition

MPS 3.0

[hardware size requirements](#)

Windows Server 2003 Enterprise Edition

MPS 3.0

[hardware size requirements](#)

Windows Server 2003 Standard Edition

MPS 3.0

[hardware size requirements](#)

Windows-based Terminal Support (WBT)

[Web Interface support](#)

Wise Solutions website

[MSI transform file creator](#)

Workspace Control

Program Neighborhood Agent Console

[configuration options](#)

Web Interface

[configuring](#)

[Web Interface support](#)

Workspace Control option

Servers mode

[Management Console](#)

workstations

Management Console (MPS)

[support requirements 2nd](#)

 PREV

NEXT 

 PREV

NEXT 

# Index

[\[SYMBOL\]](#) [\[A\]](#) [\[B\]](#) [\[C\]](#) [\[D\]](#) [\[E\]](#) [\[F\]](#) [\[G\]](#) [\[H\]](#) [\[I\]](#) [\[J\]](#) [\[K\]](#) [\[L\]](#) [\[M\]](#) [\[N\]](#) [\[O\]](#) [\[P\]](#) [\[Q\]](#) [\[R\]](#) [\[S\]](#) [\[T\]](#) [\[U\]](#) [\[V\]](#) [\[W\]](#) [\[X\]](#) [\[Z\]](#)

XML Service

MetaFrame Presentation Server (MPS)

[installation options 2nd](#)

 PREV

NEXT 

# Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Z]

zone-based administrative delegation 2nd

zones

IMA protocol

Data Collectors (DCs) 2nd

Data Collectors (DCs) elections 2nd 3rd

MetaFrame Presentation Server

Zones option

Farm node (Management Console) 2nd 3rd