Citrix Presentation Server Administrator's Guide

Citrix Presentation Server™ 4.5 for Windows®

Copyright and Trademark Notice

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

Copyright © 2001-2007 Citrix Systems, Inc. All rights reserved.

Citrix, ICA (Independent Computing Architecture), and Program Neighborhood are registered trademarks, and Citrix Presentation Server, Citrix Access Suite, Citrix Password Manager, Citrix Developer Network, and SpeedScreen are trademarks of Citrix Systems, Inc. in the United States and other countries.

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

Trademark Acknowledgements

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

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

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

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

Portions of this software are based in part on the work of the Independent JPEG Group.

Portions of this software contain imaging code owned and copyrighted by Pegasus Imaging Corporation, Tampa, FL. All rights reserved.

Macromedia and Flash are trademarks or registered trademarks of Macromedia, Inc. in the United States and/or other countries.

Microsoft, MS-DOS, Windows, Windows Media Player, Windows Server, Windows NT, Win32, Outlook, Outlook Express, Internet Explorer, ActiveX, Active Directory, Access, SQL Server, SQL Server Express Edition, and DirectShow are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

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

Oracle database is a registered trademark of Oracle Corporation.

RealOne is a trademark of RealNetworks, Inc.

SpeechMike is a trademark of Koninklijke Philips Electronics N.V.

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

Document Code: 2/21/07 (LW)

Contents

Chapter 1 Welcome

New in This Release 12
Product Documentation and Information 13
Accessing Documentation 13
Document Conventions 14
Customizing Citrix Presentation Server 15

Chapter 2 Planning for Deployment

Obtaining Installation and Update Information 17
Installation Checklist 17
Pre-Installation Update Bulletin 17
System Requirements 18
Software Requirements 18
Hardware Requirements 19
System Account Considerations 20
Establishing Domain Trust Relationships 20
Trust-Based Routing 21
Changing Domain Trust Relationships 22
Recommendations for Active Directory Environments 22
Planning for Client and Server Communications 26
Linking Clients and Servers 26
Communicating with the Citrix XML Service 32
Planning the Data Store 33
Choosing a Database 34
Planning for IMA Encryption 41
Deciding to Change Server Drive Letters 42

Chapter 3 Deploying Citrix Presentation Server

Choosing a Method of Installation 46

Preparing Your Environment 48
Remapping Server Drive Letters. 49
Setting Up the Data Store 49
Substituting Domain Accounts for Local Accounts 50
Enabling Windows MUI Support 51
Creating and Upgrading Farms. 51
Creating a New Farm 52
Choosing Options for New Farms 53
Deploying Subsequent Servers 73
Joining a Server Farm 74
Upgrading or Migrating an Existing Server Farm 77
Upgrading Automatically 81
Migrating from Earlier Versions of Citrix Presentation Server 84
Configuring Presentation Server after Installation. 85
Deploying Client Software to Users. 86
Choosing a Client Deployment Method 87
Using Remote Desktop Web Connection Software 93
Removing Citrix Presentation Server. 94

Chapter 4 Management Console Overview

Management Consoles and Other Tools 97
Choosing Which Console to Use 99
Using the Access Management Console 100
Users and Accounts 100
The Access Management Console User Interface 102
Starting the Access Management Console 104
Finding Items in Your Deployment Using Discovery 104
Customizing Your Displays Using My Views 105
Performing Tasks with the Access Management Console 106
Using the Citrix Presentation Server Console 112

Chapter 5 Publishing Resources

Using the Application Publishing Wizard 116
Specifying Locations for Published Content 118
Configuring User Access to Published Resources 118
Associating Published Applications with File Types 120
Managing Resource Launching with Content Redirection 122
Redirecting Content from Client to Server 122
Redirecting Content from Server to Client 123

Using Policies to Configure Access to Published Resources 125
Creating Policies 126
Configuring Policy Rules 127
Policy Rules 128
Applying Policies with Filters 131
Using Multiple Policies 132

Chapter 6 Advanced Resource Publishing

Using Virtual IP Addresses with Published Applications 135
How Virtual IP Addressing Works 136
Assigning IP Address Ranges 138
Configuring Virtual IP for Applications 138
Using the Client IP Address Feature 139
Providing the Client IP Address to an Application 139
Providing Virtual IP Address Ranges to Sessions 140
Providing Virtual Loopback Addresses 142
Enabling Application Processes to Use Virtual IP or Virtual Loopback 142
Monitoring Virtual Loopback and IP Addresses 143
Isolating Published Applications 144
Enabling and Disabling Isolation Environments 145
Creating an Isolation Environment 145
Configuring an Isolation Environment 146
Using an Isolation Environment 147
Isolation Environment Rules 149
Removing Applications Installed in Isolation Environments 151
Deleting Isolation Environments 152
Setting CPU Priority Levels for Published Applications 153
Assigning CPU Priority Levels to Applications 154
Providing Resources to Novell Directory Services Users 155
Enabling NDS Support 156
Publishing Resources in an NDS-Enabled Environment 159
Enabling PDA Synchronization Support 160
Enabling TWAIN Redirection Support 161

Chapter 7 Managing User Access

Setting up User Logons 163
Controlling User Logon Look and Feel 164
Providing Users with Workspace Control 164

Configuring User Connections 166
Selecting Connection Settings. 166
Establishing Connection Controls. 167
Administering User Sessions 171
Managing Sessions with the Access Management Console. 171
Using Session Shadowing 174
Configuring Client Device Mapping. 178
Optimizing Session Performance 180
Configuring Audio for User Sessions 191
Configuring Support for Active Directory Federation Services (ADFS) 196

Chapter 8 Securing Server Farms

Securing Access to Your Servers 197
Securing the Data Store 198
Securing Network Communications 200
Configuring User Authentication 214
Configuring Authentication for Workspace Control 214
Configuring Kerberos Logon 215
Using Smart Cards with Citrix Presentation Server 217
Encrypting Sensitive Configuration Logging Data 219
Using the IMA Encryption Utility 221
Enabling IMA Encryption after Installation 222
Storing the Key on a Shared Location 224
Changing Farms. 225
Enabling IMA Encryption as a Local Administrator 225
Other IMA Encryption Features 226

Chapter 9 Maintaining Server Farms

Logging Administrative Changes. 229
Enabling Configuration Logging 230
Using Configuration Logging 235
Using Health Monitoring & Recovery 238
Accessing Tests 238
Adding Tests to a Server 240
Modifying Test Settings 240
Developing Custom Tests 242
Getting Alerts. 243
Monitoring Performance of Sessions and Servers 243

Managing CPU Usage 245
Enabling CPU Utilization Management 246
Managing Virtual Memory Usage 247
Enabling Memory Utilization Management 248
Scheduling Virtual Memory Optimization 248
Excluding Applications from Memory Optimization. 249
Working with the Local Host Cache 250
Updating Citrix License Server Settings 252

Chapter 10 Managing Printers

Planning Your Deployment 255
Printer Configurations 256
Network Considerations 257
SmoothRoaming and Proximity Printing 257
Managing Drivers 258
Printing Policies. 259
Implementing Your Deployment 260
Implementing and Managing Client Printers 260
Implementing and Managing Network Printers 270
Limiting Printing Bandwidth 272
Managing Printer Drivers 273
Configuring Printing with the Presentation Server Console 278

Appendix A Citrix Presentation Server Commands

ACRCFG. 285
AIERUN 288
AIESETUP 289
ALTADDR 292
APP 294
APPUTIL 296
AUDITLOG 300
CHANGE CLIENT 302
CHFARM 305
CLTPRINT 308
CTXKEYTOOL 309
CTXXMLSS 311
DRIVEREMAP 312
DRIVEREMAP64 316
DSCHECK 320

DSMAINT 322
ENABLELB 327
ICAPORT 328
IMAPORT. 329
MIGRATETOSQLEXPRESS 330
QUERY. 331
Query Farm 331
Query Process 333
Query Server 334
Query Session 336
Query Termserver 337
Query User. 338
RADEMAINT 340
TWCONFIG 341

Appendix B Delegated Administration Tasks

Farm Folder Tasks 344
Administrators Folder Tasks. 344
Applications Folder Tasks 345
Installation Manager Folder Tasks 346
Isolation Environment Folder Tasks 347
Load Evaluator Folder Tasks 347
Monitoring Configuration Folder Tasks. 348
Policies Folder Tasks 349
Printer Management Folder Tasks 349
Resource Manager Folder Tasks 350
Servers Folder Tasks. 351

Appendix C Performance Counters

Citrix CPU Utilization Mgmt User Counters. 356
Citrix IMA Networking Counters 356
Citrix Licensing. 357
Citrix MetaFrame Presentation Server Counters 357
ICA Session Counters. 359
Secure Ticket Authority Counters. 362

Appendix D Advanced Installation Methods

Unattended Installations 365
Deploying Windows Installer Packages. 366

Creating Transforms 367
Creating and Using an Answer File 368
Using Windows Installer Commands. 369
Sample Transforms and Setup Properties 373
Editing the Sample Transforms. 373
Localdb_access_create.mst. 374
Join_Indirect.mst. 375
thirdpartydb_create_direct.mst 376
thirdpartydb_join_direct.mst 377
Setup Property Names and Values 378
Pass-Through Client Properties. 392

Appendix E Data Store Database Requirements

Supported Databases. 395
Microsoft Access 397
Minimum Requirements 397
Authenticating to the Access Database. 397
Backing up the Access Database. 398
Microsoft SQL Server 2005 Express Edition SP1 398
Minimum Requirements 400
Authenticating to the SQL Server 2005 Express SP1 Database 401
Migrating to SQL Server 2005 Express 401
Microsoft SQL Server. 405
Minimum Requirements 405
Authenticating to the Microsoft SQL Server Database 405
Configuring Microsoft SQL Server 406
Using Sockets Rather than Named Pipes 407
Failover 408
Distributed Databases 409
Migrating to SQL Server. 410
Oracle 410
Minimum Requirements 410
Authenticating to the Oracle Database 411
Configuring an Oracle Data Store. 412
Migrating to Oracle 413
Failover 413
Distributed Databases 414
Using Oracle Real Application Clusters 415

IBM DB2. 415
Minimum Requirements 416
Distributed Databases 417
Migrating to IBM DB2 417

CHAPTER 1

Welcome

This administrator's guide is part of the Citrix Presentation Server documentation set and is provided to assist you in the planning, deployment, and administration of your server farm. It is organized as follows:

- Planning your server farm deployment and then installing Citrix Presentation Server are described in Chapters 2 and 3.
- Using the management consoles is described in Chapter 4.
- Publishing resources—applications, content, and server desktops—is described in Chapters 5 and 6.
- Managing user sessions is described in Chapter 7.
- Securing your Presentation Server environment is described in Chapter 8.
- Maintaining your server farms is described in Chapter 9.
- Making printing resources available to your users is described in Chapter 10.
- Reference information concerning Citrix Presentation Server commands, delegated administration tasks, performance monitoring counters, unattended installation properties, and data store database requirements is provided in the appendices.

Important Before you install Citrix Presentation Server, review the *Citrix Presentation Server Readme*, located in the Documentation directory of the product CD.

New in This Release

The following features are new for this release:

- **Configuration Logging.** See "Logging Administrative Changes" on page 229 for more information.
- **Health Monitoring & Recovery.** See "Using Health Monitoring & Recovery" on page 238 for more information.
- **SpeedScreen Progressive Display.** See "SpeedScreen Progressive Display" on page 190 for more information.
- **Trusted Server Configuration.** See "Trusted Server Configuration" on page 198 for more information.
- **Application Streaming.** See the *Citrix Application Streaming Guide* for more information.

Note For additional information about new and important features, see *Getting Started with Citrix Presentation Server*.

Product Documentation and Information

Citrix provides a variety of information resources online, including a complete product documentation library, documentation updates, and technical articles on the Citrix Web site at http://www.citrix.com. The documentation for Citrix Presentation Server includes online guides, known issues information, and Help.

- Online guides are provided as Adobe Portable Document Format (PDF) files. To view, search, and print the PDF documentation, you need to have Adobe Acrobat Reader 5.0.5 with Search, or Adobe Reader 6.0 through 7.0. You can download these products for free from Adobe Systems' Web site at http://www.adobe.com/.
- Be sure to read all the readme files and the Installation Checklist before you install Citrix Presentation Server or when troubleshooting. These files contain important information that includes last-minute documentation updates and corrections.
- Online help is available in many components. You can access the online help from the **Help** menu or **Help** button.
- For information about terminology related to Presentation Server, see the *Citrix Presentation Server Glossary* (available from the Document Center).

Note To provide feedback about the documentation, go to www.citrix.com and click **Support > Knowledge Center > Product Documentation**. To access the feedback form, click the **Submit Documentation Feedback** link.

Accessing Documentation

The Document Center is a PDF file that provides a single point of access to the online guides and enables you to go straight to the section in the documentation that you need. It also includes:

- A list of common tasks and a link to each item of documentation.
- A search function that covers all the PDF guides. This is useful when you need to consult a number of different guides.
- Cross-references among documents. You can move among documents using the links to other guides and the links to the Document Center.

You can access the Document Center from the product CDs or install it on your servers when you install Citrix Presentation Server and its components.

To start the Document Center

1. From your product CD, navigate to the Documentation folder.

   -or-

   On a server on which you installed the Document Center, select **Documentation** from the Citrix program group on the server's **Start** menu.

2. Open **document_center.pdf**. The Document Center appears.

If you prefer to access the documentation without using the Document Center, you can navigate to the individual files using Windows Explorer.

More information about Citrix documentation, and details about how to obtain further information and support, is included in *Getting Started with Citrix Presentation Server*.

Document Conventions

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

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes, option buttons, and user input.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics are also used for new terms and the titles of books.
%SystemRoot%	The Windows system directory, which can be WINNT, WINDOWS, or any other name you specify when you install Windows.
`Monospace`	Text displayed in a text file.
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [**/ping**] means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename*[,…] means you can type additional *devicenames* separated by commas.

Customizing Citrix Presentation Server

Citrix Presentation Server includes public interfaces that allow Citrix administrators and partners to customize most aspects of managing Presentation Server through an Application Programming Interface (API). Many of the operations that you can perform through the Presentation Server consoles can be customized using these interfaces. The two main Citrix server software development kits (SDKs), the Citrix Presentation Server MPSSDK and Citrix Presentation Server CPSSDK, are the primary resources for developers using these interfaces because they provide related documentation and examples. The MPSSDK includes information about MFCOM, an interface that comprises mainly Presentation Server farm management functions. The CPSSDK is a next-generation API based on Microsoft .NET technology that provides additional information about farm management functions, including Resource Manager.

The MPSSDK and CPSSDK are available for download from the Citrix Developer Network. This open-enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate Citrix computing solutions into their products.

CHAPTER 2

Planning for Deployment

This chapter covers the planning steps to consider before you install Citrix Presentation Server and deploy your server farm.

Obtaining Installation and Update Information

Before you install Presentation Server, Citrix recommends that you read the Installation Checklist and the Pre-installation Update Bulletin.

Installation Checklist

To access the Installation Checklist, select "View installation checklist" on the Presentation Server Setup window that appears after inserting your installation CD, or navigate to \Documentation\docs\checklist.html on either installation CD.

This document includes information about:

- Downloading and installing critical updates before and after you install the product
- Meeting system requirements
- Installing and configuring Citrix Licensing

Pre-Installation Update Bulletin

The Citrix Access Suite Pre-installation Update Bulletin offers late-breaking information and links to critical updates for server operating systems and Citrix installation files. These updates may be required to install or run the product and should be applied prior to installation. Information regarding the required updates is on the Pre-installation Update Bulletin. A link to the bulletin is available on the *Installation Checklist for Citrix Presentation Server*.

System Requirements

This section briefly describes the software and hardware requirements and recommendations for installing Citrix Presentation Server. For a complete list of the system requirements for all components of Citrix Presentation Server, see the *Installation Checklist for Citrix Presentation Server.* For information about system requirements for client devices, see the administrator's guide for each client platform.

Software Requirements

You can install Citrix Presentation Server 4.5 on computers running the Microsoft Windows Server 2003 family (with SP1 or SP2): Standard Edition, Enterprise Edition, and Datacenter Edition.

Note The installation of Citrix Presentation Server on Windows domain controllers is not supported.

Citrix Presentation Server is supported on both 32-bit and 64-bit operating systems. The procedures in this guide are primarily based on 32-bit operating systems and differences for 64-bit operating systems are noted. For more information about 64-bit issues, see the *Citrix Presentation Server Readme*.

Before you begin installing Presentation Server, it is important to understand how Presentation Server Setup treats software system requirements. If you are performing an installation using any method other than Autorun, you must install all system requirements before you begin Presentation Server installation. If you are installing Presentation Server using the Autorun, some system requirements are installed for you automatically and others are not. You must install the system requirements that are not installed during Autorun Setup before you begin, otherwise the installation fails.

As a general rule, Autorun Setup installs most non-Windows system requirements, such as the Java Runtime Environment, .NET Framework Version, and Microsoft Visual J#. It does not install any Windows system requirements that are available from your operating system CD or need to be configured as roles. Likewise, it does not perform any of the pre-installation configurations that you need to perform on your server, such as specify the terminal services role, enabling Internet Information Services (IIS) and so on.

In addition, system requirements must be installed and configured in a very specific sequence. Citrix recommends that you remap server drives, if desired, before you install any system requirements, including .NET 2.0. See the Installation Checklist on the Server CD and “Preparing Your Environment” on page 48 for information about the installation sequence for pre-requisites. For more information, see “Deciding to Change Server Drive Letters” on page 42.

Important You must install the Terminal Server component (in Application Server mode) before you install Citrix Presentation Server. Terminal Server is not installed with Windows by default. The installation of Terminal Server entails using the Manage Your Server wizard to add the *terminal services* role to your server.

Citrix Presentation Server supports the 2007 change in Daylight Saving Time in the United States. If your applications are affected by change, make sure that you upgrade your installation of the Java Runtime Environment (JRE) to the same level as that specified in the Installation Checklist. The Citrix Presentation Server JRE requirement meets the level Sun recommends to resolve potential JRE issues resulting from the Daylight Saving Time change.

Hardware Requirements

The hardware requirements for a Presentation Server deployment are based on the edition of Windows Server 2003 you are using. For more information, see the Microsoft Web site for the latest system requirements for the edition of Windows Server 2003 on which you are deploying your server farm.

For information about system sizing, optimization, configuration, and deployment scenarios, see the *Advanced Concepts Guide for Citrix Presentation Server*. This guide is available from the Support area of the Citrix Web site at http://support.citrix.com.

Note Citrix recommends that you set the graphics displays for computers running the management consoles to at least 1024 x 768 pixels.

System Account Considerations

When planning your deployment and deciding how to configure your Citrix administrator accounts, consider the following points:

- One full authority administrator account must always exist in the server farm. Therefore, Citrix Presentation Server prevents you from deleting the last full authority administrator account. However, if no administrator accounts exist in the farm data store database, a local administrator account can log on to the Access Management Console to set up Citrix administrator accounts.
- To create effective Citrix administrator accounts, ensure that all users you are going to add as Citrix administrators are Domain Users for the domain in which your farm resides. Users who are Citrix administrators who take server snapshots must also be authorized Windows Management Instrumentation (WMI) users on each server on which they are taking snapshots.
- Citrix recommends that you do not mix different release versions of Citrix Presentation Server in the same server farm. Upgrade Citrix Presentation Server to the current version to ensure that custom administrator settings apply properly.
- If you want to enable the IMA encryption feature in Citrix Presentation Server during product installation, Citrix recommends that you install Presentation Server using the same network credentials. If you install it as a local administrator, after you install Presentation Server on the first server in the farm you must enable the **Add local administrators** setting in the Access Management Console on that server before installing Presentation Server on subsequent servers. You enable this setting through the Access Management Console. For more information, see "Enabling IMA Encryption as a Local Administrator" on page 225.

Establishing Domain Trust Relationships

One of the primary tasks for planning a server farm deployment is to define how you plan to authorize user access to resources in the server farm. You do this by establishing domain trust relationships implemented through user and group accounts. A published resource is available only to users who can access every server that hosts it. When multiple servers host the same resource, you cannot predict which servers users will connect to when they access the resource. Therefore, if a user is authorized to access only some servers, you cannot ensure that the user will always be able to access the resource.

For example, when you publish an application, you select the servers to host the application and the Access Management Console lists the user accounts from the trust intersection of all the servers (accounts that are trusted by all the servers). You then select the users and groups that you want to allow to use the application. After you select users, changing the list of host servers can change the trust intersection, which can make the application unavailable to users who are no longer in the servers' trust intersection. If the trust intersection changes, the console displays a message and removes users who are no longer eligible to use the resource from the authorized users list.

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

The following sections discuss how trust-based routing works and also provide recommendations for implementing it in an Active Directory environment.

Trust-Based Routing

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

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

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

Trust-based routing applies to the following operations:

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

Changing Domain Trust Relationships

If you add a new domain trust relationship, you might be unable to select user accounts in the server farm right away based on the trust relationship.

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

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

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

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

Recommendations for Active Directory Environments

Native support for Active Directory is included in Windows Server 2003, so you do not need to install additional services.

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

Recommended Domain Configurations

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

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

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

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

Using Active Directory Forests

If you use Windows Active Directory, Citrix recommends that all servers in a server farm belong to the same Active Directory forest. If your farm has servers in more than one forest, users cannot log on by entering user principal names (UPNs).

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

Important Because there is no efficient way to perform account resolution, Citrix Presentation Server does not support UPN logons if a server farm spans multiple Active Directory forests.

Implementing an Active Directory Security Model

Active Directory has the following types of security groups to which network users can belong:

- **Domain local groups.** In the Active Directory model, domain local groups can contain groups from other domains, but the domain local group can be assigned to resources only in the domain in which it exists.
- **Universal groups.** Universal groups can contain groups from other domains. Universal groups are stored in the Active Directory global catalog. Universal groups can be used for assigning permissions to resources in any domain.
- **Domain global groups.** Global groups contain groups within the same domain and can be assigned to resources in any domain. Citrix recommends that you use domain global groups for user access to published applications and network printers. Domain global groups are equivalent to non-Active Directory global groups.

You can use these security groups when you select users for published applications and network printers.

If you plan to use universal groups or domain local groups, Citrix recommends that you follow the deployment guidelines in this section regarding domain configuration and use of groups to reduce administrative complexity. For in-depth technical information about user access issues and configuration issues, see "User Permission Scenarios with Active Directory" on page 24.

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

For example, if all servers hosting an application or a printer reside in a common domain, Domain1, you can select domain local groups from Domain1 to grant access to the resource. If you then configure additional servers to host the resource and these servers do not reside in Domain1, the Access Management Console detects the change and removes the Domain1 domain local group from the configured accounts for the resource.

For more information about domains, establishing trust relationships among domains, and configuring user accounts in domains or Active Directory, see your Windows documentation.

User Permission Scenarios with Active Directory

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

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

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

	Program Neighborhood filtering	Authenticating to published applications	Authenticating to the Presentation Server Console
Domain Global Groups	No adverse effects.	No adverse effects.	No adverse effects.
Domain Local Groups	**Recommendation:** All servers in the farm must be in the same domain for Program Neighborhood filtering to work properly. **Rationale:** If a user is a member of a domain local group, the group is present in the user's security token only when logging on to a computer in the same domain as the domain local group. Trust-based routing does not guarantee that a logon request is sent to a server in the same domain as the domain local group. It guarantees only that the request is handled by a server in a domain that trusts the user's domain.	**Recommendation:** All servers that load balance an application must be in the same domain if a domain local group is authorized to use the application. **Rationale:** Domain local groups assigned to an application must be from the common primary domain of all the load balancing servers. When you publish applications, domain local groups appear in the accounts list if the first condition above is met and accounts from the common primary domain are displayed. If a published application has users from any domain local groups and you add a server from a different domain, domain local groups are removed from the configured users list, because all servers must be able to validate any user with permission to run the application.	**Recommendation:** If a user is a Citrix administrator only by membership in a domain local group, the user must connect the console to a server in the same domain as the domain local group. **Rationale:** If the user connects the console to a server in a different domain than the domain local group, the user is denied access to the console because the domain local group is not in the user's security token.
Universal Groups	**Recommendation:** No Active Directory domains in the forest to which the servers belong have explicit trust relationships with non-Active Directory domains. **Rationale:** Non-Active Directory domains have no knowledge of universal groups and the domain controllers exclude a universal group from a user's security token. As a result, applications might not appear in Program Neighborhood.	**Recommendation:** If universal groups are assigned permission to the application, all servers that manage the application must be in an Active Directory domain. **Rationale:** A server in a non-Active Directory domain could authenticate the user to run the application. In this case, universal groups are not in the user's security token, so the user is denied access to the application. It is possible for a server in a non-Active Directory domain to load balance an application with servers in an Active Directory domain if the domains have an explicit trust relationship.	**Recommendation:** If a user is authenticating to the console and is a Citrix administrator only by membership in a universal group, the console must connect to a server that belongs to an Active Directory domain in the universal group's forest. **Rationale:** Non-Active Directory domain controllers and domains outside a universal group's forest have no information about the universal group.

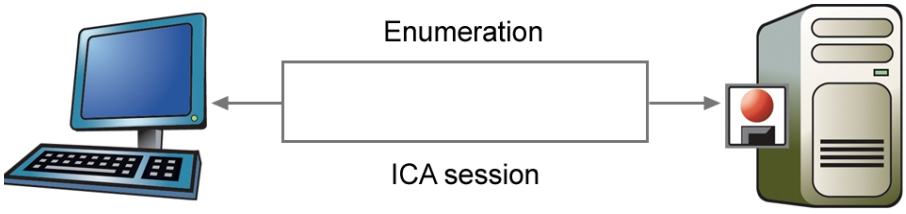
Planning for Client and Server Communications

In a server farm, several types of data transmission and communication pathways link clients and servers. Configuring Enumeration so that clients can locate published applications and servers in your farm is an important part of planning your deployment.

Note Features described in this section, such as application sets, are not available to all Citrix Presentation Server Clients. This section focuses on the features available with Clients for Windows, Version 6.0 or later.

Linking Clients and Servers

In a server farm, the main communication processes between clients and servers are application and desktop enumeration, and ICA sessions.



This diagram shows a client performing application enumeration from a server. To run an application, a client initiates an ICA session with the server.

Enumeration

Enumeration is a process in which a client transmits data to locate servers on the network and retrieves information about the server farm's published applications.

During Enumeration, clients communicate with the Citrix XML Service or the ICA browser, depending on the browsing protocol selected in the client. These options are described under "Configuring Enumeration" on page 28.

Enumeration occurs when:

- The Web Interface or Program Neighborhood client sends a request to locate the application on a server. If you are using Load Manager, a component of Citrix Presentation Server for Windows, Advanced Edition and Enterprise Edition, the client gets the address of the server with the lightest load.
- Program Neighborhood users display the Application Set list in the Find New Application Set wizard.
- Program Neighborhood users display the **Server** or **Published Application** list in the Add New ICA Connection wizard to create a custom ICA connection.

ICA Sessions

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

The default port on servers for inbound traffic from ICA sessions is 1494. The outbound port from the server used for the ICA session is allocated dynamically when the session is established.

Important If session reliability is invoked, ICA traffic is tunneled through the Common Gateway Protocol, which uses TCP port 2598 by default. Like ICA traffic, the designated port is used for inbound sessions to Presentation Server, and a dynamically allocated port is used for outbound traffic. Ports 1494 and 2598 should be opened only to *internal* inbound traffic. Sessions originating from clients connecting over the Internet should be secured by means of the Secure Gateway or Access Gateway.

In addition to computers running Citrix Presentation Server, other components, such as computers running the Web Interface, proxy servers, and Web browsers can be involved in establishing ICA sessions. In all cases, the basic communications link for an ICA session is between the client and the server.

Configuring Enumeration

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

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

Configuring Server Location Settings

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

- For new application sets and custom connections, you configure server location settings from the **Server Location** button in the Find New Application Set wizard or the Add New ICA Connection wizard in the client.
- For existing application sets and custom ICA connections, you can modify server location settings by right-clicking on an existing item and choosing **Properties**. Then click the **Connection** tab to modify the server location settings.

Note Some Citrix Presentation Server clients do not use the Enumeration process described in this section and connect only to specified servers. The options described in this section apply to Citrix Presentation Server Clients for Windows. For information about other server location options, see the Administrator's Guide for each type of client that you plan to deploy.

Specifying the Network Protocol for ICA Clients

On the **Locate Server or Published Application** dialog box, the network protocol setting that you specify for server location in the client affects the following aspects of deployment related to Enumeration:

- The communications protocol the client uses to locate servers
- The component in Citrix Presentation Server with which the client communicates
- The port through which the client communicates
- The default locations that the client contacts

Using TCP/IP + HTTP for Enumeration

The **TCP/IP + HTTP** setting is the most secure setting for the server location network protocol in the Presentation Server Client. In addition to recommending the **TCP/IP + HTTP** setting, Citrix recommends that you specify the servers that you want to connect to for Enumeration by entering the IP addresses or Domain Name System (DNS) names of these servers in the **Address List** box. When **TCP/IP + HTTP** is selected and you specify servers in the **Address List** box, the client communicates with the Citrix XML Service on a specified server for Enumeration.

By default, if no server is specified, the client attempts to resolve the name “ica” to an IP address. This is indicated by the virtual server location “ica” in the **Address List** box. This feature allows the DNS or WINS administrator to configure a host record that maps “ica” to a valid server IP address that can service XML requests from clients.

Note You can configure the clients’ DNS server to use round-robin DNS to map the name “ica” to a set of servers that can service the XML requests. This is a convenient method to use to avoid individual configuration of server location addresses on clients.

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

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

Citrix recommends using TCP/IP + HTTP protocol for Enumeration because it provides several advantages for most server farms:

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

Using TCP/IP for Enumeration

If you specify **TCP/IP** as the server location network protocol and **(Auto-Locate)** appears in the **Address List** box, clients send UDP broadcasts to locate servers and published applications.

By default, server farms do not respond to clients that use UDP broadcasts for Enumeration. Therefore, if clients are configured to use TCP/IP and to auto-locate servers, they fail to locate servers or published applications in the farm.

You can set the server farm, or individual servers, to respond to client broadcasts for compatibility with deployed clients.

Because UDP broadcast packets do not traverse subnets, using broadcasts for Enumeration works only if a server that responds to broadcasts is in the same subnet as the clients. After the client locates a server, it communicates using directed (not broadcast) UDP to port 1604.

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

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

Effects of Server Location and Network Protocol on Enumeration

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

Network protocol	Address list	Data type	Responder
TCP/IP + HTTP	Default ("ica")	XML/HTTP	Citrix XML Service
TCP/IP + HTTP	Specified server(s)	XML/HTTP	Citrix XML Service
TCP/IP	Default (Auto-Locate)	UDP broadcast	ICA browser on data collectors
TCP/IP	Specified server(s)	Directed UDP	ICA browser

Using DNS Address Resolution

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

Servers reply with an IP address as the default. You can change the default setting, which applies to the entire server farm, in the Access Management Console. In most situations, using IP addresses works well and requires less overhead.

For ease of administration, Citrix Presentation Server Clients are configured to request FQDNs if DNS addressing is enabled in the server farm. Clients connecting through the Web Interface request IP or DNS addresses based on a configuration setting. By default, Web Interface is configured to request IP addresses. Regardless of what clients are set up to request, unless DNS addressing is enabled for the server farm, IP addresses are returned.

DNS address resolution works only in server farms using Citrix Presentation Server Client 6.20.985 or later:

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

To enable or disable DNS address resolution in a farm

1. In the scope pane of the Access Management Console, expand the Presentation Server node and select a farm. Then select **Action > Modify farm properties > Modify all properties**.
2. On the **Farm Properties** dialog box, expand the Farm-wide node. Select **Presentation Server** > **General**.
3. In the right pane, select or deselect the **XML Service DNS address resolution** check box.
4. Click **OK**.

Communicating with the Citrix XML Service

Citrix XML Service is a component of Citrix Presentation Server. The service is installed by default on all servers.

When clients are configured to use TCP/IP + HTTP for Enumeration, the Citrix XML Service communicates published application information to clients using the HTTP protocol and XML data. The Citrix XML Service also communicates published application information to servers running the Web Interface.

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

With the Web Interface, for example, a user connects to a Web page using a Web browser. The Citrix XML Service provides a list of available applications to the server running the Web Interface. The Web server displays the available applications on the user's personalized application Web page.

Setting the Port for the Citrix XML Service

The Citrix XML Service uses a TCP port on the server to communicate with clients and with the Web Interface. You can set the port number while running Citrix Presentation Server Setup.

Important All servers in the farm must use the same port for the Citrix XML Service.

The Citrix XML Service default communication port is 80. If you intend to send data over a secure HTTP connection using secure socket layer (SSL), be sure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

Note Port 80 is the default port for HTTP communication with Web servers. The Citrix XML Service includes an Internet Server Application Programming Interface (ISAPI) extension that you can plug into Internet Information Services (IIS). The extension allows IIS and the Citrix XML Service to share port 80. This is necessary only if IIS is installed on servers running Citrix Presentation Server; however, installing IIS and Citrix Presentation Server on the same server is not recommended. IIS is required to run the Web Interface.

For information about configuring the Citrix XML Service port number, see "Step 9: Configuring the Citrix XML Service Port" on page 70. For information about configuring the port that the Web Interface uses, see the *Web Interface Administrator's Guide*.

Important If you change the port used by the Citrix XML Service, you must set the correct port in the client. You can specify a port number when you add a server to the **Address List** under **Server Location** in the client. If you also use the Web Interface, be sure it uses the correct port for Citrix XML Service communication. For more information about using the Web Interface, see the *Citrix Web Interface Administrator's Guide*. For instructions about configuring the clients, see the client documentation.

Planning the Data Store

When you deploy your server farm, it must have an associated *data store*. When servers in a farm come online, they query the data store for configuration information. The data store provides a repository of persistent information about the farm that each server can reference, including the following:

- Farm configuration information
- Published application configurations
- Server configurations
- Citrix administrator accounts
- Printer configurations

You can view and change data store information using management tools for Citrix Presentation Server, such as the Access Management Console and the Presentation Server Console. You can install these management tools from the Citrix Presentation Server CD.

The following sections discuss the considerations for planning your data store implementation and also how to set it up and configure connections to it. For more information about supported database and driver versions and also minimum requirements, authentication, and migration information for each supported database, see Appendix E, "Data Store Database Requirements."

Caution Ensure that the data store is properly backed up on a regular basis. If the data store database is lost, you must recreate the farm. You cannot recreate the data store from an existing farm.

Before you set up and configure connections to the database that will serve as your data store, you need to consider issues such as: which database you will use, how your system will be sized, what hardware configuration is best for your environment, and other configuration options.

Choosing a Database

As an initial planning step, you must decide which database to use for your farm's data store. You can use the following database software for the farm data store:

- **Microsoft Access.** Access is a lightweight database that is included with Windows server operating systems. The Access database is created on the first server in a new farm. It is most appropriate for small to mid-sized farms.
- **Microsoft SQL Server 2005 Express Edition SP1.** This type of database is most appropriate for small to medium-sized farms and can be administered using standard Microsoft SQL Server tools.
- **Microsoft SQL Server, Oracle database, and IBM DB2.** These are all true client/server databases that offer robust and scalable support for multiple-server data access. They are suited for use in farms of any size.

When using Microsoft Access, the data store database is created when you install Citrix Presentation Server.

When using SQL Server 2005 Express Edition SP1, first install it and then create an instance. Then run the Citrix Presentation Server Setup. The database is stored on the first server in the farm.

When using Microsoft SQL Server, Oracle, or IBM DB2, the database is housed on a server dedicated to running the database product. Set up this server prior to creating the farm because you need to configure an ODBC connection to it. Servers running Citrix Presentation Server must also have the appropriate database client software installed on them.

Caution Do not install Citrix Presentation Server on the Microsoft SQL, Oracle, or IBM DB2 database server. See your database product's documentation for specific hardware requirements for the database server.

You should consider many factors before deciding which database product to use for the data store, including but not limited to:

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

---

Important Microsoft SQL, Oracle, and IBM DB2 servers require significant expertise to install and maintain. If you do not have expertise with these products, attempting to use them in a production environment is not recommended. See the documentation included with your database product for important details such as performance tuning and database backup procedures.

Connecting Directly or Indirectly to the Data Store

Another factor in planning your data store is deciding if you want to the servers in the farm to communicate directly or indirectly (that is, through an intermediary server) with the data store. This choice is determined is determined by the type of database you choose for the data store and the size of your environment:

- If you are in an large-farm environment, have a mission-critical farm, or are using Oracle, SQL, or DB2 as the database for your data store, Citrix recommends accessing the data store *directly.*
- If you are in small to medium-sized environment and you are using SQL Server 2005 Express or Microsoft Access as the database for your data store, each server in the farm must access the data store *indirectly.*

You specify whether you want servers to communicate directly or indirectly with the data store when you run Setup to install Presentation Server on the subsequent servers in your farm. See page 73.

Direct access. To make a *direct access* to the data store, a server must have the appropriate ODBC drivers installed and configured correctly. The server then connects directly to the server on which the database is running. If you are in an large farm environment, Citrix recommends accessing the data store directly. However, during Setup joining the farm directly is only possible if your data store is on a robust database, such as Oracle or SQL.

Indirect access. For *indirect access,* a server connects to an intermediary server running Citrix Presentation Server that connects to the data store directly.

If you are using SQL Server 2005 Express and Microsoft Access as the database for your data store, during Setup select to join the farm indirectly. SQL Server Express and Microsoft Access can only access the data store indirectly.

Citrix does not recommend that you use indirect access for mission-critical farms because the intermediary server is a single point of failure.

By default, indirect access uses TCP port 2512 for communication between servers in the farm and the intermediary server that connects to the data store. If the servers are in different subnets divided by a firewall, be sure this port is open on the firewall.

System Sizing for the Data Store

The choice of which database to use for the data store depends on your implementation and environment.

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

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

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

- Microsoft Access and SQL Server Express are suitable for all small and many medium-sized environments that are located in one physical location.
- Microsoft SQL, Oracle, and IBM DB2 are suitable for any size environment and are especially recommended for all large and enterprise environments.

  When deploying large farms across a WAN, you can obtain considerable performance advantage by replicating the data store and distributing the load over multiple database servers. Microsoft SQL, Oracle, and IBM DB2 are suitable for large farms and support replication. For more information about replicating data stores, see "Using Replicated Data Store Databases" on page 40.

Suggested Hardware Configurations

This section outlines suggested hardware configurations resulting from testing in Citrix labs. All tests used Microsoft SQL Server 2000 in the default configuration without replication for the farm's data store.

Increasing the CPU power and speed of the database server can improve the response time of queries made to the data store. Increase the processing power of the data store database server to achieve improved results in the following areas:

- Starting the Citrix IMA Service on multiple servers simultaneously
- Adding a server to the farm
- Removing a server from the farm

The response time of other events occurring in the farm—such as starting the IMA Service on a single server, recreating the local host cache, or replicating printer drivers to all servers in the farm—is affected more by the size of the farm than by the response time of the data store.

Citrix testing shows that adding processors to the server hosting the data store can dramatically improve response time when multiple simultaneous queries are being executed. If the environment includes large numbers of servers coming online simultaneously and at frequent intervals, the additional processors can service requests faster.

The actual performance of a farm's data store can vary depending upon which database engine is used and the level of performance tuning that can be achieved. Depending on the characteristics of a server farm, the CPU speed and CPU quantity can vary widely.

In the chart below, five sample farm configurations are displayed and referred to as scenarios A through E. Each scenario lists measurements of various metrics in the farm.

The second chart shows, for each corresponding scenario, which hardware configurations are suggested for the server hosting the data store.

Scenario	**A**	**B**	**C**	**D**	**E**
Number of servers in farm	50	100	250	500	1000
Number of applications published to all servers	50	50	50	50	50
Number of user policies	25	25	25	25	25
Printers per server	5	5	5	5	5
Printer drivers installed per server	25	25	25	25	25
Network print servers with printers	5	5	5	5	5
Number of Load Manager load evaluators	10	10	10	10	10
Number of Resource Manager applications	10	10	10	10	10
Number of Installation Manager groups	5	5	5	5	5
Number of Installation Manager packages	5	5	5	5	5
Number of application folders in Access Management Console	10	10	10	10	10
Number of server folders in Access Management Console	8	16	25	50	50
Number of Application Isolation Environments	10	10	10	10	10

Scenario	A	B	C	D	E
Number of Resource Manager metrics per server	25	25	25	25	25
Number of Citrix administrators	10	10	10	10	10
Size of data store database in megabytes	32	51	76	125	211

Scenario	A	B	C	D	E
Dual Pentium 4/1.6GHz with 2GB RAM	X	X	X		
Dual Pentium 4/3.0GHz with 4GB RAM	X	X	X	X	
Quad Pentium 4/1.6GHz with 4GB RAM	X	X	X	X	X

Other Configuration Options

After you decide which software and hardware platforms to base your data store on, you need to consider other configuration options, such as how servers will connect to it, and whether or not to use options such as RAID and replicated databases.

In addition, after you decide which database to use for the data store, decide whether servers running Citrix Presentation Server will connect directly to it or indirectly through another server. For more information about direct and indirect connections to the data store, see “Stage 3: Specifying the Location of the IMA Encryption Key File” on page 76.

Using a RAID Environment

This section describes factors to consider if you are thinking about putting the farm's data store in a Redundant Array of Independent Disks (RAID) environment. See the table below for information about cost, performance, and fault tolerance related to four different RAID configurations.

RAID 0	RAID 0 has no redundancy. It is "striped," which means that data is divided into blocks spanning multiple disks. RAID 0 has multiple actuators (read/write mechanisms) because of the multiple disk use. More actuators improve read and write performance. Citrix does not recommend the use of RAID 0 for critical data, such as a server farm's data store. The savings realized from purchasing fewer disks does not typically make up for the costs resulting from downtime and support.
RAID 1	RAID 1 uses fully redundant disk mirroring. With disk mirroring, a complete copy of one drive is maintained on another drive. RAID 1 provides high fault tolerance and can improve read performance. However, RAID 1 writes the data twice, which can degrade write performance in single disk/controller environments. In addition, this type of redundancy requires twice the disk space.
RAID 5	Like RAID 0, RAID 5 is striped. However, because RAID 5 adds parity to the data striping, it includes fault tolerance. If one disk in a RAID 5 group fails, the logical disk continues to function. The parity information is used to recreate data on a replacement disk. The loss of two disks in a group at one time cannot be sustained. RAID 5 uses multiple disk actuators that provide improved read and write performance.
RAID 10	RAID 10 combines RAID 1 and RAID 0. It is a striped and fully mirrored set of disks. It is the best configuration for both redundancy and performance. Because of this, it is the most expensive storage option.

Using Replicated Data Store Databases

Citrix recommends using a single data store where appropriate but in some situations, a replicated data store can improve farm performance. This section covers the concerns and situations that arise from using replicated database technology.

Enhancing Performance with Replicated Databases. Because servers in a farm perform many more reads from the data store than writes to the data store, you may want to use replicated databases to increase read performance.

In a WAN environment, you can place replicas of the data store at sites with a considerable number of servers. This practice minimizes reads across the WAN link. Database replication does consume bandwidth. Limit the use of replicated databases to situations where the remote site has enough servers to justify the bandwidth cost of placing a replicated copy of the database at the site.

High Latency WAN Concerns. Crossing high latency links without the use of replicated databases can create situations where the data store is locked for extended periods of time when performing farm maintenance from remote sites. Data store reads do not generally adversely affect local connections but remote sites can experience slower performance. This means that the Citrix IMA Service may start after extended periods of time and some normal operations may fail when performed from the remote site.

Note You might experience poor performance if you use a local Access Management Console to perform farm maintenance on a remote site that has high latency. Such a situation requires communication between the console and the data store to cross the high latency link. You can publish the Access Management Console and the Presentation Server Console as applications on a server at the remote site and use a Citrix Presentation Server Client to access the published consoles.

Planning for IMA Encryption

The IMA encryption feature provides a more robust AES encryption algorithm to protect sensitive data in the IMA data store. Enabling IMA encryption provides an additional layer of security for the data preserved by the Configuration Logging feature. IMA encryption, and when to enable it, are described in more depth in “Encrypting Sensitive Configuration Logging Data” on page 219

You can enable IMA encryption during or after Presentation Server Setup. Because IMA encryption is a farm-wide setting, if you enable IMA encryption during Citrix Presentation Server installation, each server you add to the farm has IMA encryption enabled. Setup requires the same key used for the first server in the farm when you install Presentation Server on subsequent servers. If you do not enable this feature, Presentation Server uses the standard encryption used in previous versions of Presentation Server. If you are upgrading from Citrix Presentation Server 3.0 or 4.0 using the Upgrade feature in Setup, you cannot enable IMA encryption during installation. Enabling IMA encryption after Setup is described in “Enabling IMA Encryption after Installation” on page 222.

To enable IMA encryption during installation, you must generate a key, which is used for all the servers in your farm, and specify that key during Setup. You can generate the key before Setup or during Setup.

If you are performing a large-scale deployment of Citrix Presentation Server, Citrix recommends doing one of the following:

- Deploying Presentation Server by using images
- Generating a key, putting the key on a folder on your network, using a UNC path to specify the location, and performing an unattended installation

---

Note Mapped drives are not supported for specifying the path for the key during installation.

For more information about deploying Presentation Server using images and unattended installation options, see "Choosing a Method of Installation" on page 46. If you choose to generate the key before Setup, you must generate it by using the CTXKEYTOOL that is described in "To generate a key and enable IMA encryption on the first server in a farm" on page 222.

After you create a key for the first time, you do not need to create additional keys for other servers in your farm. However, if you have multiple farms in your environment, Citrix recommends that you generate separate keys for each farm.

Deciding to Change Server Drive Letters

When a user launches an ICA session, Citrix Presentation Server tries to map disk drives on the server to the typical drive letters for the client. If the drive letters are available, the server maps the client's first floppy disk drive to A, the second floppy drive to B, the first hard disk drive to C, and so on. However, a server cannot map client device drives to letters that are assigned to the server's own disk drives.

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

Default Drive Mappings

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

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

Remapping Drive Letters

To make drive access more familiar for users, you can change the server drives to use letters that are not likely to be used by client devices. This ensures that client drives retain their original drive letters. By changing the server to use higher drive letters, such as M, N, or O, the original lower drive letters become available for assignment to the drives on client devices. This can make the use of drives on client devices less confusing for users, because they see their drives identified by typical drive letters.

Caution When performing a new installation of Presentation Server if you want to remap server drives, Citrix recommends that you do so before installing Presentation Server and before installing applications on the server. Remapping server drive letters after you install Presentation Server can cause unstable performance by the server, operating system components, and installed applications.

The following table shows an example of drive letters used if you change the drive letters of a server.

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

Caution Do not use the **driveremap** or **driveremap64** utility on a server with .NET 2.0 installed. You can install .NET 2.0 after you remap server drives.

CHAPTER 3

Deploying Citrix Presentation Server

This chapter discusses the considerations, guidelines, and procedures that are associated with each of the following aspects of server farm deployment:

- Choosing a method of installation
- Preparing your environment, including enabling Windows MUI support
- Deploying Presentation Server, including how to create a new farm and how to install Presentation Server on subsequent servers in the farm
- Upgrading or migrating an existing server farm
- Deploying client software to users
- Removing Presentation Server

Where you begin reading this chapter depends on whether you are installing Presentation Server for the first time or if you are upgrading your farm from a previous release of Presentation Server.

- If you have not installed Presentation Server before, begin reading at the section that immediately follows.
- If you are familiar with installing Presentation Server already, you may want to skip the Choosing a Method of Installation section and the Creating and Upgrading Farms section and read “Preparing Your Environment” on page 48 and “Upgrading or Migrating an Existing Server Farm” on page 77.

Note If you are deploying Citrix Presentation Server for the first time, before you install this product, read “Planning for Deployment” on page 17.

Choosing a Method of Installation

Deploying Presentation Server across a farm requires repeating the same installation on many servers. Often, performing a traditional UI-based, wizard-driven installation is too time consuming to be feasible. For most farm deployments, you will want to use an automated method of installation, such as deploying images or using a silent installation.

Before you begin installing Presentation Server, choose an installation method. The following section lists the different types of installation and provides a description of when you want to use them and information to help you choose between them.

If you are installing Presentation Server for the first time and want to become familiar with its Setup, you may want to start by installing Presentation Server using the UI-based installation on a small single-server test farm. The UI-based installation gives you an easy way to get familiar with the sequence of steps for installing Presentation Server.

UI-based installations. UI-based installations can be invoked from either the Autorun program, autorun.exe, or directly from the .msi file. You can use UI-based installations to install individual servers. UI-based installations are handy if you need to install an individual component or install Presentation Server on small farms. One key difference between starting a UI-based installation from the Autorun and the .msi file is that when you invoke Setup from the Autorun, Setup automatically installs most non-Windows system requirements.

A UI-based installation is a manual method of installing Presentation Server that requires selecting options for every page of the wizard. As a result, it is not an appropriate installation method for large farms that are created without imaging.

Unattended Installations. Unattended installations provide a method of installing Presentation Server that run without user interaction. Unattended installations provide a scalable approach for installation without imaging. Once you create the unattended installation, you can store it until you are ready to deploy it and reuse it later for additional servers you add to the farm. For more information, see "Unattended Installations" on page 365. Presentation Server supports several different types of unattended installations:

- **Transforms**. If you want to perform unattended installations with Active Directory, you need to do an unattended installation using Transforms. To perform this type of unattended installation, Citrix recommends that you have some Windows Installer and database knowledge. You also need to have an MSI tool. Before performing an unattended installation with transforms, you must have a strong understanding of the properties of Presentation Server MSI properties. For more information, see "Creating Transforms" on page

367. For information about MSI editing tools, see Microsoft's Web site.

- **Answer Files.** Answer files provide one of the easiest ways to perform unattended installations. Answer files are easy to store. They are also easy to compare with other answer files. However, if you want to perform an Active Directory deployment, you cannot use answer files. They do not work with Active Directory deployments. For more information, see "Creating and Using an Answer File" on page 368.
- **Windows Installer Commands.** Windows installer commands let you prepare an unattended installation from a command line. If you have Windows Installer knowledge, this may be a good installation option for you. Windows installer commands may make it easier to pick and choose installation options. Like transform-based unattended installations, Windows Installer command installations require a solid understanding of the Presentation Server MSI properties. In addition, Windows Installer Commands do not work with Active Directory deployments. For more information, see "Using Windows Installer Commands" on page 369.

Creating a baseline installation and deploying images to additional servers. In many environments, deploying images is the standard method of performing large, corporate-wide installations. This guide does not discuss these techniques; they are beyond the scope of this guide.

Additional Supported Options

You can use the following options in conjunction with the methods of installation previously discussed to enhance your installation method:

- **Administrative Installations.** You can also perform an administrative installation when you are using either Windows Installer Commands or MSI transforms as your method of installation. This method does not require as much MSI knowledge as using transforms to install Presentation Server, and you do not need a transform-creation tool. Citrix recommends that you are familiar with our MSI property documentation before attempting an administrative installation. For more information, see "Enabling Administrative Installations" on page 370.
- **Installation Log Files.** You can create log files for Presentation Server installations. For more information, see "Creating an Installation Log File" on page 372.

Preparing Your Environment

Deploying Citrix Presentation Server is a multistage deployment. Before you install the components included with Citrix Presentation Server Setup, prepare your environment.

1. Review the *Installation Checklist for Citrix Presentation Server* on the Server CD and ensure that your computer is prepared for product installation. The Installation Checklist includes system requirements for each component. For more information about the "Installation Checklist," see page 17.
2. Before you install any system requirements, including .NET 2.0, Citrix recommends that you remap server drives, if required. For more information, see "Remapping Server Drive Letters" on page 49.
3. Install database software and create the farm data store.

   Before installing Citrix Presentation Server, you choose and install a database product to serve as your farm data store. The data store contains persistent configuration information about all servers in the farm. All servers must be able to reference this configuration information. For information about data store selection and planning, see "Planning the Data Store" on page 33. For information data store creation, see "Setting Up the Data Store" on page 49.

   You must create the data store before you install Citrix Presentation Server if you are creating a new server farm and plan to use Microsoft SQL Server, Oracle, or IBM DB2 for the farm data store. If you use Microsoft Access for the data store, you can create the data store during Setup.

Note If SQL Server 2005 Express Edition SP1 is used, you must install it and reboot the system before you install Citrix Presentation Server.

---

4. Install Citrix licensing.

Note If you choose to install multiple components on the same 64-bit server, Citrix recommends that you always install the Web Interface before the License Management Console or Citrix Presentation Server.

   For information about installing the license server, see the *Getting Started with Citrix Licensing Guide*.

5. Ensure that Setup can create the local accounts required for the Citrix Print Manager Service. For more information, see “Substituting Domain Accounts for Local Accounts” on page 50.
6. If you want to use the MUI support in Presentation Server, follow the instructions in the section that follows before installing Presentation Server.

Remapping Server Drive Letters

You can remap server drive letters by using the Remap drives option in the Autorun screen in Setup.

You may want to remap the server drive letters in your farm drive letters if you feel the drive letter conventions in Presentation Server will confuse your end users. Citrix recommends that you remap server drive letters before you install Presentation Server and all system requirements, including .NET 2.0. Remapping server drive letters after you install Presentation Server can cause unstable performance by the server, operating system components, and installed applications. For information that helps you determine when you want to remap drive letters, see “Deciding to Change Server Drive Letters” on page 42.

To change server drive letters before installation, from the initial Autorun screen, select **Remap drives**. For more information about the **driveremap** utility, see “DRIVEREMAP” on page 312.

Setting Up the Data Store

After you establish the type of data store you want to implement, you can use the database management software to create the database that will host your data store. Then, during the Citrix Presentation Server installation process, you must configure a connection to that database and also configure each server’s ODBC driver.

Caution Do not directly edit any data in the data store database with utilities or tools other than those provided by Citrix. For example, do not use IBM DB2, Microsoft SQL Server, or Oracle utilities to edit the data store. Doing so corrupts the data store database.

Creating the Data Store Database

Using a Microsoft Access or SQL Server Express database involves creating a database locally while you install Citrix Presentation Server on the first server in the farm. If you are using a SQL Server, Oracle, or IBM DB2 database for the data store, however, you must create a database independently of the Citrix Presentation Server installation.

When creating your data store database, the following tablespace settings should be used:

- Oracle
    - Minimum tablespace size = 20MB
    - User role permissions should have a minimum of connect and resource
- IBM DB2
    - Prefetch Size = 32
    - Overhead = 8.3
    - Transfer = 0.18
    - Use the *grant all* option for the selected tablespace
    - User privileges should be *grant all* to the public group

For more information, see the documentation for the database you selected.

Substituting Domain Accounts for Local Accounts

By default, the Presentation Server Setup creates a local account for the purpose of running the Citrix Print Manager Service. If the domain policies on your system prohibit the use of local accounts, the account for this service cannot be created during Setup.

To be able to use the Citrix Print Manager Service in this case, prior to the installation of Presentation Server you must create a substitute domain account with Windows privileges that are equivalent to the privileges for this local account. To substitute your newly-created domain account for the local account, during the installation of Citrix Presentation Server, run the **CTX_SERV_PRINTER_LOGON** property and provide the new domain account name as a parameter. For more information about the **CTX_SERV_PRINTER_LOGON** property, and the rights and privileges necessary for the domain user account, see Appendix D, "Advanced Installation Methods."

Enabling Windows MUI Support

Citrix Presentation Server supports Microsoft Windows Multilingual User Interface Pack (MUI) for Windows Server 2003. Users connecting from non-English language clients see their environment and applications in the language that corresponds with their language setting, provided the server's operating system and applications support it and the corresponding language packs are installed on the server. While Presentation Server supports Windows MUI, some Presentation Server components do not display in the non-English language.

If you want to use Windows MUI functionality with Citrix Presentation Server 4.5, you must perform the steps below in the sequence specified.

To enable Windows MUI support

1. Before you install Citrix Presentation Server 4.5, make sure the Windows Server 2003 Language option is set to English. The Language setting is found in Regional and Language Options. For more information, see your Microsoft documentation.
2. Install the English version of Citrix Presentation Server.
3. Install the Windows MUI language packs you want to deliver to users, and install any applications, MUI or native, required.

After performing these steps to enable Windows MUI support, you can continue on to performing standard post-installation configuration tasks such as those described on page 85.

Note Changing the Windows Server 2003 Language option to another language after you install Presentation Server may lead to display issues.

Creating and Upgrading Farms

The following sections provide information about installing and upgrading Presentation Server and other components that are included on the CD. You do not have to install all components; some components are optional depending on your environment.

The section that you want to read depends on your circumstances:

- If you are creating a farm for the first time and not upgrading to Presentation Server 4.5, see "Creating a New Farm" on page 52
- If you are upgrading or migrating to Presentation Server 4.5 from a previous release, "Upgrading or Migrating an Existing Server Farm" on page 77

The section about upgrading or migrating to Presentation Server 4.5 references the "Creating a New Farm" section extensively. If you are upgrading and are unfamiliar with Presentation Server Setup, you may want to read "Creating a New Farm" section before you read about upgrading.

Creating a New Farm

The following information is designed for people creating a farm for the first time. It assumes that you are running an installation for the first time and not upgrading to Presentation Server 4.5.

While the following information is based on using a UI-based installation to install Presentation Server components, the sequence and explanations apply to other types of installations, including the unattended installation.

Initial Installation Overview

The first time you install Presentation Server, you must create a farm. The first server you install creates the farm. When you install Presentation Server on subsequent computers, you join the farm you initially created on the first computer. The following is a high-level overview of creating a farm:

1. Install the Web Interface.

   Citrix recommends, if possible, that you install the Web Interface on a separate computer from the computer on which you are installing Citrix Presentation Server.

   If you are installing the 64-bit version of Citrix Presentation Server on the same computer as the Web Interface, Citrix strongly recommends that you install the Web Interface *before* Citrix Presentation Server. (By default, Setup installs the Web Interface and Citrix Presentation Server in this order.)

2. Install the Access Management Console, the Presentation Server Console, and the Document Center, as needed.

3. Create your farm by installing Citrix Presentation Server.

Note When you are creating your farm, do not give it a name with a hyphen if you intend to use Oracle as your Configuration Logging database.

---

4. After installation, restart the servers.

After installing Citrix Presentation Server, you must perform some post-installation configuration tasks before users can log on to published resources. For more information about these tasks, see “Using Remote Desktop Web Connection Software” on page 93.

Caution With utilities provided in Windows, it is possible to change server drive letters after you install Citrix Presentation Server. Citrix advises against remapping server drive letters after you install Citrix Presentation Server. Doing so can destroy data stored on disk drives and can leave Citrix Presentation Server and the operating system unable to operate. For more information about this, see “Deciding to Change Server Drive Letters” on page 42.

Choosing Options for New Farms

The following sections provide information that helps you determine which options you want to select during installation. You may want to print these pages out, with your choices circled, and use them as a guide during Setup.

The sections here include a stage number in their headings for clarity. However, the actual order of the screens may vary according to the options you select during Setup. At a high level, the stages are the following:

- Product installation
- Component selection
- Presentation Server installation and component installation

For illustration purposes, this section assumes a UI-based installation. The information still applies for other methods of installation. This section also assumes, for illustration purposes, that you are installing all components on one computer. However, this may not be the case in practice.

When you create a new farm, you run Setup on the computer you want to be the first server in the farm. If you are performing a UI-based installation of Presentation Server, start the installation by double-clicking on the autorun.exe.

Stage 1: The Initial Autorun Screen

The initial Autorun screen, which you invoke from the autorun.exe, has the following options:

View installation checklist. Make sure you view the Installation Checklist and prepare the product installation as outlined in the checklist. Print a copy of the checklist for easy reference.

Product installations and updates. Select this option to select the components of Citrix Presentation Server you want to install.

Citrix on the Web. Provides links to the Citrix Web site and the Citrix Support Web site.

Install Document Center. Select this option to install the Citrix Document Center on the server. The Document Center gives you a single point of access to all Presentation Server administrator's guides. For more information, see "Citrix Presentation Server Document Center. The Document Center gives you a single point of access to all administrator's guides." on page 57.

Stage 2: Starting Product Installation

If you select **Product installations and updates** from the Autorun, the Citrix Presentation Server 4.5 page appears. You can choose from the following options:

Remap drives. If you are installing Citrix Presentation Server for the first time on your server, this option appears and allows you to remap your server drive letters, as explained in "Deciding to Change Server Drive Letters" on page 42. Citrix recommends that if you want to remap drives, you do so before you install the product and its prerequisites, including .NET 2.0.

Install Citrix Licensing. Select this option to install the Citrix License Server. For more information about installing the license server, see the *Getting Started with Citrix Licensing Guide*.

Install Citrix Presentation Server 4.5 and its components. Select this option to install or upgrade to Citrix Presentation Server or its components. When you select this option, the Citrix Presentation Server Components Setup wizard appears.

Install management consoles. Select this option to install the Access Management Console and the Management Console for Citrix Presentation Server only. You can install both consoles on computers other than those running Citrix Presentation Server, such as workstations and laptops.

Stage 3: Component Selection

After selecting **Install Citrix Presentation Server 4.5 and its components**, the following screens appear:

- The License Agreement.
- The Prerequisites Installation screen, which lists the prerequisites Setup install automatically. These prerequisites are only installed when you run a UI-based installation that you invoke from the Autorun.
- The **Component Selection** page. This screen lets you select the major components you want to install. By default, all components except the license server are selected for installation. When you click **Next**, you start a sequence of separate Setup wizards, each of which guides you through the installation of a particular component of Citrix Presentation Server.

The following section describes the components you can select from the Component Selection page. Depending on the components you choose to install, you may not encounter all configuration options described in this section, or you may encounter them in different order. You can install any or all of the following components:

- **Citrix Licensing**. This option lets you install or upgrade the licensing components needed to run your Citrix product. Every server farm must have access to a Citrix License Server to function correctly. The Citrix License Server can be installed on the same server as Citrix Presentation Server or a different server, such as one you use as a Web server. You do not need to install Citrix licensing every time you install Presentation Server on a computer. Rather, you can point your computers running Presentation Server to a common Citrix license server.

  If you disable the **Citrix Licensing** component in the Component Selection page, Setup warns you that Presentation Server requires a license server. You can install the license server either now on this computer or a different one after you finish Setup. If you select **Install a license server now**, Setup starts installing a license server on this computer.

  For more information about how your server farm uses licensing and needs a license server, see the *Getting Started with Citrix Licensing Guide*.

- **Access Management Console**. The Access Management Console lets you manage all your Citrix Access Suite components from a single location, which snaps in to the Microsoft Management Console (MMC). For Setup information, see "Stage 4: Installing the Access Management Console" on page 58. For information about usage, see "Using the Access Management Console" on page 100.
- **Web Interface.** The Web Interface gives you the infrastructure to make applications available both from a Web page and through the Program Neighborhood Agent. Install the Web Interface if you want users to:
  - **Access applications through a Web browser.** Users can access published applications through the Web Interface. The Web Interface presents users with custom Web pages with links to the published applications users are authorized to launch. The links are dynamically generated based on users' settings, so different users see different links depending on the applications the users have permissions to use.
  - **Access applications through the Program Neighborhood Agent.** You do not need to publish a Web page if you want users to access published applications through the Program Neighborhood Agent. However, because this client leverages the technology provided by the Web Interface, you must install the Web Interface to use the Program Neighborhood Agent.

  Although both methods of application delivery—through a Web browser or through the Program Neighborhood Agent—offer a different user experience, both methods rely on Java object technology provided by the Web Interface and executed on a Web server.

  The Web Interface requires a server running both Microsoft Internet Information Services (IIS) Version 6.0 and the Microsoft Java Virtual Machine (JVM). For large-scale deployments, Citrix recommends that you run the Web Interface on dedicated Web servers. For small deployments, you can run Citrix Presentation Server and the Web Interface on the same server. However, scalability and security should be considered.

  For more information about configuring the Web Interface, see the *Citrix Web Interface Administrator's Guide*.
- **Citrix Presentation Server.** Selecting this option enables you to install Citrix Presentation Server and its various components. This options you can select for Presentation Server are explained in "Stage 6: Installing Citrix Presentation Server and its Components" on page 59.

- **Presentation Server Console**. The Presentation Server Console is a centralized management utility you use in conjunction with the Access Management Console to administer a farm running Citrix Presentation Server. The Presentation Server Console is installed by default when you install Citrix Presentation Server. However, you can install standalone copies of the Presentation Server Console on devices that do not have Citrix Presentation Server installed. For more information about the console, see "Using the Citrix Presentation Server Console" on page 112. To install a standalone copy of the Presentation Server Console, select **Install management consoles** from the autorun screen and then follow the instructions in the Setup wizard.

- **Citrix Presentation Server Document Center**. The Document Center gives you a single point of access to all administrator's guides.

  If you are installing Citrix Presentation Server for the first time, use the Document Center for information and in-depth guidelines about planning your server deployment, from designing server farms to updating client software. If you are upgrading from an earlier release, use the Document Center for important information about upgrading and about new features in this release.

  You can install a standalone copy of the Document Center on any Windows computer without installing Citrix Presentation Server. To ensure you have access to all relevant information when you need it, you can install the Document Center before you install or upgrade to Citrix Presentation Server.

  To view, search, and print the contents of the Document Center, install Adobe Reader 5.0.5 or later with Search on the computer. You can download Adobe Reader for free from Adobe Systems' Web site at http://www.adobe.com/.

  To install the Document Center, select **Install Document Center** from the initial autorun screen and then follow the instructions in the Setup wizard.

Stage 4: Installing the Access Management Console

The Access Management Console is a framework in to which you install features, known as snap-ins or extensions. Each extension provides additional administrative functionality for your Citrix environment.

During Access Management Console Setup, you are prompted to select the extensions you want to install from a Component Selection page. In most cases, Citrix recommends you install the default selection. The following extensions are available:

- Access Management Console—Diagnostics
- Access Management Console—Framework
- Access Management Console—Hotfix Management
- Access Management Console—Knowledge Base
- Access Management Console—Legacy Tools
- Access Management Console—Report Center
- Access Management Console—Web Interface
- License Server Administration
- Presentation Server Administration
- Presentation Server Reports

Depending on the extensions that you select, you may be prompted to install others that are required by the extensions you selected. To install the extensions, you must install the console framework.

Stage 5: Installing the Web Interface

Before installing the Web Interface, make sure you have the installation prerequisites specified in the Installation Checklist and in the *Citrix* Web Interface *Administrator's Guide.* Not having these prerequisites can cause Setup to fail.

If you select the Web Interface on the **Component Selection** page, wizard pages appear that enable you to install the Web Interface as follows:

- **Common Components.** Setup prompts you to select a location to install the common Web Interface components.
- **Clients.** Setup prompts you to install the Clients from the Components CD.

Important After installing the Web Interface, you must create one or more sites using the Access Management Console before you can use the Web Interface. Use the Access Management Console to navigate to the Web Interface node under Configuration Tools. Right-click on Web Interface, then select Create site and follow the instructions displayed by the site creation wizard.

For more information about configuring the Web Interface, see the *Citrix* Web Interface *Administrator's Guide*.

Stage 6: Installing Citrix Presentation Server and its Components

If you select Citrix Presentation Server on the **Component Selection** page, wizard pages appear that enable you to install Citrix Presentation Server and its various components described as follows:

Step 1: Selecting the Product Edition

Select the edition of Citrix Presentation Server you are licensed to run. After you purchase Citrix Presentation Server, you can select from three editions:

- **Enterprise Edition**
- **Advanced Edition**
- **Standard Edition**

If you have questions about which edition to choose, contact your reseller or go to the Product Information area of the Citrix Web site at http://www.citrix.com/products. Based on the edition you select, Setup presents you with the components that are available for installation.

Step 2: Selecting Components of Citrix Presentation Server

This **Component Selection** page presents you with a list of Presentation Server components. The components vary based on the edition of Citrix Presentation Server (Standard, Advanced, or Enterprise Edition) you are installing. Read this section to determine what components you want to install. Click **Disk Cost** to view the amount of disk space the selected components require.

Management Console. (This component is also known as the Presentation Server Console.) Installs the Presentation Server Console, which is an interface that lets you create policies, configure printing, configure zones, create isolation environments, and perform specific tasks with Citrix management tools, such as Resource Manager and Installation Manager. To administer your farm, you must install this component on at least one server in your farm or one remote computer.

Installation Manager. (Enterprise Edition only.) Provides centralized, farm-wide installation capabilities such as support for unattended installs, packager rollback, scheduled package delivery, and MSI support. The Installation Manager component includes the following subfeatures:

- **Installer Service.** (A component of Installation Manager.) Provides the ability to install applications packed by the packager to computers running Citrix Presentation Server.
- **Packager.** (A component of Installation Manager.) Monitors application installation routines and packages all application files for distribution to your server farm.

Resource Manager. (Enterprise Edition only.) Provides customizable metrics and reporting, real-time graphs and alerts, and capacity planning for server farm resources.

Application Streaming. Provides application streaming to servers and desktops. This component includes the Streaming Client subfeature. For more information about the Application Streaming component, see the *Citrix Application Streaming Guide.*

Load Manager. (Advanced and Enterprise Editions.) Provides load balancing of user connections across servers to more effectively use server resources.

Network Manager. (Enterprise Edition only.) Provides the ability to administer server farms through the native management consoles of leading network management solutions.

Program Neighborhood. Installs a pass-through client on the server. If you do not select either Program Neighborhood or Program Neighborhood Agent, Program Neighborhood Agent is installed by default. For more details, see "Step 3: Installing a Pass-Through Client" on page 61

Program Neighborhood Agent. As discussed above, this installs a pass-through client on the server. For more details, see "Step 3: Installing a Pass-Through Client" on page 61.

WMI Providers. (Enterprise Edition only.) Installs WMI providers. Windows Management Instrumentation (WMI) is the standard management infrastructure included as part of Windows Server 2003. The WMI Provider for Citrix Presentation Server supplies information about servers and server farms. This information is displayed by the Citrix Presentation Server Management Pack, which is a plug-in to Microsoft Operations Manager (MOM). You must install the WMI Provider on each server you want to monitor with MOM.

The Citrix Presentation Server Management Pack, used with the WMI Providers, allows you to use the MOM environment to monitor the health and performance of servers running Citrix Presentation Server and license servers. The Management Pack provides real-time event and performance monitoring and includes an extensive knowledge base, with links to Citrix Knowledge Center articles and other sources of information.

Step 3: Installing a Pass-Through Client

Running a pass-through client on a server gives users of other, less feature-rich clients access to the features of Program Neighborhood Agent. Users launch the pass-through client from the server desktop or as a published application and then connect to their sets of published applications from within the pass-through client. In addition, installing a pass-through client on the server allows you to test client-server connectivity.

Configuring a Server Address for the Pass-Through Client. If you select Program Neighborhood Agent as the pass-through client, you must specify the URLs of the Web server running the Web Interface. Program Neighborhood Agent uses a configuration file that is located on the Web server that hosts the Web Interface.

By default, Setup uses “localhost” as the server address. If you installed the Web Interface on a different server, specify that server’s address.

Enabling Pass-Through Authentication for the Pass-Through Client. Pass-through authentication allows the user’s local credentials to be passed to the server for authentication. If you enable pass-through authentication, users are not explicitly prompted for authentication to Citrix Presentation Server.

Step 4: Creating a Server Farm

When you run Setup on the first server in a farm, you are creating the farm. In the **Create or Join a Server Farm** screen, select **Create a new farm**.

However, before you create a new farm, you need to know the following:

- A name for the new server farm.
- Which database to use to host the farm data store. If you are using Microsoft Access, the database is created on the first server on which you run Setup.
- Which user account should be initially granted full access to all farm management tasks.

After you select the **Create a new farm** option, the Create a Server Farm page appears. This is the page on which you specify the name of the farm and zone, and where you specify the location of the data store. Depending on your database, you need to perform different steps on this screen:

- If you are creating a server farm with a SQL Server, Oracle, or DB2 data store, see "SQL Server, Oracle, or DB2 Data Store" on page 62
- If you are creating a server farm with a Microsoft Access or SQL Server Express data store, see "Microsoft Access or SQL Server 2005 Express Edition" on page 63

SQL Server, Oracle, or DB2 Data Store

The same procedure for configuring a data store connection are used whether the data store is a Microsoft SQL Server database, an Oracle database, or an IBM DB2 database.

To create a server farm with a SQL Server, Oracle, or DB2 data store

1. On the **Create or Join a Server Farm** Setup screen, select **Create a new farm** and click **Next**.
2. On the **Create a Server Farm** Setup screen, enter the following information:
   A. Enter a name for the new server farm. Farm names can include spaces but cannot be more than 32 characters in length.
   B. Select **Use the following database on a separate database server** and select the database from the list.

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

C. The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option **Use default zone name** and enter the new name.

3. Click **Next** and continue with Setup.
4. Configure the ODBC driver associated with the database you are using. For instructions for doing this for Microsoft SQL Server, Oracle, and IBM DB2 databases, see the documentation for the relevant database.

Microsoft Access or SQL Server 2005 Express Edition

To use a Microsoft Access database as the farm data store, you create the database when you install Citrix Presentation Server on the first server in the farm. To use SQL Server 2005 Express SP1 for your farm data store, you must install it on the server before you install Citrix Presentation Server. Additional servers connect to the first server using default TCP port 2512 for both database types.

To create a server farm using Access or SQL Server Express for the data store

1. On the **Create or Join a Server Farm** Setup screen, select **Create a new farm** and click **Next**.
2. On the **Create a Server Farm** Setup screen, enter the following information:

   A. Enter a name for the new server farm. Farm names can include spaces but cannot be more than 32 characters in length.

   B. Select **Use a local database on this server** and select the database from the list.

   C. The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option **Use default zone name** and enter the new name.

3. Click **Next** and continue with Setup.

For more information about choosing the type of database and other decisions related to the data store, see Chapter 2, “Planning for Deployment.”

Step 5: Assigning Farm Administrator Credentials

When you install the first server in a new server farm, you are required to provide credentials for a full authority Citrix administrator. This account has the authority to manage and administer all areas of farm management. Use this account to log on to the Access Management Console and to add other individuals to the Citrix administrators group.

After installing Citrix Presentation Server, if you want to create, delete, and configure new Citrix administrator accounts, you must log on to the Access Management Console as a full authority administrator.

To create new Citrix administrator accounts

1. In the Access Management Console, with the farm selected in the left pane, from the **Action** menu, select **New > Add Administrator**.
2. Look up or select the name of the configured user or user group account you want to designate as a Citrix administrator and click **Add**.
3. Enter the email and SMS alert contact details for the account.
4. On the **Privileges** page, select the authority level you want to grant the administrator account from the following options:
    - Select **View Only** to give the administrator view-only access to all areas of farm management
    - Select **Full Administration** to give the administrator full access to all areas of farm management
    - Select **Custom** to delegate specific, limited tasks to the administrator
5. If you selected **Custom** in the previous step, in the **Tasks** pane you must next select the tasks you want to delegate to the custom administrator.

Note To create administrator accounts with full or view-only authority, you select individual or group accounts and associate them with full or view-only *privileges*. Both full and view-only privileges apply farm-wide. To create administrator accounts with custom authority, you select individual or group accounts, assign them custom *privileges*, and then *permissions* to perform select tasks.

Step 6: Enabling IMA Encryption

This optional feature provides more robust encryption of sensitive data in the IMA data store. If you enable this feature during installation, you must enable it on all subsequent servers that join the farm.

Important Review the information in "Planning for IMA Encryption" on page 41 before enabling IMA encryption. This information provides guidance about how to prepare your environment and what you need to do before you enable IMA encryption through Setup.

Citrix recommends that you install Presentation Server using network credentials if you are enabling IMA encryption. For information about installing a computer as a local administrator, see "Enabling IMA Encryption as a Local Administrator" on page 225.

Note If you have multiple farms in your environment, Citrix recommends that you generate separate keys for each farm.

When you enable IMA encryption on subsequent servers you are installing in a farm, you can either add the key file to each computer before installation, put the key file in a shared network location that is accessible by specifying a UNC path, or put the key file on a diskette that you use for every installation. To facilitate the process in large environments where you are performing unattended installations, store the key file in a shared network location or include it as part of the image of the server on which you are deploying Presentation Server.

Note Whenever you add a key file to a network location, make sure that you have explicit rights to the key file so that you are not prompted for your credentials when you run Setup. See "Storing the Key on a Shared Location" on page 224.

Enabling IMA Encryption When Creating a Farm

The first time you create a farm you can either use a key you generated before installation using the CTXKEYTOOL or create one on the spot using the Setup program.

To enable IMA encryption when creating a farm

1. On the **Enable IMA Encryption** page, select the **Enable IMA Encryption** check box and click **Next**.
2. On the **IMA Encryption Key Type** page, select one of the following options:

    - **Install Key From File**. Select this option if you already generated a key file for this farm and you have the key file on a USB flash drive, diskette, or location to which you can browse.

      The difference between this option and the **Use Previously Loaded Key** option is that you can use this option to specify the key file for a server and load it simultaneously. The key does not have to be local. If you already loaded the key, use the **Use Previously Loaded Key** option. If you select this option, see "To install a key from a file" on page 67.

    - **Generate and Install New Key**. Select this option if you have not generated a key yet for a new farm. This option generates a key, and installs it on the local computer. You can use this option if you did not do any advance preparations for IMA encryption before you began installing the first server on your farm. If you select this option, see "To generate a new key file and install the key" on page 67. This option is disabled if you are joining a farm.

    - **Use Previously Loaded Key**. Select this option if you generated a key using the CTXKEYTOOL and loaded it on this server before you started Setup. If you select this option, see the "To use a previously loaded key during Setup" on page 68. This option is not available if a key is not present on the local computer. For information about when you want to load a key before you run Setup, see "Planning for IMA Encryption" on page 41.

To install a key from a file

Note Citrix recommends that in environments with multiple farms, you always create different keys for each farm.

1. Select **Install Key From File**. The Encryption Key File Location dialog appears.
2. Browse to the location of the key file. After you select the key file, the Citrix Licensing Settings page appears. This indicates that you have successfully loaded the key on this server.

   If the key file is on a network location, you can only specify this network location by using a UNC path.
3. Continue to "Step 7: Specifying the Citrix License Server" on page 68.

To generate a new key file and install the key

1. Select **Generate and Install New Key**. The Encryption Key Save Location dialog appears.
2. Using the dialog box, save the key with a meaningful name to any directory on your local machine. Citrix suggests naming the key after the farm it will be used on. For example, **farmakey.ctx**. Citrix also suggests saving the key to a folder that uses the name of your farm. For example, **Farm A Key**. The IMA encryption feature does not look at the extension of the file, so you can pick any extension that is available on your server and is not registered.

   After you click **Save**, the Citrix Licensing Settings screen appears. IMA encryption will be enabled on the first server in your farm when you finish Presentation Server Setup.

Important Citrix strongly recommends backing up the key file you generate for a farm immediately after you create this file. For more information about backing up a key, see "Backing Up Keys" on page 226.

To use a previously loaded key during Setup

1. Select **Use Previously Loaded Key**. This option is only available if you previously loaded a key on this server. However, note the following:
   - If you are performing an UI-based installation, Setup warns you if you loaded the wrong key for a server you are joining to this farm. (You must always use the same key and key file on a server in a farm as you used on the other servers in a farm.)
   - If you are performing a silent installation, Setup checks to make sure that the key you loaded is a valid key for IMA encryption. However, Setup does not warn you if the key you loaded does not match the rest of the keys on the farm you are joining.
2. Click **Next**. If you loaded a valid key, the Citrix Licensing Settings page appears. IMA encryption will be enabled on the first server in your farm when you finish Presentation Server Setup.

Step 7: Specifying the Citrix License Server

Before users can connect to Presentation Server, you must configure it to point to a Citrix License Server so that your software is licensed. If you do not have the necessary information (license server name and port number) available at the time you install Citrix Presentation Server, you can configure the information later from the Access Management Console.

To specify the license server for this server

1. Select one of the following options:
   - **Enter the host name for the machine hosting your Citrix License Server**. Enter the host name for the license server and the port number, if the license server is not using the default port number (27000). Subsequent servers that join the farm use this information by default.
   - **Enter the correct host name later**.
2. Click **Next**.

Note When specifying a license server, you cannot leave the license server name blank.

Step 8: Configuring Session Shadowing

You use session shadowing to monitor and interact with user sessions. When you shadow a user session, you can view everything that appears on the user's session display. You can also use your keyboard and mouse to remotely interact with the user session.

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

During Setup, you can limit or disable shadowing. You can disable shadowing of ICA sessions on all servers in a server farm, for example, if legal privacy requirements prohibit shadowing of users' sessions. Alternatively, you may want to disable shadowing on servers that host sensitive applications, such as personnel or payroll applications, to protect confidential data.

Shadowing is protocol-specific. This means you can shadow ICA sessions over ICA and Remote Desktop Protocol (RDP) sessions over RDP only.

Important Shadowing restrictions are permanent. If you disable shadowing or enable shadowing but disable certain shadowing features during Setup, you cannot change the restrictions later. Any user policies you create to enable user-to-user shadowing are subject to the restrictions you place on shadowing during Setup. Do not disable shadowing as a substitute for user- and group-specific connection policies.

Prohibit shadowing of user sessions on this server. Select this option to permanently disable shadowing of user sessions on the server. If you disable shadowing during Setup, you cannot enable it using other Citrix Presentation Server configuration utilities or by creating connection policies.

Allow shadowing of user sessions on this server. Select this option to enable shadowing of user sessions by the server. When you enable shadowing, you can apply the following restrictions:

- **Prohibit remote control**. By default, authorized users can view a session they are shadowing, and also use their keyboard and mouse to interact with it. Select this option to allow authorized users to view sessions but not to have keyboard and mouse input. Shadowing without keyboard and mouse input may conceal from the user the fact that a session is being shadowed.

- **Force a shadow acceptance popup**. By default, users are notified by an acceptance prompt when other users are attempting to shadow their sessions. Select this option to deny users the ability to shadow sessions without sending this acceptance prompt.
- **Log all shadow connections**. You can log events such as shadowing attempts, successes, and failures in the Windows event log and examine them using Event Viewer. Select this option to enable logging.

Step 9: Configuring the Citrix XML Service Port

Citrix Presentation Server uses the Citrix XML Service to supply servers running the Web Interface and TCP/IP+HTTP- connected clients with the names of published applications that are available in a server farm. By default, Setup configures the Citrix XML Service to share the default TCP/IP communication port (port 80) with Microsoft Internet Information Services (IIS).

Caution If you plan to install both Citrix Presentation Server and the Web Interface onto a 64-bit machine, ensure that the Citrix XML Service is not set to "port-sharing with IIS" (the default option set during the Presentation Server installation process). Instead you must select the option to install the Citrix XML Service on a standalone port, for example port 8080.

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

Using a different port at Setup. If you do not want the Citrix XML Service to share the TCP port with IIS, you can use a separate port for the Citrix XML Service. On the **Configure Citrix XML Service Port Setup** page, select **Use a separate port** and enter the new port number. If you plan to change the port used by the Citrix XML Service on Citrix Presentation Server, make sure the port you plan to use is not used by any other application.

For a list of ports in use, type **netstat -a** at a command prompt. Make a note of the port number you specify. If you use a port other than the default port 80, you must configure servers running the Web Interface and any clients using TCP/IP + HTTP server location to use the port you choose. For instructions about configuring Web Interface to use a different port, see the *Citrix Web Interface Administrator's Guide*. For instructions about configuring the clients to use a different port, see the client administrator's guides.

Important All servers in the farm must use the same TCP port for the Citrix XML Service.

Changing ports. If you entered a port number different from the default **Share with IIS** during Presentation Server installation, you can change the port number by modifying the XML Service server property. This option appears on the **Server Properties** page, under **XML Service**. Use the drop-down menu to choose a different port.

If you choose to share a port between IIS and the XML Service when you installed Presentation Server and you want to change the XML Service port, you must do so manually. There is no option on the **Server Properties > XML Service** page.

To manually change the XML Service port to use a port different than IIS after installation

1. At a command prompt, stop IIS by typing:

   net stop w3svc

2. Delete the following files from the IIS scripts directory on your Web server:

   - ctxadmin.dll
   - CtxConfProxy.dll
   - ctxsta.dll
   - radexml.dll
   - wpnbr.dll

3. At a command prompt, restart IIS by typing:

   net start w3svc

   The XML Service no longer shares a port with IIS.

4. To ensure the XML Service is stopped, at a command prompt, type:

   net stop ctxhttp

5. At a command prompt, to unload the XML Service from memory, type:

   ctxxmlss /u

6. To install the XML service, type:

   ctxxmlss /r*nn*

   where *nn* is the number of the port you want to use. For example, **ctxxmlss /r88** forces the Citrix XML Service to use TCP/IP port 88.

7. At a command prompt, stop the XML Service by typing:

   net stop ctxhttp

This setting takes effect only after the XML Service restarts.

To manually configure Citrix XML Service to share the TCP port with IIS

1. At a command prompt, stop the XML Service by typing:

   net stop ctxhttp

2. At a command prompt, to uninstall the Citrix XML Service, type:

   ctxxmlss /u

3. Copy the following files to the IIS scripts directory on your Web server:

   - ctxconfproxy.dll
   - ctxsta.config
   - ctxsta.dll
   - ctxxmlss.exe
   - ctxxmlss.txt
   - radexml.dll
   - wpnbr.dll

   These files are installed in \Program Files\Citrix\System32 during Presentation Server installation.

   The default scripts directory is \Inetpub\Scripts.

4. In the IIS scripts directory, create a folder called **ctxadmin** and copy the file ctxadmin.dll from \Program Files\Citrix\System32 to \Inetpub\Scripts\ctxadmin.

5. Use Internet Service Manager to give the files read and write access.

6. At a command prompt, stop and restart the Web server by typing:

   iisreset

This setting takes effect after the Web server restarts.

Step 10: Adding Users to the Remote Desktop Users Group

Only users who are members of the Remote Desktop Users group can connect remotely to the server you are installing. By default, there are no users in the Remote Desktop Users group, so users are blocked from connecting remotely. At this point in the Setup process you can add users to this group or skip this step and add them later. Note that if you do not designate any users as part of this group, only administrators can connect remotely to the server.

Note Presentation Server prompts you to restart at the end of installation. You must restart Presentation Server for it to integrate with Terminal Services properly and to finish configuring the GINA library used by Presentation Server.

Stage 7: Installing the Presentation Server Console

The Presentation Server Console is also known as the Management Console for Citrix Presentation Server and is often referred to this way in Setup.

When you install the Presentation Server Console, you must specify a destination folder where you want Setup to install it.

Stage 8: Installing the Document Center

When you install the Document Center, you must specify a destination folder where you want Setup to install the Document Center files. You must have Acrobat to display the documentation contained in the Document Center. For more information about the Document Center, see “Product Documentation and Information” on page 13.

Deploying Subsequent Servers

After you install the first server in the farm and install management components such as the Presentation Server Console and the Access Management Console, you can begin installing Presentation Server on the other servers in your environment that will eventually form your farm.

When you install Presentation Server on subsequent servers, you *join* a farm rather than create one. You do not see some of the options you saw in Setup when you created the first server in your farm, and Presentation Server Setup prompts you for the name of your farm.

In addition, Setup prompts you to join a farm directly or indirectly. When you see the **Create or Join a Server Farm** page in Presentation Server Setup, you are actually specifying how subsequent servers in the farm communicate with the data store and if they communicate through an intermediary server. It is possible to have a mixture of servers that communicate directly and indirectly with the data store.

Information to Prepare before Installing Subsequent Servers

Before you join servers to an existing server farm, you must have the following information at hand to specify the data store:

- If you are using a database (Microsoft Access or SQL Server Express) on the first server in the farm, you need to know the name of that server and the logon credentials of a user authorized to access the database.
- If you are using a database (Microsoft SQL Server, Oracle, or IBM DB2) on a dedicated server, you need to know which type of database is configured to host the data store. You also need to know the logon credentials of a user authorized to access the database.

For more information about planning the data store, see "Choosing a Database" on page 34. For information about creating a data store before running Setup, see "Setting Up the Data Store" on page 49.

In addition, if you enabled IMA encryption when you created the farm, you need to do one of the following:

- Copy the key you generated when you created the farm (that is, the key you used for the first server in the farm) to a network share that you must specify with a UNC path
- Access the key, which you generated when you created the farm, from a diskette or USB flash drive

Citrix recommends that you delete the key off the server after you load it.

For more information, see "Stage 3: Specifying the Location of the IMA Encryption Key File" on page 76.

Joining a Server Farm

The following section provides information only about the stages of installation that differ when you are installing the first server in your farm. When you want to add servers to an existing server farm, run Setup on those servers and choose the option to join an existing farm.

Stage 1: Initial Setup

Until you reach the **Create or Join a Server Farm** page of the Citrix Presentation Server for Windows Setup wizard, Setup is identical whether you are joining or creating a farm. When you are running Setup on a subsequent server in the farm you are creating, you install the major components that you want on the server just like you do when you run Setup to create a farm. See "Creating a New Farm" on page 52 for details about the initial pages in Setup.

Stage 2: Joining a Server Farm

In the **Create or Join a Server Farm** page of the Citrix Presentation Server for Windows Setup wizard, select **Join an existing farm**. After you click Next, the Join a Server Farm page appears, which requires you to configure the server's connection to the existing server farm. This page requires that you either perform one of the following:

- Specify the name of the server where you installed Presentation Server initially or the name of the server through which you want to connect to the data store (an intermediary server)
- Create an ODBC data source that you can use to connect to the SQL Server

When you do this, you are specifying whether you want the server you are currently installing to communicate with the data store directly or indirectly.

- If your data store is on a SQL Server, Oracle, or DB2 database and you want to connect to the data store directly, see "To add a server to an existing server farm with a SQL Server, Oracle, or DB2 data store" on page 75.
- If you want to use an Access or SQL Server Express database as your data store and you want to connect to the data store indirectly, see "To add a server to an existing server farm with an Access or SQL Server Express data store" on page 75.

To add a server to an existing server farm with a SQL Server, Oracle, or DB2 data store

1. On the **Create or Join a Server Farm** Setup screen, select **Join an existing farm** and click **Next**.
2. Select **Connect directly to the database using ODBC**. Select your database from the list and click **Next**.
3. Configure the ODBC driver associated with the database you are using. For instructions for doing this for Microsoft SQL Server, Oracle, and IBM DB2 databases, see the documentation for the relevant database.

To add a server to an existing server farm with an Access or SQL Server Express data store

1. On the **Create or Join a Server Farm** Setup screen, select **Join an existing farm** and click **Next**.
2. Select **Connect to a database on this server** and then enter the name of the server hosting the Access or SQL Server Express database. The default communication port is 2512.
3. Accept the default zone name or enter a different zone name, and click **Next.**

4. On the Access the Database on a Citrix Presentation Server computer page, enter credentials for the server to which you are connecting, and click **Next**.

After performing these procedures, either the Citrix Licensing Settings page or the IMA Encryption Key Type page appears depending if IMA encryption is enabled on the farm you are joining.

Stage 3: Specifying the Location of the IMA Encryption Key File

If you have IMA encryption enabled on the farm you are joining, Setup does not prompt you to enable IMA encryption. Setup automatically detects that IMA encryption is already enabled on the farm you are joining and prompts you to specify the location of the key file.

Depending on whether or not you already loaded a key on this server before you began Setup, the options that are enabled on this page vary.

You cannot generate a new key when you are joining a farm. Consequently, the **Generate and Install New Key** option is disabled when you are joining a farm.

To specify the location of the IMA encryption key file on a server that is joining a farm

1. **Install Key From File.** Select this option if you did not load a key file on this server and Setup detects that you have IMA encryption enabled on the farm. Then follow the procedure "To install a key from a file" on page 67.
2. **Use Previously Loaded Key.** Select this option if you loaded the key that you generated for the first server in the farm onto this server. This option is available only if a key is already loaded on the local server. If you are using a previously loaded key and you choose this option, follow the procedure "To use a previously loaded key during Setup" on page 68.

To verify that IMA encryption is enabled and configured properly on the servers, use the query option in the CTXKEYTOOL, which is located in the Support folder on the Server CD. For information about the query option, see "CTXKEYTOOL" on page 309.

Stage 4: Using Farm Licensing Settings

On the Citrix Licensing Settings page, you are prompted to specify licensing settings for this server. It can either use the same settings as the farm or point to a license server that the other servers in the farm do not use.

To specify the license server for this server

1. Select one of the following options:
    - **Enter the host name for the machine hosting your Citrix License Server**. Use this option if you want to specify that the server you are installing points to a different license server than the rest of the farm. Enter the host name for the license server and the port number, if the license server is not using the default port number (27000).
    - **Use the global farm settings for the license server**. Use this option if you want this server to point to the same license server as the rest of the servers in the farm.
    - **Enter the correct host name later**.
2. Click **Next**.

For more information about licensing, see *Getting Started with Citrix Licensing Guide* and the associated whitepapers listed there.

Upgrading or Migrating an Existing Server Farm

Depending upon the earlier versions of Presentation Server that are being used in your server farm, you may be able to use the *automatic upgrade process* to move to Citrix Presentation Server 4.5 or you may need to *migrate* your farm.

- *Upgrading automatically* means that you are using Setup to upgrade your farm to Citrix Presentation Server 4.5. That is, you run Presentation Server Setup on a server in your existing farm, Setup detects the presence of a previous release of Presentation Server, and runs in upgrade mode. Upgrading automatically preserves the customizations you made to each server and farm, including administrator accounts you created, load evaluators, and published applications. When you upgrade automatically, there are no additional manual processes to perform outside of Setup like there are for migration.
- *Migrating your farm* means that you perform a new installation of Citrix Presentation Server 4.5, but you do so using a manual process that allows you to preserve your farm settings.

Your upgrade or migration path depends on your starting version and environment:

Starting version	Path to Citrix Presentation Server 4.5
Presentation Server 3.0 and 4.0 on Windows Server 2003	Automatic upgrade. See "Upgrading Automatically" on page 81 for details.
Presentation Server 3.0 and 4.0 on Windows 2000 Server or prior versions of MetaFrame.	Phased migration. See "Migrating from Earlier Versions of Citrix Presentation Server" on page 84 for details.

When you migrate your farm, you do not use the upgrade mode in Setup. Migrating differs from new installations because it can preserve the configurations and settings you created in your farm. However, server and farm settings are preserved only in some situations:

- If your server is running Citrix Presentation Server 3.0 or 4.0 on Windows Server 2000, you can perform a partial or *phased* migration by joining Presentation 4.5 servers to an existing farm and removing older servers. Using this method, you maintain existing farm settings and can maintain specific server settings through a manual process—see "Migrating from Earlier Versions of Citrix Presentation Server" on page 84.
- If your server is running MetaFrame 1.0, MetaFrame 1.8, or MetaFrame XP, you must perform a *full* migration to a new farm in which no settings are retained— see "Migrating from Earlier Versions of Citrix Presentation Server" on page 84.

Additional Considerations for Upgrading and Migration

Before upgrading or migrating, consider the following information:

Presentation Server 4.5 requires upgrading Citrix licensing. If you are running the license server that came with Citrix Presentation Server 4.0, you must upgrade to the latest license server, which is included with Citrix Presentation Server 4.5. Your existing license files are compatible with the new license server. For information about upgrading your license server, see the Citrix whitepaper "Licensing: Migrating, Upgrading, and Renaming" (CTX108655).

Migrating from MSDE to a Supported Database. Citrix Presentation Server no longer supports MSDE. If you are upgrading or migrating from a previous release of Presentation Server and your data store is running on an MSDE database, you must migrate the data store from MSDE to another database, such as SQL Server Express. At a high level, the migration involves the following:

- Granting the Network Service account access to the MSDE CITRIX_METAFRAME instance
- Upgrading or migrating your Presentation Server farm to Presentation Server 4.5 using the methods described in this section
- Migrating the MSDE database

This guide provides general instructions for migrating your data store from MSDE to SQL Server Express — see “Migrating to SQL Server 2005 Express” on page 401. Citrix recommends that you review these instructions for insight in to the migration process and important requirements, even if you are migrating your MSDE database to a database other than SQL Server Express.

Upgrading 64-bit Platforms. To upgrade Presentation Server 4.0 for 64-bit Windows platforms to Citrix Presentation Server 4.5, you can use the upgrade and migration procedures discussed in this section. However, switching from the 64-bit Windows platform to 32-bit Windows Server 2003 is not supported.

Installing IMA Encryption During an Upgrade. When you upgrade a server to Citrix Presentation Server 4.5 using the Upgrade program in Setup, the IMA encryption feature is not available as an option. To enable the IMA encryption feature, you must configure it after upgrading by using the CTXKEYTOOL. If you decide that you want to enable IMA encryption, you may want to perform a migration procedure (which requires running Presentation Server Setup to create a new farm), rather than upgrading the existing farm, so that you do not have to configure IMA encryption manually post-installation. For more information about manually enabling IMA encryption, see “Encrypting Sensitive Configuration Logging Data” on page 219.

Restrictions When Upgrading the Access Management Console.

When you upgrade the Access Management Console from the version supplied with Presentation Server 3.0 to that supplied with Presentation Server 4.5, note that there are restrictions on how the later version of the console recognizes any My Views created with, or items discovered by, the earlier version.

If, after upgrading, you are asked whether or not you want to upgrade your .msc configuration file, choose one of the following options:

- If you choose to **Upgrade** the file, you cannot use the earlier version of the console to open the file. For example, this means you will no longer be able to use the earlier version to see any My Views created with it. However, you will be able to use the later version to open the file, and view, edit, and save the My Views.
- If you choose **Don't Upgrade**, the file is not upgraded. For example, this means you will be able to use both versions of the console to see the My Views, but you will be able to edit and save the My Views only in the earlier version.

Mixed Farm Environments

Citrix recommends that, when possible, you upgrade all of the servers in a farm simultaneously so that you do not have different versions of Presentation Server (for example, Presentation Server 4.0 and Presentation Server 4.5) running in the same farm.

When determining whether you want to upgrade all of a farm or part of a farm, you may want to consider whether or not you want to be able to use certain Presentation Server 4.5 features in that farm. Some new features are not available if you have a farm that contains any servers from releases prior to Presentation Server 4.5. New features such as Configuration Logging and IMA encryption are farm-wide settings; they are not supported in a mixed-farm environment. If you want to use these features, you must upgrade your entire farm to Presentation Server 4.5.

If you are using the Access Management Console in a mixed-farm environment, you must run Discovery through the Presentation Server 4.5 version of the Access Management Console. If you want to install the 4.5 version of the Access Management Console on a server running Presentation Server, you must install the console on a server running Presentation Server 4.5.

Important To use the Access Management Console delivered with Presentation Server 4.5 to manage a farm running Presentation Server 4.0 for Windows or Presentation Server 4.0 for Windows 64-bit Edition, you must upgrade at least one server in the farm to Presentation Server 4.5.

Upgrading Automatically

If your server farm is set up with Presentation Server 3.0 or 4.0 on the Windows Server 2003 platform, you can take advantage of the automatic upgrade path to move the farm to Citrix Presentation Server 4.5 and retain the server drive mappings in place from the previous configuration.

Important Some installation prerequisites have changed since Presentation Server 4.0; verify the installation prerequisites by reviewing the Installation Checklist. To access the Installation Checklist, select **View installation checklist** from the initial autorun screen.

When you run Presentation Server Setup to upgrade your farm, you see many of the same options as you see in a new installation. On the initial Autorun screen, select **Install Citrix Presentation Server 4.5 and its components** to run Setup in upgrade mode. Setup detects the existing Presentation Server installation and automatically displays the appropriate options for upgrading your farm.

This is a high-level summary of the tasks required to upgrade a server farm:

1. Upgrade the Citrix License Server.

   Before you upgrade the first server in a farm, upgrade the license server and ensure that you download current licenses.

   For information about upgrading the license server, see the *Licensing: Upgrading, Migrating, and Renaming* whitepaper in the Citrix Knowledge Center.

2. If you need to migrate your data store, do so before you run Presentation Server Setup.

   You must migrate your data store if it is on an MSDE database. Citrix provides utilities for migrating the data store from MSDE and Microsoft Access to SQL Server 2005 Express Edition. For more information, see page 401.

3. If you have configured Resource Manager, upgrade the primary and backup farm metric servers before you upgrade other servers in the farm.

   Resource Manager uses the farm metric servers to interpret information collected from other servers. Farm metric servers running earlier versions of Resource Manager than other servers in the farm may cause inconsistencies.

4. Upgrade the Presentation Server Console, Access Management Console, and Web Interface.

   To automatically upgrade the consoles and the Web Interface and preserve custom configuration settings, accept the default settings in Setup. Accepting the default settings automatically upgrades the consoles and the Web Interface before upgrading the server and preserves custom configuration settings.

5. Upgrade zone data collectors.

6. Upgrade the remaining servers in the farm.

The following procedure provides specific information about options you encounter when you run Setup in upgrade mode. This procedure assume a UI-based installation for illustration purposes.

Before you run Setup, make sure that you have fulfilled all of the installation pre-requisites, including migrating the data store from MSDE, if necessary. See "Migrating to SQL Server 2005 Express" on page 401.

To upgrade a server using Setup

1. Start the Autorun.exe and select **Product installations and updates**.

2. Select **Install Citrix Presentation Server 4.5 and its components**.

3. Accept the License Agreement and the Prerequisites Installation.

4. From the Component Selection page, select the components you want to upgrade and/or install on this server. The components listed include Citrix Licensing, the Access Management Console, the Web Interface, Citrix Presentation Server, the Presentation Server Console, and the Document Center.

   You may need to deselect components that are not installed on the server you are upgrading. Upgrade the components in the order specified on page 82, step 4.

   For more information, see "Stage 3: Component Selection" on page 55 and note the following:

   - If you do not select the Citrix Licensing component, after you click Accept, Setup prompts you to install a license server. See "Stage 3: Component Selection" on page 55 more information.
   - After you select an option on the licensing screen, component installation and upgrade begins.

5. In the Access Management Console **Component Selection** page, select the components that you want to install or upgrade. For more information about Access Management Console component installation, see “Stage 4: Installing the Access Management Console” on page 58.

   Depending on the components you chose to install, the Web Interface Setup begins.

6. Perform the following steps to install the Web Interface component:

   A. If Setup prompts you to enable ASP.NET 2.0 in Internet Information Services (IIS), click **OK**. The Web Interface Setup requires that ASP.NET 2.0 is enabled in IIS. If you are using the Setup wizard, Setup automatically prompts you to allow it to make this change.

   B. Select a location for Common Components.

   C. Specify the location of the clients.

      For more information about the Web Interface component installation, see “Stage 5: Installing the Web Interface” on page 58 and the *Citrix Web Interface Administrator’s Guide*.

   D. After you click **Finish**, the Presentation Server Components Setup begins and Presentation Server Setup begins migrating your existing farm settings.

7. When Presentation Server Setup prompts you to upgrade the server, click **Yes**.

   A. Presentation Server Setup prompts you to migrate your data store from MSDE to a supported database. If you do not have an MSDE data store or you have already migrated your data store, click **Yes**. If you do not migrate your MSDE data store, you receive an IMA Service error when you start Presentation Server and the data store eventually stops working. Not upgrading is not supported. For more information on performing the migration, see “Migrating to SQL Server 2005 Express” on page 401.

   B. Click **Close** when you are finished installing Presentation Server.

8. When the Management Console for Citrix Presentation Server 4.5 Installation Wizard prompts you to install the Presentation Server Console, click **Next**.

   A. See “Stage 2: Starting Product Installation” on page 54 for information about the Presentation Server Console installation options.

   B. Click **Finish**.

9. Install the Citrix Presentation Server Document Center.
10. Restart the computer on which you just installed Presentation Server. Restarting the server is a critical part of the Presentation Server installation process.

Migrating from Earlier Versions of Citrix Presentation Server

The automatic upgrade procedure for Citrix Presentation Server 4.5 is supported only on Windows Server 2003. You must migrate your server farm if you want to do either of the following:

- Upgrade servers running Presentation Server 3.0 or 4.0 for Windows 2000 Server
- Upgrade servers running earlier versions of Presentation Server, such as MetaFrame 1.0, MetaFrame 1.8, or MetaFrame XP

If you are migrating from Presentation Server 3.0 or 4.0 for Windows 2000 Server you can retain your farm's configuration information automatically by first having a server that is running Citrix Presentation Server 4.5 join the farm and acquire this information. After that, the migration path is the same, culminating with the decommissioning of the legacy servers.

The following procedure details a "full" migration in which no settings are retained. This approach must be used for migrating legacy server farms running MetaFrame 1.0, MetaFrame 1.8, or MetaFrame XP.

To migrate a server farm

1. Install Citrix Presentation Server 4.5 on a server that is independent of your MetaFrame 1.0, 1.8, or XP farm. This is the first server for the new farm.
2. Use the Presentation Server Console to configure your newly installed server to match the settings of your farm running MetaFrame 1.0, 1.8, or XP. Ensure that you also match the settings for published applications.

   Alternatively, you can create a script to export and import published application information. See the Citrix Developer Network for additional information about the Citrix Application Publishing SDK and Citrix Presentation Server SDK.

3. Deploy Web Interface as the primary entry point for your newly installed farm.

   Use DNS CNAME (alias) records for the Web Interface servers. Use a simple mnemonic for the DNS alias, such as *myapps*. For example, Citrix could have an internal Web Interface deployment with multiple servers that share the DNS alias myapps.citrix.com.

4. Open the new deployment for testing by pilot users.

5. After refining the pilot deployment, switch users to it.

   Instruct users to access your Web Interface server URL. Here is an example based on the previous DNS alias example:

   https://myapps.citrix.com

6. If most clients in your organization are Windows based, Citrix recommends that you deploy Web Interface with Program Neighborhood Agent.

   Use the Citrix client packager to repackage the Program Neighborhood Agent and include the URLs of your Web Interface deployment. For more information, see the *Clients for Windows Administrator's Guide*.

7. Deploy the new package to client desktops using Active Directory group policy, Microsoft Systems Management Server (SMS), or another third-party deployment product. This deployment method requires no user input.

8. Decommission the farm running MetaFrame 1.0, 1.8, or XP.

Configuring Presentation Server after Installation

After you finish installing Citrix Presentation Server, you must perform additional tasks before users can log on to your farm. At a high level, you must perform the following tasks:

1. Start the Access Management Console. See "Starting the Access Management Console" on page 104 for details.

2. Using the Access Management Console, discover the servers in your farm. See "Finding Items in Your Deployment Using Discovery" on page 104 for details.

3. Create any administrative or user accounts you need for your farm. See "Users and Accounts" on page 100 for details.

4. Create Web Interface sites, if required. See the *Citrix Web Interface Administrator's Guide* for details.

5. Publish applications. See Chapter 5, "Publishing Resources" for details.
6. Perform any additional customizations that you require, such as setting policies, configuring printing, and load balancing. See information throughout this guide and the *Load Manager Administrator's Guide* for details.

In addition, you also need to create client packages to deploy to users. Factors for choosing client packages and methods of deploying them are discussed in the section that follows and the *Clients for Windows Administrator's Guide*.

Deploying Client Software to Users

This section provides an overview of the following:

- Factors to consider when choosing a client deployment method
- Client deployment methods, such as the Web Interface and Active Directory
- Web-integrated Presentation Server deployments using the Web Interface
- Procedures for deploying the Client Packager using Active Directory
- Support for Remote Desktop Web Connection software

For information about the clients and creating client packages, see the *Clients for Windows Administrator's Guide* and the *Citrix Web Interface Administrator's Guide*.

Note Starting with Citrix Presentation Server 4.5, the Auto Client Update feature and ICA Client Creator utility are no longer supported.

Choosing a Client Deployment Method

To choose the best method for deploying client software, decide how your users will access published applications and consider the following factors before you decide which deployment method to adopt:

The clients you need to deploy. To determine which clients you need to deploy, determine which client devices and operating systems you need to support.

A smaller organization with many similar client devices might need to deploy the client on only one or two platforms. In this scenario, copying the necessary files to a central network share point for download may be the most efficient deployment method.

Heterogeneous computing environments and geographic separation of large enterprises and Application Service Providers (ASPs) can make it impossible to predetermine which client devices need to be supported. In these scenarios, Web-based installation is the most efficient deployment method.

Centralized control and configuration requirements. Determine what limits you need to impose on users' access to published applications. You can configure various settings before you initially deploy the clients. For information about preconfiguring clients, see the administrator's guide for the required client.

Ease-of-use requirements for users. Providing a simple installation process that requires little or no interaction from users might be a key factor.

Enterprises and ASPs with hundreds or thousands of users with varied computing expertise require the most foolproof deployment process. You can "push" the client software to your users by various methods, including through the use of logon scripts or Windows scripts, or through the use of a client software distribution system.

If you want to deliver applications to your users through a Web page, use the Web Interface in conjunction with Citrix Presentation Server to deploy client software.

In general, you can deliver the appropriate client software to your users and install it with the following methods:

- Using the Web Interface to provide Web-based access
- Using Active Directory Services in Windows (for clients that can be installed with Windows Installer packages), Microsoft Systems Management Server (SMS), or a similar third-party product
- Providing the client software as a download from a network share point, similar to the deployment of the server software described in "Enabling Administrative Installations" on page 370.

Using the Web Interface

A Web-integrated Presentation Server deployment consists of three components:

- A server farm
- A Web server
- Client devices

When a user logs on to the Web Interface, the Web-based client installation feature checks the user's computer for the presence of ICA or Remote Desktop Connection software. If the necessary client software is not detected, the client installation feature presents the appropriate client software for download and setup.

To use the built-in client installation feature, you must prepare the Web server's \Clients folder that is located in the common files root directory (for example, C:\Program Files\Citrix\Web Interface\4.5\Clients) by making sure that it contains the required client files. For more information about configuring the client software installation feature of the Web Interface, see the *Web Interface Administrator's Guide*.

Using Active Directory

The Citrix Presentation Server Clients for Windows (Program Neighborhood, Program Neighborhood Agent, and Web Client) are available as a single Microsoft Windows Installer package (.msi) file known as the *Client Packager*. You can customize the Client Packager using the built-in customization wizard and then use Active Directory Services (or other third-party software, such as Microsoft Systems Management Server) to distribute and install the client software.

The Client Packager file, Ica32Pkg.msi, is located in the Clients\ica32 folder on the Components CD.

Note The Windows Installer service (Msiexec.exe) is present by default on computers running Windows 2000, Windows XP, Windows Me, or Windows Server 2003.

The Microsoft definition of "publish" is to make an application available to a user for installation through **Add/Remove Programs** or by launching a file associated with the application. If the Windows Installer package is "assigned" to a user whenever the user logs on to a workstation, the Windows Installer service "advertises" the set of applications that are listed in the Active Directory Organizational Unit for that particular user. "Advertising" means that the class IDs, extensions, and shortcuts are installed for the user so that when the user double-clicks a file with an associated extension, or double-clicks the advertised shortcut, the application is fully installed for that user.

Procedures for Publishing the Client Software

The following procedures detail how Active Directory is used to publish (deploy) the Client Packager or separate client software executables.

To deploy the Client Windows Installer package on a computer or set of computers

1. Verify that your client device does not have a client installed.
2. Join an Active Directory domain. This allows you to assign or publish a Windows Installer application for computers and users in that domain or in an Organizational Unit (OU) within the Active Directory domain.
3. On a computer that belongs to the Active Directory domain, launch the Microsoft Management Console (MMC) and load the **Active Directory Users and Computers** snap-in or go to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
4. For this example, create a new OU called *MSI test* and a new user called *MSIuser*. Go to the **Computers** group and find the computer you added to the Active Directory domain. Right-click the computer and select **Move**. Select the MSI Test folder and click **OK**. Follow the same steps to add the new user from the **Users** group to the new OU folder.
5. Right-click the MSI test OU and go to **Properties**. From the **Group Policy** tab, create a new Group Policy Objects link called *Presentation Server Client Install*.
6. Select the Presentation Server Client Install policy and click **Edit**. Under **Computer Configuration > Software Settings > Software Installation**, right-click **Software Installation** and select **New** > **Package**.

7. Browse to a network share containing the Ica32pkg.msi file, select the Windows Installer package, and set the deployment method to **Assigned**. This ensures that all environment settings are present for the Automated Install for the client. Click **OK**. **Software Installation** displays a software package assignment for deployment.

Note If you use a hidden share, for example \\Servername\c$\temp\, users receive a pop-up window asking for the path to Ica32Pkg.msi when they launch Program Neighborhood (after it is deployed to the client devices). The user's client devices must have access to read from the share or Windows cannot deploy the installation.

---

8. Restart the client device. As the client restarts, Active Directory group policy automatically installs the client on the computer. In the Windows **Startup** dialog box, a message appears telling you that the client is being installed by Remote Managed Applications. This message appears before the logon dialog box appears.
9. Log on to the client device and verify that the client is installed.

Important For Windows XP Professional operating systems, the machine has to be restarted twice before the Active Directory Group Policy automatically installs the client on the computer. However, if the Active Directory is based on Windows Server 2003, you can avoid the second restart after creating the policy by going to a command line on the client device and typing **gpupdate /force**. This command prompts you to restart, but it is necessary to restart the Windows XP Professional operating system only once.

To uninstall the Client Windows Installer package from a computer or set of computers

1. On a computer that belongs to the Active Directory domain, launch the MMC and load the **Active Directory Users and Computers** snap-in or go to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the MSI Test OU folder and select **Properties**. From the **Group Policy** tab, **Edit** the Presentation Server Client Install policy. Under **Computer Configuration > Software Settings > Software Installation**, right-click the Presentation Server Client Package and select **All Tasks > Remove**. Ensure that **Immediately Uninstall** is checked, then click **OK**.

3. Restart the client device. As the system restarts, the Active Directory group policy automatically uninstalls the client from the computer. On the Windows Startup dialog status box, a message appears telling you that the client is being removed by Remote Managed Applications. This message appears before the logon dialog box appears.
4. Log on to the client device and verify that the client is completely removed from the client device.

Note Publishing the Program Neighborhood Agent, Program Neighborhood, and the Web Client Windows Installer Packages to users is not supported on Windows 2000 Server or Windows Server 2003. The only available method of using Active Directory to deploy clients to Windows 2000 Server or to Windows Server 2003 is to assign the package to a computer or to a group of computers.

To publish the Client Windows Installer package to a user or group of users in an Active Directory domain

1. On a computer that belongs to the Active Directory domain, launch the MMC and load the **Active Directory Users and Computers** snap-in or go to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. If you did not create a new test OU for previous client installations, create a new OU called *MSI test* and a new user called *MSIuser*.
3. In the Users folder, right-click MSIuser and select **Move**. Select the MSI Test OU folder and click **OK**.
4. Right-click the MSI Test OU and select **Properties**. Go to the **Group Policy** tab, highlight the Presentation Server Client Install policy, and click **Edit**. If you do not already have a Presentation Server Client Install policy from a previous example, create a new Group Policy Objects link named *Presentation Server Client Install*.

5. Under **User Configuration > Software Settings**, right-click **Software Installation** and select **New > Package**. Browse to a network share containing the Ica32pkg.msi file, select the Windows Installer package, and set the deployment method to **Published**. Click **OK**. Software Installation displays a software package assignment for deployment.

Note If you use a hidden share, for example \\Servername\c$\temp\, users receive a pop-up window asking for the path to Ica32Pkg.msi when they launch Program Neighborhood (after it is deployed to the client devices). The user's client devices must have access to read from the share or Windows cannot deploy the installation.

---

6. Close all management screens and restart the client.
7. Log on to the client device as MSIuser.
8. Go to **Add/Remove Programs** and click **Add New Programs**. Verify that the client is included in the list and is ready to be added. Click **Add** and verify that the client is successfully installed.

The Assigned Deployment Method

The client Windows Installer package can also be made available to users using the *assigned deployment* method. If you assign a package to users, only the class IDs, extensions, and shortcuts are installed. When the user double-clicks a file with an .ica extension or double-clicks the shortcut, the client is fully installed for that user.

If you answer **Yes** to the option **Would you like to enable and automatically use your local user name and password for sessions from this client?**, at least one restart is required following the installation of the client.

Using Remote Desktop Web Connection Software

Citrix Presentation Server now provides *basic* support for Remote Desktop Web Connection software. Users can access applications and content you publish through the Web Interface using both Citrix Presentation Server Client and Remote Desktop Web Connection software.

Users do not need Remote Desktop Connection software to be preinstalled on their devices to access published resources through the Web Interface. In a way similar to the Web Client, you can configure the Web Interface to download the Remote Desktop Web Connection software, an ActiveX control for use with Internet Explorer, to client devices.

The infrastructure to support Remote Desktop sessions on Citrix Presentation Server, including the Remote Desktop Web Connection ActiveX control, is installed with Citrix Presentation Server and the Web Interface. Users connecting to Citrix Presentation Server with the Remote Desktop Web Connection ActiveX control draw Citrix licenses from your license entitlement the same way users connecting with client software do.

Use the administrative controls of the Web Interface Console to configure the availability of the Remote Desktop Web Connection ActiveX control to users. Use the standard Citrix Presentation Server management tools to monitor and manage Remote Desktop sessions. For information about configuring the Web Interface, see the *Web Interface Administrator's Guide*.

Client System Requirements. Internet Explorer 5.5 or later. Supported client operating systems: Windows 2000, Windows NT 4.0, Windows Server 2003, Windows XP, Windows XP Media Center Edition, Windows XP Embedded.

Note You cannot route remote desktop sessions through Secure Gateway.

Depending on the authentication method users of the Remote Desktop Web Connection ActiveX control use to authenticate to the Web Interface, they may or may not be prompted for additional authentication when launching published applications. Refer to the following table for information about what authentication users of the Remote Desktop Web Connection ActiveX control must provide to launch applications based on the authentication methods you configure for the Web Interface.

After logging on to the Web Interface using the following authentication method....	**... users of Remote Desktop Connection software can launch applications as follows:**
Guest	Applications you publish for anonymous users: No authentication is required. Applications you publish for explicit users: Not available.
Explicit	Applications you publish for anonymous users: No additional authentication is required. Applications you publish for explicit users: No additional authentication is required.
Desktop Credential Pass-Through	Applications you publish for anonymous users: No additional authentication is required. Applications you publish for explicit users: Users must provide their password.
Smart card	Applications you publish for anonymous users: No additional authentication is required. Applications you publish for explicit users: Users must provide their PIN.

Removing Citrix Presentation Server

To remove a server from a farm, Citrix recommends that you uninstall Citrix Presentation Server. This removes the host information from the farm data store and removes the server from the list of servers displayed in the Presentation Server Console and Access Management Console.

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

Before uninstalling Citrix Presentation Server, log off from any sessions and exit all programs running on the server. For illustration purposes, the following procedure assumes that you have all installation options installed on the server.

To uninstall Citrix Presentation Server

1. Exit any applications running on the server.
2. Choose **Start** > **Control Panel** > **Add/Remove Programs**.
3. Click **Change or Remove Programs**, select Citrix Presentation Server, and click **Change**. Select **Remove** in the Application Maintenance wizard that appears and follow the instructions that appear.
4. Citrix recommends that you uninstall the Citrix Presentation Server and its components in the following order:
   A. Citrix Presentation Server—Presentation Server Reports.
   B. Citrix Access Management Console—Presentation Server Report Center.
   C. All Citrix Access Management Console extensions, as follows:
      - Citrix Access Management Console—Diagnostics
      - Citrix Access Management Console—Hotfix Management
      - Citrix Access Management Console Knowledge Base
      - Citrix Access Management Console Legacy Tools
      - Citrix Access Management Console—Web Interface
   D. Citrix Presentation Server Administration Snap-In.
   E. Citrix License Server Administration.
   F. Citrix Access Management Console Framework.
   G. Presentation Server Console, which is also known as the Management Console for Presentation Server.
   H. Citrix Presentation Server.
   I. Citrix Web Interface.
   J. Citrix Licensing.
   K. Citrix Presentation Server Document Center, if installed.

Note To complete the uninstall, you must restart the computer after you remove Presentation Server.

To force the removal of Citrix Presentation Server

1. If you need to force the removal of Citrix Presentation Server from the system, you can use the command line to add the property:

   CTX_MF_FORCE_SUBSYSTEM_UNINSTALL

   and set its value to "Yes."

2. The following sample command line enables logging of the uninstallation operation and forces the removal of Citrix Presentation Server:

   msiexec /x cps.msi /L*v c:\output.log
   CTX_MF_FORCE_SUBSYSTEM_UNINSTALL=Yes

   where cps.msi is the name and location of the msi package.

Important If you rename a computer running Presentation Server, the new server name is added to the list of servers in the farm. However, you must remove the old server name because it is still listed as a member of the farm. Before you remove the server name, be sure to update all references to the new server name, including data collector ranking, published application references, and license assignments. If you are planning to uninstall Citrix Presentation Server from the Resource Manager metric farm server or database connection server for a summary database, be sure to reassign the server before removing it from the farm. If you are using a summary database, Citrix recommends that you update the database before removing any servers from the farm. Be sure to also create any necessary billing reports from the server before you remove it.

Files that Remain after Uninstalling. When you uninstall Citrix Presentation Server or Citrix Licensing, some files remain on the server. For more details about which files remain, see the *Citrix Presentation Server Readme* and *Citrix Licensing Readme*.

CHAPTER 4

Management Console Overview

Citrix provides two management consoles, the Access Management Console and the Presentation Server Console for performing the necessary administrative tasks for your server farm. This chapter discusses how these consoles are used and how to choose between them.

Management Consoles and Other Tools

Citrix provides a comprehensive set of tools for managing servers, farms, published resources, and connections. This section provides an overview of the features of these consoles and tools. More detailed information is available in the Help for the tools.

Citrix Presentation Server includes two management consoles:

- Citrix Access Management Console
- Citrix Presentation Server Console

These consoles are installed by default when you install Presentation Server, but if you choose not to install them during Presentation Server installation, you can install them from the Citrix Presentation Server CD. Browse the autorun screens to the Management Consoles option. For a summary of which console to use to perform a particular task, see “Choosing Which Console to Use” on page 99.

Both consoles can be used on client devices as well as servers. To manage your deployment more flexibly, you can install the Access Management Console and the Presentation Server Console on a computer that is not running Presentation Server. However, for the best console performance, Citrix recommends running the Access Management Console on a computer running Presentation Server.

For more information about the installation requirements of each of the management tools, see the Installation Checklist for Presentation Server. For instructions about installing management tools, see “Upgrading or Migrating an Existing Server Farm” on page 77.

You can launch all tools by accessing the Citrix program group on the **Start** menu. Some of these tools are also available from the ICA Toolbar.

Citrix Access Management Console. The Access Management Console snaps into the Microsoft Management Console (MMC) and enables you to perform a number of management functions. It also allows you to manage items administered through other Access Suite products, such as the Citrix Access Gateway and Citrix Password Manager.

For Presentation Server, you can use the Access Management Console to set up and monitor servers, server farms, published resources, and sessions. You can create a variety of reports and configure application access (both through the Web Interface and Program Neighborhood Agent).

In addition, you can use the console to troubleshoot alerts, diagnose problems in your farms, view hotfix information for your Citrix products, set up health checks on servers and farms, and track administrative changes made with the console. For more information about using this tool, see "Using the Access Management Console" on page 100.

Citrix Presentation Server Console. Use the Presentation Server Console to connect to any server farm in your deployment and to set up policies and printers. Use the console to configure Network Manager and Resource Manager, and to manage your deployment with Load Manager and Installation Manager. For more information about using this tool, see "Using the Citrix Presentation Server Console" on page 112.

License Management Console. Use this console to manage and track Citrix software licenses. For more information about licensing, see the console's Help and the *Getting Started with Citrix Licensing Guide*.

Citrix SSL Relay Configuration Tool. Use this tool to secure communication between a server running the Web Interface and your farm. For information, see "Deploying Citrix SSL Relay" on page 206.

Shadow Taskbar. Shadowing allows users to view and control other users' sessions remotely. You can use the Shadow Taskbar to shadow sessions and to switch among multiple shadowed sessions. You can also use the Access Management Console to shadow ICA sessions. For more information about shadowing, see "Using Session Shadowing" on page 174.

SpeedScreen Latency Reduction Manager. Use this tool to configure local text echo and other features that improve the user experience on slow networks.

The rest of this section focuses on the Access Management Console and the Presentation Server Console, discussing which tasks can be performed with each.

Choosing Which Console to Use

The Access Management Console and the Presentation Server Console allow you to perform different administrative tasks as listed in the following table and described in more detail later in this chapter.

To do this:	Use this console:
Manage applications and servers, and view zones in multiple farms.	Access Management Console
Manage client sessions and server processes.	Access Management Console
Publish applications to isolation environments.	Access Management Console
Create Citrix administrators and modify their privileges.	Access Management Console
Monitor the performance of servers and server farms.	Access Management Console
Troubleshoot alerts using information in My Knowledge articles.	Access Management Console
Create reports with Report Center.	Access Management Console
Configure access to published applications using Web Interface.	Access Management Console
Create trace logs to assist Citrix Technical Support with problem analysis.	Access Management Console
View hotfix information for your Citrix products.	Access Management Console
Manage zones in a farm.	Presentation Server Console
Create policies for users' connections.	Presentation Server Console
Set up and manage printers.	Presentation Server Console
Create and modify isolation environments.	Presentation Server Console
Manage your server farm using Resource Manager, Installation Manager, Load Manager, and Network Manager.	Presentation Server Console
Create reports with Resource Manager.	Presentation Server Console

Using the Access Management Console

The Access Management Console extends your ability to manage your deployment by integrating many of the administrative features of your Citrix products into the Microsoft Management Console (MMC). The Access Management Console is a standalone snap-in to the MMC. Management functionality is provided through a number of management tools (extension snap-ins) that you can select when you install the Access Management Console or at any time later. For information about adding or removing extension snap-ins, see "Access Management Console. The Access Management Console lets you manage all your Citrix Access Suite components from a single location, which snaps in to the Microsoft Management Console (MMC). For Setup information, see "Stage 4: Installing the Access Management Console" on page 58. For information about usage, see "Using the Access Management Console" on page 100." on page 56.

Users and Accounts

Only Citrix administrators can use the Access Management Console. Depending on the privileges granted to them, administrators have varying levels of access to areas of server farm management. For example, you can specify that administrators can manage sessions running on servers in their own location without being able to view servers in other locations. You should therefore ensure that the appropriate administrator privileges are in place before allowing others to use the console.

Citrix recommends that you use a domain account to run the Access Management Console. You can use your local administrator account, but the user name and password should be the same for all local administrator accounts for all servers in your farms; this is necessary to ensure that access to every server is available when you use Dashboard and Report Center.

Caution Do not run the console in two sessions simultaneously on one computer using the same account. Changes made on the console in one session can overwrite changes made in the other.

Using the Access Management Console Remotely. If you use the Access Management Console to connect to, discover, or manage remote servers, you may receive an error message when you attempt to discover a server in your farm. This occurs when you use an account that does not have Distributed Component Object Model (DCOM) Remote Launch permissions on the remote server. To prevent this error from occurring, you must grant DCOM Remote Launch permissions to any Citrix administrators who you allow to access the farm. You can grant DCOM Remote Launch permissions to administrators on remote servers running Windows Server 2003 Service Pack 1 or Windows XP.

To grant DCOM Remote Launch permissions to administrators

1. On each server in the farm, install Remote COM+ support by following these steps:
   A. Through the Control Panel, go to **Add/Remove Programs > Add/ Remove Windows Components**.
   B. Select **Application Server** and click **Details**.
   C. Select **Enable network COM+ access** and click **OK**.
   D. Click **Next** and follow the prompts to complete the Windows Setup.
2. On each server in the farm, add all users that you will allow to manage the farm remotely to the Distributed COM Users group and give them farm administrator privileges. Alternately, you can create a domain group for this task to centralize management by following these steps:
   A. Create a group named “Citrix Administrators.” To simplify and centralize group administration, Citrix recommends that this be a domain group.
   B. Add the Citrix Administrators group to the built-in Distributed COM Users group on the remote server. This must be performed on all servers that are used to discover farms or that are managed by the console remotely.
   C. Add the Citrix administrator accounts to the Citrix Administrators group.
3. On the remote server, set the DCOM Default Impersonation Level to **Impersonate** by following these steps:
   A. Go to **Administrative Tools > Component Services > Computers**. Then right-click **My Computer** and select **Properties**.
   B. Select the **Default Properties** tab.
   C. From the **Default Impersonation Level** drop-down list, select **Impersonate** and click **OK**.

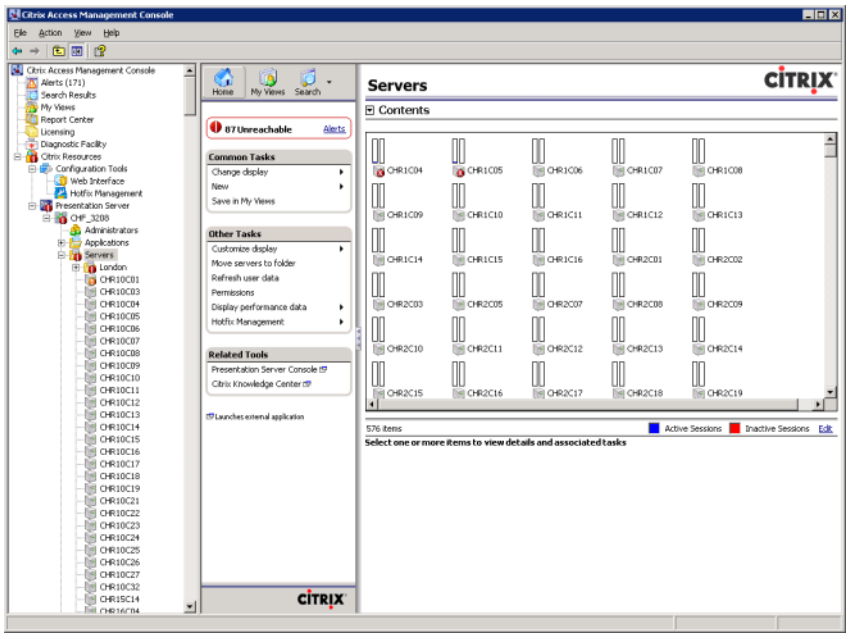
4. Allow access to the Access Management Console and Presentation Server Console through any software or hardware firewalls between the remote servers and the farm. Alternatively, you can disable these firewalls.

The Access Management Console User Interface

The main user interface of the console consists of three panes:

- The *scope pane* contains the console tree.
- The *task pane* in the middle displays administrative tasks and tools. This pane is typically not present in other MMC snap-ins.
- The *details pane* on the right displays items and information associated with the selected node in the console tree.

Typically, you move around in the console as follows. Selecting a node in the left pane updates the items and information that are displayed in the details pane. The **Change display** menu in the task pane allows you to view different items and information associated with the node. To modify or otherwise administer an item, you select it and click a task in the task pane or details pane.



This screen capture shows the layout of the console after running discovery (see "Finding Items in Your Deployment Using Discovery" on page 104). The scope pane on the left contains the console tree. The task pane is in the middle. The details pane is on the right.

The following nodes are available under the top-level node in the console tree:

- **Alerts**. Lists the alerts created by all the items in your deployment. Double-click an alert to drill down to the affected item.
- **Search Results**. Displays the results of any search that you perform. Click **Search** in the task pane to perform a standard or advanced search.
- **My Views**. Allows you to customize the information that you display in the details pane. For instructions about creating My Views, see "Customizing Your Displays Using My Views" on page 105.

In addition, nodes are also created by some Access Management Console snap-ins when they are installed. Some snap-ins are not visible as nodes in the console tree but they add features, such as extra tasks, to other snap-ins. The Access Management Console Framework is another component that performs functions common to all snap-ins. All installed snap-ins require the Framework to be present; the console as a whole cannot function without it.

Depending on your Access Management Console installation, the following snap-ins are available:

- **Report Center**. Allows you to create and schedule reports describing many aspects of your deployment.
- **Licensing**. Launches the License Management Console on your Citrix License Server(s), allowing you to manage your Citrix product licenses. For information about this console, see the *Getting Started with Citrix Licensing Guide.*
- **Diagnostic Facility**. Creates and packages trace logs and other system information to assist Citrix Technical Support in diagnosing problems.
- **Presentation Server**. Allows the console to establish contact with your deployment and lets you manage the applications, servers, and zones in your farms. You also use this snap-in to create Citrix administrators, audit the changes they make with the console, and configure and run health checks on servers. The Presentation Server snap-in is contained in the Citrix Resources node.
- **Dashboard**. Displays alerts and allows you to examine server or farm-wide performance data using monitoring profiles. You can use a variety of built-in performance metrics or customize them from Windows Performance Monitor counters. This snap-in does not appear as a separate node in the console tree but adds alerting and monitoring features to the Presentation Server snap-in.

- **My Knowledge**. Provides context-sensitive troubleshooting information about alerts using knowledge base articles from Citrix and any that your organization creates. This snap-in does not appear as a separate node in the console tree but adds troubleshooting features and some additional alert types to the Presentation Server snap-in.
- **Web Interface**. Allows you to manage how users access applications through the Web Interface and Program Neighborhood Agent sites. Web Interface is located in the Configuration Tools node under Citrix Resources.
- **Hotfix Management**. Manages hotfixes for your Citrix products. Hotfix Management is located in the Configuration Tools node under Citrix Resources.

Starting the Access Management Console

Follow the procedure below to start the Access Management Console.

To start the Access Management Console

Click **Start** > **All Programs** > **Citrix** > **Management Consoles** > **Access Management Console**.

If, when starting the Access Management Console, you are prompted to upgrade, be aware of the restrictions described in "Restrictions When Upgrading the Access Management Console" on page 79.

Important To use the Access Management Console delivered with Presentation Server 4.5 to manage a farm running Presentation Server 4.0 for Windows or Presentation Server 4.0 for Windows 64-bit Edition, you must upgrade at least one server in the farm to Presentation Server 4.5.

Finding Items in Your Deployment Using Discovery

After you start the console but before you can use it to manage the items in your deployment, you must configure and run *discovery.*

Discovery is an important Access Management Console operation that checks for items (such as devices or applications) that were added to or removed from your Citrix environment. Appropriate changes are then made to the console tree.

You discover items using the **Configure and run discovery** task. Choose this task to start the Configure and Run Discovery wizard that allows you to:

- Configure discovery to specify information required to successfully run discovery
- Run discovery to acquire information about selected extensions for use in the console

The first time you open the console, the Configure and Run Discovery wizard runs automatically. At any stage afterwards, run the wizard to locate newly installed products or snap-ins and to update the console if items are added or removed from your deployment.

When using discovery to connect to your Citrix Presentation Server deployment, you must specify the name or IP address of at least one server in each farm that you want to manage. When discovery is complete, the console tree is updated with the items that you specified.

You need to configure discovery only for some products, and the configuration process can vary between products. The **Configure and run discovery** task appears in the task pane only for configurable snap-ins, otherwise the **Run discovery** task is available.

To run the discovery process for more than one product or component

1. In the scope pane, select the Citrix Resources node.
2. Click **Configure and run discovery**.

To run the discovery process for a single product or component

1. In the scope pane, select the snap-in.
2. To configure discovery, click **Configure and run discovery**. To run discovery without any configuration, click **Run discovery**.

Customizing Your Displays Using My Views

You can create custom displays of the details pane called My Views. These are configurable displays that give you quick access to items you need to examine regularly or items in different parts of the console tree that you want to group together. Instead of repeatedly browsing the console tree, you can place the items in a single, easily retrieved display. For example, you can create a My View to monitor your preferred performance data for two sets of servers in different server farms. The performance-related information in a My View is refreshed at regular intervals.

Performing Tasks with the Access Management Console

This section describes in more detail the tasks you can perform with the Access Management Console.

Note In the Enterprise edition of Presentation Server, application streaming tasks can be performed in the Access Management Console. For information about the Application Streaming feature, see the *Citrix Application Streaming Guide*.

Managing Applications, Servers, and Zones in Multiple Farms

Use the Access Management Console to manage the applications, zones, and servers in multiple farms in your enterprise. Farms and their servers are controlled by the Presentation Server snap-in.

View and change details about any farm or its applications, servers, or zones. For example, you can:

- Publish applications
- Copy the properties from one application to another
- Add or remove servers
- Configure server and farm properties

For instructions on managing your applications, servers, zones, and farms, see the *Access Management Console Help*.

Managing Client Sessions and Server Processes

Use the Presentation Server snap-in to manage all user sessions in multiple farms in your enterprise. Alternatively, you can list sessions accessing a specific published application, sessions connecting to a specific server, or view a specific user's sessions and applications.

View details of server processes, including the names of the executable files that generated the processes.

For instructions on managing sessions and processes, see the *Access Management Console Help*.

Publishing Applications to Isolation Environments

Isolation environments protect the operating system from conflicts and other compatibility issues that frequently occur between incompatible or legacy applications. Isolate published applications on a server farm by first creating isolation environments with the Presentation Server Console and then publishing applications to them using the Access Management Console.

The use of isolation environments on farms enables safe installation and execution of your applications. It also mitigates application compatibility issues in a server environment.

For more information about isolating published applications and instructions for creating isolation environments, see the *Access Management Console* and *Presentation Server Console Help* systems.

Creating Citrix Administrators and Modifying Their Privileges

If you log on to the Access Management Console as a full authority administrator, you can make any member of a Windows or Novell Directory Services account authority a Citrix administrator. Citrix administrators are individuals tasked with managing and administrating server farms. You can customize the scope of your Citrix administrators' authority by assigning different tasks to individual administrators or groups of administrators. To do this, you create separate administrator accounts and then apply varying combinations of privileges and permissions to each.

Through the Access Management Console, you can create, modify, and delete Citrix administrator accounts. Using privileges, determine the areas of your Citrix deployment that these administrators can access and control, including the ability to set policies, publish applications, manage printer servers, and manage a selection of servers.

You can create and configure administrator accounts with three different levels of authority—administrators with full, view-only, or custom levels of access to farm management.

Full authority administrators. Full authority administrators can manage all aspects of a server farm. They can, for example, publish applications, manage printers, terminate user sessions, and create other administrator accounts. To create, delete, and configure Citrix administrator accounts, you must log on to the Presentation Server Console as a full authority administrator.

View-only authority administrators. View-only administrators can view all aspects of the server farm; they can, for example, view configuration information and monitor session states, but they cannot modify any settings.

Custom authority administrators. Custom (or *delegated*) administrators can perform select, limited sets of tasks and they have mixed levels of access to areas of farm management or specific tasks within those areas. This type of administrator can have a mixture of view-only access, write access, or no access.

The authority level you grant an administrator depends on the specific business function of the administrator. For example, your system or network administrators may need complete access to all areas of farm management, while help desk personnel may need view-only access to most areas.

A custom administrator account can be designated and configured in three ways:

- When the administrator account is created
- By editing an existing administrator's account properties
- By assigning permissions for a specific object node in the Access Management Console, such as a farm, application, or server

For more information about the permissions that can be assigned to a custom administrator, see Appendix B, "Delegated Administration Tasks."

Note Restricting access to areas of farm management may not prevent administrators from running some command-line utilities available with Citrix Presentation Server.

To create new Citrix administrator accounts

1. In the scope pane of the Access Management Console, select a farm. Then select **Action > New > Add Administrator**.
2. Look up or select the name of the configured user or user group account you want to designate as a Citrix administrator and click **Add**.
3. Enter the email and SMS alert contact details for the account.
4. On the **Privileges** page, select the authority level you want to grant the administrator account from the following options:
    - Select **View Only** to give the administrator view-only access to all areas of farm management
    - Select **Full Administration** to give the administrator full access to all areas of farm management
    - Select **Custom** to delegate specific, limited tasks to the administrator

5. If you selected **Custom** in the previous step, in the **Tasks** pane you must next select the tasks you want to delegate to the custom administrator.

Note To create administrator accounts with full or view-only authority, you select individual or group accounts and associate them with full or view-only *privileges*. Both full and view-only privileges apply farm wide. To create administrator accounts with custom authority, you select individual or group accounts, assign them custom *privileges*, and then *permissions* to perform select tasks.

Monitoring the Performance of Servers

A selection of performance metrics is available for the servers in a farm and the Access Management Console allows you to display these metrics in a highly visual way using Dashboard. For example, you may want to monitor farms located in different areas. In this case, you can use a My View to group each farm's servers on a different part of the screen and then use a background graphic to identify each location. A suitable performance metric, such as CPU Load, displayed in the My View allows you to pinpoint problems quickly on any server at any location.

Using My Views in this way helps you anticipate or identify problems with your servers or applications as soon as possible.

As well as current metrics, you can also view and graph a variety of historical data for your servers.

Important To display performance data using Dashboard, servers must have Resource Manager installed and be running the Citrix Presentation Server Provider.

For instructions about displaying performance data in the Access Management Console, see the console's help. For conceptual information about performance monitoring, see the *Monitoring Server Performance with Citrix Presentation Server Guide*.

Troubleshooting Alerts

You can get context-sensitive information about alerts in the Access Management Console using My Knowledge. Two types of information are available:

- Articles provided by Citrix
- Articles provided by your company

The Citrix articles are provided as a standard component. To provide users with local knowledge, you set up a company knowledge database. After you do this, administrators with the necessary permissions can add, edit, and delete articles.

When you set up a new company knowledge database, My Knowledge automatically creates the required tables and stored procedures in the database. To create these tables and stored procedures yourself, the necessary SQL files are provided in the My Knowledge folder on the Component CD. For instructions about adding troubleshooting information to alerts, see the console's Help.

To see all the alerts that can be generated for a server farm (and that have associated My Knowledge articles), under the Farm node, select **Monitoring Configuration > Farm Configuration** and select the **Available Alerts** display.

For configurable alerts, you can also quickly see the current configuration, which may give you a better understanding of why the alert was raised. If necessary, you can then move directly to reconfigure the alert, disable it, or delete it from your console or all consoles.

Creating Reports

Report Center in the Access Management Console extends the reporting capabilities of Resource Manager in the Presentation Server Console. It allows you to easily generate reports from a variety of real-time and historical data sources. Wizards help you select the type of report, the data to be displayed, and the schedule for running the report. You can view the status of your scheduled reports and adjust the report parameters.

You may need to create reports that describe how various aspects of your server farms are functioning. For example, quarterly data for server uptime, CPU utilization, or application availability are commonly compared with agreed figures in a service level agreement.

Report Center contains several report types that describe:

- Application usage and availability
- Server usage and availability, including CPU and memory utilization reports and a server snapshot report (that can also be created from a real-time metric graph)
- Session statistics over time, including active and disconnected sessions
- Alerts that were generated in the farm
- Distribution of client types that connect to your servers
- Administrative policies in place for the farm
- Administrative changes made using the console

For more detail about each report type, click the Report Center node in the console tree, and then **Report types** in the details pane. For troubleshooting information about report generation, see the console's help.

Configuring Application Access

With Web Interface, you can control how users access published applications and content through a standard Web browser or through Program Neighborhood Agent. You can also enable guest users to attend Conferencing Manager conferences.

For more information about configuring application access and Citrix Conferencing Manager guest attendee logons, see the *Web Interface Administrator's Guide*.

Creating Trace Logs

Diagnostic Facility allows you to gather system data for servers in multiple farms to assist Citrix Technical Support with problem analysis. Select the required servers, click **Diagnose problems > Start trace log**, and follow the on-screen instructions to create a trace log. At the request of Citrix Technical Support, you then select the Diagnostic Facility node and click **Set packaging details** to send the packaged trace log by File Transfer Protocol (FTP).

Viewing Citrix Hotfix Information

With Hotfix Management, you can check which hotfixes are applicable to your Citrix products, search for particular updates on your system, and identify servers where up-to-date hotfixes need to be applied. To use this feature, select **Citrix Resources > Configuration Tools > Hotfix Management**.

Using the Citrix Presentation Server Console

You can use the Presentation Server Console to accomplish the following on any server farm in your deployment:

- Create policies for users' connections
- Set up and manage printers
- Configure zones
- Create isolation environments
- Use Citrix management tools, such as Resource Manager and Installation Manager

You may notice that certain user interface elements are unavailable in the Presentation Server Console. These features and capabilities are now available in the Access Management Console. To compare the tasks that you perform with each console, see "Choosing Which Console to Use" on page 99.

To use the Presentation Server Console, you must be a Citrix administrator. Citrix administrators can have varying levels of access to areas of server farm management. If you try to access an area of the console that you are not authorized to use, the details pane on the right will not display the associated information and it may be blank.

The features and capabilities of the console depend on the Citrix Presentation Server edition you are running. The commands, controls, and features that you see in the console can vary from the descriptions and illustrations in this manual, depending on the components you install.

Load Manager is an optional component that is installed with Citrix Presentation Server Advanced and Enterprise Editions. Resource Manager, Installation Manager, and Network Manager are optional components that are installed with Citrix Presentation Server Enterprise Edition. When these components are installed, additional features and functions are added to the Presentation Server Console. For information about these options, see the administrator's guide for each component.

Citrix Presentation Server Setup installs the Presentation Server Console on each server in the farm by default. You can also use the Citrix Presentation Server CD to install the Presentation Server Console on other workstations you want to use to manage server farms.

Important Earlier versions of the Presentation Server Console do not recognize settings you configure using this version of the Presentation Server Console. If you run the console from devices that do not have Citrix Presentation Server installed, such as workstations or laptops, upgrade those devices to this version of the Presentation Server Console.

Screen reader software may not readily interpret some of the text that appears in the Presentation Server Console. By default, screen readers do not interpret static text areas that appear separate from input elements such as text boxes or check boxes. You can configure the console to be more fully accessible to screen readers. Use the following procedure to configure the console so that you can use the Tab key to move to static text areas you want screen readers to interpret.

To make the Presentation Server Console accessible to screen readers

1. On a computer where the Presentation Server Console is installed, locate and use a text editor to open the Isctx.log file. If you installed the console in the default location, Isctx.log is located in the \Program Files\Citrix\Administration folder.
2. On the second line of Isctx.log, type the following text, including the hyphen:

   -labelsGetFocus:true
3. Save and close the file, then restart the console.

CHAPTER 5

Publishing Resources

With Citrix Presentation Server, you can expand your users' access to information by *publishing* resources on servers. You can publish the following types of resources:

- *Applications* installed on servers running Citrix Presentation Server. When users access them, the published applications appear to be running locally on client devices.
- Data files such as Web pages, documents, media files, spreadsheets, and URLs. In Citrix Presentation Server, the combined total of data types you can publish is referred to as *content*.
- The *server's desktop*, so users can access all of the resources available on the server.

Note Citrix recommends that you not publish server desktops unless they are sufficiently locked down so that users cannot access sensitive areas of the operating system.

You can publish all of these resource types using the Application Publishing wizard in the Access Management Console. To further refine how your users launch and access published resources, you can use content redirection and Citrix Presentation Server policies. This chapter discusses these topics.

In addition to this chapter, Chapter 6, "Advanced Resource Publishing," covers the publishing of resources when further considerations are necessary, such as the use of virtual IP addresses, isolation environments, or providing support for Novell Directory Services (NDS) users. Unless you are already familiar with resource publishing, however, Citrix recommends that you read the following sections before proceeding to Chapter 6.

Using the Application Publishing Wizard

You can use the Application Publishing wizard to publish applications, content, and server desktops. This wizard is located in the Access Management Console and can be accessed in the following ways:

- In the scope pane, select either a farm or an application. Then select **Action > New > Published application**.
- In the scope pane, select a server. Then select **Action > All Tasks** > **Publish application on server**.

Note You do not have to run the Access Management Console from the server on which the applications are to be installed. The server or servers hosting a published application must be a member of the server farm.

When you publish an application, configuration information for the application is stored in the data store for the server farm. The configuration information includes which types of files are associated with the application; users who can connect to the application; and client-side session properties that include window size, number of colors, level of encryption, and audio setting. To users, published applications appear very similar to applications running locally on the client device. The way users start applications depends upon which client they are running on the client device. Consult the appropriate client administrator's guide for more information about the Presentation Server Clients with which your users start published applications.

The following task overview describes how to publish resources from the Application Publishing wizard. Many of the steps are common to all resource types, but other steps are specific to each resource type and these are described here as well.

To publish a resource using the Application Publishing wizard

1. Enter a display name for the application. This is what is displayed for clients when they access the application.

2. Specify the type of resource you want to publish. Three types of resources can be published (*server desktop*, *content*, and *application*) and the next few steps in the wizard differ based on which type you select. If you choose:

   - **Server desktop.** You must next specify the server that you want to publish.
   - **Content.** You must next enter a location (URL or UNC) where the content resides. See "Specifying Locations for Published Content" on page 118 for more information.
   - **Application.** Choose **Accessed from a server** as the application type unless you intend to stream your applications (for more information about this, see the *Citrix Application Streaming Guide*). Then you must enter the location of the executable file for the application and the server on which it will run. You can also decide whether or not to isolate the application. For more information, see "Isolating Published Applications" on page 144.

3. Specify the users who can access the resource. You can allow access to configured user accounts only or to anonymous users. See "Configuring User Access to Published Resources" on page 118 for more information.
4. Specify the appearance and location of the application shortcut provided on the client.
5. The basic settings are now complete and you can publish the resource, or you can continue and specify advanced application settings, which depend on the type of resource you are publishing:

   - **Server desktop.** Configure Advanced Access Control settings, then set application limits, client options, and application appearance.
   - **Content.** Configure Advanced Access Control settings.
   - **Application.** Configure Advanced Access Control, specify file type associations (see "Associating Published Applications with File Types" on page 120 for more information), and then set application limits, client options, and application appearance.

6. Click **Finish** to publish your resource.

Note For instructions about renaming a published application, see the *Access Management Console Help*.

Specifying Locations for Published Content

When you publish content, you can specify the location using a variety of address formats. You can enter any of the following types of information (examples shown in parentheses):

- **HTML Web site address** (http://www.citrix.com)
- **Document file on a Web server** (https://www.citrix.com/press/pressrelease.doc)
- **Directory on an FTP server** (ftp://ftp.citrix.com/code)
- **Document file on an FTP server** (ftp://ftp.citrix.com/code/Readme.txt)
- **UNC file path** (file://myServer/myShare/myFile.asf) or (\\myServer\myShare\myFile.asf)
- **UNC directory path** (file://myServer/myShare) or (\\myServer\myShare)

Important Specifying a UNC directory path does not correctly display the specified directory to users of Netscape Navigator prior to Version 6.0. Earlier versions of Navigator incorrectly interpret the path as relative to the Web server. To publish a directory to such users, consider specifying an FTP directory or listable Web server directory.

Configuring User Access to Published Resources

Before you publish resources, consider how the configuration of your users' accounts can affect their access. You publish resources for specific users and user groups.

The Application Publishing wizard allows you to set up two types of application access: anonymous access and explicit (configured) user account access.

Anonymous Users

During Citrix Presentation Server installation, Setup creates a special user group named *Anonymous*. By default, anonymous users have guest permissions. Publishing applications for this special Anonymous user group lets you completely eliminate the need for user authentication for those applications. When a user starts an application that is configured for anonymous users, the server does not require an explicit user name and password to log the user on to the server and run the application.

Anonymous users are granted minimal session permissions that include the following restrictions:

- Ten-minute idle (no user activity) time-out
- Logoff from broken or timed out connections
- The user cannot change the password (none is required)

When an anonymous user session ends, no user information is retained. The server does not maintain desktop settings, user-specific files, or other resources created or configured for the client.

Note The anonymous user accounts that Citrix Presentation Server creates during installation do not require additional configuration. If you want to modify their properties, you can do so with the standard Windows user account management tools.

Explicit Users

An *explicit user* is any user who is not a member of the Anonymous group. Explicit users have user accounts that you create, configure, and maintain with standard user account management tools.

There are limitations on explicit users who log on to a server farm to run applications: administrators can specify the type of profile, settings, and other configurations for these users.

Important Do not assign any explicit users to the Anonymous group.

Associating Published Applications with File Types

When you publish applications, you can associate the published item with certain file types present in the server's Windows registry. In addition to associating published applications with file types in the Application Publishing wizard, you can also do this from a published application's **Properties** page. By associating published applications with file types and then assigning the applications to users, you automatically implement the following:

- **Content publishing.** Users connecting through the Web Interface or using the Program Neighborhood Agent open content published on servers with applications published on servers. For example, you publish a Microsoft Word document. When you also publish the Microsoft Word application, associate it with a list of file types (files with the .doc extension, for example), and assign it to a group of users, the published content is opened in the Microsoft Word application published on the server.
- **Content redirection from client to server.** Users running the Program Neighborhood Agent open all files of an associated type encountered in locally running applications with applications published on the server. For example, when users double-click email attachments encountered in an application running locally, the attachment opens in an application that is published on the server, associated with the corresponding file type, and assigned to the user.

  For more information about content redirection, see "Managing Resource Launching with Content Redirection" on page 122.

Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

Updating File Type Associations

If you install and then publish applications after installing Citrix Presentation Server, you must update the file type associations in the server's Windows registry. You can verify which file types are associated with a published application on the **Content redirection** tab of the application's Properties page.

To update file type associations

1. In the scope pane of the Access Management Console, select the server where the applications are published.
2. Select **Action** > **All Tasks** > **Update file types from registry**.

Note If you publish applications to be hosted on more than one server, be sure to update the file types on each server.

Passing Parameters to Published Applications

When you associate a published application with file types, the symbols "%*" (percent and star symbols enclosed in double quotation marks) are appended to the end of the application's command line. These symbols act as a placeholder for client-passed parameters.

If a published application does not launch when expected, verify that its command line contains the symbols cited above. If you do not see these symbols in an application's command line, you can add them manually on the **Location** page of the application's Properties page in the Access Management Console.

If the path to the application's executable file includes directory names with spaces (such as "C:\Program Files"), you must enclose the command line for the application in double quotation marks to indicate that the space belongs in the command line. To do this, follow the instructions below for adding quotation marks around the %* symbols and then add a double quotation mark at the beginning and the end of the command line. Be sure to include a space between the closing quotation mark for the command line and the opening quotation mark for the %* symbols.

For example, change the command line for the published application Windows Media Player to the following:

"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"

Managing Resource Launching with Content Redirection

The capability to redirect application and content launching from server to client or client to server is referred to as *content redirection*.

Content redirection allows you to decide whether users access information with applications published on servers or with applications running locally on client devices.

Note For your users to access content published with a specified universal naming convention (UNC) path and through the Web Interface, you must publish and configure an application for content redirection so it is associated with the file type of the published content.

Redirecting Content from Client to Server

When you configure *client to server content redirection*, users running the Program Neighborhood Agent open all files of the associated type with applications published on the server.

Content redirection from client to server is available only for users connecting with the Program Neighborhood Agent. You must use the Web Interface to allow users to connect to published applications with the Program Neighborhood Agent. The Program Neighborhood Agent gets updated properties for published applications from the server running the Web Interface. When you publish an application and associate it with file types, the application's file type association is changed to reference the published application in the client device's Windows registry.

Note Content redirection from client to server is available only with Citrix Presentation Server Advanced or Enterprise editions.

If you have users who run applications such as email programs locally, you can use the content redirection capability in conjunction with the Program Neighborhood Agent to redirect application launching from the client device to the server. When users double-click attachments encountered in an email application running locally, the attachment opens in an application that is published on the server, associated with the corresponding file type, and assigned to the user.

Important You must enable client drive mapping to use this feature.

To configure content redirection from client to server

1. Determine which of your users connect to published applications using the Program Neighborhood Agent.
2. Verify that client drive mapping is enabled. You can enable client drive mapping for the entire server farm, for specific servers, or for specific users with user policies.
3. Publish the application to be shared or the application that corresponds to the published content's file type. For example, if you publish a Microsoft Word document file named "Quarterly_Sales.doc," publish Microsoft Word on a server running Citrix Presentation Server.
4. Associate the appropriate file type with the application.

Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

---

5. Assign the published application to the users you want to use it or else use it to open a published content file.

Redirecting Content from Server to Client

When you enable *server to client content redirection*, embedded URLs are intercepted on the server running Citrix Presentation Server and sent to the client. The user's locally installed browser is used to play the URL. Users cannot disable this feature.

For example, users may frequently access Web and multimedia URLs they encounter when running an email program published on a server. If you do not enable content redirection from server to client, users open these URLs with Web browsers or multimedia players present on servers running Citrix Presentation Server. To free servers from processing these types of requests, you can redirect application launching for supported URLs from the server to the local client device.

Note If the client device fails to connect to a URL, the URL is redirected back to the server.

The following URL types are opened locally on the Presentation Server Clients for Windows and Linux when this type of content redirection is enabled:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft's Media Format)

Note If content redirection from server to client is not working for some of the HTTPS links, verify that the client device has an appropriate certificate installed. If the appropriate certificate is not installed, the HTTP ping from the client device to the URL fails and the URL is redirected back to the server. Content redirection from server to client requires Internet Explorer Version 5.5 with Service Pack 2 on systems running Windows 98 or higher.

Complete the following tasks in the Access Management Console to enable content redirection from server to client and to publish content to be accessed with local applications.

To enable content redirection from server to client

- To enable it for the entire server farm, select the farm in the scope pane. Then select **Action > Modify farm properties > Modify all properties**. Open the **Server default** page from the **Properties** list, select the **Presentation Server** and then **Content Redirection** options and then select the option **Content redirection from server to client**.
- To enable it for a specific server, select the server in the scope pane. Then select **Action > Modify server properties > Modify all properties**. Open the **Presentation Server** page from the **Properties** list, select the **Content Redirection** option and then select the option **Content redirection from server to client**.
- To enable it for specific connections, use the Presentation Server Console and in a policy, enable the rule **User Workspace > Content Redirection > Server to client**. Assign the policy to only those connections for which you want to open supported URL file types on client devices. For more information about policies, see "Using Policies to Configure Access to Published Resources" on page 125.

When you configure Citrix Presentation Server to allow users to open published content with applications running locally on client devices, the client passes the name of the published content file to the local viewer application. The server does not download the file to the client. Instead, the local viewer application accesses the file the same as it would if a user double-clicked the file in Windows Explorer (and a file type association specified the application to use).

For example, when a user opens a published Microsoft Streaming Media file in Program Neighborhood, the Windows Media Player application runs on the client device to play the content. You can publish any content for users to view with a local viewer application.

Accessing published content with local client devices does not use Citrix Presentation Server resources or licenses because local viewer applications do not use ICA sessions to display the published content.

To publish content to be accessed with local applications

1. Publish the content file you want users to access.
2. If you publish the application that corresponds to the content file type, do not associate it with any file types if you want users to open the published content with locally installed applications.

Using Policies to Configure Access to Published Resources

Citrix Presentation Server policies are applied to users or groups of users to determine the nature of their sessions when they access published resources in the server farm. Using policies is an efficient method for controlling connection settings for groups of users, clients, and servers. You can use policies to apply select settings to connections filtered for access type, specific users, client devices, IP addresses, or servers. For example, you can create policies that apply one set of rules to connections from workstations in company headquarters and another set of rules to connections from lender laptops that you provide to a roaming sales force.

Note Policies are applied when users connect to the server farm and remain in effect for the length of the session. Therefore, changes you make to policies do not affect users who are already connected. The changes take effect the next time the users connect.

The process for using policies is:

- Create a policy and assign a name to it.
- Configure rules for the policy.
- Apply the policy to specific user accounts, client devices, or servers.
- Prioritize the policy relative to other existing policies and determine the resultant policy if using multiple policies.

Note In general, policies override similar settings configured for the entire server farm, for specific servers, or on the client. However, the highest encryption setting and the most restrictive shadowing setting always override other settings.

Creating Policies

When creating policies, decide the criteria on which to base them. You may want to create a new policy based on user job function, connection type, client device, or geographic location, or you may want to use the same criteria that you use for Windows Active Directory group policies.

To create a policy

1. In the Presentation Server Console, select the Policies node in the scope pane and choose **Actions > New > Policy** or click the **Create Policy** button on the console toolbar.
2. In the **New Policy** dialog box, enter the name and description of the policy, then click **OK**. Examples of policy names are "Accounting Department" or "Lender Laptops." The policy name appears in the details pane of the Presentation Server Console.

Configuring Policy Rules

Policies contain *rules* that define and configure connection settings to be applied when the policy is enforced. Policy rules have three states: enabled, disabled, or not configured. By default, all rules are not configured. All unconfigured rules are ignored when users log on to the server, so the rules come into play only when their state is enabled or disabled.

If you upgrade/migrate from a previous release of Presentation Server, your existing policies and their rules are maintained and all new rules are not configured. After migrating, you can open the settings for an existing policy and enable new rules and filters that you want to add to the policy. In a server farm that has servers running a previous release of Presentation Server, new filters and rules are ignored by the servers running the earlier releases.

Note Microsoft Group Policy settings can override Citrix Presentation Server policy rules if the Microsoft Group Policy settings are more restrictive. If connection behavior does not match expected results, check your Microsoft Group Policy settings for conflicting configurations.

To configure policy rules

1. You set a policy's rules on the policy's property sheet. Select the policy in the Presentation Server Console and choose **Actions > Properties** to open its property sheet. Some policy rules are organized into folders. Expand the folders to view the rules you can apply.
2. When setting policy rules, determine which settings you want to apply. For any rule you want to add to the policy, select **Enabled** and set rule options in the details pane. For any rule you want to explicitly disallow, select **Disabled**. For more information about policy rules, select the rule in question and then click **Help** or see "Policy Rules" on page 128.
3. Click **OK** when you are done. The policy rule changes go into effect the next time the affected users establish a connection.

Policy Rules

The following tables present rules you can configure within a policy. Policies can contain multiple rules.

Bandwidth

To limit bandwidth used for the following:	Use this policy rule:
Desktop wallpaper	Visual Effects > Turn off desktop wallpaper
Menu and window animations	Visual Effects >Turn off menu animations
Window contents while a window is dragged	Visual Effects >Turn off window contents while dragging
Compression level for image acceleration and image acceleration for dynamic graphics	SpeedScreen > Image acceleration using lossy compression
Client audio mapping	Session Limits > Audio
Devices connected to a local COM port	Session Limits > COM ports
Cut-and-paste using local clipboard	Session Limits > Clipboard
Access in a session to local, client drives	Session Limits > Drives
Printers connected to the client LPT port	Session Limits > LPT Ports
Custom devices connected to the client through OEM virtual channels	Session Limits > OEM Virtual Channels
Client session	Session Limits > Overall Session
Printing	Session Limits > Printer
TWAIN device (such as a camera or scanner)	Session Limits > TWAIN Redirection

Client Devices

Control whether or not to allow audio input from client microphones	Resources > Audio > Microphones
Control client audio quality	Resources > Audio > Sound quality
Control audio mapping to client speakers	Resources > Audio > Turn off speakers
Control whether or not client drives are connected when users log on to the server	Resources > Drives > Connection
Control how drives map from the client device	Resources > Drives > Mappings
Improve the speed of writing and copying files to a client disk over a WAN	Resources > Drives > Optimize > Asynchronous writes

Prevent client devices attached to local COM ports from being available in a session	Resources > Ports > Turn off COM ports
Prevent client printers attached to local LPT ports from being made available in a session	Resources > Ports > Turn off LPT ports
Allow use of USB-tethered, Windows CE-based, PDA devices	Resources > PDA Devices > Turn on automatic virtual COM port mapping
Configure resources for the use of TWAIN devices, such as scanners and cameras	Resources > Other > Configure TWAIN redirection
Prevent cut-and-paste data transfer between the server and the local clipboard	Resources > Other > Turn off clipboard mapping
Prevent use of custom devices, such as an electronic pen (stylus)	Resources > Other > Turn off OEM virtual channels
Turn off auto client update	Maintenance > Turn off auto client update

Printing

Control creation of client printers on the client device	Client Printers > Auto-creation
Allow use of legacy printer names and preserve backwards compatibility with prior versions of the server	Client Printers > Legacy client printers
Control the location where printer properties are stored	Client Printers > Printer properties retention
Control whether print requests are processed by the client or the server	Client Printers > Print job routing
Prevent users from using printers connected to their client devices	Client Printers > Turn off client printer mapping
Control installation of native Windows drivers when automatically creating client and network printers	Drivers > Native printer driver auto-install
Control when to use the universal print driver	Drivers > Universal driver
Choose a printer based on a roaming user's session information	Session printers

User Workspace

Limit the number of sessions that a user can run at the same time	Connections > Limit total concurrent sessions
Direct connections to preferred zones and failover to backup zones	Connections > Zone preference and failover
Control whether or not to use content redirection from the server to the client device	Content Redirection > Server to client
Control whether or not shadowing is allowed	Shadowing > Configuration
Allow or deny permission for users to shadow connections	Shadowing > Permissions
Use the server's time zone instead of the client's estimated local time zone	Time Zones > Do not estimate local time for legacy clients
Use the server's time zone instead of the client's time zone	Time Zones > Do not use Clients' local time
Identify which credential repository to use when using Citrix Password Manager	Citrix Password Manager > Central Credential Store
Prevent use of Citrix Password Manager	Citrix Password Manager > Do not use Citrix Password Manager
Override the delivery protocol for applications streamed to client	Streamed Applications > Configure delivery protocol Note: This rule appears only in the Enterprise Edition of Citrix Presentation Server.

Security

Require that connections use a specified encryption level	Encryption > SecureICA encryption

Applying Policies with Filters

By default, newly created policies are not applied to any sessions. Before a policy has an effect, you must create a filter for it so the server can apply it to matching sessions. You can filter sessions and apply a policy to them based on a combination of the following criteria:

- Access control through which a client is connecting to a session
- IP address of a client device connecting to a session
- Name of a client device connecting to a session
- Users or user groups associated with a session
- Server hosting a session

To apply a policy

1. In the scope pane of the Presentation Server Console, choose the Policies node.
2. From the **Contents** tab, choose the policy you want to apply.
3. From the **Actions** menu, choose **Policy > Apply this policy to**.
4. Use the **Policy Filters** dialog box to configure filters to apply the policy to a session based on access control, client IP address, client name, server the session connects to, or the user who is making the connection.
5. If a filter has an **Allow/Deny** setting, you must select **Allow** to enforce the policy.
6. Click **OK** when you are finished applying the policy filters.

Note The name of a client device is a string value that can be manually configured on the client host. Because of this, in cases where the client should not be permitted to influence the policy filtering, it may not be appropriate to make use of the client device name.

Using Multiple Policies

You can use multiple policies to tailor Citrix Presentation Server to meet users' needs based on their job functions, geographic locations, or connection types. For example, for security reasons you may need to place restrictions on user groups who regularly work with highly sensitive data. You can create a policy that requires a high level of encryption for client sessions and prevents users from saving the sensitive files on their local client drives. However, if some of the people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you need to determine how to prioritize them, how to create exceptions, and how to view the resultant policy when policies conflict.

Prioritizing Policies and Creating Exceptions

Prioritizing policies allows you to determine which policies take precedence over one another when they contain conflicting rules. When a user logs on, all policies that match the filters for the connection are identified. Presentation Server sorts the identified policies into priority order and compares multiple instances of any rule, applying the rule according to the priority ranking. If the rule appears in a policy ranked highest, those rule settings override the settings for the same rule in a policy ranked lower.

You prioritize policies by ranking their priority number. By default, new policies are given the lowest priority. In cases of conflicting policy settings, a policy with a higher priority (a priority number of "1" is the highest) overrides a policy with a lower priority. Rules are merged according to priority and the rule's condition; for example, whether the rule is disabled, enabled, or not configured. Any rule configured as "disabled" wins over a lower-ranked rule that is enabled. Policy rules that are not configured are ignored and will not override the settings of lower-ranked rules.

When you create policies for groups of users, clients, or servers, you may find that some members of the group require exceptions to some policy rules. To more effectively manage exceptions, you can create new policies for only those group members needing the exceptions, and then rank that policy higher than the policy for the entire group.

The following example demonstrates the prioritization of multiple policies and the creation of exceptions. Assume that you created a policy for your "Accounting" user group. One of the rules enabled in this policy prevents the user group from saving data to their local drives. However, two users who are members of the Accounting group travel to remote offices to perform audits and need to save data to their local drives. The following procedure describes creating a new policy for Accounting group members Carol and Martin that allows them access to their local drives while allowing the other policy rules to work the same way for them as for all other members of the Accounting group.

To create exceptions and prioritize policies

1. Determine which users need additional policies to create exceptions.

   The policy named "Accounting Profile" that is assigned to the Accounting group includes a rule that prevents access to local drives. Carol and Martin, members of the Accounting group, need access to their local drives.

2. Determine which rule or rules you do not want to apply to these users.

   You want most of the rules in this policy to apply at all times to all users, with the exception of the rule that prevents access to local drives.

3. Create a new policy and name it "Accounting Profile - local drive access."

4. Edit the description of the policy by selecting the policy and choosing **Actions > Policy > Edit Description**. Open the policy's property sheet and locate the rule you do not want to apply to Carol and Martin. Set the rule's state to **Disabled**.

5. To assign users Carol and Martin to the policy, select it and choose **Actions > Policy > Apply this policy to**. In the **Policy Filters** dialog box, select **Users** and make sure the **Filter based on users** check box is selected. Open domains or user groups in the **Look in** box until the user accounts for Carol and Martin appear and add them to the **Configured Accounts** box. Select the **Show users** option to display individual user accounts. Click **OK** when you are finished adding users.

6. Rank the "Accounting Profile - local drive access" policy higher than the "Accounting Profile" policy. By default, new policies are given the lowest rank (which corresponds to the highest priority number). Right-click the "Accounting Profile - local drive access" policy and select **Priority** > **Increase Priority** until this policy's priority number is lower than the "Accounting Profile" policy. A policy with a priority number of 1 has the highest priority.

Determining a Resultant Policy

To determine the *resultant policy*, the effective rule settings when more than one policy applies to a session, use **Search**. The search function calculates the final rule settings for any combination of a user, group, IP address, and so on after the rules' priorities are taken into account.

You can use the search function to list policies that apply to a connection based on:

- Whether or not the connection is made through Advanced Access Control
- The IP address of the client device making the connection
- The name of the client device making the connection
- The user or group membership of the user making the connection
- The server to which the connection is being made

To determine a resultant policy

1. In the Presentation Server Console, click **Actions > Search**.
2. Make sure that **Policies** is the selected entry in the **Search for** list. Search finds all policies that apply to the combination of access control, IP address, client name, user, and server criteria you set in the **Search** dialog box.
3. Select one or more search filters in turn and click **Edit** to specify search criteria for each filter.
4. Click **Search**.
5. Use the **View Resultant Policy** function after a policy search to calculate the results of multiple policies that can affect a connection. Citrix Presentation Server merges all policies that can affect a connection when enforcing policies. When there are multiple policies that can apply to a connection, it is the resultant policy that Citrix Presentation Server enforces.

CHAPTER 6

Advanced Resource Publishing

This chapter discusses *advanced* resource publishing. The fundamental considerations and procedures involved with publishing applications, content, and server desktops are covered in the previous chapter; Chapter 5, "Publishing Resources." If your Presentation Server deployment presents additional challenges, however, such as the need to isolate applications or provide applications with virtual IP addresses, the options, considerations, and procedures for doing these things are described in this chapter.

Note If you determine that your server farm needs to stream applications, see the *Citrix Application Streaming Guide* for more information.

Using Virtual IP Addresses with Published Applications

Some applications, such as CRM and CTI, use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, which, because the port is already in use, causes the failure of multiple attempts to launch an application in a multiuser environment. For such applications to function correctly in a Presentation Server environment, a unique IP address is required for each device.

With the virtual IP address feature, you can assign a static range of IP addresses to a server and have these addresses individually allocated to each session so that configured applications running within that session appear to have a unique address. Also, you can configure applications that depend on communication with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

An application requires a virtual IP address if it:

- Uses Windows sockets
- Requires a unique IP address or uses a specified TCP port number

An application requires a virtual loopback address if it:

- Uses the Windows socket loopback (localhost) address 127.0.0.1
- Uses a specified TCP port number

If the application requires an IP address for identification purposes only, configure your server to use the client IP address. For instructions, see "Providing the Client IP Address to an Application" on page 139.

How Virtual IP Addressing Works

The virtual IP Address feature works as follows:

- During IMA startup, the virtual IP *address assigner* binds the assigned IP addresses to the NIC that matches the same subnet as the virtual addresses.
- When the virtual IP feature is enabled on a specific server, the virtual IP *address allocator* allocates all new sessions connecting to the server an address from the pool of available addresses that were assigned by the virtual IP address assigner.
- Each new session is allocated an address that is removed from the pool of available addresses. When the session logs off, the allocated address is returned to the available address pool.
- After an address is allocated to a session, it uses the allocated virtual address rather than the system's primary IP address whenever the following calls are made:

  `Bind¸closesocket¸connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyname, gethostbyaddr, getnameinfo, getaddrinfo`

Note All processes that require this feature must be added to the Virtual IP Process list. Child processes do not automatically inherit this functionality. Processes can be configured with full paths or just the executable name. For security reasons, Citrix recommends that you use full paths.

Virtual Loopback

When enabled, the Virtual Loopback function does not require any additional configuration other than specifying which processes use the feature. When an application uses the localhost address (127.0.0.1) in a Winsock call, the Virtual Loopback feature simply replaces 127.0.0.1 with 127.X.X.X where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0) to the maximum of 127.255.255.255.

Virtual Loopback enables multiple published applications that depend on the localhost interface for interprocess communication to function correctly within the session. One example of such an application is Microsoft ActiveSync. To provide the PDA synchronization feature, Presentation Server automatically uses the virtual IP address feature to create Terminal Server compatibility for ActiveSync.

Binding Applications

Applications are bound to specific IP addresses by inserting a “filter” component between the application and Winsock function calls. The application then sees only the IP address it is supposed to use. Any attempt by the application to listen for TCP or UDP communications is automatically bound to its allocated virtual IP address (or loopback address), and any originating connections opened by the application are originated from the IP address bound to the application.

In functions that return an address such as gethostbyname() and GetAddrInfo(), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the session’s virtual IP address. Applications that try to get the local server’s IP address through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls (such as bind or connect).

Often an application requests to bind to a port for listening on the address “0.0.0.0.” When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these types of calls and changes the call to listen on the specific virtual IP address. This enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. Note this is changed only if it’s in an ICA session and the virtual IP address feature is turned on. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port, say 9000, they are bound to *VIPAddress1:9000* and *VIPAddress2:9000*, and there is no conflict.

Assigning IP Address Ranges

Before enabling the virtual IP address feature, configure ranges of IP addresses that are excluded from any DHCP servers or otherwise duplicated. These ranges must share the same subnets as the assigned IP addresses of the computers running Presentation Server that are configured for virtual IP, because there is no routing mechanism in place to traverse subnets.

The pool of IP addresses assigned to the server farm must be large enough to include all concurrent user sessions on every server that is configured, not just the sessions running the applications requiring virtual IP address functionality. The servers that require virtual IP address functionality that share the same subnet as the address range should be added to the range. The addresses in the range are distributed equally (by default) among the selected servers and assigned. You can then change the number of addresses assigned to each server. Citrix recommends that you configure a Load Management Server User Load rule that is equal to or fewer than the total number of addresses assigned to the server.

You can assign a specific address range to each computer or group of computers running Presentation Server. This may be a viable option within environments where the servers span subnets or where insufficient IP addresses exist within the current subnet.

Configuring Virtual IP for Applications

The following procedure explains how to view applications that bind to specific IP addresses and ports and configure the processes of these applications to use virtual IP addresses.

To configure an application to use virtual IP addresses

1. Obtain the TCPView tool from Sysinternals (http://www.sysinternals.com). This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and, using TCPView, note which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the server's IP address, 0.0.0.0, or 127.0.0.1 to use the virtual IP address feature.
5. Launch an additional instance of the application to ensure that it does not open the same IP address on a different port.

Using the Client IP Address Feature

If an application fails because it requires a unique address strictly for identification or licensing purposes, and the application does not require a virtual address for communication, you can use the Client IP Address feature. This feature hooks only calls that return a host IP address, such as gethostbyname(). Only use this feature with applications that send the value in this type of call to the server application for identification or licensing.

If you deploy this feature, consider the IP addresses used by each client device. For example, if two remote users use the same IP address, a conflict will arise due to the duplicate address.

When these values are configured, configure either the Virtual IP Processes or Virtual Loopback Processes with the same process names. This function creates and manages the following registry entry, which is still required for the Client IP feature to work:
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\VIPHook*Processname*

Note The virtual IP Address feature functions only with applications that load the user32.dll system dynamic link library.

Providing the Client IP Address to an Application

For identification purposes, some applications require the IP address be unique for a session. Such IP addresses are not needed for binding or addressing purposes. In such a case you can configure the session to use the IP address of the client.

To supply client IP addresses to published applications on a server

1. On the server on which the applications reside, start regedit.

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

---

2. Using regedit, create the following two registry entries:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP\

     Name: UseClientIP

     Type: REG_DWORD

     Data: 1 (enable) or 0 (disable, which is the default)

   - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP\

     Name: HookProcessesClientIP

     Type: REG_MULTI_SZ

     Data: multiple executable names representing application processes that use client IP addresses

3. Close regedit and restart your server.

4. After making the prescribed registry modifications, add the application process. For instructions, see "Enabling Application Processes to Use Virtual IP or Virtual Loopback" on page 142.

   Do not configure the use of client IP addresses if:

   - Clients connect using network protocols other than TCP/IP
   - Clients reconnect to disconnected sessions from different client devices
   - Sessions use a pass-through client

Providing Virtual IP Address Ranges to Sessions

Using virtual IP addresses, you can provide published applications with unique IP addresses for use in sessions. This is especially important for Computer Telephony Integration (CTI) applications that are widely used in call centers.

Users of these applications can access them on a server running Citrix Presentation Server in the same fashion that they access any other published application.

To assign virtual IP address ranges, you must have a reserved range of static IP addresses that you can assign to the server. Work with your network administrator to obtain a list of free addresses that are not part of your DHCP pool. Ensure that you do not include broadcast addresses.

Before assigning virtual IP address ranges, determine the maximum number of users you may have connecting concurrently to the server. Because every session connecting to the server is assigned an IP address (not just sessions launching the application that requires virtual IP addresses), assign at least as many static IP addresses to the server as the maximum number of users who may be connecting concurrently to that server.

Note In the event more sessions are launched on a server than IP addresses are available, the server displays the error message: *No virtual IP address is available for this session, please contact your administrator.* The inability of the server to assign a virtual IP address to a session does not prevent the user from launching an application that requires a virtual IP address within the session; however, the application may not function correctly.

To make virtual IP addresses available to applications running in sessions

1. At the farm level, configure virtual IP address ranges and assign them to servers.
2. Enable applications for use with virtual IP addresses.

In addition to configuring virtual IP address ranges and enabling applications for use with virtual IP addresses, you can also control and monitor virtual IP addresses available from each server. The sections that follow describe how to perform each of these tasks.

To configure virtual IP address ranges

1. In the scope pane of the Access Management Console, select a farm. Then select **Action** > **Modify farm properties > Modify Virtual IP properties**.
2. Open the **Address Configuration** page from the **Virtual IP** page in the farm's **Properties** list.
3. Use the **Address Configuration** dialog box to configure the virtual IP address ranges and assign them to servers.
4. Click **OK** and restart all affected servers.

After configuring virtual IP address ranges, continue by specifying the application processes that are enabled to use virtual IP addresses. For more information, see "Enabling Application Processes to Use Virtual IP or Virtual Loopback" on page 142.

Providing Virtual Loopback Addresses

Using virtual loopback, you can provide published applications with loopback addresses to use in sessions.

To make a virtual loopback address available to applications running in sessions

1. At the farm level, enable virtual loopback on servers by following the procedure below.
2. Enable application processes to use virtual loopback by following the procedure in the "Enabling Application Processes to Use Virtual IP or Virtual Loopback" section.

After you configure virtual loopback on your servers, you can control and monitor this feature at the server level. For information, see "Monitoring Virtual Loopback and IP Addresses" on page 143.

To enable virtual loopback on servers in a farm

1. In the scope pane, select a farm. Then select **Action > Modify farm properties > Modify Virtual IP properties**.
2. Open the **Loopback Configuration** page from the **Virtual IP** page in the farm's **Properties** list.
3. Use the **Loopback Configuration** dialog box to select the servers for which you want to make virtual loopback available. This automatically enables virtual loopback on the selected servers.

After configuring virtual IP loopback on your servers, continue by specifying the application processes on each server for which you want virtual loopback available. The next section describes how to enable applications for virtual loopback use.

Enabling Application Processes to Use Virtual IP or Virtual Loopback

After you configure virtual IP addresses or virtual loopback for a farm on the **Farm Properties** page, continue by specifying the application processes that can use the virtual IP addresses or virtual loopback.

To specify the process names

1. In the scope pane of the Access Management Console, select a farm. Then select **Action > Modify farm properties > Modify Virtual IP properties**.

2. Open the **Process Configuration** page from the **Virtual IP** page in the farm's **Properties** list.
3. In the **Processes Configuration** dialog box, use the **Add Process**, **Edit Process**, and **Delete Process** buttons to control lists of processes to which the server provides virtual IP and loopback addresses.

   When adding files to the lists, select the executable files associated with the applications you want to enable to use virtual IP and virtual loopback.

Depending on the list to which you add a process, the next time the process starts in a session, it uses a virtual IP address or virtual loopback.

Monitoring Virtual Loopback and IP Addresses

After you configure virtual IP address ranges or virtual loopback at the farm level, you can use virtual IP configuration settings at the server level to:

- Enable and disable the use of virtual IP addresses and virtual loopback on a server
- View the IP address ranges available on a server
- Control logging of the assignment and release of virtual IP addresses

To configure virtual IP addresses and virtual loopback on an individual server

1. In the scope pane of the Access Management Console, select a server. Then select **Action > Modify server properties > Modify all properties**.
2. Select the **Virtual IP** page in the server's **Properties** list.
3. Use the **Virtual IP** page to:
   - Disable and enable the use of virtual IP addresses on the server. (Virtual IP addresses are enabled by default when you assign an address range to a server.)
   - Enable and disable virtual loopback availability from the server. (By default, virtual loopback is enabled on each server when you enable virtual loopback for the farm.)
   - Control logging of assignment and release of virtual IP addresses.

Isolating Published Applications

Enterprise applications published using Citrix Presentation Server often share specific operating system resources. Such sharing enables efficient use of limited system resources. However, sharing of system resources also introduces interdependencies between applications which, in turn, introduce compatibility issues in a multiuser environment. For example, a simple software patch applied to a particular application could affect another that depends on a shared component. The two applications could subsequently begin to misbehave or fail.

Note Typical candidates for application isolation are legacy applications not designed for use with Terminal Server, applications that exhibit compatibility issues in a multiuser environment, or any applications that cannot coexist on a single server. Applications that install Windows services or drivers will not function correctly and, thus, are not candidates for isolation environments.

The isolation environment protects the operating system and applications from conflicts and other complications that frequently occur between incompatible or legacy applications. The isolation environment creates an environment or user-specific copy of the system resources modified by the published application during installation or runtime. This allows the application to function without affecting the rest of the system.

The isolation environment also provides a virtual mapping from an application to operating system resources. The mapping is accomplished through the use of rules that specify how an application behaves within an isolation environment.

The basic steps for isolating an application are as follows:

- Through testing, identify applications that malfunction when run within Citrix Presentation Server or Terminal Services.
- Ensure isolation environments are enabled for the farm. (By default isolation environments are enabled at the farm level.)
- Create isolation environments.
- Configure the properties of the isolation environment.
- Isolate the published application.

Enabling and Disabling Isolation Environments

Isolation environments are enabled by default. You can disable, enable, and configure isolation environments in the Access Management Console.

To enable or disable isolation environments for a farm

1. In the scope pane of the Access Management Console, select a farm. Then select **Action > Modify farm properties > Modify all properties**.
2. Select the **Server Default > Isolation Environment** page in the farm's **Properties** list.
3. Use the **Application isolation** check box to enable and disable isolation environments for the farm.

You can also use the **Farm-wide > Isolation Environment** page to change the location of where application and user data are stored on the server. For more information, see the *Access Management Console Help*.

By default, when you enable isolation environments for a farm, you enable isolation environments on all of the servers in the farm. You can disable or enable isolation environments on an individual server.

To enable or disable isolation environments on a server

1. In the scope pane of the Access Management Console, select a farm. Then select **Action > Modify server properties > Modify all properties**.
2. Select the **Isolation Environment** page in the server's **Properties** list
3. Clear the **Use farm settings** check box and use the **Application isolation** check box to enable and disable isolation environments for the farm.

Note You set isolation settings only at the farm level. To change isolation settings when isolation environments are enabled on individual servers, but not for the farm, temporarily enable isolation environments at the farm level.

Creating an Isolation Environment

Creating isolation environments on farms enables safe installation and execution of applications. It also mitigates application compatibility issues in a server environment. You create isolation environments in the Presentation Server Console.

By default, isolation environments on the farm are enabled, and this farm setting is applied to all servers in the farm. Through the Access Management Console, you can view or change this setting for the farm or for an individual server, as needed. For more information, see "Enabling and Disabling Isolation Environments" on page 145.

To create isolation environments for the farm

1. In the left pane of the Presentation Server Console, select the Isolation Environments node.
2. From the **Actions** menu, select **New > Isolation environment**.
3. Enter a name for the new isolation environment and click **OK**.

The new isolation environment appears in the Contents pane for the Isolation Environments node.

After creating the isolation environment, you have the option of configuring each isolation environment through its properties.

Configuring an Isolation Environment

The default settings of an isolation environment are designed to resolve most compatibility issues; however, you can refine and optimize isolation environment settings as required.When you opt to configure an isolation environment, you decide the following properties:

Applications. Specifies applications associated with and installed into the isolation environment and isolated applications that are published. You can also specify other applications published on the server farm that are associated with this isolation environment.

Roots. Specifies the virtual directories and registry locations in which files modified by users (user profile root) and applications (installation root) reside.

Rules. Specifies whether or not isolation, redirection, or ignore rules are to be applied to system resources, such as files, registry, and named objects. Citrix recommends that you do not modify the defined rules.

Security. Specifies the type of security policy, such as enhanced or relaxed, to apply to this isolation environment. Selecting enhanced security prevents execution of files located in the user profile root.

To configure the properties of an isolation environment

1. In the left pane of the Presentation Server Console, select **Isolation Environments**.

2. From the **Contents** tab, select the isolation environment to configure.
3. On the **Actions** menu, click **Properties**. Use the **Properties** page to configure roots, rules, and security settings for the isolation environment. For specific information about each **Properties** page, click **Help**.
4. To save your settings, click **OK**.

Using an Isolation Environment

After creating and enabling isolation environments, you can isolate an application by:

- Associating the published application with an isolation environment
- Installing an application into an isolation environment

You cannot delete an isolation environment until the applications are deleted from it. When you delete an isolation environment, the applications associated with it or installed into that isolation environment still exist but are no longer isolated.

Associating an Application with an Isolation Environment

When you associate a published application with an isolation environment, the isolation environment manages all the interactions of the published application with system resources. The isolation environment forces the application to launch in the isolation environment and access a virtualized version of system resources. This prevents direct access of key system resources by the application, which in turn prevents the occurrence of application conflicts and incompatibilities.

Associate an application with the isolation environment when you publish the application on a server in the farm.

To associate a published application with an isolation environment

1. In the scope pane of the Access Management Console, select the Applications node.
2. Select **Action > New > Published application**.
3. Use the application publishing wizard to publish the application. On the **Location** page, select the **Isolate application** check box and click the **Settings** button to select the isolation environment to use.
4. Complete the wizard by specifying the other properties for the published and isolated application. For more information, see the *Access Management Console Help*.

Installing an Application into an Isolation Environment

You install an application into an isolation environment to keep all operations of an application completely separate from other applications on the server. Application shortcuts, registry settings, paths, and configuration files reside within the confines of the isolation environment.

If an application prevents other applications from running, uninstall the application from the server, and reinstall it into the isolation environment. Installing applications in an isolation environment and then publishing them can correct problems not corrected by associating the application with an isolation environment.

You can install applications into isolation environments through Installation Manager or by using the aiesetup command from a command prompt. For information about using Installation Manager to deploy applications, see the *Installation Manager Administrator's Guide*.

Note Citrix does not support installing an application into an isolation environment through a connection made with Remote Desktop Connection.

To use aiesetup to install an application into an isolation environment

1. Ensure the application is not already installed on the server. If it is, uninstall the application.
2. Designate and configure the isolation environment that you plan to use.
3. Use the command aiesetup to install the application in an isolation environment of your farm. Install the application only after you determine that it is incompatible with Terminal Server.

   For more information about how to use the aiesetup command, see "AIESETUP" on page 289.
4. On the server, use the application publishing wizard in the Access Management Console and on the **Location** page, complete the following settings:

   A. Check the **Isolate application** check box (disabled by default) and click **Settings**.

   B. In the **Isolation Settings** dialog box, from the list of available isolation environments, select the isolation environment into which you installed the application.

C. Click the **Application was installed into the isolation environment** check box (disabled by default).

D. Select the application from the **Choose installed application** list.

E. If applicable, enter application parameters in the **Command line arguments** field.

5. Click **OK**, and continue with the steps in the wizard to publish the application.

For more information about how to publish an application, see "Using the Application Publishing Wizard" on page 116.

Isolation Environment Rules

In the Presentation Server Console you can use isolation environments to control application compatibility and accessibility. Isolation environments are constructed by defining a set of rules that specify how an application behaves within its confines. The default rules for isolation environments are adequate for most environments. However, the rules engine is powerful and flexible, and you can use it to create and alter rules, as needed, to exert control over application interactions with operating system resources. The following sections describe the general types of rules you can create, best practice information for such rules, and how they are prioritized.

Isolation Rules

When you create a new isolation environment, its default behavior is to isolate everything with a few exceptions. When an application requests access to a system resource (such as a file, registry, or named object), a per-user version of the file or key is created as required. This default behavior mitigates most application conflicts and allows applications to run correctly.

Isolation rules ensure that per user and per application level versions of files and keys are created. This is the primary method used to isolate applications from each other.

- **Isolation per user** creates an individual copy of each resource that a particular user accesses
- **Isolation per isolation environment** creates a single copy of a resource for a particular isolation environment

You can add one of these rules to ensure that there is one copy of a resource per isolation environment. For example, you can create a rule that isolates the registry hive, HKEY_LOCAL_MACHINE\SOFTWARE\classes, when you install Microsoft Office. Because each user does not require a separate version of this hive, you can create a rule that isolates this particular registry hive for the isolation environment.

Ignore Rules

You can use the rules engine to define holes in the isolation environment so that an application can write to the underlying system. Such rules are called *Ignore* rules.

There are instances when an application inside an isolation environment needs to share data with an application outside the isolation environment. For example, in a scenario where users can print to network printers available within an ICA session, these printers are automatically created when the user connects to a published application. If the published application is running within an isolation environment, called *My_AIE*, which has an isolation rule applied to it, auto-creation of network printers fails because a copy of the registry hive HKEY_CURRENT_USER\Printers is created for each user. You can ensure printer auto-creation occurs by creating a rule for *My_AIE* that ignores the registry hive HKEY_CURRENT_USER\Printers.

Redirect Rules

A "Redirect" rule redirects an application request for a file or registry key to a specified location. For example, if an application creates the file, c:\temp\data.txt, regardless of the user, you can redirect those files to c:\aietemp\%USERNAME%.

For example, if UserA runs the application in an isolation environment, c:\temp\data.txt is created in c:\aietemp\UserA\data.txt.

In this example, the administrator may choose to clean up the \temp directory each time the system starts up. By redirecting all access of **c:\temp** directory to **c:\aietemp** on a per-user basis, the administrator can clean up the temporary data easily at startup.

Prioritization of Rules

A rule for an isolation environment is based on a specific location: either a file path or a registry key path.

Rules are matched by the most specific path to the resource being accessed. A rule applies to the object (file, registry or named object) specified and **all** the children of the specified object, unless a more specific rule exists.

For instance, if you create the following rules:

- An “Ignore” rule for the file path, C:\Documents and Settings\%USERNAME%.

  Every file and directory created under C:\Documents and Settings\%USERNAME% is created in the system location because you specified, through the “Ignore” rule, that this directory location is not isolated. If an application opens the file C:\Documents and Settings\%USERNAME%\ ApplicationData\CompanyA\foo.txt, the “Ignore” rule for C:\Documents and Settings\%USERNAME% applies.

- A “per user isolation” rule for C:\Documents and Settings\%USERNAME%\Windows because you want to isolate the per user Windows directory, C:\Documents and Settings\%USERNAME%\Windows. If an application opens C:\Documents and Settings\%USERNAME%\Windows\Win.ini, the “isolate per user” rule for C:\Documents and Settings\Windows applies.

Removing Applications Installed in Isolation Environments

Unlike removing applications not installed in an isolation environment, you cannot reliably use Windows **Add/Remove Programs** to remove applications installed in an isolation environment. Windows **Add/Remove Programs** may not completely delete everything that was installed.

Important Removing applications installed in an isolation environment also removes user-specific files resident in the user profile root of the deleted isolation environment folder. Because of this, Citrix recommends that before deleting an isolation environment folder, you follow your company policy with regard to backing up user-specific files.

To remove all applications installed in an isolation environment

---

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Ensure that you back up the registry before you edit it.

---

1. Delete all the files that reside in the installation root location of the isolation environment (typically C:\Program Files\Citrix\AIE\aiename).
2. Use regedit to delete the registry entries under installation root (typically HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AIE\aiename).
3. To prevent users receiving errors when they try to connect to any published application that uses the isolation environment, you must remove the association between those applications and the servers on which they are published. The following steps remove this association using both the Access Management Console and the Presentation Server Console.
4. In the Access Management Console, select each application and click Modify servers. The Application Properties dialog box appears.
5. Select the appropriate server and click **Remove**.

   If no servers are listed in the Application Properties dialog box, you may want to delete the published application by selecting it and clicking **Action** > **Delete** application.

   If no servers are listed in the Application Properties dialog box, in the Presentation Server Console, select the isolation environment, and click **Actions > Properties > Applications**. Select the applications, and click Remove.

   Because an application file system and registry are isolated, this procedure removes the applications from the server cleanly.

Deleting Isolation Environments

When you delete an isolation environment, you remove access to it through the Presentation Server Console and access to it by your users. Deleting an isolation environment from the console does not remove application or user-specific files resident in the deleted isolation environment folder on disk.

Note Citrix recommends before deleting an isolation environment to follow your company policy for backing up user-specific files.

To delete isolation environments

1. In the left pane of the Presentation Server Console, select the Isolation Environments node.
2. On the **Contents** tab, select the isolation environments you want to delete.
3. From the **Actions** menu, choose **Application Isolation** > **Delete isolation environment(s)**.

Because applications installed into isolation environments may not function correctly after you delete the isolation environment, Citrix recommends that you also uninstall the applications installed into the isolation environment. The previous section describes how to uninstall applications installed in an isolation environment and delete the contents of the isolation environment folder.

Setting CPU Priority Levels for Published Applications

By default, Citrix Presentation Server gives all published applications equal priority for access to CPU cycles. All application instances run with normal CPU priority.

The default configuration assumes that CPU access by all applications is equally important. The default configuration does not prevent one application from consuming resources that are required by other, mission-critical applications running on the same server.

You can manage some aspects of resource usage by applications through your deployment methods. For example, you can isolate mission-critical applications by publishing them on separate servers so less important applications do not compete for server resources. You achieve better performance by publishing CPU- and memory-bound applications on high-performance servers.

Citrix Presentation Server provides a setting you can apply to published applications to prioritize their CPU access. You can use the CPU priority settings on servers running Windows server operating systems.

Note The term *published application* in this section refers to applications and server desktops that are published for users in the server farm. It does not refer to published content such as documents and media files.

You can apply a CPU priority setting to each published application. Each instance of the application that runs in the server farm is affected by the setting. When multiple servers host the same published application, the setting applies to each server in the server farm on which the application runs.

If you publish the same application more than once—for separate groups of users, different host servers, or with different settings, for example—you create separate published applications. Each can have its own CPU priority setting.

You can use this setting in any size server farm, independent of load management features in Citrix Presentation Server Advanced and Enterprise Editions. Load management distributes connections to servers based on the servers' loads. In contrast, the CPU priority setting applies to a published application that runs on any server in the server farm.

Assigning CPU Priority Levels to Applications

When you assign a CPU priority level to a published application, the priority level that you specify is used by the CPU scheduler on all servers that host the published application (and for every instance of the application that runs on a server). When a server is executing multiple applications, the CPU scheduler prioritizes CPU access by application threads according to the priority level that you assign or the default priority level.

With this option, you can assign normal or lower CPU priority to Microsoft Internet Explorer, for example, and assign high CPU priority to an application whose performance is more important to the enterprise, such as PeopleSoft Human Resources Management. A higher priority setting gives Human Resources Management a performance advantage over Internet Explorer when both applications run on the same server.

You can assign five priority levels (in order from lowest to highest priority): low, below normal, normal, above normal, and high. The default is normal.

Important High priority indicates a process that performs time-critical tasks. The threads of a high-priority process preempt the threads of low- and normal-priority processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the system. Use extreme care when using the high-priority setting. A CPU-bound application assigned high priority can consume nearly all available CPU cycles, which can cause unacceptable performance by other applications running on the server.

The CPU priority option is in the Application Publishing wizard and on the **Application Limits** page in the **Properties** sheet for each published application. You can set the priority level when you first publish applications and set or change the level for published applications using the Access Management Console.

To modify the CPU priority level of a published application

1. In the scope pane of the Access Management Console, select an application. Then select **Action > Modify application properties > Modify all properties**.
2. Open the **Limits** page from the **Advanced** options page in the application's **Properties** list.
3. Select an option from the **CPU priority level** list. The default setting is Normal.

Note When publishing a new application, its CPU priority level is set as part of the advanced application settings under *application limits*.

Providing Resources to Novell Directory Services Users

Citrix Presentation Server supports the use of Novell Directory Services (NDS) for user authentication and access. This section covers the basic concepts and procedures for using Citrix Presentation Server with NDS.

Note Citrix Presentation Server run on 64-bit operating systems does not support NDS.

The following table defines NDS terms that may be helpful for understanding the procedures and descriptions in this section:

Term	Meaning
Tree	A set of objects set up hierarchically in a tree structure. The root object of the NDS tree is at the top of the tree.
Container object	The tree may or may not branch to these NDS Container objects: *Country* (a country location for this part of the organization) *Organization* (a company, university, or departmental unit) *Organizational Unit* (a business unit, division, or project team)

Term	Meaning
Common Name	The name for a leaf object on the tree. Examples of leaf objects are: users, groups, servers, and printers.
Context	An object's position in the tree. One way to represent context is by a string of the Common Names of the objects in the path from the leaf or container object to the root.
Distinguished Name	A combination of an object's common name and its context that makes up a complete NDS path for an object. A full Distinguished Name (DN) starts with a period for the root, and has a period between each object name.

Enabling NDS Support

For Citrix Presentation Server to access NDS on Novell servers, one of the following must be installed:

- NetWare 5.1 or later
- eDirectory Version 8.5x or later

The minimum software requirements are:

- Novell Client Version 4.8
- MetaFrame XP, Feature Release 1 or later

You must install the Novell Client on servers used for NDS applications. Dedicate servers with the Novell Client to applications for NDS objects after NDS is enabled for a server farm. Do not host published applications assigned to Active Directory users on these servers. The server farm can be a mixture of servers used exclusively for NDS applications and other servers. A Citrix administrator must have NDS credentials to manage applications and printers for NDS objects and to assign Citrix administrator privilege to NDS objects.

Important If you install the Novell Client on a server before installing Citrix Presentation Server, set the value FileSysChange=off in the [386Enh] section of the System.Ini file before you install Citrix Presentation Server. Make this change in the System.ini file for all users. If this parameter is not set correctly, Citrix Presentation Server Setup reports that the FileSysChange parameter is not valid. Novell technical document 10058117 refers to this issue. See the Novell knowledge base on the Web for more information.

The following procedures describe how to enable your server farm for NDS support.

Changing Registry Settings for Novell Client Installation

If you are setting up a server that does not yet have Citrix Presentation Server installed, install the Novell Client before you install Citrix Presentation Server. If Citrix Presentation Server is already installed, you must change the following registry settings on the server before and after you install the Novell Client.

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Ensure that you back up the registry before you edit it.

To change the registry on a server when installing the Novell Client

1. Before installing the Novell Client, run **regedit** from a command prompt.
2. Edit the registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

   by double-clicking **GinaDLL** in the right-hand pane. In the String Editor dialog box that appears, replace the value **Ctxgina.dll** with **Msgina.dll**.
3. Install the Novell Client *without restarting* when prompted.
4. Edit the registry entry for **GinaDLL** as in Step 2. This time type **Ctxgina.dll** as the value.
5. With the key path for Winlogon still selected, choose **New > String Value** from the **Edit** menu.
6. Name the string value **ctxGinaDLL**.
7. Double-click **ctxGinaDLL**. In the **Edit String** dialog box, enter **nwgina.dll** to assign this value to the new **ctxGinaDLL** entry.
8. Restart the server.

Enabling NDS Support for a Server Farm

NDS support is disabled for a server farm by default. Citrix Presentation Server supports one NDS tree per farm. NDS offers access by a secure logon and organizes network resources in a directory tree for administration. When access to an NDS tree is configured in a server farm, the tree is accessed directly for NDS user account information and authentication. NDS users are assigned published applications and printers through the NDS tree.

To enable NDS support for a server farm and specify the preferred NDS tree

1. Log on to a server in the farm that has the Novell Client installed.
2. In the scope pane of the Access Management Console, select a farm. Then select **Action > Modify farm properties > Modify all properties**.
3. Open the **General** page from the **Presentation Server** page in the farm's **Properties** list.
4. Enter the NDS tree name in the **NDS preferred tree** field.
5. Click **OK**.

Important To access the preferred NDS tree, you must install the Novell Client on the computer running Citrix Presentation Server.

Controlling Drive Mapping when Using NetWare Logon Scripts

Client drive mapping and NetWare logon script execution occur in parallel. If the logon script maps NetWare network drives, it is possible that a user could find drive V mapped to client drive C during one client session but mapped to a NetWare drive during another.

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it. You can avoid this problem by adding two registry values in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\InitialNetwareDrive.

REG_SZ: InitialClientDrive. Defines the first drive letter to use for client drive mapping. The system searches backward through the alphabet to assign drive letters to client drives that could not be mapped to their "native" drive letters.

REG_SZ: InitialNetWareDrive. Defines the drive letter to use for the NetWare SYS:LOGIN directory that is mapped to the preferred server during the initial NetWare attachment. This setting is the equivalent of the DOS VLM Net.cfg setting "First Network Drive." If this value is not set, the first available drive letter starting with C and ending with Z is used for this mapping.

Publishing Resources in an NDS-Enabled Environment

After your server farm is enabled to support NDS, use the following procedures to provide access to published resources for your users.

Logging on to the Presentation Server Console as an NDS User

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

To log on to the Presentation Server Console as an NDS user

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

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

   .JoeX.Admin.PNQ

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

Publishing an Application for NDS Users

The following procedure describes how to publish an application for your users after the farm enables support for NDS.

To publish an application for NDS users

1. Log on to the Access Management Console as an NDS user.
2. Verify that the intended host server has the Novell Client installed.
3. Select **Action > New > Published application**.
4. In the **Users** dialog box of the application publishing wizard, open the NDS tree.
5. Open container or leaf objects until the object to be granted access is in the window.
6. Select the object and click **Add**. Click **Finish**.

The object and those under it can access the application.

Using the BUILTIN Group

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

You can use the BUILTIN option:

- If your network environment is configured with Windows workgroups rather than with Windows network domains
- For compatibility with Novell's ZENworks product
- To specify users for applications and printer resources using custom ICA connections in Program Neighborhood

Enabling PDA Synchronization Support

Citrix Presentation Server supports the synchronization of USB-tethered and Microsoft Windows-powered PDAs that use ActiveSync as a synchronization agent. All features of ActiveSync are supported.

When used in a load-balanced (multihost) server environment, some ActiveSync features related to file I/O require the setup of roaming user profiles and, for efficiency, optional folder redirection.

To enable PDA synchronization

1. In the Presentation Server Console, open the properties dialog box of the policy in which you want to enable PDA synchronization.
2. Enable the rule **Client Devices > Resources > PDA Devices > Turn on automatic virtual COM port mapping**.
3. Disable the rule **Client Devices > Resources > Ports > Turn off COM ports** (or set it to **Not Configured**).

Note If the PDA Devices policy rule is disabled (by default), or there is no PDA attached to the client device, a session user might access a PDA physically connected to the server.

Enabling TWAIN Redirection Support

Presentation Server 4.0 and higher (Advanced and Enterprise Editions) can redirect client-connected TWAIN imaging devices, notably document scanners, from the client to the server, regardless of connection type.This allows users to control client-attached imaging devices from applications that run on the server and the redirection is transparent. TWAIN redirection on Citrix Presentation Server supports applications on 32-bit operating systems only.

Note Version 9.*x* or later of the Presentation Server Client for Windows is required for this feature.

To capture an image, users connect to a server from a client device that has an imaging device and the associated vendor-supplied TWAIN driver installed locally. When the TWAIN application is run from within this session, the application detects and interacts with the client-side device. The server-based application that is accessed runs as a client-based application.

To enable the configuration of TWAIN redirection

1. In the Presentation Server Console, open the properties dialog box of the policy in which you want to control TWAIN redirection.
2. Enable the rule **Client Devices** > **Resources** > **Other** > **Configure TWAIN redirection**.
3. Use the options to allow and disallow TWAIN redirection, as well as control the level of data compression.

Consider the following after enabling TWAIN redirection:

- The image acquisition software must be installed on the computer running Presentation Server. Examples of supported applications include: Microsoft PictureIT, OmniPage, PaperPort, Photoshop, Paint Shop Pro, and IrFanView.

  Note 16-bit TWAIN drivers are not supported.

- Image acquisition software that provides the USB device drivers must be installed on the client platform.

- For TWAIN redirection, some applications are not Terminal Server aware and look for Twain32.dll in the \Windows directory of the user profile (by default, C:\Documents and Settings\UserName\Windows). Copying Twain32.dll into the \Windows directory of each user profile resolves this issue. You can also correct this by adding the application to the Terminal Server application compatibility list with the following two flags specified:

  - Windows application: 0x00000008
  - Do not substitute user Windows directory: 0x00000400

  To automate enabling these flags on your server, copy the following text to a text editor and save it as a .reg file.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Terminal Server\Compatibility\
Applications\Photoshop]
"Flags"=dword:00000408
```

  Note You may need to combine these flags with other compatibility flags needed for the application.

- This feature supports the following modes of TWAIN information transfer:

  - Native
  - Buffered Memory (most scanning software works by default in Buffered Memory mode).

  Note The *disk file* transfer mode is not supported.

CHAPTER 7

Managing User Access

Users access published resources through ICA connections and sessions. *Connections* are network protocol-specific listener ports that are set up on a computer running Citrix Presentation Server. When a client links to a server through a connection, it establishes a *session.* The session is an active link that runs on the server until the user logs off.

This chapter explains how to manage user access to your server farm's resources by setting up user logons, configuring connections, and also monitoring, managing, and optimizing sessions.

Setting up User Logons

When user logons are enabled, Citrix Presentation Server does not limit user access to sessions and published applications by default. Thus, users can launch multiple connections and can connect to any published application that they are authorized to use. You can control the ability of users to connect to a server in the farm by enabling or disabling logons. By default, logons are enabled when you install Citrix Presentation Server. You might want to disable logons when you install software or perform other maintenance or configuration tasks.

To disable or enable logons

Select the server in the scope pane of the Access Management Console and select **Action > All Tasks > Disable logon**.

Note If logons are currently disabled, the option is **Enable logon**.

Controlling User Logon Look and Feel

When connecting to a server, users see all connection and logon status information in a sequence of screens, from the time they double-click a published application icon on the client device, through the authentication process, to the moment the published application launches in the session.

Citrix Presentation Server achieves this logon look and feel by suppressing the status screens generated by a server's Windows operating system when a user connects. To do this, Citrix Presentation Server Setup enables the following Windows *local* group policies on the server on which you install the product:

- Administrative Templates > System > Remove Boot / Shutdown / Logon / Logoff status messages
- Administrative Templates > System > Verbose versus normal status messages

However, group policies you configure in Active Directory take precedence over equivalent *local* group policies you configure for individual servers. Therefore, when you install Citrix Presentation Server on servers that belong to an Active Directory domain and configure the group policies above in Active Directory, those policies may prevent Citrix Presentation Server from suppressing the status screens generated by the Windows operating systems of the individual servers. In that case, users see the status screens generated by the Windows operating system when connecting to that server. For optimal performance, do not configure the above group policies in Active Directory.

Providing Users with Workspace Control

The Workspace Control feature provides users with the ability to quickly disconnect from all running applications, to reconnect to applications, or to log off from all running applications. Workspace Control enables users to move among client devices and gain access to all of their open applications when they log on.

For example, you can use Workspace Control to assist health-care workers in a hospital who need to move quickly between workstations and access the same set of applications each time they log on to Citrix Presentation Server. If you configure Workspace Control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

For users accessing applications through the Web Interface or the Program Neighborhood Agent you can configure—and allow users to configure—the following activities:

- **Logging on.** By default, Workspace Control enables users to automatically reconnect to all running applications when logging on, bypassing the need to reopen individual applications. Through Workspace Control, users can open disconnected applications plus applications active on another client device. Disconnecting from an application leaves the application running on the server. If you have roaming users who need to keep some applications running on one client device while they reconnect to a subset of their applications on another client device, you can configure the logon reconnection behavior to open only the applications that the user disconnected from previously.
- **Reconnecting.** After logging on to the server farm, users can reconnect to all their applications at any time by clicking Reconnect. By default, Reconnect opens both applications that are disconnected plus any active applications currently running on another client device. You can configure Reconnect to open only those applications that the user disconnected from previously.
- **Logging off.** For users opening applications through the Web Interface, you can configure the Log Off command to log the user off from the Web Interface and all active sessions together, or log off from the Web Interface only.
- **Disconnecting.** Users can disconnect from all running applications at once without needing to disconnect from each application individually.

Workspace Control is enabled in the server farm by default and is available only for users accessing applications through the Web Interface or the Program Neighborhood Agent.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session as soon as the user logs on to the client device in the X-ray laboratory.

For more information about enabling and configuring Workspace Control for users, see the *Citrix Web Interface Administrator's Guide*.

Configuring User Connections

Citrix Presentation Server lets users run applications published on servers by enabling connections from various computer platforms through Citrix Presentation Server Client software.

If a connection breaks, a session using the connection can remain active until its state is changed by Auto Client Reconnect or ICA Keep-Alive settings, or by a Citrix administrator. For information about saving data from disconnected sessions, see the *Access Management Console Help*.

Multiple clients can establish sessions through the same connection on a server. Citrix Presentation Server associates a user ID and connection with each session.

Note Citrix Presentation Server 4.5 supports only connection configurations that use the TCP/IP protocol. IPX/SPX, NetBIOS, and asynchronous (modem or direct cable) connections are not supported.

Selecting Connection Settings

Beginning with Citrix Presentation Server 4.5, the Citrix Connection Configuration tool is no longer supported. Instead, the configuration of connection settings to your server farm is done through the Microsoft Management Console (MMC).

To select connection settings

1. From the Windows Server 2003 Start menu, select **Administrative Tools > Terminal Services Configuration**.
2. With **Connections** selected in the left pane of the console that opens, select and right-click the entry **ICA-tcp** that appears in the right pane and select **Properties**.
3. Using the tabs that appear in this Properties dialog box you can select options for configuring your connections.

Note With the exception of the **ICA Settings** tab, these tabs are all standard MMC elements, and you should consult the appropriate Microsoft documentation for further information.

Establishing Connection Controls

You can establish connection controls for servers and published applications to help maintain the availability of resources in a server farm. In an environment without connection controls, you might encounter the following problems that degrade performance and reliability:

- Errors caused by individual users who run more than one instance of a published application at the same time
- Denial-of-service attacks by malicious users who run multiple application instances that consume server resources and connection license counts
- Over-consumption of resources by non-critical activities such as Web browsing

Connection control settings, including the option to log events related to connection control, are configured in the Access Management Console. Citrix Presentation Server Clients contain no configuration options related to connection control.

Connection control provides two types of limits:

Limit type	Description
Concurrent connections to the server farm	Restricts the number of concurrent connections that each user in the server farm can establish.
Published application instances	Restricts the total number of instances of a published application that can run in the server farm at one time, and prevents users from launching more than one instance of a published application.

Limiting Connections to a Server Farm

When a user launches a published application, the client establishes a connection to a computer running Citrix Presentation Server and initiates a session. If the user launches a second published application without logging off from the first one, this creates a second concurrent connection if that application is not available and published on that same server; otherwise session sharing occurs. To conserve resources, you can limit the number of concurrent connections that users are permitted to establish. Limiting connections can help you prevent over-consumption of server resources by a few users.

Note The seamless session option in the Citrix Presentation Server Client enables *session sharing* by default, a mode in which more than one published application runs with a single connection. If a user runs multiple applications with session sharing, the session counts as one connection.

A limit on connections applies to each user who connects to the server farm. A user's active sessions and disconnected sessions are counted for the user's total number of concurrent connections. For example, you can set a limit of three concurrent connections for users. If a user has three concurrent connections and tries to establish a fourth, the limit you set prevents the additional connection. A message tells the user that a new connection is not allowed.

Connection control affects users only if a connection attempt is prevented. If a user's number of connections exceeds a connection limit, the client displays a message that describes why the connection is not available.

To limit concurrent connections to a server farm

1. Select the farm in the scope pane of the Access Management Console and select **Action > Modify farm properties > Modify all properties**.
2. Open the **Connection Limits** page in the farm's **Properties** list.
3. Select **Maximum connections per user** to limit each user's concurrent connections. Enter the number of concurrent connections to allow for each user.
4. If you want the connection limitation to apply to everyone, including local administrators, select **Enforce limit on administrators**.
5. Click **OK** to apply the settings and close the page.

Note The option **Enforce limit on administrators** refers to local administrators. By default, local administrators are exempt from the limit so they can establish as many connections as necessary.

Limiting Application Instances

By default, users in a server farm have unlimited access to the published applications that they are authorized to use. Thus, Citrix Presentation Server does not limit the number of instances of a published application that can run at one time in a server farm. Also, by default, a user can launch more than one instance of a published application at the same time.

With connection control, you can specify the maximum number of instances of a published application that can run at one time in the server farm. For example, you can publish Autodesk AutoCAD and set a limit of 30 concurrent instances in the server farm. When 30 users are running AutoCAD at the same time, no more users can launch the application because of the limit of 30 concurrent instances.

Another connection control option lets you prevent any user from running multiple instances of a particular published application. With some applications, running more than one instance in a single user context can cause errors.

You can apply application limits independently to each published application. For example, you can apply the limitations on total concurrent instances and multiple instances by a single user to one published application. You can limit only the total concurrent instances of another application. You can configure a third application to limit launching of multiple instances by individual users.

Note Connection control options apply to published applications and published desktops only and do not affect published content such as documents and media files that execute on the client device.

To publish an application or desktop with application limits

1. Run the application publishing wizard and configure all of the basic options for the application to be published.
2. Proceed to the advanced application settings and on the application limits page, select one or both of the following options:
   - **Limit instances allowed to run in server farm**. Select this option and enter the maximum number of instances that can run at one time in the server farm without regard to who launches the application.
   - **Allow only one instance of application for each user**. Select this option to prevent any user from running more than one instance of this application at the same time.
3. Configure the remaining advanced settings as desired, then click **Finish** to publish the application.

Note For applications that are already published, these settings can be configured in the Access Management Console on the **Advanced > Limits** page of the application's **Properties** list.

Logging Connection Control Events

Event logging records an entry in the System log each time a server denies a user connection because of a connection control limit. Each server records the data in its own System log. By default, this type of event logging is disabled.

To enable logging of connection control events

1. Select a farm in the scope pane of the Access Management Console and select **Action > Modify farm properties > Modify all properties**.
2. Open the **Connection Limits** page in the farm's **Properties** list.
3. Select **Log over-the-limit denials**.
4. Click **OK** to apply the setting and close the page.

Exceeding the following limits can result in connection denials that the system records if logging is enabled:

Maximum connections per user. You can limit users to a maximum of five connections, for example. If a user tries to launch a sixth connection, the server denies the connection request and records the user's name and the time in the System log.

Use the **Maximum connections per user** setting to limit how many connections each user can have.

Application instances. You can limit a published application to a certain number of concurrent instances. If you type **10** in **Maximum instances** and a user tries to launch the application when 10 instances are running, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

Use the **Limit instances allowed to run in server farm** setting on the **Limits** page of the application's Properties to limit instances of each published application.

Application instances per user. You can configure a published application to allow each user to run only one instance of the application. If a user tries to launch a second instance of the application, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

Use the **Allow only one instance of application for each user** setting in the **Limits** page of the application's Properties to limit each published application to one instance for a user.

Administering User Sessions

The following sections describe how to administer user sessions by:

- Managing sessions with the Access Management Console
- Monitoring sessions with session shadowing
- Enabling sessions by configuring client device mapping
- Optimizing session performance
- Configuring the availability of audio in sessions

These tasks are all important aspects of administering user sessions; however, you must also consider the use of policies for determining the nature of your users' sessions. For more information, see "Using Policies to Configure Access to Published Resources" on page 125.

Note You may not see some or all of the options described below if you have not been granted permission to perform these tasks. See your Citrix administrator for more information.

Managing Sessions with the Access Management Console

You can use the Access Management Console to view information about active sessions and also to perform session management activities, including logging off, disconnecting, and sending messages to users. In the Access Management Console, you can select client sessions and choose commands to manage the sessions through the **Action** menu, or the **Tasks** list that appears at the bottom of the details pane.

Finding Information about Active Sessions

To display information about active sessions in the Access Management Console, select a farm or a server in the scope pane, and select **Action** > **All Tasks > Change display > Sessions**. This displays information about active client sessions in the details pane.

The session information that appears in the console is in table format and includes details that help you identify the various types of sessions and the users associated with the sessions. Each row in the table lists details for one session. The following column labels appear on tabs that display session information.

- **User.** The name of the user account that initiates a session. In the case of anonymous connections, the user name is a string with the letters "Anon" followed by a session number.
- **Session ID.** A unique number that begins with 0 for the first connection to the console. Listener sessions are numbered from 65,537 and numbered backward in sequence.
- **Application.** The name of the published application running within this session.
- **State.** A session's state is listed as Active, Listen, Idle, Disconnected, or Down.
- **Client name.** The name of the client device that is running the session.
- **Logon Time.** The time at which the user logged on.
- **Server.** The server on which the selected application is running.

Disconnecting and Reconnecting Sessions

To disconnect a session through the Access Management Console, right-click a session and choose **Disconnect**. When you disconnect a session, you close the connection between the client and the server. However, this does not log off the user, and programs that were running in the session are still running on the server. If the client user then connects to the server (by selecting a published application or custom connection to the server), the disconnected session is reconnected to the client. When a session is disconnected, the word *Disconnected* appears in the State column on the tabs in the Access Management Console where session information appears.

You can connect to a user's disconnected session by choosing **Connect**. Your session must be capable of supporting the video resolution of the disconnected session. From the system console, you can connect only to sessions that were disconnected from the console.

Sending Messages to Users

You can send a message to a user by selecting the user's session and choosing **Send Message**. You can select multiple sessions to send a message to multiple users at the same time. To broadcast a message to all users, you can select all active user sessions in the right pane in the console.

In the **Send Message** dialog box, you can type a message title; the user name of the Citrix administrator who is logged on to the console and the current time appear in the **Title** box by default. Type the message text in the **Message** box. The text you type automatically wraps to the next line if you type past the right margin. When you finish typing the message, click **OK** to send the message to the selected sessions.

Resetting Sessions

Resetting a session with the **Reset** command terminates all processes that are running in that session. You can use the **Reset** command to remove remaining processes in the case of a session error. However, resetting a session can cause applications to close without saving data.

If you reset a disconnected session, the word *Down* appears in the State column for the session. When you refresh the console display or when the next automatic refresh occurs, the session no longer appears in the list of sessions.

Special sessions that listen for requests to connect to the server are identified by the word *Listen* in the State column. If you reset a listener session, the server resets all sessions that use the protocol associated with the listener. For example, if you reset the ICA listener session, you reset the sessions of all users who are connected to the server.

Shadowing Sessions

S*hadowing* a session means viewing the session from another session, usually running on another device. When shadowing, you can monitor the session activity as if you are watching the screen of the client that initiated the session. While you are shadowing a session, you can also use your keyboard and mouse to remotely control the user's keyboard and mouse in the shadowed session if configured.

Shadowing a session provides a powerful tool for you to assist and monitor users. Shadowing is a useful option for your Help desk staff who can use it to aid users who have trouble using an application. Help desk personnel can view a user's screen or actions to troubleshoot problems and can demonstrate correct procedures. You can also use shadowing for remote diagnosis and as a teaching tool.

For more information about session shadowing, see "Using Session Shadowing" on page 174.

Logging off Sessions

Choose **Logoff** to force a user's session to end. If you select multiple sessions, choosing the command ends each selected session.

Important Ending users' sessions with the **Logoff** command can result in loss of data if users do not close their applications first. You should send a message to warn users to exit all applications if you need to log off their sessions.

Viewing Session Information

To view detailed information about the client cache, session information client modules, and processes associated with a session, display and select the session in the Access Management Console. In the **Tasks** menu at the bottom of the right pane, choose **Show more tasks for the selected items**. To terminate a process that is associated with a session, click the **Processes** link that appears here, select an associated process, and choose the **Terminate** command.

Using Session Shadowing

You enable shadowing on a server when you install Citrix Presentation Server and select the default option, which allows shadowing on all connections on the server. A shadower can remotely control a shadowed session through the shadower's mouse and keyboard, if this action is not prohibited by options selected when Citrix Presentation Server is installed on the server. By default, the user who will be shadowed is asked to accept or deny the request to shadow the session.

Important If shadowing restrictions are selected during Citrix Presentation Server installation, the restrictions cannot be changed later. For more information, see "Step 8: Configuring Session Shadowing" on page 69.

Shadowing from the Access Management Console

When you use the Access Management Console for shadowing, you must start each shadowing session individually; if you select multiple sessions to shadow, the **Shadow** command and button are not available. To start shadowing multiple sessions at once, use the Shadow taskbar.

To use the Access Management Console for shadowing, you must have Program Neighborhood installed on the system with the console.

To shadow a session from the Access Management Console

1. Select the session in the right pane of the console.
2. Choose **Action > Shadow** or select **Shadow** from the **Tasks** menu at the bottom of the right pane.

Shadowing Using the Shadow Taskbar

To launch the Shadow taskbar, from the **Start** menu choose **All Programs > Citrix > Administration Tools > Shadow Taskbar**. The Shadow taskbar appears as a toolbar at the top of the console display. You can also click the **Shadow Taskbar** button on the ICA Administrator toolbar to launch the Shadow taskbar.

When the Shadow taskbar is running and no sessions are being shadowed, the **Shadow** button appears alone on the taskbar. Click the **Shadow** button and the **Shadow Session** dialog box appears. Use the **Shadow Session** dialog box to select the sessions you want to shadow. You can select sessions based on the server, the application, or the users who are associated with the sessions. You can select multiple sessions in the dialog box to begin shadowing several sessions at once. Click **OK** to begin shadowing the selected sessions.

For more information about shadowing with the Shadow taskbar, press F1 to view online Help when the Shadow taskbar is running.

Enabling User-to-User Shadowing

You can use the Presentation Server Console to create a user policy to enable user-to-user shadowing, which allows users to shadow other users without requiring them to be members of the Citrix administrator group. With user-to-user shadowing, multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration. Also, you can enable Help Desk personnel to shadow users' sessions or allow your Sales Department to hold an online meeting to review sales leads.

Important You are prompted to configure shadowing settings during Citrix Presentation Server Setup. If you choose to prohibit shadowing during Setup, you cannot enable shadowing with user policies.

You enable user-to-user shadowing by creating policies that define users who can shadow. You then assign the policies to the users you want to be shadowed.

To enable user-to-user shadowing

1. Create a user policy that identifies the users who can shadow other users' sessions.
2. Assign the policy to the users to be shadowed.
3. Publish the Citrix Shadow Taskbar and assign it to the users who will shadow. Be sure to instruct these users how to initiate shadowing from their client devices.

Note Instruct your users to refrain from launching the Shadow taskbar in seamless mode. The Shadow taskbar cannot function in seamless mode.

The following example demonstrates how to enable user-to-user shadowing. It assumes that you want to create a policy for your "Sales" user group that allows them to shadow the department manager for online collaboration on sales leads.The two procedures detailed here are the creation of a shadowing policy and then the assignment of that policy to the users in the Sales group.

To create a user policy for user-to-user shadowing

1. Create a new policy. For example, the policy for the Sales Department is named "Sales Group Shadowing."
2. Open the Sales Group Shadowing policy's properties by selecting the policy and choosing **Actions > Properties**.
3. Open the **Shadowing** folder under **User Workspace** in the left pane. Select the rule named **Configuration**.
   A. Set the rule's state to enabled by selecting **Enabled**.
   B. Select **Allow shadowing** to enable shadowing.

      Because the Sales Manager may work with sensitive data, select the option **Prohibit being shadowed without notification**.

      If the sales manager does not want other users to be able to take control of his mouse and keyboard, select the option **Prohibit remote input when being shadowed**.
4. Select the rule named **Permissions** in the left pane of the property sheet.
5. Set the rule's state to enabled by clicking **Enabled**.

6. Click **Configure** to select the users who will shadow the Sales Manager.

   To allow the members of the Sales Department to shadow the Sales Manager, select the Sales user group and then click **Add**. The user group is listed in the Configured Accounts list. Click **OK** when you are done adding users. The users and user groups you added to the Configured Accounts list are listed in the right pane of the policy's property sheet. By default, the shadowing permission for each user or user group is set to **Allow**. You can deny shadowing permissions by clicking **Deny**.

7. Click **OK** at the bottom of the policy's property page when you are done configuring the shadowing rules.

After you create the policy and configure the rules, you must assign the policy to the users who you want to be shadowed.

Note You can create and apply a policy that allows Novell Directory Services (NDS) users to be shadowed. However, you cannot configure NDS users to have shadowing permissions.

To assign the shadowing policy to users

1. Select the Sales Group Shadowing policy and choose **Actions > Policy > Apply this policy to**.
2. Select **Users** in the left pane and select **Filter based on users**. Select the users you want to be shadowed. To allow the Sales Manager to be shadowed, select the domain of which he is a member. Click **Show Users** to display the individual user accounts in the selected domain.
3. Select the Sales Manager's user name and then click **Add** to display his user account in the Configured Accounts list.
4. Click **OK** when you are done adding users.

Important The list of users permitted to shadow is exclusive for each user to whom a policy is assigned. For example, if you create a policy that permits User A to shadow User B, this policy allows *only* User A to shadow User B, unless you add more users to the list of users who can shadow in the same policy's Property sheet. To publish the Shadow taskbar utility to the users you want to be able to shadow, see the procedure above for enabling user-to-user shadowing.

Configuring Client Device Mapping

Citrix Presentation Server Clients support mapping devices on client computers so users can access the devices within client sessions. Client device mapping provides:

- Access to local drives and ports
- Cut-and-paste data transfer between a client session and the local clipboard
- Audio (system sounds and .wav files) playback from the client session

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

Client Drive Mapping

Client drive mapping is built into the standard device redirection facilities of Citrix Presentation Server. The client drives appear as client network objects in Windows. The client's disk drives are displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive.

By default, the drives on the client system are automatically mapped to drive letters on the server when users log on. The server tries to match the client drives to the client drive letters; for example, the client's first floppy disk drive to A, the second floppy disk drive to B, the first hard drive partition to C, and so forth. This allows the user to access client drive letters in the same way locally and within client sessions.

However, the same drive letters are often in use by the drives on the server (unless the server drives are remapped prior to the installation of Presentation Server.) In this case, client drives are mapped to different drive letters. The server starts at V and searches in ascending order for unassigned drive letters.

You can turn off client drive mapping through policies you configure in Citrix Presentation Server. You can turn off mapping to client floppy disk drives, hard drives, CD-ROM drives, or remote drives.

Note If access to the floppy disk drives is not needed, Citrix recommends disabling such access because this speeds the logon process.

As a security precaution, when a user logs onto Citrix Presentation Server, by default, the server maps client drives without user execute permission. For users to be able to execute files residing on mapped client drives, you must override this default by editing the value of **ExecuteFromMappedDrive** in the registry on a server running Citrix Presentation Server.

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

To change the ExecuteFromMappedDrive registry setting

1. After installing Citrix Presentation Server, run **regedit**.
2. Find the key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdm\Parameters\ExecuteFromMappedDrive
3. To grant users execute permission on mapped drives, set **ExecuteFromMappedDrive** to **1**.

   To deny users execute permission on mapped drives, which is the default, set **ExecuteFromMappedDrive** to **0**.
4. Restart the server for the change to take effect.

Client COM Port Mapping

Client COM port mapping allows a remote application running on the server to access devices attached to COM ports on the client device. Client COM ports are not automatically mapped to server ports at logon, but can be mapped manually using the **net use** or **change client** commands. See “Citrix Presentation Server Commands” on page 283 for more information about the **change client** command.

For more information about client COM port mapping, see the administrator’s guides for the clients you plan to deploy.

Client Audio Mapping

Client audio mapping allows applications running on the server to play sounds through a sound device on the client device. The server can control the amount of bandwidth used by client audio mapping. Audio mapping is configured with Citrix policies.

For more information about using client audio mapping, see the *Administrator's Guides* for the clients you plan to deploy.

Optimizing Session Performance

Users can lose network connectivity for various reasons, including unreliable networks, highly variable network latency, and range limitations of wireless devices. Losing connectivity often leads to user frustration and a loss of productivity.

You can leverage two features of Citrix Presentation Server to optimize the reliability of sessions and to reduce the amount of inconvenience, downtime, and loss of productivity users incur due to lost network connectivity. *Session Reliability* is available with the Advanced and Enterprise Editions of the product. *Auto Client Reconnect* is available with all levels of Citrix Presentation Server.

If you are licensed for the Advanced or Enterprise Editions of Citrix Presentation Server, you can take advantage of both features in combination.

Session Reliability

Session Reliability is available with the Enterprise and Advanced Editions of Citrix Presentation Server. This feature keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

This feature is especially useful for mobile users with wireless connections. Take, for example, a user with a wireless connection who enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the client session would be disconnected and disappear from the user's screen, and the user would have to reconnect to the disconnected session.

With Session Reliability, the client session remains active on the server. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Users of the Program Neighborhood Client can override the Session Reliability setting you configure on the server by selecting or clearing the **Enable session reliability** option in their application or connection settings. Users of Program Neighborhood Agent and the Web Client cannot override the server setting.

By default, Session Reliability is enabled at the server farm level. You can customize the settings for this feature by selecting the server farm's **Properties** page in the Access Management Console and modifying the Session Reliability settings as appropriate. You can edit the port on which Citrix Presentation Server listens for session reliability traffic and edit the amount of time Session Reliability keeps an interrupted session connected.

The **Seconds to keep sessions active** option has a default of 180 seconds, or three minutes. Though you can extend the amount of time Session Reliability keeps a session open, keep in mind that this feature is designed to be convenient to the user and that it does not, therefore, prompt the user for reauthentication. If you extend the amount of time a session is kept open indiscriminately, chances increase that a user may get distracted and walk away from the client device, potentially leaving the session accessible to unauthorized users.

Note You can use Session Reliability in conjunction with SSL.

If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure Auto Client Reconnect to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in **Seconds to keep sessions active**. After that, the settings you configure for Auto Client Reconnect take effect, attempting to reconnect the user to the disconnected session.

Important If the Session Reliability feature is enabled, the default port used for session communication changes from 1494 to 2598.

Automatic Client Reconnection

The Auto Client Reconnect feature allows Clients for Windows, Java, and Windows CE to detect broken connections and automatically reconnect users to disconnected sessions. When a client detects an involuntary disconnection of a session, it attempts to reconnect the user to the session until there is a successful reconnection or the user cancels the reconnection attempts.

When a connection breaks, it may leave the server session in an active state. Users can reconnect only to sessions that are in a disconnected, or inactive, state. Cookies containing keys to user credentials and session IDs are created on the client device when sessions are started. Because users can be reconnected only to disconnected sessions, Auto Client Reconnect uses the cookie on the client device to disconnect an active session before attempting to reconnect.

By default, Auto Client Reconnect is enabled at the server farm level, and user reauthentication is not required. You can customize the settings for this feature at the farm level and for individual servers. To do this, select **ICA** on the corresponding farm or server **Properties** page in the Access Management Console and modify the Auto Client Reconnect settings as appropriate.

Security in Auto Client Reconnect

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on to a server farm, Citrix Presentation Server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to the client. The client submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication.

When cookies expire, users must reauthenticate to reconnect to sessions. Cookies are not used if you select **Require user authentication**. Selecting this option displays a dialog box to users requesting credentials when the client is attempting to reconnect automatically. Use the Access Management Console to enable **Require user authentication**.

Note For maximum protection of users' credentials and sessions, use SSL encryption for all communication between clients and the server farm.

Configuring Auto Client Reconnect Settings

You can configure the following Auto Client Reconnect settings.

- Require user authentication upon autoreconnection. You can set this requirement at the server farm level or for individual servers.
- Enable or disable logging of reconnection events for the server farm or individual servers.
- Enable or disable auto reconnect functionality on the client using an ICA file or in the Appsrv.ini file on client devices.

You can use the Access Management Console or the **Acrcfg** command to require user authentication for automatic reconnection and reconnection event logging. Reconnection event logging is disabled by default. For more information about the Acrcfg command, see “Citrix Presentation Server Commands” on page 283.

You can disable Auto Client Reconnect on the Client for Windows by setting TransportReconnectEnabled=Off in the [WFClient] section of the client’s Appsrv.ini file. For more information about client configuration using Appsrv.ini, see the *Clients for Windows Administrator’s Guide*.

Settings for connections also affect Auto Client Reconnect.

Configuring Connections for Automatic Client Reconnection

By default, Auto Client Reconnect is enabled at the server farm level; user reauthentication is not required. However, if a server’s ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection.

In this context, the *ICA TCP connection* refers to a Citrix Presentation Server’s virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.

By default, the ICA TCP connection on a computer running Citrix Presentation Server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by the Citrix Presentation Server Client.

The connection can be configured to *reset*, or log off, sessions with broken or timed out connections. When a session is reset, attempting to reconnect initiates a new session; rather than restoring a user to the same place in the application in use, the application is restarted.

If Citrix Presentation Server is configured to reset sessions, Auto Client Reconnect creates a new session. This process requires users to enter their credentials to log on to the server.

Logging Automatic Client Reconnection Events

To enable or disable log entries for automatic reconnection events, open the **ICA** page in the **Properties** pages for the server farm or individual servers.

Logging is disabled by default. When logging is enabled, the server's System log captures information about successful and failed automatic reconnection events to help with diagnosis of network problems.

Automatic reconnection can fail if the client submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

Each server stores information about reconnection events in its own System log. The server farm does not provide a combined log of reconnection events for all servers.

Utilizing SpeedScreen Technologies

Network latency and bandwidth availability can impact the performance of connections to published applications and content. SpeedScreen technology allows you to configure several features to improve connection speed and responsiveness. Instructions for configuring these features are provided in the following sections:

SpeedScreen Latency Reduction Manager. Provides mouse click feedback and local text echo, both of which reduce a user's perception of latency when typing and clicking.

SpeedScreen Browser Acceleration. Optimizes the responsiveness of graphics-rich HTML pages in published versions of Microsoft Outlook, Outlook Express, and Internet Explorer.

SpeedScreen Multimedia Acceleration. Allows you to control and optimize the way Citrix Presentation Server passes streaming audio and video to users.

SpeedScreen Flash Acceleration. Allows you to control and optimize the way Citrix Presentation Server passes Macromedia Flash animations to users.

SpeedScreen Image Acceleration. Offers you a trade-off between the quality of photographic image files as they appear on client devices and the amount of bandwidth the files consume on their way from the server to the client.

SpeedScreen Progressive Display. Allows you to improve interactivity when displaying high-detail images by temporarily increasing the level of compression (decreasing the quality) of such an image when it is first transmitted over a limited bandwidth connection, to provide a fast (but low quality) initial display. If the image is not immediately changed or overwritten by the application, it is then improved in the background to produce the normal quality image, as defined by the normal lossy compression level.

Heavyweight Compression. Allows you to increase the compression of SpeedScreen Image Acceleration and SpeedScreen Progressive Display without impacting image quality. Because heavyweight compression is CPU intensive and affects server scalability, heavyweight compression is recommended for use only with low bandwidth connections.

SpeedScreen Latency Reduction Manager

On high-latency network connections, users may experience delays between the time they click a link and the time the link opens. As a result, users may click links more than once, possibly opening multiple copies of a file or application. Similarly, characters that a user types may not appear instantly, possibly causing the user to type characters repeatedly before seeing them onscreen.

SpeedScreen Latency Reduction Manager helps reduce a user's perception of latency with mouse click feedback and local text echo.

Mouse Click Feedback. Mouse Click Feedback, which is enabled by default, changes the appearance of the pointer from idle to busy after the user clicks a link, indicating that the system is processing the user's request.

Local Text Echo. When a user types text, the keystrokes are sent to the server, which renders the fonts and then returns the updated screen redraw to the client. You can bridge the delay between keystroke and screen redraw by enabling Local Text Echo. Local Text Echo temporarily uses client fonts to immediately display text a user types while the screen redraw from the server is in transit.

By default, Mouse Click Feedback is enabled and Local Text Echo is not enabled. You can enable and disable Mouse Click Feedback at the server level and Local Text Echo both at the server and application level. You can also configure Local Text Echo settings for individual input fields within an application. See the application help for SpeedScreen Latency Reduction Manager for more information.

Note Applications that use non-standard Windows APIs for displaying text may not support Local Text Echo.

To launch SpeedScreen Latency Reduction Manager, click its button on the ICA Toolbar or select **SpeedScreen Latency Reduction Manager** from the **Citrix > Administration Tools** program group in the **Start** menu.

Important Test all aspects of an application with Local Text Echo in a non-production environment before enabling text echo for your users to ensure that the display is acceptable to users.

When you configure SpeedScreen Latency Reduction Manager on a particular server, the settings are saved in the ss3config folder in the Citrix installation directory of that server. You can propagate the settings to other servers by copying this folder and its contents to the same location on the other servers.

Note If you plan to propagate SpeedScreen Latency Reduction Manager settings to other servers, select to Apply settings to all instances of the selected application when configuring Local Text Echo. Paths to published applications might differ from one server to another; applying the settings to all instances of the selected application ensures that the settings apply regardless of where the application is located on the destination server.

SpeedScreen Browser Acceleration

As both Web pages and HTML-based email get richer in graphics content, more bandwidth is used. You can use SpeedScreen Browser Acceleration to optimize the responsiveness of image-rich Web pages and email in published versions of Internet Explorer, Outlook, and Outlook Express. With SpeedScreen Browser Acceleration, the user can scroll the pages and use the Back and Stop buttons immediately while image files download in the background.

To further accelerate the accessibility of Web pages and email, you can enable JPEG compression with SpeedScreen Browser Acceleration. JPEG compression offers you a trade-off between the quality of JPEG files as they appear on client devices and the amount of bandwidth the files consume on their way from server to client. JPEG compression results in slightly lower image resolution and slightly higher resource consumption on both server and client. It does not affect JPEG files rendered by applications other than those mentioned above. For information about improving the throughput of image files rendered by other applications, see "SpeedScreen Image Acceleration" on page 188.

SpeedScreen Browser Acceleration requires Version 7.0 or later of the Citrix Presentation Server Clients for Windows, Internet Explorer 5.5 through 7.0, and High Color (16 bit) or greater connection color depth.

By default, SpeedScreen Browser Acceleration is enabled at the server farm level. You can customize the settings for this feature at the farm level and for individual servers. To do this, select the corresponding farm or server Properties page in the Access Management Console and modify the SpeedScreen Browser Acceleration settings as appropriate.

SpeedScreen Multimedia Acceleration

SpeedScreen Multimedia Acceleration optimizes multimedia playback through published instances of Internet Explorer, Windows Media Player, and RealOne Player. This feature offers significant performance gains in the following areas:

- **User Experience.** Multimedia playback in sessions is much smoother.
- **Server CPU Utilization.** The client device decompresses and renders multimedia content, freeing server CPU utilization.
- **Network Bandwidth.** Multimedia content is passed over the network in compressed form, reducing bandwidth consumption.

Without SpeedScreen Multimedia Acceleration, the cumulative cost of several users playing multimedia content in sessions at the same time is high, both in terms of server CPU utilization and network bandwidth consumption. When you play multimedia content in a session, the server decompresses and renders the multimedia file, which increases the server's CPU utilization. The server sends the file over the network in uncompressed form, which consumes more bandwidth than the same file requires in compressed form.

With SpeedScreen Multimedia Acceleration, the server streams multimedia to the client in the original, compressed form. This reduces bandwidth consumption and leaves the media for the client device to decompress and render, thereby reducing server CPU utilization.

SpeedScreen Multimedia Acceleration optimizes multimedia files that are encoded with codecs (compression algorithms) that adhere to Microsoft's DirectShow standards. DirectShow is an application programming interface (API) that allows, among other things, multimedia playback. To play back a given multimedia file, a codec compatible with the encoding format of the multimedia file must be present on the client device.

As a rule of thumb, if you can play back a given multimedia file locally on a given client device, you can play back the same file on the same client device within a session. Users can download a wide range of codecs, such as those supported by Windows Media Player or RealOne Player, from vendor Web sites.

By default, SpeedScreen Multimedia Acceleration is enabled at the server farm level. You can customize the settings for this feature at the farm level and for individual servers. To do this, select the corresponding farm or server Properties page in the Access Management Console and modify the SpeedScreen Multimedia Acceleration settings as appropriate.

Note With SpeedScreen Multimedia Acceleration enabled, RealOne Player's built-in volume and balance controls do not work within client sessions. Instead, users can adjust volume and balance from the volume controls available from the client notification area.

SpeedScreen Flash Acceleration

Macromedia Flash animations are a common component of many Web sites and Web applications. In earlier versions of Citrix Presentation Server, users playing Flash animations in published applications often observed poor rendering quality of the animation, slow session responsiveness, or a combination of both. This is because Macromedia Flash Player, which renders the animation on the server, starts in high-quality mode by default. While this guarantees the highest possible rendering mode for each frame, it also means that each frame consumes considerable bandwidth on its way to the user.

SpeedScreen Flash Acceleration improves the user's session responsiveness by forcing Flash Player to start up in low-quality mode, rendering animations at a lower quality level and reducing the amount of data put on the network for each frame. SpeedScreen Flash Acceleration also reduces the amount of processing power that is required to render Flash animations.

By default, SpeedScreen Flash Acceleration is enabled at the server farm level. You can customize the settings for this feature at the farm level and for individual servers. To do this, select the corresponding farm or server Properties page in the Access Management Console and modify the SpeedScreen Flash Acceleration settings as appropriate.

SpeedScreen Image Acceleration

The size of image files affects the amount of time the files take to travel from server to client. Often, image files contain redundant or extraneous data that is of little benefit to the user and slows down the user's session while downloading and rendering. SpeedScreen Image Acceleration offers you a trade-off between the quality of photographic image files as they appear on client devices and the amount of bandwidth the files consume on their way from server to client.

SpeedScreen Image Acceleration applies a lossy compression scheme to reduce the size of image files for faster throughput. The compression scheme removes redundant data while attempting to minimize the loss of information. Under most circumstances, the data loss is minimal and its effect nominal. However, Citrix recommends that you use discretion in applying this feature where preservation of image data may be vital, as in the case, for example, of X-ray images.

Unlike the other SpeedScreen features, SpeedScreen Image Acceleration is not configured through the Access Management Console. This feature is enabled by default. You can use policy rules in the Presentation Server Console to override the default settings and accommodate different user needs by applying different levels of image compression to different connections. To do this:

1. In the Presentation Server Console, select the policy for which you want to configure the rule.
2. From the **Actions** menu, select **Properties**.
3. Select **Bandwidth > SpeedScreen > Image acceleration using lossy compression** and configure the rule.

Choose no or low compression for users who need to view images at original or near original quality levels. You can accelerate image throughput by choosing one of four compression levels per policy rule:

Lossy Compression Level	Image Quality	Bandwidth Requirements
High compression	Low	Lowest
Medium compression	Good	Lower
Low compression	High	Higher
No compression	Same as original	Highest

If this policy rule is not configured, by default SpeedScreen Image Acceleration is enabled as **Medium compression; medium image quality**, but only for connections with less than 2 megabit/sec of bandwidth per user. Note that this default may not be the optimum setting for all environments, so you are encouraged to experiment with other settings. For example, enabling lossy compression for all line speeds might potentially improve performance even over a LAN, depending on site characteristics.

To configure SpeedScreen Image Acceleration without enabling SpeedScreen Progressive Display, after enabling the policy rule and choosing Compression level, for **SpeedScreen Progressive Display compression level**, choose **Disabled; no progressive display**.

SpeedScreen Progressive Display

As part of the SpeedScreen policy rule (**Bandwidth > SpeedScreen > Image acceleration using lossy compression**), you can also enable SpeedScreen Progressive Display to increase the performance of displaying images or parts of images that are changing.

SpeedScreen Progressive Display speeds the initial display of an image file by choosing an increased compression level while an image is dynamic. This initial display is then sharpened up to normal quality in the background if the image is not immediately changed or overwritten in the application. The quality of the final image is controlled by SpeedScreen Image Acceleration.

SpeedScreen Progressive Display can improve the performance not only of applications that render and display images, but also those parts of an image that are dynamic, such as when scrolling through a PDF or similar document.

You configure SpeedScreen Progressive Display along with SpeedScreen Image Acceleration, which is described in the previous section "SpeedScreen Image Acceleration" on page 188.

When the SpeedScreen policy rule is not configured, SpeedScreen Progressive Display is enabled with a compression level of **Very high compression; very low quality**, but only for connections with less than 512Kbps of bandwidth per user. Note that this is unlikely to be the optimum setting for all environments, so you are encouraged to experiment with other settings.

To configure SpeedScreen Progressive Display without enabling SpeedScreen Image Acceleration, after enabling the policy rule and choosing SpeedScreen Progressive Display compression level, for **Compression level**, choose **Do not use lossy compression**.

Heavyweight Compression

Heavyweight compression allows you to further reduce the bandwidth of SpeedScreen Image Acceleration and Progressive Display, without further degradation in screen quality. Heavyweight compression uses a more CPU intensive algorithm and impacts server performance and scalability. This type of compression is recommended only for low bandwidth connections.

If enabled in the SpeedScreen policy rule, heavyweight compression applies to all lossy compression settings. It is supported on Citrix Presentation Server Clients for Windows, but has no effect on other clients.

Configuring Audio for User Sessions

Citrix Presentation Server offers you a variety of tools to manage and control the availability of sound in client sessions, both in terms of quality and cost in resources, including:

- Audio properties you configure for individual published applications
- Audio related policies and settings you configure for specific connection types
- Audio settings the user configures on the client device

For example, you can use audio related connection polices to control bandwidth usage and server CPU utilization. You can configure a policy rule to enable audio for connections where audio is essential, and configure another rule to disable audio for connections where it is not essential.

From the Presentation Server Console, you control the availability of speakers and microphones in client sessions with separate policy rules. On the client device, a single setting controls both. To enable audio on the client device, the user selects an audio quality level from the **Settings** dialog box (for Program Neighborhood) or from the **Properties** dialog box (for Program Neighborhood Agent). The connection policies you configure on the server determine what audio quality levels are available to the user. Connection policies permitting, enabling audio on the client device turns on speakers, microphones, or both.

Important This section covers aspects of enabling audio support on servers. To use audio in client sessions, users must also enable audio on the client device. For more information about enabling audio for clients, see the administrator's guides for the clients you want to configure.

Enabling Audio for Published Applications

You can enable or disable audio for published applications. If you disable audio for a published application, audio is not available within the application under any condition. If you enable audio for an application, you can use policy rules and filters to further define under what conditions audio is available within the application.

To enable or disable audio for a published application

1. In the Access Management Console, select the published application for which you want to enable or disable audio, and select **Action > Modify application properties > Modify all properties**.
2. Under **Advanced > Client options**, select or clear the **Enable legacy audio** check box.

Note In earlier releases of Presentation Server, this option was called **Enable audio**.

Configuring Audio-Related Policy Rules

From disabling audio altogether to fine-tuning compression levels and bandwidth allocation when audio is enabled, you can use policy rules to control and manage the availability, quality, and cost of audio in client sessions.

Note The availability and quality of audio in client sessions is determined both by Terminal Services Configuration settings and by policies you configure through the Presentation Server Console. By default, Terminal Services settings are configured, whereas Presentation Server policies are not. This means that Terminal Services settings apply by default, making medium quality audio available in client sessions until you configure Presentation Server policies that override the Terminal Services settings. If configured, Presentation Server policies override Terminal Services settings.

Bandwidth Limits for Audio Throughput

Use policy rules to configure the amount of bandwidth you want to allocate to audio transfers between servers and clients. For example, you might want to create separate policy rules for groups of dial-up users and for those who connect over a LAN, accommodating the different amounts of bandwidth each group will have available.

To configure bandwidth limits for audio

1. In the Presentation Server Console, select the policy for which you want to configure the rule.
2. From the **Actions** menu, select **Properties**.
3. Expand the Bandwidth node and then the Session Limits node. Then select **Audio** to configure the rule and enter the bandwidth limit.

Audio Compression and Output Quality

As a rule of thumb, higher sound quality requires more bandwidth and higher server CPU utilization. You can use sound compression to effect a trade-off between sound quality and overall session performance. Use policy rules to configure the compression levels you want to apply to sound files.

You might want to consider creating separate policies for groups of dial-up users and for those who connect over a LAN. Over dial-up connections, where bandwidth typically is limited, users likely care more about download speed than sound quality. For such users, create a policy for dial-up connections that applies high compression levels to sound, and another for LAN connections that applies lower compression levels.

To configure audio compression and output quality

1. In the Presentation Server Console, select the policy for which you want to configure the rule.
2. From the **Actions** menu, select **Properties**.
3. Select **Client Devices > Resources > Audio > Sound quality** and configure the rule.

Choose from the following levels of sound quality:

Low sound quality; best performance. This setting is recommended for low-bandwidth connections. This setting causes any sounds sent to the client to be compressed to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Medium setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

Medium sound quality; good performance. This setting is recommended for most LAN-based connections. This setting causes any sounds sent to the client to be compressed to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device.

High sound quality; lowest performance. This setting is recommended for connections only where bandwidth is plentiful and sound quality is important. This setting allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.

Note **High sound quality** increases bandwidth requirements by sending more audio data to clients and increases server CPU utilization.

By default, the Medium sound quality level is selected.

Digital Dictation Support

For users to take and play back digital dictations in client sessions, both audio input (for microphones) and output (for speakers) must be enabled. Audio input and output are controlled by two separate policies; you must configure both to ensure that audio input and output are enabled.

To enable audio input for client sessions

1. Select the policy for which you want to enable audio input.
2. From the **Actions** menu, select **Properties**.
3. Select **Client Devices** > **Resources** > **Audio** > **Microphones**.
4. Select **Enabled** and **Use client microphones for audio input**.
5. Click **OK** when you are done.

Note Microphone input is supported on Citrix Presentation Server Clients for Windows, Windows CE, and Linux. The Clients for Linux and Windows CE do not support Philips SpeechMike products, nor does Citrix Presentation Server on 64-bit operating systems.

By default, when you configure this rule, audio input is enabled on client devices. Users can override the policy and disable their microphones by selecting No in the Client Audio Security dialog box.

Users of Program Neighborhood and Program Neighborhood Agent access this dialog box from the Program Neighborhood Connection Center (for seamless connections), or from either the Program Neighborhood Connection Center or the client's system menu (for non-seamless connections). Users of other Citrix Presentation Server Clients are automatically presented with the same dialog box at the beginning of their sessions.

To enable audio output for client sessions

1. In the Presentation Server Console, select the policy for which you want to enable audio output.
2. From the **Actions** menu, select **Properties**.
3. Select **Client Devices > Resources > Audio > Turn off speakers**. By default, the client speakers are turned off because this property is enabled.
4. Select **Disabled** and click **OK**.

Microphones and Speakers

You control audio input (for microphones) and output (for speakers) on client devices with two separate policies. This allows you to implement separate connection policies, for example, for users of mobile devices and for users who connect over a LAN. For the mobile user group, you may want to enable audio input but disable audio output. This allows mobile users to record notes from the field, but prevent the server from sending audio to the mobile devices by disabling audio output, ensuring better session performance.

On the client, users control audio input and output in a single step—by selecting an audio quality level from the **Settings** dialog box (for Program Neighborhood) or from the **Properties** dialog box (for Program Neighborhood Agent).

Configuring Support for Active Directory Federation Services (ADFS)

Important This guide does not document how to install ADFS. You should have a working ADFS installation, with external account users able to access ADFS-enabled Web applications in a resource partner.

Before you create an ADFS site, you must carry out the following steps.

Disregarding any of them can cause failure.

- Synchronize the clocks on the account partner federation server and the resource partner federation server to within five minutes of each other. If not, the security tokens generated by the account partner may not be accepted by the resource partner because the tokens appear to have expired. To avoid this problem, both organizations should synchronize their servers with the same Internet time server.
- Ensure the resource federation and Web servers can access the Certificate Authority's Certificate Revocation Lists (CRLs). ADFS may fail if the servers cannot ensure that a certificate has not been revoked.
- Ensure all servers within your deployment are trusted for delegation.
- Set up shadow accounts in the resource partner domain for each external user who can authenticate to the Web Interface through ADFS.
- Install Citrix Presentation Server 4.5, ensuring that the XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.
- Set up a trust relationship between the server running the Web Interface and any other servers in the farm running the Citrix XML Service that the Web Interface contacts.
- For security reasons, you must configure all servers running Presentation Server for constrained delegation. To provide users with access to resources on those servers you must add the relevant services to the Services list using the MMC Active Directory Users and Computers snap-in.

For more information about these tasks and configuring support for ADFS, see *Appendix B* of the *Citrix Web Interface Administrator's Guide* and the Citrix Knowledge Center article CTX110784, "Service Principal Names and Delegation in Presentation Server."

Securing Server Farms

The guidelines outlined in this chapter provide general direction when planning secure Citrix environments. Be sure to consult with your organization's security experts for a comprehensive security strategy that best fits your needs.

Securing Access to Your Servers

An important first step in securing your server farm is securing access to the servers. This section includes recommendations for securing access.

Securing the Presentation Server Console. The Presentation Server Console can be used to connect to any server in your farm. Run the console only in environments where packet sniffing cannot occur. Also, ensure that only administrators have access to the console. You can set NTFS permissions so that non-administrators do not have Execute permission for the console executable (Ctxload.exe).

Using NTFS partitions. To ensure that appropriate access control can be enforced on all files installed by Citrix Presentation Server, install Presentation Server only on NTFS-formatted disk partitions.

Installing and configuring the SNMP service. The SNMP service is not installed by default on computers running Windows Server 2003. If you install this service, you must configure the SNMP community string. You may also want to create a white list that limits the remote IP addresses that have access to the SNMP service.

The Windows SNMP service has many read/write privileges by default; however, you must give read/create permissions to the SNMP service for administrative tasks, such as logoff and disconnect through Network Manager. If you use Network Manager or other SNMP management software for monitoring the server only (and not remote management), Citrix recommends that the privileges be read only. If no SNMP consoles are used, do not install SNMP components on the server.

You can configure the SNMP community and designated management consoles to prevent unauthorized access. Configure SNMP agents to accept traps from known SNMP consoles only.

Note You can block incoming SNMP traffic from the Internet by using a firewall that prevents passage of traffic on UDP ports 161 and 162.

Trusted Server Configuration. This feature identifies and enforces trust relations involved in client connections. This can be used to increase the confidence of client administrators and users in the integrity of data on client devices and to prevent the malicious use of client connections. When this feature is enabled, clients can specify the requirements for trust and determine whether or not they trust a connection to the server. For more information about this feature, see the *Clients for Windows Administrator's Guide*.

Securing the Data Store

One of the most important aspects of securing your server farm is protecting the data store. This involves not only protecting the data in the data store database but also restricting who can access it. In general:

- Users who access your farm's servers do not require and should not be granted any access to the data store.
- When the data store connection is a direct one (that is, no intermediary server is used), all of the servers in the server farm share a single user account and password for accessing the data store. Select a password that is not easy to deduce. Keep the user name and password secure and give it to administrators only to install Presentation Server.

Caution If the user account for direct mode access to the database is changed at a later time, the Citrix IMA Service fails to start on all servers configured with that account. To reconfigure the Citrix IMA Service password, use the **dsmaint config** command on each affected server. For information about the **dsmaint config** command, see "DSMAINT" on page 322.

More specific Citrix recommendations for securing the data store vary depending on the database you use for the data store. The following sections discuss security measures to consider for each of the database products Presentation Server supports.

Microsoft Access. For an Access data store, the default user name is "citrix" and the password is "citrix." If users have network access to the data store server, change the password using **dsmaint config** and keep the information in a safe place.

Important Be sure to create a backup of your data store before using **dsmaint config** to change the password on your data store.

Microsoft SQL Server. The user account that is used to access the data store on Microsoft SQL Server has public and db_owner roles on the server and database. System administrator account credentials are not needed for data store access; do not use a system administrator account because this poses an additional security risk.

If the Microsoft SQL Server is configured for mixed mode security, meaning that you can use either Microsoft SQL Server authentication or Windows authentication, you may want to create a Microsoft SQL Server user account for the sole purpose of accessing the data store. Because this Microsoft SQL Server user account would access only the data store, there is no risk of compromising a Windows domain if the user's password is compromised.

Note For high-security environments, Citrix recommends using only Windows authentication.

Important For improved security, you can change the user account's permission to db_reader and db_writer after the initial installation of the database with db_owner permission. Changing the user account's permission from db_owner may cause problems installing future service packs or feature releases for Presentation Server. Be sure to change the account permission back to db_owner before installing a service pack or feature release for Presentation Server.

Microsoft SQL Server 2005 Express Edition. Windows authentication is supported for the Microsoft SQL Server 2005 Express Edition database. For security reasons, Microsoft SQL Server authentication is not supported. For further information, consult Microsoft documentation. The user name and password typically is the local system Administrator account. If users have access to the data store server, change the password with the command **dsmaint config** and keep the information in a safe place.

Oracle. If the data store is hosted on Oracle, give the Oracle user account used for the server farm "connect" and "resource" permissions only. System administrator (system or sys) account permissions are not needed for data store access.

IBM DB2. If the data store is hosted on IBM DB2, give the DB2 user account used for the server farm the following permissions:

- Connect database
- Create tables
- Register functions to execute to database manager's process
- Create schemas implicitly

System administrator (DB2Admin) account permissions are not needed for data store access.

Securing Network Communications

Network communication between servers and clients can be a security risk in any enterprise environment. The following sections discuss the security components that are available for enhancing the security of network communications in your server farm. Depending on your security needs, you can incorporate the following network communication security components when designing Citrix Presentation Server deployments:

- At the client-server level inside your network:
    - By encrypting the Independent Computing Architecture (ICA) protocol using SecureICA
    - SSL/TLS encryption
- At the network level, when clients are communicating with your farm remotely across the Internet:
    - The Secure Gateway
    - Secure Ticket Authority
    - Network firewalls

Securing Client-Server Communications

There are two methods of securing client-server communications: SecureICA and SSL/TLS encryption.

By default, all client-server communications are set to Basic ICA protocol encryption. The Basic setting obfuscates data but does not provide industry standard encryption. You can increase the level of SecureICA encryption up to 128-bit and/or add SSL/TLS encryption.

The difference between the two types of client-server encryption is as follows:

- **SecureICA.** The SecureICA feature encrypts the information sent between a server running Citrix Presentation Server and a client. In general, increase the level of ICA protocol encryption when you want to secure internal communication within a LAN or a WAN, or you want to secure internal access to an intranet. Increasing the level of ICA protocol encryption ensures the confidentiality of session data, but it does not perform any authentication.
- **SSL /TLS protocols.** SSL/TLS protocols can protect you from internal and external threats, depending on your network configuration. Citrix recommends that you enable SSL/TLS protocols if you have clients that communicate with your farm remotely, across the Internet. Enabling SSL/TLS ensures the confidentiality, authentication, and integrity of session data.

If you want protection against both internal and external threats, you may want to enable SecureICA and SSL encryption.

Both protocols are enabled in two places:

- On the server side, when you publish an application or resource.
- On the client side (for Program Neighborhood only). The Web Interface and Program Neighborhood Agent automatically detect and use the settings specified on the server (that is, when you publish a resource).

The settings you specify for client-server encryption can interact with any other encryption settings in Presentation Server and your Windows operating system. If a higher priority encryption level is set on either a server or client device, settings you specify for published resources can be overridden. The most secure setting out of any of the settings below is used:

- The setting in Terminal Services Configuration (TSCC)
- The Presentation Server Console policy setting that applies to the connection
- The client-server setting (that is, the level you set when you publish a resource)
- The Microsoft Group Policy

When you set an encryption level, make sure that it is consistent with the encryption settings you specified elsewhere. For example, any encryption setting you specify in the TSCC or connection policies cannot be higher than the application publishing setting.

If the encryption level for an application is *lower* than what you specified through the TSCC and connection policies, the TSCC settings and the policies override the application settings.

Using SecureICA

By default, client-server communications are obfuscated at a basic level through the SecureICA feature, which can be used to encrypt the ICA protocol.

The ICA protocol is the protocol that clients use to format user input (keystrokes, mouse clicks, and so on) and address it to a server farm for processing. Server farms use the ICA protocol to format application output (display, audio, and so on) and return it to the client device.

You can increase the level of encryption for the ICA protocol when you publish a resource or after you publish a resource.

In addition to situations when you want to protect against internal security threats, such as eavesdropping, you may want to use ICA encryption in the following situations:

- You need to secure communications from devices that use Microsoft DOS or run on Win16 systems
- You have older devices running client software that cannot be upgraded to use SSL
- As an alternative to SSL/TLS encryption, when there is little risk of a "man-in-the-middle" attack

When traversing public networks, Citrix does not recommend SecureICA as your only method of encryption. Citrix recommends using SSL/TLS encryption for traversing public networks. Unlike SSL/TLS encryption, SecureICA, used on its own, does not provide authentication of the server. Therefore information could, in theory, be intercepted as it crosses a public network and then be rerouted to a counterfeit server. Also, SecureICA does not check data integrity.

Enabling SSL/TLS Protocols

If clients in your environment communicate with your farm across the Internet, Citrix recommends enabling SSL/TLS encryption when you publish a resource. If you want to use SSL/TLS encryption, you must use either the SSL Relay feature or the Secure Gateway to relay ICA traffic to the computer running Presentation Server.

The nature of your environment may determine the way in which you enable SSL:

- For clients communicating with your farm remotely, Citrix recommends that you use the Secure Gateway to pass client communications to the computer running Presentation Server. The Secure Gateway can be used with SSL Relay on the computer running Presentation Server to secure the Secure Gateway to Presentation Server traffic, depending on your requirements.
- For clients communicating with your farm internally, you can do one of the following to pass client communications to the computer running Presentation Server:
    - Use the Secure Gateway with an internal firewall and place your farm behind the firewall
    - Use the SSL Relay to secure the traffic between servers in your farm

In larger environments, it may not be convenient to use SSL Relay because doing so requires storing certificates on every server in your farm. In large environments, you may want to use the Secure Gateway with an internal firewall if you are concerned with internal threats.

Regardless of whether you use the Secure Gateway or SSL Relay, if you want to use SSL, you must select the **Enable SSL and TLS protocols** setting when you publish an application — see the section that follows.

For information about SSL Relay, see “Using Citrix SSL Relay” on page 206. For information about the Secure Gateway, see “Using the Secure Gateway” on page 211. If you are using Web Interface in conjunction with the Secure Gateway, see the information about SSL in the *Secure Gateway Administrator’s Guide* and the *Web Interface Administrator’s Guide*.

Increasing the Level of Client-Server Security

The following procedure explains how to enable SecureICA (ICA protocol encryption) or enable SSL/TLS encryption *after* you publish an application. For information about setting encryption during application publishing, see the publishing applications topics in the *Access Management Console help*.

To increase the level of client-server security

1. In the Access Management Console, select a published application in the left pane by selecting **Citrix Access Management Console** > **Citrix Resources** > **Presentation Server** > ***your farm name*** > **Applications** > ***application name***.
2. From the **Action** menu, select **Modify application properties** > **Modify all properties**.
3. In the **Application Properties** dialog box, select **Advanced** > **Client options**.
4. In the Connection encryption section, do one or more of the following:
    - Select the **Enable SSL and TLS protocols** check box. This option requests the use of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols for clients connecting to the published application.
    - In the Encryption section, select a higher level of encryption from the drop-down list box.
    - (For Program Neighborhood only. Optional.) Select the **Minimum requirement** check box, which is available only if you increase the level of ICA protocol encryption. The **Minimum requirement** check box sets a requirement that Program Neighborhood clients connecting to a published application use the specified level of encryption or higher. This means the following:
        - If you do not select the **Minimum requirement** check box, Program Neighborhood's connections to the server are encrypted at the level that you set in Program Neighborhood. If the encryption level on the server and in Program Neighborhood do not match, you can still connect. The encryption settings you specify in Program Neighborhood override the encryption level set for the application.
        - If you select the **Minimum requirement** check box, Program Neighborhood's connections to the server must be encrypted at the same level that you set on the server, or the server refuses the client's transmission and the session is dropped.

5. Click **OK**.

If you are using Program Neighborhood as one of the clients in your environment, you must also enable encryption on the client side. See the *Program Neighborhood help* for more information.

Setting a Policy for SecureICA

If you are using SecureICA and you want to ensure that ICA traffic is always encrypted at a certain level, you can set a policy for encryption. Creating a SecureICA policy prevents you from accidentally publishing a resource at a lower level of encryption. If you have this policy enabled and you publish a resource at a lower level of encryption than the policy requires, the server rejects client connections. For clients that take their encryption settings from the server, such as the Web Interface and Program Neighborhood Agent, this can be problematic.

Therefore, Citrix recommends as a best practice, that if you enable an encryption policy, you publish applications (or resources) by replicating an existing published application and editing it so as to replace the application with the new application you want to publish.

To set a policy for ICA encryption

1. Create the policy:
   A. In the left pane of the Presentation Server Console, select **Policies**.
   B. From the **Actions** menu, click **New > Policy**.
2. Configure rules for the policy:
   A. Select the policy name in the right pane and on the **Actions** menu, click **Properties** to open its **Properties** page.
   B. From the list of folders in the left pane, select **Security** > **Encryption** > **SecureICA encryption**.
   C. Select **Enabled** and then select the encryption level you want for this policy from the **Encryption Level** list box.
3. Enable the policy by applying a filter.

For additional details about creating policies in general, see the *Presentation Server Console help*.

Using Citrix SSL Relay

Use Citrix SSL Relay to provide end-to-end Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption between specific servers and clients.

In general, use SSL Relay when:

- You want to secure communications with servers that host the Citrix XML Service
- You have a small number of servers to support (five or fewer)
- You do not need to secure access at a DMZ
- You do not need to hide server IP addresses or you are using Network Address Translation (NAT)
- You need end-to-end encryption of data between clients and servers

SSL Relay provides end-to-end encryption of the communication between the client and the computer running Citrix Presentation Server. You must install and configure SSL Relay and the appropriate server certificate on each server running Citrix Presentation Server within the server farm.

SSL Relay operates as an intermediary in the communications between the client and the Citrix XML Service running on each server. Each client authenticates the SSL Relay by checking the relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. SSL Relay decrypts the requests and passes them to the server.

When returning the information to the client, the server sends all information through SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify that each communication is not tampered with.

Deploying Citrix SSL Relay

Citrix SSL Relay can secure communications between clients, servers running the Web Interface, and computers running Citrix Presentation Server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

Note If you are using Microsoft Certificate Authority to assist in setting up SSL Relay, you can use the SSLAutoConfig tool, which is located in the Support folder on the server installation CD. For more information about how to use SSLAutoConfig, see the *Advanced Concepts Guide for Citrix Presentation Server*.

You must complete the following four steps to successfully deploy SSL Relay.

Step 1. Obtaining Server and Root SSL Certificates

A separate server certificate is needed for each server running Citrix Presentation Server on which you deploy the Citrix SSL Relay. The server certificate identifies a specific computer, so you must know the fully qualified domain name (FQDN) of each server. Certificates must be signed by a trusted entity called a Certificate Authority (CA). In addition to installing a server certificate on each server, you must install the root certificate from the same CA on each client device that will communicate with SSL Relay. Root certificates are available from the same CAs that issue the server certificates. You can install server and client certificates from a CA that is bundled with your operating system, an enterprise CA (a CA that your organization makes accessible to you), or a CA not bundled with your operating system. Consult your organization's security team to find out which of the following methods they require for obtaining certificates.

Choosing an SSL Certificate Authority

You can obtain certificates for your servers and client devices in the following ways.

- **Obtaining certificates from a CA bundled with the operating system.** Some of the newer Windows operating systems (for example, Windows Server 2003) include native support for many CAs. If you choose to install the certificate from a bundled CA, double-click the certificate file and the Windows Certificate Store wizard installs the server certificate on your server. For information about which operating systems include native support, see your Microsoft documentation.
- **Obtaining certificates from an enterprise CA.** If your organization makes a CA accessible to you for use, that CA will appear in your list of CAs. Double-click the certificate file and the Windows Certificate Store wizard installs the server certificate on your server. For more information about whether or not your company uses an enterprise CA, consult your security team.

- **Obtaining certificates from a CA not bundled with the operating system.** Certificates from CAs that are not bundled with your operating system or made accessible to you by your organization must be manually installed on both the server running Citrix SSL Relay and on each client device. For instructions about installing certificates from an external CA, see the documentation for the servers and clients in your configuration. Alternatively, you can install certificates using Active Directory or the IIS snap-in.
    - **Using Active Directory.** If your computers belong to an Active Directory server, you can install the certificates using Active Directory. For instructions about how to use Active Directory to install your certificates, see your Microsoft documentation.
    - **Using the IIS snap-in.** You can use the Microsoft Web Server Certificate wizard in the IIS snap-in to request and import a certificate. For more information about using this wizard, see your Microsoft documentation.

Acquiring a Signed SSL Certificate and Password

After you choose a CA, generate a *certificate signing request* (CSR) and send it to the CA using the Web server software that is compatible with the CA. For example, if you are using the IIS snap-in to obtain your certificates, you can use Microsoft Enterprise Certificate Services to generate the CSR. The CA processes the request and returns the signed SSL certificate and password to you. For information about what software you can use to generate the CSR, consult the documentation for your chosen CA.

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

After acquiring the signed certificate and password from your CA, install the certificates on each server and client in your configuration using the appropriate method.

Step 2. Installing the Certificate

Install the server certificate on each server. SSL Relay uses the same registry-based certificate store as IIS, so you can install certificates using IIS or the Microsoft Management Console (MMC) Certificate Snap-in. When you receive a certificate from the CA, you can restart the Web Server Certificate wizard in IIS and the wizard will install the certificate. Alternatively, you can view and import certificates on the computer using the MMC and adding the certificate as a standalone snap-in.

Step 3. Changing the SSL Port, if Necessary

To use the SSL Relay and Internet Information Services (IIS) on the same server, you must change the port number that IIS or the SSL Relay use. The Citrix SSL Relay uses TCP port 443, the standard port for SSL connections. Most firewalls open this port by default. You can optionally configure the SSL Relay to use another port. Be sure that the port you choose is open on any firewalls between the client devices and the server running the SSL Relay.

Important Microsoft Internet Information Services (IIS) Version 6.0 is installed by default on Windows Server 2003 and allocates port 443 for SSL connections. To run SSL Relay on a server running Windows Server 2003, you must configure IIS to use a different port or configure the SSL Relay to use a different port. You must install a server certificate on IIS before you change the port number. The following procedure includes instructions for adding a server certificate to IIS. You can use the same server certificate with IIS and the SSL Relay.

For instructions to change the SSL port for Internet Information Services Version 6.0, see the relevant Microsoft documentation.

To change the Citrix SSL Relay port number

1. On the server, click the **Citrix SSL Relay Configuration Tool** button on the ICA Toolbar to start the SSL Relay configuration tool.
2. On the **Connection** tab, type the new port number in the **Relay Listening Port** box.
3. Click **OK**.

See the *Citrix Web Interface Administrator's Guide* for the procedure to reconfigure servers running the Web Interface with the new port number.

To run SSL Relay on port 443 without using HTTPS

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

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

Note When you install Citrix Presentation Server, members of the User group are allowed to edit registry entries in the registry hive HKEY_LOCAL_MACHINE\SOFTWARE\Secure\Citrix\Citrix SSL Relay. You can use the Microsoft Security Configuration and Analysis tool to prevent members of the User group from editing these registry entries.

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

Step 4. Configuring SSL Relay

In the SSL Relay Configuration tool, select the server certificate and allowed ciphersuites, according to your security policy. Change the target address or port, or add additional addresses for redundancy.

To configure the SSL Relay

1. From the Citrix Programs group on the **Start** menu, choose **Administration Tools** and then **Citrix SSL Relay Configuration Tool** to start the SSL Relay Configuration tool.
2. On the **Relay Credentials** tab, select the server certificate.
3. On the **Connection** tab, configure the fully qualified domain name (or IP address) and port combinations to which the SSL Relay forwards decrypted data. The SSL Relay forwards packets only to the servers and ports listed on this tab.
4. On the **Ciphersuites** tab, select which ciphersuites to allow.

For more information, see the online help for the SSL Relay configuration tool.

Using the Secure Gateway

Use the Secure Gateway to provide SSL/TLS encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser and the Web server. Using the Secure Gateway makes firewall traversal easier and improves security by providing a single point of entry and secure access to your server farms.

In general, you use the Secure Gateway when:

- You want to hide internal IP addresses
- You want to secure public access to your farm's servers
- You need two-factor authentication (in conjunction with the Web Interface)

Using the Secure Gateway provides the following benefits:

- Secure Internet access
- Removes the need to publish the addresses of every server running Citrix Presentation Server
- Simplifies server certificate management
- Allows a single point of encryption and access to the servers

Use the Secure Gateway to create a gateway that is separate from the computers running Citrix Presentation Server. Establishing the gateway simplifies firewall traversal because ICA traffic is routed through a widely accepted port for passage in and out of firewalls. The Secure Gateway provides increased scalability.

However, because ICA communication is encrypted only between the client and the gateway, you may want to use SSL Relay to secure the traffic between the gateway and the servers running Citrix Presentation Server, including the servers hosting the Citrix XML Service.

For more information about implementing and configuring the Secure Gateway, see the *Secure Gateway Administrator's Guide*.

Using the Secure Ticket Authority

The Secure Ticket Authority (STA) is responsible for issuing session tickets in response to connection requests for published resources on Citrix Presentation Server. These session tickets form the basis of authentication and authorization for access to published resources.

When you install Presentation Server, you also install the STA. If Citrix Presentation Server is installed on a server that has an older version of the STA, it is upgraded to the new version. The STA is embedded within the Citrix XML Service.

Important If you are securing communications between the Secure Gateway and the STA, ensure that you install a server certificate on the server running the STA and implement SSL Relay. In most cases, internally generated certificates are used for this purpose.

Displaying Secure Ticket Authority Statistics

In addition to monitoring the performance of the server running the Secure Gateway, Citrix recommends monitoring the performance of the server running the Secure Ticket Authority (STA) as part of your administrative routine.

To display STA performance statistics

1. Access the Performance Monitor.
2. Right-click in the right pane and click **Add Counters**.
3. For the location of the performance counters, select **Use local computer counters**.
4. Select **Secure Ticket Authority** from the **Performance Object** drop-down list.
5. Select the performance counters you want to monitor and click **Add**.
6. Click **Close**.
7. Use the Windows Performance Console controls that appear at the top of the right pane to switch views and add counters.

Identifying Entries in the STA Log

The STA logs fatal errors to its application log, which is located in the \inetpub\scripts directory. When creating a log, the STA uses the following format for naming log files:

sta*yyyymmdd***-***xxx***.log**
where *yyyy* is the year, *mm* is the month, and *dd* is the day of the log file creation.

The first time the STA is loaded, it creates a log file.

To view entries in the STA log, use a plain-text editor to open the log file.

If the STA does not create a log file, it may be due to lack of write privileges to the \inetpub\scripts directory.

Configuring Network Firewalls

In addition to physically securing servers, most organizations install network security measures including firewalls to isolate servers running Citrix Presentation Server and Web browsers from the Internet and publicly accessible networks. To deploy Citrix Presentation Server on internal networks, secure communications between the client and server by means of SSL/TLS or other security measures.

For more information about configuring firewalls for your server farm, see the *Advanced Concepts Guide for Citrix Presentation Server*.

Configuring TCP Ports

The table below lists the TCP/IP ports that servers, Citrix Presentation Server Clients, the IMA Service, and other Citrix services use in a server farm. This information can help you configure firewalls and troubleshoot port conflicts with other software.

Communication	Default port	Configuration
Citrix XML Service	80	See “Step 9: Configuring the Citrix XML Service Port” on page 70 for configuration instructions.
Access Management Console	135	Not configurable.
Citrix SSL Relay	443	See “Step 3. Changing the SSL Port, if Necessary” on page 209 for configuration instructions.
ICA sessions (clients to servers)	1494	See “ICAPORT” on page 328 for instructions about changing the port number.
Client-to-server (directed UDP)	1604	Not configurable.

Communication	Default port	Configuration
Server to server	2512	See "Citrix Presentation Server Commands" on page 283 for information about the IMAPORT command.
Presentation Server Console to server	2513	See "Citrix Presentation Server Commands" on page 283 for information about the IMAPORT command.
Session reliability	2598	See "Session Reliability" on page 180.
Server to Microsoft SQL or Oracle server	139, 1433, or 443 for MS-SQL	See the documentation for your database software.
License Management Console	8082	See the *Getting Started with Citrix Licensing Guide* for more information.
Server to license server	27000	In the console, open the farm or server properties page, and select License Server.

Configuring User Authentication

Part of securing your server farm is making sure that only properly authenticated users can access your servers and resources.

Configuring Authentication for Workspace Control

If users log on using smart cards or pass-through authentication, you must set up a trust relationship between the server running the Web Interface and any server in the farm that the Web Interface accesses for published applications. Without the trust relationship, the Disconnect, Reconnect, and Log Off ("Workspace Control") commands fail for those users logging on with smart card or pass-through authentication. For more information about Workspace Control, see "Providing Users with Workspace Control" on page 164.

You do not need to set up a trust relationship if your users authenticate to the Web Interface or Program Neighborhood Agent by typing in their credentials.

To set up the trust relationship, open the server's **Properties** page in the Access Management Console, choose **XML Service** in the left pane, and select **Trust requests sent to the XML Service**. The Citrix XML Service communicates information about published applications between servers running the Web Interface and servers running Citrix Presentation Server.

If you configure a server to trust requests sent to the Citrix XML Service, consider these factors:

- The trust relationship is not necessary unless you want to implement Workspace Control and your users log on using smart cards or pass-through authentication.
- Enable the trust relationship only on servers directly contacted by the Web Interface. These servers are listed in the Web Interface Console.
- When you set up the trust relationship, you depend on the Web Interface server to authenticate the user. To avoid security risks, use SSL Relay, IPSec, firewalls, or any technology that ensures that only trusted services communicate with the Citrix XML Service. If you set up the trust relationship without using IPSec, firewalls, or other security technology, it is possible for any network device to disconnect or terminate client sessions.
- Configure SSL Relay, IPSec, firewalls, or other technology that you use to secure the environment so that they restrict access to the Citrix XML Service to only the Web Interface servers. For example, if the Citrix XML Service is sharing a port with IIS, you can use the IP address restriction capability in IIS to restrict access to the Citrix XML Service.

Configuring Kerberos Logon

Citrix Presentation Server Clients for Windows feature enhanced security for pass-through authentication. Rather than sending user passwords over the network, pass-through authentication leverages Kerberos authentication. Kerberos is an industry-standard network authentication protocol built into the Windows operating systems. Kerberos logon offers security-minded customers the convenience of pass-through authentication combined with secret-key cryptography and data integrity provided by industry-standard network security solutions.

System requirements. Kerberos logon requires Presentation Server 3.0 or later and Citrix Presentation Server Clients for Windows Version 8.*x* or later. It works only between clients and servers that belong to the same or to trusted Windows domains. Servers must also be *trusted for delegation*, an option you configure through the Active Directory Users and Computers management tool.

Kerberos logon is not available:

- If you use the following options in Terminal Services Configuration:
  - **Use standard Windows authentication**
  - **Always use the following logon information** or **Always prompt for password**
- If you route connections through Secure Gateway
- If the server running Citrix Presentation Server requires smart card logon

Kerberos requires Citrix XML Service DNS address resolution to be enabled for the server farm or reverse DNS resolution to be enabled for the Active Directory domain.

To enable Citrix XML Service DNS address resolution

1. In the scope pane of the Access Management Console, select the Farm node and select **Action** > **Modify farm properties > Modify all properties**.
2. Open the **Presentation Server** page from the farm's **Properties** list and select the **General** option.
3. In the details pane, select the option **XML Service DNS address resolution**.
4. Click **OK**.

To disable Kerberos logon to a particular server

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

To disable Kerberos logon to a particular server, set the following registry key on the server:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Logon\DisableSSPI = 1

You can configure the Presentation Server Client for Windows to use Kerberos with or without pass-through authentication. For more information about client configuration, see the *Clients for Windows Administrator's Guide*.

Using Smart Cards with Citrix Presentation Server

You can use smart cards in your Citrix Presentation Server environment. Smart cards are small plastic cards with embedded computer chips.

In a Presentation Server environment, smart cards can be used to:

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

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

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

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

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

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

Note Citrix Presentation Server does not support RSA Security Inc.'s PKCS (Public-Key Cryptography Standard) #11 functional specification for personal cryptographic tokens.

You can also use smart cards with the Web Interface for Citrix Presentation Server. For details about configuring the Web Interface for smart card support, see the *Web Interface Administrator's Guide*.

Smart Card Requirements

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

The following components are required on the server:

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

These components are required on the device running the supported Citrix Presentation Server Client:

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

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

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

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

Configuring the Server

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

Smart cards are supported for authenticating users to published applications or for use within published applications that offer smart card functionality. Only the former is enabled by default upon installation of Citrix Presentation Server.

Setting Windows Policies for Smart Cards

Microsoft Windows supports two security policy settings for interactive logon to a server session. Citrix Presentation Server Client sessions can use the following policies:

- **Require smart card for interactive session logon.** This is a user policy that requires the user to insert a smart card for authentication.
- **Smart-card removal policy.** This is a computer policy that has three possible settings to determine the client device behavior when the user removes the smart card from the smart card reader:
  - None (no effect)
  - Lock Workstation (disconnects all user sessions)
  - Force Logoff (logs off all user sessions)

Configuring the Client

The following clients support smart cards:

- Citrix Presentation Server Clients for Windows
- Client for Linux
- Client for Windows-based terminals

To configure smart card support for users of these clients, see the administrator's guide for the clients in your environment.

Encrypting Sensitive Configuration Logging Data

Independent Management Architecture (IMA) is the underlying architecture used in Citrix Presentation Server for configuring, monitoring, and operating all Presentation Server functions. The IMA data store stores all Presentation Server configurations.

The IMA encryption feature protects administrative data used by the configuration logging feature. This information is stored in the IMA data store. For IT environments with heightened security requirements, enabling IMA encryption provides a higher degree of security for the configuration logging feature. One example would include environments that require strict separation of duties or where the Citrix Administrator should not have direct access to the configuration logging database.

IMA encryption is a farm-wide setting that applies to all servers in the farm once it is enabled. Consequently, if you want to enable IMA encryption, you must enable it on all servers in the farm. IMA encryption has the following components:

- **CTXKEYTOOL.** CTXKEYTOOL, also known as the IMA encryption utility, is command-line utility that you can use to manage IMA encryption and generate key files. CTXKEYTOOL is in the Support folder of the Server CD for Presentation Server.
- **A key file.** The key file is a file that contains the encryption key used to encrypt sensitive IMA data. You create the key file by using the CTXKEYTOOL, during Setup, or while changing farms (**chfarm**). To preserve the integrity of the encryption, Citrix recommends that you keep the key file in a secure location and that you do not freely distribute it.
- **A key.** The same valid IMA encryption key must be loaded on all servers in the farm if IMA encryption is enabled. After copying the farm's key file to a server, you load the key by using the CTXKEYTOOL, during Setup, or using the functionality in **chfarm**.

It is easier to enable IMA encryption as part of the installation process than after installation. Enabling IMA encryption after installation requires performing a manual process on each server. For information about installation methods when you are enabling IMA encryption during Setup in large-farm environments, see "Planning for IMA Encryption" on page 41.

Regardless of when you enable IMA encryption, the process has the same basic elements. At a high level, you perform the following tasks in the order given:

- Generate a key file
- Make the key file accessible to each server in the farm, or put it on a shared network location
- Load the key on to the server from the key file
- Enable IMA encryption

The sections that follow provide the following information about IMA encryption:

- How to use the IMA encryption utility (CTXKEYTOOL)
- How to enable IMA encryption after installation
- How to change farms
- How to back up farm keys
- Steps to perform if you installed Presentation Server as a local administrator when you enabled IMA encryption

Citrix recommends that, if you are enabling IMA encryption in environments that have multiple farms, you give the keys for each farm a different name.

Important Citrix strongly recommends backing up the farm key to a safe, secondary location. For information, see “Other IMA Encryption Features” on page 226.

Using the IMA Encryption Utility

Citrix provides a utility for performing various administrative functions after you install Citrix Presentation Server. This utility is known as the IMA encryption utility, and you run it from the CTXKEYTOOL command. You can use the IMA encryption utility to enable and disable the IMA encryption feature and generate, load, replace, enable, disable, and retrieve lost key files. You can also use the IMA encryption utility to check to see if a key is loaded on the local computer, if IMA encryption is enabled for the farm, and if your key matches the farm key. For more information about the command’s syntax, see “CTXKEYTOOL” on page 309.

Storing the IMA Encryption Utility Locally

The IMA encryption utility is in the Support folder of the Server CD for Presentation Server. If you want to run the utility locally, perform the following:

To copy the key to a local computer

1. Copy the CTXKEYTOOL.exe file from the Support folder of the Server CD for Presentation Server to your local computer.
2. Create a folder named Resource at the same level in your directory structure as the CTXKEYTOOL file.
3. Copy the entire **Support\Resource\en** folder from the Server CD to the Resource folder.

You can store the CTXKEYTOOL.exe file and its accompanying Resource\en folder anywhere on your computer, provided you maintain the same relative directory structure that they were stored in on the Server CD.

Enabling IMA Encryption after Installation

You can enable IMA encryption after you install or upgrade to Citrix Presentation Server 4.5. To enable IMA encryption, perform the following tasks:

- On any server in the farm, use the IMA encryption utility to generate a key
- Load the key on to that server and enable IMA encryption
- Load the key on subsequent servers on the farm

To generate a key and enable IMA encryption on the first server in a farm

1. On the server on which you want to enable IMA encryption, run the **generate** option of the CTXKEYTOOL command. The following is an example of the command line to use to accomplish this:

   ctxkeytool generate <*full UNC or absolute path, including the file name of the key you want to generate, to the location where you want to store the key file*>

   Citrix suggests naming the key after the farm it will be used on. For example, **farmakey.ctx**. Citrix also suggests saving the key to a folder that uses the name of your farm. For example, **Farm A Key**.
2. Press **Enter**. The following message appears indicating that you successfully generated a key file for that server, "Key successfully generated."

3. To obtain the key from the file and put it in the correct location on the server, run the **load** option of the CTXKEYTOOL command on the server on which you want to add the key. The following is an example:

   ctxkeytool load <*full UNC or absolute path, including the key file name, to the location where you stored the key file*>

4. Press **Enter**. The following message appears indicating that you successfully loaded the key on to that server, "Key successfully loaded." You are now ready to enable the IMA encryption feature in the data store.

5. Run the **newkey** option of the CTXKEYTOOL command to use the currently loaded key and enable the key.

   ctxkeytool newkey

6. Press **Enter**. The following message appears indicating that you successfully enabled the IMA encryption feature in the data store, "The key for this farm has been replaced. IMA Encryption is enabled for this farm."

   However, you must have a key on every server in the farm for IMA encryption to work correctly.

7. Continue on to the next procedure to load the key to each server, or, if you are enabling IMA encryption when you are running Setup on subsequent servers in the farm, see "Deploying Subsequent Servers" on page 73.

To load a key on subsequent servers in the farm

1. If you do not have the key file on a shared network location, on the next server on which you want to begin enabling IMA encryption, load the key file to the server from a diskette or a USB flash drive.

2. To obtain the key from the file and put it in the correct location on the server, run the **load** option of the CTXKEYTOOL command on the server on which you want to add the key. The following is an example:

   ctxkeytool load <*full UNC or absolute path, including the key file name, to the location where you stored the key file*>

3. Press **Enter**. The following message appears indicating that you successfully loaded the key on to that server, "Key successfully loaded."

   You do not need to enable IMA encryption again (using the **newkey** option) since you have already enabled it on one server in the farm.

4. Repeat this process on every server in the farm.

Storing the Key on a Shared Location

If you choose to store the key on a shared network location, Citrix recommends the following:

- Make sure that the folder has a meaningful name that specifies the name of the farm for which the key was created. This is especially important in situations when you follow the Citrix best practice recommendation of creating a unique key for farm.
- Make sure that the account you use to generate the key is the same as the account that will be used to install all the servers in the farm. You must use the same account for both tasks.
- Grant Read/Execute access to the key file to each machine that will be joining the farm and to the administrator performing the installation.

In addition, if you want to specify this key when you are enabling IMA encryption during Setup, you must specify it using a Universal Naming Convention (UNC) path.

The following procedures explain how to store a key on a shared network location and how to select that location when installing Presentation Server on subsequent servers. The procedures assume that you are performing an Autorun-based installation and generating a key from Setup while you are installing the first server on the farm. The guidelines provided in these steps apply to other situations in which you specify the key, such as **chfarm** and unattended installations.

To store the key on a network location

1. When you generate the key file, save it to a local directory (like you normally would).
2. After enabling IMA encryption on the server where you originally generated the key, copy the key file to the shared network location that you want to use for the subsequent server installations.
3. Grant Read/Execute access to the key file to each machine that will be joining the farm and to the administrator performing the installation.

For more information about enabling IMA encryption, see "Step 6: Enabling IMA Encryption" on page 65.

Changing Farms

If you need to move a server to a farm that has IMA encryption enabled, you must use the **chfarm** command. When you run **chfarm**, a wizard similar to the Presentation Server Setup wizard launches. This Setup wizard prompts you to specify a key the same way as product Setup does when you choose to enable IMA encryption. If, before running **chfarm**, you choose to load the new farm's key on to the server, note that adding a key to a server with the same name as an existing key overwrites the existing key.

If you are moving a server to a farm that does not have IMA encryption enabled, Setup does not prompt you to provide a key file and IMA encryption is automatically disabled on the server you are moving. For specific details on the IMA encryption options when changing farms, see "CHFARM" on page 305.

Enabling IMA Encryption as a Local Administrator

Citrix recommends that if you are going to enable IMA encryption during Setup and you want to connect to the data store indirectly, you install Citrix Presentation Server using a domain account that has local administrative privileges on the system.

You cannot enable IMA encryption when you join a farm, either during Setup or when changing farms, if you are logged in as a local administrator and you attempt to connect to the data store indirectly. If you use a local administrator account that is not part of the Citrix administrator group, then Setup issues a warning message. You can prevent this problem by doing one of the following:

- Creating a test domain and creating a domain user account for yourself, if you are installing Presentation Server on a test farm.
- Before you begin to install the second ("joining") server on the farm, open up the Access Management Console on the first server in the farm and configure all local administrators as Citrix administrators. This setting is not enabled by default. This task is explained in the procedure that follows.

This procedure is only required for farms on which you are connecting to the data store indirectly. You do not need to configure local administrators as Citrix administrators if you are connecting to the data store directly.

To configure local administrators as Citrix administrators

1. Expand the Presentation Server node in the Access Management Console.
2. In the left pane, under the Farm node, select the Administrators node and select **Action > New** > **Add administrator**. The Add Citrix Administrator wizard appears.
3. On the **Add Citrix Administrator** page, which is the first page of the wizard, select the **Add local administrators** check box.

   Selecting this option adds all previously created local administrators to the Citrix administrators group and automatically adds any local administrators you create going forward to the Citrix administrators group.
4. Continue enabling other options in the wizard, and click **Finish**. See the Access Management Console help for more details about adding new Citrix administrator accounts.

Other IMA Encryption Features

This section discusses other tasks you may want to perform as you use the IMA encryption feature, including the following:

- Backing up keys
- Retrieving lost, deleted, or accidentally overwritten keys
- Disabling and reenabling IMA encryption

Backing Up Keys

Citrix strongly recommends backing up the farm key to a safe, secondary location, such as a CD, immediately after you generate a key. You can create a copy of the key file when you create it, or you can back up the farm key by using the **backup** option in the CTXKEYTOOL as described on page 309.

Retrieving Lost Keys

It is possible to recreate a key file that you have accidentally deleted, if, for example, you need it to join a new server to the farm. This is for Since all servers in the same farm use the same key, you can obtain a key from another server on the farm. Presentation Server does not allow you to access keys. Consequently, to obtain the lost key, you must recreate the entire key file by running the **backup** option on any server in the farm with IMA encryption that has the key and is functioning properly. For more information, see "CTXKEYTOOL" on page 309.

Disabling IMA Encryption

You can disable IMA encryption by running the **ctxkeytool disable** command on any server in the farm. Since IMA encryption is a farm-wide feature, you do not need to run this command on every server in the farm. Running it on one server, disables the feature for all servers.

If you disable IMA encryption, to access Configuration Logging database, you must re-enter the password for the Configuration Logging database. In addition, no configuration information is logged until you reenter your database credentials in the Access Management Console. For information about updating the password for the Configuration Logging database, see the *Access Management Console Help*.

If you want to reenable IMA encryption after you disabled it, use the **enable** option of the CTXKEYTOOL command. After running the **enable** option, Citrix recommends that you always run the **query** option to verify that IMA encryption is enabled. For more information, see “CTXKEYTOOL” on page 309.

CHAPTER 9

Maintaining Server Farms

As a Citrix administrator, in addition to securing your server farm, publishing resources, and managing user sessions, you must also configure and maintain your server farm. This chapter discusses how to perform a number of the tasks associated with this, such as logging administrative tasks, monitoring system health, and managing the usage of system resources. For additional procedural information, see the help for the management consoles.

Logging Administrative Changes

The Configuration Logging feature allows you to keep track of administrative changes made to your server farm environment. By generating the reports that this feature makes available, you can determine what changes were made to your server farm, when they were made, and which administrators made them. This is especially useful when multiple administrators are modifying the configuration of your server farm. It also facilitates the identification and, if necessary, reversion of administrative changes that may be causing problems for the server farm.

When this feature is enabled for a licensed server farm, administrative changes initiated from the Access Management Console, the Presentation Server Console, some command-line utilities, and tools custom built with the MPSSDK and CPSSDK lead to the creation of log entries in a central *Configuration Logging database*.

Before you enable the Configuration Logging feature, Citrix recommends that you decide the following:

1. Determine the level of security and control you need over the configuration logs. This determines if you need to set up additional database user accounts and if you want to make Presentation Server administrators enter credentials before clearing logs. See “Clearing the Log” on page 236.
2. Determine how strictly you want to log tasks. For example, if you want to log administrative tasks and if you want to allow administrators to make changes to a farm if the task cannot be logged (for example, if the database is disconnected). See “Setting the Configuration Logging Properties” on page 234.

The following section describes how the Configuration Logging feature and the database that supports it need to be configured.

Enabling Configuration Logging

The following sections detail the steps that are needed before Configuration Logging reports can be generated.

- Set up the Configuration Logging database
- Define the Configuration Logging database access permissions
- Configure the Configuration Logging database connection
- Test the connection to the Configuration Logging database
- Set the Configuration Logging properties
- Delegate administrative permissions, as needed

Note To securely store the credentials used for accessing the Configuration Logging database, you can enable the IMA encryption feature when you deploy your server farm. After this is enabled, however, you cannot disable it without losing the data it encrypted. Citrix recommends that you configure IMA encryption before The Configuration Logging feature is configured and used.

Setting up the Configuration Logging Database

For Citrix Presentation Server 4.5, the Configuration Logging feature supports Microsoft SQL Server 2000 and 2005 and Oracle Version 9.2 and 10.2 databases.

The Configuration Logging database must be set up before Configuration Logging can be enabled. Only one Configuration Logging database is supported per server farm, regardless of how many domains are in the farm. When the Configuration Logging database is set up, you also must ensure that the appropriate database permissions are provided for Presentation Server so that it can create the database tables and stored procedures (preceded by "CtxLog_AdminTask_") needed for Configuration Logging. Do this by creating a database user who has "ddl_admin" or "db_owner" permissions for SQL Server, or a user who has the "connect" and "resource" roles and "unlimited tablespace" system privilege for Oracle; this is used to provide Presentation Server full access to the Configuration Logging data.

General Requirements

- The Configuration Logging feature does not allow you to use a blank password to connect to the Configuration Logging database.
- Each server in the server farm must have access to the Configuration Logging database.

Considerations for SQL Server

- For SQL Server 2000 and 2005, only one server farm is supported per Configuration Logging database. To store Configuration Logging information for a second farm, create a second Configuration Logging database.
- For SQL Server 2000 and 2005, when using Windows Integrated Authentication, only fully qualified domain logons are valid. Local user account credentials will fail to authenticate on the database server that hosts the Configuration Logging database.
- Tables and stored procedures for SQL Server 2000 databases are created in the schema associated with the user who initially configured the Configuration Logging feature.
- For SQL Server 2005, ensure that all Citrix administrators accessing the same farm are configured to use the same default schema. The database user who will create the Configuration Logging tables and stored procedures must be the owner of the default schema. If you are using dbo as the default schema, the database user must have db_owner permissions. If you are using ddl_admin as the default schema, the database user must have ddl_admin permissions.

Note For additional instructions about how to manage and use schemas in SQL Server, see your SQL Server documentation.

Considerations for Oracle

- For Oracle, only one farm is supported per schema. To store Configuration Logging information for a second farm in the same database instance, use a different schema. Tables and stored procedures are created in the schema associated with the user who initially configured the Configuration Logging feature. For instructions about how to manage and use a different schema, see your Oracle documentation.
- Prior to running the Access Management Console, you must update the Oracle client file "tnsnames.ora" to include the connectivity information needed to access the available databases.

Defining Database Permissions

The first time the Configuration Logging feature is enabled, it connects to the Configuration Logging database and discovers that the database schema does not exist. Presentation Server then creates the database schema, tables, and stored procedures. To create a database schema, Presentation Server needs full access to the database as described in the previous section. After the database schema is created, full access is no longer necessary and you have the option of creating additional users with less permissions.

The following table lists the minimum permissions required to perform the Configuration Logging tasks.

Configuration Logging task	Database permissions needed
To create log entries in the database tables	**INSERT** for the database tables, **EXECUTE** for the stored procedures, and **SELECT** for *sysobjects* and *sysusers* (SQL Server) or *sys.all_objects* (Oracle) (Oracle also requires **SELECT** for sequence objects and the *create session* system privilege)
To clear the log	**DELETE/INSERT** for the database tables, **EXECUTE** for the *GetFarmData* stored procedure, and **SELECT** for *sysobjects* and *sysusers* (SQL Server) or *sys.all_objects* (Oracle) (Oracle also requires **SELECT** for sequence objects and the *create session* system privilege)
To create a report	**EXECUTE** for the Citrix Configuration Logging stored procedures **SELECT** for *sysobjects* and *sysusers* (SQL Server) or *sys.all_objects* (Oracle) (Oracle also requires the *create session* system privilege)

Note The Configuration Logging components must have access to the GetFarmData stored procedure to find out if a Configuration Logging database is associated with a farm. If you do not have permission to execute an existing GetFarmData stored procedure, this farm is invisible to the Configuration Logging components.

Considerations for SQL Server

- Before you configure the Configuration Logging database connection, grant **EXECUTE** permission to the system stored procedure *sp_databases* to list the databases on the database server.
- The authentication mode must be the same for the database user who creates log entries in the database tables and the database user who clears the log.

Setting Up the Configuration Logging Database Connection

After the Configuration Logging database is set up by your database administrator and the appropriate database credentials are provided to Presentation Server, the connection to the Configuration Logging database must be configured through the Configuration Logging Database wizard.

To access the Configuration Logging Database wizard

1. In the Access Management Console, expand the Farm node in the scope pane and select a farm. Then select **Action > Modify farm properties > Modify configuration log properties**.
2. In the **Configuration Logging** dialog box that appears, click the **Configure Database** button to open the wizard.

In this wizard, if you are using a SQL Server database, you need to provide or select: the name of the database server, an authentication mode, the name of the database, and the logon credentials for the database user that were created when you set up the Configuration Logging database.

Note When you use SQL Server, the **Use encryption** connection option in the wizard is enabled by default. If your database does not support encryption, you must disable this option.

If you are using an Oracle database, you must instead provide a net services name as well as the logon credentials. The net services names listed in the Data Source drop-down list are found in the Oracle client file "tnsnames.ora." You are then asked to specify various connection and pooling options. For information about how to configure these options, see your SQL Server or Oracle documentation.

Note Credentials are always required for both Oracle and SQL Server, even if you are using Windows Integrated Authentication. The credentials are stored using the IMA encryption feature. Each server that creates log entries uses the credentials to connect to the Configuration Logging database.

Testing the Configuration Logging Database Connection

The last page of the Configuration Logging Database wizard contains a button to **Test Database Connection**. Clicking this is a quick and easy way to determine if you have any configuration issues that are affecting the connection to your database server.

Setting the Configuration Logging Properties

The following Configuration Logging properties are set through the **Configuration Logging** dialog box.

Note Some of these properties will be grayed out until you configure the Configuration Logging database connection.

- **Log tasks**. The properties in this section are:
  - **Log administrative tasks to logging database**. Select this check box to enable the Configuration Logging feature.
  - **Allow changes to the farm when database is disconnected**. This check box is selected by default; however, when the database is disconnected, log entries resulting from administrative actions are lost.

Note When the Configuration Logging database is disconnected and Configuration Logging information is lost, an entry is made in the Windows Event Log. If you are using Citrix Presentation Server, Enterprise Edition, these entries are used to generate alerts.

- **Clearing log**. Contains the **Require administrators to enter database credentials before clearing the log** property. Select this check box if you want to force administrators to enter appropriate database access credentials before being permitted to clear the Configuration Logging tables of all entries.

Delegating the Administration of Configuration Logging

Full Citrix administrators can edit the Configuration Logging settings and select the task to clear the log in the Access Management Console, or they can authorize other administrators to perform these tasks by assigning them the delegated administration permission **Edit Configuration Logging Settings**. Without this permission, ordinary administrators cannot perform these functions.

Using Configuration Logging

The Configuration Logging feature, after it is properly enabled, runs in the background as administrative changes trigger entries in the Configuration Logging database. The only activities that are initiated by the user are generating reports, clearing the Configuration Logging database, and displaying the Configuration Logging properties.

Viewing Configuration Logging Properties

You can view Configuration Logging properties at the farm level.

To view Configuration Logging properties

1. In the Access Management Console, select the Farm node in the scope pane and select **Action > Properties** to display the properties of the farm.
2. Open the **Configuration Logging** page. The Configuration Logging properties are contained within the table that is displayed.

Clearing the Log

It may become necessary to clear the entries in the Configuration Logging database occasionally if the population of the tables becomes too large. To clear the log, you must:

- Be a full or delegated Citrix administrator with the permissions to edit the Configuration Logging settings. These permissions allow you to select the Clearing the Log task in the Access Management Console.
- Have the correct database user account permissions. These permissions allow you to clear the log in the database. By default, the database credentials defined in the database wizard are used to clear the log.

To manage which database users can clear the configuration log, Citrix recommends that you enable the **Require administrators to enter database credentials before clearing the log** check box. This ensures only database users with permissions to clear logs can clear them. Therefore, anyone attempting to use the Clearing the Log option will be prompted for database credentials.

If you configured a SQL Server database and you want to clear a log, you can only enter credentials that correspond with the same type of authentication mode that you selected when you connected to the database initially. Specifically...

- For SQL authentication, credentials with permissions for the Configuration Logging database on the SQL server are required.
- For Windows Integrated authentication, Citrix Presentation Server impersonates the database user when it connects to the SQL database, so you must enter the credentials for the Windows user account.

To clear the log, from the Farm node of the Access Management Console, select **Action > All tasks > Clear configuration log**.

Generating Configuration Logging Reports

Reports that draw the information from the tables created in the Configuration Logging database can be configured and generated in the Access Management Console's Report Center.

Important

- When the Configuration Logging feature is enabled, only administrative changes made to servers running Citrix Presentation Server 4.5 are logged and appear in the reports that are generated.
- The supported versions of Microsoft SQL Server are verified for MDAC 2.8.

To generate a Configuration Logging report

1. Select the Report Center node in the scope pane of the Access Management Console and choose **Generate report**. The Select Report Type screen appears.
2. Click the **Report type** drop-down list and select **Configuration Logging Report**. Then click **Next** to start the Configuration Logging Report wizard.
3. Follow the steps in the wizard to generate a report.

Note If you are using SQL Server or Oracle database authentication, the **Allow Saving of password** check box must be selected.

Reports can be generated based on the following filter criteria (wildcards are not supported):

- **Time period**. When the actions occurred that you want to review. The actions covered in the report are displayed with the local time where the report is generated.
- **Type of item**. Select the type of object for which you want to report changes.
- **Name of item**. After you select an item type, you can provide the name of a specific object on which to report. The name of the item search does not support wildcards; therefore, enter the exact name of the object to get the desired result.
- **User name**. The Citrix administrators whose actions will be covered in the report.

When no filter criteria are selected, the default, all log entries are included in the report. After you select the filtering criteria for the report, it can be published from the Report Center.

Note To generate a report from an Oracle logging database, you must first install the Oracle Provider for OLE DB. This can be done by performing a custom installation of the Oracle client.

Using Health Monitoring & Recovery

Health Monitoring & Recovery is a feature that is available only with the Enterprise Edition of Citrix Presentation Server. You can use the Health Monitoring & Recovery feature to run tests on the servers in a server farm to monitor their state and discover any health risks. Citrix provides a standard set of tests, and you can also develop your own tests. The tests that are included with Presentation Server allow you to monitor Terminal Services, Citrix XML Service, IMA Service, and logon/logoff cycles. These standard tests are described in "Modifying Test Settings" on page 240 and the process to develop your own tests is described in "Developing Custom Tests" on page 242.

After you enable Health Monitoring & Recovery on a farm, by default, the tests run on all servers in the farm including the data collector. Typically, you do not need to run these tests on the data collector because, particularly in a large farm, the data collector is not used for serving applications. If you do not want Health Monitoring & Recovery to run on the data collector, you must disable it manually.

Use the load balancing feature of Presentation Server in conjunction with Health Monitoring & Recovery to ensure that if a server in the farm experiences a problem (for example the Citrix IMA Service is down), the state of that server does not interfere with the user's ability to access the application because the user's connection to that application is redirected through another server. For more information about load balancing applications and using Load Manager, see the *Load Manager Administrator's Guide*.

Accessing Tests

To access the Health Monitoring & Recovery tests

1. Through the Access Management Console:

    - To access the tests by server, in the scope pane, expand the Presentation Server and Servers nodes, and select a server. Then select **Action > Modify server properties > Modify all properties**. The **Server Properties** dialog box appears.

    - To access the tests by farm, in the scope pane, expand the Presentation Server node and select a farm. Then select **Action > Modify farm properties > Modify all properties**. On the **Farm Properties** dialog box, expand the Server Default node.

2. Select **Health Monitoring & Recovery**. The **Health Monitoring & Recovery** page that appears allows you to view the following standard tests and any custom tests that you import.

   - **Terminal Services test**. This test enumerates the list of sessions running on the server and the session user information, such as user name.
   - **Citrix XML Service test**. This test requests a ticket from the Citrix XML Service running on the server and prints the ticket.
   - **Citrix IMA Service test**. This test queries the service to ensure that it is running by enumerating the applications available on the server.
   - **Logon monitor test**. This test monitors session logon/logoff cycles to determine whether or not there is a problem with session initialization. If there are numerous logon/logoff cycles within a short time period, the threshold for the session is exceeded and a failure occurs. The session time, interval, and threshold can be configured by modifying the parameters in the **Test file** field. These parameters are listed and described in the following table.

Logon Monitor test parameter	Description
SessionTime	Defines the maximum session time for a short logon/logoff cycle. Default is five seconds.
SessionInterval	The time period designated to monitor logon/logoff cycles. Default is 600 seconds.
SessionThreshold	The number of logon/logoff cycles that must occur within the session interval for the test to fail. Default is 50 cycles.

Note Through this **Health Monitoring & Recovery** page, you can configure the feature to allow custom tests to run on your servers. For more information, see “Developing Custom Tests” on page 242.

Adding Tests to a Server

There are two types of Health Monitoring & Recovery tests that you can add to your servers: tests supplied by Citrix through the Citrix Developer's Network, and custom tests developed by your organization or by third parties.

To add tests to your servers

1. On the **Health Monitoring & Recovery** page, click **New**. The **New Health Monitoring & Recovery Test** dialog box appears.
2. Select the **Allow running custom Health Monitoring tests** check box. This setting is disabled by default. If you select this check box, you can then import a test by typing or navigating to the appropriate file path in the **Test file** field.

Citrix recommends that you store all tests in the following location:

%Program Files%\Citrix\HealthMon\Tests\Citrix\

where %Program Files% is the location in which you installed Presentation Server. Store Citrix-supplied tests in the Citrix folder and custom tests in the Custom folder.

Note For information about developing custom tests, see "Developing Custom Tests" on page 242.

Modifying Test Settings

You can modify the settings of Health Monitoring & Recovery tests by server or across all servers in a farm. For instructions about accessing the **Health Monitoring & Recovery** page by server or farm, see "Accessing Tests" on page 238.

On the **Health Monitoring & Recovery** page, click **Modify**. Through the **Modify Health Monitoring Test** dialog box that appears, you can modify the following settings for each Health Monitoring & Recovery test.

Note The default values for these settings vary for each test.

- **Interval.** The amount of time to wait before running the test.
- **Threshold.** The number of times this test will fail before triggering an action.

- **Time-out.** If a test does not return within this specified amount of time, the test will time-out.
- **Recovery Action.** You can choose different actions to be taken if a server fails a test; these include restarting the server or preventing user connections from being initiated on it until the problem is fixed. If a server fails a test, an alert appears in the Access Management Console. For each alert, you can display a Citrix My Knowledge article that provides information about the possible causes and resolutions for the problem. Through the Health Monitoring & Recovery page, you can configure one of the following actions to be taken automatically if a test fails:
  - **Alert Only.** Sends an error message to the event log, but takes no other action. The test continues to run, and if it subsequently successfully passes, an event is sent to the system log. This recovery action is the default for all tests except the Citrix XML Service test.

    Remove Server from load balancing. Excludes the server from load balancing. Clients do not attempt to make new connections to this server through Load Manager. However, existing connections are maintained, and attempts are made to reconnect disconnected sessions. You can make new direct connections to the server; this enables you to try to correct any problems. To prevent possible farm-wide outages, this is the default recovery action for the Citrix XML Service test.

    You can set a limit on the percentage of servers in the farm that can be offline at any one time. For details, see the **Limit servers for load balancing** setting below.

    To restore one or more servers to load balancing, use the **enablelb** command-line utility, which is described in “ENABLELB” on page 327.
  - **Shut Down IMA.** Shuts down the Citrix IMA Service. After this happens, tests continue to run but failures will not trigger events to be sent to the Event log until the Citrix IMA Service is up and running again.

- **Restart IMA.** Shuts down and then restarts the Citrix IMA Service. After this happens, tests will run but failures will not trigger events to be sent to the Event log until the Citrix IMA Service is up and running again.
- **Reboot Server.** Restarts the server. An alert will be triggered before the server is restarted. After the system is restarted, the tests will resume.

Note If the Recovery Action list contains the entry Action ID followed by a number, this means that Citrix supplied a new action through a hotfix, and that although you have applied the hotfix to the selected server, you did not apply it to the computer on which the Access Management Console is running. When the hotfix is fully applied, a meaningful name for the new action is added to the list.

Limit servers for load balancing. This setting allows you to set a limit on the percentage of servers in the farm that can be offline at any one time. This percentage includes both servers that are excluded from load balancing and servers that are offline for other reasons. The default for this setting is 10 percent. To access this setting, in the **Farm Properties** window, expand the Farm-wide node and select **Health Monitoring & Recovery**.

Note You can configure additional settings for the Logon Monitor test only. For details, see "Accessing Tests" on page 238.

Developing Custom Tests

If you want to perform particular tests that are not included in Health Monitoring & Recovery, you can develop custom tests using the Health Monitoring & Recovery SDK package. This package includes a Readme file with information that you will need to use the SDK, including security requirements and return values. In addition, the SDK contains various sample test scripts that you can use as examples to develop custom tests that can be run on a server farm or on individual servers in a farm. The Health Monitoring & Recovery SDK package is available for download from the Citrix Developer Network.

For information about adding custom tests to your servers, see "Adding Tests to a Server" on page 240.

Getting Alerts

In the event of a test failure, an HCAService Test Failed alert is raised for the relevant server. This alert, displayed in the Access Management Console, indicates the name of the test that failed. For information about the alert that appears, you can choose to view the Citrix Knowledge Center article associated with the alert.

The default recovery action for all tests (except the Citrix XML Service test) is that an error message is sent to the Event log. For the Citrix XML Service test, the default action is to exclude the server from load balancing to prevent possible farm-wide outages. For more information about recovery actions, see “Modifying Test Settings” on page 240.

Note In the Advanced Edition of Citrix Presentation Server, XML ticketing failures also result in the server being excluded from load balancing. This action is performed by the Citrix XML Service and not by Health Monitoring & Recovery, so no alerts are sent. For any servers excluded in this way, the IMA service needs to be restarted for the server to rejoin the load balancing tables.

If the test is run again and it is successful, an event is sent to the Event log.

Monitoring Performance of Sessions and Servers

Performance monitoring counters for ICA data are installed with Citrix Presentation Server and can be accessed from Performance Monitor, which is part of the Windows operating system. Performance monitoring provides valuable information about utilization of network bandwidth and helps determine if a bottleneck exists.

By using Performance Monitor, you can monitor the following counters:

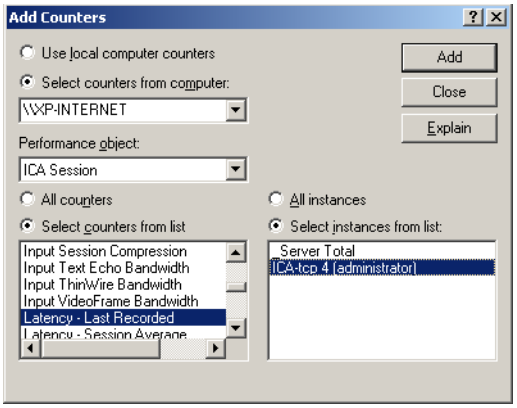
- Bandwidth and compression counters for ICA sessions and computers running Citrix Presentation Server
- Bandwidth counters for individual virtual channels within an ICA session
- Latency counters for ICA sessions

Note The entire ICA counter list is exposed only on a server running the Platinum or Enterprise Edition of Citrix Presentation Server. On a server running the Advanced or Standard Edition, only latency-related counters are available.

For more information about specific counters available with Citrix Presentation Server, see "Performance Counters" on page 355.

To access ICA performance counters

1. Select **Start > All Programs > Administrative Tools > Performance**.
2. Select **System Monitor** in the Tree view.
3. Click the **Add** button.
4. In the **Add Counters** dialog box, click the **Performance object** drop-down list and select **ICA Session**. The ICA performance counters are listed under **Select counters from list**.



This screen capture shows the Add Counters dialog box with computer-selection drop-down list, Performance object drop-down list, and counters list.

5. Select **All counters** to enable all available ICA counters or select **Select counters from list** and then highlight the individual counters you need.
6. Select **All instances** to enable all instances of the selected ICA counters or select **Select instances from list** and highlight only the instances you need.

   In Performance Monitor, the instance list contains all active ICA sessions, which includes any session (shadower) that is shadowing an active ICA session (shadowee). An active session is one that is logged on to successfully and is in use; a shadowing session is one that initiated shadowing of another ICA session.

Note In a shadowing session, although you can select ICA counters to monitor, you will see no performance data for that session until shadowing is terminated.

---

7. Click **Add** and then click **Close.**

   You can now use Performance Monitor to view and analyze performance data for the ICA counters you added. For more information about using Performance Monitor, see your Windows documentation.

Managing CPU Usage

The CPU utilization management feature (requiring an Enterprise edition license) can be used to improve the ability of a farm to manage resources and normalize CPU peaks when the farm's performance becomes limited by CPU-intensive operations. When you enable CPU utilization management, the server allocates an equal share of the CPU to each user. This prevents one user from impacting the productivity of other users and allows more users to connect to a server.

The CPU utilization management feature ensures that CPU resources are equitably shared among users. This is accomplished by providing CPU reservation and CPU shares.

- CPU reservation is defined as a percentage of your server's CPU resource that is guaranteed to be available to a user. If all of such a reserved allocation is not being used, other users or processes can use the available resource, as needed. Note that approximately 20% of the CPU resource is reserved and not available to users. The percentages stated here are of the available, not the total, CPU resource.
- CPU shares are percentages of the CPU time. By default, CPU utilization management allocates eight shares for each user. If two users are logged on to a server (and no console session), each of the users gets 50% of the CPU. If there are four users with eight shares each, each user receives 25% of the CPU time.

Important The range for CPU share is 1-64. For CPU reservation, the total cannot be more than 100%, which represents the entire CPU resource on the computer.

Do not enable CPU optimization 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.
- Special users who are considered to have a higher priority access to servers. You can exclude specified users from CPU restrictions.

Note The Citrix CPU Utilization Mgmt/CPU Rebalancer service is installed on Windows Server 2003 multiprocessor systems. The CPU rebalancer service is used to alleviate a Microsoft issue that appears in environments where many short-lived processes are started and stopped. Due to the performance impact the CPU rebalancer service can have, by default it is set to **Manual**. If your environment is running many short-lived applications that all appear to be running on the same CPU, Citrix recommends setting the service to **Automatic**.

Enabling CPU Utilization Management

You can enable CPU utilization at the farm level and at an individual server level. This feature is not enabled by default.

To enable CPU utilization management for a farm

1. In the scope pane of the Access Management Console, select the farm for which you want to enable CPU utilization management.
2. Select **Action > Modify farm properties > Modify all properties**.
3. In the left pane of the **Farm Properties** dialog box, click **Server Default > Memory/CPU > CPU Utilization Management**.
4. On the **CPU Utilization Management** page, select the **CPU Utilization Management** check box, if desired.

To enable CPU utilization management for a server

1. In the scope pane of the Access Management Console, select the server for which you want to enable CPU utilization management.
2. Select **Action > Modify server properties > Modify all properties**.
3. In the left pane of the **Server Properties** dialog box, click **Memory/CPU > CPU Utilization Management**.
4. On the **CPU Utilization Management** page, select the **CPU Utilization Management** and **Use Farm Settings** check boxes, as appropriate.

Managing Virtual Memory Usage

You can improve system speed, performance, and scalability by controlling virtual memory utilization for a farm or individual servers. This feature is especially useful when user demand exceeds available RAM and causes farm performance to degrade. Performance degradation can occur during peak times when users run memory-intensive applications in multiple sessions.

To increase the number of users who can use a server and improve a farm's ability to optimize the use of DLLs stored in virtual memory, enable memory utilization management. When you enable memory utilization management, you enable the rebasing of DLLs for virtual memory savings without actually changing the DLL files. You can also schedule the rebasing of DLLs for off peak hours, exclude specific applications from DLL rebasing, and rebase DLLs through a user account with permissions to access application files stored on file servers.

You do not want to enable memory utilization management on farms or servers that exclusively host signed or certified applications. Presentation Server can detect only some published applications that are signed or certified.

Caution If, after enabling memory utilization management and running scheduled memory optimization, published applications fail, exclude those applications from memory optimization.

Before deploying memory utilization management

1. Using a test server hosting your published applications, enable memory utilization management.
2. Schedule memory optimization.
3. After memory optimization completes, run all published applications.
4. Add to the exclusion list those applications that fail.

Enabling Memory Utilization Management

You can enable memory utilization management at the farm level and at an individual server level. This feature is not enabled by default.

To enable memory optimization for a server

1. In the scope pane of the Access Management Console, select the server for which you want to enable memory optimization and select **Action** > **Properties**.
2. In the left pane of the **Server Properties** dialog box, click **Memory/CPU > Memory Optimization**.
3. On the **Memory Optimization** page, select the appropriate check boxes.

When you enable virtual memory optimization at the server level, virtual memory optimization occurs at a time set by the farm-wide schedule. After enabling memory optimization, create a schedule when the servers can rebase DLLs. For instructions about how to create a farm-wide memory optimization schedule, see the next section.

Scheduling Virtual Memory Optimization

After enabling virtual memory optimization, you create a virtual memory optimization schedule that identifies when a server rebases DLLs for greater operating efficiency.

When a server rebases a DLL:

- It makes a hidden copy of the DLL
- It modifies the starting address of the DLL to avoid conflicts that result in multiple copies of a single DLL held in virtual memory

Schedule virtual memory optimization at a time when your servers have their lightest loads.

To create a memory optimization schedule

1. In the scope pane of the Access Management Console, select the farm for which you want to create a virtual memory optimization schedule.
2. Select **Action > Modify farm properties > Modify all properties**.
3. In the **Farm Properties** dialog box, choose **Memory/CPU > Optimization Interval**.

4. On this page you can set:

   - **The optimization interval.** The frequency at which the server rebases DLLs. You can set the frequency to be every time you restart your server, every day, once a week, or once a month.
   - **The optimization time.** The time at which the server begins rebasing DLLs. The value of optimization time is based on a twenty-four hour clock.
   - **The local or remote account that will access the application files.** If you store application files on a file server or remote server that requires special access permissions, such as a domain administrator, clear the check box **Use local system account** and provide the account and password that has permissions to access the remotely stored application files.

Excluding Applications from Memory Optimization

Some applications are excluded from being rebased by virtual memory optimization:

- Applications that have digitally signed components.
- Applications whose DLLs are protected by Windows Rights Management. For example, applications such as Office 2003 do not benefit from this feature.
- Applications whose executable programmatically checks the DLL after it is loaded.
- Applications that fail after you enable memory optimization. Add the applications' executables to the memory optimization exclusion list.

To add an application to the excluded applications list

1. In the scope pane of the Access Management Console, select the farm. Then select **Action > Modify farm properties > Modify all properties**.
2. In the **Properties** dialog box, choose **Memory/CPU > Exclude Applications**.
3. On this page, click **Add** and choose the executable of the application you want to exclude from memory optimization.

Working with the Local Host Cache

A subset of data store information, the local host cache, exists on each server in the farm, providing each member server with quick access to data store information. The local host cache also provides redundancy of the data store information, if for example, a server in the farm loses connectivity to the data store.

When a change is made to the farm's data store, a notification to update the local host cache is sent to all the servers in the farm. However, it is possible that some servers will miss an update because of network problems. Member servers periodically query the data store to determine if changes were made since the server's local host cache was last updated. If changes were made, the server requests the changed information.

Tuning Local Host Cache Synchronization

You can adjust the interval by which member servers query the farm's data store for missed changes. The default interval is 30 minutes. In most cases, this default setting is sufficient.

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

You can configure the interval using the following registry key on each server you want to adjust, with the value expressed in hexadecimal notation:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\
DCNChangePollingInterval (DWORD)

Value: 0x1B7740 (default 1,800,000 milliseconds)

You must restart the IMA Service for this setting to take effect.

Most changes made through the Access Management Console or Presentation Server Console are written to the data store. When you open the console, it connects to a specified server. The Citrix IMA Service running on this server performs all reads and writes to the data store for the console.

If the data store is experiencing high CPU usage when there should not be significant read or writes to the data store, it is possible that the data store is not powerful enough to manage a query interval of 30 minutes. To determine whether or not the data store query interval is causing the high CPU usage on the data store, you can set the query interval to a very large number and test CPU usage. If the CPU usage returns to normal after you set a large query interval, the data store query interval is probably the cause of the high CPU usage. You can adjust the query interval based on performance testing.

To test the query interval, set the interval to 60 minutes and then restart all the servers in the farm. If the data store is still experiencing constant high CPU usage, increase the query interval further. If the CPU usage returns to normal, you can try a smaller value. Continue these adjustments until data store CPU usage is normal.

Important Do not set the data store query interval higher than necessary. This interval serves as an important safeguard against lost updates. Setting the interval higher than necessary can cause delays in updating the local host cache of the farm's member servers.

The next section tells you how to force the local host cache to refresh.

Refreshing the Local Host Cache

You can force a manual refresh of a server's local host cache by executing **dsmaint refreshlhc** from a command prompt (see "DSMAINT" on page 322). This action forces the local host cache to read all changes immediately from the farm's data store. Refreshing the local host cache is useful, for example, if the Citrix IMA Service is running, but published applications do not appear correctly when users browse for application sets.

A discrepancy in the local host cache occurs only if the IMA Service on a server misses a change event and is not synchronized correctly with the data store.

Recreating the Local Host Cache

You can manually create the local host cache from the farm's data store. If the Citrix IMA Service fails to start or you have a corrupt local host cache, you may need to recreate it.

To recreate the local host cache, stop the IMA Service and then run the command **dsmaint recreatelhc** (see "DSMAINT" on page 322). Running this command performs three actions:

- Sets the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\Runtime\PSRequired to 1
- Deletes the existing local host cache (Imalhc.mdb)
- Creates an empty local host cache (Imalhc.mdb)

You must restart the IMA Service after running **dsmaint recreatelhc**. When the IMA Service starts, the local host cache is populated with fresh data from the data store.

The data store server must be available for **dsmaint recreatelhc** to work. If the data store is not available, the Citrix IMA Service fails to start.

Updating Citrix License Server Settings

The settings for your Citrix License Server are configured automatically when you install the licensing components as part of the Setup program for your Citrix product. Two of these settings are the name of the license server that your farm accesses to check out licenses and the port number the license server uses to communicate. You may want to change these settings in the following instances:

- You rename your license server.
- You want to specify another license server to point to (either for an entire farm or for individual servers only) to relieve some of the traffic to the license server. For example, you have many connections and you find that it is slowing down the network, or you would like to add a second license server to the farm and point half of the connections to it.

- You want to specify another license server to point to individual servers to segregate licenses. For example, you want to host the accounting department's licenses on a different server than the human resources department.
- The default port number (27000) is already in use.
- You have a firewall between the license server and the computers running your Citrix products, and you must specify a static Citrix vendor daemon port number.

To change the name of the license server or port number that it uses to communicate, type the license server name or its IP address in the Name field of the **License Server** page of the server's or farm's **Properties** screen in the Access Management Console (to apply the changes to either an individual server or an entire farm). Changing the settings on this page is only one part of the procedure. You must also take the following actions:

- **Changing the license server name**. If you decide to change the license server name, first ensure that a license server with the new name already exists on your network. Because license files are tied to the license server's host name, if you change the license server name, you must download a license file that is generated for the new license server. This may involve returning and reallocating the licenses. To return and reallocate your licenses, go to www.mycitrix.com. For additional information, see the *Licensing: Migrating, Upgrading, and Renaming* whitepaper in the Citrix Knowledge Center.
- **Changing the port number**. If you change the port number, you must specify the new number in all license files on the server. For additional information, see the *Licensing: Firewalls and Security Considerations* whitepaper in the Citrix Knowledge Center.

CHAPTER 10

Managing Printers

This chapter describes the different types of printer configurations available with Citrix Presentation Server, and how to configure and manage your printing configuration.

Planning Your Deployment

The exact configuration of your printer deployment depends upon your server farm and user requirements. This section describes the different types of printer connections available, and how to choose an implementation based upon your requirements.

To plan your printer deployment you must:

- Determine the types of printer configurations that already exist in your organization, using the list in “Printer Configurations” on page 256.
- Determine your network requirements and limitations on bandwidth. See “Network Considerations” on page 257.
- Determine the best method for managing printer drivers for your implementation. See “Managing Drivers” on page 258.
- Determine the printing requirements of your users.
- Determine what printing configuration and what Policy settings would best suit your user and network requirements. See “SmoothRoaming and Proximity Printing” on page 257, “Implementing and Managing Client Printers” on page 260, “Implementing and Managing Network Printers” on page 270, and “Printing Policies” on page 259.

Printer Configurations

There are three basic printer configurations in Presentation Server:

Redirected Client Printers. Client printers are those printers physically attached to or mapped from a client device. These printers are typically created and managed by the local client operating system. During logon to a server running Presentation Server, redirected client printers are auto-created for the new session based on the printing policy settings. Client printers that are not auto-created by policy can be mapped manually in a user session through the Windows Add Printer wizard or by running the Citrix Client Printer Configuration utility (PrintCfg.exe).

Note Client printers can include printers on a TCP/IP-based port or print server mapped from the client.

Network Printers. Shared printers attached to print servers on a Windows network. This configuration uses printer drivers installed on print servers, as well as print devices configured and accessible through these print servers. These printers are imported into Presentation Server and can be assigned to users through policies. By default, network print jobs are routed directly from Presentation Server to the print server and do not go through an ICA protocol.

Server Local Printers. Printers physically attached, and network printers configured, on each server running Presentation Server. These are managed using Windows print management tools on the server. Server local printers require additional resources on the computer running Presentation Server, and therefore are not commonly used.

The type of printer used depends upon your user requirements and your system resources.

Network Considerations

The configuration of auto-created printers and network printers, as well as the print job routing policy, directly influence the amount of traffic that traverses the network. All print jobs that are initiated by the server-hosted application are delivered to the Presentation Server Client by the ICA protocol. Whether the next step of the print job is compressed through the ICA protocol or traverses the network uncompressed depends on the type of printers configured and the print job policy.

The impact of print job routing on the network is as follows:

Auto-created printers. By default, all print jobs route from the client to the server, back through the client, and then to the print device. The print job traffic from the server and back through the client is compressed by means of the ICA protocol.

Network printers. By default, all print jobs route from the server and directly to the print server. The print job traffic from the server to the print server is not compressed and is treated as regular network traffic.

Print job routing policy. This policy stipulates the routing of the print job traffic and changes the default if configured. Although it may at first seem counterintuitive to designate that network print jobs should be routed through the client device, the reduction in network traffic is generally greater than the resource cost on the client device.

When print jobs must traverse a network where bandwidth is limited, such as a heavily-used WAN link, it is advantageous to route the print job through the client device so that the ICA protocol compresses the print job. Also, by doing so, printer bandwidth can be controlled.

SmoothRoaming and Proximity Printing

SmoothRoaming (or Workspace control) allows a user to disconnect from one ICA session and reconnect from another device to continue that same session. When this happens, the printers assigned on the first device are replaced on reconnection with the printers designated on the second client device. This means that users are always presented with applicable printer options from wherever they connect.

Proximity Printing is based on the Session Printers policy and allows an administrator to control the assignment of network printers. By using the Session Printers rule, you can construct a hierarchy of rules that resolve to the appropriate printers based on the correct client device.

In situations where client workstation names can be controlled, it may also be possible to use a simple naming convention for the clients and assign policy filters based on the client name.

By using policies and filters, users can always be presented with sensible printing choices wherever they connect. For example, if users connect from their main computer on the first floor of their office, the connection allows them access to the auto-created printers on their client. In this case, the auto-created printers are printers on the first floor. Later, when the users attend a meeting on the second floor of a different building, they connect to the same session as before but are now in a different location on a different client device. Now, the auto-created printers presented to them are those preconfigured on the new client device, even though that are connected to the same session. This allows them to access the local printers on the second floor of this different building.

Managing Drivers

There are three basic strategies for managing printer drivers:

Universal Print Driver. Citrix Presentation Server Universal Printing is designed to relieve the burden of administering a multitude of printer drivers and avoid problems with driver maintenance, replication, and other client printing issues in diverse environments. See "Using Advanced Universal Printing" on page 273.

Using Native Drivers. Native drivers can be used for the printers available using Presentation Server. When printers are auto-created (see "Auto-Created Client Printers" on page 263), the specific drivers for these printers must be available on the server. These drivers can then be replicated throughout the server farm (see "Setting up Automatic Replication of Printer Drivers" on page 277).

Client Printer Driver Mapping. Mapping of printer drivers refers to identifying printer drivers that have different names for the same printer on different client and server operating systems. Use mapping if drivers you install on servers have names different from the drivers used by clients. You can also use this mapping functionality to map a driver to one available on the server; for example, mapping the HP LaserJet 4L driver to HP LaserJet 4. Printer mappings can be managed in the Presentation Server Console or in a mapping file supplied by the administrator called Wtsuprn.inf. See "Remapping Client Printer Drivers" on page 276.

Printing Policies

Configuration of printer management is accomplished through Citrix Presentation Server policies created in the Presentation Server Console. Similar in concept to Windows group policies, Presentation Server policies provide a mechanism to define a collection of system settings that can be associated with a broader range of criteria than just users, groups, and computers. For more information about using Citrix policies, see “Using Policies to Configure Access to Published Resources” on page 125.

Presentation Server policies are assigned through filters that apply the associated rules through any combination of the following criteria:

- Access Control
- Client IP address
- Client Name
- Servers
- Users

Client access filters defined in the Citrix Advanced Access Control Option can also be used to further qualify clients and users for the purposes of policy application.

During logon, the system searches all defined policies and selects the policy rules that should apply based on the Administrator-defined filters. Policies are also assigned a numeric priority for resolving conflict. When the resultant policy set includes multiple instances of the same policy rule with potentially different settings, conflicts are resolved in favor of the highest priority (lowest numeric value) policy.

Policies can be used to establish farm-wide defaults for settings. However, they can also create complex hierarchies of settings that are applied dynamically based on different client, server, and user attributes.

Presentation Server policies are normally used with Windows group policies because they control different system settings. However, there is some overlap of settings. In these cases, conflicts between Group policies and Presentation Server policies are resolved in favor of the applicable Presentation Server policies.

In the Presentation Server Console, policies are organized in a tree view allowing related settings to be grouped together. All printing-related policies are under the Printing node with two logical subgroupings: Client Printers and Drivers.

Any of these policy rules can be independently enabled and then assigned a range of possible settings.

Implementing Your Deployment

This section describes how to:

- Implement and manage client printers
- Implement and manage network printers
- Manage printer drivers

Implementing and Managing Client Printers

This section describes how to implement client printers, and how to manage their configuration.

Client Printer Naming

By default, in Citrix Presentation Server 4.*x*, auto-created client printers are named according to standard Windows conventions. Previous versions of Presentation Server used the client name to help identify printers.

The Citrix Presentation Server naming convention for client printers and the client printer ports they connect to include the session ID as part of the name. This ensures no name collisions, thereby enhancing security.

The naming convention uses spaces to separate component parts of the printer name, and keeps the most recognizable part at the beginning of the name. This is helpful for viewing on small screens.

Printers connected through a pass-through server use the session ID to uniquely identify the printer, keeping the remainder of the name the same. This allows the user to identify both the printer and client it is connected to, without identifying which pass-through server it might have connected through.

Note Mixed version installations may not be able to adjust immediately to the Citrix Presentation Server printer naming convention. If this is the case, enabling the Legacy Printers policy rule allows the old naming convention to be used.

Client Printer Security

Unlike network printer connections, client printers auto-created in a Presentation Server session are actually local printers managed by the local print provider and Citrix spooler extensions. The local print provider maintains a single shared namespace for all local printers on a server. This means that a user's client printers may be visible and potentially accessible, to users from other sessions on the server.

By default, the Citrix Presentation Server printer naming convention helps combat this problem by avoiding the potential for printers and ports to be shared between sessions. However, this change alone does not guarantee that users from one session cannot use another user's printer in a different session.

To solve this problem, in Presentation Server 4.0 and above, the default security descriptor applied to client printers restricts access to:

- The account that the print manager service runs in (default: Ctx_cpsvcuser)
- Processes running in the SYSTEM account such as the spooler
- Processes running in the user's session

Access to the printer from all other processes on the system are blocked by Windows security. Furthermore, requests for services directed to the print manager must originate from a process in the correct session. This prevents the possibility of bypassing the spooler and talking to the remote printing interfaces of CpSvc.exe directly.

Members of the Administrators group do not have access to client printers from another session. Because administrator users always see all local printers, this prevents them from inadvertently printing to printers in another session.

If an Administrator needs to adjust the access control list (security settings) of a printer in another session for administrative purposes, they can do so through Windows Explorer or by using a script.

Note If Administrators require frequent access to printers in other sessions, add the **Admins Can Manage** bit flag to default print flags in the system registry of your server. See the *Advanced Concepts Guide for Citrix Presentation Server* for more information.

Configuring Auto-Creation for DOS and Windows CE Clients

Citrix Presentation Server provides auto-creation of client redirected printers (printers that are physically attached to client devices or mapped from client devices) for DOS and Windows CE Clients. Auto-creation configures the servers to download appropriate printer definitions to the client device to make the client printer available in client sessions.

The sections that follow describe how to set up and configure this auto-creation process.

To monitor and configure printer auto-creation for Clients for DOS and Windows CE

1. Under the Printer Management node of the Presentation Server Console, select **Printers**.
2. From the **Actions** menu, choose **Printer Management > Client Printers**.

   You can view the status of printers for clients on DOS and Windows CE platforms in the **Client Printers** dialog box. In the dialog box, the word <downloaded> appears in the list when information for client printer setup is sent from the server to the client device.

   Use the **Client Printers** dialog box to add, remove, reset, edit, and delete the configuration for the clients for DOS and Windows CE printers.

These printers are available only on the client, and appear only in server-based applications during the client user's ICA session.

Turning off Client Printer Auto-Creation

You can configure a policy so that no client printers are auto-created. This means that only network printers or local printers (printers attached directly to a server) can be used.

To configure an existing policy to turn off client printer auto-creation

1. In the Presentation Server Console, select the Policies node.
2. On the **Contents** tab, choose the policy for which you want to configure printing rules.
3. From the **Actions** menu, choose **Properties**.
4. In the policy's **Properties** dialog box, expand **Printing**, then **Client Printers**.
5. Under **Client Printers**, enable the **Auto-creation** rule.
6. Select **Do not auto-create client printers**.
7. Save and enable the policy.

Overriding Default Settings for Client Printers

To override Windows default settings for client printers, use Presentation Server policies to create and enable policies and printer rules to apply to sessions.

Auto-Created Client Printers

The printer auto-creation process involves:

- Presentation Server policies for administrative control
- Citrix print manager service (CpSvc.exe) for auto-creation

Policies control client printer mapping and naming, which printers connect by default, which drivers to use, and how printer properties associated with these printers are managed.

Printing policies are evaluated during initial logon and remain in force throughout the session. After evaluating these policies, printers are enumerated from the client and, depending on the policies in effect for the session, are auto-created.

After auto-creating the required printers, any retained printer properties are applied to restore the printer state. On logoff or a session reset, all auto-created client printers for the session are deleted. Before deleting these client printers, printer properties modified during the course of the session are saved for future reference. Depending upon the client and printer properties retention policies in force, these retained properties come from the client itself or the server-side user profile.

At the time of a disconnect, client printers are put into an offline state that remains in force until the original client reconnects to the session if workspace control is invoked or the printer is deleted by reconnecting from another client or logging off.

When a client reconnects to a session, existing printers are enabled if the reconnection is from the same client. If not, client printers associated with the previous client are removed and new client printers are constructed within the session based on the policies that were in force at the time of logon.

Also during a reconnection, Session Printers policies are reevaluated, leading to the potential connection of additional network printers and/or the adjustment of the default printer.

During logoff, network printer connections that were constructed by the application of a Session Printers policy rule are deleted. If you want the user to keep these network printer connections, thereby preserving personal printer settings, disable the delete-on-logoff behavior by changing the default printing flags in the system registry. Changes to this flag cannot be overridden by policies.

Printer Properties Retention

Printer properties include:

- The metadata used to construct the printer, including name, port, driver, print processor, comment, location, and printer attributes. These correspond to the fields of the Windows PRINTER_INFO_2 data structure.
- User printing preferences (default document settings) such as orientation, resolution, and media type. These items are represented by the Windows DEVMODE data structure. Some of these settings are common for all printers, but much of this data is driver specific.
- Printer device settings (printer driver data) such as tray-form table or the data representing the state of configured options. These data items are generally kept in the form of named values written by the driver with the SetPrinterData() function. Such values are normally found in the PrinterDriverData key for each printer in the Windows system registry. The actual names and interpretation of these values is always driver-specific.

In MetaFrame Presentation Server 3.0 and earlier products, the properties of auto-created client printers were retained in the server-side user profile. During logoff, user printing preferences, printer device settings, and other data were written into the HKEY_CURRENT_USER\Printers\Citrix key. During logon, retained properties in the profile were applied to the created client printers, effectively recreating the printer exactly as it was the last time the user logged on.

MetaFrame Presentation Server 3.0 and earlier products were also able to read a limited set of printer properties from the remote client, assuming of course that the client could provide them. The settings actually read were a subset of the user's printing preferences for the printer on the client. More specifically, these properties were the device-independent settings of DEVMODE (such as orientation, resolution, and so on). In the absence of retained properties in the profile during logon, the common properties were read and used to initialize the auto-created printer.

The common properties could also optionally be read and merged with the retained settings from the profile.

In Citrix Presentation Server 4.0 and higher, printer-retained properties are streamed to the client, so that they are retained for roaming profiles. Not all clients support the new protocol extensions required to service this functionality, so properties are still retained in the server-side user profile as needed.

The default system behavior is to first try to save/restore properties on the client. If the client does not support this operation, the user profile on the server is used.

In Citrix Presentation Server 4.0 and higher, support for retaining printer properties on the client (including the retained/restored printers feature) is available only for the Windows clients. Sessions from non-Windows clients or even older Windows clients use the user profiles on the server for properties retention.

The Printer Properties Retention policy rule can be used to change the default behavior described above and force either client-side properties retention or server-side properties retention. Enabling this policy allows the Administrator to either:

- Force properties to be saved/restored only on the client
- Avoid any properties exchange with the client and save/restore printer properties strictly in the server-side user profile

Auto-Retained Client Printers

By default, Presentation Server tries to create client printers in the session for every printer discovered and reported by the client software. However, client printer creation is an intensive activity for the spooler process of the server.

Limiting printer creation using the auto-creation policy often improves the performance of servers that are resource constrained (for example, by auto-creating only the user's default client printer). However, the user cannot then print to a client printer that was not auto-created by policy at session startup. In this case, the Citrix Client Printer Configuration utility (PrintCfg.exe) can be published as an application; this offers a facility to connect client printers that were not auto-created.

All of the above rely on the AddPrinterConnection() service of the client network print provider (cpprov.dll) to discover and optionally create client printers that were not auto-created by policy. In addition, in Presentation Server 4.0 and higher, the mechanism used to retain printer properties is also used to remember when someone creates a client printer using AddPrinterConnection(). During subsequent logons, these remembered connections are restored. Client printers created using this process are known as *retained printers*.

When recreating a retained printer, all policies except the auto-creation policy are used. This means that retained client printers are created exactly as if the auto-creation policy would select them. Such printers continue to be recreated with every logon from the same client until the client printer within the session is deleted manually, the remembered printer connection is removed from the client's properties store, or the client side printer is inaccessible.

On a Windows client, the properties store is in the user profile under HKEY_CURRENT_USER\Software\Citrix\PrinterProperties.

Permanent and Auto-Restored Client Printers

Administrators or Power users can manually add printers by running the Add Printer wizard and creating a local printer that is attached to a client printer port.

Depending upon the type of client printer port to which the printer is attached, there are two types of printer you can create manually:

- Permanent client printers
- Auto-restored client printers (that are automatically restored on subsequent logons)

Permanent Client Printers

A permanent client printer is a manually created printer on a server running Presentation Server that is attached to a legacy style client printer port. A legacy style printer port is a port that was created in Presentation Server 3.0 or earlier. To allow legacy style printer ports to be used, enable the Legacy Printers policy rule.

A permanent client printer remains on the server until it is manually deleted. When the client connects to this printer, the status of the printer is "online" and print jobs will be delivered. When the client disconnects from the printer, the status of the printer is "offline" and additional print jobs that are sent will accumulate in the queue until the client reconnects to the server.

To create a permanent client printer

1. Create a local printer on the server using the Add Printer wizard.
2. Attach the printer to a legacy style client printer port.

   Legacy client printer ports have names using the following format:

   client*CLIENTNAME#**PRINTERNAME*

   Where *CLIENTNAME* is the name of the client workstation and *PRINTERNAME* is the name of the printer on the client

Such legacy ports are tied to the client workstation by name. If a manually created printer is attached to one of these ports, both the port and printer become permanently associated with the server on which they are created.

Whenever the specific client is not connected to the server, the port is marked offline. However, if a session is opened from the client, the port is marked online and any queued print jobs begin to print on the specific client printer.

Permanent client printers are particularly useful if you are using client printers directly attached to thin client devices and want to share them among session users. You can construct the printer on the server by selecting the required driver and appropriate client printer port. After creation, you can adjust the security of the printer to allow the required users to access this client printer.

The printer definitions created on one server can be replicated to other servers by exporting the appropriate registry entries from HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers\ or by scripting the printer creation using PrintUI.dll or PrnAdmin.dll.

Note PrnAdmin.dll is included as part of the Windows Server Resource kit.

Auto-Restored Client Printers

An auto-restored client printer is created manually and attached to a standard port that is tied to the session ID. An auto-restored client printer is down at logoff and rebuilt during logon.

To create an auto-restored client printer

1. Create a printer manually using the Add Printer wizard.
2. Attach the printer to a standard client printer port.

   Standard client printer ports have names with the format:

   client:*ID*:*PRINTERNAME*

   Where *ID* is the session ID number of an active session and *PRINTERNAME* is the name of the printer on the client.

Standard ports are tied to a client only through an active session. During logoff, all of the states associated with an auto-restored printer are retained either on the client or in the server user profile, depending upon the client capabilities and policies in use.

During a subsequent logon, an identical printer is recreated. Restored client printers are recreated exactly as they were originally created, except that the port name is adjusted for the new session and the comment identifies it as *auto-restored*. The security applied is the same as with other auto-created client printers, meaning that the restored printers are accessible only to processes operating in the same session.

As with retained printers, restored printers are monitored by the print manager service. If one of these printers is deleted by an agent other than the print manager service itself, the retained printer definition is removed from the properties stores in the user profile and on the client. Therefore, deleting a restored printer while the session is active erases the retained printer definition.

Configuring Client Printers Policies

Client redirected printers are auto-created using the **Auto-creation** rule setting in a policy. This section describes how to configure such a policy.

To configure an existing policy for auto-creation of client printers

1. In the Presentation Server Console, select the Policies node.
2. On the **Contents** tab, choose the policy you want to configure for printing rules.
3. From the **Actions** menu, choose **Properties**.
4. In the policy's **Properties** dialog box, expand **Printing**, then **Client Printers**.
5. Under **Client Printers**, enable the **Auto-creation** rule. Select either:
    - **Auto-create all client printers**. All network printers and any printers attached to or mapped from the client preconfigured in **Printers and Faxes** are auto-created in the session.
    - **Auto-create local (non-network) client printers only**. Any non-network printers attached to the client preconfigured in **Printers and Faxes** are auto-created in the session.
    - **Auto-create the client's default printer only**. Only the client's default printer that is attached to or mapped from the client preconfigured in **Printers and Faxes** is auto-created in the session.
    - **Do not auto-create client printers**. Client printers are not auto-created.
6. Under **Client Printers**, enable and configure the following rules, as necessary:
    - **Legacy client printers.** Enable this rule to choose the style of client printers that should be auto-created, choosing from:
        - To create printers that use default Citrix Presentation Server 4.0 and later naming conventions, choose **Create dynamic session-private client printers**.
        - To create printers that use printer names that are compatible with Presentation Server 3.0 or earlier, choose **Create old-style client printers**.

- **Printer properties retention.** Enable this rule to control where the server stores modified, client-printer properties, choosing from:

  - To store printer properties on the client or the user profile, choose **Held in profile only if not saved on client**. When no policy is enabled, this setting is the default.

  If the server cannot store printer properties on the client, it stores them in the user profile. In performing the necessary system checking, there may be delays in logon time and use of additional bandwidth.

  Choose this option if your server farm requires backward compatibility with prior versions of Presentation Server and its clients and is not constrained by bandwidth or logon performance.

  - If users are assigned a Terminal Services mandatory profile, choose **Saved on the client device only**. This can be used for a Terminal Service roaming profile

  Only choose this option if all the servers in your farm are running this version of Citrix Presentation Server and your users are using client versions 9.*x* and above.

  - If your server farm includes servers running prior versions of Presentation Server or is constrained by bandwidth and logon speed, or your users use legacy clients, choose **Retained in user profile only**. Note that this is applicable only if a Terminal Services roaming profile is used.

7. Enable the rule Print job routing to allow connecting directly from the server to the print server of a mapped client printer. Then configure according to the following:

   - If the network print server is not across a WAN from the server, choose **Connect directly to network print server if possible**. When no policy is enabled, this setting is the default.

   - If the network print server is across a WAN from both the client device and the server, choose **Always connect indirectly as a client printer**.

8. Save and enable the policy.

Implementing and Managing Network Printers

This section describes how to set up and manage network printers, routing straight from Presentation Server to a print server.

To set up network printers for users

1. Import network printers from a network print server into the farm (see "Importing Print Servers" on page 271).

   To support network printer connections using the Session Printers policy, Presentation Server must know certain information about the network printer to establish the connection. The most important information is the name of the server and the name of the printer on the server. This is usually represented by the pathname of the printer, in the form \\servername\printersharename. Presentation Server also needs to know the driver model to use when constructing the printer connection. This information is collected on import and retained as a list of known print queues. The information associated with a specific print queue can be discovered as needed in the Session Printers policy.

   Importing network print servers into the server farm makes all printers that are connected to the print server available as specified through the Session Printers policy rule. After you install required printer drivers, users can print to these printers in their ICA sessions.

   If the necessary drivers are not included in the Windows native set or native printer driver auto-install is disabled, install the printer drivers for your network printers on a server in the farm. Use the **Replicate Drivers** command to distribute the drivers to all the servers in the farm.

   Note Drivers are installed from the native driver set that is provided with Windows. If a driver cannot be installed from the Windows driver set, the printer is not connected. This prevents drivers from being downloaded automatically by Windows point-and-print facility for any auto-created printer.

   ---

2. Allocate network printers to users through session printers policies.

   When a specified user logs on to a server in the farm, session printer policies determine which printers are automatically available to the user.

   For more information about configuring a policy to use session printers, see "Assigning Network Printers through the Session Printer Policy" on page 271.

Importing Print Servers

To import printers on a print server

1. Select Printer Management in the Presentation Server Console.
2. From the **Network Print Servers** tab, choose **Actions > Printer Management > Import Network Print Server**.
3. Specify the network print server to import. You can import all the printers on the selected server, or select individual printers from the list displayed.
4. Click **OK**.

When the operation finishes, the print server appears on the **Network Print Servers** tab in the Presentation Server Console.

Assigning Network Printers through the Session Printer Policy

Previous versions of Presentation Server and MetaFrame XP allowed an administrator to provision network printer connections to their users. In Presentation Server 4.0 and higher, a similar feature is provided by the Session Printers policy rule.

Filters are available to assign the rule based on client name, client IP, address range, server, user, or group or combinations of these attributes. However, rather than adjusting a system setting, the Session Printer policy provides a mechanism for connecting one or more network printer connections at logon or during a reconnect based on these standard policy filter criteria.

In addition to connecting one or more network printers by policy, the administrator can also apply overrides for the default printer settings for each connected network printer and then choose how the default printer should be set. The default printer can be set to any of the rule's associated network printers, the client's main printer, or left completely undisturbed.

To assign printers using the Session Printers policies

1. In the Presentation Server Console, select the Policies node.
2. From the **Contents** tab, choose the policy for which you want to configure printing rules.
3. From the **Actions** menu, choose **Properties**.
4. In the policy's **Properties** dialog box, expand **Printing**, then select **Session printers**.

When configuring session printers for a policy:

- Identify network printers to which you want the applicable sessions to connect by adding printers to the list
- Use the drop-down list to choose the default printer for all sessions to which the policy is applied
- Use a filter to apply the policy

When multiple policies are applied to a user session, printer rules are merged. For information about policies, see "Using Policies to Configure Access to Published Resources" on page 125.

Limiting Printing Bandwidth

When users access servers through slower networks or dial-up connections, data sent during printing can affect video updates and application performance. To achieve the best performance for some users, you can limit the bandwidth used by print data streams in ICA sessions.

By limiting the data transmission rate for printing, you make more bandwidth available in the ICA data stream for transmission of video, keystrokes, and mouse data. More available bandwidth can help prevent degradation of the user experience during printing.

There are two ways you can limit printing bandwidth in client sessions:

- Use a policy to configure bandwidth session limits
- Use individual server settings to limit printing bandwidth in the server farm (see "Bandwidth Tab" on page 279)

You can set a policy rule to limit bandwidth in sessions to which the policy is applied. Citrix recommends that you apply such a policy to sessions that have slow connection speeds.

To configure a printing bandwidth rule

1. In the left pane of the Presentation Server Console, select the Policies node.
2. In the right pane of the console, select a policy that you apply to sessions with low connection speeds.
3. From the **Actions** menu, choose **Properties**.
4. In the policy **Properties** page, open **Bandwidth > Session Limits**, and choose **Printer**.

5. Use the Printer rule to enable and disable the printing bandwidth session limit. When enabling the printing bandwidth session limit, provide a bandwidth limit in kilobits per second.
6. Click **OK**.

After configuring a printing bandwidth limit in a policy, sessions to which it is applied adhere to the limit. You must apply a policy through a filter for the policy to affect sessions.

Managing Printer Drivers

This section describes how printer drivers are installed and managed in Presentation Server.

Using Advanced Universal Printing

Note Advanced Universal Printing is available only to the latest Windows clients (9.0 or higher).

The Universal Printing feature available with Citrix Presentation Server 4.0 and higher is designed to relieve the burden of administering a multitude of printer drivers, avoid problems with driver maintenance, replication, and other client printing issues.

The universal printing solution employs a Citrix-developed universal driver along with the underlying network infrastructure that allows this driver to remotely manipulate most of the settings of a client-side printer. The universal printer driver is automatically installed on all computers running Presentation Server where it acts like a proxy for printer drivers operating on the Windows client. For example, actual printer capabilities and validated printer document settings are retrieved directly from the client (with intelligent caching) as required by applications on the server.

The universal printer driver facilitates the exchange of capabilities and document settings with the remote client. When a print request is sent, all document settings (including the device-dependent settings) are placed in the spool file. The spool file is then sent to the client for processing.

As well as increased speed and better handling functionality, the universal printer driver provides a **Preview** option that allows a user to preview the print job on the client before printing.

You have the option of using the Advanced Universal Printing feature to create a single generic universal printer that is not bound to any specific client printer. When enabled, this can be used to drive any client printer. This effectively limits the number of auto-creations of printers, thereby limiting the impact on system resources. For information about how to configure this functionality, see Citrix Knowledge Center article CTX 106812.

For a discussion of the technical background to the universal printer driver, see Citrix Knowledge Center article CTX 108170.

Specifying Printer Drivers for Client Printing

When client printers are auto-created, you configure policies to specify whether the client printers use universal drivers available with Universal Printing, native printer drivers that must be installed on the server, or both. Native drivers are installed by default.

To set policy rules that specify which printer drivers to use for sessions

1. In the Presentation Server Console, select the Policies node.
2. On the **Contents** tab, choose the policy for which you want to configure printing rules.
3. From the **Actions** menu, choose **Properties**.
4. In the policy's **Properties** dialog box, expand **Printing**, then **Drivers**.

Under **Drivers**, you can configure the following rules:

Native printer driver auto-install. Use this rule to configure whether or not to install native printer drivers automatically on servers.

You can reduce printer administration by configuring native printer drivers to be installed automatically on servers when printers are auto-created. However, this can become unmanageable over time.

A specific client printer can be created on a server only when its native driver is also installed on the server. A standard set of native printer drivers is provided with the respective Windows Server operating system. Citrix Presentation Server can automatically install printer drivers from the standard Windows drivers and automatically create both network and client printers.

To automatically install native print drivers, enable this rule. Enabling the rule automatically sets **Install Windows native drivers as needed**. This option has the potential to create a large number of printer drivers, and so administrative control over those printer drivers may become difficult. You can limit which drivers are installed by using the driver compatibility list. For more information about how to set up and use a driver compatibility list, see "Maintaining Driver Compatibility Lists" on page 276.

Third-party drivers that are not provided with the respective Windows Server operating system must be manually installed on the server before you can configure Citrix Presentation Server to automatically create the printers that use those drivers. You can also replicate a third-party driver from another server in the farm.

To prevent drivers from being installed automatically, choose the option **Do not automatically install drivers**.

Universal driver. To control the assignment of a universal printer driver for client printers, configure this rule. When you configure the universal driver rule, you can select the following options:

- **Use universal driver only if requested driver is unavailable**. Select this option to use native drivers for client printers, if they are available. If the driver is not available on the server, the client printer is automatically created with the appropriate universal driver.
- **Use only printer model specific drivers**. Select this option if you do not want to use the universal print driver.
- **Use universal driver only**. Select this option if you do not want to use native drivers.

Replicating Printer Drivers

After you install printer drivers (for information about installing printer drivers, see the relevant Windows documentation), you can use the driver replication feature in the Presentation Server Console to copy the driver files and registry settings to other servers in the server farm. This feature saves time when you install printer drivers, and ensures that all drivers are available on all servers so that users can print to the client and network printers in the farm.

Managing Drivers for Auto-Created Printers

Some printer drivers can cause server problems when users print to client printers in the server farm. Because printing to a client printer with a defective driver can cause a fatal system error on a server, you might need to prevent auto-creation of client printers that use certain printer drivers.

If a defective driver is replicated throughout a server farm, it is difficult and time consuming to remove it from every server to prevent its use with client printers. Use the printer driver compatibility feature to designate drivers that you want to allow or prohibit for use with client printers.

Note When you designate a printer driver to be incompatible for printers in the farm, you cannot create a printer driver mapping with the same driver.

Maintaining Driver Compatibility Lists

Citrix Presentation Server has a driver compatibility list for each server platform in use in the server farm.

To add or remove drivers or edit driver names in the compatibility list

1. Under the Printer Management node of the Presentation Server Console, select **Drivers**.
2. From the **Actions** menu, choose **Printer Management > Compatibility**.
3. Use the **Driver Compatibility** dialog box to manage the printer driver compatibility list for each server platform. You can list the printer drivers you allow or the drivers you do not allow to be used in the farm. To add drivers to the list, choose from the menu of all drivers that are installed on servers in the farm.

Citrix Presentation Server by default installs drivers and auto-creates client printers for all users who have client printers installed on their client devices.

When users log on:

- Citrix Presentation Server checks the client printer driver compatibility list before it sets up the client printers
- If a printer driver is on the list of drivers that are not allowed, Citrix Presentation Server does not set up the printer unless the Universal Printing feature is enabled
- When the compatibility list prevents setup of a client printer, Citrix Presentation Server writes a message in the server's Event log

Remapping Client Printer Drivers

The drive remapping feature of Presentation Server allows you to substitute specific Windows printer drivers for client printers. Each client will provide information about these client-side printers during logon, including the printer model name. During client printer auto-creation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The auto-creation process then employs the identified, available printer drivers to construct redirected client print queues.

In some cases, the printer model names provided by the client do not correspond directly to the printer driver names on the Windows server. Autocreation may fail unless the administrator designates a surrogate driver. Administrators may also use this facility to force families of compatible printers to use a single reliable driver.

To remap client printer drivers on a farm-wide basis, use the Presentation Server Console. Alternatively, you can define the driver mappings on each server by using the Wtsuprn.inf mapping file.

To define client printer driver mappings for all servers in the farm

1. In the Presentation Server Console, expand the Printer Management node and select **Drivers.**
2. From the **Actions** menu, choose **Printer Management > Mapping**.
3. In the **Driver Mapping** dialog box, choose a server platform and add the names of client printer drivers that correspond to the drivers you installed on servers in the farm.

To define client printer driver mappings for a specific server

1. Add mapping entries for the specific client and server driver names to the Wtsuprn.txt template file located in the /Program Files/Citrix/System32/ directory.
2. Rename the file to Wtsuprn.inf and copy it to the same directory on all servers on which you want to apply similar mappings.

Note You can use wildcards to match a range of client driver names using a single mapping entry; for example, “hp laserjet*” will match any client driver with an identical prefix.

Setting up Automatic Replication of Printer Drivers

You can set up automatic printer driver replication so Citrix Presentation Server performs replication when you add a server to the farm or when you restart a server in the farm.

Citrix Presentation Server maintains one auto-replication list for each platform in the server farm. When you select a printer driver for replication, Citrix Presentation Server adds the driver to the appropriate auto-replication list. You can add or remove drivers from the auto-replication lists by choosing **Auto-replication** from the **Drivers** tab in the Presentation Server Console.

When you edit the auto-replication list, you can use a specific server or any server as the source for a particular printer driver. If you specify that you want to use any server, Citrix Presentation Server copies the driver from any server that is available in the farm at the time of auto-replication to a new or restarted server. This setting avoids the possibility that a specific source server for a printer driver might be unavailable when new or restarted servers need to receive a printer driver. However, if servers are not consistent, the user's ability to print may not be consistent.

Citrix Presentation Server cannot replicate drivers from network printers (drivers installed on network print servers) because it does not have access to the driver files.

If driver replication fails because of communication errors, the console displays an error message and records the error in the server System log for each server where the operation failed.

Note Administrators have more control over printer driver replication when manual replication is used. Do this during low usage periods.

Configuring Printing with the Presentation Server Console

This section describes the different components of the Presentation Server Console that you can use to configure your printing implementation.

- When you select Printer Management in the Presentation Server Console tree, the right pane displays tabs labeled **Contents**, **Bandwidth**, and **Network Print Servers**
- When you expand the Printer Management node, the left pane displays objects labeled **Printers** and **Drivers** in the tree

Contents Tab

When you select the Printer Management node, the **Contents** tab displays objects labeled **Drivers** and **Printers**.

Network Print Servers Tab

Importing a network print server makes those printers available for assignment through session printer policies.

After you import print servers, the **Network Print Servers** tab displays the name of each print server and the date and time when the Presentation Server Console last updated the print server information. The tab uses the time zone of the machine to which the console is connected for the date and time display. From this tab, an administrator can import network print servers, update network print server information, or discard network print servers.

Bandwidth Tab

When you select the Printer Management node in the Presentation Server Console tree, the **Bandwidth** tab displays the print stream bandwidth setting for each server in the farm.

Note While you can limit print stream bandwidth through server settings, the best practice is to do so through policies. For more information about configuring a policy to include a print stream bandwidth limit, see "Limiting Printing Bandwidth" on page 272.

You can use this tab to set or remove print stream bandwidth limits on servers and copy settings from one server to others. Limiting printing bandwidth can improve application performance for clients when printing and application data must compete for limited bandwidth over the ICA protocol.

Drivers Tab

When you select **Printer Management** > **Drivers** in the Presentation Server Console tree, the right pane displays information about printer drivers installed on servers running Citrix Presentation Server. The driver information includes each driver's name and operating system platform. Select a specific server from the **Server** drop-down menu to display the drivers installed on one server, or select **(Any)** to display all drivers on all servers in the farm.

During the installation of Citrix Presentation Server, unless it is prevented by the Native printer driver auto-install rule, the drivers needed for the auto-creation of client or network printers are installed. Citrix Presentation Server installs these drivers from the primary set of native printer drivers provided with the Windows operating system. If a specific printer driver is not on this list and the Universal Driver is not used, that printer cannot be auto-created until you obtain and install the driver on the servers. After installing the driver on one or more servers, you can use the **Drivers** tab to replicate the installed driver to other servers in the farm.

Use the **Drivers** tab to copy printer drivers to other servers in a farm. If printer drivers are not already installed, copy the drivers to each server where users need access to the driver for printing to client or network printers.

To copy a driver, select the driver and then use the **Replicate Drivers** command from the console toolbar.

Note To display the drivers installed on a server, select a server under the Servers node in the Presentation Server Console tree and select the **Printer Drivers** tab.

Printers Tab

Select **Printers Management** > **Printers**. The **Printers** tab in the right pane lists all of the printers that you can configure in the server farm. The list includes the following printers:

- Local Presentation Server shared printers that you install and connect directly to servers in the farm
- Network printers that are installed and connected to network print servers when you import the print servers into the farm
- Printers discovered and attached through the Session printers policy rule

The printer list shows the printer name, print server name, driver name, and server operating system platform for each local Presentation Server printer. For network printers, the list shows only the printer name and print server name.

Note To connect to a session printer, the end user must have the necessary Windows user or group permissions.

Using the Servers Node

When you select the Servers node in the Presentation Server Console, multiple tabs appear in the right pane. The tab that relates to printer management is the **ICA Printer Bandwidth** tab. This tab displays the same information as the **Bandwidth** tab that appears when you select Printer Management in the Presentation Server Console tree. See "Bandwidth Tab" on page 279.

Printers Tab

When you select a server under the Servers node in the Presentation Server Console and click the **Printers** tab in the right pane, information about a server's local printers is displayed. For printer information to appear, you must have selected the Shared option when you install the printers. Information is not displayed for printers that you did not share.

You can select a local printer on the **Printers** tab and use the console to replicate the drivers and settings for the printer to other servers.

Printer Drivers Tab

When you select a server under the Servers node in the Presentation Server Console tree and click the **Printer Drivers** tab, a list of the printer drivers that are installed on the server appears. Select a driver name in the list to display the names of all the servers that have the driver installed. Use the Replicate Drivers command on the toolbar to copy the driver to other servers in the farm. Copy printer drivers to each server on which they must be accessible for users to send print jobs to client or network printers.

Note The Replicate Drivers process can take considerable time, and requires a lot of system resources. Citrix recommends that you consider running this process outside of normal office hours.

APPENDIX A

Citrix Presentation Server Commands

This appendix describes Citrix Presentation Server commands. They provide additional methods for maintaining and configuring servers and farms. These commands must be run from a command prompt on a server running Citrix Presentation Server.

Command	Description
acrcfg	Configure auto-reconnect settings.
aierun	Run isolation environment. Primarily for use in scripting environments.
aiesetup	Install or uninstall an application from an isolation environment.
altaddr	Specify server alternate IP address.
app	Run application execution shell.
apputil	Add servers to Configured Servers list for published applications.
auditlog	Generate server logon/logoff reports.
change client	Change client device mapping.
chfarm	Change the server farm membership of the server.
cltprint	Set the number of client printer pipes.
ctxkeytool	Generate, enable, disable, and retrieve a farm key for IMA encryption.
ctxxmlss	Change the Citrix XML Service port number.
driveremap	Remap the server's drive letters for 32-bit systems.
driveremap64	Remap the server's drive letters for 64-bit systems.
dscheck	Validate the integrity of the server farm data store.
dsmaint	Configure the server farm's data store.
enablelb	Enable load balancing for servers that fail health monitoring tests.
icaport	Configure TCP/IP port number used by the ICA protocol on the server.
imaport	Change IMA ports.

Command	Description
migratetosqlexpress	Migrate the server farm's data store from a Microsoft Access database to a SQL Server 2005 Express Edition SP1 database.
query	View information about server farms, processes, servers, ICA sessions, and users.
rademaint	Revoke offline access and return the license to the pool even if the offline license has not expired.
twconfig	Configure ICA display settings.

ACRCFG

Use **acrcfg** to configure Auto Client Reconnect settings for a server or a server farm.

Syntax

acrcfg [**/server:***servername* **|** /**farm**] [**/query | /q**]

acrcfg [**/server:***servername* **|** /**farm**] [**/require:**on | off] [**/logging:**on | off]

acrcfg [**/server:***servername*] [**/inherit:**on | off] [**/require:**on | off] [**/logging:**on | off]

acrcfg [**/?**]

Parameters

servername
The name of a server running Citrix Presentation Server.

Options

Caution The **/inherit** and **/farm** options are incompatible; therefore, avoid using these options at the same time.

/query, /q
Query current settings.

/server
The server to be viewed or modified by the other command-line options. The server specified by *servername* must be in the same server farm as the server on which the command is run. This option and the /**farm** option are mutually exclusive. The local server is the default if neither /**server** nor /**farm** is indicated.

/farm
The options on the command-line after /**farm** are applied to the entire server farm.

/inherit:on | **off**
To use the Auto Client Reconnect settings from the server farm, set /**inherit** to **on** for a server. To disregard the Auto Client Reconnect settings from the server farm, set /**inherit** to **off**. By default, /**inherit** is set to **on** for a server.

Note The **/inherit** option must be used in conjunction with the **/server** option.

/require:on | **off**

If you want users to be prompted for credentials during automatic reconnection, set /**require** to **on**. Servers inherit the server farm setting unless /**inherit** is **off**. To allow users to automatically reconnect to disconnected sessions without providing credentials, set /**require** to **off**. By default, /**require** is set to **off** for both a server and a server farm.

/logging:on | **off**

You can enable logging of client reconnections in the Application Event log on a server. Logging can be set only when /**required** is set to **off**. Logging is set to **off** for both servers and server farms by default.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

Enabling automatic client reconnection allows users to resume working where they were interrupted when an ICA connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

However, automatic reconnection can result in a new ICA session being launched (instead of reconnecting to an existing session) if a client's cookie, containing the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be reentered because /**require** is set to **on**. Auto Client Reconnect is not triggered if users intentionally disconnect.

The Auto Client Reconnect feature is enabled by default and can be disabled using Appsrv.ini or an ICA file only on the Client for Windows or with the Web Interface.

The /**require** and /**logging** options are valid with either /**server** or /**farm**, but /**inherit** is not used with /**farm**. If neither /**server** nor /**farm** is selected and the /**inherit**, /**require**, or /**logging** options are used, they are applied to the local server. You can set /**require** only when /**inherit** is set to **off**. You can set logging only when /**require** and /**inherit** are set to **off**. When logging is not valid, it disappears from later queries. A query shows the required setting whether or not it is on.

Settings and values are not case-sensitive.

Examples

The following four commands result in the following configurations:

- Require users to enter credentials when they automatically reconnect to servers configured to inherit farm-wide settings
- Show the results
- Allow users to be reauthenticated automatically to the local server and set the server to log client reconnections
- Show the results

```
C:\>acrcfg /farm /require:on

Update successful
C:\>acrcfg /farm /q
Auto Client Reconnect Info for: Farm-wide Settings
REQUIRE:       on
C:\>acrcfg /inherit:off /require:off /logging:on
Update successful
C:\>acrcfg /q
Auto Client Reconnect Info for: Local Server
INHERIT:       off
REQUIRE:       off
LOGGING:       on
```

Security Restrictions

You must be a Citrix administrator to make changes.

AIERUN

Use **aierun** to launch an application into an isolation environment.

Syntax

aierun [/64] [/w] *AIE_Name Application* [*application parameters*]

aierun [/?]

Parameters

AIE_Name
The name of an isolation environment.

Application
The name of the application to launch in the named isolation environment. You can also append application parameters, if any.

Options

/w
Waits for the application launched by **aierun** to exit before continuing. This option is useful when **aierun** is used in a script or batch file.

/?
Displays the syntax for the command and information about the command options.

/64
Defines the application as 64-bit so that the SYSTEM32 and SYSWOW64 directories are properly set up.

Remarks

aierun is an internal launcher used by Citrix Presentation Server during application launching.

Use of **aierun** from a desktop session is not supported.

Security Restrictions

None.

AIESETUP

Use **aiesetup** to install an application into an isolation environment.

Syntax

aiesetup [/d] [/n] [/q] [/64] [/w] *AIE_Name Setup_application* [*application parameters*]

aiesetup [/e] *AIE_Name*

aiesetup [/?]

Parameters

AIE_Name
The name of an isolation environment.

Setup_application
The name of an application installer, such as an .msi, to run. You can also append any parameters that the installer is required to process at runtime. When using **aiesetup** with an .msi file, use **msiexec.exe** with the **/i** option.

Options

/d
Disables the automatic discovery process for the isolation environment.

/n
Disables automatically setting the Windows server to install mode (through the **change user install** command).

/q
Installs the application in quiet mode and does not require user intervention, such as pressing **Enter** to begin discovery prompt. This is useful in automated application deployments, such as when using Installation Manager.

/w
Waits for the application launched by **aiesetup** to exit before continuing. This option is useful when **aiesetup** is used in a script or batch file.

/64
Defines the application as 64-bit so that the SYSTEM32 and SYSWOW64 directories are properly set up.

/e
Enumerates the applications in the specified isolation environment.

/?
Displays the syntax for the command and command option information.

Usage

aiesetup launches the specified application installer and forces the application to install within the specified isolation environment.

At runtime, if you did not use the **/d** option, **aiesetup** displays the following message at a command prompt:

```
Press <Enter> to start the application discovery process when
application installation completes.

Press Q to skip application discovery and quit.
```

When installation is complete, the silent application discovery process is invoked. The application discovery process locates application shortcuts added by the installer and adds the information to the data store. Data collected by the application discovery process facilitates publishing of applications installed in an isolation environment.

Press **Q** to omit the application discovery process if it is not already running and return to a command prompt. Alternatively, you can use the /d option with Aiesetup to omit the application discovery process.

Remarks

Application isolation functionality includes the ability to install applications into an isolation environment as well as uninstall applications installed into an isolation environment. This is useful in cases when different versions of an application cannot be installed on a single server.

To install an application into an isolation environment, follow the procedure outlined below.

1. Create an isolation environment with isolation rules as appropriate. For information about creating isolation environments, see "Creating an Isolation Environment" on page 145.
2. Ready a copy of the .msi or .exe file for the application to be installed into the isolation environment.

AIESetup discovers installed applications only if their link files or shortcuts are created in either \document and settings*user*\StartMenu\Programs or \document and settings\AllUsers\StartMenu\Programs. If an application installer does not create a .LNK file in one of these folders, then the application is not discovered by AIESetup even when it is installed in isolation.

Security Restrictions

To execute **aiesetup**, you must be a Citrix administrator with the permissions to perform the following tasks:

- Manage isolation environments for the farm
- Publish applications and edit properties for the farm

Run the **aiesetup** command on the server where you are installing the application. Citrix does not support installing an application into an isolation environment through a remote desktop connection.

ALTADDR

Use **altaddr** to query and set the alternate (external) IP address for a server running Citrix Presentation Server. The alternate address is returned to clients that request it and is used to access a server that is behind a firewall.

Syntax

altaddr [**/server:***servername*] [**/set** *alternateaddress*] [**/v**]

altaddr [**/server:***servername*] [**/set** *adapteraddress alternateaddress*] [**/v**]

altaddr [**/server:***servername*] [**/delete**] [**/v**]

altaddr [**/server:***servername*] [**/delete** *adapteraddress*] [**/v**]

altaddr [**/?**]

Parameters

servername
The name of a server.

alternateaddress
The alternate IP address for a server.

adapteraddress
The local IP address to which an alternate address is assigned.

Options

/server:*servername*
Specifies the server on which to set an alternate address. Defaults to the current server.

/set
Sets alternate TCP/IP addresses. If an *adapteraddress* is specified, *alternateaddress* is assigned only to the network adapter with that IP address.

/delete
Deletes the default alternate address on the specified server. If an adapter address is specified, the alternate address for that adapter is deleted.

/v (verbose)
Displays information about the actions being performed.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

The server subsystem reads the **altaddr** settings for server external IP addresses at startup only. If you use **altaddr** to change the IP address setting, you must restart the IMA Service for the new setting to take effect.

If **altaddr** is run without any parameters, it displays the information for alternate addresses configured on the current server.

Examples

Set the server's alternate address to 1.1.1.1:

```
altaddr /set 1.1.1.1
```

Set the server's alternate address to 2.2.2.2 on the network interface card whose adapter address is 1.1.1.1:

```
altaddr /set 2.2.2.2 1.1.1.1
```

Security Restrictions

None.

APP

App is a script interpreter for secure application execution. Use **App** to read execution scripts that copy standardized .ini type files to user directories before starting an application, or to perform application-related cleanup after an application terminates. The script commands are described below.

Syntax

app *scriptfilename*

Parameter

scriptfilename
The name of a script file containing app commands (see script commands below).

Remarks

If no *scriptfilename* is specified, **app** displays an error message.

The Application Execution Shell reads commands from the script file and processes them in sequential order. The script file must reside in the %SystemRoot%\Scripts directory.

Script Commands

The script commands are:

copy *sourcedirectory\filespec targetdirectory*
Copies files from *sourcedirectory* to *targetdirectory. Filespec* specifies the files to copy and can include wild cards (*,?).

delete *directory\filespec*
Deletes files owned by a user in the *directory* specified. *Filespec* specifies the files to delete and can include wild cards (*,?). See the Examples section for more information.

deleteall *directory\filespec*
Deletes all files in the *directory* specified.

execute
Executes the program specified by the path command using the working directory specified by the **workdir** command.

path *executablepath*
Executablepath is the full path of the executable to be run.

workdir *directory*
Sets the default working directory to the path specified by *directory.*

Script Parameters

directory
A directory or directory path.

executablepath
The full path of the executable to be run.

filespec
Specifies the files to copy and can include wildcards (*,?).

sourcedirectory
The directory and path from which files are to be copied.

targetdirectory
The directory and path to which files are to be copied.

Examples

The following script runs the program Notepad.exe. When the program terminates, the script deletes files in the Myapps\Data directory created for the user who launched the application:

```
PATH C:\Myapps\notepad.exe
WORKDIR C:\Myapps\Data
EXECUTE
DELETE C:\Myapps\Data\*.*
```

The following script copies all the .wri files from the directory C:\Write\Files, executes Write.exe in directory C:\Temp.wri, and then removes all files from that directory when the program terminates:

```
PATH C:\Wtsrv\System32\Write.exe
WORKDIR C:\Temp.wri
COPY C:\Write\Files\*.wri C:\Temp.wri
EXECUTE
DELETEALL C:\Temp.wri\*.*
```

The following example demonstrates using the script file to implement a front-end registration utility before executing the application Coolapp.exe. You can use this method to run several applications in succession:

```
PATH C:\Regutil\Reg.exe
WORKDIR C:\Regutil
EXECUTE
PATH C:\Coolstuff\Coolapp.exe
WORKDIR C:\Temp
EXECUTE
DELETEALL C:\Temp
```

Security Restrictions

None.

APPUTIL

Use **apputil** to add servers to the Configured Servers list for a published application and to install or uninstall Installation Manager packages or package groups on specified servers.

Syntax

apputil [**/?**]

apputil [**/q**]

apputil [**/i** *applicationID servername*]

apputil [**/u** *applicationID servername*]

apputil [**/qj** *jobID*]

apputil [**/qp**]

apputil [**/ip** *packageID servername* [/AIE *AIE_Name*] [**reboot**]]

apputil [**/up** *packageID servername* [/AIE *AIE_Name*] [**reboot**]]

Parameters

applicationID
The ID of a published application, as displayed by the /**q** option.

servername
For the /**i** and /**u** options, this is the name of the server to add to the Configured Servers list for the published application. For the /**ip** and /**up** options, this is the name of the server that the Installation Manager package or package group will be installed on or uninstalled from.

jobID
The ID of job that installs or uninstalls an Installation Manager package or package group.

packageID
The ID of an Installation Manager package or package group, as displayed by the /**qp** option.

AIE_Name
The name of an isolation environment.

Options

/?
Display the syntax for the utility and information about the utility's options.

/q

Queries a list of all available published applications, published desktops, and published applications bundled into Installation Manager packages.

/i

Add a server to the Configured Servers list for a specified published application.

You can use the /**i** option with the following types of published resources:

- **Standard published applications.** Note that any server-specific overrides you configure when you publish the application (such as overrides to the command line and working directory entries) are not applied to the specified server when it is added to the Configured Servers list. To use the /**i** option with the published application, be sure that the target application is located in the default location you specify when you published the application.
- Published server desktops.
- **Installation Manager packages.** When you run **apputil** for published applications associated with Installation Manager packages, the packaged application is scheduled for immediate installation on the target host, and the server is added to the Configured Servers list for the published application.

/u

Remove a server from the Configured Servers list for a specified published application. Note that if the application published an Installation Manager package, that package is not uninstalled from the target host.

/qj

Query the status of a specified job. Typically, a job's status progresses from *Pending* to *Started* to *Success*.

/qp

Query a list of all available Installation Manager packages and package groups.

/ip

Schedule the installation of an Installation Manager package or package group on a specified server. The /**AIE** option identifies the application isolation environment where the package or package group should be installed. Use **reboot** to force the server to restart after the job completes.

/up

Schedule the uninstall of an Installation Manager package or package group on a specified server. The /**AIE** option identifies the application isolation environment from where the package or package group should be uninstalled. Use **reboot** to force the server to restart after the job completes.

Remarks

You must run this utility from a server running Citrix Presentation Server Enterprise Edition and Installation Manager.

When you use the /**i** option with an Installation Manager package, an unnamed Installation Manager job is created. When the job completes successfully, connections to the published application are enabled on the server.

When you manually add servers to the Configured Servers list for Installation Manager packages, or install and uninstall packages or package groups, you can schedule when this should occur. However, when you use the **apputil** utility, these tasks are scheduled immediately.

If an error occurs during execution of the utility, the process exit code "1" is returned. **Apputil** returns "0" on success.

Examples

The following examples display the correct syntax and usage for the **apputil** utility.

```
C:\>apputil /q
Available published applications: 3.
Application ID      Type         Description
2e0e-0009-000010a9  Application  Word
2e0e-0009-000010ac  Desktop      Desktop
2e0e-0009-000010af  Package      Acrobat Reader

C:\>apputil /i 2e0e-0009-000010a9 SERVERA
Success. The published application is now configured for the
specified server.

C:\>apputil /i 2e0e-0009-000010ac SERVERA
Success. The published desktop is now configured for the
specified server.

C:\>apputil /i 2e0e-0009-000010af SERVERA
Success. The packaged application has been scheduled for
immediate installation.

C:\>apputil /qp
There are 2 packages and package groups available.
Package ID            Type           Description
05d1-007a-00000301    Package Group  Accounts Package Group
05d1-0037-00000300    Package        Acrobat Reader

C:\>apputil /ip 05d1-007a-00000301 SERVERA

Successfully scheduled install job. Job ID: 05d1-0038-000003b8

C:\>apputil /qj 05d1-0038-000003b8

Job status: SUCCESS
```

Running the following script (Rollout.cmd) adds a server specified as a command-line parameter, to the Configured Servers list for a published application.

```
AppUtil.exe /i 397e-0009-00000430 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-00000491 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-00000494 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-0000049a %1
@IF ERRORLEVEL 1 goto Error
@ECHO Success!
@GOTO End
:Error
@ECHO Failure!
:End
Usage: Rollout.cmd <server>
```

Security Restrictions

To run this utility, you must be a Citrix administrator with the permissions to perform the following tasks:

- To use the /**q** option, you must at least have permission to view published applications and content.
- To use the /**i** or /**u** options for published applications and published desktops, you must have permission to view published applications, to publish applications, and to edit a published application's properties.
- To use the /**i** option for Installation Manager packaged applications, you must have permission to edit Installation Manager, in addition to the permissions described above.
- To use the /**qp** and /**qj** options, you must have View Installation Manager permission.

To use the /**ip** and /**up** options for Installation Manager packages or package groups, you must have Install and Uninstall Packages permission.

AUDITLOG

Auditlog generates reports of logon/logoff activity for a server based on the Windows Server security event log. To use **auditlog**, you must first enable logon/logoff accounting. You can direct the auditlog output to a file.

Syntax

auditlog [*username* | *session*] [**/eventlog:***filename*] [**/before:***mm/dd/yy*] [**/after:***mm/dd/yy*] [[**/write:***filename*] | [**/detail** | **/time**] [**/all**]]

auditlog [*username* | *session*] [**/eventlog:***filename*] [**/before:***mm/dd/yy*] [**/after:***mm/dd/yy*] [[**/write:***filename*] | [**/detail**] | [**/fail**] | [**/all**]]

auditlog [**/clear:***filename*]

auditlog [**/?**]

Parameters

filename
The name of the eventlog output file.

session
Specifies the session ID for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular session.

mm/dd/yy
The month, day, and year (in two-digit format) to limit logging.

username
Specifies a user name for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular user.

Options

/eventlog:*filename*
Specifies the name of a backup event log to use as input to **auditlog**. You can back up the current log from the Event Log Viewer by using **auditlog /clear:***filename.*

/before:*mm/dd/yy*
Reports on logon/logoff activity only before *mm/dd/yy.*

/after:*mm/dd/yy*
Reports on logon/logoff activity only after *mm/dd/yy.*

/write:*filename*
Specifies the name of an output file. Creates a comma-delimited file that can be imported into an application, such as a spreadsheet, to produce custom reports or statistics. It generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on.

If *filename* exists, the data is appended to the file.

/time
Generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on. Useful for gathering usage statistics by user.

/fail
Generates a report of all failed logon attempts.

/all
Generates a report of all logon/logoff activity.

/detail
Generates a detailed report of logon/logoff activity.

/clear:*filename*
Saves the current event log in *filename* and clears the Event log. This command does not work if *filename* already exists.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

Auditlog provides logs you can use to verify system security and correct usage. The information can be extracted as reports or as comma-delimited files that can be used as input to other programs.

You must enable logon/logoff accounting on the local server to collect the information used by **auditlog**. To enable logon/logoff accounting, log on as a local administrator and enable logon/logoff accounting with the Audit Policy in Microsoft Windows.

Security Restrictions

None.

CHANGE CLIENT

Change client changes the current disk drive, COM port, and LPT port mapping settings for a client device.

Syntax

change client [**/view | /flush | /current**]

change client [{**/default | [/default_drives**] | [**/default_printers**]} [**/ascending**]] [**/noremap**] [**/persistent**] [**/force_prt_todef**]

change client [**/delete** *host_device*] [*host_device client_device*] [**/?**]

Parameters

host_device
The name of a device on the host server to be mapped to a client device.

client_device
The name of a device on the client to be mapped to *host_device.*

Options

/view
Displays a list of all available client devices.

/flush
Flushes the client drive mapping cache. This action forces the server and the client to resynchronize all disk data. See "Remarks" for more information.

/current
Displays the current client device mappings.

/default
Resets host drive and printer mappings to defaults.

/default_drives
Resets host drive mappings to defaults.

/default_printers
Resets host printer mappings to defaults.

/ascending
Uses ascending, instead of descending, search order for available drives and printers to map. This option can be used only with **/default**, **/default_drives**, or **/default_printer**.

/noremap
If **/noremap** is specified, client drives that conflict with server drives are not mapped.

/persistent
Saves the current client drive mappings in the client device user's profile.

/force_prt_todef
Sets the default printer for the client session to the default printer on the client's Windows desktop.

/delete *host_device*
Deletes the client device mapping to *host_device.*

/? (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

You can use **chgcdm** as a shortened form of the **change client** command.

Typing **change client** with no parameters displays the current client device mappings; it is equivalent to typing **change client /current**.

Use **change client** *host_device client_device* to create a client drive mapping. This maps the *client_device* drive letter to the letter specified by *host_device;* for example, **change client v: c:** maps client drive C to drive V on the server.

The **/view** option displays the share name, the share type, and a comment describing the mapped device. Sample output for **change client /view** follows:

```
C:>change client /view
Available Shares on client connection ICA-tcp#7
```

Sharename	Type	Comment
\\Client\A$	Disk	Floppy
\\Client\C$	Disk	FixedDrive
\\Client\D$	Disk	CdRom
\\Client\LPT1:	Printer	Parallel Printer
\\Client\COM1:	Printer	Serial Printer

The **/flush** option flushes the client drive cache. This cache is used to speed access to client disk drives by retaining a local copy of the data on the server running Citrix Presentation Server. The time-out for hard drive cache entries is 60 seconds and the time-out for diskette data is two seconds. If the client device is using a multitasking operating system and files are created or modified, the server does not know about the changes.

Flushing the cache forces the data on the server to be synchronized with the client data. The cache time-out for diskettes is set to five seconds because diskette data is usually more volatile; that is, the diskette can be removed and another diskette inserted.

The **/default** option maps the drives and printers on the client device to mapped drives and printers on the server running Citrix Presentation Server. Drives A and B are always mapped to drives A and B on the server. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the server. If the corresponding drive letter is in use on the server, the default action is to map the drive to the highest unused drive letter. For example, if both computers have drives C and D, the client drives C and D are mapped to V and U respectively. These default mappings can be modified by the **/ascending** and **/noremap** options.

The **/default_printers** option resets printer mappings to defaults. **/default_printers** attempts a one-to-one mapping of all client printers; for example, the client's LPT1 and LPT2 ports are mapped to the server's LPT1 and LPT2 ports. If the **/ascending** option is specified, the mapping is done in ascending order.

The **/default_drives** option resets host drive mappings to defaults. **/default_drives** attempts a one-to-one mapping of all client drives; for example, client drives A and B are mapped to server drives A and B. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the server. If the corresponding drive letter is in use on the server, the default action is to map the drive to the highest unused drive letter. For example, if both computers have drives C and D, the client drives C and D are mapped to V and U respectively. If the **/ascending** option is specified, the mapping is done in ascending order.

The **/ascending** option causes the mapping to occur in ascending drive letter order. For example, if the first two available drive letters on the server are I and J, drives C and D in the preceding example are mapped to I and J respectively.

The **/noremap** option causes the mapping to skip drive letters occupied on the server. For example, if the server has a drive C but no drive D, the client's drive C is mapped to D on the server, but the client's drive D is not mapped.

The **/persistent** option causes the current device mappings to be saved in the user's profile. Drive conflicts can occur if the **/persistent** option is in use and the user logs on from a client device that has a different disk drive configuration, or logs on to a server that has a different disk drive configuration.

The **/force_prt_todef** option sets the default printer for the ICA session to the default printer on the client's Windows desktop.

Security Restrictions

None.

CHFARM

Change farm is used to change the farm membership of a server. The **chfarm** utility is installed in %ProgramFiles%\citrix\system32\citrix\IMA. To run this utility, choose **Run** from the **Start** menu. Enter **chfarm**.

Caution Be sure that the Presentation Server Console and the Access Management Console are closed before you run the chfarm command. Running chfarm while the console is open can result in loss of data and functionality.

Syntax

chfarm

Remarks

chfarm lets you move a server to another farm. Specifically, you can move the server to an existing farm, or you can create a new server farm at the same time that you move the server. Citrix recommends that you back up your data store before running **chfarm**. **chfarm** stops the IMA Service on the server.

Important If the server you want to move provides information for a Resource Manager summary database, update the summary database before using **chfarm**. If you do not update the summary database, you will lose approximately 24 hours worth of summary data stored on the server. To update the summary database, click the Resource Manager node in the Presentation Server Console, select the **Summary Database** tab, and click **Update** Now.

When you run **chfarm**, it starts the Citrix Presentation Server Setup wizard. On the first page, you can join an existing server farm or create a new server farm.

The wizard continues and you specify an existing data store (to join an existing server farm) or set up a new data store (if you create a new server farm). While running **chfarm**, you are prompted for the user name and password of the user you want to designate as the initial Citrix administrator for the farm. For information about data store setup and server farm configuration, see “Planning the Data Store” on page 33.

If you are creating a new farm and you want to enable IMA encryption, you can enable it using the same methods that are available in Citrix Presentation Server Setup. For more information, see “Step 6: Enabling IMA Encryption” on page 65.

If you are moving the server to a farm with IMA encryption enabled, you must provide access to or load the key file for the farm you are joining to the server you are moving. The Setup wizard prompts you to either **Install Key From File** or **Use Previously Loaded Key** the same way as it does when you are joining an existing farm during Setup. If you are moving the server to a new farm that you are creating with the **chfarm** command, Setup provides you with the same options that you would see if you were creating a farm for the first time during Setup. **Chfarm** prompts you for the key for the new farm when you run the **chfarm** command. For more information, see "To specify the location of the IMA encryption key file on a server that is joining a farm" on page 76.

If **chfarm** reports any error, continuing the process can corrupt the data store. If you cancel the data store configuration part of the Citrix Presentation Server Setup wizard, the server you are switching rejoins the original farm.

After the farm membership is changed or a new farm is created, restart the server.

Do not remove a server that hosts a server farm's data store from the server farm, unless all other servers are removed first. Doing so renders the farm unstable.

Important Notes for SQL Server Express Data Stores

- If you want to use SQL Server 2005 Express Edition SP1 to host a new server farm's data store, a named instance must be installed on the server on which you run **chfarm**. The default named instance that chfarm uses is CITRIX_METAFRAME.
- Running **chfarm** does not automatically install SQL Server 2005 Express Edition SP1; you must install it separately.
- Use these options when running **chfarm** to create a new farm with SQL Server 2005 Express Edition SP1 as the data store:

/instancename:<*name*>
: The name of the SQL Server 2005 Express Edition SP1 instance to which to migrate. The default value is CITRIX_METAFRAME.

/database:<*name*>

The name of the SQL Server 2005 Express Edition SP1 database to which to migrate. The default value is MF20.

Note You cannot migrate a database to the same named instance of SQL Server Express that is already in use. If you are already using SQL Server Express and you want to migrate to a new farm using SQL Server 2005 Express Edition SP1, you must either migrate to another database (Access or a third-party database) and then back to SQL Server 2005 Express Edition SP1, or install another named instance of SQL Server 2005 Express Edition SP1 and then launch **chfarm** with the /**instancename** option.

To move a server to a new server farm using SQL Server Express as the data store

1. Create a named instance of SQL Server 2005 Express Edition SP1 by installing it on the first server in the new farm.
2. Run **chfarm** on the server that you want to use to create the new farm using the /instancename: *name* option, where *name* is the name of the instance of SQL Server Express you created in Step 1.

Note If you name an instance of SQL Server 2005 Express "CITRIX_METAFRAME," you do not need to use the /**instancename** option.

CLTPRINT

Use **cltprint** to set the number of printer pipes for the client print spooler.

Syntax

cltprint [**/q**] [**/pipes**:*nn*] [**/?**]

Options

/q

Displays the current number of printer pipes.

/pipes:*nn*

Sets the specified number of printer pipes. The number represented by *nn* must be from 10 to 63.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

Printer pipes are used to send data from applications to client print spoolers. The number of pipes specifies the number of print jobs that can be sent to the spooler simultaneously.

The default number of printer pipes is 10.

The Spooler service must be stopped and restarted after changing the number of pipes. Print jobs already spooled continue printing.

Print jobs sent to the spooler trigger an error message while the service is stopped. Make sure no users start printing during the time the Spooler service is stopped.

Security Restrictions

None.

CTXKEYTOOL

Use **ctxkeytool** to enable and disable the IMA encryption feature and generate, load, replace, enable, disable, or retrieve lost farm keys (**backup**). See remarks for important information about the sequence of commands. The ctxkeytool is located in the Support folder of the Server CD for Presentation Server.

Syntax

ctxkeytool [generate | load | backup] *filepath*

ctxkeytool [enable | disable | query | newkey]

Options

generate

Creates a new key and saves it to the *filepath*. (This command alone is not sufficient to enable IMA encryption.)

load

Can be used to load:

- A new key onto a server with no preexisting key
- The correct key onto a server that has an existing key

newkey

Can be used to

- Load a new key on the data store and enable the IMA encryption feature
- Replace an old key with a new key

backup

Generate a transferable version of a lost key. To retrieve a lost key, run this option on a server that still has a valid key loaded.

enable

Re-enables the IMA encryption feature for the farm but only after you have disabled the IMA encryption feature. Before using this option, you must have the existing, previously enabled key on the farm.

disable

Disables the IMA encryption feature for the farm. Running this command requires reentering your Configuration Logging database password in the Access Management Console.

query

Can be used to check:

- For a key on the local computer
- To see if IMA encryption is enabled for the farm
- If your key matches the farm key

Remarks

The first time you generate a key for the first server on the farm on which you are enabling IMA encryption, use the following sequence of options: **generate**, **load**, and **newkey**. On each subsequent server in the farm, you just need to **load** the key. After you activate the IMA encryption feature on one server, the feature is enabled for the entire farm.

If you lose the key file for a server, you can get a duplicate key file by running the **backup** option on another server in the same farm that still its a key. This command recreates the key file. After recreating the key file, use **load** to load it to the server on which it was lost and then use **newkey** to enable the IMA encryption feature.

After using the **disable** option to disable the IMA encryption feature, you must reenter the configuration logging database password. If you want to activate the IMA encryption feature again, run **enable** on any server in the farm.

Security Restrictions

Only Citrix administrators with local administrator privileges can run **ctxkeytool**.

CTXXMLSS

Use **ctxxmlss** to change the Citrix XML Service port number.

Syntax

ctxxmlss [/**r***nnn*] [/**u**] [/**k***nnn*] **[/b:a] [/b:l]** [/**?**]

Options

/r*nnn*

Changes the port number for the Citrix XML Service to *nnn*.

/u

Unloads Citrix XML Service from memory.

/k*nnn*

Keeps the connection alive for *nnn* seconds. The default is nine seconds.

/b:a

Binds the service to all network interfaces. This is the default setting.

/b:l

Binds the service to localhost only.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

For more information, see "Step 9: Configuring the Citrix XML Service Port" on page 70.

Security Restrictions

None.

DRIVEREMAP

Use the **driveremap** utility to change the server's drive letters on a 32-bit operating system or to update the 32-bit SQL Server 2005 Express Edition SP1 or SQL Server database locations. Citrix Presentation Server Setup installs this utility (driveremap.exe) in the \Program Files\Citrix\System32 directory.

Important Considerations

- If you are using a 64-bit operating system, run the **driveremap64** command.
- You must run this command from a network share or CD-ROM drive.
- Do not use the **driveremap** utility on a server with .NET 2.0 installed. You can install .NET 2.0 after you remap server drives.
- If you are installing Citrix Presentation Server on a server that is not running a previous version of Presentation Server, run the **driveremap** utility before you install Citrix Presentation Server. Citrix recommends that you do not change server drive letters after you install Citrix Presentation Server or applications you want to publish for users to access.

Syntax

driveremap /?

driveremap /dbscript:*filename*

driveremap /drive:M

driveremap /u

driveremap /noreboot

driveremap /IME

Options

The following parameters can be used with **driveremap** at a command line.

/?

Displays the syntax for the utility and information about the utility's options.

/dbscript:*filename*

Sets the path to Fixsecuritydatabase.cmd to *filename*. For Windows Server 2003, the Fixsecuritydatabase utility is run to update drive information in the Windows security database after you remap the system drive.

If you run **driveremap** from a location other than the Citrix Presentation Server CD, use the /**dbscript** switch to specify the path to Fixsecuritydatabase.cmd. If you copy Fixsecuritydatabase.cmd to a folder with the same relative location to Driveremap.exe as on the Citrix Presentation Server CD (\Support\Install\Fixsecuritydatabase.cmd), you do not need to specify a new path with the /**dbscript** switch.

After remapping drives on Windows Server 2003, ensure that you restart the server and log on with an administrator account that has read access to the Fixsecuritydatabase.cmd file specified by /**dbscript**.

/drive:M
Specifies the drive letter to use for the first remapped drive.

/u
Permits unattended or silent installation where no dialog boxes appear and no user input is required. You must use this option in conjunction with the /**drive:** option.

/noreboot
Surpresses the Restart Computer message and does not restart the system. Citrix strongly recommends that you restart the system after running this utility.

/ime[*filename***]**
Changes the drive letter specified in Software\Microsoft\Windows\CurrentVersion\Ime\Japan\IMEJP \Dictionaries for all of the loaded hives under HKEY_USERS.

Remarks

The **driveremap** utility allows you to select the drive letters you want to map. Before installation, you can run the Drive Remapping utility from the autorun screens of the Citrix Presentation Server CD. After installing Citrix Presentation Server, you can open the utility by running Driveremap.exe with no parameters.

Caution Do not run **driveremap** within an ICA or RDP session, for example from a command prompt of a server desktop published as an application. Running **driveremap** in an ICA or RDP session can cause the server to become unstable.

Examples

The following command remaps the server's drive letters. The first available drive is changed to M. The command uses the **noreboot** option, which suppresses the appearance of any dialog boxes.

```
driveremap /u /drive:M /noreboot
```

The following command returns the server's drive letters to the drive letters that start at C and then prompts you to restart the server.

driveremap /u /drive:M /drive:C

Known Issues

The following items are known issues you may encounter when running the **driveremap** utility.

- When running **driveremap** with no parameters, the drive letter choices in the drop-down list may be unavailable. This can occur if the server has non-contiguous drive letters; for example, C, D, X. The mapped drive letters are spread over the interval [a..z] and no reasonable interval shifting can be performed. Network drives are also taken into account.

  To work around this issue, change the drive letters to C, D, and E and then run the **driveremap** utility.

- At a command prompt, if you remap to a letter that is in use, nothing happens and you are returned to the prompt. Locate the server's drive letters in Windows Explorer to verify that the drive letters are changed.

- Installation of the Web Interface on a server running Citrix Presentation Server may fail if you are upgrading a server with remapped drives. See article CTX240747 in the online Citrix Knowledge Center at http://support.citrix.com for more information.

- If you upgrade from MetaFrame 1.8 to Citrix Presentation Server on a server with changed server drive letters, the Windows Pass-Through Client is not updated. To avoid this issue, be sure the server is operating in install mode before running Setup.

Security Restrictions

Only Citrix administrators can execute this command.

Additional Information

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

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

Presentation Server also updates the pagefile entry and the following shortcut files:

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

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

DRIVEREMAP64

If you are using a 64-bit operating system, run the **driveremap64** command to change the server's drive letters. Citrix Presentation Server Setup installs this utility (DriveRemap64.exe) in the \Program Files (x86)\Citrix\System32 directory.

Important Considerations

- If you are using a 32-bit operating system and you want to change the server's drive letters, or if you want to update the 32-bit SQL Server 2005 Express Edition SP1 or SQL Server database locations, use the **driveremap** command.
- You must run this command from a network share or CD-ROM drive.
- Do not use the **driveremap64** utility on a server with .NET 2.0 installed. You can install .NET 2.0 after you remap server drives.
- If you are installing Citrix Presentation Server on a server that is not running a previous version of Presentation Server, run the **driveremap64** utility before you install Citrix Presentation Server. Citrix recommends that you do not change server drive letters after you install Citrix Presentation Server or applications you want to publish for users to access.

Syntax

driveremap64 /?

driveremap64 /dbscript:*filename*

driveremap64 /drive:M

driveremap64 /u

driveremap64 /noreboot

driveremap64 /IME

Options

The following parameters can be used with **driveremap64** at a command line.

/?

Displays the syntax for the utility and information about the utility's options.

/dbscript:*filename*

Sets the path to Fixsecuritydatabase.cmd to *filename*. For Windows Server 2003, the Fixsecuritydatabase utility is run to update drive information in the Windows security database after you remap the system drive.

If you run **driveremap64** from a location other than the Citrix Presentation Server CD, use the /**dbscript** switch to specify the path to Fixsecuritydatabase.cmd. If you copy Fixsecuritydatabase.cmd to a folder with the same relative location to Driveremap64.exe as on the Citrix Presentation Server CD (\Support\Install\Fixsecuritydatabase.cmd), you do not need to specify a new path with the /**dbscript** switch.

After remapping drives on Windows Server 2003, ensure that you restart the server and log on with an administrator account that has read access to the Fixsecuritydatabase.cmd file specified by /**dbscript**.

/drive:M
Specifies the drive letter to use for the first remapped drive.

/u
Permits unattended or silent installation where no dialog boxes appear and no user input is required. You must use this option in conjunction with the /**drive:** option.

/noreboot
Surpresses the Restart Computer message and does not restart the system. Citrix strongly recommends that you restart the system after running this utility.

/ime[*filename***]**
Changes the drive letter specified in Software\Microsoft\Windows\CurrentVersion\Ime\Japan\IMEJP \Dictionaries for all of the loaded hives under HKEY_USERS.

Remarks

The **driveemap64** utility allows you to select the drive letters you want to map. Before installation, you can run the Drive Remapping utility from the autorun screens of the Citrix Presentation Server CD. After installing Citrix Presentation Server, you can open the utility by running Driveremap64.exe with no parameters.

Caution Do not run **driveremap64** within an ICA or RDP session; for example, from a command prompt of a server desktop published as an application. Running **driveremap64** in an ICA or RDP session can cause the server to become unstable.

Examples

The following command remaps the server's drive letters. The first available drive is changed to M. The command uses the **noreboot** option, which suppresses the appearance of any dialog boxes.

driveremap64 /u /drive:M /noreboot

The following command returns the server's drive letters to the drive letters that start at C and then prompts you to restart the server.

driveremap64 /u /drive:M /drive:C

Known Issues

The following items are known issues you may encounter when running the **driveremap64** utility.

- When running **driveremap64** with no parameters, the drive letter choices in the drop-down list may be unavailable. This can occur if the server has non-contiguous drive letters; for example, C, D, X. The mapped drive letters are spread over the interval [a..z] and no reasonable interval shifting can be performed. Network drives are also taken into account.

  To work around this issue, change the drive letters to C, D, and E and then run the **driveremap64** utility.

- At a command prompt, if you remap to a letter that is in use, nothing happens and you are returned to the prompt. Locate the server's drive letters in Windows Explorer to verify that the drive letters are changed.

- Installation of the Web Interface on a server running Citrix Presentation Server may fail if you are upgrading a server with remapped drives. See article CTX240747 in the online Citrix Knowledge Center at http://support.citrix.com for more information.

- If you upgrade from MetaFrame 1.8 to Citrix Presentation Server on a server with changed server drive letters, the Windows Pass-Through Client is not updated. To avoid this issue, be sure the server is operating in install mode before running Setup.

Security Restrictions

Only Citrix administrators can execute this command.

Additional Information

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

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

Presentation Server also updates the pagefile entry and the following shortcut files:

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

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

DSCHECK

Use **dscheck** to validate the consistency of the database used to host the server farm's data store. You can then repair any inconsistencies found.

Syntax

dscheck [/clean] [/?]

Options

/clean

Attempts to fix any consistency error that is found.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

Dscheck performs a variety of tests to validate the integrity of a server farm's data store. When run without parameters, only these tests are run. Run **dscheck** on a server in the farm that has a direct connection to the data store.

When you run **dscheck** with the /**clean** option, the utility runs tests and removes inconsistent data (typically servers and applications) from the data store. Because removing this data can affect the farm's operation, be sure to back up the data store before using the /**clean** option. Contact Citrix Technical Support for assistance in restoring a backed up data store.

When you run the utility with the /**clean** option, you may need to run the **dsmaint** command with the **recreatelhc** parameter on each server in the farm to update the local host caches. Running this command sets the PSRequired registry value to one in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\Runtime.

Dscheck reports the results of the tests in several ways. First, it sends any errors found as well as a summary to the Event log and to the command window. You can also write the output produced by **dscheck** to a file.

Second, several performance monitor values are updated under the performance object for Citrix Presentation Server. These values include a count of server errors, a count of application errors, a count of group errors, and an overall flag indicating that errors were detected. The performance monitor values can be used with Resource Manager to detect when problems are present.

Third, **dscheck** returns an error code of zero for a successful scan (no errors are found) and an error code of one if any problems are encountered.

Dscheck looks primarily at three data store objects: servers, applications, and groups. For each of these object types, **dscheck** performs a series of tests on each object instance.

For example, for each server object in the data store, **dscheck** verifies that there is a corresponding common server object and then further verifies that both objects have matching host IDs and host names.

Examples

To run consistency checks only:

dscheck

To check consistency and fix errors:

dscheck /clean

Security Restrictions

To run this utility, you must have direct access to the data store.

DSMAINT

Use **dsmaint** to configure the IMA data store for a server farm.

When using this command, user names and passwords may be case-sensitive, depending on the database and the operating system you are using.

Syntax

dsmaint config [/**rade**] [/**user:***username*] [/**pwd:***password*] [/**dsn:***filename*]

dsmaint backup *destination_path*

dsmaint failover *direct_server*

dsmaint compactdb [/**ds**] [/**lhc**] [/**rade**]

dsmaint compare {/**srcdsn:***dsn1* /**srcuser:***user1* /**srcpwd:***pwd1* /**dstdsn:***dsn2* /**dstuser:***user2* /**dstpwd:***pwd2*}

dsmaint migrate [{/**srcdsn:***dsn1* /**srcuser:***user1* /**srcpwd:***pwd1*}] [{/**dstdsn:***dsn2* /**dstuser:***user2* /**dstpwd:***pwd2*}] [/**patchindex**:1 to enable][/**reccreteindex**] [/**debug**] [/**ignoreerrors**]

dsmaint publishsqlds {/**user:***username* /**pwd:***password*}[/**joblogin**:*joblogin*][/**jobpwd**:*jobpassword*]

dsmaint recover [*source_path\database_to_recover*]

dsmaint recreatelhc

dsmaint recreaterade

dsmaint verifylhc [/**autorepair**]

dsmaint /?

Parameters

destination_path
Path to the backup data store.

dsn1
The name of the source data store.

dsn2
The name of the destination data store

filename
The name of the data store.

direct_server
The name of the new direct server for IMA data store operations.

password
The password to connect to the data store.

pwd1
The source data store password.

pwd2
The destination data store password.

user1
The source data store user logon.

user2
The destination data store user logon.

username
The name of the user to use when connecting to the data store.

Options

config
Changes configuration parameters used to connect to the data store.

/rade
Compacts the offline data store.

/user:*username*
The user name to connect to a data store.

/pwd:*password*
The password to connect to a data store.

/dsn:*filename*
The filename of an IMA data store.

backup
Creates a backup copy of the Access database that is the farm's data store. Run this command on the server that hosts the data store. Requires a path or share point to which the database file will be copied. The backup command cannot be used to create backups for Oracle or SQL data stores.

failover
Switches the server to use a new direct server for IMA data store operations.

compactdb
Compacts the Access database file.

/ds
Specifies the database is to be compacted immediately. If the IMA Service is running, this can be executed from the direct server or an indirect server. If the IMA Service is not running, this can be executed only on the direct server.

/lhc
Specifies the local host cache is to be compacted immediately.

/rade
Compacts the offline data store.

migrate
Migrates data from one data store database to another. Use this command to move a data store to another server, rename a data store in the event of a server name change, or migrate the data store to an Oracle, SQL Server, or DB2 database.

/srcdsn:*dsn1*
The name of the data store from which to migrate data.

/srcuser:*user1*
The user name to use to connect to the data store from which the data is migrating.

/srcpwd:*pwd1*
The password to use to connect to the date store from which the data is migrating.

/dstdsn:*dsn2*
The name of the data store to which to migrate the data.

/dstuser:*user2*
The user name that allows you to connect to the data store to which you are migrating the source data store.

/dstpwd:*pwd2*
The password that allows you to connect to the data store to which you are migrating the source data store.

/patchindex:1 to enable
Use value 1 to enable this function.

/recreateindex
Recreates the index.

/debug
Debugs any errors.

/ignoreerrors
Ignores any errors.

publishsqlds
Publishes a data store to allow replication.

/user:*username*
The user name that allows you to publish a data store.

/pwd:*password*
The password that allows you to publish a data store.

/joblogin:*joblogin*

The job login that allows you access to the job.

/jobpwd:*jobpassword*
The password that allows you access to the job.

recover
Restores an Access data store to its last known good state. This must be executed on the direct server while the IMA Service is not running.

source_path
The source path to the database that will be recovered.

database_to_recover
The database that will be recovered.

recreatelhc
Recreates the local host cache database.

recreaterade
Recreates the offline license database.

verifylhc
Verifies the integrity of a Microsoft Access local host cache. If the local host cache is corrupt, you are prompted with the option to recreate it. With the **verifylhc** /**autorepair** option, the local host cache is automatically recreated if it is found to be corrupted.

/autorepair
Automatically creates the local host cache if it is found to be corrupted.

/?
Displays the syntax and options for the utility.

Remarks

compactdb
During database compaction, the database is temporarily unavailable for both reading and writing. The compacting time can vary from a few seconds to a few minutes, depending on the size of the database and the usage.

config
For Access databases, this command resets the password used to protect the database, setting the matched security context to allow IMA access to this database.

You must stop the IMA Service before using **config** with the **/pwd** option.

Caution You must specify a **/dsn** for **dsmaint config** or you will change the security context for access to the SQL or Oracle database.

---

migrate

Existing data store databases can be migrated to different database software. For example, you can create a farm with an Access database and later migrate the farm data store to a SQL Server database. For more information about migrating the data store to different database software and which migrations are supported, see "Planning the Data Store" on page 33.

Important By default, the Access database does not have a user name or password. When migrating a database from Access, leave the /**srcuser**: and /**srcpwd**: parameters blank.

The connection to a local Access database is based on the host server's name. If the name of the server changes, use **migrate** to change the name of the database.

publishsqlds

Execute **publishsqlds** only from the server that created the farm. The publication is named **MFXPDS**.

Security Restrictions

The **dsmaint config** and **dsmaint migrate** commands can be executed only by a user with the correct user name and password for the database.

ENABLELB

If one or more servers is removed from load balancing because they failed a Health Monitoring & Recovery test, use **enablelb** to restore them to the load balance tables.

Syntax

enablelb *servername* [*servername servername* …]

Parameters

servername

The name of a computer running Citrix Presentation Server.

Security Restrictions

To use this utility you must be a Citrix administrator with edit privileges for Other Farm Settings and Other Server Settings for the server you want to restore to load balancing.

ICAPORT

Use **icaport** to query or change the TCP/IP port number used by the ICA protocol on the server.

Syntax

icaport {**/query** | **/port**:*nnn* | **/reset**} [**/?**]

Options

/query

Queries the current setting.

/port:*nnn*

Changes the TCP/IP port number to *nnn*.

/reset

Resets the TCP/IP port number to 1494, which is the default.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

The default port number is 1494. The port number must be in the range of 0–65535 and must not conflict with other well-known port numbers.

If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every client that will connect to that server. For instructions for changing the port number on clients, see the administrator's guide for the clients that you plan to deploy.

Examples

To set the TCP/IP port number to 5000:

icaport /port:5000

To reset the port number to 1494:

icaport /reset

Security Restrictions

Only Citrix administrators can run **icaport**.

IMAPORT

Use **imaport** to query or change the IMA port.

Important When you run Citrix Presentation Server Setup, Setup references port 2513 for communication with the Presentation Server Console. If you change this port number on the first server in the farm on which you install Citrix Presentation Server, you cannot join additional servers to the server farm.

Syntax

imaport {/**query** | /**set** {**IMA**:*nnn* | **ds**:*nnn* | **cmc**:*nnn*}* | /**reset** {**IMA** | **DS** | **CMC** | **ALL**} } [/**?**]

Options

/query

Queries the current setting.

/set

Sets the designated TCP/IP port(s) to a specified port number.

ima:*nnn*

Sets the IMA communication port to a specified port number.

cmc:*nnn*

Sets the Presentation Server Console connection port to a specified port number.

ds:*nnn*

Sets the data store server port to a specified port number (indirect servers only).

/reset

Resets the specified TCP/IP port to the default.

ima

Resets the IMA communication port to 2512.

cmc

Resets the Presentation Server Console connection port to 2513.

ds

Resets the data store server port to 2512 (indirect servers only).

all

Resets all of the applicable ports to the defaults.

/?

Displays the syntax for the utility and information about the utility's options.

MIGRATETOSQLEXPRESS

Use **migratetosqlexpress** to migrate a server farm's data store from Microsoft Access to Microsoft SQL Server 2005 Express Edition SP1.

Migratetosqlexpress offers fail-safe operation and automatically rolls back any changes that it makes to the system in the event of any failures.

The utility is located on the Citrix Presentation Server CD in the Support\SqlExpress directory.

Syntax

migratetosqlexpress [**/instancename:***instancename* **| /dbname:***dbname* **| /accessuser:***user* **| /accesspwd:***pwd* **| /revert** | [**/?**]

Options

/instancename:*instancename*

Specify a named instance of SQL Server 2005 Express Edition SP1 other than the default value of CITRIX_METAFRAME.

/dbname:*dbname*

Specify a database other than the default value of MF20.

/accessuser:*user*

/accesspwd:*pwd*

Specify the user and pwd values for your Access database if you changed them using the **Dsmaint Config** utility.

/revert

Reverts to the Access database originally used as the server farm's data store. Running this command restores backups that were made when the migration was initially done. Any changes made to the farm since the migration from Access to SQL Server 2005 Express Edition SP1 are lost.

/?

Displays the syntax for the utility and information about the utility's options.

QUERY

Use **query** to display information about server farms, processes, servers, sessions, terminal servers, and users within the network.

Query Farm

Syntax

query farm [*server* [**/addr | /app | /app** *appname* **| /load | /ltload**]]

query farm [**/tcp**] [**/continue**]

query farm [**/app | /app** *appname* **| /disc** | **/load | /ltload | /lboff | /process**]

query farm [**/online | /online** *zonename*]

query farm [**/offline | /offline** *zonename*]

query farm [**/zone | /zone** *zonename*]

query farm [**/?**]

Parameters

appname
The name of a published application.

server
The name of a server within the farm.

zonename
The name of a zone within the farm.

Options

farm
Displays information about servers within an IMA-based server farm.You can use **qfarm** as a shortened form of **query farm**.

***server* /addr**
Displays address data for the specified server.

/app
Displays application names and server load information for all servers within the farm or for a specific server.

/app *appname*
Displays information for the specified application and server load information for all servers within the farm or for a specific server.

/continue
Do not pause after each page of output.

/disc
Displays disconnected session data for the farm.

/load
Displays server load information for all servers within the farm or for a specific server.

/ltload
Displays server load throttling information for all servers within the farm or for a specific server.

/lboff
Displays the names of the servers removed from load balancing by Health Monitoring & Recovery.

/process
Displays active processes for the farm.

/tcp
Displays TCP/IP data for the farm.

/online
Displays servers online within the farm and all zones. The data collectors are represented by the notation "D."

/online *zonename*
Displays servers online within a specified zone. The data collectors are represented by the notation "D."

/offline
Displays servers offline within the farm and all zones. The data collectors are represented by the notation "D."

/offline *zonename*
Displays servers offline within a specified zone. The data collectors are represented by the notation "D."

/zone
Displays all data collectors in all zones.

/zone *zonename*
Displays the data collector within a specified zone.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

- **Query farm** returns information for IMA-based servers within a server farm.
- You can use **qfarm** as a shortened form of the **query farm** command.

Security Restrictions

Only a Citrix administrator can run **query farm**.

Query Process

Syntax

query process [***** | *processid* | *username* | *sessionname* | **/id:***nn* | *programname*] [**/server:***servername*] [**/system**]

query process [**/?**]

Parameters

***

Displays all visible processes.

processid

The three- or four-digit ID number of a process running within the farm.

programname

The name of a program within a farm.

servername

The name of a server within the farm.

sessionname

The name of a session, such as **ica-tcp#7**.

username

The name of a user connected to the farm.

Options

process

Displays information about processes running on the current server.

process *

Displays all visible processes on the current server.

process *processid*

Displays processes for the specified *processid*.

process *username*

Displays processes belonging to the specified user.

process *sessionname*

Displays processes running under the specified session name.

process /id:*nn*

Displays information about processes running on the current server by the specified ID number.

process *programname*
Displays process information associated with the specified program name.

process /server:*servername*
Displays information about processes running on the specified server. If no server is specified, the information returned is for the current server.

process /system
Displays information about system processes running on the current server.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

You can use **qprocess** as a shortened form of the **query process** command.

Security Restrictions

None.

Query Server

Syntax

query server [*server* [**/ping** [**/count:***n*] [**/size:***n*] | **/stats** | **/reset** | **/load** | **/addr**]]

query server [**/tcp**] [**/tcpserver:***x*]

query server [**/license** | **/app** | **/gateway** | **/serial** | **/disc** | **/serverfarm** | **/video**]

query server [**/continue**] [**/ignore**] [**/?**]

Parameters

n
The number of times to ping a server (the default is five times) or the size of ping buffers (the default is 256 bytes).

server
The name of a server within the farm.

x
The default TCP server address.

Options

server *server*
Displays transport information for the specified server.

/addr
Displays address information for the specified server.

/app
Displays application names and server load for the specified server.

/continue
Do not pause after each page of output.

/count:*n*
Number of times to ping the specified server.

/disc
Displays disconnected session data on the current server.

/gateway
Displays configured gateway addresses for the current server.

/ignore
Ignore warning message about interoperability mode.

/license
Displays user licenses for the current server.

/load
Displays local data on the specified server.

/ping
Pings selected server. The default is five times.

/reset
Resets the browser statistics on the specified server.

/serial
Displays license serial numbers for the current server.

/serverfarm
Displays server farm names and server load.

/size:*n*
Size of ping buffers. The default is 256 bytes.

/stats
Displays the browser statistics on the specified server.

/tcp
Displays the TCP/IP data for the current server.

/tcpserver:*x*
Defines the TCP/IP default server address.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

- **Query server** displays data about only the servers present on a network within a server farm running in interoperability mode. It shows every server within the farm, even if the server is not currently connected to the farm. Query farm is the recommended command for displaying this information in a farm that is not running in interoperability mode.
- You can use **qserver** as a shortened form of the **query server** command.

Security Restrictions

None.

Query Session

Syntax

query session [*sessionname* | *username* | *sessionid*]

query session [**/server:***servername*] [**/mode**] [**/flow**] [**/connect**] [**/counter**]

query session [**/?**]

Parameters

servername
The name of a server within the farm.

sessionname
The name of a session, such as "**ica-tcp#7"**.

sessionid
The two-digit ID number of a session.

username
The name of a user connected to the farm.

Options

session *sessionname*
Identifies the specified session.

session *username*
Identifies the session associated with the user name.

session *sessionid*
Identifies the session associated with the session ID number.

session /server:*servername*
Identifies the sessions on the specified server.

session /mode
Displays the current line settings.

session /flow
Displays the current flow control settings.

session /connect
Displays the current connection settings.

session /counter
Displays the current Terminal Services counter information.

/?
Displays the syntax for the utility and information about the utility's options.

Security Restrictions

None.

Query Termserver

Syntax

query termserver [*servername*] [**/domain:***domain*] [**/address**] [**/continue**]

query termserver [**/?**]

Parameters

servername
The name of a server within the farm.

domain
The name of a domain to query.

Options

termserver *servername*
Identifies a Terminal Server.

/address
Displays network and node addresses.

/continue
Do not pause after each page of output.

/domain:*domain*
Displays information for the specified domain. Defaults to the current domain if no domain is specified.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

If no parameters are specified, **query termserver** lists all Terminal Servers within the current domain.

Security Restrictions

None.

Query User

Syntax

query user [*username* | *sessionname* | *sessionid*] [**/server:***servername*]

query user [**/?**]

Parameters

servername

The name of a server within the farm.

sessionname

The name of a session, such as "**ica-tcp#7"**.

sessionid

The ID number of a session.

username

The name of a user connected to the farm.

Options

user *username*

Displays connection information for the specified user name.

user *sessionname*

Displays connection information for the specified session name.

user *sessionid*

Displays connection information for the specified session ID.

user /server:*servername*

Defines the server to be queried. The current server is queried by default.

/?

Displays the syntax for the utility and information about the utility's options.

Remarks

If no parameters are specified, **query user** displays all user sessions on the current server. You can use **quser** as a shortened form of the **query user** command.

Security Restrictions

None.

RADEMAINT

Use **rademaint** to revoke offline access and return the license to the pool even if the offline license has not expired. Citrix recommends that you use this tool only to revoke a license quickly and put it back into the license pool.

To locate rademaint.exe, on the Server CD, expand **Support** > **debug**.

Syntax

rademaint OFFLINELICENSE [**/r:***username* | **/l:***username* (or ***)]

Parameters

username

The name of the user with an offline license.

Options

/r: *username*

Removes the offline license for the specified user.

/l: *username*

Lists the offline license for the specified user (or all if * is specified).

/?

Displays the syntax for the utility and information about the utility's options.

Security Restrictions

Only a Citrix administrator can run **rademaint**.

TWCONFIG

Use **twconfig** to configure ICA display settings that affect graphics performance for clients.

Syntax

twconfig [**/query | /q**]

twconfig [**/inherit:on | off**]

twconfig [**discard:on | off**]

twconfig [**/supercache:on | off**]

twconfig [**/maxmem:***nnn*]

twconfig [**/degrade:res | color**]

twconfig [**/notify:on | off**]

twconfig [**/?]**

Options

/query, /q
Query current settings.

/inherit:on | off
Set to **on** to use the ICA display properties defined for the farm. Set to **off** to use the settings specified for this server. By default, this is set to **on**.

/discard:on | off
Discard redundant graphics operations.

/supercache:on | off
Use alternate bitmap caching method.

/maxmem:*nnn*
Maximum memory (in kilobytes) to use for each session's graphics (150KB minimum, 8192KB maximum).

/degrade:res | **color**
When the **maxmem** limit is reached, degrade resolution first or degrade color depth first.

/notify:on | off
If **on**, users are alerted when **maxmem** limit is reached.

/?
Displays the syntax for the utility and information about the utility's options.

Remarks

A server can be set to inherit its ICA display settings from the server farm ICA display settings. Use /**query** to display the current inherit settings. If /**inherit** is on, the settings displayed with /query are the server farm settings. When /**inherit** is off, the settings shown are for the current server only.

Within the **maxmem** limit, various combinations of session size and color depth are available. The session size and color depth values are determined using the following formula: *height x width x depth* ≤ *maxmem*, where the *height* and *width* are measured in pixels and *depth* is the color depth in bytes according to the following table:

Color depth	Bytes
True Color (24-bit)	3
High Color (16-bit)	2
256 Colors (8-bit)	1
16 Colors (4-bit)	.5

The following is a list of the maximum session sizes with a 4:3 aspect ratio for each color depth at the default **maxmem** value (height by width by color depth):

- 1600 by 1200 by 24-bit color
- 1920 by 1440 by 16-bit color
- 2752 by 2064 by 256 colors
- 3904 by 2928 by 16 colors

Security Restrictions

None.

Delegated Administration Tasks

You can delegate specified tasks to custom administrators through the Access Management Console.

Note For information about creating custom administrators, see "Step 5: Assigning Farm Administrator Credentials" on page 64.

To delegate tasks to existing custom administrators

1. Expand the Administrators node and select an administrator.
2. Under Tasks in the lower right portion of the Administrator page, click **Modify Administrator Properties**. The Citrix Administrator Properties page appears.
3. Click **Permissions** to view the task permissions assigned to the administrator.
4. Click on a folder in the Folders list to view additional tasks.
5. To select the tasks to which the administrator has access, select or clear the task check boxes, as appropriate.

The following tables list the delegated administration tasks that you can assign to custom administrators.

Note If you change an administrator's ODBA permissions, he or she will need to manually rerun discovery.

Farm Folder Tasks

The following table lists the tasks that appear when the Farm folder is selected.

Task	Description
Farm Management	Toggles on/off all subtasks. Allows full access to view and modify all areas of farm management. To disable subtasks, clear the check boxes.
Edit All Other Farm Settings	Allows administrators to edit all farm properties, with the exception of zones.
Edit Configuration Logging Settings	Allows administrators to edit Configuration Logging settings and clear the log.
Edit Zone Settings	Allows administrators to configure zones, move servers to zones, and set election preferences.
View Farm Management	Allows view-only access to the farm properties.

Administrators Folder Tasks

The following table lists the tasks that appear when the Administrators folder is selected

Task	Description
Administrators	Toggles on/off all subtasks. Allows administrators to open the Presentation Server Console and Web Interface Console and to view the properties of other administrators. To disable subtasks, clear the check boxes.
Edit centrally configured Web Interface sites	Allows administrators to configure Web Interface Web sites.
Log on to Management Console	Allows administrators to open the Access Management Console.
View Administrators	Allows administrators to view the properties of other administrators.

Applications Folder Tasks

The following table lists the tasks that appear when the Applications folder is selected.

Task	Description
Published Applications	Toggles on/off all subtasks. Allows full access to view and edit properties for published applications in the specified folder. To disable subtasks, clear the check boxes.
Publish Applications and Edit Properties	Allows administrators to publish applications and edit their properties. This permission is also required when adding Resource Manager metrics to published applications.
View Published Applications and Content	Allows administrators to view published applications and content.
Resource Manager	Toggles on/off all subtasks. Allows full access to view and modify all areas of resource management in the specified folder. To disable subtasks, clear the check boxes.
Create RM Applications and Edit Properties	Allows Administrators to create, edit, rename, or delete Resource Manager applications. This permission also allows administrators to add, remove, snooze, sleep, awaken, and edit the properties of metrics associated with Resource Manager applications and published applications. When creating or editing Resource Manager applications, the servers to which the administrator can assign the application are controlled by the "Assign RM Applications to Servers" permission for the server folder. Automatically selects and requires the View permission.
Receive SMS and Email Notifications	If an application metric is configured to send out SMS or email notifications, this permission allows administrators to receive SMS or email notifications related to applications, using the contact information specified in the "Alert Contact Details" section of their profile. Automatically selects and requires the View permission. Note: Administrators can be given permission to receive other types of SMS and email notifications in the resource-related tasks or server-based tasks.
View RM Applications and Content	Allows administrators to view any Resource Manager applications, as well as any metrics associated with the application. Administrators can also select the metric and generate a real-time graph that displays the current metric count and the metric error and warning thresholds. If administrators also have the "View Published Applications and Content" or "View Session Management" permissions for the same folder, they can view metrics associated with published applications in the specified folder and generate real-time graphs for these metrics. The RM watcher is available to display application-related Resource Manager alerts. Note: Administrators can be given permission to view resource-related Resource Manager alerts using "View Resource Management Configuration and Alerts" and server-related Resource Manager alerts using "View RM Information and Alerts."

Servers	Toggles on/off the Terminate Processes subtask. Allows full access to terminate processes on accessible servers. To disable subtask, clear the check boxes.
Terminate Processes	Allows administrators to terminate processes on accessible servers.
Sessions	Toggles on/off all subtasks. Allows full access to view and modify all areas of session management for the specified folder. To disable subtasks, clear the check boxes.
Connect Sessions	Allows administrators to connect to a session. Automatically selects and requires the View permission.
Disconnect Users	Allows administrators to disconnect one or more sessions. Automatically selects and requires the View permission.
Log Off Users	Allows administrators to log off one or more sessions. Automatically selects and requires the View permission.
Reset Sessions	Allows administrators to reset client and disconnected sessions. Automatically selects and requires the View permission.
Send Messages	Allows administrators to send desktop messages to one or more sessions. Automatically selects and requires the View permission.
View Session Management	Allows view-only access to session management.

Installation Manager Folder Tasks

The following table lists the tasks that appear when the Installation Manager folder is selected.

Task	Description
Installation Manager	Toggles on/off all subtasks. Allows full access to view and modify all areas of installation management. To disable subtasks, clear the check boxes.
Edit Configurations	Allows administrators to edit and/or install/uninstall packages, package groups, server groups, and Installation Manager properties. Automatically selects and requires the View permission.
View Installation Manager	Allows view-only access to the Installation Manager node in the Presentation Server Console, the Installation Manager properties, all of the available packages and package groups, package and package group properties, and installation information. Administrators can view a server group only if they have the "Install and Uninstall Packages" server folder permission for at least one server in the group, and they can view only the individual servers in the group for which they have this permission.

Isolation Environment Folder Tasks

The following table lists the tasks that appear when the Isolation Environment folder is selected.

Task	Description
Isolation Environments	Toggles on/off all subtasks. Allows full access to view and modify all areas of isolation environments. To disable subtasks, clear the check boxes.
Manage Isolation Environments	Allows administrators to create and modify isolation environments, as well as publish applications in an isolation environment. To publish applications in an isolation environment, administrators also need the "Publish Applications and Edit Properties" permission. Automatically selects and requires the View permission.
View Isolation Environments	Allows view-only access to isolation environments and the applications published in them.

Load Evaluator Folder Tasks

The following table lists the tasks that appear when the Load Evaluator folder is selected.

Task	Description
Load Manager	Toggles on/off all subtasks. Allows full access to view and modify all areas of load management. To disable subtasks, clear the check boxes.
Assign Load Evaluators	Allows administrators to assign load evaluators to servers and published applications.
Edit Load Evaluators	Allows administrators to edit load evaluation settings. Automatically selects and requires the View permission.
View Load Evaluators	Allows view-only access to load evaluator settings.

Monitoring Configuration Folder Tasks

The following table lists the tasks that appear when the Monitoring Configuration folder is selected.

Task	Description
Monitoring and Alerting	Toggles on/off all subtasks. Allows full access to view and modify all areas of monitoring and alerting. To disable subtasks, clear the check boxes. These tasks are related to the My Knowledge extension - Configuration and Alerts**.**
Edit Farm Monitoring and Server Default Monitoring Information	Allows administrators to change the server default configuration and to modify the current configuration of alerts generated by the My Knowledge extension (SMA alerts). This information includes thresholds, polling intervals, and whether the alert is enabled or disabled. Automatically selects and requires the "View Farm Monitoring and Server Default Monitoring Information" permission. To apply the configuration of all the My Knowledge extension alerts of the currently selected farm (the source farm) to other discovered farms that have SMA enabled (the target farms), administrators must have the "View Farm Monitoring and Server Default Monitoring Information" permission for the source farm and "Edit Farm Monitoring and Server Default Monitoring Information" permission for the target farms.
Edit My Knowledge Configuration	Allows administrators to create a new configuration and edit or delete the current company knowledge configuration for the farm. Automatically selects and requires the "View My Knowledge Configuration" permission. To copy the company knowledge database configuration from another discovered farm that has its company knowledge database configured (the source farm) to the currently selected farm, the administrator must also have the "View My Knowledge Configuration" permission in the source farm.
View Farm Monitoring and Server Default Monitoring Information	Allows view-only access to the server default configuration and to the current configuration of alerts generated by the My Knowledge extension. This information includes thresholds, polling intervals, and whether the alert is enabled or disabled.
View My Knowledge Configuration	Allows view-only access to the current company knowledge configuration of alerts generated by the My Knowledge extension.

Policies Folder Tasks

The following table lists the tasks that appear when the Policies folder is selected.

Task	Description
User Policies	Toggles on/off all subtasks. Allows full access to view and modify all areas of user policies. To disable subtasks, clear the check boxes.
Edit User Policies	Allows administrators to create and modify policies. Automatically selects and requires the View permission.
View User Policies	Allows view-only access to policies.

Printer Management Folder Tasks

The following table lists the tasks that appear when the Printer Management folder is selected.

Task	Description
Printers	Toggles on/off all subtasks. Allows full access to view and modify all areas of printer management. To disable subtasks, clear the check boxes.
Edit All Other Printer Settings	Allows administrators to import network print servers, map drivers, and edit all other printer settings, with the exception of editing printer drivers, editing printers, and replicating printer drivers. Automatically selects and requires the View permission.
Edit Printer Drivers	Allows administrators to edit driver-related features. Automatically selects and requires the View permission.
Edit Printers	Allows administrators to add, edit, delete, or reset client printers. Automatically selects and requires the View permission.
Replicate Printer Drivers	Allows administrators to replicate printer drivers from one server to another and to manage the auto-replication list. Automatically selects and requires the View permission.
View Printers and Printer Drivers	Allows view-only access to printers and printer drivers.

Resource Manager Folder Tasks

The following table lists the tasks that appear when the Resource Manager folder is selected.

Task	Description
Resource Management	Toggles on/off all subtasks. Allows full access to view and modify all areas of managing resources for the farm. To disable subtasks, clear the check boxes.
Configure Resource Management	Allows administrators to edit the configuration of all the areas described in the "View Resource Management Configuration" permission. Automatically selects and requires the View permission.
Generate Billing Reports	Allows administrators to generate billing reports, manage cost centers, manage fee profiles, and view saved reports. Saved reports can also be viewed using any Web browser. Automatically selects and requires the View permission.
Generate Current and Summary Reports	Allows administrators to generate current and summary reports and view any saved reports. Saved reports can also be viewed using any Web browser. Automatically selects and requires the View permission.
Receive SMS and Email Notifications	If the summary database is configured to send out SMS or email notifications, this permission allows administrators to receive the SMS or email notification related to resource management tasks (those not related to applications or servers), using the contact information specified in the "Alert Contact Details" section of their profile. Automatically selects and requires the View permission. Note: Administrators can be given permission to receive other types of SMS and email notifications in the application-related tasks or server-based tasks.
View Resource Management Configuration and Alerts	Allows administrators to view the **Resource Manager** node in the Presentation Server Console, including the current configuration of the following areas of Resource Manager: - Summary database configuration - SMS servers, gateways, and the receivers of SMS alerts - Community string used for sending SNMP alerts - Configuration of the currently selected method for sending email alerts (SMTP or MAPI), and the receivers of email alerts - Primary and backup farm metric servers The RM watcher lets you display any current Resource Manager alerts, other than alerts related to applications or servers. Note: Administrators can be given permission to view application-related Resource Manager alerts using "View RM Applications and Content" and server-related Resource Manager alerts using "View RM Information and Alerts."

Servers Folder Tasks

The following table lists the tasks that appear when the Servers folder is selected.

Task	Description
Installation Manager	Toggles on/off all subtasks. Allows full access to install and uninstall packages on servers in the specified folder. To disable subtasks, clear the check boxes.
Install and Uninstall Packages	Allows administrators to install and uninstall packages on all the servers in the specified folder. This permission also controls which servers and server groups administrators can view in the "Server Groups" section of the Installation Manager node for the farm. Administrators can view a server group only if they have the "Install and Uninstall Packages" server folder permission for at least one server in the group, and they can view only the individual servers for which they have this permission.
Monitoring and Alerting	Toggles on/off the Assign Monitoring Profiles to Servers subtask. Allows full access to assign monitoring profiles to servers. To disable this subtask, clear the check boxes.
Assign Monitoring Profiles to Servers	Allows administrators to assign monitoring profiles to servers. For additional information about monitoring and alerting, see the *Monitoring Server Performance Guide*.
Published Applications	Allows full permissions for administering published applications on servers in the specified folder. To disable this subtask, clear the check boxes.
Assign Applications to Servers	Allows administrators to publish applications from servers. To publish applications from a server, administrators must also have the "Publish Applications and Edit Properties" permission.
Resource Manager	Toggles on/off all subtasks. Allows full access to Resource Manager for servers in the specified folder. To disable subtasks, clear the check boxes.
Assign RM Applications to Servers	Allows administrators to assign the servers on which a Resource Manager application can be monitored. Servers for which administrators do not have this permission are not visible when the administrators assign servers to a Resource Manager application. Note: This permission does not have any effect on the servers that can be assigned to published applications.
Edit RM Information	Allows administrators to add, remove, snooze, sleep, awaken, and edit the properties of metrics associated with servers. Administrators can also modify the configuration of the following sections in the server properties: - Ignored processes - Metric summary schedule - Reboot schedule - Resource Manager alert recipients Automatically selects and requires the View permission. Note: The ignored processes and metric summary schedule properties are configured from a monitoring profile in the Access Management Console.

Receive SMS and Email Notifications	If a server metric is configured to send out SMS or email notifications, this permission allows administrators to receive SMS or email notifications related to servers, using the contact information specified in the "Alert Contact Details" section of their profile. Automatically selects and requires the View permission. Note: Administrators can be given permission to receive other types of SMS and email notifications in the resource-related tasks or application-related tasks.
View RM Information and Alerts	Allows the administrators to view any metrics that were added to the servers in the specified folder. Administrators can also select a metric and generate a real-time graph that displays the current metric count and the metric error and warning thresholds. If administrators also have the "Generate Current and Summary Reports" permission, they can generate reports directly from the graph. Administrators can view the Resource Manager server log and view the current configuration of the following sections in the server properties dialog: - Ignored processes - Metric summary schedule - Reboot schedule - Resource Manager alert recipients The RM watcher is available to display server-related Resource Manager alerts. Note: The ignored processes and metric summary schedule properties are configured from a monitoring profile in the Access Management Console. Note: Administrators can be given permission to view application-related Resource Manager alerts using "View RM Applications and Content" and resource-related Resource Manager alerts using "View Resource Management Configuration and Alerts."
Servers	Toggles on/off all subtasks. Allows full access to view and modify all areas of server administration in the specified folder. To disable subtasks, clear the check boxes.
Edit License Server Settings	Allows administrators to edit settings for the Citrix License Server.
Edit Other Server Settings	Allows administrators to edit all server settings, with the exception of SNMP settings, moving and removing servers, terminating processes, and Citrix License Server settings.
Edit SNMP Settings	Allows administrators to set up notifications of events by the SNMP agent.
Move and Remove Servers	Allows administrators to move servers between server folders and remove servers from the farm.
Terminate Processes	Allows administrators to terminate processes on accessible servers.
View Server Information	Allows view-only access to server information.
Sessions	Toggles on/off all subtasks. Allows full access to view and modify all areas of session administration. To disable subtasks, clear the check boxes.
Connect Sessions	Allows administrators to connect to user sessions. Automatically selects and requires the View permission.

Disconnect Users	Allows administrators to disconnect user sessions. Automatically selects and requires the View permission.
Log Off Users	Allows administrators to log off users. Automatically selects and requires the View permission.
Reset Sessions	Allows administrators to reset user sessions. Automatically selects and requires the View permission.
Send Messages	Allows administrators to send messages to users, such as broadcasting information about an upgrade or a warning about a system shutdown. Automatically selects and requires the View permission.
View Session Management	Allows view-only access to session management.

Performance Counters

Performance monitoring counters that directly relate to the performance of ICA sessions, networking, and security are installed with Citrix Presentation Server. You can access these counters from the Performance Monitor, which is part of Windows operating systems. Citrix recommends that you use performance monitoring to get accurate accounts of system performance and the effects of configuration changes on system throughput.

You can add and then view the following categories of Citrix Presentation Server-related counters, called *performance objects* in Performance Monitor:

- Citrix CPU Utilization Mgmt User
- Citrix IMA Networking
- Citrix Licensing
- Citrix MetaFrame Presentation Server
- ICA Session
- Secure Ticket Authority

You must choose one of the above performance objects in the **Add Counters** dialog box of Performance Monitor to select individual counters for monitoring. For more information about adding counters to Performance Monitor, see “Monitoring Performance of Sessions and Servers” on page 243.

Caution If you are using a 64-bit version of Windows Server 2003, you must use the 32-bit version of Performance Monitor to track performance metrics related to Citrix Presentation Server. This version of the tool is located in the windows\syswow64 directory.

Citrix CPU Utilization Mgmt User Counters

The following counters are available through the Citrix CPU Utilization Mgmt User performance object in Performance Monitor.

Counter	Description
CPU Entitlement	The percentage of CPU resource that Citrix CPU Utilization Management makes available to a user at a given time.
CPU Reservation	The percentage of the total machine CPU resource reserved for a user, should that user require it.
CPU Shares	The proportion of CPU resource assigned to a user. The value is an integer in the range 1-64.
CPU Usage	The percentage of CPU resource consumed by a user at a given time, averaged over a few seconds.
Long-term CPU Usage	The percentage of CPU resource consumed by a user, averaged over a longer period than the CPU Usage counter.

Citrix IMA Networking Counters

The following counters are available through the Citrix IMA Networking performance object in Performance Monitor.

Counter	Description
Bytes Received/sec	This counter is for inbound bytes per second.
Bytes Sent/sec	This counter is for outbound bytes per second.
Network Connections	Number of active IMA network connections to other IMA servers.

Citrix Licensing

The following counters are available through the Citrix Licensing performance object in Performance Monitor.

Counter	Description
Average License Check-In Response Time (ms)	The average license check-in response time in milliseconds.
Average License Check-Out Response Time (ms)	The average license check-out response time in milliseconds.
Last Recorded License Check-In Response Time (ms)	The last recorded license check-in response time in milliseconds.
Last Recorded License Check-Out Response Time (ms)	The last recorded license check-out response time in milliseconds.
License Server Connection Failure	The number of minutes that Presentation Server has been disconnected from the License server.
Maximum License Check-In Response Time	The maximum license check-in response time in milliseconds
Maximum License Check-Out Response Time	The maximum license check-out response time in milliseconds.

Citrix MetaFrame Presentation Server Counters

The following counters are available through the Citrix MetaFrame Presentation Server performance object in Performance Monitor.

Counter	Description
Application Enumerations/sec	The number of application enumerations per second.
Application Resolution Time (ms)	The time in milliseconds that a resolution took to complete.
Application Resolutions Failed/sec	The number of application resolutions failed per second.
DataStore Connection Failure	The number of minutes that the server running Presentation Server has been disconnected from the data store.
DataStore bytes read	The number of bytes read from the data store.
DataStore bytes read/sec	The number of bytes of data store data read per second.
DataStore bytes written/sec	The number of bytes of data store data written per second.
DataStore reads	The number of times data was read from the data store.

Counter	Description
DataStore reads/sec	The number of times data was read from the data store per second.
DataStore writes/sec	The number of times data was written to the data store per second.
DynamicStore bytes read/sec	The number of bytes of dynamic store data read per second.
DynamicStore bytes written/sec	The number of bytes of dynamic store data written per second.
DynamicStore Gateway Update Count	The number of dynamic store update packets sent to remote data collectors.
DynamicStore Gateway Update, Bytes Sent	The number of bytes of data sent across gateways to remote data collectors.
DynamicStore Query Count	The number of dynamic store queries that were performed.
DynamicStore Query Request, Bytes Received	The number of bytes of data received in dynamic store query request packets.
DynamicStore Query Response, Bytes Sent	The number of bytes of data sent in response to dynamic store queries.
DynamicStore reads/sec	The number of times data was read from the dynamic store per second.
DynamicStore Update Bytes Received	The number of bytes of data received in dynamic store update packets.
DynamicStore Update Packets Received	The number of update packets received by the dynamic store.
DynamicStore Update Response Bytes Sent	The number of bytes of data sent in response to dynamic store update packets.
DynamicStore writes/sec	The number of times data was written to the dynamic store per second.
Filtered Application Enumerations/sec	The number of filtered application enumerations per second.
LocalHostCache bytes read/sec	The number of bytes of IMA local host cache data read per second.
LocalHostCache bytes written/sec	The number of bytes of IMA local host cache data written per second.
LocalHostCache reads/sec	The number of times data was read from the IMA local host cache per second.
LocalHostCache writes/sec	The number of times data was written to the IMA local host cache per second.
Maximum Number of XML Threads	The maximum number of threads allocated to service Web-based sessions since the server rebooted.

Counter	Description
Number of XML Threads	The number of threads allocated to service Web-based sessions.
Resolution WorkItem Queue Executing Count	The number of resolution work items that are currently being executed.
Resolution WorkItem Queue Ready Count	The number of resolution work items that are ready to be executed.
WorkItem Queue Executing Count	The number of work items that are currently being executed.
WorkItem Queue Pending Count	The number of work items that are not yet ready to be executed.
WorkItem Queue Ready Count	The number of work items that are ready to be executed.
Zone Elections	The number of zone elections that occurred. This value starts at zero each time the IMA Service starts and is incremented each time a zone election takes place.
Zone Elections Won	The number of times the server won a zone election.

ICA Session Counters

The following counters are available through the ICA Session performance object in Performance Monitor.

Note For Citrix Presentation Server, Advanced and Enterprise Editions, only the counters marked with an asterisk (*) are installed.

Counter	Description
Input Audio Bandwidth	The bandwidth, measured in bps, used when playing sound in an ICA session.
Input Clipboard Bandwidth	The bandwidth, measured in bps, used when performing clipboard operations such as cut-and-paste between the ICA session and the local window.
Input COM 1 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client COM 1 port.
Input COM 2 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client COM 2 port.
Input COM Bandwidth	The bandwidth, measured in bps, used when sending data to the client COM port.

Counter	Description
Input Control Channel Bandwidth	The bandwidth, measured in bps, used when executing LongCommandLine parameters of a published application.
Input Drive Bandwidth	The bandwidth, measured in bps, used when performing file operations between the client and server drives during an ICA session.
Input Font Data Bandwidth	The bandwidth, measured in bps, used when initiating font changes within a SpeedScreen-enabled ICA session.
Input Licensing Bandwidth	The bandwidth, measured in bps, used to negotiate licensing during the session establishment phase. There is normally no data for this counter because this negotiation takes place before logon.
Input LPT 1 Bandwidth	The bandwidth on the virtual channel that prints to a client printer attached to the client LPT 1 port through an ICA session that does not support a spooler. This is measured in bps.
Input LPT 2 Bandwidth	The bandwidth on the virtual channel that prints to a client printer attached to the client LPT 2 port through an ICA session that does not support a spooler. This is measured in bps.
Input Management Bandwidth	The bandwidth, measured in bps, used when performing management functions.
Input PN Bandwidth	The bandwidth, measured in bps, used by Program Neighborhood to obtain application set details.
Input Printer Bandwidth	The bandwidth, measured in bps, used when printing to a client printer through a client that has print spooler support enabled.
Input Seamless Bandwidth	The bandwidth, measured in bps, used for published applications that are not embedded in a session window.
Input Session Bandwidth	The bandwidth, measured in bps, used from client to server for a session.
Input Session Compression	The compression ratio used from client to server for a session.
Input Session Line Speed	The line speed, measured in bps, used from client to server for a session.
Input SpeedScreen Data Channel Bandwidth	The bandwidth, measured in bps, used from client to server for data channel traffic.
Input Text Echo Bandwidth	The bandwidth, measured in bps, used for text echoing.
Input ThinWire Bandwidth	The bandwidth, measured in bps, used from client to server for ThinWire traffic.
Input VideoFrame Bandwidth	The bandwidth from client to server traffic on a virtual channel. Measured in bps.
Latency - Last Recorded*	The last recorded latency measurement for the session.

Counter	Description
Latency - Session Average*	The average client latency over the lifetime of a session.
Latency - Session Deviation*	The difference between the minimum and maximum measured latency values for a session.
Output Audio Bandwidth	The bandwidth, measured in bps, used for playing sound in an ICA session.
Output Clipboard Bandwidth	The bandwidth, measured in bps, used for clipboard operations such as cut-and-paste between the ICA session and the local window.
Output COM 1 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client COM 1 port.
Output COM 2 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client COM 2 port.
Output COM Bandwidth	The bandwidth, measured in bps, used when receiving data from the client COM port.
Output Control Channel Bandwidth	The bandwidth, measured in bps, used when executing LongCommandLine parameters of a published application.
Output Drive Bandwidth	The bandwidth, measured in bps, used when performing file operations between the client and server drives during an ICA session.
Output Font Data Bandwidth	The bandwidth, measured in bps, used when initiating font changes within a SpeedScreen-enabled ICA session.
Output Licensing Bandwidth	The bandwidth, measured in bps, used to negotiate licensing during the session establishment phase. There is normally no data for this counter because this negotiation takes place before logon.
Output LPT 1 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client LPT 1 port.
Output LPT 2 Bandwidth	The bandwidth, measured in bps, used when routing a print job through an ICA session that does not support a spooler to a client printer attached to the client LPT 2 port.
Output Management Bandwidth	The bandwidth, measured in bps, used when performing management functions.
Output PN Bandwidth	The bandwidth, measured in bps, used by Program Neighborhood to obtain application set details.
Output Printer Bandwidth	The bandwidth, measured in bps, used when printing to a client printer through a client that has print spooler support enabled.
Output Seamless Bandwidth	The bandwidth, measured in bps, used for published applications that are not embedded in a session window.

Counter	Description
Output Session Bandwidth	The bandwidth, measured in bps, used from server to client for a session.
Output Session Compression	The compression ratio used from server to client for a session.
Output Session Line Speed	The line speed, measured in bps, used from server to client for a session.
Output SpeedScreen Data Channel Bandwidth	The bandwidth, measured in bps, used from server to client for data channel traffic.
Output Text Echo Bandwidth	The bandwidth, measured in bps, used for text echoing.
Output ThinWire Bandwidth	The bandwidth, measured in bps, used from server to client for ThinWire traffic.
Output VideoFrame Bandwidth	The bandwidth from server to client traffic on a virtual channel. Measured in bps.

Secure Ticket Authority Counters

The following performance counters are available for the Secure Ticket Authority.

Performance Counter	Description
STA Bad Data Request Count	The total number of unsuccessful ticket validation and data retrieval requests during the lifetime of the STA.
STA Bad Refresh Request Count	The total number of unsuccessful ticket refresh requests received during the lifetime of the STA.
STA Bad Ticket Request Count	The total number of unsuccessful ticket generation requests received during the lifetime of the STA.
STA Count of Active Tickets	Total count of active tickets currently held in the STA.
STA Good Data Request Count	The total number of successful ticket validation and data retrieval requests received during the lifetime of the STA.
STA Good Refresh Request Count	The total number of successful ticket refresh requests received during the lifetime of the STA.
STA Good Ticket Request Count	The total number of successful ticket generation requests received during the lifetime of the STA.
STA Peak All Request Rate	The maximum rate of all monitored activities per second.
STA Peak Data Request Rate	The maximum rate of data requests per second during the lifetime of the STA.

Performance Counter	Description
STA Peak Ticket Refresh Rate	The maximum rate of refresh requests per second during the lifetime of the STA.
STA Peak Ticket Request Rate	The maximum rate of ticket generation requests per second during the lifetime of the STA.
STA Ticket Timeout Count	The total number of ticket time-outs that occur during the lifetime of the STA.

Advanced Installation Methods

The appendix provides information about the different methods you can use to install Presentation Server. These include the following:

- Unattended Installations
- Windows Installer Packages
- Transforms
- Answer Files
- Windows Installer Commands

Unattended Installations

An alternative to autorun installations is the installation of Citrix Presentation Server and its components through the deployment of the Windows installer package (.msi file) that contains them. Such *unattended* installations, are often performed with Windows Installer *transforms* (files with the .mst extension) that manipulate the installation database contained in the Windows Installer package. A transform makes changes to elements of the database and modifies the installation package when it is being installed and dynamically affects the installation behavior.

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

You can configure Citrix Presentation Server Setup to run without assistance with the following methods:

- Applying transforms to the installation database. A transform modifies the Windows Installer package (.msi file) at installation time and applies the values you set. Sample transform files are located on the Citrix Presentation Server CD in Support\Install.
- Creating an answer file to provide answers to the questions asked during Setup. A sample answer file is located on the Citrix Presentation Server CD in Support\Install.

The following sections describe installation packages, creating and applying transforms, creating answer files, using Windows Installer commands, and creating installation log files.

Deploying Windows Installer Packages

Citrix Presentation Server and its components are compiled into a Windows Installer package (.msi) file. Windows Installer is a component of the Windows operating system that manages the installation and removal of applications. Windows Installer applies a set of centrally defined setup rules during the installation process that define the configuration of the application.

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

You can deploy Windows Installer packages using Installation Manager, Microsoft Active Directory Services, Systems Management Server, or other third-party products. For more information about Windows Installer technology and the Windows Installer Service, see the Windows online Help or the Microsoft Web site at http://www.microsoft.com.

If you encounter problems when running a Windows Installer package, you can check the Windows Event Viewer for a list of the problems. Check the Application Log for any entries in the Source column of the type "MSIInstaller."

Creating Transforms

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

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

When you create a transform to apply to the Citrix Presentation Server Windows Installer package, you set your desired values for properties in the package. When you then apply the transform to the installation package, the "questions" you would be asked during Setup are answered. Creating a transform allows you to install Citrix Presentation Server in unattended mode. There are several third-party tools you can use to create or edit transforms.

Citrix provides four sample transforms on the Citrix Presentation Server CD, located in the Support\Install directory. The transforms include sample values for select properties, allowing you to determine which properties you can edit to achieve a certain configuration.

For definitions and possible values of the properties in the sample transforms, see "Advanced Installation Methods" on page 365.

Important Do not apply the sample transforms to Citrix Presentation Server Setup without editing them to include your required values. Some of the third-party Windows Installer packaging tools allow you to edit existing transforms. Use the sample transforms as a guideline to achieve the desired configuration.

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

1. Using your preferred tool for editing Windows Installer packages, open the Citrix Presentation Server Setup Windows Installer installation package, MPS.msi, located on the Citrix Presentation Server CD in the \Citrix Presentation Server directory.
2. Apply the transform that includes the properties and values you want to modify.
3. Enter new values for the properties you want to change.
4. Generate the transform file and save it with a new name.

Applying Transforms

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

To apply a transform

Type the following at a command prompt, where *package* is the name of the Windows Installer installation package and *TransformList* is the list of the transforms that you want to apply:

msiexec /i *package* TRANSFORMS=*TransformList*

If you are applying multiple transforms, separate each transform with a semicolon. For further information about the parameters and switches you can use with these options, go to the Microsoft Web site at http://www.microsoft.com and search on "msiexec."

Creating and Using an Answer File

Alternatively, you can create an *answer file* to provide answers to the questions asked when you run Setup. A sample answer file is located on the Citrix Presentation Server CD in Support\Install. Instructions are provided in the file for setup options. Copy the sample answer file to another location and modify it for your needs.

To perform an unattended installation with an answer file

1. On the Citrix Presentation Server CD, navigate to and open the sample answer file UnattendedTemplate.txt, located in the directory Support\Install, in any text editor. Save the file with another name.
2. Enter the values for the entries you want to set. The file includes definitions and possible values for each entry.

3. Type the following at a command prompt where *path-to-mps.msi* is the full path to your Presentation Server installation, and *answer_file.txt* is the name of the text file you created in Step 2:

```
UnattendedInstall.exe <path-to-mps.msi>
<answer_file.txt> [MSIPROPERTY1="VALUE1"] ...
[MSIPROPERTYN="VALUEN"]
```

Note Passwords are no longer stored in the answer file. Passwords must be provided on the command-line when invoking UnattendedInstall.exe. See the unattended template file for the specific password command-line options required for the scenario you use.

Using Windows Installer Commands

You can also use the Msiexec command to install Citrix Presentation Server. Set properties by adding *Property="value"* on the command line after other switches and parameters. For definitions of the properties in the Citrix Presentation Server Windows Installer package, see "Advanced Installation Methods" on page 365.

You can use the Msiexec command to install, modify, and perform operations on Windows Installer packages from the command line. The Citrix Presentation Server Windows Installer package, Mps.msi, is located in the Citrix Presentation Server folder of the Citrix Presentation Server CD-ROM.

You also use the Msiexec command to run administrative installations. Administrative installations allow you to store preconfigured, customized images of Citrix Presentation Server Setup on network share points. You can then access the Citrix Presentation Server Windows Installer package and install Citrix Presentation Server from anywhere on your network. For more information about creating customized administrative installation share points, see "Unattended Installations" on page 365.

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

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

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

```
msiexec /i mps.msi /L*v c:\output.log
```

Access Management Console Installations. To perform silent or unattended installations of the Access Management Console, use the individual MSI files located in the \Administration\Access Management Console\Setup folder on the Server CD for Citrix Presentation Server. The installer that you start from the autorun screen cannot be used for these purposes.

Enabling Administrative Installations

In addition to performing unattended installations, you can use Windows Installer to perform an *administrative* installation of Citrix Presentation Server. An administrative installation is a type of unattended installation that decompresses the installation files and copies them to a network share point. You can create customized images of Citrix Presentation Server Setup on share points. Users who can access the share point can then run Citrix Presentation Server Setup from the source image.

When you create and maintain an administrative source image, you can apply any Windows Installer patch files (files with the .msp extension) to the image as they are released. Applying patch files to the source image allows you to install the patches when you install the application on a clean system; you do not have to install the patches separately after you install the application.

You create administrative installations on network share points only once. Citrix recommends that you create the following two administrative installation source images:

- The installation package and any transforms needed to create the server farm. Run this image on the first server in the server farm.
- The installation package and any transforms needed to join other servers to the server farm. Run this image on all servers joining an existing server farm.

Follow the steps below to create an administrative installation on a network share point.

To create an administrative installation

1. Copy the Citrix Presentation Server CD image to a network location that is accessible to administrators and servers.
2. Create the appropriate transform files to create a new server farm and to join a server farm.
3. Run the **msiexec** /a command to create two network images from which Citrix Presentation Server can be installed:

   - The image to use when creating a server farm
   - The image to use when joining a server farm

   The following is an example of the command line to use to accomplish this:

   ```
   msiexec /a <full path to the base mps.msi package> /L*v <full
   path to a log file> /qb TARGETDIR="<full path to the network
   location>" TRANSFORMS=<semi-colon delimited list of the
   appropriate transform file(s) created from Step 2 (example:
   sql_join.mst)>
   ```

4. Run Citrix Presentation Server Setup from the network share points you created. Start with the share point that contains the image used to create the first server in the farm. The following is an example of a command line to accomplish this:

   ```
   msiexec /i <full path to my new share point mps.msi> /L <full
   path to a log file location> /qb-
   ```

Creating an Installation Log File

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

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

---

Caution Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before making changes to it.

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer

Type: REG_SZ
Name: Logging
Value data: voicewarmup

A log file is created in the %Tmp% directory for each operation.

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

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

Sample Transforms and Setup Properties

Four sample transforms are provided on the Citrix Presentation Server CD:

- Localdb_access_create.mst
- Join_Indirect.mst
- thirdpartydb_create_direct.mst
- thirdpartydb_join_direct.mst

This appendix discusses how to edit these sample transforms to perform various types of unattended installations and also details the setup property names and values contained within the transforms.

Editing the Sample Transforms

The properties within the sample transforms can be edited using commercially available Windows Installer editing tools. The transforms include sample values for select properties, allowing you to determine which properties to edit to achieve a certain configuration.

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

1. Using your preferred tool for editing Windows Installer packages, open the Citrix Presentation Server Setup Windows Installer package, Mps.msi, located on the Citrix Presentation Server CD in the \Citrix Presentation Server directory.
2. Apply the transform that includes the properties and values you want to modify.
3. Enter new values for the properties you want to change.
4. Generate the transform file.
5. Save the file with a new name.

Localdb_access_create.mst

This sample transform can be used to create a new server farm using a locally hosted database for the farm data store. The database is stored locally on the first server in the farm on which you installed Citrix Presentation Server.

Properties and Sample Values

CTX_MF_NEW_FARM_NAME=FarmAccess

CTX_MF_USER_NAME=Administrator

CTX_MF_DOMAIN_NAME=Domain1

CTX_MF_FARM_SELECTION=Create

CTX_MF_CREATE_FARM_DB_CHOICE=Local

CTX_MF_LOCAL_DATABASE=SQL

CTX_MF_MSDE_INSTANCE_NAME=CITRIX_METAFRAME

CTX_MF_LICENSE_SERVER_NAME=License_Server

CTX_MF_SHADOWING_CHOICE=Yes

CTX_MF_ENABLE_VIRTUAL_SCRIPTS=Yes

CTX_MF_XML_PORT_NUMBER=80

CTX_MF_XML_CHOICE=Share

CTX_MF_SERVER_TYPE=a

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

Join_Indirect.mst

This sample transform can be used to join an existing server farm that uses a locally hosted data store. In this sample transform, the existing server farm uses a Microsoft SQL Server 2005 Express database stored on one of the servers running Citrix Presentation Server.

Note If you use this transform, it does not attempt to enable IMA encryption. If you are using this transform and you want to enable IMA encryption, you must enable it manually after installation by using the CTXKEYTOOL. See "CTXKEYTOOL" on page 309 for details.

Properties and Sample Values

CTX_MF_FARM_SELECTION=Join

CTX_MF_INDIRECT_JOIN_USER_NAME=Administrator

CTX_MF_INDIRECT_JOIN_DOMAIN_NAME=Domain1

CTX_MF_JOIN_FARM_SERVER_NAME=Server1

CTX_MF_JOIN_FARM_SERVER_PORT=2512

CTX_MF_JOIN_FARM_DB_CHOICE=Indirect

CTX_MF_LICENSE_SERVER_NAME=License_Server

CTX_MF_ENABLE_VIRTUAL_SCRIPTS=Yes

CTX_MF_XML_PORT_NUMBER=80

CTX_MF_XML_CHOICE=share

CTX_MF_SERVER_TYPE=a

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=Yes

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

You must add the following row to the transform because it is not available in the default Windows Installer package. If you have a blank password, do not add the password property. In general, if a property exists in the .msi file and you want to set it to "Null," delete the property in the transform file.

CTX_INDIRECT_JOIN_PASSWORD=Password

thirdpartydb_create_direct.mst

This sample transform can be used to create a new server farm using a data store on a separate database server. This sample transform creates a farm that uses a Microsoft SQL Server, Oracle, or IBM DB2 database for the farm data store. The database is stored on a dedicated database server and is configured for direct access by the servers in the farm.

Properties and Sample Values

CTX_MF_NEW_FARM_NAME=Farm-ThirdParty

CTX_MF_CREATE_FARM_DB_CHOICE=ThirdParty

CTX_MF_USER_NAME=Administrator

CTX_MF_DOMAIN_NAME=Domain1

CTX_MF_FARM_SELECTION=Create

CTX_MF_ODBC_USER_NAME=sa

CTX_ODBC_PASSWORD=citrix

CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix

CTX_MF_LICENSE_SERVER_NAME=License_Server

CTX_MF_SHADOWING_CHOICE=Yes

CTX_MF_XML_PORT_NUMBER=180

CTX_MF_XML_CHOICE=Separate

CTX_MF_SERVER_TYPE=e

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

You must add the following row to the transform because it is not available in the default Windows Installer package.

CTX_MF_SILENT_DSNFILE =\\fileserver\image\TestSQL.DSN

thirdpartydb_join_direct.mst

This sample transform can be used to join an existing server farm that uses a data store on a separate database server. In this sample transform, the existing server farm uses a Microsoft SQL Server, Oracle, or IBM DB2 database stored on a dedicated database server. The new server joining the farm accesses the data store directly.

Properties and Sample Values

CTX_MF_FARM_SELECTION=Join

CTX_MF_JOIN_FARM_DB_CHOICE=Direct

CTX_MF_ODBC_USER_NAME=sa

CTX_ODBC_PASSWORD=citrix

CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix

CTX_MF_LICENSE_SERVER_NAME=License_Server

CTX_MF_SHADOWING_CHOICE=Yes

CTX_MF_XML_PORT_NUMBER=180

CTX_MF_XML_CHOICE=Separate

CTX_MF_SERVER_TYPE=e

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

You must add the following row to the transform because it is not available in the default Windows Installer package.

CTX_MF_SILENT_DSNFILE =\\fileserver\image\TestSQL.DSN

Setup Property Names and Values

Some values, such as passwords, may be case-sensitive. Values that include spaces must be enclosed in quotation marks ("") if you are using them in a command line.

CTX_USE_EXISTING_JRE

Definition: Use this property to indicate to the installer to accept the version of JRE currently installed on your computer.

Possible values: "Yes" or "No"

Default value: "No"

CTX_MF_FARM_SELECTION

Definition: Defines whether you are creating a new server farm or joining an existing farm. If this server is joining an existing farm, you must set CTX_MF_JOIN_FARM_DB_CHOICE.

Possible values: "Create" or "Join"

Default value: "Create"

CTX_MF_NEW_FARM_NAME

Definition: The name of the new farm; always specify if you are creating a new farm.

Possible values: User defined

Default value: "NewFarmName"

CTX_MF_USER_NAME

Definition: User name for the initial Citrix administrator credentials; applies only when creating a farm.

Possible values: User defined

Default value: "UserName"

CTX_MF_DOMAIN_NAME

Definition: Domain name for the farm administrator credentials; applies only when creating a farm.

Possible values: User defined

Default value: "DomainName"

CTX_MF_CREATE_FARM_DB_CHOICE

Definition: When creating a new server farm, specify whether the database is a local database stored on the first server in the new farm, or a third-party database stored on a separate database server.

Possible values:

- "Local" (Access or SQL Server 2005 Express)
- "Third Party" (SQL, Oracle, or IBM DB2)

Default value: "Local"

CTX_MF_LOCAL_DATABASE

Definition: Type of locally stored database that stores the farm data store.

Possible values: "Access" or "SQL" ("SQL" for SQL Server 2005 Express)

Default value: "Access"

CTX_MF_MSDE_INSTANCE_NAME

Definition: If you are using SQL Server Express for a local database, you can specify an installed instance of SQL Server Express instead of using the default. If you specify an instance of SQL Server Express other than the default — for example, if you install SQL Server Express using a command prompt and specify custom options — you must enter the name of the custom instance you install.

Possible values: User defined

Default value: "CITRIX_METAFRAME"

CTX_ODBC_PASSWORD

Definition: Password for a third-party database that stores the farm data store.

Possible values: User defined

Default value: "Password"

CTX_MF_ODBC_USER_NAME

Definition: User name for a third-party database that stores the farm data store.

Possible values: User defined

Default value: "UserName"

CTX_MF_SILENT_DSNFILE

Definition: Path to the DSN file to be used for the data store; use for silent installation.

Possible values: Complete path to the DSN file

Default value: "" (null)

CTX_MF_JOIN_FARM_DB_CHOICE

Definition: Use when joining this server to an existing server farm.

Possible values: "Direct", "Indirect"

Set this property's value to "indirect" if you are using a Microsoft Access or SQL Server 2005 Express database, stored locally on the first server in the farm on which you installed Citrix Presentation Server, for the data store. Set this property's value to "direct" if you are using a Microsoft SQL, Oracle, or IBM DB2 database, stored on a separate dedicated database server, for the data store.

Default value: "Direct"

CTX_MF_INDIRECT_JOIN_DOMAIN_NAME

Definition: Domain name of a user account that has full administrative rights in Citrix Presentation Server. Define if you are joining a farm that uses a Microsoft Access or SQL Server 2005 Express database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: Can be any user's domain (the user account must have full administrative rights in Citrix Presentation Server).

Default value: "DomainName"

CTX_MF_INDIRECT_JOIN_USER_NAME

Definition: User name of a user account that has full administrative rights in Citrix Presentation Server. Define if you are joining a farm that uses a Microsoft Access or SQL Server 2005 Express database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: Can be any user who has full administrative privileges in Citrix Presentation Server.

Default value: "Administrator"

CTX_INDIRECT_JOIN_PASSWORD

Definition: The password for a user account that has full administrative rights in Citrix Presentation Server. Define if you are joining a farm that uses a Microsoft Access or SQL Server 2005 Express database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: The password for the user name entered in CTX_MF_INDIRECT_JOIN_USER_NAME.

Default value: "" (null)

CTX_MF_JOIN_FARM_SERVER_NAME

Definition: Name of a server in the server farm that you want to join.

Possible values: The name of a server hosting the Access or SQL Server 2005 Express data store

Default value: "ServerName"

CTX_MF_JOIN_FARM_SERVER_PORT

Definition: The port number for the IMA communication port used to communicate with the locally stored server farm data store (for example, if you are using a Microsoft Access or SQL Server 2005 Express database, stored locally on the first server in the farm on which you installed Citrix Presentation Server, for the data store).

Possible values: User defined

Default value: "2512"

CTX_MF_ZONE_NAME

Definition: The name of the zone to which the server belongs.

Possible values: Not applicable

Default value: None. The default value for the zone name is generated programatically, based on the subnet address of the server.

CTX_MF_ADD_ANON_USERS

Definition: Determines whether or not anonymous users added to the Users group are included in the Remote Desktop Users group on Windows Server 2003. This property is ignored during upgrades.

If set to "Yes" and if CTX_MF_CREATE_REMOTE_DESKTOP_USERS is set to "CopyUsers" or "DoNothing" during a clean install, the anonymous users are added to the Remote Desktop Users group. If CTX_MF_CREATE_REMOTE_DESKTOP_USERS is set to "AddEveryone," this property is ignored because the Remote Desktop Users group is configured so that every user in the Users group is also a remote desktop user. Set this property to "No" during a clean install to prohibit anonymous connections to Citrix Presentation Server running on Windows Server 2003.

Possible values: "Yes" or "No"

Default value: "Yes"

Note CTX_MF_CREATE_REMOTE_DESKTOP_USERS takes precedence over CTX_MF_ADD_ANON_USERS. If CTX_MF_CREATE_REMOTE_DESKTOP_USERS is set to "AddEveryone" and CTX_MF_ADD_ANON_USERS is set to "No," anonymous connections to Citrix Presentation Server are enabled on this server.

CTX_MF_CREATE_REMOTE_DESKTOP_USERS

Definition: Determines whether or not to add users to the Remote Desktop Users group on a Windows Server 2003 system. Users must be members of the Remote Desktop Users group to log on remotely to a Windows Server 2003 system.

Setting this property has no effect if the Remote Desktop Users group already has members.

Possible values:

"AddEveryone" — Adds the Authenticated Users group to the Remote Desktop Users group. This option allows all current and future authenticated users to log on remotely to the server.

"CopyUsers" — Copies all current users from the Users group to the Remote Desktop Users group. Any user accounts you add must be added to the Remote Desktop Users group manually.

"DoNothing" — Does not add any users to the Remote Desktop Users group. Choosing this option means that no users will be allowed to log on remotely to the server until you add users to the Remote Desktop Users group in Windows Server 2003.

Default value: "CopyUsers"

CTX_MF_SHADOWING_CHOICE

Definition: Turns session shadowing on/off.

Important If you turn session shadowing off when you install Citrix Presentation Server, you cannot enable shadowing at a later time through user policies or connection configuration.

Possible values: "Yes" (turn it on) or "No" (turn it off)

Default value: "Yes"

CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA

Definition: Prohibits or allows remote control of mouse and keyboard in ICA sessions.

Possible values: "Yes" (prohibit) or "No" (allow)

Default value: "No"

CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION

Definition: Prohibits or allows shadowing connections without user notification.

Possible values: "Yes" (prohibit) or "No" (allow)

Default value: "No"

CTX_MF_SHADOW_PROHIBIT_NO_LOGGING

Definition: Prohibits or allows shadow connections without logging.

Possible values: "Yes" (prohibit) or "No" (allow)

Default value: "No"

CTX_MF_XML_CHOICE

Definition: Determines whether Microsoft Internet Information Services (IIS) and the Citrix XML Service share the same port on this server or use separate ports. If you do not want IIS and the Citrix XML Service to share the same port, you must set the Citrix XML Service port number in CTX_MF_XML_PORT_NUMBER.

Possible values: "Share" (share with IIS) or "Separate" (use separate port, set in CTX_MF_XML_PORT_NUMBER)

Default value: "Share"

CTX_MF_XML_PORT_NUMBER

Definition: Port number you want the Citrix XML Service to use when you do not want the Citrix XML Service and IIS to share ports.

Possible values: User defined

Default value: "80"

CTX_MF_SERVER_TYPE

Definition: The edition of Citrix Presentation Server to be installed. If you are performing a silent installation and using a command line, the command line arguments for this property must be set to the correct value.

Possible values: "E" (Enterprise Edition), "A" (Advanced Edition), or "S" (Standard Edition).

Default value: "E"

CTX_MF_ENABLE_VIRTUAL_SCRIPTS

Definition: Directs Citrix Presentation Server Setup to create the virtual scripts directory. If the value is set to "Yes" or "1," Setup does not display the dialog box asking for permission to create the virtual scripts directory, even if you are running Setup in full UI mode.

If you are running a silent installation where this property is not set to "Yes" or "1," and the XML port on the server is shared with IIS (for example, if you are installing the Web Interface), Setup aborts and the following error message is added to the installation log file:

"ERROR: SetIISScriptsDir - Could not get the scripts path because the Virtual Scripts directory in not enabled in IIS or the property CTX_MF_ENABLE_VIRTUAL_SCRIPTS is not set to Yes."

If the property is defined, the silent installation continues with no error.

Possible values:

- "Yes" or "1" (Create the virtual scripts directory if it does not already exist.)
- Not defined, "0" or "No" (Do not create the virtual scripts directory if it does not already exist. You are prompted during Setup to create the virtual scripts directory.)

Default value: Not defined

CTX_IMA_PROTECTION_ENABLE

Definition: Use this property (set the property to 1) to inform Citrix Presentation Server Setup that IMA encryption should be enabled for the farm. This property is useful only during the creation of a farm to Presentation Server 4.5. This property has no affect during a join to a Presentation Server 4.5 farm.

Possible values: “1” or “0”

Default value: “0”

CTX_PROTECT_KEY_TYPE

Definition: Use this property to indicate how the encryption key will be provided. The “existing” value informs Citrix Presentation Server Setup that a key is already loaded on the computer, and Setup will not attempt to replace the existing key with a new key from the file. If you want to provide a path to the location where the key file resides, choose the “file” setting and then use the CTX_PROTECT_KEY_PATH property. If you want to provide a writable location where the key file can be stored after the install generates a new encryption key, choose the “generate” setting and then use the CTX_PROTECT_NEW_KEY_PATH property. This property has functional impact only if you use it in conjunction with either the CTX_PROTECT_KEY_PATH property or the CTX_PROTECT_NEW_KEY_PATH property.

Possible values: “file,” “generate,” or “existing”

Default value: “file”

CTX_PROTECT_KEY_PATH

Definition: Use this property to indicate the complete path to where a valid encryption key file is stored. This property should be used in conjunction with the CTX_PROTECT_KEY_TYPE property with a value of “file.” Failure to set both keys correctly will cause Citrix Presentation Server Setup not to activate the encryption settings for the current server.

Possible values: The full path where an encryption key file is stored

Default value: “” (null)

CTX_PROTECT_NEW_KEY_PATH

Definition: Use this property to indicate the complete path to a file that can be created to store the encryption key. This location must be writable because it will store the newly-created key file. If the location is not writable, the install will fail. This property should be used in conjunction with the CTX_PROTECT_KEY_TYPE property with a value of "generate." Failure to set both keys correctly will cause Citrix Presentation Server Setup not to activate the encryption settings for the current server.

Possible values: The full path where an encryption key file can be stored

Default value: "" (null)

CTX_MF_ADD_LOCAL_ADMIN

Definition: If enabled, creates Citrix administrator accounts for all user accounts in the local Administrators group.

Possible values: "Yes" or "No"

Default value: "No"

CTX_ADDLOCAL

Definition: This property is similar to the Windows Installer ADDLOCAL property.

Possible values: Blank (default), All, CTX_MF_MetaFrame_Core, CTX_MF_IM, CTX_MF_IM_Packager, CTX_MF_IM_Service, CTX_MF_LM, CTX_MF_NM, CTX_MF_RM, PN_ENGINE, PN, PN_AGENT, WMI, MetaFrame_XP, CTX_MF_CMC, CTX_MF_ICA_Shell_Editor, CTX_MF_IMA_Core, CTX_MF_IM_Plugin, CTX_MF_RM_Plugin, CTX_SMA, CTX_MF_CTXCPU, CTX_MF_CTXSFO, CTX_MF_ASCII.

Separate entries by commas. Valid configurations are:

All — Install every feature (XPE configuration).

MetaFrame_XP,CTX_MF_MetaFrame_Core,CTX_MF_IMA_Core,CTX_MF_ICA_Shell_Editor,CTX_SMA,CTX_MF_CTXCPU,CTX_MF_CTXSFO — Core MetaFrame, required for any configuration (referred to below as @Core).

PN, PN_ENGINE — Install the full Program Neighborhood client as the Pass-Through Client (referred to below as PN).

PN_AGENT, PN_ENGINE — Install the Program Neighborhood Agent as the Pass-Through Client.

CTX_MF_CMC,CTX_MF_IM_Plugin,CTX_MF_RM_Plugin — Install the Presentation Server Console (referred to below as @CMC).

CTX_MF_IM_Service — Install the Installation Manager installer service.

CTX_MF_IM_Packager — Install the Installation Manager Packager.

CTX_MF_IM,CTX_MF_IM_Service,CTX_MF_IM_Packager — Install all Installation Manager components (referred to below as @IM).

CTX_MF_RM — Install Resource Manager.

@Core,CTX_MF_LM,WMI,@CMC,PN,@IM,CTX_MF_RM,CTX_MF_ASCII — Install all default Citrix Presentation Server Enterprise Edition components.

@Core,CTX_MF_LM,@CMC,PN — Install all default Citrix Presentation Server Advanced Edition components.

@Core,@CMC,PN — Install all default Citrix Presentation Server Standard Edition components.

Default value: Blank

Note *@Core* is a placeholder and should not actually be used in your command.

CTX_RDP_DISABLE_PROMPT_FOR_PASSWORD

Definition: Setting this property to "Yes" changes the security setting on the server so that passwords from users of Microsoft Remote Desktop Web Connection software are not required. Users must still enter credentials when logging on to the Web Interface, but can launch applications without further prompts for credentials by the server.

Possible values: "Yes" or "No"

Default value: "No"

CTX_MF_LIC_CHOICE_FOR_CREATE

Definition: Configures the server to point to an existing Citrix License Server. If set to "Point," ensure that CTX_MF_LICENSE_SERVER_NAME points to a valid license server. If you install the license server after installing Citrix Presentation Server, set CTX_MF_LIC_CHOICE_FOR_CREATE to "DontKnow."

Possible values: "Point" or "DontKnow"

Default value: "Point"

Note You can also use the Access Management Console to configure the server to point to the license server.

CTX_MF_LICENSE_SERVER_NAME

Description: Defines the Citrix License Server to which the server points. Only applies:

- When performing a new installation while joining an existing server farm or performing an upgrade and CTX_MF_LIC_CHOICE_FOR_JOIN_OR_UPGRADE is set to "Point"
- When performing a new installation while creating a new server farm and CTX_MF_LIC_CHOICE_FOR_CREATE is set to "Point"

Possible values: User defined

Default value: "localhost"

CTX_MF_LIC_CHOICE_FOR_JOIN_OR_UPGRADE

Definition: Configures the server to point to an existing Citrix License Server. If set to "Point", ensure that CTX_MF_LICENSE_SERVER_NAME points to a valid license server. If set to "UseFarmSettings," ensure that the existing server farm is configured to use a license server. If you install the license server after installing Citrix Presentation Server, set CTX_MF_LIC_CHOICE_FOR_JOIN_OR_UPGRADE to "DontKnow."

Note You can also use the Presentation Server Console to configure the server to point to the license server.

Possible values: "Point" or "UseFarmSettings" or "DontKnow"

Default value: "UseFarmSettings"

CTX_MF_LICENSE_SERVER_PORT

Definition: If the value of CTX_MF_LICENSE_SEVER_PORT_DEFAULT is set to “” (null), CTX_MF_LICENSE_SERVER_PORT specifies the number of the port to use when communicating with the Citrix License Server.

Possible values: An integer representing the number of the port through which the license server has been configured to listen for requests.

Default value: “27000”

CTX_MF_LICENSE_SERVER_PORT_DEFAULT

Definition: When set to “” (null), specifies to use the value of CTX_MF_LICENSE_SERVER_PORT as the number of the port to use when communicating with the Citrix License Server.

Possible value: “” (null)

Default value: “1”

CTX_IGNORE_MCM

Definition: Citrix Presentation Server is not compatible with Conferencing Manager 2.0. If you upgrade to Citrix Presentation Server before upgrading Conferencing Manager, Conferencing Manager fails on this server. Therefore, Citrix recommends that you upgrade Conferencing Manager before upgrading to Citrix Presentation Server. The latest version of Conferencing Manager is available from the Citrix Presentation Server components installation CD.

If the installer detects Conferencing Manager 2.0 on the server, an error message appears. Set this property to “Yes” for the installer to ignore the error message and continue the installation.

Possible values: “Yes” or “No”

Default value: “No”

CTX_REMOVE_WI_TURNKEY

Definition: When upgrading from earlier versions of Presentation Server that include the Web Interface, you must upgrade the Web Interface before upgrading to Citrix Presentation Server. Otherwise, the Web Interface may be removed from the server as a result of the upgrade. Set this property to “Yes” if you do not object to the removal of the Web Interface from the server.

Possible values: “Yes” or “No”

Default value: “No”

CTX_MF_ONLY_LAUNCH_PUBLISHED_APPS

Definition: Citrix Presentation Server features a security enhancement that prohibits non-administrative users from launching desktop sessions (but not published applications). If set to "Yes," the security enhancement is enabled.

Possible values: "Null," "Yes," or "No"

Default value: "Null"

Note If set to a value other than "Yes" or "No," the security enhancement is enabled when performing a clean install but disabled when performing an upgrade.

CTX_SERV_PRINTER_LOGON

Definition: Defines the Citrix Print Manager Service as the printer user rather than using the built in accounts created by Presentation Server.

Default value: ctx_cpsvcuser

Format: USERID:PASSWORD:DOMAIN/MACHINENAME

CTX_SERV_MALOO_LOGON

Definition: Defines the Citrix CPU Utilization Mgmt/CPU Rebalancer Service as the CPU user rather than using the built-in accounts created by Presentation Server.

Default value: ctx_cpuuser

Format: USERID:PASSWORD:DOMAIN/MACHINENAME

INSTALLDIR

Definition: The target location for the installation.

Possible values: User defined

Default value: %Program Files%\Citrix

REBOOT

Definition: Standard Windows Installer property that controls whether you restart a server or prompt for the server to be restarted.

Possible values:

"Force" (forces restart to occur; no further prompts are displayed)

"Suppress" (forces restart to *not* occur by default; a prompt occurs if action is necessary)

"ReallySuppress" (forces restart to *not* occur; no prompts appear)

Default value: "Force"

REINSTALLMODE

Definition: Specifies the type of reinstall to perform. Options are case-insensitive and order-independent.

Important Citrix recommends that you do not modify this property.

Possible values:

p - install missing files

o - replace older versioned or missing files

c - replace corrupt files (checksum validation)

e - replace same versioned or missing files

d - replace files of differing versions

a - replace all files regardless of version

u - replace user registry settings

m - replace machine registry settings

s - replace shortcuts

v - replace the cached .msi package with the package being installed from

Default value: "oums"

Pass-Through Client Properties

Use the following properties if you are installing the Pass-Through Client.

CLIENT_NAME

Definition: Identifies the client device to the server farm.

Possible values: User defined

Default value: %COMPUTERNAME%

CLIENT_UPGRADE

Definition: Upgrades the client with the more current version.

Possible values: "Yes" or "No"

Default value: "Yes"

CLIENT_INSTALLDIR

Definition: The target location for the Pass-Through Client installation.

Possible values: User defined

Default value: %Program Files%\Citrix\ICA Client

ENABLE_DYNAMIC_CLIENT_NAME

Definition: When using the Pass-Through Client, turn on/off the capability to use the computer name as the client device name and recognize changes to the client name.

Possible values: "Yes" or "No"

Default value: "Yes"

PROGRAM_FOLDER_NAME

Definition: *Start Menu Program Folder Name*, where *Start Menu Program Folder Name* is the name of the Programs folder on the Start menu containing the shortcut to the Program Neighborhood or Program Neighborhood Agent software.

Possible values: User defined

Default value: "Citrix\MetaFrame Access Clients"

SERVER_LOCATION

Definition: The URL of the server running the Web Interface. This server hosts the configuration file for the Program Neighborhood Agent. You must enter the server address if you want to use the Program Neighborhood Agent as the Pass-Through Client. The server address can use HTTP or HTTPS.

Possible values: User defined

Default value: "localhost"

DEFAULT_NDSCONTEXT

Definition: Include this parameter if you want to set a default context for NDS. If you are including more than one context, place the entire value in quotation marks, and separate the contexts by a comma.

Examples of correct parameters:

```
DEFAULT_NDSCONTEXT=Context1
```

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

Example of an incorrect parameter:

```
DEFAULT_NDSCONTEXT=Context1,Context2
```

ENABLE_SSON

Definition: Set to "Yes" to enable Single Sign-On (Pass-Through Authentication) for the Pass-Through Client. Set to "No" to disable Single Sign-On for the Pass-Through Client.

Possible values: "Yes" or "No"

Default value: "Yes"

APPENDIX E

Data Store Database Requirements

The following appendix provides information about the database requirements for the data store, including the following:

- A list of the databases that are supported
- Information about configuring connections to these databases
- Migrating from Microsoft SQL Server Desktop Engine (MSDE) 2000 to SQL Server 2005 Express

Supported Databases

You can use the Microsoft Access or SQL Server 2005 Express Edition SP1 database engines or a Microsoft SQL Server, Oracle, or IBM DB2 database for the farm's data store. The supported database versions are listed below.

- Microsoft Access Jet Database Engine for Windows Server 2003 with Service Pack 1
- Microsoft Access Jet Database Engine for Windows Server 2003 x64
- Microsoft SQL Server 2005 Express Edition (32-bit) with Service Pack 1 for Windows Server 2003 with Service Pack 1
- Microsoft SQL Server 2005 Express Edition (32-bit) with Service Pack 1 for Windows Server 2003 x64
- Microsoft SQL Server 2000 with Service Pack 4 for Windows Server 2003 with Service Pack 1
- Microsoft SQL Server 2005 for Windows Server 2003 with Service Pack 1
- Microsoft SQL Server 2005 for Windows Server 2003 x64

- IBM DB2 Enterprise Version 8.2 for Windows Server 2003 with Service Pack 1
- IBM DB2 Universal Database Version 8.2 for Windows Server 2003 x64
- Oracle Enterprise 9.2.0.1 for Windows Server 2003 with Service Pack 1
- Oracle Enterprise 9.2.0.1 for Solaris SPARC 32
- Oracle Enterprise 10.2.0.1.0 for Windows Server 2003 with Service Pack 1
- Oracle Enterprise 10.2.0.1.0 for Windows Server 2003 x64

Microsoft SQL Server, Oracle, and IBM DB2 databases require an ODBC database client driver installed on each server that connects directly to them. Servers that connect to the data store database indirectly (that is, through another server running Citrix Presentation Server) do not require an ODBC client driver.

Note The supported versions of Microsoft Access, SQL Server and SQL Server 2005 Express Edition SP1 are verified for MDAC 2.8.

The following table lists the supported database client versions:

Database	Supported Client Version
IBM DB2 Enterprise Version 8.2 for Windows Server 2003 with Service Pack 1	8.2
IBM DB2 Universal Database Version 8.2 for Windows Server 2003 x64	UDB 8.2
Oracle Enterprise 9.2.0.1	9.2.0.1
Oracle Enterprise 10.2.0.1.0	10.2.0.1.0

Note Before installing an update of Microsoft Data Access Components (MDAC), stop the Microsoft Terminal Services Licensing service. Restart the Terminal Services Licensing service before beginning Citrix Presentation Server Setup.

Microsoft Access

Choosing **Use a local database on this server** and selecting the Access Database entry from the list of possible databases during Citrix Presentation Server Setup creates a Microsoft Access database on the first server in the new farm. This database acts as the farm's data store.

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

Minimum Requirements

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

- Approximately 50MB of disk space for every 100 servers. Increase disk space if there are a large number of published applications in the farm.
- 32MB of additional RAM if the server also hosts connections.

Authenticating to the Access Database

If you decide to create a local Microsoft Access database for the data store, Setup creates a database file called Mf20.mdb. The default user name and password for this database file are both "citrix."

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

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

For more information about dsmaint and other commands, see "Citrix Presentation Server Commands" on page 283.

Backing up the Access Database

You can use the **Dsmaint** command to back up or recover a Microsoft Access data store. Back up the data store regularly with a batch file script or before such events as making configuration changes.

Some backups occur automatically—each time the Citrix IMA Service is stopped or a server is restarted, the existing Mf20.mdb file is backed up, compacted, and copied as Mf20.bak. Each time the IMA Service starts, it deletes Mf20.bak if it exists and renames the Mf20.unk file to Mf20.bak. This process helps ensure that the Mf20.bak file is a valid farm database.

Caution If the server runs out of disk space on the drive where the Mf20.mdb file is stored, automatic backups stop. Ensure that the amount of free disk space is at least three times the size of the Mf20.mdb file.

The Mf20.mdb file and all automatic backup files are located by default in the %ProgramFiles%\Citrix\Independent Management Architecture folder (*%ProgramFiles(x86)%*\Citrix\Independent Management Architecture for 64-bit implementations).

Caution Do not try to recover the data store with the **dsmaint recover** command without first verifying that the Mf20.bak file exists because this command removes the existing Mf20.mdb file from the server. If the Mf20.bak file does not exist, run **dsmaint backup**.

Microsoft SQL Server 2005 Express Edition SP1

To use SQL Server 2005 Express Edition SP1 for the farm data store, install it on the server before you run Citrix Presentation Server Setup. If you intend to remap the server drives for Presentation Server, remap the server drives prior to installing SQL Server 2005 Express Edition SP1.

You can install SQL Server 2005 Express Edition SP1 using one of the following methods:

- Run the SetupSqlExpressForCPS.cmd batch file. Use this method if you do not have an instance of SQL Server 2005 Express Edition SP1 already installed on the server and you want to use the default instance name and password values. SetupSqlExpressForCPS.cmd is located in the Support\SqlExpress_2005_SP1 folder on the Citrix Presentation Server CD.

- Launch SQL Server 2005 Express Edition SP1 Setup from a command prompt. Use this method if you cannot use the default instance name and password. You must install Citrix Presentation Server using a manual method if you specify an instance name for SQL Server 2005 Express SP1 different from the default.

Important If you install SQL Server 2005 Express Edition SP1 and specify an instance name different from the default "CITRIX_METAFRAME," you must install Citrix Presentation Server using a manual installation method so that you can set the Citrix Presentation Server Setup property CTX_MF_MSDE_INSTANCE_NAME to the new instance name. See "Advanced Installation Methods" on page 365 for more information about Setup properties.

To install SQL Server 2005 Express Edition SP1 using default options

If you do not have an instance of SQL Server 2005 Express Edition SP1 already installed on the server and you are not using SQL authentication, you can run SetupSqlExpressForCPS.cmd, located on the Citrix Presentation Server CD in the \Support\SqlExpress_2005_SP1 directory.

Running the SetupSqlExpressForCPS.cmd batch file installs SQL Server 2005 Express Edition SP1 using the default instance name "CITRIX_METAFRAME" and sets the administrator ("SA") password to "CITRIX."

Note The administrator SA password is required to be set; however, SQL authentication is not enabled by default when you install SQL Server 2005 Express Edition SP1 using SetupSqlExpressForCPS.cmd. Because SQL authentication is not enabled, the SA password is not used. Setting the SA password to "CITRIX" is not a security risk unless you are using SQL authentication.

SetupSqlExpressForCPS.cmd creates the required files and directories for SQL Server 2005 Express Edition SP1 support in the \Program Files\Microsoft SQL Server directory and the named instance directory, MSSQL$CITRIX_METAFRAME.

If you need to specify an instance name and SA password, follow the procedure below to install SQL Server 2005 Express Edition SP1 at a command prompt using custom options.

To install SQL Server2005 Express Edition SP1 using custom options

1. At a command prompt, change to the \Support\SqlExpress_2005_SP1 directory on the Citrix Presentation Server CD. For example, if your CD drive is E, type:

   E:

   cd \Support\SqlExpress_2005_SP1

2. Change to installation mode by typing:

   change user /INSTALL

3. Launch the SQL Server 2005 Express Edition SP1 installer, specifying the instance name and SA password. For example, type:

   setup.exe INSTANCENAME=*name* SAPWD=*password*

4. After you install SQL Server 2005 Express Edition SP1, choose **Use a local database on this server** and select the **SQL Server Express Database** entry from the list of possible databases during Citrix Presentation Server Setup.

Minimum Requirements

The server hosting the SQL Server 2005 Express Edition SP1 database should meet the following minimum requirements:

- Approximately 50MB of disk space for every 100 servers and 25 applications in the farm
- 32MB of additional RAM if the server also hosts connections
- 70MB of disk space for the database

Important If you intend to use SQL Server 2005 Express Edition SP1 to host your farm's data store, do not use double-byte characters in the name of the server on which the database will be stored.

Authenticating to the SQL Server 2005 Express SP1 Database

Windows authentication is supported for the SQL Server 2005 Express Edition SP1 database. For security reasons, Microsoft SQL Server authentication is not supported.

Migrating to SQL Server 2005 Express

Presentation Server now supports SQL Server 2005 Express Edition SP1 edition. Presentation Server no longer supports using MSDE as the database for your data store; a good alternative is to migrate your database from MSDE to SQL Server Express. There are utilities on the Server CD that help you migrate your Microsoft Access data store or your MSDE data store to SQL Server Express.

Migrating from Access SQL Server Express

You can migrate a data store using Microsoft Access to SQL Server 2005 Express Edition SP1. To perform such a migration, run the **MigrateToSqlExpress** utility located in the \Support\SqlExpress_2005_SP1 directory on the Server CD.

For more information about the MigrateToSqlExpress utility, see “Citrix Presentation Server Commands” on page 283.

Migrating from MSDE to SQL Server Express

Citrix Presentation Server no longer supports Microsoft SQL Server Desktop Engine (MSDE). If your data store is running on an MSDE database and you are upgrading or migrating from a previous release of Presentation Server, you must migrate the data store from MSDE database to another database, such as SQL Server Express Edition SP1.

At a high level, you need to perform the following tasks to migrate your data store from a database run on MSDE to SQL Server Express:

- Grant the Network Service account access to the database
- Upgrade Presentation Server on your farm
- Run the Migrate to SQL Server Express utility to migrate the data store to the new database

The following procedure provides steps to guide you through these tasks.

To migrate your data store from MSDE to SQL Server Express

1. Give the Network Service account access to the MSDE CITRIX_METAFRAME instance. You can do this in one of the following ways:

   - **Use Microsoft SQL Server Management Studio Express.** Using this tool lets you grant the Network Service account access through a user interface. See "Using the SQL Server Management Studio Express" on page 403.
   - **Use a command-line script.** You can change the permissions by running the script Citrix provides in this manual. See "To use a script to update MSDE permissions" on page 404.

2. Upgrade or migrate your Presentation Server farm to Presentation Server 4.5. See "Upgrading or Migrating an Existing Server Farm" on page 77.
3. After running Setup to upgrade or migrate, **restart** the computer on which you installed Presentation Server 4.5 when prompted.

Important Do not proceed with the data store migration unless you have restarted the server on which you installed Presentation Server 4.5.

   After restarting the computer running Presentation Server, you may receive event log messages because Presentation Server 4.5 is temporarily using MSDE for the data store. After you complete the migration to SQL Server Express, these messages will not appear.

4. After restarting the computer on which you installed Presentation Server 4.5, stop the Citrix Independent Management Architecture service.

   You can stop this service using one of the following methods:

   - Stopping the Citrix Independent Management Architecture service in the Windows Services panel
   - Typing the following at a command prompt, and entering **y** when prompted:

     net stop "Citrix Independent Management Architecture"

5. Migrate the MSDE database by running the Migrate to SQL Server Express utility (MigrateToSqlExpress.exe), which is located on the Server CD for Presentation Server 4.5, under Support\SqlExpress_2005_SP1\.
6. **Restart** the server on which you just performed the migration when prompted.

Using the SQL Server Management Studio Express

You can grant the Network Service account access to MSDE CITRIX_METAFRAME instance by using a UI-based migration utility do this manually using SQL Server Management Studio Express. See Option A below.

Before you begin this procedure you must download and install the following:

- **Microsoft Core XML Services (MSXML) 6.0.** Download and install this package, which includes the Microsoft XML Parser, to update your XML services. It is available from the Download page of the Microsoft Web site.
- **SQL Server Management Studio Express.** Download and install this package. It provides tools that let you manage SQL Server Express that are not included with the standard installation. This is available on the MSDN Web site at http://msdn.microsoft.com/vstudio/express/sql/download/.

The following procedure is designed for use with the version of SQL Server Management Studio Express tool that is for Microsoft SQL Server 2005. The instructions may vary with if you are using another version of this tool.

To use SQL Server Management Studio Express to update MSDE permissions

1. Start SQL Server Management Studio Express and connect to the CITRIX_METAFRAME instance.
2. In SQL Server Management Studio Express, open the **Security** folder.
3. Right-click on **Logins** folder, then click **New Login**.
4. With the Windows authentication option selected, type the following:

   Login name: NT AUTHORITY\NETWORK SERVICE
5. Open the **Databases** folder, the **MF20** folder, and then the **Security** folder.
6. Right-click on the **Users** folder, then click **New User**.
7. With the **Login name** option selected, type the following:

   User name: NETWORK SERVICE

   Login name: NT AUTHORITY\NETWORK SERVICE.
8. In the Database role membership section, select the **db_owner** check box.
9. Click **OK**.

The Network Service account now has access to the MSDE CITRIX_METAFRAME instance.

To use a script to update MSDE permissions

Important Before running this script, you must have the environment variable for your system path set to the bin directory for your MSDE instance. This script does not work unless you set this environment variable.

1. Create a folder and name it Netservice.
2. In that folder, save the following script in a text file; name the file **netservice_perm.txt**:

```
USE MF20
go
sp_grantlogin 'NT AUTHORITY\NETWORK SERVICE'
go
sp_grantdbaccess 'NT AUTHORITY\NETWORK SERVICE'
go
sp_addrolemember 'db_owner','nt authority\network service'
go
```

3. From a command prompt within the Netservice folder, type the following command:

```
osql -E -S localhost\CITRIX_METAFRAME -i netservice_perm.txt
```

The Network Service account now has access to the MSDE CITRIX_METAFRAME instance.

Microsoft SQL Server

Citrix Presentation Server supports the following versions of Microsoft SQL Server for the farm's data store:

- SQL Server 2000 with Service Pack 4: MDAC 2.8, Windows Server 2003 with Service Pack 1
- SQL Server 2005: MDAC 2.8, Windows Server 2003 with Service Pack 1
- SQL Server 2005: MDAC 2.8, Windows Server 2003 x64

Minimum Requirements

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

The server hosting the SQL Server database should meet the following minimum requirements:

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

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

Authenticating to the Microsoft SQL Server Database

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

- Microsoft SQL Server supports Windows and Microsoft SQL Server authentication. For high-security environments, Citrix recommends using Windows authentication only.
- The user account used for installing, upgrading, or applying hotfixes to the data store must have database owner (db_owner) rights to the database.

- When you finish installing the database with database owner rights, set the user permissions to read/write only. Doing this increases the security of the database.

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

- When using Microsoft SQL Server in a replicated environment, be sure to use the same user account for the data store on each Microsoft SQL Server.

Configuring Microsoft SQL Server

Consider the following issues when planning the configuration of the server to host the Microsoft SQL Server data store database:

- Each farm requires a dedicated database. However, multiple databases can be running on a single server running Microsoft SQL Server. Do not configure the farm to use a database that is shared with any other client/server applications.
- Set the **Truncate log on Checkpoint** option in your database to control log space.
- Back up the database regularly and follow Microsoft recommendations for configuring database and transaction logs for recovery.
- If your database server hosts more than 256 connections (each server running Citrix Presentation Server uses one connection) and uses a Microsoft SQL Server data store, the number of worker threads available for the database must be equal to or greater than the number of connections. See the Microsoft SQL Server documentation for procedures to increase worker threads.

Using Sockets Rather than Named Pipes

Two common protocols that can be used to connect to a database are TCP/IP sockets and named pipes. Named pipes is an authenticated communication protocol so any time you attempt to open a connection to the SQL Server database using named pipes, the Windows authentication process occurs. TCP/IP sockets do not rely on Windows authentication to establish a connection, but do provide user/password authentication to the database after the connection is established. This eliminates the possibility of an error that could occur if you are using Windows authentication, and the server running SQL Server and the server running Citrix Presentation Server do not have the correct domain or Active Directory trust relationship. Therefore, for better performance, Citrix recommends that you use TCP/IP sockets instead of named pipes to connect servers running Citrix Presentation Server to a server hosting Microsoft SQL Server.

Note If a Data Source Name (DSN) is set up on a Windows 2000 server, named pipes may be selected by default. To change this setting to use a TCP/IP sockets connection, during DSN configuration, on the **Create a New Data Source to SQL Server** window, click the **Client Configuration** button. On the **Add Network Library Configuration** window, select **TCP/IP**.

Note Although Citrix recommends using TCP/IP sockets, if you are running SQL Server 2005 and you want to use named pipes to establish a connection to the database, the named pipes option must be enabled manually on the database server. To enable named pipes, use the Surface Area Configuration tool that is packaged with SQL Server 2005. For additional information about how to use named pipes to connect to a SQL Server 2005 database, see your SQL Server 2005 documentation.

The following procedures explain how to configure the connection to use TCP/IP sockets.

To create a SQL Server data source connection during Citrix Presentation Server Setup

1. Enter the data source description and select the SQL Server to which to connect. Click **Next**.
2. Select **NT Authentication** or **SQL Server Authentication**.
3. Click **Client Configuration**.

4. Select **TCP/IP** from the available network libraries. Click **OK**.
5. After installing Presentation Server, modify the Data Source Name (DSN) you created during installation and change its client configuration to use TCP/IP.

To modify a DSN, use the Windows ODBC Data Source Administrator utility to open the File DSN, which is located by default in the %ProgramFiles%\Citrix\Independent Management Architecture folder (*%ProgramFiles(x86)%*\Citrix\Independent Management Architecture for 64-bit implementations), and select TCP/IP as the connection protocol for the client configuration.

Failover

For fault tolerance with Microsoft SQL Server, use Microsoft clustering, which provides failover and failback for clustered systems. If failover of the SQL Server database occurs in a clustered environment, the failover of the database is transparent to Citrix Presentation Server.

A Microsoft Cluster Services cluster group is a collection of resources, such as disk drives, that are owned by one of the failover cluster nodes. You can transfer the ownership of the group from one node to another, but each group can be owned by only one node at a time.

The database files for an instance of Microsoft SQL Server are placed in a single cluster group owned by the node on which the instance is installed. If a node running an instance of Microsoft SQL Server fails, the cluster group containing the data files for that instance is switched to another node. Because the new node already has the executable files and registry information for that instance of Microsoft SQL Server on its local disk drive, it can start up an instance of Microsoft SQL Server and start accepting connection requests for that instance.

Note Microsoft Cluster Services clustering does not support load balancing among clustered servers because it functions in active/passive mode only.

Distributed Databases

Citrix Presentation Server supports distributed (replicated) databases. Replicated databases are useful when too many read requests to the data store create a processing bottleneck. Microsoft SQL Server uses replication to create the distributed database environment.

Citrix Presentation Server requires data to be coherent across multiple databases. Coherent data is the same across the databases and synchronized for updating. A two-phase commit algorithm is required to maintain data coherency when there are writes to the database.

When configuring Microsoft SQL Server for a two-phase commit, you must use the Immediate Updating Subscriber model. See your Microsoft SQL Server documentation for information about setting up replication with the Immediate Updating Subscriber model.

Caution Do not use merged replication. Using merged replication corrupts the data store.

The following procedure explains how to set up a distributed database environment for an existing farm.

To set up a distributed environment for an existing farm

1. Configure a Publisher (the Microsoft SQL Server currently hosting the data store) and Subscribers (remote sites) using Microsoft SQL Server Enterprise Manager.
2. Execute the **dsmaint publishsqlds** command on a server in the farm. This step executes the necessary SQL statements to create the published articles on the current Microsoft SQL Server (Publisher). For more information about the **dsmaint** command, see “DSMAINT” on page 322.
3. Configure the remote sites (Subscribers) to subscribe to the published articles you created in Step 2.

Migrating to SQL Server

Migration of a farm data store to Microsoft SQL Server is supported for the database versions listed in the following table. For information about data store migration, see "DSMAINT" on page 322.

Original platform	Target platform
Microsoft Access	SQL Server 2000 with SP 3a
Oracle 9.2.0.1	SQL Server 2000 with SP 3a
Oracle 10.2.0.1.0	SQL Server 2000 with SP 3a
IBM DB2 version 8.2	SQL Server 2000 with SP 3a
Microsoft Access	SQL Server 2005
SQL Server 2005 Express Edition	SQL Server 2005
Oracle 9.2.0.1	SQL Server 2005
Oracle 10.2.0.1.0	SQL Server 2005
IBM DB2 version 8.2	SQL Server 2005
SQL Server 2000 with SP 3a	SQL Server 2005

Oracle

Citrix Presentation Server supports the following Oracle databases for the farm's data store:

- Oracle Enterprise 9.2.0.1 for Windows Server 2003 with Service Pack 1
- Oracle Enterprise 9.2.0.1 for Solaris SPARC 32
- Oracle Enterprise 10.2.0.1.0 for Windows Server 2003 with Service Pack 1
- Oracle Enterprise 10.2.0.1.0 for Windows Server 2003 x64

Minimum Requirements

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

The server hosting the Oracle database should meet the following minimum requirements.

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- The Oracle Client must be installed on the server before you install Citrix Presentation Server.

Authenticating to the Oracle Database

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

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

Configuring an Oracle Data Store

Consider the following guidelines when configuring an Oracle server to host the server farm's data store.

- Use Shared/Multi-Threaded Server mode to reduce the number of processes in farms with more than 100 servers. However, performance may be affected during periods of high data store load. Consult your Oracle documentation for information about configuring the database to run in Multi-Threaded Server mode.
- When using an Oracle server in dedicated mode, add one additional process for each server connected directly to the Oracle database. For example, if the Oracle server uses 100 processes before installing Citrix Presentation Server and the farm has 50 servers, set the processes value to at least 150 in the Init.ora file on the Oracle server. Consult the Oracle documentation for more information.
- If you are running Oracle in Multi-Threaded Server mode, verify that the following parameters in the Init.ora file are greater than or equal to the values shown below. If you are running multiple farms on the same Oracle database, include all servers running Citrix Presentation Server for the calculations listed below. Round up for fractional values.

  `shared_servers = Number of servers / 10`

  `max_shared_servers = Number of servers / 5`

  Where *Number of servers* is the total number of servers running Citrix Presentation Server.
- Citrix recommends online backups using Archivelog mode. Archivelog mode reduces the recovery time of an unresponsive database.

Note If you are using the same Oracle database for multiple server farms, Citrix recommends that you create a unique tablespace with its own user name and password for added security for each farm. Do not use the default system account within Oracle.

Migrating to Oracle

Migration of a farm data store to an Oracle database is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 322.

Original platform	Target platform
Microsoft Access	Oracle 9.2.0.1
SQL Server 2005 Express Edition	Oracle 9.2.0.1
IBM DB2 version 8.2	Oracle 9.2.0.1
SQL Server 2000 with SP 3a	Oracle 9.2.0.1
SQL Server 2005	Oracle 9.2.0.1
Microsoft Access	Oracle 10.2.0.1.0
SQL Server 2005 Express Edition	Oracle 10.2.0.1.0
IBM DB2 version 8.2	Oracle 10.2.0.1.0
SQL Server 2000 with SP 3a	Oracle 10.2.0.1.0
SQL Server 2005	Oracle 10.2.0.1.0

Note If you migrate from an Access database to an Oracle 8.1.7 database, the Citrix IMA Service fails to start because the Oracle 8.1.7.0 driver alters the logon authentication method. To avoid this problem, disable the Oracle NT Security feature in the Oracle Advanced Security settings before migrating an Access database to Oracle 8.1.7.

Failover

With Oracle, you can maintain a standby database for quick disaster recovery. A standby database maintains a copy of the production database in a permanent state of recovery.

Citrix recommends the use of standby databases. See the Oracle documentation for instructions about setting up a standby database.

Distributed Databases

Citrix Presentation Server supports distributed databases. Distributed databases are useful when too many read requests to the data store create a processing bottleneck. Oracle uses replication to create the distributed database environment. Important items concerning distributed databases are listed below.

- To reduce the load on a single database server, install read/write replicas and distribute the farm servers evenly across the master and replicas.
- Citrix Presentation Server requires data coherency across multiple databases. Therefore, a two-phase commit algorithm is required for writes to the database.

Using Oracle as a distributed database solution requires the following:

- All participating databases must be running Oracle
- All participating databases must be running in Multi-Threaded Server/Shared mode (rather than Dedicated mode)
- All clients (servers running Citrix Presentation Server that connect directly to the Oracle database) must be SQL*Net Version 2 or Net8
- Install the farm data store database first on the master site, and then configure replication at the sites being used for database replication snapshots
- Replicate all objects contained in the data store user's schema (tables, indexes, and stored procedures)

Note If the performance at the replicated database site is significantly slower, verify that all the indexes for the user's schema are successfully replicated.

When configuring Oracle for a two-phase commit, Citrix recommends the following:

- Use synchronous snapshots that can be updated with a single master site. Citrix Presentation Server does not work with read-only snapshots. Some functions need write access to the data store.
- Use the Oracle Fast Refresh feature where possible (this requires snapshot logs).

- Do not configure conflict resolution when setting up the replication environment.
- Set the replication link interval to be as frequent as the network environment allows (Citrix recommends one minute). With Oracle replication, if no changes are made, data is not sent over the link.
- If Oracle is configured in Multi-Threaded Server mode and remote reads or writes are initiated from the remote site, these can block local reads or writes. This is because all connections share a set of worker threads called Multi-Threaded Servers. To remedy this, increase the value of the Max_Mts_Servers parameter in the Init.ora file.

Using Oracle Real Application Clusters

Oracle Real Application Clusters can provide exceptional performance gains in extremely large farms where having only a single front-end database server creates a performance bottleneck.

An Oracle Real Application Cluster configuration provides a load-balanced environment where multiple front-end Oracle servers share the same disk subsystem and database tables. Oracle Real Application Clusters distribute load evenly across all participating servers and, in the event of a server failure, automatically routes connections to the surviving nodes.

Note Because of the hardware configuration required for Oracle Real Application Clusters, this product was not tested in the Citrix test labs. Oracle Real Application Clusters are designed to allow multiple database servers to access the same back-end database. In theory, this provides good scalability in centrally located farms with hundreds of servers.

IBM DB2

Citrix Presentation Server supports the following versions of IBM DB2 for the farm's data store.

- IBM DB2 Enterprise Version 8.2 for Windows Server 2003 with Service Pack 1
- IBM DB2 Universal Database Version 8.2 for Windows Server 2003 x64

Install the IBM DB2 Run-Time Client on each server accessing the database server. If you have multiple farms, create a separate database/tablespace for each farm data store.

Important Restart the system after you install the IBM DB2 Run-Time client and before you install Citrix Presentation Server. See the DB2 documentation for more information.

Minimum Requirements

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

The server hosting the DB2 database should meet the following minimum requirements:

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- Citrix labs tested the IBM DB2 environment with the following permissions assigned to the user: connect database, create tables, register functions to execute to database manager's process, and create schemas implicitly.
- If you create a data source name (DSN) for use with an unattended installation of IBM DB2, Citrix recommends that you create the DSN using the Microsoft ODBC Data Source Administration screen. Doing so ensures that the DSN is populated according to server requirements for proper connectivity to the DB2 database or tablespace.
- Give the DB2 user account that is used for the farm the following permissions:
    - Connect database
    - Create tables
    - Register functions to execute to database manager's process
    - Create schemas implicitly

    System administrator (DB2Admin) account permissions are not needed for data store access.
- Consult DB2 documentation for tuning database performance.

Distributed Databases

Citrix Presentation Server supports distributed databases. Distributed databases are useful when too many read requests to the data store create a processing bottleneck. You can use a distributed database to distribute the load of read requests. IBM DB2 uses replication to create the distributed database environment.

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

Migrating to IBM DB2

Migration of a farm data store to an IBM DB2 database is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 322.

Original platform	Target platform
Microsoft Access	IBM DB2 version 8.2
SQL Server 2005 Express Edition	IBM DB2 version 8.2
Oracle 9.2.0.1	IBM DB2 version 8.2
Oracle 10.2.0.1.0	IBM DB2 version 8.2
SQL Server 2000 with SP 3a	IBM DB2 version 8.2
SQL Server 2005	IBM DB2 version 8.2

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

Index

A

Access
    migrating to SQL Server Express 401
Access Management Console 98
    choosing when to use 99
    creating reports 110
    customizing displays 105
    discovery 104
    installing 56, 58
    isolation environments 107
    managing applications 106
    managing hotfixes 111
    managing servers 106
    managing sessions 106
    managing zones 106
    monitoring server performance 109
    My Views 105
    snap-ins 103
    troubleshooting alerts 110
    user interface 102
    users and accounts 100
    using Web Interface 111
accessing
    resources, users 20
Acrcfg command 285
Active Directory 22
    deploying clients with 88
    forests 23
    global groups 23
    universal groups 23
    user authentication 23
    user permissions 25
administrative installations 370
Aierun command 288
Aiesetup command 289
alerts, troubleshooting 110
Altaddr command 292
anonymous users 118
answer file 368
App command 294
application publishing wizard 116
applications, published
    configuring access to 111
    installing into an isolation environment 148
    managing 106
    uninstalling from isolation environment 151
    using isolation environments 107
Apputil command 296
audio
    enabling for published applications 192
    mapping 180
Auditlog command 300
auto-created printers 257, 275
Automatic Client Reconnection 182

B

backing up
    IMA encryption keys 226

C

Change Client command 302
changing farms
    IMA encryption 225
Chfarm command 305
Citrix administrators
    assigning during installation 64
    creating and modifying 99, 107
    local 225
    logging the actions of 229
Citrix licensing
    upgrade requirement 78
Citrix SSL Relay 98, 206
    default TCP port 213

Citrix XML Service 31–32, 311, 383
changing the port number for 283, 311
configuring 70
default TCP Port 213
DNS address resolution 216
health monitoring test 239
setting the port for 32
client
security (overview) 201
client device mapping 178
client encryption
increasing 204
client IP address 139
Client Packager 88
client printers 256, 258, 260
clients
enabling SSL 203
client-server connections
encrypting 201
Cltprint command 308
COM port mapping 179
configuration
post-installation instructions 85
Configuration Logging
Configuration Logging database 230
database permissions 232
reports 236
configuring
anonymous user accounts 119
audio settings 191
Citrix administrator accounts 20
Citrix SSL Relay 206
Citrix XML Service 70
client device mapping 178
client reconnection settings 183
constrained delegation 196
farms after installation 85
ICA browsing 28
isolation environments 146
shadowing 69
SNMP service 197
connections
audio mapping 180
COM port mapping 179
controlling 167
logging control events 170
constrained delegation
configuring 196
content publishing 122
content redirection 120, 122
configuring 122
from client to server 120, 122
from server to client 123
counters, performance 243
CPSSDK 15
CPU priority for applications 153
CPU utilization management 245
creating a license server 55
CTXKEYTOOL
location of on CD 221
overview 221
Ctxkeytool command 309
Ctxxmlss command 311
customizing Citrix Presentation Server 15

D

Dashboard snap-in 103
data store
choosing a database 34
connecting to 36, 76
database requirements 395
Dsmaint command 199
migrating from Access 401
migrating from MSDE 401
replicating 40
securing 198
suggested hardware configurations 37
system sizing 37
using a RAID environment 40
using IBM DB2 200, 415
using Microsoft Access 199, 397
using Oracle 200, 410
using SQL Server 199, 405
using SQL Server Express 199, 398
databases
migrating to SQL Server Express 79
MSDE migration 79
delegated administration 108, 235, 343
deploying
farms 85
servers after installation 85
Diagnostic Facility snap-in 103
disabling
IMA encryption 227
discovery, running 104
displaying
STA statistics 212

distributed databases
with IBM DB2 417
with Oracle 414
with SQL Server 409
DLL optimization 247
DNS address resolution 31
Document Center 13, 54, 57, 73
domain trust relationships 20
drive letters, changing 42
drive mapping 42
Driveremap command 49, 312
Driveremap64 command 316
Dscheck command 320
Dsmaint command 199, 322

E

Enablelb command 327
enabling
Windows MUI Support 51
encryption
increasing after publishing 204
explicit users 119
external IP addresses 292

F

failover
on Oracle 413
on SQL Server 408
farms
changing, IMA encryption 225
configuring after installation 85
file type association 120
Flash animations 188

G

glossary 13

H

hardware requirements 19
Health Monitoring & Recovery 238
heavyweight compression 185
Hotfix Management snap-in 104
hotfixes, managing 111

I

IBM DB2
migrating to 417
requirements 416
securing 200
using DB2 for the data store 62
with distributed databases 417
ICA browsing 26
DNS address resolution 31
TCP/IP network protocol 30
TCP/IP+HTTP network protocol 29
ICA protocol
increasing level of encryption 204
ICA protocol encryption 202
overview 201
ICA sessions 27
browsing configuration 28
controlling logons 171
disconnecting sessions 172
managing 106
monitoring 172, 243
performance monitoring 243
resetting 173
sending messages to users 173
Session ID 172
session reliability 180
shadowing 98, 174
Icaport command 328
IMA encryption 219, 230, 283, 309, 385
backing up keys 226
changing farms 225
configuring during upgrades 79
disabling 227
enabling 65
enabling after installation 222
local administrators 225
location of CTXKEYTOOL 222
network folders 224
overview 219
planning before installation 41
reenabling 227
retrieving lost keys 226
storing utility locally 222
IMA encryption utility
overview 221
running locally 222
image download optimization 188
Imaport command 329
increasing
encryption for published resources 204

installation
Access Management Console 56, 58
administrative installations 370
assigning Citrix administrators 64
creating a log file 372
creating answer files for unattended installation 368
enabling MUI support 51
instructions for after 85
licensing settings 76
pass-through client 61
Presentation Server components 59
shadowing restrictions 69
unattended 365, 370
unattended, sample transforms 373
uninstalling Citrix Presentation Server 94
uninstalling Citrix Presentation Server, files remaining after 96
Web Interface 56, 58
Installation Checklist 17, 54
Installation Manager 38, 60, 98, 112, 148, 296, 346, 351, 366
IP addresses
of client made available to sessions 139
ranges for server sessions 140
IP addresses and loopback
monitoring at server level 143
IP addressing 292
isolation environments 107
Aierun command 288
Aiesetup command 289
associating with applications 147
configuring 146
creating 145
deleting 152
rules 149

J

join_indirect.mst 375

K

Kerberos logon 215
keys
retrieving lost 226

L

latency reduction 98
License Management Console 98, 214
license server 81
default TCP port for 214
upgrade requirement 78
licensing 48, 54–55, 68, 81, 96, 103, 214, 252
settings during Setup (join) 76
upgrade requirement 78
Licensing snap-in 103
load balancing 24, 60, 238, 283, 327
Load Manager 24, 27, 38, 60, 98, 112, 238, 347
local administrators
configuring 225
local host cache 250
localdb_access_create.mst 374
logons
controlling look and feel 164
enabling and disabling 163
Kerberos 215
NetWare logon scripts 158
reporting 300
with smart cards 219
loopback addresses 142

M

Management Console 60
management consoles, choosing which one to use 99
management tools 97
messages, sending to users 173
Microsoft Access
as data store host 199
migrating to SQL Server Express 401
requirements 397
securing 199
using Access for the data store 63
Microsoft Management Console (MMC) 56, 98, 100, 166
certificate snap-in 208
MigratetoSqlExpress command 330
migrating
Access to SQL Server Express 401
data store from MSDE 79
MSDE 401
SQL Server 2005 Express 401
to SQL Server Express 401
migrating server farms 84
migration
data store migration tools 403
monitoring ICA sessions 172, 243
monitoring server performance 109
moving a server to a different farm 305
MPSSDK 15

MSDE
migrating 401
migrating data store 79
Msiexec 369
MSXML
prerequisite for SQL Server Express migration 403
MUI support
enabling during Setup 51
multimedia, optimizing performance 187
My Knowledge snap-in 104
My Views, in Access Management Console 105

N

network firewalls 30, 213
network folders
IMA encryption keys 224
network printers 256–257, 270
new features 12
Novell Directory Services
BUILTIN group 160
NetWare drive mapping assignments 158
supporting 155
terms 155
NTFS partitions 197

O

Oracle
as logging database 230
authentication and security 413
distributed databases 414
failover 413
migrating to 413
Real Application Clusters 415
requirements 410
securing 200
using Oracle for the data store 62

P

pass-through client
installing 61
transform properties for 392
PDA synchronization, enabling 160
performance counters 243, 355
Citrix Presentation Server 357
CPU utilization 356
ICA session 359
IMA networking 356
STA 362
performance monitoring 243, 355
permissions, Access Management Console 100
policies
applying with filters 131
configuring rules 127
creating 126
encryption 205
printing 259
rules, bandwidth 128
rules, client devices 128
rules, printing 129
rules, security 130
rules, user workspace 130
searching for 134
Secure ICA 205
using multiple 132
ports used by Citrix Presentation Server 213
Pre-installation update bulletin 17
Presentation Server Clients
deployment methods 87
logging activity 300
shadowing 98
Presentation Server Console 98
choosing when to use 99
components for printing configuration 278
configuring policy rules 127
creating isolation environments 145
creating policies 126
enabling PDA synchronization 160
enabling TWAIN redirection 161
installing 57, 73
securing 197
uses for 112
Presentation Server snap-in 103
printer drivers, managing 273
printing
auto-created printers 257, 275
bandwidth consumption 279
client printers 256, 258, 260
installed printers 280
managing drivers 273
network printers 256–257, 270
policies 259
Printers tab 280
replicating printer drivers 275, 277
Session Printers policy 129, 270–271
Universal Printing 258, 273
privileges, modifying 107
Program Neighborhood Agent
encryption settings 201

published applications
encryption for 201
SSL/TLS encryption 201
publishing
enabling SSL/TLS protocols 203
publishing resources
application publishing wizard 116
associating with file types 120
content publishing locations 118
limiting application instances 168
passing parameters to published applications 121
publishing content 120
redirecting launching 122
types 115
using policies to configure access to 125

Q

Query command 331
Query Farm 331
Query Process 333
Query Server 334
Query Session 336
Query Termserver 337
Query User 338

R

RAID environments 40
recreating
lost keys 226
reenabling
IMA encryption 227
Remote Desktop Connection software 93
remote desktop users group 73
Report Center snap-in 103
reports, creating 110
requirements
data store database 395
hardware 19
IBM DB2 416
Microsoft Access 397
Oracle 410
smart cards 218
SQL Server 405
SQL Server Express 400
system software 18
Reset command 173
resetting ICA sessions 173
Resource Manager 38, 60, 81, 96, 98, 110, 112, 305, 345, 350
retrieving
lost IMA encryption keys 226

S

Secure Gateway 211
Secure ICA
increasing level of encryption 204
overview 201
policies 205
Secure Ticket Authority (STA) 212, 362
security
policies 205
sending messages to users 173
server
enabling SSL 203
security (overview) 201
server clocks
synchronizing 196
server farms
creating 51
creating or joining 62, 74–75
removing servers from 94
upgrading or migrating 77
server location 28
servers
synchronizing clocks 196
Session ID 172
Session Printers policy 129, 270–271
session reliability 27, 180
default TCP port for 214
sessions
see ICA sessions
Setup
enabling MUI support 51
planning for IMA encryption 41
shadowing 69, 98, 130, 174, 383
from the Access Management Console 174
Shadow Taskbar 98
user-to-user shadowing 175
smart cards
requirements 218
using with Presentation Server 217
SmoothRoaming 257

snap-ins
Access Management Console 103
Dashboard 103
Diagnostic Facility 103
Hotfix Management 104
Licensing 103
My Knowledge 104
Presentation Server 103
Report Center 103
Web Interface 104
SNMP service, configuring 197
software requirements 18
specifying
licensing settings during Setup 76
SpeedScreen
Browser Acceleration 186
Flash Acceleration 188
Heavyweight Compression 190
Image Acceleration 188
Latency Reduction Manager 98
Multimedia Acceleration 187
Progressive Display 190
SQL Server
as logging database 230
creating data source connection during setup 407
failover 408
migrating to 410
requirements 405
securing 199
server configuration 406
using SQL for the data store 62
SQL Server Express
and the Chfarm command 306
MigratetoSqlExpress command 330
migrating from Access 401
migrating from MSDE 79
migrating to 401
requirements 400
securing 199
using SQL Server Express for the data store 63
SSL
enabling for client-server 203
SSL/TLS encryption
published applications 201
SSL/TLS protocols
enabling for applications 203
STA
displaying statistics 212
storing
IMA encryption keys on the network 224
synchronizing
server clocks 196

T

TCP ports 213
thirdpartydb_create_direct.mst 376
thirdpartydb_join_direct.mst 377
transforms 367
sample transforms 374–377
Transport Layer Security (TLS) 206
trust query cycle 21
trust relationships 20
trust-based routing 21
trusted server configuration 198
TWAIN redirection, enabling 161
Twconfig command 341

U

UDP broadcasts 30
unattended installations 365
administrative installation 370
creating answer file 368
of the Access Management Console 370
sample transforms 373
uninstalling Citrix Presentation Server 94
files remaining after 96
Universal Printing 258, 273
Upgrading
IMA encryption 79
upgrading server farms 81
user authentication
configured for Workspace Control 214
Kerberos 215
with Active Directory 23
with smart cards 217
users and accounts, Access Management Console 100
user-to-user shadowing 175

V

virtual IP addresses 135–140
virtual loopback 142
virtual memory usage 247

W

Web browsers, optimizing performance 186

Web Interface
and the Citrix XML Service 32
configuring application access with 111
encryption settings 201
installing 56, 58
Web Interface snap-in 104
Windows Installer
and client deployment 89
creating a log file 372
installation log file 372
Msiexec command 369
packages, deploying 366
transforms 367
Windows MUI
enabling Presentation Server support 51
WMI Provider 61
Workspace Control 164, 214, 257

Z

zones, managing 106