# Citrix XenApp Administrator's Guide

**Citrix XenApp™ 5.0 for Microsoft® Windows Server® 2008**

**Copyright and Trademark Notice**

Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement. A printable copy of the End User License Agreement is included with the installation media.

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.

© 2001-2008 Citrix Systems, Inc. All rights reserved.

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

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

**Trademark Acknowledgements**

Adobe, Acrobat, Flash, and PostScript 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/).

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

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.

Microsoft, MS, Windows, Windows Media Player, Windows Server, Windows Vista, Windows NT, Win32, Outlook, Outlook Express, Internet Explorer, ActiveX, Active Directory, Access, ClearType, Excel, SQL Server, SQL Server Express Edition, MS Proxy Server, DirectShow, and DirectX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or 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.

IBM, AIX, DB2, Tivoli, NetView, PowerPC, and WebSphere are registered trademarks or trademarks of IBM Corporation in the U.S. and other countries.

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.

FLEXnet Operations and FLEXnet Publisher are trademarks and/or registered trademarks of Acresso Software Inc. and/or InstallShield Co. Inc.

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

Document Code: August 21, 2008 (jp)

# Contents


**1 Welcome . . . . . 13**

New Names for Citrix Presentation Server Components . . . . . 14
Finding Documentation . . . . . 14
Documentation Conventions . . . . . 15
Getting Support and Training . . . . . 15

**2 Management Consoles and Other Tools . . . . . 17**

Access Management Console Overview . . . . . 17
XenApp Advanced Configuration Overview . . . . . 18
License Management Console Overview . . . . . 18
Citrix SSL Relay Configuration Tool Overview . . . . . 18
Shadow Taskbar Overview . . . . . 18
SpeedScreen Latency Reduction Manager Overview . . . . . 19
Choosing the Console or Tool to Use . . . . . 19
To start the Access Management Console . . . . . 20
Displaying Items in the Access Management Console . . . . . 20
To use the discovery process to specify more than one server farm for console management . . . . . 21
To run the discovery process for more than one product or component . . . . . 21
To run the discovery process for a single product or component . . . . . 21
The Access Management Console User Interface . . . . . 21

Performing Tasks with the Access Management Console . . . . . 24
Assigning Farm Administrator Credentials . . . . . 24
Customizing Your Displays Using My Views . . . . . 24
Managing Applications and Servers in Multiple Farms . . . . . 25
To view zones with the Access Management Console . . . . . 25
Managing User Sessions and Server Processes . . . . . 25
Creating Reports with the Access Management Console . . . . . 26
Configuring Application Access with Access Management Console . . . . . 26
Creating Trace Logs with the Access Management Console . . . . . 26
Viewing Citrix Hotfix Information . . . . . 27
Conserving Bandwidth for Remote Monitoring when Using the Access Management Console . . . . . 27
Enabling Citrix Administrators to Manage Farms Remotely . . . . . 27
To grant DCOM Remote Launch permissions to administrators . . . . . 27
Using Citrix XenApp Advanced Configuration . . . . . 28
Conserving Bandwidth for Remote Monitoring when Using Advanced Configuration . 29
To configure the Advanced Configuration tool for screen reader accessibility . . . . . 29

**3 Managing Citrix Administrator Accounts . . . . . 31**

Planning Administrator Accounts . . . . . 31
Types of Citrix Administrator Accounts . . . . . 32
Managing Citrix Administrator Accounts . . . . . 33
To create new Citrix administrator accounts . . . . . 33
To change Citrix administrator properties . . . . . 33
Disabling and Removing Administrators . . . . . 34
Delegating Tasks to Custom Administrators . . . . . 35
To delegate tasks to existing custom administrators . . . . . 35
Assigning Folder Permissions to Administrators . . . . . 36
Assigning Tasks to Administrators . . . . . 36

**4 Delivering Resources to Users . . . . . 39**

Making Resources Available to Users . . . . . 40
Installing Applications for Multiple Users . . . . . 40
Publishing in Domains with Thousands of Objects . . . . . 41
To publish a resource using the Publish Application wizard . . . . . 41

Managing Delivery Options for Published Resources . . . . . 43
To select a resource type and delivery method . . . . . 43
To configure locations of applications for publishing . . . . . 45
To configure locations of published content . . . . . 47
To configure locations of servers for published resources . . . . . 47
To configure user access to applications . . . . . 48
To configure shortcuts for client devices . . . . . 51
To configure access controlled by the Access Gateway . . . . . 52
To configure content redirection . . . . . 52
To configure application limits . . . . . 59
To configure application importance . . . . . 60
To configure audio and encryption options for published applications . . . . . 61
To configure application appearance . . . . . 63
To reduce user privileges for a streamed application . . . . . 63
Managing Published Applications . . . . . 64
To rename a published application . . . . . 64
To disable or enable a published application . . . . . 65
To delete a published application . . . . . 65
To move a published application to another folder . . . . . 66
To duplicate published application settings . . . . . 66
To export published application settings to a file . . . . . 66
To export multiple published application settings to a file simultaneously . . . . . 68
To import published application settings from a file . . . . . 68
Making Virtual IP Addresses Available to Applications . . . . . 69
How Virtual IP Addressing Works . . . . . 70
To determine whether an application needs to use virtual IP addresses . . . . . 71
To make virtual IP addresses available to applications running in sessions . . . . . 72
To assign virtual IP address ranges to servers . . . . . 73
To enable application processes to use virtual IP addresses or virtual loopback . . . . . 74
To supply client IP addresses to published applications on a server . . . . . 75
To make a virtual loopback address available to applications running in sessions . . . . . 77
To enable or disable virtual loopback for a farm . . . . . 77
To configure virtual IP addresses and virtual loopback on an individual server . . . . . 78

**5 Creating Policies . . . . . 81**

An Introduction to XenApp Policies . . . . . 81
Configuring XenApp Policies . . . . . 82
Creating XenApp Policies . . . . . 82
Configuring Policy Rules . . . . . 83
Applying Policies . . . . . 84

**6 Managing Policies . . . . . 89**

Configuring Initial Policy Rules . . . . . 89
Configuring Client Device Settings . . . . . 90
Setting Printing Policy Rules . . . . . 90
Changing Settings Based on User Location . . . . . 90
Configuring Policies and Filters for Web Access . . . . . 91
Using Multiple Policies . . . . . 93
Using Citrix policies with Active Directory . . . . . 94
Prioritizing Policies and Creating Exceptions . . . . . 95
Determining Which Policies Apply to a Connection . . . . . 97
To discover which policies apply to a connection . . . . . 98
Resolving Search Results that Partially Match Criteria . . . . . 98
Troubleshooting Policies with Conflicting Rules . . . . . 99
To delete a policy . . . . . 100
To disable a policy . . . . . 100
To reenable a policy . . . . . 101
Enabling Scanners and Other TWAIN Devices . . . . . 101
To enable the configuration of TWAIN redirection . . . . . 102

**7 Managing Session Environments and Connections . . . . . 105**

Session Environments and Connections . . . . . 105
Defining User Environments in XenApp . . . . . 106
Controlling the Appearance of User Logons . . . . . 107
Controlling Access to Devices and Ports . . . . . 108
Displaying Local Special Folders in Sessions . . . . . 110
Configuring Audio for User Sessions . . . . . 114
Ensuring Session Continuity for Mobile Workers . . . . . 119
Maintaining Session Activity . . . . . 120
Understanding Session Basics . . . . . 126
Managing and Monitoring XenApp Sessions . . . . . 127
Monitoring Session Status . . . . . 127
Using Session Shadowing to View a User Session . . . . . 130
Managing User Sessions . . . . . 136
Sending Messages to Users . . . . . 139
Controlling Client Connections in XenApp . . . . . 140
Preventing Specific Client Connection Types . . . . . 141
Specifying Connection Limits . . . . . 142
Controlling Connections with Terminal Services Configuration . . . . . 146
Preventing User Connections during Farm Maintenance . . . . . 148

Optimizing User Sessions for XenApp . . . . . 148
Optimizing Web Page and Email Responsiveness . . . . . 150
Optimizing Audio and Video Playback . . . . . 153
Optimizing Flash Animations . . . . . 157
Optimizing Throughput of Image Files . . . . . 159
Optimizing Display of Image Files . . . . . 160
Optimizing Keyboard and Mouse Responsiveness . . . . . 161
Configuring ICA Display Settings . . . . . 168
Configuring ICA Browser Settings . . . . . 169

**8 Securing Server Farms . . . . . 171**

Support for Microsoft Security Templates . . . . . 171
Securing Access to Your Servers . . . . . 171
Securing the Data Store . . . . . 172
Securing Network Communications . . . . . 174
Securing Client-Server Communications . . . . . 175
Configuring SSL/TLS Between Servers and Clients . . . . . 179
Using the Secure Gateway . . . . . 186
Using the Secure Ticket Authority . . . . . 187
Configuring Network Firewalls . . . . . 188
Configuring User Authentication . . . . . 190
Configuring Authentication for Workspace Control . . . . . 190
Configuring Kerberos Logon . . . . . 191
Using Smart Cards with Citrix XenApp . . . . . 193
Logging Administrative Changes to a XenApp Farm . . . . . 195
Enabling Configuration Logging . . . . . 196
Working with Configuration Logs . . . . . 203
Encrypting Sensitive Configuration Logging Data . . . . . 205
Using the IMA Encryption Utility . . . . . 207
Enabling IMA Encryption After Installation . . . . . 207
Storing the Key on a Shared Location . . . . . 209
Changing Farms . . . . . 209
Other IMA Encryption Features . . . . . 210
XenApp Service Account Privileges . . . . . 211

**9 Understanding XenApp Printing . . . . . 217**

Introduction to Windows Printing Concepts . . . . . 218
Local and Remote Print Job Spooling . . . . . 220

XenApp Printing Concepts . . . . . 222
Overview of Client and Network Printing Pathways . . . . . 223
Provisioning Printers for Sessions . . . . . 227
Device or Session-Based Print Settings . . . . . 234
Setting Default Printers . . . . . 238
Printing and Mobile Workers . . . . . 238
Optimizing Printing Performance by Routing . . . . . 239
Managing Printer Drivers . . . . . 240
Planning Your Printing Configuration . . . . . 245
Default Printing Behavior . . . . . 246
Printing Policy Configuration . . . . . 247
Printing Security . . . . . 248
Purchasing Printing Hardware . . . . . 249

**10 Configuring and Maintaining XenApp Printing . . . . . 251**

Configuring Printing . . . . . 251
Configuring Printer Autocreation Settings . . . . . 252
Configuring Citrix Universal Printing . . . . . 253
Configuring Auto-Creation for DOS and Windows CE Clients . . . . . 255
Configuring Network Printers for Users . . . . . 257
Configuring Printers for Mobile Workers . . . . . 263
Changing Network Print Job Routing . . . . . 264
Providing Tools for User Provisioning . . . . . 265
Controlling Users' Printing Preferences . . . . . 266
To store users' printer properties . . . . . 266
To synchronize printer properties set out of sessions . . . . . 267
Controlling Printer Driver Automatic Installation . . . . . 268
Configuring Universal Printer Drivers on Farm Servers . . . . . 270
Mapping Client Printer Drivers . . . . . 272
Maintaining Printing . . . . . 274
Increasing Printing Speed and Session Performance . . . . . 274
Updating Network Print Server Information . . . . . 277
Replicating Printer Drivers Across a Farm . . . . . 278
Displaying Printers . . . . . 281
Displaying Printers Using the Network Printing Pathway . . . . . 282
Displaying Printers Using the Client Printing Pathway . . . . . 284
Displaying Drivers . . . . . 285
To display a list of the drivers on a server . . . . . 285
To display a list of the printer drivers available from a server in your farm . . . . . 285

**11 Maintaining Server Farms . . . . . 287**

Displaying and Organizing Your Farm . . . . . 288
To view farm information . . . . . 288
To view server information . . . . . 288
Organizing Your Farm Display in the Console . . . . . 289
To configure general farm properties . . . . . 291
To search for objects in your farm . . . . . 292
Connecting to a Server . . . . . 293
Connecting to a Server's Console . . . . . 293
Connecting to a Server's Published Desktop . . . . . 294
Connecting Directly to a Server's Desktop . . . . . 295
Limiting Connections . . . . . 296
Controlling Server Logons . . . . . 297
Enabling Content Redirection and Remote Console Connections . . . . . 297
Configuring Auto Client Reconnect . . . . . 298
Restarting Servers at Scheduled Times . . . . . 300
To define when multiple servers restart . . . . . 300
To define when a single server restarts . . . . . 300
To stop restarts for a server . . . . . 301
To repair a XenApp installation . . . . . 301
Changing XenApp Farm Membership . . . . . 301
To move a XenApp server to a new server farm using SQL Server Express . . . . . 302
Removing and Reinstalling XenApp . . . . . 302
To uninstall XenApp . . . . . 304
To force the uninstallation of XenApp . . . . . 305
To remove a server from the farm . . . . . 305
To rename a XenApp server . . . . . 306
Monitoring Server Performance with Health Monitoring & Recovery . . . . . 307
Enabling and Disabling Health Monitoring & Recovery . . . . . 310
Modifying Health Monitoring & Recovery Test Settings . . . . . 310
Adding Health Monitoring & Recovery Tests . . . . . 312
Developing Custom Health Monitoring & Recovery Tests . . . . . 313
Getting Health Monitoring & Recovery Alerts . . . . . 314
Using Citrix Performance Monitoring Counters . . . . . 314
To access ICA performance counters . . . . . 314

Enabling SNMP Monitoring . . . . . 315
Installing and Configuring the Microsoft SNMP Service . . . . . 316
SNMP Security Considerations . . . . . 316
Enabling the Citrix SNMP Agent and Configuring Trap Settings . . . . . 317
Troubleshooting SNMP Monitoring . . . . . 319
Monitoring Traps from SNMP Network Management Products . . . . . 319
Using the Citrix Management Information Base . . . . . 320
Optimizing Server Performance . . . . . 320
Assigning Load Evaluators to Servers . . . . . 320
Assigning a Load Evaluator to a Published Application . . . . . 321
Using Preferential Load Balancing . . . . . 322
Using CPU Utilization Management . . . . . 325
Managing Virtual Memory Usage . . . . . 328
Optimizing Simultaneous Logon Performance . . . . . 331
Managing Farm Infrastructure . . . . . 332
Maintaining the Local Host Cache . . . . . 332
Data Collectors and Elections . . . . . 335
Enhancing the Performance of a Remote Group of Servers . . . . . 337
Updating Citrix License Server Settings . . . . . 340
To specify a default license server for a farm . . . . . 341
To specify a license server for individual servers . . . . . 342
Setting the Product Edition . . . . . 342
To set the product edition . . . . . 343
Setting the Citrix XML Service Port . . . . . 343
To configure the Citrix XML Service port for a server . . . . . 344
To manually change the XML Service port to use a port different from IIS after installation . . . . . 345
To manually configure Citrix XML Service to share the TCP port with IIS . . . . . 346

**12 Citrix XenApp Commands Reference . . . . . 347**

ACRCFG . . . . . 348
ALTADDR . . . . . 350
APP . . . . . 351
AUDITLOG . . . . . 353
CHANGE CLIENT . . . . . 355
CHFARM . . . . . 358
To move a server to a new server farm using SQL Server Express . . . . . 361
CTXKEYTOOL . . . . . 362
CTXXMLSS . . . . . 363
DSCHECK . . . . . 364

DSMAINT . . . . . 365
ENABLELB . . . . . 370
ICAPORT . . . . . 371
IMAPORT . . . . . 371
MIGRATETOSQLEXPRESS . . . . . 373
QUERY . . . . . 373
Query Farm . . . . . 374
Query Process . . . . . 376
Query Session . . . . . 377
Query Termserver . . . . . 378
Query User . . . . . 379
TWCONFIG . . . . . 380

**13 Delegated Administration Tasks Reference . . . . . 383**

Farm Folder Tasks . . . . . 383
Administrators Folder Tasks . . . . . 384
Applications Folder Tasks . . . . . 384
Load Evaluator Folder Tasks . . . . . 385
Policies Folder Tasks . . . . . 385
Printer Management Folder Tasks . . . . . 385
Servers Folder Tasks . . . . . 386

**14 Performance Counters Reference . . . . . 387**

Citrix CPU Utilization Mgmt User Counters . . . . . 387
Citrix IMA Networking Counters . . . . . 388
Citrix Licensing . . . . . 388
Citrix MetaFrame Presentation Server Counters . . . . . 389
ICA Session Counters . . . . . 391
Secure Ticket Authority Counters . . . . . 394

**15 Policy Rules Reference . . . . . 395**

Policy Rules: Quick Reference Table . . . . . 395

Policy Rule Definitions . . . . . 399
Bandwidth Folder . . . . . 399
Client Devices Folder . . . . . 405
Printing Folder . . . . . 411
Client Printers Folder . . . . . 411
Drivers Folder . . . . . 413
User Workspace Folder . . . . . 413
Security Folder . . . . . 420
Service Level Folder . . . . . 421

CHAPTER 1

# Welcome

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

- Using the management console and other tools is described in Chapter 2
- Managing Citrix administrator accounts is described in Chapter 3
- Publishing resources—applications, content, and server desktops—is described in Chapters 4
- Creating and managing XenApp policies are described in Chapters 5 and 6
- Managing user sessions is described in Chapter 7
- Securing your XenApp environment is described in Chapter 8
- Making printing resources available to your users is described in Chapters 9 and 10
- Maintaining your server farms is described in Chapter 11
- Reference information concerning Citrix XenApp commands, delegated administration tasks, performance monitoring counters, and policy rules is provided in Chapters 12 through 15

For planning and installation information, see the *Citrix XenApp Installation Guide*.

---

**Important:** Before you install Citrix XenApp, review the *Readme for Citrix XenApp* document.

---

# New Names for Citrix Presentation Server Components

*Citrix XenApp* is the new name for Citrix Presentation Server. The following clients and components have been updated to reflect that product name.

- *Citrix XenApp Advanced Configuration* is the new name for the Presentation Server Console
- *Citrix XenApp Plugin for Hosted Apps* is the new name for the plugin for server-side virtualization (formerly named Citrix Presentation Server Client), which contains the following plugins:
  - Citrix XenApp, formerly named Program Neighborhood Agent
  - Citrix XenApp Web Plugin, formerly named the Web Client
  - Program Neighborhood
- *Citrix XenApp Plugin for Streamed Apps* is the new name for the plugin for client-side virtualization, formerly named the Citrix Streaming Client
- *Citrix XenApp Provider* is the new name for the WMI Provider
- *Citrix XenApp Management Pack* is the new name for the System Center Operations Manager and MOM Management Packs

# Finding Documentation

"Welcome to Citrix XenApp" (Read_Me_First.html), which is included on the installation media, contains links to documents that will help get you started. It also contains links to the most up-to-date product documentation for XenApp and its components, plus related technologies. After installing documentation and help from Autorun, you can access this document by clicking **Start > All Programs > Citrix > XenApp Server > Documentation**.

The Citrix Knowledge Center Web site, http://support.citrix.com, contains links to all product documentation, organized by product. Select the product you want to access and then click the **Documentation** tab from the product information page.

Known issues information is included in the product readme.

See the *Citrix XenApp Comparative Feature Matrix* at http://www.citrix.com/xenapp/comparativematrix for information about which features are supported in the XenApp editions.

To provide feedback about the documentation, click the **Article Feedback** link located on the right side of the product documentation page.

# Documentation Conventions

For consistency, Windows Vista and Windows Server 2008 (64-bit) terminology is used throughout the documentation set; for example, “Documents” rather than “My Documents” and “Computer” rather than “My Computer” are used.

Citrix XenApp documentation uses the following typographic conventions.

| Convention | Meaning |
|---|---|
| **Boldface** | Commands, names of interface items such as text boxes, option buttons, and user input. |
| *Italics* | Placeholders for information you provide. For example, filename means you type the actual name of a file. Italics are also used for new terms and titles of books. |
| `Monospace` | Text displayed in a text file. |
| {braces} | In a command, a series of items, one of which is required. For example, {**yes** \| **no** } means you must type yes or no. Do not type the braces themselves. |
| [ brackets ] | In a command, optional items. For example, [/**ping**] means you can type /**ping** with the command. Do not type the brackets themselves. |
| \| (vertical bar) | In a command, a separator between items in braces or brackets. For example, { **/hold** \| **/release** \| **/delete** } means you must type **/hold** or **/release** or **/delete**. |
| ... (ellipsis) | The previous item(s) in the command can be repeated. For example, /route:*devicename*[,…] means you can type additional *devicename*s separated by commas. |

# Getting Support and Training

Citrix provides an online user forum for technical support. This forum can be accessed at http://support.citrix.com/xenappforum/. The Web site includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

The Citrix Knowledge Center (http://support.citrix.com) offers a variety of technical support services, tools, and developer resources.

Information about Citrix training is available at http://www.citrix.com/edu/.

# Management Consoles and Other Tools

Citrix provides a comprehensive set of tools for managing servers, farms, published resources, and connections, which includes a management console and a management tool: the Access Management Console and Citrix XenApp Advanced Configuration. This section provides an overview of the features of these consoles and tools and describes how to choose between them. More detailed information is available in the Help for the tools.

You can launch all tools by accessing the Citrix program group on the **Start** menu.

Related topics:

"Choosing the Console or Tool to Use" on page 19

## Access Management Console Overview

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

For Citrix XenApp, you can use the Access Management Console to set up and monitor servers, server farms, published resources, and sessions. Create a variety of reports and configure application access (both through the Web Interface and the Citrix XenApp plugin).

In addition, use the Access Management 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.

Related topics:

"Performing Tasks with the Access Management Console" on page 24

# XenApp Advanced Configuration Overview

Use the XenApp Advanced Configuration tool (formerly named the Presentation Server Console) to connect to any server farm in your deployment and to set up policies and printers. Use the tool to configure and manage your deployment with Load Manager.

Related topics:

"Using Citrix XenApp Advanced Configuration" on page 28

# License Management Console Overview

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

# Citrix SSL Relay Configuration Tool Overview

Use this tool to secure communication between a server running the Web Interface and your farm.

Related topics:

"Securing Server Farms" on page 171

# Shadow Taskbar Overview

Shadowing allows users to view and control other users' sessions remotely. 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.

Related topics:

"Using Session Shadowing to View a User Session" on page 130

# SpeedScreen Latency Reduction Manager Overview

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

Related topics:

“Configuring SpeedScreen Latency Reduction” on page 161

# Choosing the Console or Tool to Use

Managing your XenApp deployment involves working with the:

- Citrix Access Management Console
- Citrix XenApp Advanced Configuration tool

To manage your deployment more flexibly, install the Access Management Console and the Advanced Configuration tool on a computer that is not running XenApp. However, for the best console performance, Citrix recommends running the Access Management Console on a XenApp server.

For more information about the installation requirements of each of the management tools, see the *Installation Checklist for XenApp.*

Tasks you can perform with each are listed in this table.

| **Use the Access Management Console to perform these tasks:** |
|---|
| Assign load evaluators to applications. |
| Create Citrix administrators and modify their privileges. |
| Create reports with Report Center. |
| Configure access to published resources through the Web Interface and Citrix XenApp plugin. |
| Configure and manage applications (including Streamed Applications), servers, and farms. |
| Configure health tests for servers and farms using Health Monitoring & Recovery. Create trace logs to assist Citrix Technical Support with problem analysis. |
| Manage plugin sessions and server processes. |
| Monitor server performance and view zones in multiple farms. |
| Track administrative changes made through the console by setting up Configuration Logging. |
| View hotfix information. |

| Use the Advanced Configuration tool to perform these tasks: |
| --- |
| Create and manage zones in a farm. |
| Create policies for users' connections. |
| Configure and manage printers. |
| Configure, adjust, and monitor server and application loads with Load Manager. |

# To start the Access Management Console

Do not run the Access Management 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.

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

---

**Important:** Interoperability of XenApp 5.0 for Windows Server 2008 with versions prior to Presentation Server 4.5 for Windows Server 2003 is not supported

---

.

# Displaying Items in the Access Management Console

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.

The first time you open the Access Management Console you are automatically prompted to start the discovery process: you are guided through selecting the components you want, configuring the discovery process, and finding the items to manage.

After this, run the discovery process only if you want to configure discovery for a component, or if items were added to or removed from your deployment.

When using discovery to connect to your Citrix XenApp 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.

Configure discovery only for some components. The configuration process can vary among components. The **Configure and run discovery** task appears in the task pane only for configurable components; otherwise, only the **Run discovery task** is available.

### To use the discovery process to specify more than one server farm for console management

1. In the console tree, select **Citrix Resources**.
2. Click **Configure and run discovery**.
3. Specify the name or IP address of at least one server running XenApp in each farm that you want to manage.

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

1. In the console tree, select **Citrix Resources**.
2. Click **Configure and run discovery**.

### To run the discovery process for a single product or component

1. In the console tree, select the product or component.
2. To configure discovery, click **Configure and run discovery**. To run discovery without any configuration, click **Run discovery.**

## The Access Management Console User Interface

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

- The *left 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 use the console as follows:

- Select a node in the left pane, which updates the items and information displayed in the details pane

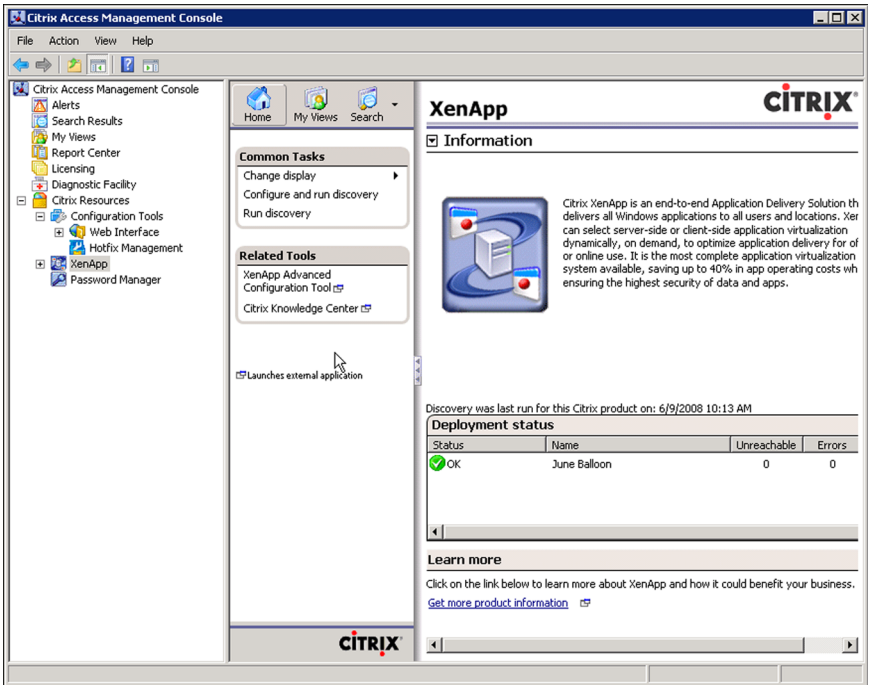
- The **Change display** menu in the task pane allows you to view different items and information associated with the node
- To modify or otherwise administer an item, select it and click a task in the task pane or details pane

Be aware that there is a limit of 1000 unique application icons. When that limit is exceeded, the Access Management Console displays a generic icon for all new applications in the left pane.

---

**Note:** When you are browsing a list of objects in the Access Management Console (for example, the list of administrators) and the list table in the right pane is too small to list all the objects, a dialog box might appear stating there was an unhandled exception. The exception might prevent the table from populating properly. To avoid this, enlarge the table by dragging the horizontal line separating the table of items in the upper-right pane from the list of tasks in the lower-right pane.

---




*This screen capture shows the layout of the console after running discovery. The left pane contains the console tree. The task pane is in the middle. The details pane is on the right.*

These 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. See "Customizing Your Displays Using My Views" on page 24 for instructions about creating My Views.

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, some or all of these 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.
- **XenApp.** Allows the console to establish contact with your deployment and lets you manage applications and servers, and view 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. XenApp is contained in the Citrix Resources node.
- **Web Interface.** Allows you to manage how users access applications through the Web Interface and Citrix XenApp plugin 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.

# Performing Tasks with the Access Management Console

Only Citrix administrators can use the Access Management Console. You can create *custom administrators* and grant them privileges, allowing them varying levels of access to areas of server farm management. For example, create *custom administrators* and specify that these administrators can manage sessions running on servers in their own locations without being able to view servers in other locations. In the Access Management Console left pane, select the **Farm** node and select **Action** > **New** > **Add administrator** to use the Add Citrix Administrator wizard to 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 Report Center.

Related topics:

"Managing Citrix Administrator Accounts" on page 31

"Delegated Administration Tasks Reference" on page 383

## Assigning Farm Administrator Credentials

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

## 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 must examine regularly or items in different parts of the console tree that you want to group together. Instead of repeatedly browsing the console tree, place the items in a single, easily retrieved display. For example, 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.

# Managing Applications and Servers in Multiple Farms

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

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

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

# To view zones with the Access Management Console

A zone is a configurable grouping of XenApp servers. Zones enhance the performance of a server farm by grouping geographically related servers together, whether they are connected to the same network subnet or not. By default, all servers in a farm that are on the same network subnet belong to the same zone.

Each zone in a server farm contains one server that is designated as the data collector for the zone. Data collectors store information about the servers and published applications in the zone. They act as communication gateways between zones in server farms that have more than one zone.

Zones are view-only in the Access Management Console. Use XenApp Advanced Configuration to configure zones by selecting a Farm node in the tree and choosing Actions > Properties > Zones.

1. In the Access Management Console left pane, under the **Zone** node, select a zone.
2. In the **Details** pane, choose **Servers** in the drop-down menu to display the servers in the chosen zone.

# Managing User Sessions and Server Processes

Use the Access Management Console to manage all user sessions in multiple farms in your enterprise. Alternatively, 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 about managing sessions and processes, see the Access Management Console *Help*.

## Creating Reports with the Access Management Console

Use Report Center in the Access Management Console 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. View the status of your scheduled reports and adjust the report parameters.

Report Center contains these reports:

- Application
- Configuration Logging
- Policy
- Virtual Memory Optimization

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 Access Management Console

Use the Access Management Console with the Web Interface site to configure how users access published applications and content through a standard Web browser or through the Citrix XenApp plugin.

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

## Creating Trace Logs with the Access Management Console

Use the Diagnostic Facility to gather system data for servers in multiple farms to assist Citrix Technical Support with problem analysis.

In the Access Management Console left pane, select the required servers and in the task pane, click **Diagnose problems > Start trace log**. 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, check which hotfixes are applicable to your Citrix products, search for particular updates on your system, and identify servers where up-to-date hotfixes must be applied. To use this feature, in the Access Management Console left pane, select **Citrix Resources > Configuration Tools > Hotfix Management**.

## Conserving Bandwidth for Remote Monitoring when Using the Access Management Console

When using the Access Management Console to monitor a farm at a remote site, conserve bandwidth across the WAN by publishing the console application on a remote server and connecting to it using the Citrix XenApp plugin locally. Ensure that you specify a working directory when publishing the console.

# Enabling Citrix Administrators to Manage Farms 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. Check the details of the discovery failure error to narrow down the potential causes of the failure.

One of the reasons this might occur is that you are using an account that does not have Distributed Component Object Model (DCOM) Remote Launch permissions on the remote server. To prevent this error from occurring, grant DCOM Remote Launch permissions to any Citrix administrators whom you allow to access the farm. You can grant DCOM Remote Launch permissions to administrators on remote servers running Windows Server 2008.

## To grant DCOM Remote Launch permissions to administrators

1. On each server in the farm, install Remote COM+ support.
    A. From the Server Manager, choose **Roles**, **Add Roles**, and then click **Server Roles** in the left pane.

B. Select **Application Server**.

C. Select **COM+ Network Access**, click **Next**, and then click **Install**.

2. On each server in the farm, add all users permitted to manage the farm remotely to the Distributed COM Users group and give them farm administrator privileges. Alternatively, 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. Perform this step 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**.

   A. Run the MMC and add the **Component Service** snap-in.

   B. Select **Computers**, right-click **My Computer**, and select **Properties**.

   C. Select the **Default Properties** tab.

   D. From the **Default Impersonation Level** drop-down list, select **Impersonate**.

4. Allow access to the Access Management Console and the XenApp Advanced Configuration tool through any software or hardware firewalls between the remote servers and the farm or disable these firewalls.

# Using Citrix XenApp Advanced Configuration

To use the Advanced Configuration tool, 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 tool that you are not authorized to use, the details pane on the right does not display the associated information.

XenApp Setup installs the Advanced Configuration tool on each server in the farm by default. Use the XenApp installation media to install the Advanced Configuration tool on other workstations you want to use to manage server farms.

**Important:** Earlier versions of the XenApp Advanced Configuration tool (called the Presentation Server Console) do not recognize settings you configure using this version of the tool. If you run the tool from devices that do not have XenApp installed, such as workstations or laptops, upgrade those devices to this version of the Advanced Configuration tool.

## Conserving Bandwidth for Remote Monitoring when Using Advanced Configuration

When using the Advanced Configuration tool to monitor a farm at a remote site, conserve bandwidth across the WAN by publishing the Advanced Configuration tool application on a remote server and connecting to it using the Citrix XenApp plugin locally.

## To configure the Advanced Configuration tool for screen reader accessibility

Screen reader software might not readily interpret some of the text that appears in the Advanced Configuration tool. By default, screen readers do not interpret static text areas 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 this procedure to configure the tool so that you can use the Tab key to move to static text areas you want screen readers to interpret.

1. On a computer where the XenApp Advanced Configuration tool is installed, locate and open the Isctx.log file using a text editor. If you installed the tool in the default location, Isctx.log is located in the \Program Files\Citrix\Administration folder.
2. On the second line of Isctx.log, type this text, including the hyphen:

   ```
   -labelsGetFocus:true
   ```

3. Save and close the file, then restart the tool.

# Managing Citrix Administrator Accounts

Citrix administrators are individuals tasked with managing and administrating server farms. You can make any member of a Windows or Novell Directory Services account authority a Citrix administrator. When planning your deployment, you can customize the scope of your Citrix administrators' authority by assigning different tasks to individual administrators or groups of administrators.

This topic discusses the following topics:


- "Planning Administrator Accounts" on page 31
- "Managing Citrix Administrator Accounts" on page 33
- "Disabling and Removing Administrators" on page 34
- "Delegating Tasks to Custom Administrators" on page 35


## Planning Administrator Accounts

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, the Access Management Console 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 console to set up Citrix administrator accounts. If the data store database contains at least one Citrix administrator account, a local administrator account cannot log on to the console.
- Citrix recommends that you add your standard network administrators group to your Citrix administrators group so that network administrators have access to manage network resources.

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

You can delegate tasks to custom Citrix administrator accounts when you create the accounts or by editing an existing account's properties.

# Types of Citrix Administrator Accounts

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 Access Management 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. If custom authority administrators try to access areas of the console that they are not authorized to use, the right pane of the console may be blank.

For more information about the permissions that can be assigned to a custom administrator, see "Delegated Administration Tasks Reference" on page 383.

**Important:** If you run Microsoft Windows Server 2003 Service Pack 1 and connect remotely to the Access Management Console, you may receive an error message when trying to discover a server in your farm. This occurs when you use an account that does not have DCOM Remote Launch permissions on the remote server. To prevent this error from occurring, you need to grant these permissions to any Citrix administrator who accesses the farm.

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

# Managing Citrix Administrator Accounts

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.

## To create new Citrix administrator accounts

1. In the left 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. On the **Privileges** page, select the authority level you want to grant the administrator account.
4. If you are creating a custom administrator account, in the Tasks pane, select the tasks you want to delegate to the custom administrator.

## To change Citrix administrator properties

You must be a Citrix administrator with full access to change Citrix administrator accounts. Citrix administrator properties comprise privileges and custom permissions.

1. From the left pane of the Access Management Console, select the **Administrators** node.
2. In the details pane, select the administrator whose properties you want to change.

3. From the Tasks menu, click **Modify administrator properties**.
4. Choose from the following options:
    - To change an administrator's privilege level, open the **Privileges** page
    - To assign or update custom permissions, open the **Permissions** page

# Disabling and Removing Administrators

You may need to disable Citrix administrator accounts to temporarily remove access from an administrator but retain the account and settings. Additionally, you may need to remove Citrix administrator accounts, for example, to accommodate changes to personnel. Only administrators with full access can disable or remove other Citrix administrator accounts.

---

**Important:** If only one Citrix administrator account with full access remains on the list, you cannot remove it.

---

## To disable a Citrix administrator account

1. In the left pane of the Access Management Console, select the **Administrators** node.
2. In the detail pane, select the administrator whose privileges you want to disable.
3. Under **Tasks**, click **Disable**.

When an administrator account is disabled, the administrator's icon appears in grey and an **Enable** task becomes available.

## To enable an administrator account

In the detail pane of the Access Management Console, select the administrator whose privileges you want to enable and then, under **Tasks**, select **Enable**.

## To remove a Citrix administrator account

1. In the left pane of the Access Management Console, select the **Administrators** node.
2. In the detail pane, select the administrator or administrators whose account you want to remove.
3. Under **Tasks**, click **Delete administrator**.

# Delegating Tasks to Custom Administrators

You delegate tasks by associating custom Citrix administrator accounts with *permissions* to perform select tasks. You do this through the Access Management Console.

Citrix recommends you create Windows, Active Directory, or NDS groups to assign these permissions. When you create custom Citrix administrators, simply select the group instead of individual users. This allows you to add and remove users to these groups without reconfiguring all of the permissions.

Permissions you set on nodes apply farm wide. Permissions you set on folders (applications, servers, and any folders within) apply only to the applications and servers contained within the selected folder.

You cannot grant permissions to applications and servers directly. To grant permissions to applications and servers, you must first place the applications or servers in folders and then grant permissions at the folder level. Therefore, before you delegate tasks for applications and servers, make sure you group the applications and servers in folders that allow you to delegate the tasks in a meaningful way.

---

**Note:** To apply the same permissions to a new folder as to its parent folder, select the **Copy permissions from the parent folder** option when you create the new folder.

---

Related topics:

"To delegate tasks to existing custom administrators" on page 35

## To delegate tasks to existing custom administrators

1. In the left pane of the Access Management Console, select the **Administrators** node and then in the detail pane, select an administrator.
2. Under **Tasks**, click **Modify Administrator Properties**.
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 check boxes, as appropriate.
6. If you set permissions on a node or a folder that contains a subfolder, the **Copy to Subfolders** button becomes active. Click this button if you want to

copy the permissions from the parent node or folder to the constituent folder.

**Note:** If you change an administrator's permissions, he or she will need to manually rerun discovery.

# Assigning Folder Permissions to Administrators

You can select the administrators to whom you want to grant access to the folders in the left pane of the Access Management Console.

You can view, change, and update the administrators who have access to the Applications, or Servers folders and the permissions they have on those folders. If you are a full administrator, you can change the permissions for any custom administrator in the top pane.

## To assign folder permissions

1. From the left pane of the Access Management Console, select the folder under the farm to which you want to grant access.
2. From the task pane, under **Other Tasks**, click **Permissions**. The resulting dialog box lists the administrators who currently have access to the selected folder.
3. To give access to an administrator that is not on the Administrators list, click **Add** and then click the check box to allow access to the folder.

   If the administrator to whom you want to give access does not appear in the **Add Access to folder** dialog box, click **Add** to create the administrator.

# Assigning Tasks to Administrators

To allow custom administrators to perform specific tasks in the farm, you assign object permissions at the farm level. You can view and change permission on objects that are managed primarily in XenApp Advanced Configuration tool, for example, printers. You must be a Citrix administrator with full access to view and change object permissions.

## To assign or change object permissions

1. From the left pane of the Access Management Console, select a farm and then, in the task pane under **Other Tasks**, click **Set permission on objects**.
2. Select the object whose permissions you want to change and click **Permissions**.

   Under **Administrators**, you can see the administrators who have access to tasks related to the object.

3. From the **Administrators** list select the administrator to whom you want to assign additional or change existing folder permissions. If the administrator you want is not on the list, click **Add** and select the administrator.

   If the administrator you want is not a custom administrator, click **Edit** and change the administrator's privilege level to **Custom**. This allows you to change the administrator's permissions.

4. With the administrator selected, use the check boxes to change specific permissions in the **Tasks** pane.

If the folder contains subfolders, the following options become available:

- Choose **Copy the permissions of this administrator for this folder to its subfolders** to copy newly configured permissions to all folders nested in the selected folder for the custom administrator.
- Choose **Copy the permissions of all administrators for this folder to its subfolders** to copy the newly configured permissions of each custom administrator who has access to the selected folder to the folders nested within it.

---

**Note:** If you change the permissions later in the top level folder, the changes are not automatically copied to the nested folders. When you make changes to top level folders, use either the **Copy the permissions of this administrator for this folder to its subfolders** or the **Copy the permissions of all administrators for this folder to its subfolders** function to copy the permissions again.

---

# Delivering Resources to Users

With XenApp, you provide users with access to information by virtualizing resources on servers or desktops by publishing the following types of resources:

- *Applications* installed on servers running XenApp. When users access them, the published applications appear to be running locally on client devices.
- *Streamed applications* installed in application profiles and stored on a file server. Users access the profile and virtualize the applications on their client desktops. For information about preparing and publishing applications for streaming, see the *Citrix Application Streaming Guide.*
- *Data files* such as Web pages, documents, media files, spreadsheets, and URLs. In XenApp, the combined total of data types you publish is referred to as *content*.
- The *server desktops*, 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.

Publish all of these resource types using the Publish Application wizard in the Access Management Console. To further refine how your users launch and access published resources, use content redirection and XenApp policies.

**Important:** Before you begin, refer to *Getting Started with Citrix XenApp* to review the new and discontinued features for publishing applications on XenApp for Windows Server 2008.

Additionally, refer to the *Installation Checklist* for supported platforms and system prerequisites.

# Making Resources Available to Users

Use the Publish Application wizard to deliver a common set of resources, including applications, streamed applications, server desktops, and content to different types of client devices. Users can access these resources from a server without knowing the name or address of the server.

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; importance level for Preferential Load Balancing; 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 plugin they are running on the client device. Consult the appropriate plugin (or client) administrator's guide for more information about the plugin with which your users start published applications.

Related topics:

"To publish a resource using the Publish Application wizard" on page 41

## Installing Applications for Multiple Users

Before installing applications that you want to publish on a server, enable **Terminal Services**. Install applications for publication before or after you install XenApp on the server. See the *Installation Checklist* for more information about recommended changes in Terminal Services configuration for Windows Server 2008, such as clearing the default setting that restricts users to a single session.

In addition, the User Account Control (UAC), which is enabled by default in Windows Server 2008, affects how you install applications for publication. Unless you install applications for all users, multiple users cannot connect to a published application simultaneously.

To ensure applications are enabled for multiple users, install the applications using one of the following methods:

- Install applications as the Built-in Administrator
- Select an "install for multiple users" option in the installation wizard for the application, if the Setup for the application provides this option
- Install the application for all users from a command line, as described in "To install an application for all users" on page 41

### To install an application for all users

After enabling Terminal Services, use these steps before installing the application:

1. Open a command prompt so that you running it with Administrator privileges; for example, by right-clicking the command prompt and selecting **Run as Administrator**.
2. Run the following command at a command prompt:
   `change user /install`
3. From the command prompt, run the Setup executable for the application.

## Publishing in Domains with Thousands of Objects

For directory services or domain environments, such as Novell Directory Service or Microsoft Active Directory Service, containing over 10,000 objects, Citrix recommends the following:

- Use groups to categorize and assign permissions to large numbers of users. An application published to one group of 1,000 users requires XenApp to validate only one object for all 1,000 users. The same application published to 1,000 individual user accounts requires IMA to validate 1,000 objects.
- When adding users through the Citrix User Selector, if the Users container holds thousands of objects, instead of scrolling to locate a user, click **Add List of Names**.

## To publish a resource using the Publish Application wizard

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.

Steps and options in the wizard vary depending on the application type you select. This procedure describes the basic options.

1. Under the **XenApp** node of the Access Management Console, expand the farm or server to which you want to publish an application.

---

**Tip:** To add a server to the list of servers for a published desktop or application (after publishing the application), drag and drop the server onto the published desktop or application in the left pane of the console. You can also drag and drop the published desktop or application onto the server.

---

2. Select the **Applications** node and from the **Common Tasks** pane choose **New** > **Folder**. Create a folder for the application you are publishing.
3. Select the folder you created and from the **Common Tasks** pane choose **New** > **Publish application**.
4. In the Publish Application wizard, on the **Name** page, provide a display name (maximum 256 characters) and application description. The name appears on client devices when users access the application and on the Access Management Console for the farm applications. To change the display name or application name, see "To rename a published application" on page 64.
5. On the **Type** page, specify the type of resource you want to publish and the delivery method. Three types of resources can be published (*server desktop*, *content*, and *application*). The next few steps in the wizard differ based on which type you select. For more information, see "To select a resource type and delivery method" on page 43.
6. On the **Location** page, add the command-line and working directory (optional) to locate the application. For more information, see "To configure locations of applications for publishing" on page 45 or "To configure locations of published content" on page 47.
7. On the **Servers** page, add the individual servers on which the published application runs when accessed by an ICA connection. For more information, see "To configure locations of servers for published resources" on page 47.
8. On the **Users** page, create the **Configured users** list for users or groups who have access to the application. Use the options to allow access to configured user accounts only or to anonymous users. For more information, see "To configure user access to applications" on page 48.
9. On the **Shortcut presentation** page, select the icon for the application and choose how the application is enumerated on the client device. For more information, see "To configure shortcuts for client devices" on page 51.

   The Access Management Console has a limit of 1,000 unique application icons. When that limit is exceeded, the console displays a generic icon for all new applications.
10. On the **Publish immediately** page, choose whether or not to make the published application immediately available to users.

    - By default, the published application is available when you click **Finish**.
    - To prevent users from accessing the application until you manually enable it through application properties, select **Disable application**

**initially**. For more information, see “To disable or enable a published application” on page 65.

11. To view and select advanced options, check **Configure advanced application settings now**. Alternatively, modify the advanced settings using the application properties described in the following topics:

    - “To configure access controlled by the Access Gateway” on page 52
    - “To configure content redirection” on page 52
    - “To configure application importance” on page 60
    - “To configure audio and encryption options for published applications” on page 61
    - “To configure application appearance” on page 63
    - “To reduce user privileges for a streamed application” on page 63

When you finish, published resources (unless disabled) are available for users.

# Managing Delivery Options for Published Resources

The following delivery options are available in the Publish Application wizard and the application properties:

- Selecting a resource type to publish
- Configuring locations for applications or published content
- Configuring user access for applications
- Configuring shortcuts
- Configuring advanced options, such as access control, content redirection, application limits, client options, application appearance, application importance, and user privileges

Related topics:

“To publish a resource using the Publish Application wizard” on page 41

## To select a resource type and delivery method

You select the resource type initially in the Publish Application wizard. To change the resource type, from the **Action** menu, select **All Tasks** > **Change application type** and follow the instructions in the wizard.

1. Select one of the following options:

- **Server desktop**. Publishes the entire Windows desktop of a server in the farm. When the plugin connects to the server, the user sees a desktop interface from which any application installed on that server can be started. After selecting this application type, you must specify the server that you want to publish.

  To publish a desktop, you must be running XenApp. If you are running the console on a computer that is not running XenApp, you cannot publish the local desktop.

- **Content**. Publishes nonexecutable information, such as media, Web pages, or documents. After selecting this application type, you must specify the URL (Uniform Resource Locator) or UNC (Uniform Naming Convention) path to the file you want to publish. Click **Browse** to view available content resources on your network. See "To configure locations of published content" on page 47 for more information.

- **Application** (selected by default). Publishes an application installed on one or more servers in the farm. Note that if you are running the console on a computer that is not a member of the farm, you cannot publish local applications.

  You need to indicate one of the following application types:

  - **Accessed from a server**. Grants users access to applications that run on a XenApp server and use shared server resources. If you choose this option, you must then enter the location of the executable file for the application and the XenApp server on which it will run. Choose this option as the application type unless you intend to stream your applications.

  - **Streamed if possible, otherwise accessed from a server** (also called *dual mode streaming*). Grants users access to a profiled application that streams from the file share to their client devices and launches locally from within an isolation environment. Alternatively, for client devices that do not support streamed applications (for example, if the XenApp Plugin for Streamed Apps is not installed), use an ICA connection to access the application installed on or streamed from a XenApp server.

  - **Streamed to client.** Grants users access to a profiled application that streams from the file share to their client desktops and launches locally from within an isolation environment. With this option, the application uses client resources instead of server resources. Users must have the XenApp Plugin for Streamed Apps installed and access the

application using XenApp Plugin for Hosted Apps or a Web Interface site. If selected, client devices that do not support client-side application virtualization (such as, they use a non-Windows client) or do not have the XenApp Plugin for Streamed Apps installed locally cannot launch the application.

2. If you selected **Accessed from a server** or **Streamed if possible, otherwise accessed from a server**, you also need to select the **Server application type**. These are:

   - **Installed application**. Enables users to launch an application installed on a XenApp server.
   - **Streamed to server**. Grants users access to stream a profiled application from the file share to a XenApp server and launch it from XenApp through an ICA connection.

   **Note:** For more information about client-side application virtualization through streaming, see the *Citrix Application Streaming Guide.*

# To configure locations of applications for publishing

To access this option in the Access Management Console, from the Publish Application wizard, continue to the **Location** page. Alternatively, select a published application and under **Common Tasks**, select **Modify application properties** > **Modify all properties** > **Basic** > **Location**.

Use this page to configure the command-line and working directory (optional) for the application by adding the following information:

- **Command-line**. The full path of the application's executable file. Append the symbols "%*" (percent and star symbols enclosed in double quotation marks) to the end of the command-line to act as a placeholder for client-supplied application parameters. When a plugin makes a connection request, the server replaces the symbol "%*" in the command-line with application parameters provided by the plugin.

  If the path to the application's executable includes directory names with spaces, enclose the command line for the application in double quotation marks. Include a space between the closing quotation mark and the double quotation marks around the percent and star symbols. An example of the format to use with a path with spaces and a placeholder is:

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

**Important:** Changing the command-line text removes all file type associations from the application. If you change the command-line text, use the Content Redirection property page to select the file types you want to associate with the application for client to server content redirection.

- **Working directory**. By default, this path is the same as the path in the **Command line** field. To run the application from a different directory, add an absolute path to this field.

## Validating Command-Line Parameters for Published Applications

By default, XenApp validates published application command-line parameters passed from the client to the server. When you use the symbols "%*", XenApp ensures the parameters are valid before the application launches. If the parameters are invalid, the application launches without passing the parameters. XenApp records all failed validation attempts in the server's system log and in the security event log.

XenApp provides command-line validation for content that is redirected from the client to the server only.

### Establishing Trust Between Content and Published Applications

When using command-line validation, add all servers that store content, such as Word documents or PDF files, to the Trusted Sites list on the XenApp server. When adding servers to the Trusted Sites list, ensure you are logged on to the XenApp server as Administrator.

If the content servers reside in separate domains, ensure trust relationships are established between these servers and the XenApp server.

### To disable command-line validation for selected published applications

If your environment includes published applications that use customized client-supplied parameters for purposes other than content redirection from client to server, these applications might not function correctly when command-line validation is enabled. To ensure client-supplied parameters are passed from client to server, disable command-line validation for these published applications.

From the **Location** page of the application properties, append the symbols "%**" (percent and two star symbols enclosed in double quotation marks) to the command-line parameter.

### To disable command-line validation for all published applications on a server

If your XenApp environment consists of a mixed farm and includes published applications that use customized client-supplied parameters, use the following steps to disable command-line validation for all applications:

---

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

---

1. On the server where the applications reside, run **regedit**.
2. Modify the following entry:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

   Name: PublishedAppCommandLineFlag

   Type: DWORD

   Data: 1 (enable validation, default) or 0 (disable validation)

## To configure locations of published content

When you publish content, specify the location using address formats such as the following types (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)

## To configure locations of servers for published resources

Choose the server on which the published application or desktop is available through the **Servers** page of the Publish Application wizard, or from the **Action** menu, select **Modify application properties** > **Modify servers**.

**Important:** For installed applications, select the server where the published application is installed. For streamed-to-server applications, select the server to which the profiled application will stream and execute.

- The **Servers** list displays the servers that belong to the farm. Initially, all servers in the farm appear. Use a filter to display only servers running a particular operating system or Citrix version.

  **Note:** If you apply a filter (in the **Select Servers** dialog box), the filter settings remain in effect each time the Publish Application wizard is run until the filter is removed or changed.

- Use the **Import from file** option to import an application server list file (*.asl). You export the server list of a previously published application and then import this settings file when creating a new published application. For information, see "To export published application settings to a file" and "To import published application settings from a file".

If you modify your servers for a published application, some users may not be in a trusted domain for that server. If you receive an error message when trying to modify configured servers for a published application, duplicate the application and then modify the servers and users lists of the new application.

## To configure user access to applications

Choose the user accounts that can access applications through the **Users** page of the Publish Application wizard, or from the application properties, by selecting **Actions**, select **Modify application properties** > **Modify users**.

Before you publish resources, consider how the configuration of the accounts of your users can affect their access: anonymous access and explicit (configured) user account access.

**Note:** As a best practice, use groups for unique roles to categorize and assign permissions to large numbers of users. An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users. That same application published to 1,000 individual user accounts requires the validation of 1,000 objects.

1. Select how to configure user accounts:

   - Select **Allow anonymous users** to let all users log on anonymously and start the streamed application without specifying a user name,

domain name, and password (selected by default). This selection disables the remaining options on the page. For more information, see "Granting Access to Anonymous Users".

- Select **Allow only configured users** to allow only configured users to start the application. Selecting this option enables the **Select directory type** drop-down list, which allows you to configure the users for this application. For more information, see "Granting Access to Explicit Users".

---

**Note:** These options are not shown if you enabled the application for offline access, which does not support anonymous users.

---

2. Use the **Select directory type** drop-down box to select either **Citrix User Selector** or **Operating System User Selector**.
3. Click **Add**.

   If you selected **Citrix User Selector**, complete the following tasks in the **Select Users or Groups** dialog box:

   - Select your account authority from the **Look in** drop-down list. The drop-down list contains all trusted account authorities configured on the servers in the farm. These include Novell Directory Services (NDS) trees, Windows NT domains, Active Directory domains, and local servers. (NDS trees appear only if previously configured.) When you select an account authority, the user accounts that are part of the selected authority appear in the window below the drop-down list. By default, only user groups appear.
   - Select **Show users** to display all user names in the selected domain. This option displays every user in the selected domain. For NDS, alias objects also appear. The user accounts you select are listed in **Configured users**.

   ---

   **Tip:** Instead of selecting names from the list, type them in a text box. To do this, click **Add List of Names** and use semicolons (;) to separate names.

   ---

   If you selected **Operating System User Selector**, use the standard Windows dialog box to select your user or group.

**Note:** This option has several limitations. You can browse only account authorities and select users and groups that are accessible from the computer running the Access Management Console. In addition, you might initially select users and groups outside the trust intersection of the farm, which causes errors later. Other limitations include the inability to add NDS users and groups.

The list of user accounts is added to the **Configured Accounts** list. Changes take effect the next time the user launches the application.

## Granting Access to Anonymous Users

During XenApp 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 device.

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

## Granting Access to 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.

## To configure shortcuts for client devices

Configure or modify the application shortcut presented to client devices on the **Shortcut presentation** page of the Application Publishing wizard or by selecting **Modify application properties** > **Modify all properties** > **Basic** > **Shortcut presentation**.

1. To select a new icon for the application, click **Change icon** and use the options on the window.
2. To organize applications within folders on the client device, under **Client application folder**, enter a folder name for this application. When users view their **Citrix XenApp** applications, this application is listed in the folder you entered.
3. To specify the placement of the application shortcut, in the **Application shortcut placement** section, select one or more of these options:
    - **Add to the client's Start menu.** Creates a shortcut to this application in the user's local **Start** menu. A folder appears in the first pane of the Start menu in the location you select:
        - **Place under Programs folder**. This option creates a shortcut under the Programs folder of the local Start menu. If a folder structure is specified in the Start Menu Folder text box, the folder structure is created within the local Programs folder.
        - **Start menu folder**. The location of the shortcut within the Start menu (or Programs folder, if selected). For example, to have the application appear under a folder called "Reports," enter Reports. For more than one level of folders, separate each folder name with a backslash; for example, "Reports\HR\survey." If no folder structure is specified, the application is available from the top level of the Start menu.
    - **Add shortcut to the client's desktop**. Creates a shortcut to this application on the user's local desktop.

Changes take effect after the user reconnects or refreshes the client device.

# To configure access controlled by the Access Gateway

Use the **Access control** page of the Publish Application wizard or the application properties to specify the types of connections through which users can start sessions to access published applications on the farm.

If Access Gateway (Version 4.0 or later) is installed, use the **Access Control** page of the Publish Application wizard or select **Access Control** from the **Advanced Application Properties** page to specify the type of connections that allow the application to appear in the list of published applications on the client device.

For example, if Access Gateway is installed and the application has software requirements, define a filter in Access Gateway and apply the filter to the published application using XenApp.

---

**Important:** To use this feature, set your servers that receive XML requests to trust those requests.

---

Use this page to view or modify connection types:

- **Allow connections made through Citrix Access Gateway Advanced Edition (Version 4.0 or later).** This is the default. Select the type of connections that allow the application to appear in the list of applications:
  - **Any connection.** Allows connections made through Access Gateway (Version 4.0 or later), regardless of filters. This is the default.
  - **Any connection that meets any of the following filters.** Allows connections made through Access Gateway (Version 4.0 or later) that meet one or more of the connection filters specified in the list.

    To Add or Edit a filter, click the respective button and enter the predefined Access Gateway farm name and filter.
- **Allow all other connections.** Allows all connections except those made through Access Gateway (Version 4.0 or later). This is the default.

Users who do not have the required software running on the client device cannot access the published application.

# To configure 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.

This topic includes the following information:

- "Redirecting Content from Client to Server"
- "Redirecting Content from Server to Client"
- "To associate published applications with file types"
- "To update file type associations"
- "To pass parameters to published applications"

---

**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

Configure content redirection from client to server by associating published applications with file types and then assigning them to the users you want to be affected. When you configure *client to server content redirection*, users running the XenApp Plugin for Hosted Apps 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 Citrix XenApp. You must use the Web Interface server to allow users to connect to published applications. Citrix XenApp 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 file type association is changed to reference the published application in the Windows registry on the client device.

If you have users who run applications such as email programs locally, use the content redirection capability with Citrix XenApp 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 Citrix XenApp.
2. Verify that client drive mapping is enabled, either for the entire 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 file type for the published content. For example, if you publish a Microsoft Word document file named "Quarterly_Sales.doc," publish Microsoft Word on a XenApp 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 access it.

### Using Windows Explorer on Client Devices When Content Redirection is Configured

When you configure content redirection from client to server, context menu commands available from within Windows Explorer function differently than on client devices that do not use this feature. For example, if you right-click a file in Windows Explorer on a client device with content redirection from client to server enabled for the file type, the **Open** command opens the file with the remote application on XenApp. For a streamed application, the file could be opened either on the client device or on the XenApp server, depending on the delivery configuration.

Most commands on the Windows Explorer context menu are unaffected because they are not configured under keys modified by XenApp. Context menu items are generally defined by each application when installed.

## Redirecting Content from Server to Client

When you enable *server to client content redirection*, embedded URLs are intercepted on the XenApp server and sent to the client device. The browser locally installed on the client device 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 XenApp. To free servers from processing these types of requests, 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 through client devices 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 Media Format)

---

**Important:** 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.

---

### To enable content redirection from server to client

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 for the farm, select the farm in the left pane. Then select **Action > Modify farm properties > Modify all properties**. Open the **Server default** page from the **Properties** list, select **XenApp** and then **Content Redirection** options, and then select the option **Content redirection from server to client**.
- To enable content redirection for a specific server, select the server in the left pane. Then select **Action > Modify server properties > Modify all properties**. Open the **XenApp** page from the **Properties** list, select the

**Content Redirection** option, and then select the option **Content redirection from server to client**.

- To enable content redirection for specific connections, use the Advanced Configuration tool 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.

When you configure XenApp 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 device. 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. Use this method to publish any content for users to view with a local viewer application.

Accessing published content with local client devices does not use XenApp 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.

## To associate published applications with file types

As you publish applications, you associate the published item with certain file types present in the Windows registry on the server. You associate published applications with file types initially in the Publish Application wizard or later from a **Properties** page for the published application. By associating published applications with file types and then assigning the applications to users, you implement the following automatically:

- **Content publishing.** Users connecting through the Web Interface or using Citrix XenApp 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 Citrix XenApp Plugin 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.

**Note:** If you do not want specific users to launch published applications automatically when opening published content, do not assign published applications associated with file types to those users.

File type association is a two-step process. For example, if you want to associate Microsoft Word with the .doc file extension:

- Publish a document of the Microsoft Word for Windows file type.
- Publish the Microsoft Word application and associate it with the Microsoft Word for Windows file type. When users double-click the document from the client device, it opens in the Microsoft Word application published on the server.
- Users connecting through the Web Interface or using Citrix XenApp Plugin can open published content with published applications.

Associate published applications with file types initially from the Publish Application wizard, on the **Content redirection** page, or later from the **Action** menu, select **Modify application properties** > **Modify content redirection properties**

1. Select one or more of the buttons to select the file types that you want the application to open when a user opens a file. Published applications can be associated with one or more file types.
2. To list all file types associated with the application, click **Show all available file types for this application**. Clear the check box to display only the selected file types.

   When changing the available file types for an application, select this check box to display the superset of file types available, not just those selected when initially publishing 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.

## To update file type associations

File types are associated with applications in a server's Windows registry. If you install and then publish applications after installing XenApp, you must update the file type associations in the Windows registry on the server. Use **Update file types** to associate these file types with the application in the server farm's data store. To verify which file types are associated with a published application, use the **Content redirection** tab of the **Properties** page for the application.

---

**Important:** Updating the file type association data for a farm can take a long time. It depends on the number and availability of servers, the number of streamed applications, and the availability of the streamed application file shares. If you do not have permission to access these file shares, an alert appears.

---

Update the file type associations in the data store if:

- You installed an application but have not yet published it.
- You plan to enable content redirection from client to server or have users open published content using the application.
- The data store does not already contain the file type associations. If you updated the file types from the registries of other servers hosting the application, the data store already contains the associations.

Choose which file types are opened with a published application. When you publish an application, a list of available file types appears on the Content redirection page. This list is current only if the data store was updated with the file type associations for the application. Update the data store from the registries of several servers containing an application to associate a complete set of file types with the application.

If needed, update file types for the farm or for an individual server:

1. In the Access Management Console, select a farm in the left pane and from the **Action** menu, select **All Tasks** > **Update file types**.
2. Select a server in the left pane and from the **Action** menu, select **All Tasks** > **Update file types from registry**.

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

### To pass parameters to published applications

Use the **Location** page of the application properties in the Access Management Console to pass 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 command line for the application. 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 correct symbols. By default, XenApp validates client-supplied parameters when the symbols "%*" are appended. For published applications that use customized client-supplied parameters, the symbols "%**" are appended to the command line to bypass command line validation. If you do not see these symbols in a command line for the application, add them manually.

If the path to the 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"
"%*"
```

## To configure application limits

When a user starts a published application, the plugin establishes a connection to a server in the farm and initiates a session. If the user then starts another published application without logging off from the first application, the user has two concurrent connections to the server farm. Use the Publish Application wizard **Limits** page or the **Action** menu > **Modify application properties** > **Modify all properties** > **Advanced** > **Limits** page to limit the number of concurrent connections that users can make.

Under **Concurrent instances**, select from the following options:

- **Limit instances allowed to run in server farm** and then enter the numerical limit in **Maximum instances**
- **Allow only one instance of application for each user**

## To configure application importance

If Preferential Load Balancing is available in your XenApp edition, this setting (along with the session importance policy setting) determines the Resource Allotment associated with the session. The higher the Resource Allotment of the session, the higher the percentage of CPU cycles allotted to it.

You can configure application limits from the Publish Application wizard **Limits** page, or from the **Action** menu > **Modify application properties** > **Modify all properties** > **Advanced** > **Limits**.

In the **Application Importance** list box, set the priority that is used with the **Session Importance** setting to determine the level of service for the session in the XenApp farm: **High**, **Normal**, and **Low**.

Related topics:

"Using Preferential Load Balancing" on page 322

"Resource Allotment" on page 322

"Multiple Published Applications in the Same Session" on page 324

# To configure audio and encryption options for published applications

Use the **Client Options** page of the application Properties in the Access Management Console to configure the plugin audio and encryption options for when users connect to a published application.

To locate the page, select the application, and from the **Action** menu, select **Modify application properties** > **Modify all properties** > **Advanced** > **Client options**.

The settings that plugins use to communicate with a published application vary according to the type of plugin. The Citrix XenApp Plugin and Web Interface automatically use the settings you specify here to communicate with this published application.

For Program Neighborhood, you must configure the client-side encryption setting to correspond with the encryption level you specify in this wizard. Selecting the **Minimum requirement** check box ensures that the server rejects any Program Neighborhood communications that do not meet the level of encryption you set for this application.

Set the encryption level for communications in multiple places in XenApp and your Windows operating system. If a higher priority encryption level is set elsewhere, the settings that you specify can be overridden. The most secure setting out of the settings below is used:

- The setting in Terminal Services Configuration (TSCC) and/or the setting in Citrix Connection Configuration Tool (Mfcfg.exe)
- The policy setting that applies to the connection
- The application setting (that is, the level you are setting in this dialog box)
- The Microsoft Group Policy

The encryption settings specified here when publishing an application should be at the same level as the encryption settings you specified elsewhere. That is, 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 any settings you specified for TSCC and connection policies, those settings override the application settings. If the minimum requirements check box is selected and the plugin connection does not meet the most restrictive level of encryption, the server rejects the ICA connection when the plugin tries to connect to the application. If the minimum requirements check box is selected, the plugin setting is always used. However, the plugin setting must be as secure as the server setting or the connection is denied.

If you select **Minimum requirement** under the Encryption list box, plugins can connect to the published application only if they are communicating using the specified level of encryption or higher. After you set this encryption level on the server, any plugins connecting with that server must connect at that encryption level or higher. This means the following:

- If you do not select the **Minimum requirement** check box, the Program Neighborhood connections to the server are encrypted at the level that you set in Program Neighborhood. If the two encryption levels 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, the Program Neighborhood connections to the server must be encrypted at the same level that you set on the server, or the server refuses the transmission and the session is dropped.

If a plugin is running on a 64-bit computer, only basic encryption is supported. In this situation, setting a level of encryption higher than Basic and selecting the minimum requirements check box prevents plugins from connecting.

Specify plugin audio options through the **Client options** page of the Publish Application wizard, or from the **Action** menu, select **Modify application properties** > **Modify all properties** > **Advanced** > **Client options**.

- Select **Client audio** options:

  **Enable legacy audio**. Select this option to allow audio support for applications to which SpeedScreen Multimedia Acceleration does not apply.

  ---

  **Note:** By default, audio is disabled on the client device. To allow users to listen to audio in ICA sessions, turn on audio or give the users permission to turn on audio themselves in the plugin interface they are using, such as Citrix XenApp.

  ---

  - **Minimum requirement**. Select this option to allow plugins to connect to the published application only if they have audio support. The **Minimum requirement** check box under the Client audio list box applies only to the legacy audio setting. It does not apply to SpeedScreen Multimedia Acceleration.
- In the **Connection encryption** section, select one or more of the following:

- **Enable SSL and TLS protocols**. This option requests the use of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols for plugins connecting to the published application.
- **Encryption**. Select an RC5 encryption level for the ICA connection.

- In the **Printing** section, select or clear **Start this application without waiting for client printers to be created**.

  Selecting this option can allow the plugin to connect faster. However, if you select this option, the printers may take a few seconds to be created; do not select this option for applications that print to the printer immediately after being launched.

## To configure application appearance

Define how the application appears to the user through the **Appearance** page of the Publish Application wizard, or from the **Action** menu, select **Modify application properties** > **Modify all properties** > **Advanced** > **Appearance**.

- Select the **Session window size** to set the default window size for ICA connections. Specify window size as a standard resolution, custom resolution, percentage of the client desktop, or full screen.
- Select the **Colors** to set the color depth for the application. The available options are 16 Colors, 256 Colors, High Color (16-bit), or True Color (24-bit).
- In the **Application Startup Settings** section, specify to hide the application title bar and maximize the application at startup.

## To reduce user privileges for a streamed application

For streamed applications only, use this setting to reduce the user privileges for the application, thus reducing security risks. From the **User privileges** page of the Publish Application wizard or from the **Action** menu, select **Modify application properties** > **Modify all properties** > **User privileges**.

---

**Important:** Before you select this option, test the application with a limited access configuration. Some applications expect users to have elevated privileges and might fail to operate correctly when launched by users with a least-privileged user account.

---

Select **Run application as a least-privileged user account** (not selected by default). This setting configures all users, even those with an administrator account, to run the application with normal user privileges.

For more information about least-privileged user accounts, see "Using a Least-Privileged User Account" on the Microsoft Web site.

# Managing Published Applications

After publishing applications through the Publish Application wizard, manage the published applications and their properties:

- Rename, move, disable, and delete published applications
- Change, duplicate, import, and export published application settings

Only a Citrix administrator with full access to the Published Applications task can change published applications. Use the application properties to change settings for a published application, including the location of the published application, the servers on which the published application is available, and the user accounts allowed to access the published application.

From the **Action** menu, select **Modify application properties** > **Modify all properties**.

---

**Important:** The resource type you publish (application, content, or server desktop) determines your path through the Publish Application wizard; consequently, the properties associated with the resource may vary.

---

## To rename a published application

Use the **Name** property to rename a published application without having to remove it and then republish the application. This feature can distinguish among multiple versions of the same application.

1. In the left pane of the Access Management Console, select the published application.
2. From the **Action** menu, select **Modify application properties** > **Modify all properties** > **Name**.
3. Change the name as needed. The **Display name** is the name users will see on their client device, and it must be unique within the folder. The **Application** name appears in the Access Management Console and should be unique within a farm (maximum 38 characters). When the application is published, these names are the same by default.

**Important:** If a duplicate application name is found in the farm, a four-digit hexadecimal number is appended to the original string. If the character limit is reached and duplicated, the console replaces the end characters with four-digit hexadecimal numbers, starting from the right. The application name appears in the left pane of the Properties dialog box for an application.

## To disable or enable a published application

Take published applications offline temporarily or indefinitely when you are maintaining a published application, such as applying an upgrade or a service pack to it. While an application is offline, it is not accessible to users. You can disable multiple applications simultaneously.

You might initially disable an application as you publish it in the publishing wizard or enable or disable it anytime from the Access Management Console.

- From the Publish Application wizard, continue to the **Publish immediately** page and select the **Disable application initially** check box. When checked, the application is published but users cannot access it until you enable it.
- In the Access Management Console, select the application in the navigation pane, and from the **Action** menu, select **Enable application** or **Disable application.**

**Note:** If the **Disable application initially** option is selected and cannot be cleared, either the application requires configured users but none are specified, or the application is of a type that runs on a server (such as an installed application or streamed-to-server application) but no servers are specified. For more information, see “To configure user access to applications” and “To configure locations of servers for published resources”.

## To delete a published application

As you publish updated applications on your servers, delete the older or less-frequently used applications. Deleting a published application does not uninstall the application. It simply removes access to the application through plugin connections. You can delete multiple applications simultaneously.

1. In the left pane of the Access Management Console, select the application.
2. On the **Action** menu, select **Delete application**.

## To move a published application to another folder

Use this option to move a published application to another folder in the Access Management Console tree or to move servers to another server folder. Published applications can be moved only to **Applications** or folders under **Applications**. Similarly, servers can be moved only to **Servers** or folders under **Servers**. You can move multiple applications simultaneously.

1. In the left pane of the Access Management Console, select the application.
2. On the **Action** menu, select **Move to folder**.
3. Use the **Select destination** folder dialog box to change the location of the application.

Alternatively, drag applications into a new folder.

## To duplicate published application settings

Use the settings of a published application as a template to publish other applications. For example, if you published an application with a specified user list, you might want to apply the same user list to a new application hosted on the same set of servers. If so, copy the first published application, change the name and location to those of the second application, and thereby publish a different application with the same user and server properties. You can duplicate multiple applications simultaneously.

1. In the left pane of the Access Management Console, select the application.
2. From the **Action** menu, select **Duplicate application** and a copy of the application appears under the Applications node.
3. Select the duplicated application and change the required properties.

## To export published application settings to a file

Exporting published application settings to a file allows you to import these settings files and create new applications at a later time. First you export the desired settings to a settings file, and then you import this file to create new applications easily. For information, see "To import published application settings from a file". In particular, import these settings files to overwrite the settings on a previously published application.

This export option offers choices to export a single application, the user list only, or server list only. To export multiple applications, see "To export multiple published application settings to a file simultaneously".

A Citrix administrator requires the View permission for the application folder in which the application resides to export published application settings.

1. In the left pane of the Access Management Console, select the application whose settings you want to export.
2. From the **Action** menu, select **All Tasks** > **Export application settings to a file**. Select what to export:

   - **Entire Application**. Exports the application and all the settings associated with the published application to an APP file. If you choose this option, export settings from multiple applications; select them from the left pane of the console before selecting the export task.

     ---

     **Important:** If application settings are exported as a batch, they must be imported as a batch.

     ---

   - **User List Only**. Exports only the list of configured users for the application to an AUL file. This option can export the user list associated with one published application only. Then select a published application and import the user list, replacing the existing user list.
   - **Server List Only**. Exports only the list of configured servers for the application to an ASL file, including any per-server command-line overrides, if applicable. Then select an application and import the server list, replacing the existing server list. Alternatively, import this list of servers when publishing an application by clicking **Import from file** on the **Servers** page of the Publish Application wizard. For information, see “To configure locations of servers for published resources”.

     ---

     **Note:** This task is available only for applications that have servers associated with them. For this reason, this task is unavailable for published content or streamed-to-client applications. You can export the server list associated with one published application only.

     ---

3. Settings files are saved in XML format.

   The settings associated with your published application are saved to a settings file with one of the following extensions: APP, AUL, or ASL. The file name is the same as the application by default. For example, if you choose to export all the application settings of a published application called Notepad123, the default file name for the exported application settings file is Notepad123.app.

## To export multiple published application settings to a file simultaneously

This export option limits you to exporting the entire application or multiple applications simultaneously.

1. In the left pane of the Access Management Console, select the Applications folder that contains the applications whose settings you want to export.
2. In the right pane of the console, press **CTRL** and select the names of the applications you want to export.
3. From the **Action** menu, select **All Tasks** > **Export application settings to a file** > **Entire Application**.
4. Use the **Save As** dialog box to locate where to save your settings.

   The settings associated with your published applications are saved to an application settings file with the .app extension.

## To import published application settings from a file

After you export published application settings to a file, use them to create a new application or alter the user or server settings of a previously published application.

Citrix administrators require Published Application permissions for the application folder in which the application resides to import application settings.

1. In the left pane of the Access Management Console, select either the folder into which you would like to place a new published application or the published application whose user or server settings you want to change.
2. From the **Action** menu, select **All Tasks** > **Import application settings from a file**.
3. Use the **Open** dialog box to locate the settings file you want to import.
   - If you selected a folder in Step 1 of this procedure and an APP file in Step 2, the new application appears under the folder you selected.
   - If you selected a previously published application in Step 1 and either an ASL or AUL file in Step 2, click **Yes** to confirm that you want to overwrite existing settings. The imported ASL or AUL file updates the server settings or user settings of the application, respectively.

**Note:** If any of the servers or users that were exported for a published application cannot be imported, a warning message appears identifying the list of users or servers that could not be imported. You either proceed or cancel the import at that point. Cancelling the import cancels the entire import operation. This situation might occur if a server was removed from the farm after a published application was exported, if a user was removed from the domain, or if the administrator does not have proper permissions to publish the application on one or more of the servers that were exported.

# Making Virtual IP Addresses Available to 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 XenApp environment, a unique IP address is required for each device.

Use the virtual IP address feature to 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, this feature lets you 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.*).

Processes require **Virtual IP** if either:

- They use a hard-coded TCP port number, *or*
- They do *both* of the following:
  - Use Windows sockets, and
  - Require a unique IP address or require a specified TCP port number

Processes require **Virtual loopback** if they do either of the following:

- Use the Windows socket loopback (localhost) address (127.0.0.1)
- Use a hard-coded 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 “To supply client IP addresses to published applications on a server”.

# 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 primary IP address for the system 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 inherit this functionality automatically. 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.

## 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 bound to its allocated virtual IP address (or loopback address) automatically, 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 virtual IP address of the session. Applications that try to get the IP address of the local server 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 is 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, such as 9000, they are bound to *VIPAddress1:9000* and *VIPAddress2:9000* and there is no conflict.

# To determine whether an application needs to use virtual IP addresses

View applications that bind to specific IP addresses and ports and configure the processes of these applications to use virtual IP addresses.

1. Obtain the TCPView tool from Microsoft. 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 IP address of the server, 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.

# To make virtual IP addresses available to applications running in sessions

Use virtual IP addresses to 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 XenApp 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 to 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 require 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.

---

- At the farm level, configure virtual IP address ranges and assign them to servers. For information, see "To assign virtual IP address ranges to servers".
- Enable applications to use virtual IP addresses. For information, see "To enable application processes to use virtual IP addresses or virtual loopback".

In addition to configuring virtual IP address ranges and enabling applications for use with virtual IP addresses, this feature can control and monitor virtual IP addresses available from each server.

# To assign virtual IP address ranges to servers

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 XenApp servers 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. Add the servers that require virtual IP address functionality that share the same subnet as the address range 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.

Use the Access Management Console to assign a specific address range to each XenApp computer or group of computers. This may be a viable option within environments where the servers span subnets or where insufficient IP addresses exist within the current subnet. You can also modify existing ranges to increase or decrease the number of addresses in the range. When programs running in multiple, concurrent user sessions have problems with TCP port conflicts, the system uses these virtual addresses to assign each user session a unique IP address. Servers with virtual IP disabled appear in the left pane with a red circle and “x” in their icon. When virtual IP is enabled, server icons do not have the red circle or “x.”

1. In the left pane of the Access Management Console, select a farm. Then select **Action > Modify farm properties > Modify Virtual IP properties**.
2. From the **Virtual IP** page, select **Address Configuration**.The **Virtual IP address ranges** list appears. This displays the ranges defined for the farm, the servers assigned to the range, and the number of assigned addresses for each server.
3. Use the **Address Configuration** dialog box to configure the virtual IP address ranges and assign them to servers. Use the buttons provided to configure the ranges:
    - **Add IP Range**. Allows you to define a new range of IP addresses. Make sure all addresses in the range are valid and on the same subnet as the XenApp server. Specifically, do not include:
        - IP addresses in use by other devices on the network
        - Broadcast addresses

- **Configure Servers**. Opens a dialog box to add or remove servers in the selected range and modify the number of addresses assigned to each server.

4. Select the **Enable logging of IP address assignment and release** check box to log IP address assignments and releases in the system's application log (not selected by default). This information includes virtual IP addresses, user names, and session IDs. Clear the check box to remove information from the log.

---

**Important:** When you finish, restart all affected servers to apply the changes.

---

By default, servers use the settings selected for the farm. To customize the setting for individual servers, use the **Server Properties** page to override the farm settings. For more information, see "To configure virtual IP addresses and virtual loopback on an individual server".

After configuring virtual IP address ranges, continue by specifying the application processes that are enabled to use virtual IP addresses. For more information, see "To enable application processes to use virtual IP addresses or virtual loopback".

## To enable application processes to use virtual IP addresses or virtual loopback

After you configure virtual IP addresses or virtual loopback for a farm, continue by specifying the application processes (that is, the executables that run the applications) that can use the virtual IP addresses or virtual loopback.

---

**Note:** For more information about when to use virtual IP or virtual loopback, see "Making Virtual IP Addresses Available to Applications".

---

You configure the virtual IP feature for application processes through the **Process Configuration** page of the Access Management Console. This page displays two lists of processes that are enabled for virtual IP and virtual loopback, respectively.

1. In the left pane of the Access Management Console, select the farm.
2. Select **Action > Modify farm properties > Modify Virtual IP properties**.
3. From the **Virtual IP** page, select **Process Configuration**.
4. In the **Processes Configuration** dialog box, use the buttons to control lists of processes to which the server provides virtual IP and loopback addresses.

The **Add Process** option allows you to type the executable name to add the process to the list. You can add executables to one or both lists. (Do not specify the path; specify only the executable name.)

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.

# To supply client IP addresses to published applications on a server

Use 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. 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\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\VIPHook\Processname`

On XenApp, 32-bit Edition, this entry is:`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.

---

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, configure the session to use the IP address of the client device.

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\Wow6432Node\Citrix\VIP\

     Name: UseClientIP

     Type: REG_DWORD

     Data: 1 (enable) or 0 (disable, which is the default)

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP\

     Name: HookProcessesClientIP

     Type: REG_MULTI_SZ

     Data: multiple executable names representing application processes that use client IP addresses

**Note:** On XenApp, 32-bit Edition, these entries are found in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP\.

3. Close regedit and restart your server.
4. After making the prescribed registry modifications, add the application process. For instructions, see "To enable application processes to use virtual IP addresses or virtual loopback".

   Do not configure the use of client IP addresses if:

   - Plugins connect using network protocols other than TCP/IP
   - Plugins reconnect to disconnected sessions from different client devices
   - Sessions use a pass-through plugin

# To make a virtual loopback address available to applications running in sessions

Use virtual loopback to provide published applications with loopback addresses to use in sessions hosted on a server. An administrator can publish applications that require separate loopback addresses per session. Users of these applications can access them on XenApp servers in the same way that they access any other published application. Use virtual IP addresses or virtual loopback for applications that fail or do not behave properly when running in multiple, concurrent user sessions. These problems occur mainly with in-house or customized applications that have trouble running on Windows Terminal Services.

The behavior of the applications determines whether they use virtual IP or virtual loopback.

---

**Note:** For more information about when to use virtual loopback and virtual IP addresses, see “Making Virtual IP Addresses Available to Applications” on page 69.

---

1. At the farm level, enable virtual loopback on servers. For information, see “To enable or disable virtual loopback for a farm”.
2. Enable application processes to use virtual loopback. For information, see “To enable application processes to use virtual IP addresses or virtual loopback”.

After you configure virtual loopback on your servers, control and monitor this feature at the server level. For information, see “To configure virtual IP addresses and virtual loopback on an individual server”.

# To enable or disable virtual loopback for a farm

You configure virtual loopback for the servers in a farm through the **Loopback Configuration** page of the Access Management Console. You have the option to configure this feature for specified servers or all servers associated with a farm.

1. In the left pane of the Access Management Console, select a farm. Then select **Action > Modify farm properties > Modify Virtual IP properties**.
2. On the **Virtual IP** page, select **Loopback Configuration**.
3. Select the servers in the list for which you want to enable virtual loopback and click **Add**, or click **Add All** to enable virtual loopback on all servers in the farm.
4. Select **Include subfolders** if you want to configure servers contained in subfolders.

5. To disable virtual loopback, select a server in the **Selected items** list and click **Remove**, or click **Remove All** to disable virtual loopback on all the servers in the farm.

After configuring virtual IP loopback on your servers, continue by specifying the application processes on each server for which you want virtual loopback available. For instructions to enable applications for virtual loopback use, see "To enable application processes to use virtual IP addresses or virtual loopback".

After enabling the option for the farm, see "To configure virtual IP addresses and virtual loopback on an individual server".

## To configure virtual IP addresses and virtual loopback on an individual server

After you configure virtual IP address ranges or virtual loopback at the farm level, use virtual IP configuration settings at the server level to:

- Enable and disable the use of virtual IP 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

By default, servers in a farm use the settings defined for the farm. To override the farm setting, configure an individual setting for a particular server. For example, use this feature to temporarily disable the use of virtual IP addresses for a server.

---

**Note:** For more information about when to use virtual loopback and virtual IP addresses, see "Making Virtual IP Addresses Available to Applications".

---

Then configure the options on each server:

1. In the left pane of the Access Management Console, select a server. Then select **Action > Modify server properties > Modify all properties**.
2. From the **Server Properties** list, select **Virtual IP**.
3. On the **Virtual IP** page, if you want to enable virtual IP, select **Enable virtual IP for this server**. This option allows sessions to use virtual IP addresses on the server. Virtual IP addresses are enabled by default when you assign an address range to a server.

**Note:** This option is available only after you enable virtual IP on the **Farm Properties** page and then add this server to one or more address ranges. The list in the dialog box shows the address ranges already defined for the server.

Clear the check box to disable the use of virtual IP addresses for this server. Disabling a server's virtual IP addresses does not affect the assignment of addresses to the server. The assigned addresses remain reserved for the server.

4. If you want to enable logging, select the **Use farm settings for IP address logging** check box.

   By default, servers use the farm setting for logging events to the system's Application log. This option applies the farm setting to the selected server.

   Clear the check box to customize the logging option for the server.

5. If desired, select the **Enable logging of IP address assignment and release on this server** check box.

   This option logs IP address assignments and releases in the system's Application log. This information includes virtual IP addresses, user names, and session IDs.

6. If you want to enable virtual loopback, select the **Enable virtual loopback for this server** check box. This option allows sessions to use virtual loopback on the server (selected by default if you assigned addresses for this server on the **Properties** page for the farm).

# Creating Policies

This topic provides an overview of policies and instructions for setting up policies:

- Creating a policy
- Configuring rules for the policy
- Applying the policy

Related topics:

"Managing Policies" on page 89

"Policy Rules Reference" on page 395

## An Introduction to XenApp Policies

To control user access or session environments, configure a XenApp policy. XenApp policies are the most efficient method of controlling connection, security, and bandwidth settings.

You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple rules. For example, you can configure rules to:

- Control sound quality for client devices
- Allow users to access the Documents folder on their local client device
- Route print jobs from specific workstations directly from the server to the printer, rather than through the client device
- Set a required encryption level for specific Citrix XenApp Plugins
- Direct users to connect to servers in a specific remote zone in the event of failure
- Set the session importance level, which, along with the application importance level, determines Resource Allotment for Preferential Load Balancing

If you create more than one policy in your environment, make sure that you prioritize the policies so that it is clear, if there is conflict, which policy should take precedence.

In Citrix products, Citrix policies always supersede all other policies and settings in your environment, including Active Directory policies and Windows settings.

# Configuring XenApp Policies

The process for configuring policies is:

1. Create and name the policy.
2. Configure policy rules.
3. Apply the policy to connections by filtering according to access control, client IP address, client name, servers, and users.
4. Prioritize the policy.

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.

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

## Creating XenApp Policies

Before you create a policy, decide which group of users or devices you want it to affect. You may want to create a policy based on user job function, connection type, client device, or geographic location. Alternatively, you can use the same criteria that you use for Windows Active Directory group policies.

If you already created a policy that applies to a group, consider editing the policy and configuring the appropriate rules instead of creating another policy. Avoid creating a new policy solely to enable a specific rule or to exclude the policy from applying to certain users.

This topic includes procedures for using the Citrix Advanced Configuration tool, included in the installation media, to configure policies; however, you can also use the XenApp Management SDK (MPSSDK) for this purpose. For information about the XenApp Management SDK, see the Citrix Developer Network.

### To create a policy

1. In the Advanced Configuration tool, select **Policies** in the left pane and select **Actions** > **New** > **Policy**.

2. In the **New Policy** dialog box, enter the policy name and, optionally, a description. Consider naming the policy according to who or what it affects; for example, Accounting Department or Remote Users.
3. If you want to use a preconfigured set of rules for the policy, select **Optimize initial policy settings for a connection type** and select the connection type from the drop-down list. The rules are optimized for:
   - **WAN**. Configures policy rules suitable for most networks.
   - **Satellite**. Configures policy rules suitable for high latency conditions.
   - **Dial-up**. Configures policy rules suitable for low-bandwidth, high latency conditions.

### To edit a policy

1. In the Advanced Configuration tool, select **Policies** in the left pane.
2. Right-click the name of the policy you want to edit and select one of the following:
   - **Edit Description**
   - **Rename Policy**
   - **Properties**

## Configuring Policy Rules

Policies contain rules that define and configure connection settings to be applied when the policy is enforced. Policy rules can be enabled, disabled, or not configured. By default, most rules are not configured. Rules are applied only when they are enabled.

### To configure policy rules

1. In the Advanced Configuration tool, select the policy, then select **Actions > Properties**.
2. Expand the folders to view the rules you can apply.
3. Decide how to use rules in the policy and change their state accordingly. Policy rules can be in one of three states:
   - **Not Configured**. By default, most rules are not configured, meaning they are ignored when users log on to the server. If you want to disable a rule in this policy but you want to be able to enable this rule in a lower-ranked policy, select **Not Configured**.
   - **Enabled**. Adds the rule to the policy and allows you to set the rule options in the details pane.

- **Disabled**. Explicitly disallows the rule. If you disable a rule, it is not enabled in any lower-ranked policies. Disabling a feature's rule **does not** enable the inverse of the rule. That is, you cannot turn a feature on in the product by disabling its rule.

The policy rule changes come into effect the next time the relevant users establish a connection, provided you already applied the policy by enabling a filter.

# Applying Policies

For a policy to become active, you must create a filter for it so the server can apply it to matching connections.

You can create filters based on a combination of the following criteria:

- IP address of the client device used to connect to the session
- Name of the client device from which the session is connected
- User or group membership of the user connecting to the session
- Server hosting a session
- Access control through which a client is connecting to a session

You can add as many filters as you want to the policy. The policy is applied only to connections that meet all filtering conditions.

When a user logs on, all policies that match the filters for the connection are identified. XenApp sorts the identified policies into priority order, compares multiple instances of any rule, and applies the rule according to the priority ranking of the policy.

Any rule that is disabled takes precedence over a lower-ranked rule that is enabled. Policy rules that are not configured are ignored.

## To apply a policy

You must add at least one filter to a policy for that policy to be applied.

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **Contents** tab, select the policy you want to apply.
3. From the **Actions** menu, select **Policy > Apply this policy to**.

4. In the **Policy Filters** dialog box, configure filters:
   A. From the policy filters list, select a filter for the policy. You can filter based on:
      - **Access Control**. See "To apply a policy filter based on existing Access Gateway policies" on page 92 for details.
      - **Client IP Address**. See "To filter based on client IP address" on page 85 for details. If you are concerned about network access and identity and want to use filters to enforce your security goals, Citrix does not recommend filtering by client IP address, because a malicious user can change the IP address reported by the client.
      - **Client Name**. See "To filter based on client name" on page 87 for details. If users can change the name of their client devices, you may not want to filter policies by client device name. If you are concerned about network access and identity and want to use filters to enforce your security goals, Citrix does not recommend filtering by client device name, because a malicious user can change the IP address reported by the client.
      - **Servers**. See "To filter based on servers" on page 86 for details.
      - **Users**. See "To filter based on users" on page 86 for details.
   B. To enable the filter for the policy, select **Filter based on *type of filter***.
   C. Repeat these steps for each filter you want to apply.

The policy is applied the next time the relevant users establish a connection.

## To filter based on client IP address

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **Contents** tab, select the policy you want to apply.
3. From the **Actions** menu, select **Policy > Apply this policy to**.
4. In the **Policy Filters** dialog box, select **Client IP Address**.
5. Select **Filter based on client IP address**.
6. Select one of the following:
   - **Apply to all client IP addresses** to apply this policy to all connections. To add most but not all addresses, select **Apply to all client IP addresses** and then create exceptions. To create exceptions, add the addresses to which you do not want the policy to apply, then select **Deny** for each address.

- **Add** to add specific client addresses. Make sure **Allow** is selected for each address or range chosen.

## To filter based on servers

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **Contents** tab, select the policy you want to apply.
3. From the **Actions** menu, select **Policy > Apply this policy to**.
4. In the **Policy Filters** dialog box, select **Servers**.
5. Select **Filter based on servers**.
6. To specify servers to which you do not want to apply this policy, from the check mark drop-down list beside the server name, select **Do not apply to this server.**

---

**Important:** If you filter a policy based on a server, the **Configure delivery protocol** policy rule, which is used to configure the Citrix application streaming feature, does not apply. For more information about application streaming, see the *Citrix Application Streaming Guide*.

---

## To filter based on users

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **Contents** tab, select the policy you want to apply.
3. From the **Actions** menu, select **Policy > Apply this policy to**.
4. In the **Policy Filters** dialog box, select **Users**.
5. Select **Filter based on users**.
6. Use the controls to apply the policy to all users, all explicit users, all anonymous users, or a list of users.

---

**Tip:** You can add users or groups by clicking **Add List of Names** or using the **Look in** list box. The **Look in** list box locates all trusted account authorities configured on the farm servers, including Novell Directory Services (NDS) trees, Active Directory domains, and local servers.

---

To add a list of names in the **Add List of Names** dialog box, do one of the following:

- Enter the user names you want to add. Separate user names with a semicolon.

- Enter Windows NT Domain account names in the “domain\account” format and Active Directory account names in the “account@example.company.com” format.

  **Important:** To use Active Directory Domain Local Groups and Universal Groups, your server farm must meet specific network configuration conditions. For more information, see the *Citrix XenApp Installation Guide*.

- If NDS is enabled, enter NDS account names in the “ndstree\account” format, where account is the distinguished name of the account.

  **Note:** When adding NDS users, you must have rights to edit farm settings. Use the **Look In** list to assign NDS users to objects in any area of management; for example, applications to which you want them to have access.

## To filter based on client name

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **Contents** tab, select the policy you want to apply.
3. From the **Actions** menu, select **Policy > Apply this policy to**.
4. In the **Policy Filters** dialog box, select **Client Name**.
5. Select **Filter based on client name**.
6. Select one of the following:

   - **Apply to all client names** to apply this policy to all connections. To add most but not all client names, select **Apply to all client names** and then create exceptions. To create exceptions, add the client names to which you do not want the policy to apply, then select **Deny** for each name.
   - **Add** to add specific client names. Make sure **Allow** is selected for each name chosen.

     In the **Add Client Name to Policy Filter** dialog box, you can include wildcard characters.

**Important:** Web Interface client names are assigned randomly with a prefix of WI_; therefore, specific client names cannot be anticipated. To filter Web Interface connections by client name, use the wildcard expression WI_*. Consider using client name filtering in conjunction with IP address filtering for users who access XenApp servers from the Web Interface.

# Managing Policies

This topic discusses how to manage policies. The topic covers:

- Policy rules you might want to enable during your initial farm deployment
- Prioritizing policies and creating exceptions to them
- Troubleshooting conflicting rules in policies

Related topics:

"Creating Policies" on page 81

"Policy Rules Reference" on page 395

## Configuring Initial Policy Rules

When you first deploy XenApp, you may want to configure some initial policy rules. Some examples of initial rules include:

- "Configuring Client Device Settings" on page 90
- "Setting Printing Policy Rules" on page 90
- "Changing Settings Based on User Location" on page 90
- "Configuring Policies and Filters for Web Access" on page 91
- "Enabling Scanners and Other TWAIN Devices" on page 101
- "Displaying Local Special Folders in Sessions" on page 110
- "Using Session Shadowing to View a User Session" on page 130

Citrix recommends the following best practices:

- Assign user policies to groups rather than individual users. If you assign user policies to groups, assignments are updated automatically when you add or remove users from the group.

- Do not enable conflicting or overlapping settings in Terminal Services Configuration tool or in the farm settings of the Access Management Console. In some cases, the Terminal Services Configuration tool and the farm-wide settings in the Access Management Console provide similar functionality to XenApp policy rules. When possible, keep all settings consistent (enabled or disabled) for ease of troubleshooting.
- Disable unused policies. Policies with all the rules set to Not Configured create unnecessary processing.
- Set unused policy rules to Not Configured. Disabling unused policy rules disables the rule in all policies lower ranked policies.

# Configuring Client Device Settings

You can configure policies that control users' access to their client devices during sessions. For example, you can use the mappings rule to prevent remote users from being able to save to their hard drives from a session. You can also disable the Windows clipboard or disable ports.

In addition, you can use the Client Device rules, such as sound quality, to limit quality, control overall performance, or turn off speakers.

Related topics:

"Client Devices Folder" on page 405

# Setting Printing Policy Rules

Many printing features are implemented through printing policies. There are policies for:

- "Auto-Creation" on page 411
- "Legacy Client Printers" on page 412
- "Printer Properties Retention" on page 412
- "Print Job Routing" on page 413
- "Turn Off Client Printer Mapping" on page 413

# Changing Settings Based on User Location

You can use multiple policies to selectively apply XenApp settings to users tailored to how they connect.

For example, you may have staff members who download high resolution graphics. You can create two policies, one that enables compression when users employ dial-up connections, and one that disables compression when they use high-speed connections.

### To create policies to customize the user experience based on how users connect

1. Determine how you want policy rules to apply to specific connections. For example, you may want to enable compression for everyone except those connecting from a specific IP address range.
2. Create policies for the connections to which you want to apply specific rules.
3. Use filters to set conditions that a connection must meet for a policy to be applied. For example, when you assign an IP address range filter to a policy, that policy applies only to connections in that IP address range. A user's connection must meet all filtering conditions in a policy for that policy to be applied to the user's session.
4. Prioritize policies so that rules are applied in the correct order. For example, rank a policy that disables compression for specific IP addresses higher than the policy that enables compression for everyone in general.
5. Use Search to confirm how final policy rules are merged for a specific connection. Search calculates the final rule settings for any combination of a user, group, and IP address after the rules' priorities are taken into account.

## Configuring Policies and Filters for Web Access

You can create a policy that is applied to Access Gateway connections or to Access Gateway connections with certain properties.

You can create XenApp policies to accommodate different access scenarios based on factors such as authentication strength, logon point, and client device information such as endpoint analysis. For example, you can include endpoint analysis information collected by Access Gateway Advanced Edition within a XenApp policy to determine access to a published application. You can selectively enable client-side drive mapping, cut and paste functionality, and local printing based on the logon point used to access the published application.

For example, you might define a filter in Access Gateway that is applied if antivirus software is not installed on the client device. Then in XenApp, you can create a policy and set its rules so that client drive mapping is turned off. Next, you can apply the policy to connections that meet the Access Gateway filter. This prevents users who do not have the antivirus software running on the client from having their client drives mapped.

**Prerequisites for Filtering on Access Gateway Connections**

For Citrix XenApp to filter on Access Gateway connections, you must complete all of the following:

- Create one or more filters within Access Gateway Advanced Edition. See the *Administrator's Guide for Access Gateway Enterprise* for more information about creating filters.

---

**Note:** You must be using Access Gateway with the Access Gateway Advanced Edition (Version 4.0 or later) to create filters that work with XenApp.

---

- Select **Allow connections made through Access Gateway Advanced Edition** for published applications.
- On each server, select **Trust requests sent to the XML Service**.
- Ensure that your farm is configured to allow Access Gateway connections, which it is by default.
- Create policies within XenApp that reference Access Gateway Advanced Edition filters.

## To apply a policy filter based on Access Gateway connections

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. Select an existing policy or create a new policy for the access control filter.
3. From the **Actions** menu, select **Policies** > **Apply this policy to**.
4. In the left pane, select **Access Control**.
5. Select **Filter based on Access Control**.
6. Select **Apply to connections made through Access Gateway**.
7. Select **Any connection** to apply this policy to connections made through Citrix Access Gateway servers (Version 4.0 or later) without considering Access Gateway policies.

## To apply a policy filter based on existing Access Gateway policies

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. Select an existing policy or create a new policy for the access control filter.
3. From the **Actions** menu, select **Policies** > **Apply this policy to**.
4. In the left pane, select **Access Control**.

5. Select **Filter based on Access Control**.
6. Select **Any connection that meets any of the following filters**.
7. Click **Add**. The **Add Access Gateway Filter** dialog box appears.
8. In the **Access Gateway farm** list box, enter the name of the Access Gateway farm.
9. In the **Access Gateway filter** list box, select the Access Gateway policy for XenApp to use.

**Important:** XenApp does not validate Access Gateway farm and filter names, so always verify the names with the Access Gateway administrator.

### To apply a policy to every connection except those based on Access Gateway

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. Select an existing policy or create a new policy for the access control filter.
3. From the **Actions** menu, select **Policies** > **Apply this policy to**.
4. In the left pane, select **Access Control**.
5. Select **Filter based on Access Control**.
6. Select **Apply to all other connections**. Doing so applies this policy to all connections except those made through Access Gateway (Version 4.0 or later).

## Using Multiple Policies

You can use multiple policies to tailor XenApp 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 sessions and prevents users from saving 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 effective policy when policies conflict.

In general, policies override similar settings configured for the entire server farm, for specific servers, or on the client. The exception to this principle is security. The highest encryption setting in your environment, including the operating system and the most restrictive shadowing setting, always overrides other settings and policies.

XenApp policies interact with policies you set in your operating system. Some Windows policies take precedence over XenApp policies. For some policy rules, such as Secure ICA, the settings in policies must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the settings that you specify in the Secure ICA policy or when you are publishing an application can be overridden.

For example, the encryption settings that you specify when you are publishing an application should be at the same level as the encryption settings you specified throughout your environment.

# Using Citrix policies with Active Directory

Active Directory and Windows policies do not take precedence over XenApp policies. In a XenApp environment and with XenApp features, Citrix policies always take precedence over Windows policies and settings. Citrix designed XenApp policies so that they do not conflict with Active Directory policies.

In a Citrix environment, XenApp policy rules override the same settings configured in an Active Directory policy or using the Terminal Services Configuration tool. They also override Microsoft policies, including those that are related to typical Remote Desktop Protocol (RDP) client connection settings such as the policies for Desktop wallpaper, Menu animations, and Windows contents while dragging.

However, XenApp policy rules do not always override policies for encryption and shadowing. These policies behave according to the most restrictive settings configured by the Terminal Services Configuration tool, Active Directory group policies, application configuration, and Citrix policies.

If you are familiar with Active Directory, note these important distinctions:

- For Active Directory policies, the disabled setting affects how the feature functions. That is, it disables or enables the feature.
- For XenApp policies, the disabled setting only prevents a lower-priority policy from being able to enable the policy rule. Disabling a XenApp policy rule does not disable its corresponding feature in the product.

# Prioritizing Policies and Creating Exceptions

Prioritizing policies allows you to define the precedence of policies when they contain conflicting rules. The process XenApp uses to evaluate policies is as follows:

1. When a user logs on, all policies that match the filters for the connection are identified.
2. XenApp sorts the identified policies into priority order and compares multiple instances of any rule, applying the rule according to the priority ranking of the policy.

You prioritize policies by giving them different priority numbers. By default, new policies are given the lowest priority. If policy settings conflict, 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 disabled rule overrides a lower-ranked rule that is enabled. Policy rules that are not configured are ignored and do not override the settings of lower-ranked rules.

When you create policies for groups of users, client devices, 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.

## Sample Process for Prioritizing Policies and Creating Exceptions

In this example, you work for a company that has an existing policy for its 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 example illustrates the process of creating a new policy for Accounting group members Susan and Brian 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.

1. Determine which users need exceptions.

   In this example, Brian and Susan need exceptions to the Connection rule (**Resources** > **Drives** > **Connection**).

2. Determine which rules you want to apply to these users.

   All the rules in this policy apply to Susan and Brian, except the Connection rule, which prevents access to local drives.

3. Create a new policy based on the existing policy by selecting the Accounting Profile policy, then selecting **Actions > Policy > Copy Policy**.
4. Rename the policy "Accounting Profile — local drive access" by selecting the new policy, then selecting **Actions > Policy > Rename Policy**.
5. Edit the description of the policy by selecting the policy and choosing **Actions > Policy > Edit Description**.

   Enter a meaningful description, such as "Excludes Brian and Susan from local drive access policy."
6. Open the policy's property sheet and locate the Connection rule. Set the rule to **Disabled**.
7. Assign Susan and Brian to the new policy:
   A. Select the new policy and choose **Actions > Policy > Apply this policy to**.
   B. In the **Policy Filters** dialog box, select **Users**, then select **Filter based on users**.
   C. Open domains or user groups in the **Look in** box until the user accounts for Susan and Brian appear and add them to the **Configured Accounts** box.
   D. Leave the **Allow Deny** option in the **Configured Accounts** box set to **Allow**.
8. Rank the "Accounting Profile - local drive access" policy higher than the "Accounting Profile" policy. By default, new policies are given the lowest rank. 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.

## To display the priorities of all policies

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. From the **View** menu, select **Details**.

## To give a policy a higher priority

1. Select the policy.
2. From the **Actions** menu, select **Policy > Priority**.
3. Select **Increase Priority** until the policy has the preferred rank.

# Determining Which Policies Apply to a Connection

Depending on the filters you applied to a policy, sometimes more than one policy applies to a connection so that connection may not respond in the way you expect. If a higher priority policy also applies to a connection, it can override the rules you set in the original policy. Use the Policy Search feature to:

- Find all policies that can apply to a specific connection
- Determine how final policy rules are merged for the connection (that is, determine the resultant policy)

To find out which policies apply to connections, you can search by specifying the same filters that are used to apply policies, adding more search filters if necessary.

If the expected policies are not listed in the Search results, check the filters assigned to the policies and your search criteria. For example, verify that you have the **Allow** option set for a configured account within a user filter assigned to a policy.

## To discover which policies apply to a connection

1. From the **Actions** menu, select **Search**.
2. In the **Search Criteria** list, select a filter name.

   You can narrow the selection by defining multiple search criterion.
3. Click **Edit**.
4. Do one of the following, depending on the search criteria you selected:

   - **Enter Access Control Search Criteria**. Select an Access Control connection to find all policies that match or partially match this connection type.
   - **Enter Client IP Search Criteria**. Select a client IP address to find all policies with filters that match or partially match this address.
   - **Enter Client Name Search Criteria**. Select a client name to find all policies with filters that match or partially match this name.
   - **Enter Server Search Criteria**. Select a server to find all policies with filters that match or partially match this server.
   - **Enter User Search Criteria**. Select a user or group to find all policies with filters that match or partially match this name.

     If you search to see which policies apply to a domain user, the search results do not list any policies that are applied to any local groups of which the user is a member.
5. Click **Search**.

   Accept any prompts that appear. The results appear in the **Search Results** display at the bottom of the dialog box.
6. Do one of the following:

   - Resolve partial matches, as described in "Resolving Search Results that Partially Match Criteria" on page 98.
   - Display the resultant policy, as described in "Troubleshooting Policies with Conflicting Rules" on page 99.

## Resolving Search Results that Partially Match Criteria

When you use the Search feature to discover which policies apply to a connection, the results list all policies that match or partially match the search criteria that you selected.

When the search criteria that you selected match some, but not all, of the Search feature's filtering criteria, that policy is shown as a *partial match*.

The procedure that follows explains how to resolve partial matches. You can eliminate partial matches when you locate all valid matches for the connection about which you want information.

### To resolve search results that partially match search criteria

This procedure assumes that you performed a search and the search results included a policy that partially matches the search criteria.

1. Right-click the policy in the **Search Results** pane and select **Why is this policy a partial match?**
2. Return to the **Search** dialog box and supply any additional search criteria to the connection about which you want information.
3. Do one of the following:
   - Eliminate partial matches when you locate all valid matches for the connection about which you want information
   - If a message appears saying that no rules are configured for a policy, see "When No Policy Rules are Configured" on page 100 for further details

---

**Note:** Partial matches might make some of the resultant policy settings appear in an indeterminate state. However, settings that are not affected by the partially matched policies still appear normally.

---

## Troubleshooting Policies with Conflicting Rules

Because rules set in some policies can conflict with rules set in others and policies can have multiple filters, a policy may not behave in the way you expect or it may not run at all. Users, IP addresses, and other filtered objects can have more than one policy that applies to them simultaneously. When this happens, XenApp merges these policies' rules to form, in effect, a new policy resulting from the existing ones. This combination of rules is known as the *resultant* policy. When there are multiple policies that can apply to a session, it is the resultant policy that XenApp enforces.

If you have multiple policies in your environment and you are having trouble figuring out why a policy won't run, Citrix recommends that you determine the resultant policy.

### To determine a resultant policy

1. Search to determine which policies apply to a connection. See "To discover which policies apply to a connection" on page 98.
2. In the **Search results** dialog box, make sure partial matches are not selected in the **Include** column, then select **View Resultant Policy**.

### When No Policy Rules are Configured

When a resultant policy does not contain any configured rules, users connecting to their applications under conditions that match the search criteria are not affected by any policy rules.

When you perform a search, you can end up with a resultant policy that has no configured rules when:

- No policies have a filter set that matches the search criteria
- Policies that match the filter do not have any rules configured
- Policies that match the filter have their rules disabled

If you want to apply policy rules to the connections that meet the specified criteria:

- Make sure the rules that you want to apply to those connections are enabled
- Rank the policy that you want to apply higher than other policies

## To delete a policy

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. In the **Contents** tab, select the policy you want to delete.
3. From the **Actions** menu, select **Policy** > **Delete Policy**.

## To disable a policy

1. In the left pane of the Advanced Configuration tool, select **Policies**.
2. In the **Contents** tab, select the policy you want to disable.
3. From the **Actions** menu, select **Policy** > **Disable Policy**.

   The policy appears in the right pane with an orange bar through it.
4. To reenable a policy, select **Policy > Enable Policy**.

# To reenable a policy

Select the policy you want to reenable and from the **Actions** menu, select **Policy** > **Enable Policy**.

# Enabling Scanners and Other TWAIN Devices

XenApp lets users control client-attached TWAIN imaging devices, such as scanners and cameras, from published applications. This feature is known as *TWAIN redirection* because XenApp provides TWAIN support by redirecting commands sent from a published application on the server to the client device.

Users can connect regardless of connection type. However, XenApp requires the following for TWAIN support:

- The imaging device must be connected locally to the client and have the associated vendor-supplied TWAIN driver installed locally.
- Citrix Presentation Server Client Version 9.*x* or later, the Citrix XenApp Plugin for Hosted Apps, or the Citrix XenApp Plugin for Streamed Apps.
- XenApp 32-bit and 64-bit servers support TWAIN redirection for 32-bit TWAIN applications only. XenApp does not support 16-bit TWAIN drivers.
- The Configure TWAIN redirection policy rule must be enabled.

The following table lists the TWAIN hardware and software tested with XenApp. While other TWAIN devices may work, only those listed are supported.

| | |
|---|---|
| Scanners and Scanning Devices | Canon CanoScan 3200F |
| | Canon CanoScan 8000F |
| | Canon CanoScan LiDE600F |
| | Epson Perfection 3170 Photo |
| | Fujitsu fi-6140 |
| | HP Office Jet 7130 All-In-One |
| | HP ScanJet 8250 |
| | HP ScanJet 8290 |
| | Microtek ScanMaker 5950 |
| | Visioneer OneTouch 9320 |
| | Xerox DocuMate 510 |

| | |
|---|---|
| Web/Digital Cameras | D-Link VisualStream DSB-C310 PC Camera |
| | Logitech QuickCam Messenger |
| Software | Adobe Acrobat Capture |
| | Adobe Pagemaker 7.0 |
| | Corel Paint Shop Pro |
| | Microsoft Digital Image Suite 9 |
| | Microsoft Digital Image Suite 10 |
| | Microsoft Office Document Scanning |
| | Microsoft Office Publisher 2003 |
| | Microsoft Office Publisher 2007 |
| | Microsoft Picture It! |
| | OmniPage SE Version 2.0 |

## To enable the configuration of TWAIN redirection

1. In the Advanced Configuration tool, 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 XenApp server.
- Image acquisition software that provides the USB device drivers must be installed on the client platform.
- 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, type the following text in 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.

---

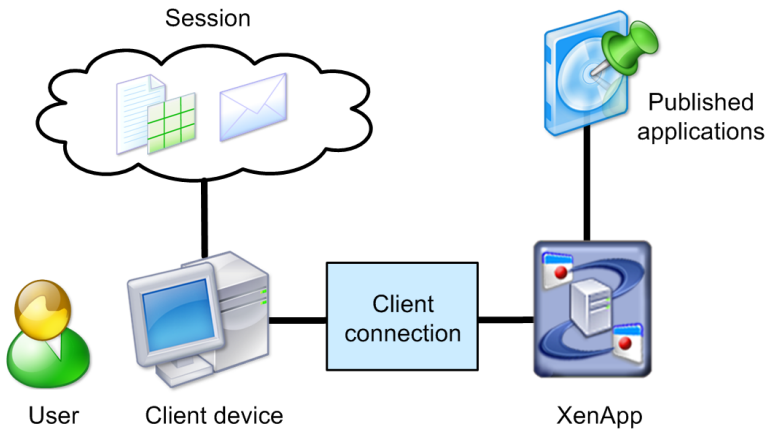
# Managing Session Environments and Connections

This topic explains how to provide user access to your server farm's resources by:

- Customizing user environments
- Controlling connections
- Monitoring, managing, and optimizing sessions

## Session Environments and Connections

When a user initially connects to your farm and opens a published application, the server opens the application in a session. In XenApp, the term *session* refers to a particular instance of a user's activity on the server; sessions are the virtualization of the user's environment.




*Users access published applications in sessions after the client device establishes a connection with the server.*

When a user logs on to the farm, the client device links to the server through a connection and establishes a session. This connection is known as the *client connection*. Users access published resources through client connections, inside of sessions.

As an administrator, you can customize users' environments, including whether or not users can access mapped drives, such as the local client device's hard disk; if they can access local special folders, the printers that are available, and the amount of bandwidth used for audio support. You can change these settings based on the location from where the users are connecting.

XenApp provides settings to ensure sessions remain reliable. You can also monitor users' sessions, and their sessions' status, by shadowing.

Related topics:

"Defining User Environments in XenApp" on page 106

"Managing and Monitoring XenApp Sessions" on page 127

"Controlling Client Connections in XenApp" on page 140

"Optimizing User Sessions for XenApp" on page 148

"XenApp Printing Concepts" on page 222

# Defining User Environments in XenApp

XenApp provides different ways to control what users experience in their session environments. You can customize user environments in the following ways:

- By suppressing the number of progress bars users see when they first open an application, so that XenApp appears to be more seamlessly part of their environment.
- By either allowing or preventing users from accessing their local devices or ports during a session. You can also prevent users from accessing devices and ports during remote sessions.
- By defining whether or not users can hear audio or use microphones during sessions. If you enable audio support, you can specify the level of audio compression and limit bandwidth, if necessary. You can control audio either at the group level through policies or at the published application level.
- By ensuring that mobile workers, such as travelling salespeople or workers inside a hospital, always have the most appropriate printers and devices available to them inside of a session.

For Citrix XenApp Plugin for Hosted Apps, you can also customize the user's experience by choosing whether you want published applications and desktops to appear in a window within a Remote Desktop window or "seamlessly." In seamless window mode, published applications and desktops appears in separate resizable windows, which make the application appear to be installed locally. Certain features are available only in seamless mode.

Some features that relate to session environments or connections, such as dual-monitor mode support and information about logons, are plugin specific. Details are in the *XenApp Plugin for Hosted Apps for Windows Administrator's Guide* and the *Web Interface Administrator's Guide*.

Related topics:

"Controlling the Appearance of User Logons" on page 107

"Controlling Access to Devices and Ports" on page 108

"Configuring Audio for User Sessions" on page 114

"Ensuring Session Continuity for Mobile Workers" on page 119

# Controlling the Appearance of User Logons

When users connect to a server, they 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.

XenApp 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, XenApp 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, Active Directory group policies take precedence over equivalent *local* group policies on servers. Therefore, when you install XenApp on servers that belong to an Active Directory domain, those Active Directory policies may prevent XenApp 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 these group policies in Active Directory.

# Controlling Access to Devices and Ports

Citrix XenApp Plugin for Hosted Apps supports mapping devices on client computers so users can access the devices within sessions. Client device mapping provides:

- Access to local drives and ports
- Cut-and-paste data transfer between a session and the local clipboard
- Audio (system sounds and .wav files) playback from the session

During logon, the plugin informs the server of the available client drives and COM ports. By default, client drives are mapped to server drive letters so the drives appear to be directly connected to the server. These mappings are available only for the current user during the current session. The mappings are deleted when the user logs off and recreated the next time the user logs on.

## Mapping Client Drives

By default, the drives on the client system are mapped automatically to drive letters on the server when users log on. The client's disk drives appear as shared folders with mapped drive letters. These drives are used by Windows Explorer and other applications like any other network drive.

In general, XenApp tries to match the client drives to the client drive letters; for example, the client device's first floppy disk drive to A, the second floppy disk drive to B, the first hard disk partition to C, and so forth. This allows the user to access client drive letters in the same way locally and within sessions.

However, the same drive letters are often in use by the drives on the 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 XenApp. Similarly, you can turn off mapping to client floppy disk drives, hard drive, CD-ROM drives, or remote drives.

If access to the floppy disk drives is not needed, consider disabling access to speed up the logon process.

As a security precaution, when a user logs on to XenApp, by default, the server maps client drives without user execute permission. For users to be able to execute files residing on mapped client drives, override this default by editing the value of **ExecuteFromMappedDrive** in the registry on a XenApp 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.

Related topics:

"Mappings" on page 407

### To change the ExecuteFromMappedDrive registry setting

1. After installing XenApp, 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**. This is the default setting.

   To deny users execute permission on mapped drives, set **ExecuteFromMappedDrive** to **0**.
4. Restart the server.

## Mapping Client COM Ports and Audio

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 mapped automatically to server ports at logon, but can be mapped manually using the **net use** or **CHGCDM** commands.

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 client COM port and audio mapping, see the administrator's guides for the plugins you plan to deploy.

Related topics:

"Creating Policies" on page 81

# Displaying Local Special Folders in Sessions

To make it easier for your users to save files to their special folders locally, you can enable Special Folders Redirection. *Special folders* is a Microsoft term that refers to Windows folders such as **Documents**, **Computer**, and the **Desktop**.

---

**Note:** For the purpose of consistency in this topic, special folders are referred to in the style of Windows Vista. For example, **Documents** and **Computer**. In Windows XP, these special folders were known as **My Documents** and **My Computer**.

---

Without Special Folder Redirection enabled, the **Documents** and **Desktop** icons that appear in a session point to the user's Documents and Desktop folders on the server. Special Folder Redirection *redirects* actions, such as opening or saving a file, so that when users save or open files from special folders, they are accessing the special folder on their local computers. In addition, for the Citrix XenApp plugin, the Documents folder in the **Start** menu maps to the Documents folder on the client device.

## Requirements

To use Special Folder Redirection, users must access the farm with the Citrix XenApp Plugin 11.*x* or the Web Interface.

## Restrictions

Do not enable Special Folders Redirection in situations when a user connects to the same session from multiple client devices simultaneously. For Special Folder Redirection to work, the user must log off from the session on the first client device and start a new session on the second client device. If users must run multiple sessions simultaneously, use roaming profiles or set a home folder for that user in the **User Properties** in Active Directory.

Because Special Folder Redirection must interact with the client device, some settings prevent Special Folder Redirection from working. You cannot have policy rules that prevent users from accessing or saving to their local hard drives.

Currently, for seamless and published desktops, Special Folder Redirection works only for the Documents folder. For seamless applications, Special Folder Redirection only works for the Desktop and Documents folders. Citrix does not recommend using Special Folder Redirection with published Windows Explorer.

Special Folder Redirection requires access to the Documents and Desktop folders on the user's local computer. When a user launches an application through the Web Interface and uses **File Security** to select **No Access** in the **File Security** dialog box in Connection Center, access is denied to the user's local workstation drives, including the user's local Documents and Desktop folders. As a result, some applications might be unstable when trying to perform read/write operations to the denied folders. To avoid this, always grant full local access when Special Folder Redirection is enabled.

---

**Caution:** Special Folder Redirection does not redirect public folders on Windows Vista and Windows Server 2008. If users are connecting to servers that are not in their domain, instruct users not to save to public folders. If users save documents to public folders, they are saving them to a local folder on the server hosting the published application. In large environments where many servers host the same application, it could be difficult to determine which server contains the public folder where the user saved the document.

---

## Enabling

Special Folder Redirection support is enabled by default, but you must provide this feature to users through the Citrix XenApp plugin and Web Interface functions in the Access Management Console. You can either enable Special Folder Redirection for all users or configure that users must enable the feature themselves in their client settings.

You can prevent specific users from having redirected special folders by enabling the **Special folders redirection** policy rule.

The process for enabling Special Folder Redirection is:

1. Enable support for Special Folder Redirection for the clients in your environment through the Access Management Console.
2. Decide if you want to let users turn this feature on and off in their sessions.

   Instructions for users are provided in their plugin help.
3. Exclude users that you do not want accessing local Special Folders by enabling the **Special folder redirection** policy rule in the policies that apply to the users.
4. Ensure you do not have any policy rules enabled that are not supported with Special Folder Redirection:

   - If the Mappings policy rule (**Resources > Drives > Mappings**) is enabled, clear the **Turn off Hard Drives** check box

- If the Connection policy rule (**Resources > Drives > Connection**) is enabled, clear the **Do Not Connect Client Drives at Logon** check box

If you enable Special Folder Redirection without success, use **Search** to determine if any rules are enabled that conflict with this feature.

---

**Tip:** Let your users know that other Special Folders, such as Music or Recent Documents, still point to the server. If users save documents to these folders, they are saved to the server.

---

Related topics:

"To enable Special Folder Redirection" on page 112

"To prevent local special folders from being redirected" on page 113

"Troubleshooting Policies with Conflicting Rules" on page 99

## To enable Special Folder Redirection

This procedure requires that you already created a XenApp Services site or a XenApp Web site.

1. Choose one of these procedures.

| **To enable Special Folder Redirection for the...** | **perform the correct procedure...** |
|---|---|
| Web Interface | 1. In the left pane of the Access Management Console, select **Citrix Resources** > **Configuration Tools** > **Web Interface** > *XenApp Web Site Name*.<br><br>2. From the **Action** menu, choose **Manage session preferences**.<br><br>3. In the Managing Session Preferences page, select **Remote Connection** > **Local Resources**. |
| Citrix XenApp plugin | 1. In the left pane of the Access Management Console, select **Citrix Resources** > **Configuration Tools** > **Web Interface** > *XenApp Services Site Name*> **config.xml**.<br><br>2. From the **Action** menu, choose **Change session options**.<br><br>3. In **Change Session Options**, click **Local Resources**. |

2. Select the correct check box.

| To ... | select the correct check box... |
|---|---|
| Enable Special Folder Redirection by default and let users turn it off in their session options | • **Provide Special Folder Redirection to all users**<br>• **Allow users to customize Special Folder Redirection** |
| Disable Special Folder Redirection by default, but let users turn it on in their session options | • **Allow users to customize Special Folder Redirection** |
| Enable Special Folder Redirection by default and prevent users from turning it on or off | • **Provide Special Folder Redirection to all users** |

Related topics:

"Displaying Local Special Folders in Sessions" on page 110

## To prevent local special folders from being redirected

1. In the Advanced Configuration tool, select the policy that contains the users or devices you want to prevent from seeing local special folders.
2. Choose **Actions > Properties**.
3. Select **Client Devices > Resources > Drives > Special folder redirection**.
4. Select **Enabled**. This prevents special folders from being redirected to the local client device in the sessions to which this policy applies.

---

**Tip:** You can prevent this rule from affecting specific users or devices (for example) in a group by specifying them in the **Configured Accounts** section of the **Policy Filter** dialog box and selecting **Deny**. Selecting **Deny** for these individuals means that their special folders will be redirected.

---

The policy rule changes take effect the next time the affected users establish a connection.

Related topics:

"To filter based on users" on page 86

"Troubleshooting Policies with Conflicting Rules" on page 99

"Sample Process for Prioritizing Policies and Creating Exceptions" on page 95

# Configuring Audio for User Sessions

XenApp provides tools to manage and control the availability of sound in 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 policies 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.

You control the availability of speakers and microphones in sessions with 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 **Options** dialog box (for the Citrix XenApp plugin). 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 topic covers aspects of enabling audio support on servers. To use audio in sessions, users must also enable audio on the client device. For more information about enabling audio for plugins, see the administrator's guides for the specific plugins.

---

When audio is enabled, you can also use policy rules to fine tune compression levels and bandwidth allocation.

---

**Note:** The availability and quality of audio in sessions is determined by Terminal Services (TS Config) settings and policies you configure through the Advanced Configuration tool. By default, Terminal Services settings are configured, whereas XenApp policies are not. This means that Terminal Services settings apply by default, making medium quality audio available in sessions until you configure XenApp policies that override the Terminal Services settings. When configured, XenApp policies override Terminal Services settings.

---

## 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.

## Limiting Bandwidth for Audio Throughput

Use policy rules to configure the amount of bandwidth you want to allocate to audio transfers between servers and client devices. 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

In this procedure, you are editing an existing policy that applies to a specific group of filtered objects, such as servers or users.

1. In the Advanced Configuration tool, select the policy for which you want to configure the rule.
2. From the **Actions** menu, select **Properties**.
3. Expand **Bandwidth**.
4. Select one of these folders:
   - **Session Limits**. Lets you specify the bandwidth available for audio in kilobits per second (for example, 70Kbps).
   - **Session Limits** (%). Lets you limit the bandwidth available for audio to a percentage of the overall bandwidth available.

   **Note:** If you want to specify bandwidth as a percentage using the Session Limits (%) rule, you must enable the Overall Session rule in the Session Limits folder as well.
5. Select **Audio** to configure the rule and enter the bandwidth limit.

## Setting Audio Compression and Output Quality

Generally, higher sound quality requires more bandwidth and higher server CPU utilization. You can use sound compression to balance sound quality and overall session performance. Use policy rules to configure the compression levels you want to apply to sound files.

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

In this procedure, you are editing an existing policy that applies to a specific group of filtered objects (such as, servers and users).

1. In the Advanced Configuration tool, 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.
4. Choose from these 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 device 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.** (Default.) This setting is recommended for most LAN-based connections. This setting causes any sounds sent to the client device 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 client devices 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 client devices and increases server CPU utilization.

## Enabling Microphone and Speaker Support

For users to use speaker and microphones in sessions, both audio input (for microphones) and output (for speakers) must be enabled. Audio input and output are controlled by two separate policy rules; you must configure both to ensure that audio input and output are enabled.

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 lets mobile users record notes from the field, but prevents the server from sending audio to the mobile devices, ensuring better session performance. Enabling audio input and output also enables support for digital dictation.

On the client device, 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 **Options** > **Session Options** dialog box (for the Citrix XenApp plugin).

By default, when you configure this rule, audio input is enabled on client devices. Web Interface users can override the policy and disable their microphones by selecting **No** in the **Audio Security** dialog box, which they access from the Citrix Connection Center.

### To enable audio input for sessions

In this procedure, you are editing an existing policy that applies to a specific group of filtered objects, such as servers or users.

1. In the Advanced Configuration tool, 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**.

**Note:** Microphone input is supported on Citrix XenApp Plugin for Hosted Apps for Windows, Windows CE, and Linux.

### To enable audio output for sessions

1. In the Advanced Configuration tool, 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 device's speakers are turned off because this property is enabled.
4. Select **Disabled**.

## Setting Up for Digital Dictation Devices

If you have enabled microphone and speaker support, XenApp requires no additional configuration to allow users to record audio using a standard microphone. However, to allow users to use digital dictation devices such as Philips SpeechMike devices and dictation software such as WinScribe Internet Author and Internet Typist, you must install and configure the associated software and set session sound quality to accommodate them.

---

**Note:** The plugins for Linux and Windows CE do not support Philips SpeechMike products, nor does XenApp on 64-bit operating systems.

---

To make Philips SpeechMike devices or similar products available in user sessions, install the device drivers associated with the products on the XenApp server and on client devices. Citrix recommends you install Philips SpeechMike device drivers before installing XenApp. To make dictation software such as WinScribe Internet Author and Internet Typist available, install this software on the XenApp server. After installation, you might be required to enable the controls for the dictation device within the dictation software. Refer to the product documentation for instructions on installation and enabling controls.

Within the Web Interface, set sound quality for the XenApp service site to at least medium quality. To enable the use of Philips SpeechMagic Speech Recognition server in conjunction with WinScribe software, set sound quality to high to enable accurate speech-to-text translation.

### To set sound quality for digital dictation devices

1. In the left pane of Access Management Console, select **Citrix Resource** > **Configuration Tools** > **Web Interface** > *XenApp Services Site Name* > **config.xml**.
2. From the **Action** menu, select **Change session options**.
3. In **Change Session Options**, select **Color and Sound**.
4. In the **Sound** area, select **Medium quality** or **High quality**.

# Ensuring Session Continuity for Mobile Workers

The Workspace Control feature provides users with the ability to disconnect quickly 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 XenApp. 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 Citrix XenApp plugin, you can configure—and allow users to configure—these activities:

- **Logging on.** By default, Workspace Control enables users to reconnect automatically 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 applications that are disconnected plus any 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 Citrix XenApp plugin.

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 at the session startup.

You can customize what printers appear to users when they change locations as well as control whether they can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For more information about enabling and configuring Workspace Control for users, see the *Web Interface Administrator's Guide.*

Related topics:

"Printing and Mobile Workers" on page 238

# Maintaining Session Activity

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 these three features of XenApp 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
- Auto Client Reconnect
- ICA Keep-Alive

## Configuring Session Reliability

Session Reliability 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 session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session.

With Session Reliability, the 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 Program Neighborhood can override the Session Reliability setting by selecting or clearing the **Enable session reliability** option in their application or connection settings. Users of the Citrix XenApp plugin and the Citrix XenApp Web Plugin cannot override the server setting.

By default, Session Reliability is enabled at the server farm level. You can customize the settings for this feature from 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 XenApp 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, this feature is designed to be convenient to the user and 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 Secure Sockets Layer (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.

---

## Configuring Automatic Client Reconnection

The Auto Client Reconnect feature allows plugins for Windows, Java, and Windows CE to detect broken connections and automatically reconnect users to disconnected sessions. When a plugin 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, XenApp encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to the plugin. The plugin 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 plugin attempts 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 these 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 device using an ICA file or using Group Policy to configure **Session reliability and automatic reconnection** on client devices.

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 XenApp Commands Reference" on page 347.

Disable Auto Client Reconnect on the plugin for Windows by using the icaclient.adm file. For more information about plugin configuration, see the *XenApp Plugin for Hosted Apps 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 XenApp'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 XenApp 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 plugin.

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 XenApp 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 plugin 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.

### To configure a default Auto Client Reconnect setting for a farm

Follow this procedure to configure server reconnection settings to be used when connections between client devices and XenApp servers are broken.

1. Select the farm in the left pane.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **ICA** > **Auto Client Reconnect**.
4. Choose one of these options:
   - **Require user authentication**. Select this option if you want users to be prompted for credentials during automatic reconnection to an ICA session. Do not select this option if you want users to be reauthenticated automatically during reconnection. Settings for automatic client reconnection override similar settings configured in Microsoft Windows Group Policy.
   - **Reconnect automatically** (default setting). Select this option if you do not want users to be prompted for credentials. Selecting this option also allows reconnection attempts to be logged.
5. If you selected **Reconnect automatically** in the previous step, you can select the **Log automatic reconnection attempts** check box to record information about successful and failed automatic reconnection events to each server's system log.

### To configure an Auto Client Reconnect setting for a server

Follow this procedure to configure server reconnection settings to be used when connections between client devices and a XenApp server are broken.

1. Select the server in the left pane.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **ICA** > **Auto Client Reconnect**.
4. If you want the server to use the default farm settings, select the **Use farm settings** check box; otherwise, follow Steps 4 and 5 in the "To configure a default Auto Client Reconnect setting for a farm" procedure.

## Configuring ICA Keep-Alive

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if XenApp detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Terminal Services from disconnecting that session. XenApp sends Keep-Alive packets every few seconds to detect if the session is active. If the session is no longer active, XenApp marks the session as disconnected.

However, the ICA Keep-Alive feature does not work if you are using Session Reliability. Session Reliability has its own mechanisms to handle this issue. Only configure ICA Keep-Alive for connections that are not using Session Reliability.

You can configure Keep-Alive as a farm-wide server default setting or as an individual setting for a particular server.

### To configure ICA Keep-Alive settings for a farm

Use this procedure to configure default server TCP/IP-based ICA connection settings so users can reconnect to sessions from which they are disconnected.

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **ICA** > **Keep-Alive**.
4. Select the **ICA Keep-Alive time-out value (1-3600 seconds)** check box to allow users to reconnect to disconnected sessions and resume working where they were interrupted in their published applications.

   Do not select this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.

   ICA Keep-Alive settings override Keep-Alive settings that are configured in Microsoft Windows Group Policy.

   ---

   **Important:** Servers running the Citrix Access Gateway intercept packets being sent from servers to client devices. Set Keep-Alive values on the Access Gateway servers to match Keep-Alive values on XenApp servers. Doing so allows ICA sessions to be changed from active to disconnected as intended.

   ---

5. Specify an interval between 1 and 3600 seconds.

   Do not select this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern.

ICA Keep-Alive settings override Keep-Alive settings that are configured in Microsoft Windows Group Policy.

---

**Important:** Servers running the Citrix Access Gateway intercept packets being sent from servers to client devices. Set Keep-Alive values on the Access Gateway servers to match Keep-Alive values on XenApp servers. Doing so allows ICA sessions to be changed from active to disconnected as intended.

---

The 60 second default interval causes ICA Keep-Alive packets to be sent to client devices every 60 seconds. If a client device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.

### To configure ICA Keep-Alive settings for a server

Use this procedure to configure default server TCP/IP-based ICA connection settings so users can reconnect to sessions from which they are disconnected.

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **ICA** > **Keep-Alive**.
4. If you want the server to use the default farm settings, select the **Use farm settings** check box; otherwise, follow Steps 4 and 5 in the "To configure ICA Keep-Alive settings for a farm" procedure.

# Understanding Session Basics

This topic is designed to help you understand basic aspects of sessions, such as how to end a session correctly. This topic also includes procedures that explain how to perform some of these tasks within a user's session at a general level. For specific information about how to perform these tasks within a plugin, see that plugin's online help.

In general, if a session disconnects in which a user is running multiple applications, the applications continue to run on the server until the user closes the applications. However, some applications that rely on virtual channels, such as media players, may behave differently. For example, if you disconnect from a session running Media Player while playing audio, the audio stops playing because the audio virtual channel is no longer available.

To end the application's session, exit the application and log off from the farm. If users disconnect without exiting the application or logging off from the farm, their session remains active. In this case, when they reconnect from another client device, XenApp reconnects them to the same session.

# Managing and Monitoring XenApp Sessions

XenApp lets you monitor sessions either by displaying their status or monitoring the session directly through shadowing.

You can also interact with sessions directly by saving disconnected sessions, terminating sessions and processes, and sending messages to users.

## Monitoring Session Status

Use the Access Management Console to display information about every session running on each server in the farm.

You can display the incoming and outgoing traffic for a session. When you display the session status, you can see the number of bytes, frames, bytes per frame, and frame errors; the percentage of frame errors; time-out errors; and compression ratios.

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.

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**.

Related topics:

“Disconnecting Sessions and Terminating Processes” on page 136

### To display information about a session

1. In the left pane of the Access Management Console, select the server on which you want to monitor sessions.
2. From the **Action** menu, select **Change display** > **Sessions**.

   The right pane of the Access Management Console displays all sessions running on the server.
3. Click **Choose columns** to specify the columns that you want to display and the order in which you want to see them.
4. Select a session and these tasks become available: **Reset**, **Log off**, **Disconnect**, **Send Message**, and **Shadow**.
5. Click **Show more tasks for the selected items** to obtain a list of available displays including Client Cache, Session Information, Client Modules, and Processes.

## To display information about active sessions

1. In the Access Management Console, select a server in the left pane.
2. From the **Action** menu, select **Change display** > **Sessions**.

   Information about active sessions appears in the details pane. 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.
   - **Type.** The type of session – ICA or RDP.
   - **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.

## To display session status

1. In the left pane of the Access Management Console, select the server hosting the session.
2. From the **Action** menu, select **Change display** > **Sessions**.
3. In the right pane of the Access Management Console, select the session for which you want to display the status.
4. From the **Action** menu, select **All Tasks** > **Status**.

A Session Status dialog box appears.

## To display session properties

1. In the left pane of the Access Management Console, select the server hosting the session.
2. From the **Action** menu, select **Change display** > **Sessions**.

The right pane of the Access Management Console displays all sessions running on the server.

3. Select a session, click **Show more tasks for the selected items**, and select one of these menu commands:

   - **Client Cache**. Displays the session cache, including the client and bitmap caches.
   - **Session Information**. Displays the details of the session, including the client name, build number, directory, and address.
   - **Client Modules**. Lists the client modules associated with the session.
   - **Processes**. Lists the processes associated with the session.

## Refreshing User Data

Refreshing user data automatically is disabled by default in the Access Management Console. You can control the frequency of automatic updates to server, server folder, and published application information on the Access Management Console you are running. The auto-refresh settings apply only to the Access Management Console you are running and not other instances of the console on your network.

---

**Note:** Do not enable this feature if you have many sessions, because it can impact performance.

---

### To refresh user data automatically

1. In the left pane, select one of these nodes (depending on what type of user data you want to refresh automatically):

   - The farm for which you want to refresh the user data automatically
   - The server for which you want to refresh the user data automatically
   - The application for which you want to refresh the user data automatically

2. In the center pane, from the Other Tasks section or the Common Tasks section (depending on the node that you selected), click **Refresh user data** and choose one of these options:

   - **Automatically refresh user data for servers**. Selecting this option enables automatic refreshing of each server's configuration and connection information. After selection, the associated Refresh rate field becomes available.

- **Automatically refresh user data for server folders**. Selecting this option enables automatic refreshing of each server's folder organization. After selection, the associated Refresh rate field becomes available.
- **Automatically refresh user data for applications**. Selecting this option enables automatic refreshing of each published application's configuration and connection information. After selection, the associated Refresh rate field becomes available.

3. In the **Refresh rate (seconds)** box, select the number of seconds between each update (10, 30, 60, or 90).

# Using Session Shadowing to View a User Session

You can view another user's session on another device by using *shadowing*. When shadowing, you can monitor the session activity as if you are watching the screen of the client device that initiated the session. If configured, you can also use your keyboard and mouse to control the user's keyboard and mouse remotely in the shadowed session.

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. 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. You can shadow using either the Access Management Console or the Shadow Taskbar.

You enable shadowing on a server when you install XenApp and select the default option, which allows shadowing on all connections on the server. If you do not leave the shadowing option enabled during Setup, you must reinstall XenApp to get shadowing functionality.

By default, the user is notified of the pending shadowing and asked to allow or deny shadowing.

---

**Important:** Your client device and shadowing ICA session must be capable of supporting the video resolution of the user's ICA session (the shadowed session). If not, the operation fails. You cannot shadow a system console from another session.

---

For shadowing options by connection type, such as keyboard, mouse, and user notification options, use the Terminal Services Configuration tool.

## Shadowing Using the Shadow Taskbar

Use the Shadow Taskbar to shadow multiple ICA sessions from a single location, including the server console. Use the **Shadow** button to start shadowing one or more users.

The Shadow Taskbar uses the client to launch an ICA session to monitor a user. A separate ICA session is started for each shadowed user.

You are required to enter your user name and password to start an ICA session on the server running the Shadow Taskbar.

Note the following:

- The client uses a license to log on to the server and start shadowing a user.
- The Shadow Taskbar shows sessions on the server or domain you logged on to. You can view servers in a different domain by logging on to an account in that domain and restarting the Shadow Taskbar.
- Each shadow session consumes memory on the server, so limit the number of simultaneous shadow sessions.

Each shadowed session is represented by a task button on the Shadow Taskbar. Use this button to switch quickly between the shadowing sessions you have open.

- To launch the Shadow taskbar, from the **Start** menu choose **All Programs** > **Citrix** > **Administration Tools** > **Shadow Taskbar**
- To configure options, click an empty area of the Shadow Taskbar and press SHIFT + F10.
- To switch to a shadow session, click its button in the Shadow Taskbar.

For more information about shadowing with the Shadow Taskbar, press F1 to view online Help when the Shadow taskbar is running.

You can also launch shadowing from the Access Management Console.

## To exit the shadow taskbar

Click an empty area of the Shadow Taskbar and press ALT + F4.

## To select users for shadowing

Use the **Shadow Session** dialog box to select users to shadow. The **Available Users** list shows user sessions that can be selected for shadowing in the current domain. User sessions are organized by servers, published applications, and users. You can shadow only client user sessions. The **Shadowed Users** list shows user sessions selected for shadowing and existing shadow sessions.

The **Shadowed Users** list also displays the user name of currently shadowed users next to the shadow icon. If a shadowed user is removed from the **Shadowed Users** list, the shadow session ends when you click **OK**.

1. On the Shadow Taskbar, click the **Shadow** button.
2. In the **Available Users** list, select the user to shadow and click **Add**. The selected user is added to the **Shadowed Users** list.

**Tip:** You can add multiple users to the **Shadowed Users** list. Shadowing is initiated for all users in the **Shadowed Users** list when you click **OK**.

## To end a shadowing session

1. On the Shadow Taskbar, click the **Shadow** button.
2. In the **Shadowed Users** list, select the users to stop shadowing and click **Remove**.

Shadowing ends for all users removed from the Shadowed Users list.

**Tip:** You can end a shadow session by right-clicking the session's task button on the Shadow Taskbar and clicking **Stop Shadow**. You can end all shadow sessions by right-clicking the Shadow Taskbar and clicking **Stop All Shadowed Sessions**.

## To shadow using 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.

1. In the left pane of the Access Management Console, select the server to which the user is connected.
2. From the **Action** menu, select **Change display** > **Sessions**.

   The right pane of the console displays all sessions running on the server.
3. Select the required session, and from the **Action** menu, select **Shadow**.
4. On the **Shadow** dialog box, select the key sequence that will end shadowing.

   If the user's permission is required, the session does not appear until the user grants permission.

## Enabling Logging for Shadowing

After installation, you can enable shadow logging and configure it so that it outputs to one of two locations on the server:

- **In a central file.** Configuring this option records a limited number of logging events, such as when and who started a shadowing session and who is being shadowed. If you configure shadow logging through the Shadow Taskbar, the logged events are not recorded in the Windows Event log. Instead, they go to a file that you specify.
- **In the Windows Event log.** Configuring this option logs several different event types to the Windows Event log. These include user shadowing requests, such as when users stop shadowing, failure to launch shadowing, and access to shadowing denied. However, these events are logged as they occur and it can be cumbersome to see a shadowing history because the events are strewn throughout the Event log.

For ease of management, consider logging events in a central file. Because only shadowing events go in to this file, they are more centralized and easier to review.

### To configure shadow logging to log in a central file

When you enable this option on a XenApp server, the shadowing events are logged in a central file on that server.

1. Click on an empty area of the Shadow Taskbar and press SHIFT + F10.
2. Click **Logging Options**.
3. Select the **Enable Logging** check box and specify a log file path.

Click **Clear Log** to empty the current log file.

### To enable shadow logging in the Windows Event Log

When you enable this option on a XenApp server, the shadowing events are logged in the Application log of the Windows Event log.

1. Select the server in the left pane of the Access Management Console.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **XenApp** > **Shadow Logging**
4. Select the **Log shadowing sessions** check box if you want all shadow sessions initiated from the server to be written to the Application log.

## Enabling User-to-User Shadowing with Policies

You can use the Advanced Configuration tool 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 XenApp 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 to be shadowed.

### To create a user policy to define users who can shadow

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 users not to launch the Shadow taskbar in seamless mode. The Shadow taskbar cannot function in seamless mode.

---

### Example: To create a user policy for user-to-user shadowing

This example demonstrates how to enable user-to-user shadowing by creating a policy for your "Sales" user group that allows them to shadow the department manager for online collaboration on sales leads. This procedure shows the creation of a shadowing policy.

1. Create a new policy 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. In the left pane of the property sheet, select the rule named **Permissions**.
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 appear 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**.

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.

---

#### Example: To assign the shadowing policy to users

This procedure shows the assignment to the users in the Sales group of the policy you created.

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 the manager 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 the user account in the Configured Accounts list.

**Important:** The list of users permitted to shadow is exclusive for each user for 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 "Example: To create a user policy for user-to-user shadowing" on page 134.

#### To merge shadowers in multiple policies

Use this procedure to allow merging of shadow policies. If you create multiple shadowing policies, you must also select this option. If you do not enable this option, the resultant policy uses the shadowing policy with the highest priority and ignores the rest of the shadowing policies, even if they do not conflict.

1. In the Access Management Console, select the farm in the left pane.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Farm-wide** > **XenApp** > **Shadow Policies**.
4. Under **Shadow policies**, select the **Merge shadowers in multiple policies** check box.

# Managing User Sessions

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.

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.

You can perform these tasks to better manage your disconnected sessions:

- Disconnecting sessions
- Ending sessions

## Disconnecting Sessions and Terminating Processes

You can use the console to disconnect a user session from a server or terminate a process in a session. A disconnected session is still active and its applications continue to run, but the client device is no longer communicating with the server.

A user can reconnect to a disconnected session from a different client device without loss of data. For example, you might disconnect users' sessions if they experience problems on their client device and do not want to lose data from their applications.

When you disconnect a session, you close the connection between the client device 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. 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 use the Access Management Console to log off users from their sessions. You can also reset a user's client session or a disconnected session.

You can also connect to a user's disconnected session when you are using the Access Management Console from within a client session on a XenApp server. To connect, you must know the password of the user who started the session. Your session must be capable of supporting the same video resolution as the disconnected session.

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 ICA sessions of all users who are connected to the server.

### To terminate processes in a user's session

1. In the left pane of the Access Management Console, right click the server to which the user is connected and select **Change display** > **Users**.

   The right pane of the console displays all users connected to the server.

2. Select the user's session for which you want to terminate the process.
3. In the Tasks list at the bottom of the right pane, click **Show more tasks for the selected items**.
4. In **Available Displays**, click **Processes**.
5. Select the process you want to terminate.

6. From the **Action** menu, select **Terminate**.

---

**Note:** Terminating a process may abruptly end a critical process and leave the server in an unusable state.

---

### To disconnect a session

1. In the left pane of the Access Management Console, right click the server to which the user is connected and select **Change display** > **Users**.

   The right pane of the console displays all users connected to the server.

2. Select the user's session you want to disconnect.

3. From the **Action** menu, select **Disconnect**.

---

**Note:** If you disconnect a session in which a user is running multiple applications, all the applications the user is running are terminated.

---

### To connect to a user's session from Program Neighborhood

To connect to a disconnected or live session remotely through Program Neighborhood, your session must support the video resolution of the disconnected session. Also, you can connect only to disconnected sessions that were disconnected from the Access Management Console.

1. Using Program Neighborhood, create a direct custom connection to the server hosting the session.

   A. In Program Neighborhood, create a **Custom ICA Connection** directly to the server.

   B. Use your new custom ICA connection to connect to the desktop of the server hosting the session.

2. After you authenticate to the host server, open the Access Management Console.

3. In the left pane of the Access Management Console, select the server to which the user was connected (that is, the server to which you just connected).

4. From the **Action** menu, select **Change display** > **Sessions**.

   The right pane of the console displays all sessions running on the server.

5. Select the session you want to log off and from the **Action** menu, select **Connect**.

### To reset a session

**Caution:** Resetting effectively deletes the session and results in loss of data for the user. Only reset a session when it is not responding or malfunctions.

1. In the left pane of the Access Management Console, select the server to which the user is connected.
2. From the **Action** menu, select **Change display** > **Sessions**.

   The right pane of the console displays all sessions running on the server.
3. Select the session you want to reset, and from the **Action** menu, select **Reset**.

   You can select and reset multiple sessions at the same time.

### To log off from a session

**Important:** Ending users' sessions with the **Logoff** command can result in loss of data if users do not close their applications first. Send a message to warn users to exit all applications if you need to log off their sessions.

1. In the left pane of the Access Management Console, select the server to which the user is connected.
2. From the **Action** menu, select **Change display** > **Sessions**.

   The right pane of the console displays all sessions running on the server.
3. Select the session you want to log off and from the **Action** menu, select **Log off**.

   You can select and log off multiple sessions at the same time.
4. Confirm the logoff when prompted.

# Sending Messages to Users

You can use the Access Management Console to send a message that appears in user sessions. For example, you can broadcast information about new applications and upgrades, request a shadowing session, or warn of system shutdowns. To broadcast a message to all users, you can select all users in the right pane in the console.

## To send a message to one or more users

1. In the left pane of the Access Management Console, select the server to which the users are connected.

**Tip:** To send a message to all user sessions in the farm, you can select the Farm node instead of a server.

2. From the **Action** menu, select **Change display** > **Users**.
3. In the right pane of the Access Management Console, select the sessions to which the user is connected.
4. Select one or more sessions and from the **Action** menu, select **Send Message**.
5. In the **Send Message** dialog box, edit the title of the message, if required, and enter the content of the message in the **Message** text box.

The message is sent to users immediately.

# Controlling Client Connections in XenApp

You can control XenApp client connections in different places:

- **XenApp policies**. Policies let you define how you want clients to connect, including SSL or encryption requirements, and the properties for the user's environments after the connection is established.
- **Application Publishing**. You can define connection settings on a per-application basis when you are publishing a resource. Settings you can define include the maximum number of connections to an application, importance level of the application, maximum number of instances an application can run in the farm, types of connections that can access an application, audio properties, and encryption requirements.
- **Terminal Services Configuration**. Terminal Services Configuration (TS Config), which is part of Windows Server 2008, lets you define XenApp connection settings similar to the ones found in XenApp policies. However, these TS Config settings must be defined on a per-server basis. Because defining settings using TS Config requires setting them on each server in your farm, Citrix recommends using TS Config to define connection settings only for test farms or very small server farms.
- **Active Directory**. Citrix provides a Group Policy Object (GPO) template, the icaclient.adm, that contains Citrix-specific rules for securing client connections. This GPO lets you configure rules for network routing, proxy servers, trusted server configuration, user routing, remote client devices, and the user experience. The icaclient.adm template is in the XenApp installation media. For more information about the icaclient.adm template,

see the *XenApp Plugin for Hosted Apps for Windows Administrator's Guide*.

Citrix recommends using XenApp policies whenever possible to control connections. Connection settings defined through XenApp policies also supersede all other connection settings in your environment, including those at the operating system level, in TS Config, and specified when you publish an application

Related topics:

"To configure application importance" on page 60

"Limit Total Concurrent Sessions" on page 414

# Preventing Specific Client Connection Types

You can specify the types of client connections from which users can start sessions.

For example, to increase security, you can specify that users must connect through Access Gateway Advanced Edition (Version 4.0 or later). This allows you to benefit from filters created in Access Gateway.

Related topics:

"To apply a policy filter based on Access Gateway connections" on page 92

## To configure connection access controls

This procedure specifies the types of client connections from which users can start sessions. Use this procedure if you want to affect all servers on your farm. If you want more granular control, perform this task by configuring a policy.

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Farm-wide** > **Connection Access Controls**.
4. Select one of these options:
    - **Any connections** (selected by default). Allows access to published applications through any connection.
    - **Citrix Access Gateway**, **Citrix XenApp plugin**, and **Web Interface connections only.** Allows access to published applications through the listed connections, including any version of Access Gateway. Denies access through any other connection.

- **Citrix Access Gateway connections only**. Allows access to published applications only through Access Gateway Advanced Edition servers (Version 4.0 or later).

# Specifying Connection Limits

To help maintain the availability of resources in a server farm, you can limit the number of connections to servers and published applications. Setting connection limits helps prevent:

- Performance degradation and errors resulting from 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 limits, including the option to log denials resulting from connection limits, are configured in the Access Management Console. (You cannot configure connection limits in the plugins.)

The Access Management Console provides two types of connection limits:

| Limit type | Description |
|---|---|
| Concurrent connections to the server farm | Restricts the number of simultaneous connections that each user in the server farm can establish. See "Limiting Connections to a Server Farm" on page 142. |
| Published application instances | Restricts the total number of instances of a published application that can run in the server farm at one time, and prevents users from launching more than one instance of a published application. See "Limiting Application Instances" on page 145. |

By default, XenApp does not limit connections in any way. If you want to limit connections, enable these settings.

## Limiting Connections to a Server Farm

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.

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 plugin displays a message that describes why the connection is not available.

You can also limit the number of connections on a farm by ensuring that session sharing is enabled.

### To limit concurrent connections to a server farm

1. In the left pane of the Access Management Console, select the farm and select **Action > Modify farm properties > Modify all properties**.
2. From the **Properties** list, select **Farm-wide** > **Connection Limits**.
3. Select **Maximum connections per user** to limit each user's concurrent connections. Enter the number of concurrent connections to allow for each user.

   For example, you can limit users to a maximum of five connections. 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.
4. If you want the connection limitation to apply to everyone, including local administrators, select **Enforce limit on administrators**.

---

**Important:** Limiting connections for Citrix administrators can adversely affect their ability to shadow other users. By default, local administrators are exempt from the limit so they can establish as many connections as necessary.

---

## Sharing Sessions and Connections

Depending on the plugin, when a user opens an application, it can either appear in a *seamless* or *non-seamless* window. These window modes are available for most plugins, including the Web Interface, Citrix XenApp plugin, and Program Neighborhood.

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

In non-seamless window mode, published applications and desktops are contained within an ICA session window. This creates the effect of the application appearing in two windows.

The mode that you choose typically depends on the type of client device that your users will be using and whether you are publishing a desktop or individual applications. Desktops are typically published in non-seamless window mode. This table provides examples of when you might want to publish desktops and applications.

| **If your users will be using...** | **then you...** |
|---|---|
| Local computers | Might want to publish desktops or individual applications. |
| Local computers with locally installed applications | Might want to publish individual applications. |
| Thin clients | Must publish desktops. |
| Kiosks | Might want to publish desktops, which allows the user to have a more holistic experience and provide more control from a security perspective. |

When a user launches a published application, the plugin establishes a connection to a XenApp server and initiates a session. If session sharing is not configured, a new session is opened on the server each time a user opens an application. Likewise, every time a user opens a new application, a new client connection is created between the client device and the server.

*Session sharing* is a mode in which more than one published application runs on a single connection. Session sharing occurs when a user has an open session and launches another application that is published on the same server; the result is that the two applications run in the same session. For session sharing to occur, both applications must be hosted on the same server. Session sharing is configured by default when you specify that applications appear in seamless window mode. If a user runs multiple applications with session sharing, the session counts as one connection.

If you want to share sessions, ensure all applications are published with the same settings. Inconsistent results may occur when applications are configured for different requirements, such as encryption.

---

**Note:** Session sharing is not supported on PocketPC clients.

---

Session sharing always takes precedence over load balancing. That is, if users launch an application that is published on the same server as an application they are already using but the server is at capacity, XenApp still opens the second application on the server. Load Manager does not transfer the user's request to another server where the second application is published.

If you want to disable session sharing, see the Citrix Knowledge Center article, "Troubleshooting and Explaining Session Sharing."

## Limiting Application Instances

By default, XenApp does not limit the number of instances of a published application that can run at one time in a farm. By default, a user can launch more than one instance of a published application at the same time.

You can specify the maximum number of instances that a published application can run at one time or concurrently in the server farm. For example, you can publish an application and set a limit of 30 concurrent instances in the farm. Once 30 users are running the application at the same time, no more users can launch the application because the limit of 30 concurrent instances was reached.

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.

---

Related topics:

"To configure application importance" on page 60

### To specify a limit for a published application or desktop

1. In the left pane of Access Management Console, select **Citrix Resources** > **XenApp** > *yourfarmname* > **Applications** and select the published application or desktop you want to modify.
2. From the **Actions** menu, select **Modify application properties** > **Modify all properties**.
3. In the Properties tree, select **Limits**.

4. On the **Limits** page, select one or both of these 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.

     For example, 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 time and the name of the published application in the System log.

   - **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.

## Logging Connection Denial 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.

You can configure XenApp to log when limits are reached (and connections denied) for the following:

- Maximum connections per user, as set in the server farm properties
- Application instance limits, as set for a published application
- Application instances per user, as set for a published application

### To enable logging of connection denial events

1. Select a farm in the left 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**.

# Controlling Connections with Terminal Services Configuration

**Important:** Citrix recommends controlling connections by using Citrix policies. While you can use the Terminal Services Configuration (TS Config) tool, Citrix policies are better suited for farm-level changes. Using the TS Config tool is more time-consuming and requires that you specify settings on each XenApp server.

You can control connection settings for individual servers using TS Config, which is a snap-in you can add to the Microsoft Management Console (MMC). You can specify these settings in either TS Config or XenApp policies:

- Redirection, including disabling drive mapping
- Printing
- Ports
- The clipboard
- Other settings, including color depth on plugins

You might need to use the TS Config in these situations:

- If you want to configure a test farm or create a very small farm and you do not want to configure policies, specifying settings in TS Config might be easier than configuring policies.
- When you want to configure certain TS Config policies that do not have a corresponding Citrix policy, such as policies that correspond with these tasks:
    - **Idle Session Limit**. In the ICA-tcp properties in TS Config, select the Sessions tab, enable Override user settings and then specify the Idle Session Limit.
    - **Restrict users to one session**. This setting is in **Terminal Services Configuration** in the Server Manager. Citrix strongly recommends that you turn this setting off because it might affect your user sessions negatively.

For more information about TS Config, see your Microsoft documentation.

Related topics:

“To configure application importance” on page 60

“Limit Total Concurrent Sessions” on page 414

## To control connections on a server with TS Config

To use TS Config to control connections on a remote computer that has XenApp installed, XenApp must be installed on the local computer; otherwise, the **ICA Settings** tab on the properties dialog box does not appear.

This procedure assumes that you already added the TS Config tool snap-in to the MMC. If not, do so before proceeding. See your Microsoft documentation for details as needed.

1. From the **Start** menu, select **Administrative Tools** > **Terminal Services** > **Terminal Services Configuration**.
2. With **Connections** selected in the left pane of the console that opens, right-click **ICA-tcp** 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:** The Citrix Connection Configuration tool is no longer available. It has been replaced by the **ICA-tcp** entry in TS Config.

---

## Preventing User Connections during Farm Maintenance

You might want to prevent logons to a server when you install software or perform other maintenance or configuration tasks. This is helpful when you are installing applications that require there be no active sessions on the server. It also lets you restart the server without having to wait for users to disconnect.

By default, logons are enabled when you install XenApp and users can launch an unlimited number of sessions and instances of published applications. You can prevent users from connecting to a server in the farm by disabling logons.

### To disable logons on a server

Select the server in the left pane of the Access Management Console and select **Action > All Tasks > Disable logon**.

---

**Note:** To reenable disabled logons, use the **Enable logon** option.

---

# Optimizing User Sessions for XenApp

XenApp includes various features that allow you to enhance user experience by maintaining session activity and improving session responsiveness.

Network latency and bandwidth availability can impact the performance of connections to published applications and content. These SpeedScreen and ICA technologies allow you to improve connection speed and responsiveness during user sessions. Instructions for configuring these features are provided in the corresponding topics:

- **SpeedScreen Browser Acceleration.** Optimizes the responsiveness of graphics-rich HTML pages in published versions of Microsoft Outlook Express, Outlook 2003, Windows Mail, and Internet Explorer.
- **SpeedScreen Multimedia Acceleration.** Allows you to control and optimize the way XenApp servers deliver streaming audio and video to users.
- **SpeedScreen Flash Acceleration.** Allows you to control and optimize the way XenApp servers deliver Adobe Flash animations to users.
- **SpeedScreen Image Acceleration.** Enables you to create a balance 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 the image when it is first transmitted over a limited bandwidth connection, providing 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, thereby reducing bandwidth further without impacting image quality. Heavyweight compression uses a more CPU-intensive algorithm and impacts server performance and scalability. Because heavyweight compression is CPU intensive and affects server scalability, this type of compression is recommended for use only with low bandwidth connections.

  If enabled in the SpeedScreen policy rule, heavyweight compression applies to all lossy compression settings. It is supported on XenApp Plugins, but has no effect on other clients.
- **SpeedScreen Latency Reduction.** 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 helps reduce a user's perception of latency when typing and clicking. It provides visual feedback for mouse clicks and

Local Text Echo; a feature that accelerates the display of input text, effectively shielding the user from experiencing latency on the network.

- **ICA display.** ICA display gives you control over settings that let you reserve bandwidth by limiting session-memory usage and discarding obsolete queued images on the client.
- **ICA browser.** ICA browser gives you control over whether or not the servers in your network will respond to broadcast messages sent from Program Neighborhood. You may reduce bandwidth consumption if you disable these options.

# Optimizing Web Page and Email Responsiveness

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 Microsoft Internet Explorer, Outlook 2003, and Windows Mail. 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, enable JPEG compression with SpeedScreen Browser Acceleration. JPEG compression lets you find a balance 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.

Users with limited bandwidth connections benefit the most from SpeedScreen Browser Acceleration. Users connecting on the LAN may see improvement only when networks are congested. Enabling this feature uses more resources on both servers and clients.

Enabling SpeedScreen Browser Acceleration results in:

- **Background image delivery**. Users can click Back and Stop while images are being downloaded in the background.
- **Progressive drawing**. Users can interact with elements of a page while the page continues to download.
- **Responsive scrolling**. Scrolling speed and responsiveness is similar to scrolling in a local browser.
- **JPEG image recompression**. You can select a compression level for JPEG images. Higher compression results in less bandwidth used but lowers image quality.

- **Adaptive JPEG image recompression**. The available bandwidth is used to determine how much images are compressed. If enough bandwidth is available, images are not compressed. You can limit the compression level.

SpeedScreen Browser Acceleration requires at least Version 7.0 or later of the Presentation Server Clients for Windows or Citrix XenApp Plugin for Hosted Apps 11.*x* for Windows, Internet Explorer 5.5 through 7.0, and High Color (16-bit) or greater connection color depth.

Speed Screen Browser Acceleration is not supported with Microsoft Outlook 2007; Citrix supports Speed Screen Browser Acceleration for Microsoft Outlook 2003 only.

By default, SpeedScreen Browser Acceleration is enabled at the server farm level.

Related topics:

"Optimizing Throughput of Image Files"

## SpeedScreen Browser Acceleration and Play Animation in Web Pages

At installation XenApp disables the Internet Explorer setting **Play Animations in Web pages** for all users on the server. For optimal performance with SpeedScreen Browser Acceleration, Citrix recommends that you keep this setting disabled.

When **Play Animations in Web pages** is enabled, animated GIF images are rendered as animations and SpeedScreen Browser support for GIF images is disabled. When this feature is disabled, SpeedScreen Browser Acceleration support for GIF images is enabled. The secondary benefit is a bandwidth reduction due to the absence of animations that consume significant bandwidth.

If a user subsequently enables **Play Animations in Web pages**, only an administrator can modify it again by making changes to specific values in the registry.

Users can access **Play Animations in Web pages** by opening Internet Explorer and selecting **Tools** > **Internet Options** > **Advanced** or by navigating to **Internet Options** under Control Panel.

## SpeedScreen Browser Acceleration Limitations

- **Support for Images.** SpeedScreen Browser Acceleration supports JPEG and nontransparent GIF images.
- **Adobe Flash.** SpeedScreen Browser Acceleration is not compatible with Adobe Flash.
- **Images Resized in HTML.** The HTML that describes a Web page can also specify the width and the height of an image. This might be different than the actual width and height of the image. In this case, Internet Explorer

grows or shrinks the image as required to fit it into the size specified in the HTML. SpeedScreen Browser Acceleration does not support images that are resized using this technique. Images that are resized in HTML are drawn in legacy mode.

---

**Note:** *Image resizing in HTML* described here is not the same as the Internet Explorer Automatic Image Resizing feature.

---

## Configuring SpeedScreen Browser Acceleration

When ICA connections have limited bandwidth, downloading images can be slow. SpeedScreen Browser Acceleration can improve responsiveness for users when they are using Internet Explorer 5.5 or later as published applications. Specifically, this feature helps ensure that images display cleanly and scrolling is smooth in Web browsers.

You can configure SpeedScreen Browser Acceleration as a farm-wide server default setting or as an individual setting for a particular server.

Do not enable Flash content in your Web browser display if you want SpeedScreen Browser Acceleration to be used. Regardless of whether you configured the optimization settings for Speedscreen Flash Acceleration, SpeedScreen Browser Acceleration does not work when Flash content is on a page.

---

**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.

---

SpeedScreen Browser Acceleration is disabled if Internet Explorer is running in Protected Mode. However, you can turn on SpeedScreen Browser Acceleration even when Internet Explorer is running in Protected Mode by adding **EnableProtectedModeSpeedBrowse** and setting it to **1** in the HKEY_LOCAL_MACHINE\SOFTWARE\CITRIX\SpeedBrowse registry key.

### To configure SpeedScreen Browser Acceleration for a farm

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **SpeedScreen** > **Browser Acceleration**.

4. Select the **SpeedScreen Browser Acceleration** check box to improve responsiveness when users run HTML-capable published applications.
5. Select the **Compress JPEG images to improve bandwidth** check box to improve bandwidth.
6. Select one of these options if the ICA connections have very low bandwidth:

---

**Note:** Compressing JPEG images reduces image quality.

---

- **Image compression levels**. Select High, Medium, or Low compression for JPEG images. The higher the compression, the less bandwidth used and the lower the image quality. Select High when bandwidth usage is most important, such as when running a published application over a WAN connection. Select Low if image quality is more important than bandwidth usage.
- **Adjust compression level based on available bandwidth**. Select this option if the available bandwidth can vary for ICA connections. The available bandwidth and image size are used to determine how much images are compressed. If enough bandwidth is available, images are not compressed.

### To configure SpeedScreen Browser Acceleration for a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **SpeedScreen** > **Browser Acceleration**.
4. If you want the server to use the default farm settings, select the **Use farm settings** (available server level only) check box; otherwise, follow Steps 4 to 6 in "To configure SpeedScreen Browser Acceleration for a farm" on page 152.

# Optimizing Audio and Video Playback

SpeedScreen Multimedia Acceleration improves the user's experience of accessing published audio-visual applications and content. Enabling this feature increases the quality of audio and video in ICA sessions to a level that compares with audio and video played locally on a client device. In addition, it reduces use of network bandwidth and server processing and memory because compressed multimedia files are intercepted and forwarded to the client to be uncompressed.

This feature optimizes multimedia playback through published instances of Internet Explorer, Windows Media Player, and RealOne Player. It offers significant performance gains in these 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.

---

**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.

---

Without SpeedScreen Multimedia Acceleration, the cumulative cost of several users playing multimedia content in sessions simultaneously 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, DirectX Media Objects (DMO), and Media Foundation standards. DirectShow and Media Foundation are application programming interfaces (APIs) that allow, 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.

Generally, 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.

Users accessing audio-visual applications on servers on which SpeedScreen Multimedia Acceleration is enabled use a little more memory but far less bandwidth than when this feature is disabled. Users use only a little more memory or bandwidth when accessing audio-visual applications compared to regular enterprise applications.

By default, audio is disabled on any custom connections created with Program Neighborhood. To allow users to run multimedia applications in ICA sessions, turn on audio or give the users permission to turn on audio themselves in Program Neighborhood. By default, all other clients and methods are configured with audio enabled and medium sound quality.

Other requirements for using SpeedScreen Multimedia Acceleration are:

- Users must be running a XenApp Plugin.
- The client device must have the same memory and processing speed as is needed for playing multimedia locally.
- The correct codec, or compression algorithm, to decompress the media file type used (MPEG for example) must reside on the client device. Windows clients have the most common codecs already installed. If you need additional codecs, you can download them from the Web sites of the manufacturers of media players.

---

**Important:** To make Windows Media Player 11 and Media Foundation components available on your XenApp server, install and configure the Microsoft Windows Server 2008 Desktop Experience in the Server Manager.

---

Applications and media formats supported by SpeedScreen Multimedia Acceleration are:

- Applications based on Microsoft's DirectShow, DirectX Media Objects (DMO), and Media Foundation filter technologies such as Windows Media Player, RealPlayer
- Applications like Internet Explorer and Microsoft Encarta are also supported, as they leverage Windows Media Player
- Both file-based and streaming (URL-based) media formats: WAV, all variations of MPEG, and unprotected Windows Media Video (WMV) and Windows Media Audio (WMA)

---

**Note:** SpeedScreen Multimedia Acceleration does not support media files protected with Digital Rights Management (DRM).

---

When the quality of media playing on a client device deteriorates, possible solutions are:

- If video appears in slowly changing slides while audio is intact or audio becomes choppy, this is caused by low bandwidth. Arrange for users to play media on the network where more bandwidth is available.
- If audio and video are not synchronized, generally only the video or audio is played using SpeedScreen Multimedia Acceleration. This can happen if a client device lacks a codec for either video or audio. Install the needed codec on the client or use media content on the server for which clients have both codecs.

---

**Note:** Volume and balance selections do not work with RealOne in an ICA session. Users can still control volume and balance outside the RealOne application with controls on the client.

---

By default, SpeedScreen Multimedia Acceleration is enabled at the server farm level.

## Configuring SpeedScreen Multimedia Acceleration

You can configure SpeedScreen Multimedia Acceleration as a farm-wide server default setting or as an individual setting for a particular server.

---

**Note:** By default, audio is disabled on the client. To allow users to run multimedia applications in ICA sessions, turn on audio or give the users permission to turn on audio themselves in their client interface.

---

### To configure SpeedScreen Multimedia Acceleration for a farm

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **SpeedScreen** > **Multimedia Acceleration**.
4. Select the **SpeedScreen Multimedia Acceleration** check box.

   By default, SpeedScreen Multimedia Acceleration is enabled. Turn off this setting only if playing media using SpeedScreen Multimedia Acceleration appears worse than when rendered using basic ICA compression and regular audio. This is rare but can happen under low bandwidth conditions; for example, with media in which there is a very low frequency of key frames.

5. Choose one of these options:
   - Accept the recommended default buffering of five seconds.
   - Select **Custom buffer time in seconds (1-10)** and enter another figure.

     You can see how much server memory the selected buffer can use by changing the buffer time.

### To configure SpeedScreen Multimedia Acceleration for a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **SpeedScreen** > **Multimedia Acceleration**.
4. If you want the server to use the default farm settings, select the **Use farm settings** (available server level only) check box; otherwise, follow Steps 4 and 5 in "To configure SpeedScreen Multimedia Acceleration for a farm" on page 156.

## Optimizing Flash Animations

SpeedScreen Flash Acceleration allows you to optimize the way XenApp renders and delivers Adobe Flash animations to users. To display Flash animations in sessions, you must have the Flash plug-in and the corresponding Active X control installed in the Web browser before you publish it.

In earlier versions of XenApp, users playing Flash animations in published applications often observed poor rendering quality of the animation, slow session responsiveness, or a combination of both. This occurs when Adobe 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 use simpler graphics (for example, no smoothing or anti-aliasing). This feature 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. However, the Web browser, and not this feature, controls if Flash content appears. SpeedScreen Flash Acceleration lets you specify the optimization settings when Flash is present on a Web page.

You can configure the optimization settings for SpeedScreen Flash Acceleration as a farm-wide server default setting or as an individual setting for a particular server.

**Note:** SpeedScreen Flash Acceleration now supports Adobe Flash 9.

## To configure SpeedScreen Flash Acceleration for a farm

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **SpeedScreen** > **Flash Acceleration**.
4. Select the **Enable Adobe Flash Player** check box to configure Flash optimization settings.
5. Under **Optimize Adobe Flash animation options**, you can select one of these options to reduce the amount of Flash data sent from the server to client devices:
   - **Do not optimize**. Select this option if bandwidth is not limited.
   - **Restricted bandwidth connections**. Select this option to improve responsiveness when Flash content is sent to users on restricted bandwidth connections (under 150Kbps). On restricted bandwidth connections, such as over a WAN, less data is downloaded and the quality of Flash content is lower. When bandwidth is not limited, for example on a LAN, users get higher quality Flash animation.
   - **All connections**. Select this option to always reduce the amount of Flash data sent to users. The result is that CPU usage is minimized on the servers on which users are using Flash within Internet Explorer.
6. From the **Properties** list, select **Server Default** > **ICA** > **Display** and select the **Discard queued image that is replaced by another image** check box to reduce bandwidth consumption and improve video playback and server scalability.

## To configure SpeedScreen Flash Acceleration for a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **SpeedScreen** > **Flash Acceleration**. If you want the server to use the farm settings, select the **Use farm settings** (available on server level only) check box. If not, follow Steps 4 to 5 in "To configure SpeedScreen Flash Acceleration for a farm" on page 158.

4. From the **Properties** list, select **ICA** > **Display**. If you want the server to use the farm settings, select the **Use farm settings** (available on server level only) check box. If not, follow Steps 4 to 6 in "To configure SpeedScreen Flash Acceleration for a farm" on page 158.

# Optimizing Throughput of Image Files

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. Using lossy image compression, SpeedScreen Image Acceleration lets you find a balance 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 that the server sends to the client for faster throughput. The compression scheme removes redundant or extraneous data from the files 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 Advanced Configuration tool 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 Advanced Configuration tool, 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** for all connections.

---

**Note:** This default may not be the optimum setting for all environments, so you are encouraged to experiment with other settings.

---

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**.

You can reduce bandwidth further by using heavyweight compression in conjunction with this feature.

# Optimizing Display of Image Files

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.

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 1 Mbps of bandwidth per user. Note that this may not be the optimum setting for all environments, so 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**.

You can reduce bandwidth further by using heavyweight compression in conjunction with this feature.

Related topics:

"Optimizing Throughput of Image Files"

# Optimizing Keyboard and Mouse Responsiveness

*SpeedScreen Latency Reduction* is a collective term used to describe features such as Local Text Echo and Mouse Click Feedback that help enhance user experience on a slow network.

- **Mouse Click Feedback.** On high latency connections, users often click the mouse multiple times because there is no visual feedback that a mouse click resulted in an action. 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. When the user clicks the mouse, the ICA software immediately changes the mouse pointer to an hourglass to show that the user's input is being processed. You can enable and disable Mouse Click Feedback at the server level.
- **Local Text Echo.** On high latency connections, users often experience significant delays between when they enter text at the keyboard and when it is echoed or displayed on the screen. When a user types text, the keystrokes are sent to the server, which renders the fonts and returns the updated screen 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, Local Text Echo is disabled. You can enable and disable this feature both at the server and application level. You can also configure Local Text Echo settings for individual input fields within an application.

  **Note:** Applications that use non-standard Windows APIs for displaying text may not support Local Text Echo.

## Configuring SpeedScreen Latency Reduction

SpeedScreen Latency Reduction Manager, a tool provided with XenApp, allows you to configure SpeedScreen Latency Reduction settings for a XenApp server, for single or multiple instances of an application, as well as for individual input fields within an application. You can also use it as a troubleshooting tool to fine-tune SpeedScreen Latency Reduction behavior for applications, or input fields within an application, that exhibit incompatibility with this SpeedScreen feature.

SpeedScreen Latency Reduction Manager must be installed on a XenApp server, and can be used to customize SpeedScreen Latency Reduction settings only on that server.

To launch SpeedScreen Latency Reduction Manager, select SpeedScreen Latency Reduction Manager from the **Citrix > Administration Tools** program group in the Start menu.

**Note:** To run the Speedscreen Latency Reduction Manager with the User Account Control (UAC) enabled, you must be a domain administrator, delegated administrator, or part of the Administrators group on the local computer, or you will be prompted for administrator credentials.

Through SpeedScreen Latency Reduction Manager, you can configure common SpeedScreen Latency Reduction settings for all applications on a server or select custom settings for individual applications. Before you can configure any settings, you must add the application.

## Adjusting SpeedScreen Latency Reduction for an Application

If a published application exhibits abnormal behavior after it is configured to use SpeedScreen Latency Reduction, you can use the Add New Application wizard included with SpeedScreen Latency Reduction Manager to adjust latency reduction functionality for the selected application, or all instances of the selected application on the server. To optimize usability of the application, use this wizard to adjust, turn on, or turn off SpeedScreen Latency Reduction for the application.

**Note:** The application must be running before you can use this wizard to modify existing settings.

### To adjust SpeedScreen Latency Reduction for an application

Before you can adjust Speedscreen Latency Reduction for an application, you must add the application to the Speedscreen Latency Reduction Manager.

1. From the **Start** menu, select **All Programs** > **Citrix** > **Administration Tools** > **SpeedScreen Latency Reduction Manager**.
2. From the **Applications** menu of SpeedScreen Latency Reduction Manager, select **New** to start the wizard and follow the prompts.
3. Use the **Define the Application** screen to select an application instance on the server. To specify the application, use one of these methods:
   - Click the icon at the bottom of the page and drag the pointer onto the window of an application. The application must be running when you select it.
   - Click the **Browse** button and navigate to the application.
4. Specify whether Local Text Echo is enabled or disabled on the application by selecting or clearing the **Enable local text echo for this application** check box.

For a definition of Local Text Echo, see “Optimizing Keyboard and Mouse Responsiveness” on page 161

5. Specify whether the setting you selected in the previous step should be applied to all instances of the application on the server or just the instance selected.

Test all aspects of an application with Local Text Echo in a non-production environment before enabling it 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 **Apply settings to all installations of the selected application** when configuring Local Text Echo through the wizard. Paths to published applications might differ from one server to another; therefore, 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.

---

### To configure latency reduction settings for all applications on a server

1. From the **Start** menu, select **All Programs** > **Citrix** > **Administration Tools** > **SpeedScreen Latency Reduction Manager**.
2. From the **Application** menu, select **Server Properties.**

   The **Server Properties** dialog box containing existing settings for the selected server appears.
3. Configure the SpeedScreen Latency Reduction settings that you want to be applied to all of the applications on the server. All users connecting to the server benefit from the SpeedScreen options you set here.

   Changes made to SpeedScreen Latency Reduction settings at an application level override any server-wide settings.

   - **Enable local text echo as default for all applications on this server.** Select this check box to enable Local Text Echo for all applications on the server.
   - **Enable mouse click feedback as default for all applications on this server.** Select this check box to enable Mouse Click Feedback for all applications on the server.

- **Latency threshold times for SpeedScreen (in milliseconds).** Latency threshold times are used when the client device setting for SpeedScreen is set to Auto.
  - **High latency threshold.** Specify a threshold value above which SpeedScreen options should be enabled.
  - **Low latency threshold.** Specify a threshold value below which SpeedScreen options should be disabled.

For a definition of Local Text Echo and Mouse Click Feedback, see "Optimizing Keyboard and Mouse Responsiveness" on page 161

### To configure custom latency reduction settings for an individual application

1. From the **Start** menu, select **All Programs** > **Citrix** > **Administration Tools** > **SpeedScreen Latency Reduction Manager**.
2. In the SpeedScreen Latency Reduction Manager, select the application.
3. From the **Application** menu, select **Properties.**

   The **Application Properties** tab containing existing SpeedScreen Latency Reduction settings for the selected application appears. It contains this information:

   - **Application Name.** The application executable name appears here; for example, Excel.exe.
   - **Path to Application.** The path to the application executable appears here; for example, C:\Microsoft Office\Excel.exe.
4. If desired, configure application settings:
   - **Disable local text echo for this application.** The current setting for Local Text Echo is displayed. Select the check box to disable Local Text Echo for this application. Clear the check box to enable it.
   - **Limit local text echo for this application.** The current Local Text Echo setting for the application appears. Select the check box to limit Local Text Echo functionality for this application, and select the type of text display you need from the drop-down list.
   - **Forces Speedscreen to treat all input fields in the selected application in native mode.** Select the check box if you configure a setting that forces SpeedScreen to treat all input fields in the selected application in native mode.

## Configuring Latency Reduction for Input Fields in an Application

Input fields in an application are fields where text can be added. You can use SpeedScreen Latency Reduction Manager to set latency reduction behavior for selected input fields in a configured application to reduce delays between when users enter text at the keyboard and when it is echoed or displayed on the screen.

### To configure latency reduction settings for input fields in an application

1. From the **Start** menu, select **All Programs** > **Citrix** > **Administration Tools** > **SpeedScreen Latency Reduction Manager**.
2. Select an application.
3. From the **Applications** menu, select **Properties**. The **Application Settings** window appears.
4. Select the **Input Field Configuration** tab, then configure these settings as needed.

    - **Configured Input Field List.** The list of configured input fields appears here. SpeedScreen Latency Reduction uses a window hierarchy to identify the input fields that need special settings. The entries shown in the tree view are the window class names of the configured fields. For example, _WwG is the window class name of the main document window in Microsoft Word.
    - **New**. Click this button to run the Advanced Input Field Compatibility wizard to add a new input field. This wizard guides you through the process of configuring SpeedScreen Latency Reduction settings for an input field.
    - **Delete.** To delete an input field, select an input field name from the list of configured input fields.

    - **Enable local text echo for this input field.** Select this check box to enable Local Text Echo. If this check box is selected, you can apply more Local Text Echo settings to the selected field.
    - **Limit local text echo.** Input fields in nonstandard applications may not behave correctly. Use these options to force the desired behavior. Select one of the two available settings.
        - **Display text in place.** Text is echoed in place.
        - **Display text in a floating bubble.** Text is echoed within a floating bubble.
    - **Reduce font size.** Input fields in non-standard applications may display misaligned text, oversized fonts, or other undesirable font

behavior. You can force the field to display text using a reduced font size to overcome this problem. Choose the percentage by which the font size is to be reduced. Percentage values available are 10%, 20%, and 30%.

- **Use system default colors.** SpeedScreen Latency Reduction tries to auto-detect the text and background colors used in input fields; however, non-standard input fields sometimes report incorrect or inadequate information. As a result, text echo in input fields on nonstandard applications can appear corrupted. To overcome this problem, use these settings to turn off auto-detection and force input fields to use system default colors.
  - **Both the text and background.** System default colors are applied to both text and background.
  - **The background only.** System default colors are applied only to the background.
- **Input field is a password.** Typically, hidden characters are located in password entry fields. Text echo in non-standard input fields might make these hidden characters appear as normal text, compromising security. Use these options to force non-standard input fields to display hidden characters as asterisks or spaces.
  - **Hidden characters denoted by "*".** Select this option if you want Local Text Echo for such input fields to be replaced by asterisks.
  - **Hidden characters denoted by spaces.** Select this option if you want Local Text Echo for password input fields to be replaced by spaces.

## Creating Exception Entries for Non-Standard Input Fields

Some input fields do not conform to standard Windows behavior and thus do not work correctly with SpeedScreen Latency Reduction. You can create exception entries for such fields, while still providing minimal latency reduction functionality for the rest of the application. The Input Field Compatibility wizard included with SpeedScreen Latency Reduction Manager guides you through the process of selecting non-standard input fields and creating exception entries for them.

---

**Note:** The application must be running before you can configure an input field within it.

---

### To create exception entries for non-standard input fields in an application

1. Start the application.
2. Select **Start** > **All Programs** > **Citrix** > **Administration Tools** > **SpeedScreen Latency Reduction Manager**.
3. From the **Applications** menu in SpeedScreen Latency Reduction Manager, select **Properties**. The **Application Settings** window appears.
4. Select the **Input Field Configuration** tab. Click **New** to start the wizard and follow the prompts.
5. With the application running, select the input field you want to configure and complete these steps:
   A. Drag the pointer onto the input field window for which SpeedScreen behavior needs to be customized.
   B. If the SpeedScreen Latency Reduction Manager window is obscuring the target input field, check the **Hide SpeedScreen Latency Reduction Manager** check box. This causes the SpeedScreen Latency Reduction Manager window to be hidden from view.
6. To define the level of compatibility for the input field, select the level of SpeedScreen Latency Reduction compatibility to apply to the selected input field. Use the slider bar to select the desired compatibility level.

   The default compatibility level is Auto, which provides full SpeedScreen Latency Reduction functionality. However, because the field being configured is not displaying the desired behavior, downgrade the latency reduction functionality level to Medium, Low, or Off.

   - **Medium Compatibility.** Use this level of compatibility for input fields that are incompatible with the default Auto setting. Text echo appears in place with limited acceleration.
   - **Low Compatibility.** If an input field is incompatible with both the Auto and Medium compatibility settings, select Low. Text echo appears in a floating text bubble rather than within the input field.
   - **Off, or Zero Compatibility.** If an input field is incompatible with Auto, Medium, and Low compatibility settings, disable Local Text Echo for that field by selecting **Off**.

Related topics:

“To adjust SpeedScreen Latency Reduction for an application” on page 162

# Configuring ICA Display Settings

You can configure common ICA display settings for all servers in a farm or select custom settings for an individual server.

## To configure ICA display settings for a farm

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **ICA** > **Display**.
4. Select the **Discard queue image that is replaced by another image** check box to improve response when graphics are sent to the client.

   Queued images that are replaced by another image are discarded. This is useful when bandwidth is limited. A drawback to selecting this option is that it can cause animations to become choppy because intermediate frames get dropped.
5. Select the **Cache image to make scrolling smoother** check box if you want to make scrolling smoother because sections of an image can be retrieved from the cache.
6. Enter the maximum memory to be used on the server for each client connection in the **Maximum memory to use for each session's graphics (KB)** box.

   You can specify an amount in kilobytes from 300 to 65536. Using more color depth and higher resolution for connections requires more memory. You can calculate the maximum memory required by using this equation:

   (color depth in bits per pixel / 8) * vertical resolution in pixels * horizontal resolution in pixels = memory required in bytes

   For example, if the color depth is 24, the vertical resolution is 600, and the horizontal resolution is 800, the maximum memory required is:

   (24bpp / 8) * 600 pixels * 800 pixels = 1440000 bytes of memory required

   You can specify 1440KB in maximum memory to handle ICA connections with these settings.
7. Under **Degradation bias**, select one of these options to prioritize when the session memory limit is reached.

   - **Degrade color depth first**. Select this option if you want color depth to be reduced before resolution is lowered when the session memory limit is reached.

- **Degrade resolution first**. Select this option if you want resolution to be lowered before color depth when the session memory limit is reached.

8. Select the **Notify user of session degradation** check box to display a brief explanation to the user when a session is degraded.

   Possible reasons for degradation include exceeding the memory limit and connecting with a client that cannot support the requested parameters.

### To configure ICA display settings for a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **ICA** > **Display**.
4. If you want the server to use the default farm settings, select the **Use farm settings** check box; otherwise, follow Steps 4 and 8 in "To configure ICA display settings for a farm" on page 168.

## Configuring ICA Browser Settings

ICA browser settings control whether or not a server responds to client broadcast messages. If these options are enabled, all servers in your network respond to broadcast messages. If you are running Program Neighborhood with HTTP Browsing, do not enable these options. This procedure applies only to environments with Program Neighborhood.

### To configure ICA browser settings for a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **ICA** > **Browser**.
4. Select either of these check boxes:

   - **Create browser listener on UDP network**. This setting is enabled by default. When enabled, this setting lets the ICA browser on the selected server respond to any ICA browser network packets on UDP networks. Each server that has this setting enabled has a listener on the network. Clearing this setting disables the listener for a server. In large environments, you may want to clear this check box on specific servers because having a listener enabled for every server on your network consumes network resources. Clearing this check box on

some servers in large environments allows you to optimize your network.

- **Server responds to client broadcast messages**. This setting is disabled by default. Enabling it makes configuring Program Neighborhood easier; users do not have to enter an address in Program Neighborhood for the server to which they want to connect. When enabled, this option allows the server it is enabled on to broadcast messages on the network and responds to messages clients broadcast.

# Securing Server Farms

The guidelines described in this topic provide general direction when planning secure Citrix environments:


- "Support for Microsoft Security Templates" on page 171
- "Securing Access to Your Servers" on page 171
- "Securing the Data Store" on page 172
- "Securing Network Communications" on page 174
- "Configuring User Authentication" on page 190
- "Logging Administrative Changes to a XenApp Farm" on page 195
- "Encrypting Sensitive Configuration Logging Data" on page 205


Consult with your organization's security experts for a comprehensive security strategy that best fits your needs.

## Support for Microsoft Security Templates

The Citrix XenApp plugins are compatible with and function in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security template is used. These templates are supported in the Microsoft Windows XP and Vista platforms. Refer to the Windows XP and Windows Vista security guides available at http://technet.microsoft.com for more information about the template and related settings.

## Securing Access to Your Servers

An important first step in securing your server farm is securing access to the servers. This topic includes recommendations for securing access.

**Securing XenApp Advanced Configuration.** The XenApp Advanced Configuration tool can be used to connect to any server in your farm. Run the tool only in environments where packet sniffing cannot occur. Also, ensure that only administrators have access to the tool. You can set NTFS permissions so that non-administrators do not have Execute permission for the tool executable (Ctxload.exe).

**Using NTFS partitions.** To ensure that appropriate access control can be enforced on all files installed by XenApp, install XenApp only on NTFS-formatted disk partitions.

**Installing and configuring the Simple Network Management Protocol (SNMP) service.** The SNMP service is not installed by default on computers running Windows Server 2003 and 2008. 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.

# 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 farm servers 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 XenApp.

---

**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 365.

---

More specific Citrix recommendations for securing the data store vary depending on the database you use for the data store. The following topics discuss security measures to consider for each of the database products XenApp supports.

---

**Important:** Be sure to create a backup of your data store before using `dsmaint config` to change the password on your data store.

---

**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.

**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 XenApp. Be sure to change the account permission back to db_owner before installing a service pack or feature release for XenApp.

**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 are those for the local system Administrator account. If users have access to the data store server, change the password with the `dsmaint config` command and keep the information in a safe place.

**Oracle.** If the data store is hosted on Oracle, give the Oracle user account employed 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 employed 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 topics 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 XenApp deployments:

- At the client-server level inside your network:

    - By encrypting the Independent Computing Architecture (ICA) protocol using SecureICA
    - Secure Socket Layer/Transport Layer Security (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
    - Proxy servers

# Securing Client-Server Communications

There are two methods for encrypting the session data transmitted between clients and servers: SecureICA and SSL/TLS encryption.

By default, all ICA 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 session data sent between a server running XenApp and a client. In general, increase the level of ICA protocol encryption when you want to encrypt internal communication within a LAN or a WAN, or you want to encrypt internal access to an intranet. Increasing the level of ICA protocol encryption prevents session data from being sent in clear text, 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. Enabling SSL/TLS ensures the confidentiality, authentication, and integrity of session data.

If you enable protection against both internal and external threats, you must enable SSL encryption. Using SecureICA with SSL or TLS provides end-to-end 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 XenApp plugin for Hosted Apps 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 XenApp 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 XenApp Advanced Configuration 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.

Plugins use the ICA protocol to encode user input (keystrokes and mouse clicks) and address it to a server farm for processing. Server farms use the ICA protocol to format application output (display and audio) 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 plugin software that cannot be upgraded to use SSL

- As an alternative to SSL/TLS encryption, when there is no 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 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 client devices 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 XenApp.

The nature of your environment may determine the way in which you enable SSL:

- For client devices communicating with your farm remotely, Citrix recommends that you use the Secure Gateway to pass client communications to the computer running XenApp. The Secure Gateway can be used with SSL Relay on the computer running XenApp to secure the Secure Gateway to XenApp traffic, depending on your requirements.
- For client devices communicating with your farm internally, you can do one of the following to pass client communications to the computer running XenApp:
    - Use the Secure Gateway with an internal firewall and place your farm behind the firewall
    - Use the SSL Relay feature 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.

If you are using Web Interface with the Secure Gateway, see the information about SSL in the *Secure Gateway Administrator's Guide* and the *Web Interface Administrator's Guide*.

## To configure session data encryption

The following procedure explains how to increase the level of encryption by enabling SecureICA (ICA protocol encryption) or SSL/TLS encryption after you publish an application.

1. In the Access Management Console, select a published application in the left pane by selecting **XenApp > *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 plugins 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 plugins in your environment, you must also enable encryption on the client side.

**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 this policy is enabled and you publish a resource at a lower level of encryption than the policy requires, the server rejects client connections. For plugins that take their encryption settings from the server, such as the Web Interface and the Citrix XenApp plugin, 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 XenApp Advanced Configuration tool, select **Policies**.
   B. From the **Actions** menu, click **New > Policy**.
2. Configure rules for the policy:
   A. In the right pane, select the policy name; on the **Actions** menu, click **Properties** to open then **Properties** page.
   B. From the list of folders in the left pane, select **Security > Encryption > SecureICA encryption**.
   C. Select **Enabled;** from the **Encryption Level** list box, select the encryption level you want for this policy.
3. Enable the policy by applying a filter.

For additional details about creating policies in general, see “Creating Policies” on page 81.

# Configuring SSL/TLS Between Servers and Clients

For XenApp to accept connections encrypted with SSL or TLS, you must use SSL Relay to configure support on each XenApp server.

Citrix SSL Relay can secure communications between clients, servers running the Web Interface, and XenApp servers that are using SSL or TLS. Data sent between the two computers is decrypted by the SSL Relay and then redirected using SOCKSv5 to the Citrix XML Service.

SSL Relay operates as an intermediary in the communications between the plugin and the Citrix XML Service running on each server. Each plugin authenticates the SSL Relay by checking the relay's server certificate against a list of trusted certificate authorities. After this authentication, the plugin 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 plugin, 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.

In general, use SSL Relay for SSL/TLS support when you:

- Want to secure communications with servers that host the Citrix XML Service.
- Have a small number of servers to support (five or fewer). To use SSL/TLS to protect against internal threats in larger farms, consider configuring SSL/TLS support with Secure Gateway.
- Do not need to secure access at a DMZ.
- Do not need to hide server IP addresses or you are using Network Address Translation (NAT).
- Need end-to-end encryption of data between clients and servers.

Configure SSL Relay and the appropriate server certificate on each XenApp server in the server farm. By default, SSL Relay is installed with XenApp in *C*:\Program Files (x86)\Citrix\SSLRelay, where *C* is the drive where you installed XenApp.

The Citrix XML Service provides an HTTP interface for enumerating applications available on the server. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The Citrix XML Service is included in the server. The default port for the Citrix XML Service is 80.

## Task Summary for Implementing SSL Relay

To implement the SSL Relay, perform the following steps:

| Task | See this topic |
|---|---|
| Obtain and install server and root SSL certificates. | "Obtaining and Installing Server and Root SSL Certificates" on page 181 |
| Enable the SSL relay and select the server certificate in the **Relay Credentials** tab of the SSL Relay Configuration Tool. | "To enable the SSL Relay and select the relay credentials" on page 183 |

| Task | See this topic |
| --- | --- |
| Use the features available from the **Connection** tab to change the target server or port, or add servers for redundancy. | "TCP Ports and the SSL Relay" on page 183<br><br>"Using the SSL Relay with the Microsoft Internet Information Service (IIS)" on page 184<br><br>"Configuring the Relay Port and Server Connection Settings" on page 184 |
| Use the features available from the **Ciphersuites** tab of the SSL Relay Configuration Tool to select which ciphersuites to allow. | "Configuring the Ciphersuites Allowed by the SSL Relay" on page 186 |

## Installing and Configuring the SSL Relay Tool with User Account Control Enabled

If you configure the SSL Relay tool with the User Account Control (UAC) feature of Microsoft Windows enabled, you might be prompted for administrator credentials. To run the SSL Relay tool, you must have privileges and associated permissions as follows:

- Domain administrator
- Delegated administrator
- Administrator group of the local computer where you are installing the tool

## Obtaining and Installing Server and Root SSL Certificates

A separate server certificate is required for each XenApp server on which you want to configure SSL or TLS. 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.

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 stand-alone snap-in.

### Choosing an SSL Certificate Authority

You can obtain and install certificates for your servers and client devices in the following ways:

- **Certificates from a CA bundled with the operating system.** Some of the newer Windows operating systems 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.
- **Certificates from an enterprise CA.** If your organization makes a CA accessible to you for use, that CA appears 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.
- **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 installed manually 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.

## To enable the SSL Relay and select the relay credentials

1. On the server where you installed Citrix SSL Relay, click **All Programs** > **Citrix** > **Administration Tools** > **Citrix SSL Relay Configuration Tool**.
2. Click the **Relay Credentials** tab.
3. Select the **Enable SSL relay** check box to enable the relay features.
4. Select the **Display Friendly Name** check box to display the certificate's friendly name, if available.

   This check box determines which information from the certificate appears in the **Server Certificate** list. Some certificates contain an additional friendly name field. If you check this box and no friendly name exists, the certificate's subject common name is used (which is typically the server name). If **Display Friendly Name** is not checked, the entire subject name is used.
5. Select the server certificate from the **Server Certificate** drop-down box (used to identify the SSL Relay identity).

## TCP Ports and the SSL Relay

The SSL Relay relays packets only to the target computers listed on the **Connection** tab. By default, the SSL Relay is configured to relay packets only to the target computer on which the SSL Relay is installed. You can add other computers in the same server farm for redundancy through the **Connection** tab. See "Configuring the Relay Port and Server Connection Settings" on page 184.

**Note:** You can configure the SSL Relay to relay packets to any port and any server, but this is not recommended because it is a security vulnerability.

See "Configuring TCP Ports" on page 189 for a list of ports used in a server farm.

## Using the SSL Relay with the Microsoft Internet Information Service (IIS)

To use the SSL Relay and Microsoft Internet Information Services (IIS) on the same server, for example, if you install the Web Interface and XenApp on the same server, you must change the port number that IIS or the SSL Relay use. SSL Relay uses TCP port 443, the standard port for SSL connections. Most firewalls open this port by default. Optionally, you can 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.

Microsoft IIS is installed by default on Windows Server 2003 and allocates port 443 for SSL connections. It is not installed by default on Windows Server 2008. To run SSL Relay on a server running Windows Server 2003 or 2008 (with Web Server IIS installed and enabled), you must:

- Install a server certificate on IIS before you change the port number. You can use the same server certificate with IIS and the SSL Relay.
- Configure IIS to use a different port or configure the SSL Relay to use a different port.

To change the SSL port for Internet Information Services, see the relevant Microsoft documentation.

## Configuring the Relay Port and Server Connection Settings

Use the **Connection** tab to configure the listener port and allowed destinations for the SSL Relay. The SSL Relay relays packets only to the target computers listed on the **Connection** tab. The target server and port specified on your server running the Web Interface or XenApp plugin must be listed on this tab. By default, no servers are listed.

Once a certificate is added, the default ICA and Citrix XML Service ports are added for the local computer.

- **Relay Listening Port.** The TCP port where SSL clients connect to the SSL Relay. The default port number is 443. If your server has multiple IP addresses, this port is used on all of them. If you change this value, you must make the same change on the client device. You may also need to open the port on any firewalls between the client device and the SSL Relay.

- **Encryption Standard.** SSL Relay can be configured to use either SSL or TLS. The protocol that is required is configured using the SSL Relay configuration tool.
- **Server Name.** The fully qualified domain name (FQDN) of the server to which to relay the decrypted packets. If certificates are not configured, no servers are listed. If certificates are configured, the FQDN of the server on which the SSL Relay is running appears here.
- **Ports.** The TCP ports where ICA and the Citrix XML Service are listening.

---

**Important:** If you change the default Citrix SSL Relay port, you must set SSLProxyHost to the new port number in the Citrix XenApp Plugin for Hosted Apps icaclient.adm file. For more information about client settings, see the *XenApp Plugin for Hosted Apps Administrator's Guide*.

---

#### To add a server to the destination server list

1. On the server where you installed Citrix SSL Relay, click **All Programs** > **Citrix** > **Administration Tools** > **Citrix SSL Relay Configuration Tool**.
2. Click the **Connection** tab and click **New**.
3. Type the FQDN of the computer in the **Server Name** box or click **Any** to allow connections to any server.
4. Type the port number of the Citrix XML Service in the **Destination ports** box and click **Add**. Type the port number where ICA is listening in the **Destination Ports** box and click **Add**.

These additional servers must also be specified in the configuration of servers running the Web Interface.

#### To change the port for a server listed in the destination server list

1. If you did not already do so, select the **Connection** tab.
2. Click the entry that you want to edit to select it.
3. Click **Edit** to display the **Target Server Properties** dialog box.
4. Select a destination port to remove and click **Delete**.
5. In the field below **Destination ports**, type the number of the new destination port and click **Add**.

To allow connections to any port on any server, click the **Any** button.

#### To run the 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.

The SSL Relay uses port 443 before IIS, including when the server is restarted.

---

**Note:** When you install XenApp, members of the User group are allowed to edit registry entries in the registry hive HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Secure\Citrix\Citrix SSL Relay, or HKEY_LOCAL_MACHINE\SOFTWARE\Secure\Citrix\Citrix SSL Relay on XenApp, 32-bit Edition. You can use the Microsoft Security Configuration and Analysis tool to prevent members of the User group from editing these registry entries.

---

## Configuring the Ciphersuites Allowed by the SSL Relay

Use the **Ciphersuites** tab to configure which combinations of ciphersuites the SSL Relay will accept from the client (a server running the Web Interface or XenApp plugin). The **Ciphersuites** dialog box lists the available and allowed ciphersuites. The SSL Relay accepts connections only from clients that support at least one of the allowed ciphersuites. Installing additional ciphersuites is not supported.

Available ciphersuites are grouped into GOV (Government) or COM (Commercial). Note that GOV ciphersuites are normally used when TLS is specified. However, any combination of ciphersuite and security protocol can be used. Contact your organization's security expert for guidance about which ciphersuites to use.

Descriptions of ciphersuites are found in Appendix C of the Internet Society RFC 2246, available online at http://www.rfc-editor.org.

By default, connections using any of the supported ciphersuites are allowed.

### To configure ciphersuites used by the SSL Relay

1. On the server where you installed Citrix SSL Relay, click **All Programs** > **Citrix** > **Administration Tools** > **Citrix SSL Relay Configuration Tool**.
2. Select a ciphersuite from either the left column and click **Add** to allow it or from the right column and click **Remove** to disallow it.

# 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 XenApp
- 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 XenApp. 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 XenApp, including the servers hosting the Citrix XML Service.

For more information about implementing and configuring the Secure Gateway, see the *Secure Gateway for Windows 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 XenApp. These session tickets form the basis of authentication and authorization for access to published resources.

When you install XenApp, you also install the STA. 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. From the **Performance Object** drop-down list, select **Secure Ticket Authority**.
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:

```
stayyyymmdd-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 XenApp and Web browsers from the Internet and publicly accessible networks. To deploy XenApp on internal networks, secure communications between the client and server by means of SSL/TLS or other security measures.

## Configuring TCP Ports

The table below lists the TCP/IP ports that servers, Citrix XenApp Plugin for Hosted Apps, 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 |
|---|---|---|
| Access Management Console | 135 | Not configurable. |
| Citrix SSL Relay | 443 | See "Using the SSL Relay with the Microsoft Internet Information Service (IIS)" on page 184 for configuration instructions. |
| Citrix XML Service | 80 | See the information about configuring the XML Service port in the *Citrix XenApp Installation Guide* for configuration instructions. |
| Client-to-server (directed UDP) | 1604 | Not configurable. |
| ICA sessions (clients to servers) | 1494 | See "ICAPORT" on page 371 for instructions about changing the port number. |
| License Management Console | 8082 | See the *Getting Started with Citrix Licensing Guide* for more information. |
| XenApp Advanced Configuration to server | 2513 | See "Citrix XenApp Commands Reference" on page 347 for information about the IMAPORT command. |
| Server to license server | 27000 | In the console, open the farm or server properties page, and select License Server. |
| Server to Microsoft SQL or Oracle server | 139, 1433, or 443 for MS-SQL | See the documentation for the database software. |
| Server to server | 2512 | See "Citrix XenApp Commands Reference" on page 347 for information about the IMAPORT command. |
| Session reliability | 2598 | See "Configuring Session Reliability" on page 120. |

## Using Proxy Servers

A proxy server accepts connection requests from client devices and redirects those requests to the appropriate XenApp servers. Using a proxy server, much like using a firewall, gives you more control over access to the XenApp servers and provides a heightened level of security for your network. A proxy server, as opposed to a firewall, uses a different port from that used by the XenApp servers.

For information about using proxy servers with the Citrix XenApp Plugins for Hosted Apps, see the *Citrix XenApp Plugin for Hosted Apps Administrator's Guide*.

Supported proxy servers are:

- Microsoft Internet Security and Acceleration (ISA) Server 2004 and 2006
- iPlanet Web Proxy Server 3.6
- Squid 2.6 STABLE 4
- Microsoft Proxy Server 2.0

# Configuring User Authentication

Part of securing your server farm is making sure that only properly authenticated users can access your servers and resources. The following topics describe how to configure authentication for users in your farm:

- "Configuring Authentication for Workspace Control"
- "Configuring Kerberos Logon"
- "Using Smart Cards with Citrix XenApp"

## 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 "Ensuring Session Continuity for Mobile Workers" on page 119.

You do not need to set up a trust relationship if your users authenticate to the Web Interface or XenApp Plugin for Hosted Apps 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 among servers running the Web Interface and servers running XenApp.

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 XenApp Plugin for Hosted Apps features 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 users 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 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 XenApp 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 left pane of the Access Management Console, select the Farm node and select **Action > Modify farm properties > Modify all properties**.
2. From the farm's **Properties** list, open the **XenApp** page 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 server

**Caution:** Using Registry Editor 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.

To prevent Kerberos authentication for users on a specific server, create the following registry key as a DWORD Value on the server:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Logon\
DisableSSPI = 1

**Note:** On XenApp, 32-bit Edition, create the key in this location:
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Logon\DisableSSPI = 1

You can configure the XenApp Plugins to use Kerberos with or without pass-through authentication.

## Windows Server 2008 User Access Control and Administrator Sessions

The User Access Control feature of the Windows Server 2008 operating system prompts users to enter their credentials when all of the following requirements are met:

- Kerberos logon is enabled on a computer hosting the Windows 2008 Server operating system and running XenApp
- Users logging on to the computer running XenApp are members of the Administrator group on that computer

- After logon, Administrator group users attempt to access network resources such as shared folders and printers.

# Using Smart Cards with Citrix XenApp

You can use smart cards in your XenApp environment. Smart cards are small plastic cards with embedded computer chips.

In a XenApp 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:** XenApp 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 XenApp. For details about configuring the Web Interface for smart card support, see the *Web Interface Administrator's Guide*.

## Smart Card Requirements

The following topic presents the basic guidelines for using smart cards with XenApp. 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 XenApp plugin:

- 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.

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.

If you are using pass-through authentication to pass credentials from your client device to the smart card server session, CSP software must be present on the client device.

## 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 XenApp.

### Setting Windows Policies for Smart Cards

Microsoft Windows supports two security policy settings for interactive logon to a server session. Citrix XenApp plugin 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 or plugins support smart cards:

- Citrix XenApp Plugin for Hosted Apps
- Client for Linux
- Client for Windows-based terminals
- Client for MacIntosh

To configure smart card support for users of these plugins and clients, see the administrator's guide for the plugins and clients in your environment.

## Logging Administrative Changes to a XenApp Farm

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 Advanced Configuration tool, 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:

- 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 XenApp administrators enter credentials before clearing logs. See "Clearing the Log" on page 203.
- 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 Configuration Logging Properties" on page 202.
- Determine if you want to allow administrators to be able to clear configuration logs and if you want them to have to supply credentials for this purpose. This requires the permission to Edit Configuration Logging settings.

# Enabling Configuration Logging

This topic details the steps that are needed before Configuration Logging can be used.

- 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

The Configuration Logging feature supports Microsoft SQL Server 2005 and 2008 and Oracle Version 10.2 and 11.1 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 XenApp 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 XenApp 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 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 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.
- 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.

- Before running the Access Management Console, you must update the Oracle tnsnames.ora client file to include the connectivity information needed to access the available databases.
- If you are using Oracle Version 10.2, Citrix recommends that you apply the Oracle patch 10.2.0.1.4P (patch 4; patchset 4923768) and any subsequent patches. These patches ensure that the Oracle client software can operate correctly if installation directories contain a parenthesis character; for example, a directory folder named **Program Files/(x86)**.

## Defining Database Permissions for Configuration Logging

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. XenApp then creates the database schema, tables, and stored procedures. To create a database schema, XenApp needs full access to the database as described in "Setting up the Configuration Logging Database" on page 196. After the database schema is created, full access is no longer necessary and you have the option of creating additional users with fewer 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)<br>(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)<br>(Oracle also requires **SELECT** for sequence objects and the *create session* system privilege) |

| Configuration Logging task | Database permissions needed |
|---|---|
| To create a report | **EXECUTE** for the Citrix Configuration Logging stored procedures<br>**SELECT** for *sysobjects* and *sysusers* (SQL Server) or *sys.all_objects* (Oracle)<br>(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 XenApp, 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 left pane of the Access Management Console, select a farm.
2. In the task pane, under Common Tasks, click **Modify farm properties > Modify configuration log properties**.
3. In the **Configuration Logging** dialog box, click the **Configure Database** button to open the 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

- The logon credentials for the database user that were created when you set up the Configuration Logging database

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 provide a net services name as well as the logon credentials. The net services names listed in the Data Source drop-down list are in the Oracle tnsnames.ora client file. 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.

---

---

**Note:** After you configure the connection to the Configuration Logging database, you cannot set the database back to **None**. To stop logging, clear the **Log administrative tasks to Configuration Logging database** check box in the **Configuration Logging** dialog box.

---

## To configure a SQL Server database for configuration logging

1. Under **Database configuration** on the **Configuration Logging** page of your **Farm Properties** dialog box, click **Configure Database**.
2. On the **Select Connection Details** page, select **SQL Server** as a connection type.
3. Use the drop-down list to select a SQL Server. You can also enter a server name manually if the server is available but does not appear in the drop-down list.
4. Select **Use Windows integrated security** (recommended) or **Use SQL Server authentication**.
5. Enter a valid user name and password for your SQL Server database.
6. Click **Next**. The **Select Database** page opens. Use the **Specify the database** drop-down list to enter the name of your database. You can also enter a database name manually here.
7. Click **Next**. The **Select Advanced Options** page opens. Configure the following connection and connection pooling options:

- Connection options comprise **Connection time-out (seconds)**, **Packet size (bytes)**, and **Use encryption**.
- Under Connection pooling on the database server, if desired, clear **Connection pooling enabled**. This disables the Connection Pooling feature.

---

**Note:** It is not necessary to modify the default values of these settings for the configuration to work. A possible exception is the **Use encryption** setting. For security reasons the default value of this setting is **Yes**. However if the SQL Server database server you are connecting to does not support encryption, the connection will fail. Click the **Test Database Connection** button on the **Check New Connection Summary** page to check whether or not the database supports encryption. If it does not, an error message to that effect is returned.

---

8. Click **Next**. The **Check New Connection Summary** page opens with a summary of the settings you configured. Click **Back** to return and alter any settings if required.
9. Click **Test Database Connection**. A dialog box appears telling you whether or not the connection was successfully established.

## To configure an Oracle database for configuration logging

1. Under **Database configuration** on the **Configuration Logging** page of your **Farm Properties** dialog box, click **Configure Database**.
2. On the **Select Connection Details** page, select **Oracle** as an information type. This selection dynamically changes some of the information for which you will be asked.
3. Use the drop-down list to select a net service name. You can also enter a net service name manually.
4. Enter a valid user name and password for your Oracle database.
5. Click **Next**. The **Select Advanced Options** page opens. Configure the following connection and connection pooling options.
   - Connection options comprise **Connection time-out (seconds)**, **Packet size (bytes)**, and **Use encryption**.
   - Under Connection pooling on the database server, if desired, clear **Connection pooling enabled**. This disables the Connection Pooling feature.

**Note:** It is not necessary to modify the default values of these settings for the configuration to work.

6. Click **Next**. The **Check New Connection Summary** page opens with a summary of the settings you configured. Click **Back** to return and alter any settings if required.
7. Click **Test Database Connection**. A dialog box appears telling you whether or not the connection was successfully established.

## Setting Configuration Logging Properties

After establishing a connection to the database, you enable the Configuration Logging feature, allow or prohibit changes to the farm when the Configuration Logging database is offline, and require authorization of administrators when clearing logs.

### To set Configuration Logging properties

Before you set Configuration Logging properties, ensure a SQL Server or Oracle database is configured. Otherwise, the Log Tasks and Clearing log areas of the Configuration Logging page are not active.

1. In the left pane of the Access Management Console, select a farm.
2. In the task pane, under Common Tasks, click **Modify farm properties > Modify configuration log properties**.
3. Under **Log tasks**, select **Log administrative tasks to logging database** to enable configuration logging.

   If you want administrators to be able to make changes to the farm when the database is disconnected, select **Allow changes to the farm when database is disconnected**, which becomes available when configuration logging is enabled.
4. To prompt administrators to enter their credentials before clearing the log, under **Clearing log**, select the **Require administrators to enter database credentials before clearing the log** check box.

**Note:** A Citrix administrator requires the Edit Configuration Logging Settings permission to change any Configuration Logging settings or clear the log.

## 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.

# Working with Configuration Logs

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 left pane of the Access Management Console, select a farm.
2. In the task pane, under Common Tasks, click **Modify farm properties > Modify configuration log properties**.

## 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 in Configuration Logging properties. This ensures only database users with permissions to clear logs can clear them. Therefore, anyone attempting to clear the log is 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, XenApp impersonates the database user when it connects to the SQL database, so you must enter the credentials for the Windows user account

### To clear log entries from the Configuration Logging database

1. From the left pane of the Access Management Console, select a farm.
2. From the task pane, under **Other Tasks**, click **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 XenApp are logged and appear in the reports that are generated.

The supported versions of Microsoft SQL Server are verified for MDAC 2.8.

---

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 appears 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.

### To generate a Configuration Logging report

1. In the left pane of the Access Management Console, select the **Report Center** node.
2. In the task pane under **Common Tasks**, click **Generate report**.
3. From the **Report type** drop-down list, select **Configuration Logging Report**.
4. Click **Next** to start the Configuration Logging Report wizard. Follow the steps in the wizard to generate a report.

**Note:** If you are using SQL Server or Oracle database authentication, the **Allow saving password** check box must be selected.

# Encrypting Sensitive Configuration Logging Data

Independent Management Architecture (IMA) is the underlying architecture used in XenApp for configuring, monitoring, and operating all XenApp functions. The IMA data store stores all XenApp 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 after encryption 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 a command-line utility that you can use to manage IMA encryption and generate key files. CTXKEYTOOL is in the Support folder of the XenApp media.

- **A key file.** The key file 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 the information about planning for IMA encryption in the *Citrix XenApp Installation Guide*.

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 topics 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 XenApp 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 210.

---

# Using the IMA Encryption Utility

Citrix provides a utility for performing various administrative functions after you install XenApp. 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 362.

## Storing the IMA Encryption Utility Locally

If you want to run the utility locally, perform the following procedure:

### To copy the key to a local computer

1. Copy the CTXKEYTOOL.exe file from the Support folder of the XenApp media 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 to the new 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 in which they were stored on the media.

# Enabling IMA Encryption After Installation

You can enable IMA encryption after you install or upgrade to XenApp. 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 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 on which it will be used; 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."

   You must have a key on every server in the farm for IMA encryption to work correctly.
7. Continue to the next procedure to load the key to each server.

## 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) because 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 the 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 computer 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. 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 (as 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 computer that will be joining the farm and to the administrator performing the installation.

# 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 Citrix XenApp 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 to the server, note that adding a key to a server with the same name as an existing key overwrites the existing key.

You cannot enable IMA encryption when you join a farm, either during Setup or when changing farms, if you are logged on as a local administrator and you attempt to connect to the data store indirectly. For more information, see the *Citrix XenApp Installation Guide*.

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 disabled automatically on the server you are moving.

Related topics:

"Changing XenApp Farm Membership" on page 301

"CHFARM" on page 358

# Other IMA Encryption Features

This topic 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" on page 362.

## Retrieving Lost Keys

It is possible to recreate a key file that you accidentally deleted, if, for example, you need it to join a new server to the farm. Because all servers in the same farm use the same key, you can obtain a key from another server on the farm. XenApp 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 362.

## Disabling IMA Encryption

You can disable IMA encryption by running the `ctxkeytool disable` command on any server in the farm. Because 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 the Configuration Logging database, you must reenter 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.

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 362.

# XenApp Service Account Privileges

This topic provides information about the services installed by default with XenApp, their accounts, associated permissions, and privileges.

**XenApp Services Overview**

The table that follows lists the display name for the service, which is the name that appears in the Services panel. When the display name and the service name differ, the table provides service name in (parentheses). The Dependencies column in the table lists the system components, such as Windows services, Citrix services, or drivers, on which the service depends. The Dependencies column also includes sub-dependencies that may not appear on the **Dependencies** tab for the service.

Licensing services, which are not listed here, might also appear if the license server is installed on the same server as XenApp.

| Display Name (Service Name) | Executable | Logon Account / Startup Type | Description | Dependencies |
|---|---|---|---|---|
| Citrix 64-bit Virtual Memory Optimization | ctxsfosvc64.exe | Local System<br>Manual | Dynamically optimizes 64-bit applications running on a XenApp server. | None |
| Citrix Client Network<br>(CdmService) | cdmsvc.exe | Local System<br>Automatic | Maps client drives and peripherals for access in sessions. | Client Drive Mapping (CDM)<br>Windows Management Instrumentation Driver Extensions<br>Workstation |

| Display Name (Service Name) | Executable | Logon Account / Startup Type | Description | Dependencies |
|---|---|---|---|---|
| Citrix CPU Utilization Mgmt/ CPU Rebalancer<br>(CTXCPUBal) | ctxcpubal.exe | .\ctx_cpuuser<br>Manual | One of the services for the CPU Utilization Management feature.<br>This service enhances resource management across multiple CPUs.<br>This service is installed only on servers that have multiple CPUs. | None |
| Citrix CPU Utilization Mgmt/ Resource Mgmt<br>(ctxcpuSched) | ctxcpusched.exe | Local System<br>Manual | One of the services for the CPU Utilization Management feature.<br>Manages resource consumption to enforce entitlement policies. | Remote Procedure Call (RPC) |
| Citrix Diagnostic Facility COM Server<br>(CdfSvc) | CdfSvc.exe | NT AUTHORITY\ Network Service<br>Automatic | Manages and controls diagnostic trace sessions, which are used to diagnose problems on a XenApp server. | Remote Procedure Call (RPC) |
| Citrix Encryption Service | encsvc.exe | NT AUTHORITY\ Local Service<br>Automatic | Enables secure communication with RC5 128-bit encryption between XenApp Plugins and XenApp. | Windows Management Instrumentation Driver Extensions |
| Citrix End User Experience Monitoring<br>(Citrix EUEM) | SemsService.exe | Local Service<br>Manual | Collects and collates end-user experience measurements. | Citrix SMC Support Driver |
| Citrix Health Monitoring and Recovery<br>(CitrixHealthMon) | HCAService.exe | NT AUTHORITY\ Local Service<br>Automatic | Provides health monitoring and recovery services in the event problems occur. | Citrix Independent Management Architecture service<br>Terminal Services |

| Display Name (Service Name) | Executable | Logon Account / Startup Type | Description | Dependencies |
|---|---|---|---|---|
| Citrix Independent Management Architecture<br>(IMAService) | ImaSrv.exe | NT AUTHORITY\ NetworkService<br>Automatic | Provides management services in the XenApp farm. | Citrix Services Manager service<br>IPsec Policy Agent<br>Remote Procedure Call (RPC)<br>TCP/IP Protocol Driver<br>Server<br>Windows Management Instrumentation Driver Extensions<br>Workstation |
| Citrix MFCOM Service<br>(MFCom) | mfcom.exe | NT AUTHORITY\ NetworkService<br>Automatic | Provides COM services that allow remote connections from the management tools. | Remote Procedure Call (RPC)<br>Citrix Independent Management Architecture service<br>Citrix Services Manager service |
| Citrix Print Manager Service<br>(cpsvc) | CpSvc.exe | .\ctx_cpsvcuser<br>Automatic | Manages the creation of printers and driver usage within XenApp sessions.<br>This service supports the Citrix Universal Printing features. | Print Spooler<br>Remote Procedure Call (RPC) |
| Citrix Secure Gateway Proxy<br>(CtxSecGwy) | CtxSGSvc.exe | NT AUTHORITY\ Network Service<br>Automatic | Proxy to the Citrix Secure Gateway server. | None |

| Display Name (Service Name) | Executable | Logon Account / Startup Type | Description | Dependencies |
|---|---|---|---|---|
| Citrix Services Manager<br>(IMAAdvanceSrv) | IMAAdvanceSrv.exe | Local System<br>Automatic | Provides XenApp with an interface to the operating system. Other services use this services to perform elevated operations. | None |
| Citrix Streaming Service<br>(RadeSvc) | RadeSvc.exe | .\Ctx_StreamingSvc<br>Automatic | Manages the Citrix XenApp Plugin for Streamed Apps when streaming applications. | Remote Procedure Call (RPC) |
| Citrix Virtual Memory Optimization | CTXSFOSvc.exe | Local System<br>Manual | Dynamically optimizes applications running on a XenApp server to free up server memory. | None |
| Citrix WMI Service<br>(CitrixWMIservice) | ctxwmisvc.exe | NT AUTHORITY\ Local Service<br>Manual | Provides the Citrix WMI classes for information and management purposes. | Citrix Independent Management Architecture service<br>Citrix Services Manager service<br>IPsec Policy Agent<br>Remote Procedure Call (RPC)<br>TCP/IP Protocol Driver<br>Server<br>Windows Management Instrumentation Driver Extensions<br>Workstation |

| Display Name (Service Name) | Executable | Logon Account / Startup Type | Description | Dependencies |
|---|---|---|---|---|
| Citrix XML Service (CtxHttp) | ctxxmlss.exe | Network Service Automatic | Services XML data requests sent by XenApp components | None |
| Citrix XTE Server (CitrixXTEServer) | XTE.exe | NT AUTHORITY\ NetworkService Manual | Services network requests for session reliability and SSL from XenApp components. | None |

The tables that follow detail the user accounts for Citrix services.

**Caution:** Citrix does not recommend altering account permissions and privileges. If you delete the accounts or alter their permissions incorrectly, XenApp might not function correctly.

### Permissions for Service User Accounts

The following table lists the permissions associated with accounts XenApp services use.

| Account Name | Permissions | Notes |
|---|---|---|
| Local Service | Limited | NT AUTHORITY\LocalService |
| Network Service | Limited, network resources | NT AUTHORITY\NetworkService |
| Local System | Administrator | NT AUTHORITY\System |
| Ctx_StreamingSvc | Domain or local user | Acts as a User |
| ctx_cpsvcuser | Domain or local user | Acts as a Power User |
| Ctx_ConfigMgr | Domain or local user | Acts as a Power User |
| Ctx_CpuUser | Domain or local user | Acts as a User |

### Privileges for Service User Accounts

If your organization requires that service accounts run as domain accounts and not as local accounts, you can create domain accounts to replace the ctx_cpsvcuser, Ctx_ConfigMgr, and Ctx_CpuUser accounts before installing XenApp and specify the new accounts during Setup. Citrix does not support changing the account for the Citrix Streaming Service (Ctx_StreamingSvc). Follow the guidelines in the *Citrix XenApp Installation Guide*, and ensure the new account has the same privileges as the default account.

The following table indicates the privileges XenApp service accounts require.

| Privileges | Local Service | Network Service | Ctx_StreamingSvc | ctx_cpsvcuser | Ctx_ConfigMgr | Ctx_CpuUser |
|---|---|---|---|---|---|---|
| Change the system time | x | x | | | | |
| Generate security audits | x | x | | | | |
| Increase quotas | x | x | | | | |
| Load and unload device drivers | | | | x | | |
| Log on as a batch job | x | x | x | x | x | x |
| Log on as a service | x | x | x | x | x | x |
| Replace a process level token | x | x | x | | | |
| Restore files and directories | | | x | | | |
| Debug programs | | | | | | x |
| Increase scheduling priority | | | | | | x |

# Understanding XenApp Printing

Configuring and administering printing in multiuser environments, such as XenApp and Terminal Services, is by nature more complex than administering printing in a single-user Windows environment. The complexity stems from the difficulties in preserving printing settings in a dynamic workspace, the instability that can result from drivers that were not tested for multiuser environments, and the burden of driver management across a large number of servers.

Because of the multiuser, non-persistent nature of a XenApp environment, there are differences in how print jobs are routed and how printing to network and local printing devices works in a Citrix environment.

Managing printers in a XenApp environment is a multistage process. The cycle for managing printers on a farm requires that you:

1. Design your printing configuration. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and what a realistic printing management model would look like for your organization (that is, assessing that the administrative overhead of printing pathway you choose is realistic in your environment).
2. Configure your printing environment, including creating the policies necessary to deploy your printing design.
3. Test a pilot printing deployment before rolling it out to users.
4. Maintain your Citrix printing environment, including updating policies when new employees or servers are added and maintaining drivers on your farm servers.
5. Troubleshoot issues that may arise in your printing environment.

Before you begin planning your deployment, make sure that you understand these major concepts for printing in XenApp:

- The concept of printer provisioning in a session and the two major types of provisioning (auto-created and self-provisioned). To understand these concepts, you need to understand, among other things, the difference between a printer, a printing device, and a printer driver.

- How print jobs can be routed in XenApp.
- The policies that you can create to manage drivers.

XenApp printing concepts build on Windows printing concepts. To configure and successfully manage printing in a Citrix environment, you must understand how Windows network and client printing works and how this translates into printing behavior in a Citrix environment.

Related topics:

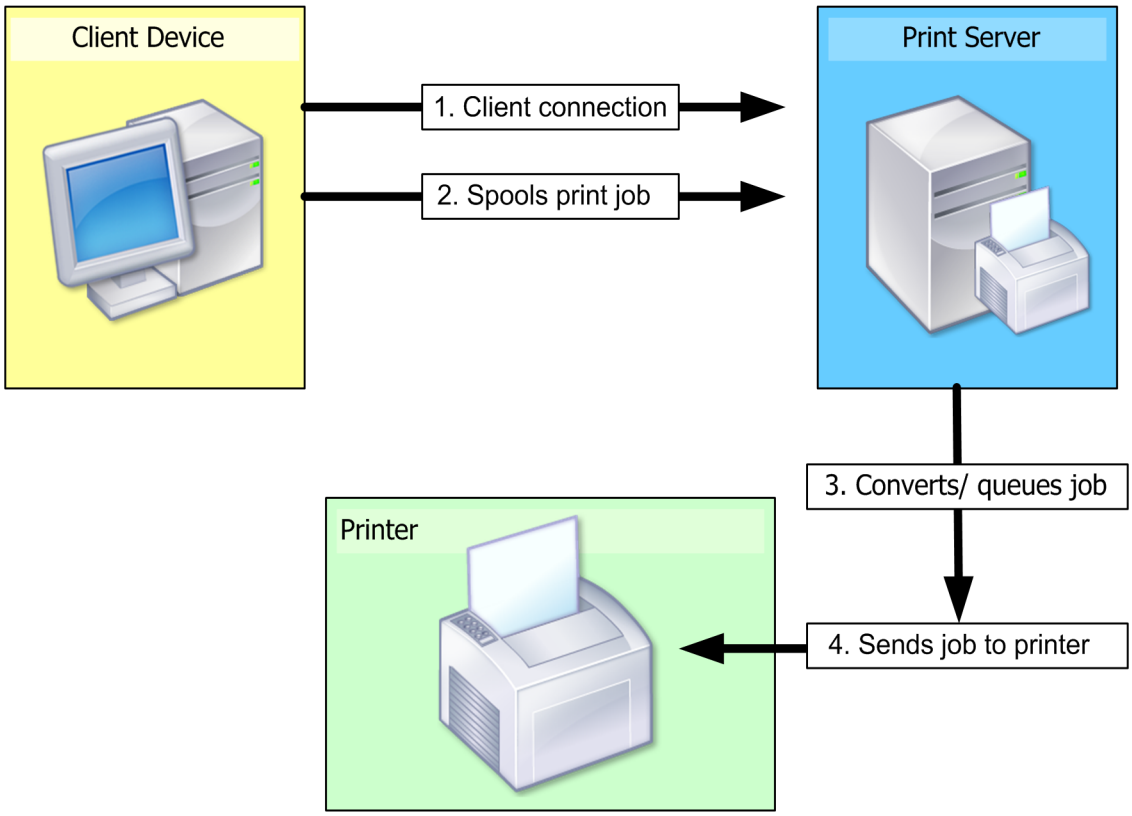
"Introduction to Windows Printing Concepts" on page 218

"XenApp Printing Concepts" on page 222

# Introduction to Windows Printing Concepts

This section provides a limited overview of basic printing concepts in a standard (non-Terminal Services) Windows environment. However, Citrix recommends reviewing the Windows documentation about network printing, print servers, and Terminal Services printing before learning about Citrix printing concepts.

In a Windows environment, you can either print from your computer to a locally attached desktop printer (for example, a printer on LPT1 or COM1) or you can print to a *network printer* that is managed by a *print server*.




*This diagram shows how print jobs are spooled from the client device to a print server and then sent to the printing device in a Windows network.*

Here are a few basic definitions:

- **Printing Device**. In the context of this topic, the term *printing device* refers to the physical printer (that is, the hardware device to which you send print jobs).
- **Printers**. The term *printer* refers to the software representation of a printing device. Computers must store information about printers so they can find and interact with printing devices. When you see printer icons in the Printers panel in the Control Panel, you are seeing the software representation of the printers. (You are not seeing the printer drivers.)

  For clarity, the term *printer object* is sometimes used to denote the software representation of a printing device.
- **Printer driver**. The *printer driver* is the software program that lets the computer communicate with this hardware device. This program converts the information to be printed to a language that the printing device can

process. It also understands the device and job settings of the printing device and presents a user interface for users to configure these. In Windows systems, printer drivers are distinct from the software representation of printers.

- **Print job**. When a user prints a document, the data sent to the printer is known as a *print job*. Jobs are queued to the printer in a specific sequence, which the *print spooler* controls. When this sequence appears, it is known as the *print queue*.
- **Print spooler**. The spooler is the Windows service that manages printer objects, coordinates drivers, lets you create new printers, determines where print jobs are processed, and manages the scheduling of print jobs. The print spooler also determines if the printer prints each page as it receives it or if the printer waits until it receives all pages to print the job.

  Typically, when a print job is spooled to a printer, the spooler loads documents into a buffer. The printing device then retrieves the print jobs from the buffer when it is ready to print the job. By storing the job, the computer can perform other operations while the printing occurs in the background.
- **Print queue**. A sequential, prioritized list of the print jobs waiting to be printed. The spooler maintains this list for each printer object in the computer.
- **Print server**. A computer that manages the communications between client devices and printers. In this context, the term *print server* refers to dedicated computers that are running a Windows server operating system and hosting *x* number of shared printers. Print servers provide client workstations with drivers they need to print and store files, or print jobs, in a print queue until the printer can print them. A print server is a remote print spooler.
- **Network printer**. A shared printer object accessed through a network print server.

Related topics:

"XenApp Printing Concepts" on page 222

# Local and Remote Print Job Spooling

Print job spooling is important because where print jobs are spooled to is where print jobs are *processed*. Processing location affects network traffic, resource utilization, and has additional implications in a XenApp context.

Print jobs can be spooled either locally or remotely. Typically, print jobs sent to locally attached printers are spooled locally, and jobs sent to network printers are spooled remotely.

**Locally Spooled Print Jobs**

When print jobs are spooled *locally*, the local Windows computer processes the job. The application creates a spooled print job; the local print spooler, aided by the printer driver, processes the print job, and sends the rendered output to the printing device.

In a Windows environment, when you print to a printer connected to your local computer (when print jobs are spooled locally), the printer drivers and settings are stored on the computer itself. A typical printing process for locally spooled print jobs is:

1. The application tells the local spooler to create a print job and an associated spool file on the local computer.
2. On the local computer, Windows writes the application's drawing commands to the local spool file. This process of writing commands occurs repeatedly until the job is completely spooled.
3. The local spooler processes the job with the printer driver in a process known as *rendering*.
4. The local spooler delivers the rendered data to the printing device (for example, a locally attached printer).

**Remotely Spooled Print Jobs**

When print jobs are spooled *remotely*, the Windows print server processes the print job.

A typical printing process for remotely spooled print jobs is

1. The application tells the remote spooler to create a print job on the print server and an associated spool file.
2. On the local computer, Windows writes the application's drawing commands to the remote spool file. This process of writing commands across the network occurs repeatedly until the job is completely spooled.
3. The remote spooler processes the job with the printer driver in a process known as *rendering*.
4. The print server delivers the rendered data to the printing device (typically a network printer).

### Key Differences Between Remote and Local Spooling

Unlike remote spooling, local spooling does not use any network resources. Remote spooling requires that the local computer and the remote printer exchange many messages across the network. Even in a non-Citrix environment, if a WAN has substantial latency, users will have a poor user experience if the print jobs are spooled remotely across the WAN.

However, in some situations, for example when the resources on the local computer are needed for other tasks, remote spooling is preferable. In remote spooling, the print job is processed on the print server, which off-loads processing from the local computer.

# XenApp Printing Concepts

In a XenApp environment, all printing is initiated (by the user) on the server. However, print jobs are not always sent directly from the server to the printing device. Instead, the print jobs can be redirected through the client device.

Because there is no persistent workspace for users in XenApp (when a session ends, the user's workspace is deleted), all settings need to be rebuilt at the beginning of each session. As a result, each time a user starts a new session, XenApp must reprovision (recreate or restore) the printers available in a session.

When a user clicks **Print**, XenApp:

- Determines what printers (that is, printer objects) to provide to the user. This is known as *printer provisioning*.
- Restores the user's printing preferences.
- Determines which printer is the default for the session.

However, you can customize how XenApp performs these tasks by configuring options for printer provisioning, print job routing, printer property retention, and driver management. Settings for these options can impact the performance of printing in your environment and the user experience. For example, you can reduce the amount of latency when users print by choosing a method of provisioning that is appropriate for your network configuration.

As a result, understanding key printing concepts is critical when planning your printing configuration:

- The difference between the client and network printing pathway and how this is not the same as local printers and network printers
- The term *printer provisioning*, the types of printer provisioning (static and dynamic), printer autocreation, and user self-provisioning
- Print job routing and when changing it can improve utilization

- The basics of printer driver management

A discussion of these concepts is included in this series of topics. Because understanding XenApp policy is essential when configuring printing, you might want to review XenApp policies at this time.

Related topics:

"Provisioning Printers for Sessions" on page 227

"Optimizing Printing Performance by Routing" on page 239

"Managing Printer Drivers" on page 240

"Policy Rules Reference" on page 395

# Overview of Client and Network Printing Pathways

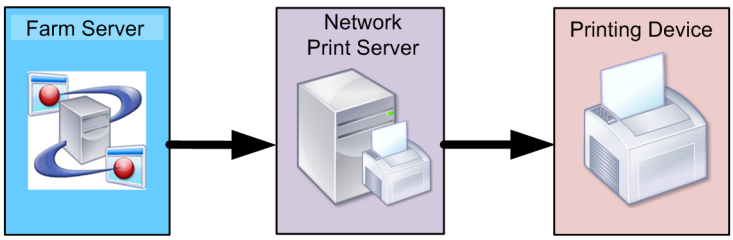
An important concept in XenApp is the printing pathway. The term *printing pathway* encompasses both the path by which print jobs are routed and the location where print jobs are spooled. Both aspects of this concept are important. Routing affects network traffic. Spooling affects utilization of local resources on the device that processes the job.

In XenApp, print jobs can take two different printing pathways:

- Client printing pathway
- Network printing pathway

**Network Printing Pathway**

The term *network printing pathway* refers to print jobs that are routed from the farm server hosting the user's session to a print server and spooled remotely.




*This diagram shows a XenApp network printing example: Printing begins on the farm server hosting the user's session (where the application is published and executing). XenApp routes the print job over a network connection to the network print server. The network print server then routes the print job to an associated network printing device.*

When a print job is spooled remotely in a Windows environment, it uses this process:

1. The application tells the remote spooler to create a print job and an associated spool file.
2. The Windows Print Provider sends the spool file to the print server.
3. The print server processes the spool file.
4. The print server then sends the print job to the appropriate network printer.

### Server Local Printers

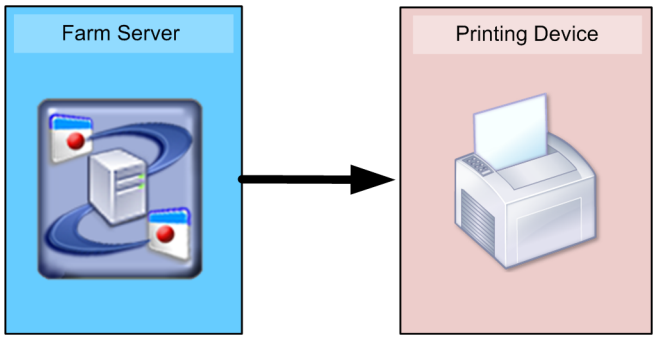
The term *server local printers* refers to a configuration that uses the network printing pathway where printing devices are attached locally to a XenApp farm server. Server local printers are shared printing devices that are physically attached to a farm server.

---

**Note:** To use a locally attached printer as a server local printer in a XenApp farm, the printer must be shared; otherwise XenApp does not recognize it.

---

Server local printers are often a good choice for printing in small farm environments. However, server local printers are not used widely in enterprise environments because they require installing the printer drivers on each server in the farm and require additional resources on the XenApp server. Server local printers are managed and configured in the same ways as network printers.




*This diagram shows a XenApp server local printing example: Printing begins on the farm server hosting the user's session and is routed to a printing device attached locally to the server.*

### Client Printing Pathway

The term *client printing pathway* refers to print jobs that are routed over the ICA protocol through the client device to the printer (either a printer connected directly to the client device or connected through a print server) and spooled on the Citrix XenApp Plugin for Hosted Apps.

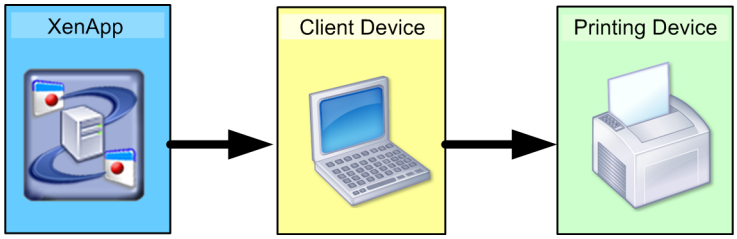
When using the client printing pathway, a virtual printer is constructed in the session that redirects to the printer object on the client device. The client device, in turn, sends the print job to the printing device.

Importantly, because all processing occurs on the XenApp server, when users print a document from a published application, they are actually starting that print job on the XenApp server. These jobs are spooled locally on the XenApp server.

There are two different configurations of the client printing pathway: one for printers attached directly to the client device and another for network printers.

#### Locally Attached Client Printers

The simplest configuration is the one where the printer is attached directly to the client device. In this configuration, the application server sends the print job back to the client/client device. The client device then relays it to a locally attached printer.




*This diagram shows a simplified XenApp client printing example: Printing begins on the server where the application is published. XenApp sends the print job over the connection to the client device. The client device then routes the print job to the printer connected locally to the client device.*

When a print job is spooled to a client along the client printing pathway, it uses this process:

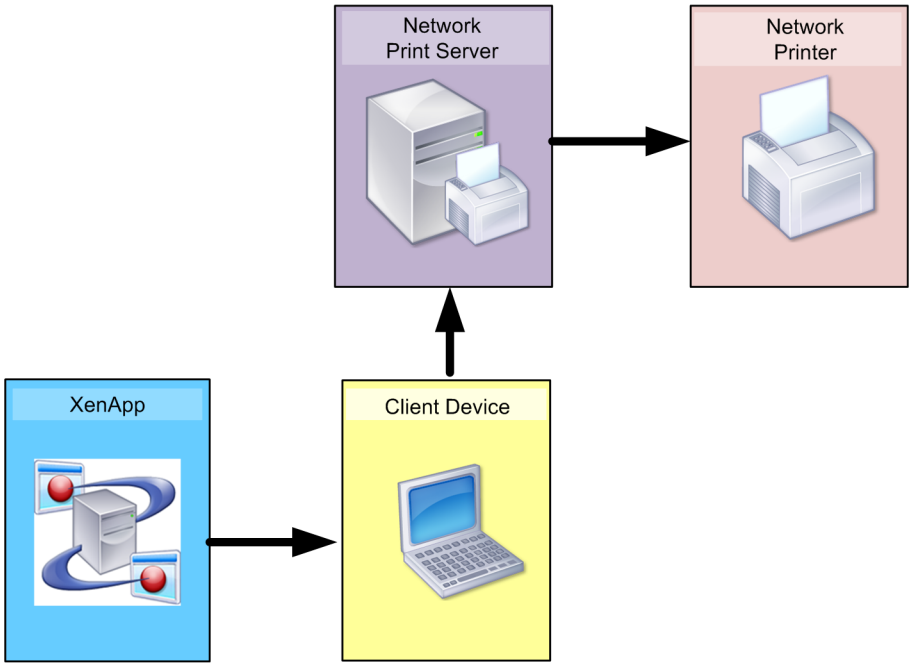
1. The published application tells the local spooler on the server hosting the application (that is, the host server) to create a print job and an associated spool file on the host server.
2. On the host server, Windows writes the application's drawing commands to the local spool file. (This process of writing commands occurs repeatedly until the job is completely spooled.)

3. The local spooler processes the job with the printer driver in a process known as *rendering*.
4. The rendered data is delivered to the client device through the ICA protocol.
5. The client device relays the print data to the client-side printing device (a locally attached printer in this example).

**Client Printers on the Network**

While client printers are often printers physically attached to client devices, they can also be printers on the network. In this case, print jobs are routed through the client device to the print server.

The process is the same as for printing to a local printing device through the client. However, instead of sending the job to the client device, the job is sent to the network print server.




*This diagram shows client printing to a network printer: Printing begins on the server where the application is published. XenApp routes the print job over the connection to the client device. The client device then routes the print job over the network to the print server, which in turn routes the print job to the network printer.*

When a print job is spooled to a network printer along the client printing pathway, it uses this process:

1. The application server sends the print job to the client for processing.

2. The client processes the spooled job and sends it to the Windows print server for processing.
3. The Windows print server then sends the print job to the appropriate network printer.

Configuring XenApp to use the client printing pathway for network printing devices is useful when a print server is in a domain different from the farm servers (and the client devices have access to the print server's domain). Using the client printing pathway lets application servers send print jobs over the ICA connection to access the printer through the client device.

Configuring the client printing pathway for network printing is useful for low bandwidth connections, such as WANs, that can benefit from the traffic compression that results from sending jobs over the ICA connection. The client printing pathway also lets you limit traffic or restrict bandwidth allocated for print jobs.

Related topics:

"Introduction to Windows Printing Concepts" on page 218

"XenApp Printing Concepts" on page 222

"Overview of Client and Network Printing Pathways" on page 223

"Provisioning Printers for Sessions" on page 227

"Optimizing Printing Performance by Routing" on page 239

"Managing Printer Drivers" on page 240

"Increasing Printing Speed and Session Performance" on page 274

# Provisioning Printers for Sessions

For a computer to process a print command, it needs both the required printer object and a printer driver. Because sessions are hosted in a virtual workspace instead of locally on a hard drive, printers and their drivers are not stored on the local computer. Instead, they are restored at logon or reconnect. The process by which XenApp makes printers available in a session is known as *provisioning*.

You can control printer provisioning and the way you configure it affects what printers users see in sessions and the speed of the printers.

There are two types of printer provisioning:

- **Static.** Server local printers are provisioned only once, when you connect them to the farm server. After that, they are always created in sessions with the same properties and do not vary according to policies.
- **Dynamic**. The printers that are available in a session are determined as the session is built. As a result, they can change according to changes to

policies, changes in user location, and changes to the network (provided they are reflected in policies). When printers are provisioned dynamically, the printers that appear in a session are not predetermined and stored. Rather, the printers are assembled, based on policies, as the session is built.

Because provisioning static printers is relatively simple, this topic focuses on provisioning printers dynamically. While there are other ways in which printers can be provisioned, such as through Active Directory policies, this topic discusses the most common methods using XenApp.

The two most common methods of dynamic printer provisioning are:

- User provisioning
- Autocreation

To control what printers users have in their sessions and ensure printers are available when users start their sessions, provision their printers through autocreation. If you do not want to specify (and administer) user printers, you can let users self-provision their printers.

**User Provisioning**

You can allow users to add printers to their sessions on their own. Users can map client printers that are not autocreated by policy manually in a user session through the Windows **Add Printer** wizard on the server (in their sessions). If users have thin clients or cannot access their client devices, they can self-provision by running the ICA Client Printer Configuration tool (PrintCfg.exe). For users to self-provision with the utility, you must publish PrintCfg.exe on your farm.

If you choose, you can prevent printer autocreation and let users provision printers visible from their client device.

**Autocreation**

The term *autocreation* refers to printers XenApp creates automatically, at the beginning of each session, based on what printers are configured on the client device and any policies that apply to the session.

By default, XenApp makes printers available in sessions by creating all printers configured on the client device automatically, including locally attached and network printers. After the user ends the session, the printers for that session are deleted. The next time a session starts, XenApp evaluates any policies for printer creation and enumerates the appropriate printers from the client device.

You can change the default autocreation policy settings to limit the number or type of printers that are auto-created. XenApp can auto-create:

- Client redirected printers, including auto-created client printers and a Universal Printer

- Network printers

There is maintenance associated with provisioning by printers by using client and network printer autocreation. When you add new printers, you need to update the autocreation list. Also, the drivers for these printers must be added to all servers on the farm; however, you can specify for XenApp to do this automatically.

This topic comprises:

- Auto-Creating Client Printers
- Provisioning a Citrix Universal Printing Solution
- Auto-Creating Network Printers
- Letting Users Provision Their Own Printers

All of these provisioning methods use the client printing pathway except for "Auto-Creating Network Printers," which uses the network printing pathway.

Related topics:

"To add a printer to the Windows CE and DOS auto-creation list" on page 255

"To modify printer auto-creation behavior" on page 252

"Configuring Auto-Creation for DOS and Windows CE Clients" on page 255

"Letting Users Provision Their Own Printers" on page 234

## Auto-Creating Client Printers

The main purpose of the autocreation feature is to create a list of printers that a user can use when they log in. When the user logs in, their print drivers will be installed and all printers returned in this list will be available for use.

XenApp can auto-create redirected client printers in two different ways:

- By creating a one-to-one match with printers on the client device
- By creating one generic printer, the Citrix Universal Printer, that represents all (or any) printers on the client device

In many environments, especially large ones, Citrix recommends that you auto-create only one default printer. Auto-creating a smaller number of printers creates less overhead on the server and is better for CPU utilization.

However, in environments where users with limited computer skills need to print to a wide variety of local printing devices, you may want to leave the default autocreation setting so that all printers are created on logon.

If you do not want large numbers of printers created at the beginning of each session, consider specifying for XenApp to use the Citrix Universal Printer.

### Auto-Creating Printers from the Client Device

At the start of a session, XenApp auto-creates all printers on the client device by default. You can control what, if any, types of printers are provisioned to users and prevent autocreation entirely.

The Auto-creation policy rule lets you control autocreation and specify that:

- All printers visible to the client device, including network and locally attached printers, are created automatically at the start of each session
- All non-network printers physically attached to the client device are created automatically
- Only the default printer for the client device is created automatically
- No printers visible to the client device are created automatically

You can also use the Auto-creation policy rule to specify that XenApp auto-creates network printing devices that are accessible through the client device only. An example is printing devices in a domain different from the application server.

When configuring policies for printer autocreation, ensure:

- User accounts are not shared
- Users are not in the local power user or administrators group on the client devices
- You add Microsoft native or fully tested drivers only
- Users have write access on the server to %systemroot%\system32\spool

These points help ensure that printers auto-create successfully.

### Provisioning a Citrix Universal Printing Solution

Citrix Universal printers and drivers are printing solutions that let users print regardless of whether or not they have the correct printers and drivers installed.

Universal printing solutions are printers and drivers not tied to any specific device. Consequently, they simplify administration by reducing the number of drivers required on farm servers or the number of printers created at the beginning of sessions. Because users need to access fewer printers and drivers, the speed of starting a session is increased and the complexity of printer administration is decreased.

XenApp includes two types of universal printing solutions:

- **Citrix Universal Printer.** A generic printer object, replacing the printers that appear in the users Printers control panel during their session. This printer can be used with almost any printing device.

- **Citrix Universal Printer Drivers**. Two types of Universal printer drivers are installed with XenApp:
  - **Windows Native Printer Drivers.** These drivers are generic enough to work with almost any printer. These printer drivers also work for non-Windows clients.
  - **Citrix-created Universal printer drivers.** There are two Citrix Universal printer drivers: the Citrix XPS Universal Printer driver and the EMF-based Citrix Universal Printer driver.

These printing solutions can be used in one of these ways:

- **Auto-created device printer with Citrix Universal printer driver**. A device-specific printer gets auto-created but uses a Citrix Universal printer driver. For example, configured policy rules specify that the printer LaserJet5L still gets auto-created at the beginning of each session; however, the session uses the Citrix Universal printer driver to communicate with the driver on the client device and the print job is processed on the client device.
- **Auto-created Citrix Universal Printer with a Citrix Universal printer driver**. A Citrix Universal Printer gets auto-created and it uses a Citrix Universal printer driver. That is, at the beginning of each session, the only printer that is auto-created is the Citrix Universal Printer. Like the first example, the session uses the Citrix Universal printer driver to communicate with the driver on the client device and the print job is processed on the client device.
- **Auto-created device printers, auto-created Citrix Universal Printer with a Citrix Universal printer driver**. At the beginning of the session, the Citrix Universal Printer and device-specific printers are auto-created. Both printers use the Citrix Universal printer driver.

Whether you use a Citrix Universal printing solution depends on various factors:

- The Citrix Universal Printer and printer driver might not work for all client devices or plugins in your environment. The Citrix Universal Printer and printer driver solution requires the Citrix XenApp Plugin for Hosted Apps or the Citrix XenApp Plugin for Streamed Apps (when streaming to the server).

  The Citrix Universal Printer does not work if plugins are not connecting through the ICA channel, such as when you are using the Citrix XenApp Plugin for Streamed Apps and streaming applications to the client.

  If you want to use a universal printing solution for non-Windows plugins, use one of the other universal printer drivers that are based on postscript/ PCL and installed automatically with XenApp.

- The Citrix Universal printer driver might also create smaller print jobs than older or less advanced printer drivers. However, sometimes it might be better to use a device-specific driver because the driver might be able to optimize print jobs for its associated printer.

---

**Note:** If you want the Citrix Universal Printer to appear in sessions, make sure that the rule **Printing > Client Printers > Legacy client printers** is not set to **Create old-style client printers** in any policies affecting those sessions. If the **Legacy client printers rule** is enabled, set it to **Create dynamic session-private client printers**.

---

Universal printer drivers are installed by default on each farm server; the printer is not enabled, however. To get the best results when configuring your farm, use both the Citrix Universal Printer and a Citrix Universal printer driver.

---

**Note:** Citrix Universal Printing is available for Citrix Presentation Server Client, Version 9.x or later and the Citrix XenApp Plugin for Streamed Apps (streamed to server). This feature is available in Presentation Server 4.0 to XenApp 5.0

---

**Citrix Universal Printer**

The Citrix Universal Printer is a generic printer created at the beginning of sessions that can be used with almost any printing device. This printer can print to and communicate, through the client, with any client-side printer.

You may also want to use the Citrix Universal Printer because the printer name does not change when users reconnect. Changing printer names can cause problems for some applications.

The Citrix Universal Printer is created on a per-session basis. When used in conjunction with a Citrix Universal Printer driver, it can greatly reduce the resource usage at the start of a session from printer autocreation. When you use the Universal Printer, you can specify that only the Universal Printer be auto-created for each printer on the client device.

Unlike many printing settings, the Universal Printer does not appear in the policy rules. By default, the Universal Printer does not appear in XenApp unless you enable it by editing the registry. When enabled, an extra printer is created in the session with the name **Citrix UNIVERSAL Printer in session *number of session***. To use only the Citrix Universal Printer in sessions and not auto-create any printers on the client device, enable the Universal Printer through the registry and set the **Printing > Client Printers > Auto-creation** rule to **Do not auto-create client printers**.

The user experience varies depending on the type of Citrix Universal Printer.

Because the Citrix Universal Printer is not tied to a specific printing device, both the EMF-based and XPS-based Citrix Universal Printers provide ways to preview and select settings:

- **EMF-based Citrix Universal Printer**. The EMF-based Citrix Universal Printer can display a Print Previewer before printing. Clicking **Local Settings** in the Citrix Print Previewer is the only way users can select a different printer, control the device settings for the printer hardware, and preview the print job. You control whether or not the **Local Settings** button is available to users. If you do not allow users to change their printer through the **Local Settings** button, the Citrix Universal Printer prints to the default printer on the client device.
- **XPS-based Citrix Universal Printer**. Like Microsoft XPS Document Writer, the Citrix XPS Universal Printer sends documents to Internet Explorer if a user selects Print Preview or modifies the print settings, displaying them in Microsoft's XPS "electronic paper" format.

---

**Note:** The Print Previewer cannot be controlled by the administrator unless users have the Citrix Presentation Server Client, Version 10.100 or later or the Citrix XenApp Plugin for Hosted Apps, Version 11.*x*.

---

## Auto-Creating Network Printers

By default, any network printing devices on the client device are created automatically at the beginning of sessions; however, if possible, XenApp always tries to route jobs directly from XenApp to the print server and not through the client connection.

To specify that specific printers are created in sessions rather than auto-create all the network printing devices available from the client device, configure the Session Printer policy rule.

The key difference between provisioning network printers with the **Printing > Client Printers > Auto-creation** rule and the **Printing > Session** printers rule is that the Auto-creation rule automatically creates all printers on the client device whereas the Session printers rule lets you specify which printers are created. Network printers created with the Session printers rule can vary according to conditions where the session was initiated, such as location (by filtering on objects such as subnets).

Before you can configure the Session printers rule, you must import the printer objects stored on your print server into your XenApp farm. After importing printers into XenApp, you can assign them to user sessions through the Session Printer policy rule.

**Note:** For printers in domains that do not have a trust relationship with the XenApp farm, configure them as redirected client printers using the Auto-creation rule. When network printing devices are provisioned in this way, the print jobs are routed through the client using the client printing pathway.

### Letting Users Provision Their Own Printers

If you do not want specific printers to be auto-created at the beginning of each session, leave users to add their own printers.

By default, provided they can access the network from their client devices, all users can add printing devices to be used in a session. The only time users cannot add printers to their sessions is when they cannot access their client device because they are using a thin client and there are no applications published that let them browse and add printers.

Printers that users create on their own during a session are known as *retained printers* because they are created again (or remembered) at the start of the next session. When XenApp recreates a retained printer at the start of a session, it considers all policy rules except the Auto-creation rule.

Retained printers appear in sessions on that device 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.

Users might need to use the PrintCfg.exe tool to add printers if they cannot browse to the printer from within the session or cannot access their client desktop. If they use this tool, the printers are routed along the client printing pathway.

## Device or Session-Based Print Settings

By default, all changes users make to the printer device settings and preferences, whether in a session or working on their local computer, are saved and used locally and in a session. This means that printer settings and preferences are always the same on the client device and in a session. XenApp policies let you change the way XenApp software saves and applies printer device settings and preferences.

You can configure sessions to obtain print settings, specifically user printing preferences, from either the printer object or the printing device.

XenApp can write printer settings to the printer object at the end of a session or to a client printing device, provided the user's network account has sufficient permissions. By default, XenApp Plugins use the settings stored in the printer object in the session, before looking in other locations for settings and preferences.

The main reason you want sessions to obtain their print settings from the printing device is if Windows users make changes to local printers outside of sessions (that is, on their local computer offline). Non-Windows plugins synchronize changes made out of sessions automatically.

## Device-Based Print Settings

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

If you have Windows users with locally attached printers who work on applications locally and on the server, you might want to retain changes to the printer settings the users make locally outside of a session. To do so, create and set the Win32FavorRetainedPrinterSettings registry key to False, as described in "To synchronize printer properties set out of sessions" on page 267.

When the registry key is modified, the plugin gives priority to settings from the printer, rather than retained settings. Settings in the session stay synchronized with settings on the printing device. If a change was made to the printer out of a session, the change is picked up. If a change is made to the printer inside the session, the plugin attempts to write the change back to the printer on the client device when logging off.

For this configuration to work well, you must have exactly the same driver on the client device and server. If you do not, only a subset of settings is exchanged between the real printer and the virtual printer in the session. Some device independent settings are inherited and others are not.

## Controlling Printing Settings and User Preferences

To understand how printing preferences are retained and applied, you must understand:

- The locations printing settings can be stored in a XenApp environment
- The priority XenApp software uses to apply printing preferences from previous sessions to the printers in a newly created session
- Where XenApp software stores printing preferences by default and if there are factors in your environment that will prevent the software from successfully storing them in this location (that is, when you need to change this setting)

### General Locations of Printing Preferences

In Windows printing environments, changes made to printing preferences can be stored on the local computer or in a document. In a XenApp environment, when users modify printing settings, the settings are stored in these locations:

- **On the client device itself.** The settings are set on the client device by right-clicking the printer in **Control Panel > Printers** and selecting **Printing Preferences**. For example, if **Landscape** is selected as page orientation, landscape is saved as the default page orientation preference for that printer. This type of preference is known as *Device Settings*.
- **Inside of a document**. In word-processing and desktop-publishing programs, settings, such as page orientation, are often stored inside documents. These settings are often referred to as *Document Settings*. For example, when you queue a document to print, Microsoft Word typically stores the printing preferences you specified, such as page orientation and the printer name, inside the document. These settings appear by default the next time you print that document.
- **From changes a user made during a session**. XenApp keeps only changes to the printing settings of an auto-created printer if the change was made in the **Control Panel > Printers** in the session; that is, on the server.
- **On the server**. These are the default settings associated with a particular printer driver on the server.

If you want to control user printing preferences, it is important to understand that the settings preserved in any Windows-based environment vary according to where the user made the changes. This also means that the printing settings that appear in one place, such as in a spreadsheet program, can be different than those in others, such as documents. As result, printing settings applied to a specific printer fluctuate throughout a session.

### Hierarchy of Users' Printing Preferences

Because printing preferences can be stored in multiple places, XenApp processes them according to a specific priority. Also, it is important to note that Device Settings are treated distinctly from, and usually take precedence over, Document Settings.

XenApp searches for settings in this order:

1. XenApp checks for retained printer settings.

   If XenApp finds retained settings, it applies these settings when the user prints.

2. If there are no retained printer settings, XenApp searches for any changes to the printer settings for the default printer for the client device.

If XenApp finds any changes to printing preferences on the client device, it applies these settings when the user prints.

3. If there are no retained or client printer settings, XenApp applies the default printer settings stored on the server when the user prints.

At this point, the printer settings are merged. Generally, XenApp merges any retained settings and the settings inherited from the client device with the settings for the default printer driver on the server.

By default, XenApp always applies any printing settings a user modified during a session; that is, the retained settings, before considering any other settings.

**Saving Users' Printing Preferences**

By default, XenApp attempts to store printing properties, a combination of the user's printing preferences and printing device-specific settings, on the client device. If the client does not support this operation, XenApp stores printing properties in its user profile for that user. Sessions from non-Windows XenApp plugins or even older Windows XenApp plugins use the user profiles on the server for properties retention. You can use the Printer Properties Retention policy rule to force properties to be saved on either the client or on the server.

If one of the following apply, you might need to reconfigure how XenApp stores user printing preferences:

- **Client version**. Not all XenApp plugins support storing the printer properties on a client device. Users must be running Citrix Presentation Server Client 9.*x* and higher to store user-modified printer properties on the client device.
- **Type of Windows user profile**. That is, if you are using local, roaming, or mandatory profiles on your Windows network.

  If you are using a mandatory profile and you want to retain the user's printer properties, you must store the properties on the client device.
- **Farm Size**. If you have a large farm and you are load balancing applications, users will experience inconsistent printing behavior and properties if you use local profiles. The only way you can get consistent printing behavior is to save the printer properties on the client device.
- **Type of workers**. If you have mobile or remote workers and you are using roaming profiles, you must save the printer properties to the user's profile and not the client device.

If none of these factors apply to you, Citrix recommends you not change where the printer properties are stored. Leaving the default setting, which saves the printer properties on the client device, is the easiest way to ensure consistent printing properties.

You can specify whether you want these settings stored on the client device or with the user's profile. You can also change this default behavior so settings are not stored. However, before you make these decisions, you must understand how XenApp determines what print settings it applies and also what the difference is between storing print settings on the client device or with a profile.

## Setting Default Printers

The printer that XenApp selects for a session's default printer can be based on:

- A network printer you specify as the default
- The default printer on the client device

If you want to base the default session printer on either of these, use the **Session printers** policy rule.

However, if you specified that XenApp auto-create the default client printer, then, if no other printers are provisioned in sessions, you might not need to specify a default session printer.

## Printing and Mobile Workers

In situations where users move among different workstations or sites, you can make sure that the closest printers are presented to them wherever they try to print. Examples of such users include hospital workers who move among workstations in different wings of a hospital, reconnecting to the same session using a smart card, or employees who travel to remote business units.

If you have mobile workers and need this type of printing functionality, use one of these features:

- **SmoothRoaming**, or Workspace control, lets a user disconnect from one session, move to another device, and reconnect to continue that same session. The printers assigned on the first client device are replaced on reconnection with the printers designated on the second client device. As a result, users are always presented with applicable printer options from wherever they connect.
- **Proximity Printing** lets you control the assignment of network printers so that the most appropriate printer is presented, based on the location of the client device.

The Proximity Printing solution is enabled through the **Session printers** policy rule.

Proximity Printing can make administration easier even if you do not have mobile workers. For example, if a user moves from one department or floor to another, you do not need to assign additional printers to that user if Proximity Printing is implemented. When the workstation is recognized within the new location's IP address range, it has access to all network printers within that range.

However, if you configure Proximity Printing, you must maintain the Session printer policy. For example, as network printers are added or removed, you must update this policy to reflect the current set of network printers. Likewise, if you modify the DHCP IP address ranges for floors or departments, you must update this policy.

Proximity Printing requires that you can filter the policy on some type of geographic indicator, such as:

- The name of the workstation, if the name relates to the workstation's location
- Your network's IP addresses, if they correlate with user locations

Related topics:

"Ensuring Session Continuity for Mobile Workers" on page 119

"Configuring Printers for Mobile Workers" on page 263

# Optimizing Printing Performance by Routing

In a XenApp environment, you can control how print jobs destined for network printers are routed. Jobs can take two paths to a network printing device: along the client or network printing pathway.

By default, XenApp routes print jobs along the client printing pathway as follows:

- **Auto-created client printers.** XenApp routes jobs to locally attached printers from the server, through the client, and then to the print device. The ICA protocol compresses the print job traffic. When a printing device is attached locally to the client device, the jobs must be routed through the plugin.
- **Auto-created network printers.** By default, all print jobs destined for network printers route from the server, across the network, and directly to the print server. However, if the application server and the print server are on different domains, XenApp automatically routes the print job through the plugin.

When network printers are visible from the server, you can use policies to control how print jobs are routed to network printers. You can configure that jobs be routed to network printers:

- **Through the plugin.** This is accomplished by auto-creating the network printer but specifying its jobs to route through the plugin.
- **Over the network.** This is accomplished either by leaving the default settings so that the network printer is auto-created (or configuring a policy to do this) or by provisioning the network printer through the Session printers policy rule.

Routing jobs along the network printing pathway is ideal for fast local networks and when you want users to have the same user experience that they have on their local client device (that is, when you want the printer names to appear the same in every session).

However, print jobs relayed using the network printing pathway are not suited to WANs. The spooling of print jobs using the network printing pathway method is "chatty;" many packets are exchanged between the host server and the print server. Consequently, users might experience latency while the print jobs are spooling over the WAN. Also, the print job traffic from the server to the print server is not compressed and is treated as regular network traffic.

When printing jobs across a network with limited bandwidth, Citrix recommends routing jobs through the client device so that the ICA protocol compresses the jobs. To do so, enable the **Printing > Client Printers > Print job routing** policy rule and select the **Always connect indirectly as a client printer** option.

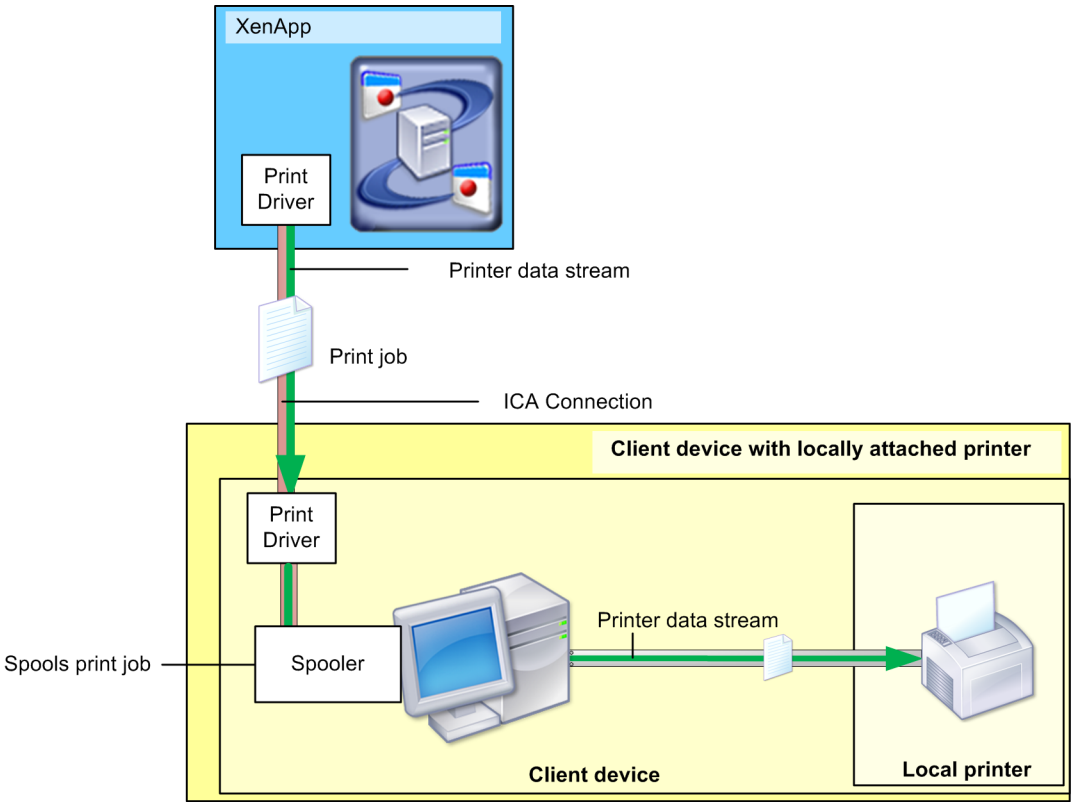
Related topics:

"Increasing Printing Speed and Session Performance" on page 274

# Managing Printer Drivers

During printer auto-creation, if XenApp detects a new local printer connected to a client device, it checks the server hosting the published application (from which the user is trying to print) for the required printer driver. By default, XenApp automatically installs a native driver if one is not found on the server hosting the published application.

Because users in a XenApp environment do not have a persistent workspace, drivers cannot be stored on the client. To print to a local device, XenApp must find the correct driver on: (a) its server or in the server's Windows operating system, and (b) the client device. The diagram that follows shows how the printer driver is used in two places for client printing.




*This diagram shows client printing to a local printer: The printer driver on the server routes the job over the ICA channel to the client device. The client device then routes the print job through the same printer driver, which is accessible on the client device. The printer driver on the client device relays the print job to the print spooler on the client device, which in turn routes the print job to the local printer.*

The printer driver on the server and the driver used by the client device must match exactly. If not, printing fails. As a result, XenApp provides features to manage drivers, install them automatically, and replicate them across your farm.

The following problems can arise from not managing client printer drivers correctly:

- Any missing drivers can prevent users from printing successfully. If a third-party printer driver has multiple or inconsistent names across your farm, a session might not be able to find it and a user's job may fail to print.
- Printing to a client printer with a defective driver can cause a fatal system error on a server.

- If the driver cannot be installed using Windows drivers, XenApp attempts to download the driver from the print server. However, if the print server is a 32-bit server and the XenApp server is a 64-bit system, the driver might not work.

  As a workaround, you can use either two print servers, one 32-bit and one 64-bit, or use the Citrix Universal printer driver exclusively.

- 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.

When planning your driver management strategy, determine if you will support device-specific or the Universal Printing driver, or both.

If you support standard drivers, you also need to determine:

- What types of drivers you want to support
- If you want printer drivers automatically installed when they are missing on farm servers
- If you want to create driver compatibility lists
- If you want to replicate drivers across your farm servers automatically

## Types of Printer Drivers

There are two categories of printer drivers:

- **Citrix Universal Printer driver**.
- **Standard printer drivers**. Specifically, Windows printer drivers or manufacturer's printer drivers.

These drivers are covered in this topic. However, Citrix recommends, when possible, using the Citrix Universal Printer driver exclusively because it reduces the number of drivers on farm servers and simplifies administration.

### Universal Printer Drivers Overview

The Citrix Universal Printer drivers provide basic printer driver functionality to almost all printers, regardless of make or model. Deploying one of these drivers relieves the burden of administering multiple printer drivers and avoids problems with driver maintenance, replication, and other client printing issues.

In XenApp 5.0, Citrix provides several different types of Universal printer drivers:

- **Citrix Universal XPS Printer driver.** This driver is based on the new Windows XML Paper Specification (XPS) printing technology that is being introduced in Windows Server 2008. Windows XPS printing technology

uses XML to create a platform-independent “electronic paper” similar to Adobe’s PDF format.

The XPS format is a device-independent XML-based spool file format that provides a compressed XML description of a page’s graphic elements. Printing devices can use XPS-formatted print jobs directly without translation.

The Citrix Universal XPS Printer driver creates the XPS print job using the Microsoft XPS printer driver on the client device. The Citrix Universal XPS Printer driver obtains printing device-specific information from the client device.

Provided your farm servers are running XenApp 5.0 and your client devices have .NET 3.0 installed on them, which comes with Windows Vista, you can use the Citrix Universal XPS Printer driver.

- **Citrix Universal Printer driver.** This driver uses Windows’ Enhanced Metafile Format (EMF) technology. EMF is a device-independent format for capturing the graphical elements printed on each page of a print job. A client-side renderer uses EMF and provides a substantial reduction in the processing time of Citrix Universal print jobs on the client.
- **Stock or standard Windows printer drivers.** Citrix also uses standard printer drivers, which are sufficiently compatible to support a broad range of printing devices, to provide universal printing functionality. You can use these printer drivers for universal printing for non-Windows plugins, such as Macintosh or UNIX clients. These drivers include the following:
  - HP Color LaserJet 4500 PCL 5 (Citrix PCL5c Universal Driver)
  - HP Color LaserJet 4500 PS (Citrix PS Universal Printer Driver)
  - HP LaserJet Series II (Citrix PCL4 Universal Driver)

When a Universal Printer driver is configured, by default, XenApp uses the EMF-based Citrix Universal Printer. If you change the default driver to be the Citrix Universal XPS Printer driver, the XPS driver is used provided the plugin or client device meet the XPS driver’s requirements. If a requirement is missing, XenApp uses (that is, “falls back” to) the EMF-based Citrix Universal Printer.

If you use the Citrix Universal XPS Printer driver, the print jobs it processes might have a smaller footprint on your network. However, users might perceive the EMF-based Citrix Universal driver as printing faster. The EMF-based driver spools print jobs one page at a time, so each page prints as the printer receives it. In contrast, with the XPS-based printer driver, printers cannot print until they receive the last page of the job.

### Citrix Universal XPS Printer Driver Overview

The Citrix Universal Printer driver uses Microsoft's XPS printer driver on the server to create an XPS print job that can be read by the printing device. It uses this process:

1. The XPS print job (*.*xps) that will be ultimately read by the printing device is created on the server in a session:
    - On the server hosting the published application, the application sends the data to the printer (object) for the target printing device
    - The printer object then sends the print data to the XPS printer driver on the server where it is rendered into an XPS file
2. The XenApp server sends the XPS file across the printing virtual channel to the XPS Print Helper (which is part of the Citrix XenApp Plugin for Hosted Apps and the Web Interface).
3. The XPS Print Helper does one of two things:
    - If the XPS printer driver is bound to a specific printer that was auto-created at the beginning of a session, the XPS file is sent directly to the printer and the XPS Viewer does not appear.
    - If the XPS printer driver is not bound to a specific printer, the user must choose a printer. The XPS file is sent to the XPS Viewer in Internet Explorer and the user can select the printer from Internet Explorer.

### Standard Printer Drivers Overview

In this topic, the term *standard printer drivers* refers to any printer driver that is not a Citrix Universal Printer driver. There are two types of standard printer drivers:

- **Windows printer drivers**. The drivers included with Windows operating systems are sometimes known as *native* printer drivers because they are part of, or native to, the operating system.

  These drivers are manufacturer-specific and they are the drivers that Windows automatically installs when you use the Windows Add Printer wizard. These are not synonymous with manufacturer's drivers.

- **Manufacturer's printer drivers**. The term *manufacturer's printer drivers* refers to the printer drivers that come with a printer; for example, on a CD or as a download from the manufacturer's Web site. Manufacturer's printer drivers are also known as *third-party printer drivers*.

You may need to use standard drivers from the Windows operating system or the manufacturer in some situations, including:

- When your environment has extremely new printers, older printers, or specialty printers
- When users require specialty printing features that are not available through the Citrix Universal Printer driver, such as support for certain paper sizes

If you must use standard printer drivers, use the Windows printer drivers included with the Windows operating system, over the manufacturers drivers, whenever possible. The drivers with Windows typically go through a higher level of Windows certification that includes testing for multiuser environments. However, sometimes if there is not a comparable Windows driver or if users require a feature, such as postscript, you may need to use the manufacturer's driver for that printing device.

The Universal driver policy rule lets you control which type of printer drivers are used during printer autocreation. You can specify:

- Model-specific drivers only
- Universal drivers only
- Universal drivers only if a model-specific driver is not available

If you do not enable the Universal driver policy rule, XenApp uses model-specific drivers if they are available. If XenApp cannot find the correct model-specific driver, it uses a Universal printer driver.

If you are supporting standard device-specific printer drivers, determine how you want to manage the drivers on your farm. See "Managing Printer Drivers" on page 240.

# Planning Your Printing Configuration

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration. Without performing any printing configurations, users can print in most environments. However, users might not get the printing experience they expect and default printing configurations might not be appropriate for your environment.

Your printing configuration depends upon:

- Your business needs and your existing printing infrastructure. Design your printing configuration around the needs of your organization. Your existing printing implementation (user's ability to add printers, which users have access to what printers, and so on) might be a useful guide when defining your XenApp printing configuration.

- If your organization has security policies that reserve printers for certain users (for example, printers for Human Resources or payroll).
- If users need to print while away from their primary work location; for example, workers who move between workstations or travel on business.

When designing your printing configuration, try to give users the same experience in a session as they have when they print when working on their local client devices.

Related topics:

"Printing Security" on page 248

"Purchasing Printing Hardware" on page 249

"Increasing Printing Speed and Session Performance" on page 274

# Default Printing Behavior

By default, if you do not configure any policy rules, XenApp has this printing behavior:

- All printers configured on the client device are created automatically at the beginning of each session. This behavior is equivalent to enabling the **Printing > Client Printers > Auto-creation** policy rule with the **Auto-create all client printers** option selected.
- XenApp routes all print jobs queued to printers locally attached to client devices as client print jobs (that is, over the ICA channel and through the client device).
- XenApp attempts to route all print jobs queued to network printers directly from the server hosting the published application.

  If XenApp cannot route the jobs over the network, it will route them through the client device as a redirected client print job.

  This behavior is equivalent to enabling the **Printing > Client Printers > Print job routing** policy rule with the **Connect directly to network print server if possible** option selected.
- XenApp retains all properties and settings users configure for printers they provision themselves in sessions.

  XenApp attempts to store printing properties on the client device. If the client device does not support this operation, XenApp stores printing properties in the user profile for that user.

This behavior is equivalent to enabling the **Printing > Client Printers > Printer properties retention** policy rule with the **Held in profile only if not saved on client** option selected.

- XenApp uses the Windows version of the printer driver if it is available on the server hosting the application.

  If the printer driver is not available, the XenApp server attempts to install the driver from the Windows operating system.

  If the driver is not available in Windows, it uses one of the Citrix Universal printer drivers.

  This behavior is equivalent to enabling the **Printing > Drivers > Native printer driver auto-install** policy rule with the **Install Windows Native drivers as needed** option selected, and enabling the **Printing > Drivers > Universal driver** policy rule with the **Use universal driver only if requested driver is unavailable** option.

---

**Note:** If you are unsure about what the shipping defaults are for printing, you can display them by creating a new policy and setting all printing policy rules to Enabled. The option that appears is the default shipping option.

---

# Printing Policy Configuration

When users access printers from published applications, you can configure XenApp policies to specify:

- How printers are provisioned (or added to sessions)
- How print jobs are routed
- How printer drivers are managed

You can have different printing configurations for different client devices or users or any other objects on which policies are filtered. You must understand the ramifications of setting the options in printing policies, so review the information in the printing topics carefully before configuring them.

Related topics:

“XenApp Printing Concepts” on page 222

# Printing Security

Client printing can, potentially, let a user from one session use another user's printer in a different session. Unlike network printer connections, client printers auto-created in a XenApp session are 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 XenApp printer naming convention helps combat this problem by avoiding the potential for printers and ports to be shared between sessions. Printers connected through a pass-through server use the session ID to identify the printer uniquely, 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 through which it might have connected.

In addition, to increase client printing security, access to the client printers is restricted 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

Windows security blocks access to the printer from all other processes on the system. Furthermore, requests for services directed to the print manager must originate from a process in the correct session. This prevents bypassing the spooler and communicating directly with CpSvc.exe.

As an administrator, you cannot access client printers from another session; this prevents you from inadvertently printing to printers in another session. If you need to adjust security settings of a printer in another session, you can do so through Windows Explorer. If you have the UAC control enabled, install the Windows Server 2008 Print Services role on each farm server and using the **Print Management** console to manage client print queues.

---

**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 Citrix Knowledge Center for more information.

---

# Purchasing Printing Hardware

Before purchasing printers for your organization, Citrix recommends finding out if the printer models that you are considering were tested for multiuser environments, such as Windows Terminal Services environments and Citrix XenApp.

When purchasing a printer, make sure that it is PCL or PS compatible. Also, make sure the printer is not a *host-based printer*. Host-based printers use the processor on the host computer to generate print jobs; they are often labelled as "GDI," "HOST only," or "LIDL." Because these printers require software on the client device to generate the print job, they are difficult to run in a XenApp environment.

Whether or not printers work in a XenApp environment is determined by the printer manufacturer, not by Citrix. Check with the manufacturer to see if the company guarantees that specific model works in a XenApp environment. Some companies have done extensive testing with XenApp and published white papers indicating which printers they support. For information about these white papers, contact Citrix Technical Support.

# Configuring and Maintaining XenApp Printing

This topic provides procedures for configuring and maintaining printing. This topic assumes that you understand the information provided in “Understanding XenApp Printing” on page 217 and that you already planned your printing deployment.

This topic complements the information about printing policies in the “Policy Rules Reference” on page 395.

## Configuring Printing

Most XenApp printing functions are configured through XenApp policies. To find printing policy rules, select the following in the Advanced Configuration tool:

- **Bandwidth > Session Limits > Printer**. This rule restricts the bandwidth allocated to printers.
- **Printing > Client Printers**. These rules affect the client redirected printers and printing using the client printing pathway.
- **Printing > Drivers**. These rules control driver management.
- **Printing > Session printers**. This rule configures how network printers are provisioned and specifies a default network or client printer.

However, some printing management tasks are performed in the **Printer Management** node of the Advanced Configuration tool, which controls farm connections to print servers, drivers, and printing bandwidth on a per-server basis

If you do not enable any policy rules that affect printing, XenApp uses the default printing behavior that is described in “Planning Your Printing Configuration” on page 245.

Printing policy rules follow standard XenApp policy behavior:

- Printing rules in policies are evaluated during initial logon and remain in force throughout the session. Any new printers added to a policy or a client device during a session do not appear in the session until the user logs off and logs on, creating a new session.
- The policies are filtered on standard objects that apply to all XenApp policy rules. Therefore, when configuring printing rules, you need to determine which filter objects best achieve your goals. Filtering on Client Device Name is useful if you are trying to configure proximity printing. Filtering on Client IP address is useful when associating network printers with specific workstations.

When configuring printing rules, pay attention to the following:

- **XenApp policy behavior.** Xenapp policies do not behave like Microsoft policies. Review the distinction between **Not Configured** and **Disabled**, best practices for creating policies, resultant policies, and other policy topics. These topics are often misunderstood.
- **The prioritization of the policy.** All printing rules follow standard XenApp prioritization. Xenapp policies always take precedence over Windows policies in a XenApp environment.
- **Policy maintenance.** Changes in your network often result in the need to update printing policy configurations. For example, users changing departments or workstation locations require that you update the printing policies associated with that user. Adding or removing printers from your network require that you update any configured Session printers policy rules.

This topic is intended to be used with the information in "Understanding XenApp Printing" on page 217. To find the background information for a specific task, see the Related Topics.

# Configuring Printer Autocreation Settings

Enable this rule to control how or if printers are created automatically at the start of sessions. By default, this rule is not enabled, so XenApp creates all printers on the client device.

Related topics:

"To add a printer to the Windows CE and DOS auto-creation list" on page 255

## To modify printer auto-creation behavior

1. In the Advanced Configuration tool, 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. Select **Printing** > **Client Printers** and enable the **Auto-creation** rule.
5. Select one of the following:
    - **Auto-create all client printers.** All network printers and any printers attached to or mapped from the client device preconfigured in the **Printers Control Panel** are auto-created in the session.
    - **Auto-create local (non-network) client printers only.** Any non-network printers attached to the client device preconfigured in **Control Panel > Printers** are auto-created in the session.
    - **Auto-create the client's default printer only.** Only the client's default printer attached to or mapped from the client preconfigured in **Control Panel > Printers** is auto-created in the session.
    - **Do not auto-create client printers.** Client printers are not auto-created.

### To configure legacy client printer support

Enable this rule to auto-create client printers before MetaFrame 3.0.

1. In the Advanced Configuration tool, 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. Select **Printing** > **Client Printers** and enable the Legacy client printers rule.
5. Select one of the following:
    - **Create dynamic session-private client printers** to create printers that use default Presentation Server 4.0 to XenApp 5.0 naming conventions
    - **Create old-style client printers** to create printers that use printer names that are compatible with MetaFrame 3.0 or earlier

## Configuring Citrix Universal Printing

There are several different Universal Printing solutions. You can configure:

- Citrix XPS Universal Printer driver

- Citrix Universal Printer driver, which is EMF-based
- Auto-created Citrix Universal Printer with a Citrix Universal printer driver

Configuring only a Universal printer driver will not improve session start time (printers on the client device are still enumerated and auto-created at the beginning of sessions). However, configuring a Universal printer driver does improve printer driver performance.

Related topics:

"Provisioning a Citrix Universal Printing Solution" on page 230

"Universal Printer Drivers Overview" on page 242

## To configure the Citrix Universal Printer

The following procedure provides instructions about configuring the Citrix Universal Printer. If you want to use the Universal Printer, configure it on each server hosting published applications in your farm.

---

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

---

1. Find the following registry key on each server:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Print

2. Modify the registry key, DefaultPrnFlags, so that it has a bit value of 0x00000020.
3. Restart the Citrix Print Manager Service.

## To change the default settings on the Universal Printer

You can change the default settings for the Citrix Universal Printer, including settings for paper size, paper width, print quality, color, duplex, and the number of copies. You override the default settings of the Citrix Universal Printer and modify these settings by manually setting registry keys. For a list of the specific registry values, see the Citrix Knowledge Center.

# Configuring Auto-Creation for DOS and Windows CE Clients

If devices running the Client for Windows CE have local printers, the Advanced Configuration tool can auto-create these client printers for users each time the client devices connect to the server farm. In this case, *client printers* refers to client redirected printers (printers that are physically attached to client devices or mapped from client devices) for DOS and Windows CE Clients.

---

**Note:** Unlike devices running the Client for Windows CE with local printers, client printers available from other clients are auto-created based on the settings configured using Printing policies.

---

When you configure auto-creation, XenApp downloads appropriate printer objects to the client device to make the client printer available in client sessions.

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.

## To add a printer to the Windows CE and DOS auto-creation list

Use this dialog box to define the client printers that are available to named devices running the Client for Windows CE. Each time users of those devices log on to your farm, those client printers are available to them automatically.

After adding a new client printer at your organization for use by Windows CE and DOS users, update the auto-creation list to ensure the definition is available when printers are auto-created at the beginning of sessions.

1. Under the **Printer Management** node of the Advanced Configuration tool, select **Printers**.
2. From the **Actions** menu, choose **Printer Management > Client Printers**.

   The **Client Printers** dialog box appears. This dialog box lets you add, reset, edit, and delete the printers that will be auto-created for the clients for DOS and Windows CE printers.

   ---

   **Note:** These printers are available only on the client and appear only in server-based applications during the user's session.

   ---

3. Click **Add**.
4. In the **Add Client Printer** dialog box, type the name of the client device in the **Client Name** box.

5. Specify the printer driver name by doing one of the following:
   - In the **Driver** box, type the name of the driver on the client printer.
   - Browse for the **Driver Mapping** by clicking one of the following buttons:
     - **Browse Mappings**. Opens a dialog box from which you can select a driver mapping. This dialog box displays the name of the client printer driver and the server printer driver.
     - **Browse Drivers**. Opens a dialog box from which you can select a printer driver. All printer drivers available in the farm are listed. The driver name that appears is the name of the server printer driver.
6. In the **Port** drop-down box, select the printer port. The client printer information is downloaded the next time the client device connects to the farm.

**Tip:** You can check if the client printer information was downloaded in the **Status** column - Pending or Downloaded.

## To display auto-created printers for Windows CE and DOS clients

1. Under the **Printer Management** node of the Advanced Configuration tool, select **Printers**.
2. From the **Actions** menu, choose **Printer Management > Client Printers**.

   The information about each selected client printer appears under the following columns:
   - **Client Name**. The name of the client device.
   - **Printer Name**. The name of the client printer.
   - **Driver**. The name of the driver on the client printer.
   - **Port**. The port on which the client printer is connected to the client device.
   - **Status**. Displays one of three values: Pending, Downloaded, or Deleting:
   - **Pending**. The client has not yet connected to the farm to allow information download for the client printer.

- **Downloaded**: The client connected and the client printer information was downloaded.
- **Deleting**: The auto-creation setting for the client printer is set to be deleted, but the client has not connected to the farm. When the client connects, the client printer is removed from the client and the client printer entry is removed from the displayed list.

---

**Note:** These printers are available only on the client device and appear only in server-based applications during the user's session.

---

3. To include client printers with Downloaded status in the list, click the **Show downloaded printers** check box.
4. To change the status of the selected client printer, click the **Reset**.

   For printers that are currently Deleting, the status is changed to Downloaded. For printers that are currently Downloaded, the status is changed to Pending. When the plugin next connects, the client printer information is downloaded.

### To update auto-created DOS and Windows CE client printer entries

Perform any of the following tasks to update your auto-created DOS and Windows CE client printer entries:

- To change the driver or port assigned to a client printer, click **Edit** to open the **Edit Client Printer** dialog box.
- To delete a client printer from the list, click **Delete**.
- To download the client printer configuration again, click **Reset**. The status of the client printer is set to Pending and its information is downloaded the next time the client device connects to the farm.

## Configuring Network Printers for Users

Before you can make network printers available to users, you must import information about these printers into your farm. This lets farm servers establish a connection to a network printer when a user prints. Making printers available to users requires performing two tasks, in sequence:

1. Importing the network print server information.
2. Assigning the imported network printer to users (that is, making it appear in sessions by filtering on an object that applies to the user's session).

You can import all the information either for one printer or all the printers on a print server. Before importing, have on hand the path for the printer in the form servername\printersharename or its IP address.

XenApp also needs to know the driver to use when constructing the printer connection. This information is collected on import and retained as a list of known print queues. However, you can also add individual printers from within the Session printers policy rule, which is handy if you did not import all information from a print server.

Importing printers from a print server identifies the drivers XenApp requires, but does not install these drivers. After importing printers, if the corresponding drivers are not installed automatically by Windows (because you configured a policy rule preventing auto-installation or they are third-party drivers), you must add the corresponding drivers to your farm servers manually.

Import printers before using the Session Printers policy rule to assign auto-created network printers.

After importing the information from your network print servers into your farm, make these printers available so your users can access this printer from within a session.

---

**Note:** Early versions of XenApp allowed an administrator to provision network printer connections to their users. In Presentation Server 4.0 and higher, the **Session printers** policy rule provides this functionality.

---

You can also configure XenApp to route print jobs to network printers through the client printing pathway.

Related topics:

"Auto-Creating Network Printers" on page 233

## To import printers from a network print server

1. In the left pane of the Advanced Configuration tool, select the **Printer Management** node.
2. On the **Actions** menu, select **Printer Management > Import Network Print Server**.
3. In the **Server** box, type one of the following:
   - The name of the print server you want to add. If using the name of the server, do not include the backslash characters; for example, type printserver1, not \\printserver1
   - The static IP address of the print server you want to add

4. Enter credentials to authenticate to the print server by doing one of the following:

   - Clear the **Use your Citrix Administrator credentials** check box and enter credentials for a network user account with access to printers on the specified server.
   - Select the **Use your Citrix administrator credentials** check box if you want to use the local user credentials that you enabled in Pass-Through Authentication.

   The printers available from the server are limited to those available to the user account entered. If you do not enter any user information, information about only those printers available to all users is imported.

   When the operation finishes, the print server appears on the **Network Print Servers** tab in the Advanced Configuration tool.

---

**Note:** If you do not want to add all the printers on the network print server, you can add individual printers when you configure the Session printers policy rule instead, as described in "To add a network printer while configuring the Session printers rule" on page 260.

---

## To import printers from other domains

Printers cannot be imported from a network print server when the printer resides in a different workgroup or the printer is in a different domain from any servers in the server farm. To import printers from other domains, there has to be a trust relationship between the domain the user is logging on to and the domain on which the print server resides.

1. Enable the printer to be imported by doing one of the following:

   - Add the network print server to the same domain as the servers in the farm
   - Add one of the computers running XenApp to the same domain as the network print server

2. Assign the printers to the Everyone group, rather than specific groups or users. Authenticate without credentials to receive the list of printers assigned to everyone.

   ---

   **Tip:** To allow Novell users access to Microsoft print servers, you must enable the Guest account and assign Everyone or Guest access.

   ---

If you cannot use one of these strategies to import network printers from other domains, you can still allow users to print to network print servers that are not in the same domain as the farm servers by using client printing.

## To assign printers using the Session printers policy rule

Before assigning printers using this rule, import any printers you want to assign from your network printer servers.

1. In the Advanced Configuration tool, 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**.

---

**Important:** The server merges all enabled session printer rules for all applied policies, starting from the highest to lowest priorities. However, if you disable a session printer rule in a policy, the merging stops at that policy and ignores all session printer rules in lower-priority policies, even if the option is enabled.

---

## To add a network printer while configuring the Session printers rule

1. On the **Printing > Session printers** policy rule page, click **Add**. If the rule is not currently enabled, click **Enabled** on the Session Printers rule page to display the **Add** button.
2. In the **Add printers** dialog box, click **New**.
3. In the **Add Network Printers to Farm** dialog box, select either authentication method:
   - **Console Administrator**. Use the current administrator credentials.
   - **Other**. Enter different credentials for authentication. These credentials must have Access permissions for the printer.
4. Click **Next**.
5. Using one of the following options, specify the **Network Printer Location**:
   - **Enter UNC Path**. Enter the path using the format servername\printername.
   - **Browse for Printer**. Locate a printer on the network.

Related topics:

"To assign printers using the Session printers policy rule" on page 260

## To specify a default printer for a session

To specify a network printer, it must already be imported it into your farm and added to the policy in which you are enabling the **Session printers** policy rule.

1. Complete the procedure, "To add a network printer while configuring the Session printers rule" on page 260.
2. On the **Session printers** rule page, from the **Choose client's default printer** drop-down list, choose one of the following:
   - **Name of the network printer you want to be default for this policy**. Printers do not appear in this list unless you added them to this policy.
   - **Set default printer to the client's main printer**. Sets the default printer for the session to the client's current default printer. If the client's main printer is not mapped, this option has no effect.

     ---

     **Important:** Mapping for the client's main printer can be disabled in other ways, such as through other Advanced Configuration tool policies, group policies, or Terminal Services settings.

     ---

   - **Do not adjust the user's default printer**. Uses the current Terminal Services or Windows user profile setting for the default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. You can use this option to present users with the nearest printer through profile settings (functionality known as Proximity Printing).

     When **Do not adjust the user's default printer** is selected, the default printer in a session will be the first printer autocreated in the session, which is either:

     - The first printer added locally to the Windows server in **Control Panel > Printers**
     - The first autocreated printer, if there are no printers added locally to the server.
3. Apply the policy to the group of users (or other filtered objects) you want to affect.

## To edit the printer settings in the sessions policy

1. On the **Session printers** rules page, select the name of the printer for which you want to modify the settings.
2. Click **Settings**.
3. Check **Apply customized settings**.
4. Change the settings for **Paper Size**, **Copy Count**, **Print Quality**, and **Orientation**.
5. To ensure that the settings you specify here are restored in concurrent sessions even if users modify them in their initial session, select the **Apply customized settings at every logon** check box.

   This check box applies to additional sessions opened while the user's first session is still active.

   ---

   **Important:** The type of Windows profiles configured in your environment change the effect of settings. For more information, see "Controlling Printing Settings and User Preferences" on page 235.

   ---

   If you clear this check box and a user opens his or her initial session, changes these printer settings, and then opens a second session (while the first session is still active), the settings you specified in this dialog box are not carried over to the second session.

   For example, if you specified **Landscape** as a custom Orientation setting, the check box is selected, a user starts a session (Session1), the user changes the Orientation to Portrait, and then starts another simultaneous session (Session2), Session2 uses your custom settings and the Orientation is Landscape. If you clear **Apply customized settings at every logon**, XenApp carries the user's changes into Session2 so the Orientation is Portrait.

   After clicking **OK**, the **Settings** value in the list of printers on **Session printers** properties page changes to **Modified**.

Related topics:

"To assign printers using the Session printers policy rule" on page 260

## To configure server local printers

To let users connecting to the farm print to a printer that is local to a farm server, physically connect the printer to a farm server and share it as follows:

1. On the server to which the printer is physically connected, in **Control Panel > Printers**, select the printer you want to share.

2. Choose **File > Properties**.
3. In the **Sharing** tab, select these check boxes:
   - **Share this printer**
   - **Render print jobs on client computers**
4. Verify the printer is shared by checking to see if the printer appears in the **Printer Management > Printers** tab of the Advanced Configuration tool. If the printer is not shared correctly, it does not appear in the **Printers** tab.

# Configuring Printers for Mobile Workers

When you want to make sure that users always see the closest printer to their client device in a session, you can configure the Proximity printing solution. Proximity printing enables users within a specified IP address range to automatically access the network printing devices that exist within that same range.

The ability to configure proximity printing assumes that your network is designed as follows:

- It uses a DHCP server to assign your users' IP addresses by their location (for example, floor of a building)
- All departments/floors within the company have unique designated IP address ranges
- Network printers are assigned IP addresses within the range of IP addresses for the department/floor in which they are located

Related topics:

"Printing and Mobile Workers" on page 238

## To configure Proximity Printing using IP addresses

1. Create a separate policy for each subnet (or to correspond with printer location).
2. In each one of these policies, enable the Session Printers policy rule and do the following:
   - Add the printers in that subnet's geographic location
   - Set **Choose client's default printer** to **Do not adjust the user's default printer**
3. Filter the policies by Client IP address.

Related topics:

"To assign printers using the Session printers policy rule" on page 260

# Changing Network Print Job Routing

By default, XenApp routes jobs to network printers from the application server directly to the print server (along the network printing pathway).

---

**Note:** Print jobs sent over the network printing pathway are not compressed. When routing printing jobs across a network with limited bandwidth, Citrix recommends routing jobs through the client device so that the ICA protocol compresses the jobs. To do so, select the **Always connect indirectly as a client printer** in the **Print job routing** rule.

---

Related topics:

"Overview of Client and Network Printing Pathways" on page 223

"Local and Remote Print Job Spooling" on page 220

## To configure client print job routing for network printers

1. In the Advanced Configuration tool, 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. Select **Printing** > **Client Printers**, and enable the **Print job routing** rule.
5. Select one of the following:
    - **Connect directly to network print server if possible**. This setting routes print jobs queued to a network printer directly from the farm server, if possible. That is, the XenApp server sends the print job over the network to the print server.
    - **Always connect indirectly as a client printer**. This setting routes jobs queued to a network printer through the ICA session and the client device. This setting lets users print to network printers that are accessible to them but not accessible to the farm servers (for example, a network print server that is on a different domain from the farm servers).

**Note:** Citrix Universal Printing is not available for network printers. If you enable the **Use Universal Print Driver Only** setting in the Printing > Drivers > Universal Driver rule, all print jobs queued to client-side network printers are routed through the client device, regardless of any settings in the Print job routing rule.

# Providing Tools for User Provisioning

The following groups of users cannot add printers to sessions unless you publish printer provisioning tools for them:

- Windows users who do not have access to the Add Printer wizard on the local client device or any applications that let them browse to printers
- Non-Windows plugin users

If you want these users to add printers on their own, publish either:

- The ICA Client Printer Configuration Tool (PrintCfg.exe). This tool lets Windows CE and DOS users add printers.
- The Add Printer wizard. Publishing this Windows wizard lets users with Windows plugins add printers that are on the local client device or network. Publishing this wizard is also referred to sometimes as publishing the Print Manager.

After a user adds printers using either of these methods, XenApp retains the printer information for the next time a user logs on from that client device. Client printers created using this process are considered *retained printers*.

## To publish the Windows Add Printer wizard

This procedure assumes that you already published Windows Explorer on the server on which you want to publish the Add Printer wizard.

1. Create the following folder at the root level of one of the XenApp server's drives:

   *C*:\Printers.{2227A280-3AEA-1069-A2DE-08002B30309D}

   where *C* represents a drive on the XenApp server.

   When you press **Enter**, the folder icon changes to a printer icon.

2. Create a published application with the following properties:

   **Command line.** "Path of explorer.exe" C:\Printers.{2227A280-3AEA-1069-A2DE-08002B30309D}

   **Working directory.** The path where explorer.exe is located.

If you get a path error and cannot access the published printers folder, modify the command line to include %*. For example,

**Command line**. "Path of explorer.exe" %*C:\Printers.{2227A280-3AEA-1069-A2DE-08002B30309D}

### To publish the ICA Client Printer Configuration Tool

1. Follow the instructions for publishing an application in "To publish a resource using the Publish Application wizard" on page 41.
2. On the **Location** page, enter the path for the ICA Client Printer Configuration tool (printcfg.exe) on your server.

   On a 64-bit system, the default location for the tool is C:\Program Files (x86)\Citrix\system32\printcfg.exe.

   On a 32-bit system, the default location for the tool is C:\Program Files\Citrix\system32\printcfg.exe.

## Controlling Users' Printing Preferences

This topic includes the following procedures:


- "To store users' printer properties" on page 266
- "To synchronize printer properties set out of sessions" on page 267


Related topics:


"Device or Session-Based Print Settings" on page 234

"Setting Default Printers" on page 238

"Controlling Printing Settings and User Preferences" on page 235


## To store users' printer properties

1. In the Advanced Configuration tool, 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, select **Printing** > **Client Printers** > **Printer properties retention**.
5. Select one of the following to specify where the printer properties should be stored:

   - **Held in profile only if not saved on client** (selected by default). Allows the system to determine the method. It stores printer

properties on the client device, if available, or if not, in the user profile. Although this option is the most flexible, it can also slow down logon time and use extra bandwidth to perform the needed system-checking.

Choose this option if your server farm requires backward compatibility with prior versions of XenApp and its plugins and is not constrained by bandwidth or logon performance.

- **Saved on the client device only**. Stores printer properties only on the client device. If users are assigned a Terminal Services mandatory profile or roaming profile, select this option.

  Choose this option only if all the servers in your farm are running XenApp 5.0 and your users are using Citrix XenApp Plugin versions 9.*x* and above.

- **Retained in user profile only**. Stores printer properties in the user profile on the server and prevents any properties exchange with the client device. This option is useful if your system is constrained by bandwidth (this option reduces network traffic) and logon speed or your users use legacy plugins. Note that this is applicable only if a Terminal Services roaming profile is used.

## To synchronize printer properties set out of sessions

To pick up printer properties directly from the printer itself, rather than from the properties store, use the following procedure. This procedure ensures that changes made offline to printers on the local computer are used next time a user starts a session.

---

**Caution:** Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

---

1. Open the Registry Editor and navigate to one of the following registry locations:

   - For 64-bit, HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences
   - For 32-bit, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences

2. Create the following registry key:

   Name:Win32FavorRetainedPrinterSettings

   Data Type: REG_SZ

   Value Data: false

3. Restart the Citrix Print Manager Service.

# Controlling Printer Driver Automatic Installation

Managing printer drivers is important for your servers' health and a successful printing experience. When XenApp autocreates printers, it determines if their corresponding drivers are missing. By default, XenApp installs any missing printer drivers from the Windows native printer driver set. If a problematic printer driver is installed automatically, it can cause issues.

You can either prevent printer drivers from being installed automatically, or, if you want to have them installed automatically, you can control what drivers are installed on farm servers by specifying the drivers on a compatibility list:

- If you know what printer drivers cause problems, you can specify banned printer drivers in the compatibility list
- If you do not know what drivers cause problems or you want tighter control over the drivers on the farm, specify to install only drivers on the compatibility list

When users log on:

- XenApp 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, XenApp does not set up the printer unless the Universal Printing feature is enabled
- When the compatibility list prevents setup of a client printer, XenApp writes a message in the server's Event log

To prevent drivers from being installed automatically, configure the **Printing > Drivers > Native printer driver auto-install** policy rule. See "To add or remove drivers or edit driver names in the compatibility list" on page 269 to ban specific printer drivers.

## To specify how client printer drivers are installed on farm servers

1. In the Advanced Configuration tool, 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**.
5. Under **Drivers**, you can configure the following rules:

    - **Native printer driver auto-install.** Use this rule to control whether Windows native drivers are automatically installed when auto-creating either a client or network printer. Enabling this rule lets you prevent the automatic installation of printer drivers. See "To control the automatic installation of printer drivers" on page 269.
    - **Universal driver.** Use this rule to specify whether auto-created client printers use universal printer drivers, model-specific printer drivers, or both. The universal drivers can enable printing even when model-specific drivers are not available. See "To specify the Universal Printer driver for sessions" on page 271.

## To control the automatic installation of printer drivers

1. Choose the **Native printer driver auto-install** policy rule.
2. On the **Native printer driver auto-install** properties page, select **Enabled**.
3. Select one of the following:

    - **Install Windows native drivers as needed** (selected by default). Allows XenApp to install Windows native printer drivers (those present in driver.cab) automatically when auto-creating either a client or network printer.

      **Caution:** Enabling this option may result in the installation of a large number of native drivers.

    - **Do not automatically install drivers**. Requires administrators to install individual native printer drivers manually.

## To add or remove drivers or edit driver names in the compatibility list

1. In the left pane of the Advanced Configuration tool, select **Printer Management > Drivers**.
2. On the **Actions** menu, select **Printer Management > Compatibility**.
3. Choose the required platform from the drop-down list.
4. Select one of the following **Compatibility list** options:

- **Allow only drivers in the list.** Keeps a list of incompatible drivers that are not allowed to be used by client printers and allow all others.
- **Allow all drivers except those in the list.** Keeps a list of compatible drivers that client printers are allowed to use and bans all others.

5. Update the list.

# Configuring Universal Printer Drivers on Farm Servers

If you configure a Universal printer driver for sessions, by default, XenApp always uses the XPS Universal Printer driver, when it is available. If it is not available, XenApp uses the Citrix Universal (EMF) Printer driver. The EMF Universal printer driver can be configured as the default by editing the registry.

The Citrix Universal printer drivers are listed in the **Drivers** tab of the **Print Server Properties** dialog box, which appears when you click the **Server Properties** button in **Control Panel > Printers**. Provided all prerequisites for the driver were installed when you ran XenApp Setup, the following drivers appear:

- Citrix Universal Printer, which is the .EMF driver
- Citrix XPS Universal Printer
- HP Color LaserJet 4500 PCL 5 (Citrix PCL5c Universal Driver)
- HP Color LaserJet 4500 PS (Citrix PS Universal Printer Driver)
- HP LaserJet Series II (Citrix PCL4 Universal Driver)

If you need a Universal driver that does not appear in this list, you must install it.

## To install a Citrix Universal Printer Driver on a farm server

1. Make sure the server has .NET 3.0 with SP1 is installed. If the server did not have .NET 3.0 with SP1 installed when you installed XenApp, install either .NET 3.0 with SP1 or .NET 3.5 from the \Support folder on the installation media.
2. Open the Microsoft Add Printer Driver wizard by clicking **Add** on the Print Server properties page and accept the initial default options.
3. Browse to the XPS Universal printer driver (CitrixUpd.inf) in one of the following folders in the installation media:
   - For 32-bit systems, \XenApp Server\w2k8\Program Files\Citrix\Drivers
   - For 64-bit systems, \XenApp Server\w2k8x64\Program Files\Citrix\Drivers

4. On the **Printer Driver** Selection page of the Add Printer Driver wizard, select one of the following drivers:
    - **Citrix Universal Printer**, which installs the .EMF based Citrix Universal printer driver
    - **Citrix XPS Universal Printer**

## To specify the Universal Printer driver for sessions

1. In the Advanced Configuration tool, 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. Choose the **Printing > Drivers> Universal driver** policy rule.
5. On the **Universal driver** properties page, select **Enabled**.
6. Select one of the following:
    - **Use universal driver only**. Specifies that the client printer uses the Universal printer driver only. Select this option if you do not want to use native drivers.
    - **Use universal driver only if requested driver is unavailable.** Uses native drivers for client printers if they are available. If the driver is not available on the server, the client printer is created automatically with the appropriate Universal driver.
    - **Use only printer model specific drivers**. Specifies that the client printer uses only the native drivers that are autocreated at logon. If the native driver of the printer is unavailable, the client printer cannot be autocreated.

### To change the default Citrix Universal Printer driver

To make XenApp try to use the Citrix XPS Universal Printer driver before the EMF-based Citrix Universal Printer driver, modify the registry.

1. Open the Registry Editor and select HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers.

   The Driver List registry key appears in the right pane after you select UniversalPrintDrivers.

2. In the Value data in the Driver List registry key, make one of the following changes:

   - To specify a different default printer driver, place the abbreviation for the printer driver at the beginning of the Value data string.

     For example, to make XenApp attempt to use the Citrix XPS Universal Printer driver before the EMF-based Citrix Universal Printer driver, specify XPS;EMF;PCL5c;PCL4;PS.

   - To prevent XenApp from using a specific Universal Printer driver, remove its abbreviation from the Value data string.

3. Restart the Citrix Print Manager Service.

## Mapping Client Printer Drivers

If the servers in your farm have the same drivers as the client printers but the drivers themselves are named differently (for example, "HP LaserJet 4L" versus "HP LaserJet 4"), XenApp may not recognize the drivers are the same and users will have difficulty printing or printer autocreation may fail.

You can resolve this issue by overriding, or *mapping,* the printer driver name the client provides and substituting an equivalent driver on the server. Mapping client printer drivers gives server applications access to client printers that have the same drivers as the server but different driver names.

You can use the printer driver remapping feature to substitute

- Good printer drivers for bad drivers
- Specific Windows printer drivers for manufacturer's client printer drivers
- A driver that is available on Windows server for a client driver name

Each client provides information about client-side printers during logon, including the printer model name. During client printer autocreation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The autocreation process then employs the identified, available printer drivers to construct redirected client print queues.

## To define client printer driver mappings for all servers in the farm

1. In the Advanced Configuration tool, expand the **Printer Management** node and select **Drivers**.
2. From the **Actions** menu, choose **Printer Management > Mapping**.

   Use the **Driver Mapping** dialog box to maintain a list of mappings between client drivers and server drivers if they are known to have different names.
3. In the **Driver Mapping** dialog box, choose a server platform. The mapping you create maps all the servers in the farm on the platform you specify here to the client driver you specify in the **Add Mappings** dialog a box.
4. Click **Add** to 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.

---

## To map client printer drivers to server printer drivers

1. In the left pane of the Advanced Configuration tool, select **Printer Management > Drivers**.
2. On the **Actions** menu, click **Printer Management > Mapping**.
3. In the **Driver Mapping** dialog box, choose the required platform from the drop-down list and click one of the following:
   - **Add**. Lets you associate a server printer driver with a client printer driver.
   - **Edit**. Lets you edit an existing mapping. Select the driver mapping you want to modify and click **Edit**.
4. In the **Add/Edit Mappings** dialog box, enter the client printer driver name and select the server driver from the drop-down list that you want to substitute for the client printer driver.

**Tip:** To display driver information for a specific server, select the server from the **Servers** folder in the left pane of the Advanced Configuration tool and select the **Printer Drivers** tab.

# Maintaining Printing

You might need to perform some of the following maintenance tasks:

- "Increasing Printing Speed and Session Performance" on page 274
- "Updating Network Print Server Information" on page 277
- "Replicating Printer Drivers Manually" on page 278
- "Replicating Printer Drivers Automatically" on page 280

You can also perform basic printing management tasks from the Advanced Configuration tool, such as displaying drivers and printers.

## Increasing Printing Speed and Session Performance

While printing files from published applications to client printers, other virtual channels (such as video) may experience decreased performance due to competition for bandwidth especially if users are accessing servers through slower networks or dial-up connections. To prevent such degradation, you can limit the bandwidth used by client printing.

**Important:** The printer bandwidth limit is always enforced, even when no other channels are in use.

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 the Printer policy rule to enable and disable the printing bandwidth session limit.
- Use individual server settings to limit printing bandwidth in the server farm. You can perform this task in either the Access Management Console or the Advanced Configuration tool.

You can use the Citrix Session Monitoring and Control Console to obtain real-time information about printing bandwidth. The print spooling virtual channel control (that is, the CTXCPM Client printer mapping virtual channel control) lets you set a priority and bandwidth limit for bandwidth control of this virtual channel. For more information, see the Citrix Community Web site.

## To configure a printing bandwidth rule in an existing policy

1. In the left pane of the Advanced Configuration tool, select the **Policies** node.
2. In the right pane of the tool, select a policy that is suitable for sessions with low connection speeds (for example, it contains the group of users affected).
3. From the **Actions** menu, choose **Properties**.
4. Expand **Bandwidth**.
5. Select one of the following folders:
   - **Session Limits**. Specifies the bandwidth available for printing in kilobits per second (kbps).
   - **Session Limits** (%). Limits the bandwidth available for printing to a percentage of the overall bandwidth available.

   **Note:** If you want to specify bandwidth as a percentage using the Session Limits (%) rule, you must enable the Overall Session rule in the Session Limits folder as well.
6. Select **Printer** to configure the rule and configure the bandwidth limit.

## To limit printer bandwidth for a server using the Access Management Console

1. In the left pane of the Access Management Console, select **Citrix Resources** > **XenApp** > ***farmname*** > **Servers folder** > ***servername***.
2. From the **Actions** menu, choose **Properties**.
3. In the **Properties** tree, select **ICA** > **Printer Bandwidth**.
4. Select one of the following options:
   - **Unlimited client printer bandwidth**. Client print jobs use as much available bandwidth in the connection as possible.
   - **Limit bandwidth to use (kbps)**. Sets an upper limit (in kbps) for the bandwidth used by client print jobs. Enter the maximum amount of

bandwidth in kilobits per second. This is the amount of bandwidth that a print job can consume in an ICA connection.

---

**Tip:** The same information is available from the **ICA Printer Bandwidth** tab when you select the Servers folder in the XenApp Advanced Configuration tool.

---

## To display the client printer bandwidth for a server

1. In the Advanced Configuration tool, select the **Printer Management** node.
2. In the right pane, select the **Bandwidth** tab.

   The **Bandwidth** pane appears, displaying the maximum bandwidth that a print job queued from a client printer can use in a single connection. By default, the bandwidth is unlimited.

## To limit printer bandwidth for a server using the Advanced Configuration Tool

1. In the Advanced Configuration tool, select the **Servers** folder.
2. In the right pane, select the **ICA Printer Bandwidth** tab.
3. In the right pane, select the server name for which you want to limit the bandwidth.
4. Select the server in the right pane and, on the **Actions** menu, click **Printer Management > Edit**.

   The **Edit Bandwidth Limit** dialog box appears. Use this dialog box to limit the bandwidth allocated to printing for the selected server.
5. Select one of the following options:

   - **Unlimited bandwidth**. This option allows client print jobs to use as much available bandwidth in the connection as possible.
   - **Limit bandwidth to use (kbps)**. This option sets an upper limit (in kbps) for the bandwidth used by client print jobs. Enter the maximum amount of bandwidth in kilobits per second that a print job can consume in an ICA connection.

## To copy one server's limit to one or more servers

1. In the Advanced Configuration tool, follow Steps 1 to 3 from "To limit printer bandwidth for a server using the Advanced Configuration Tool" to select the server whose limit you want to copy.
2. On the **Actions** menu, click **Printer Management > Copy**.

3. Select the destination servers in the **Copy Bandwidth Settings** dialog box.

   The dialog box lists all servers in the farm except the source server.

# Updating Network Print Server Information

Whenever you add or remove printers from a network print server in the farm, update the information to ensure the Advanced Configuration tool displays an accurate listing of printers. You can:

- Update one individual printer that you added to your network.
- Update all of the printers in a print server after you imported the initial list of printers from your print server.
- Remove outdated print server information from the server farm. Removing a print server from your Windows network is not reflected automatically in the Advanced Configuration tool. You must discard the print server information referenced by the Advanced Configuration tool. Discarding information for a network print server also removes any associated autocreation settings.

## To update information about a network print server

1. In the left pane of the Advanced Configuration tool, select **Printer Management**.
2. On the **Network Print Servers** tab, select the print server you want to update.
3. On the **Actions** menu, select **Printer Management > Update Network Print Server**.
4. In the **Update Network Print Server** dialog box, enter the credentials for a user account with access to printers on the specified print server.

   The printers available from the server are limited to those available to the user account entered.

## To discard information for a network print server

1. In the left pane of the Advanced Configuration tool, select **Printer Management** and select the **Network Print Servers** tab.
2. Select the print server you want to remove from the Advanced Configuration tool.
3. On the **Actions** menu, select **Printer Management > Discard Network Print Server**.

# Replicating Printer Drivers Across a Farm

To print from a published application accurately, the driver for the selected printer must be installed on the application's server. To maintain consistent drivers across your farm, you can copy or *replicate* drivers from one server to another. Replication copies driver files and registry settings from a source server to one or more destination servers.

Replication may be easier than visiting all the servers and installing the driver on each machine. You can replicate drivers for both client and network printers.

XenApp provides two driver replication features:

- Use **Replicate** to copy a driver manually to specific existing servers. For example, to add the driver for a plotter only to the servers hosting the relevant application.
- Use **Autoreplicate** to push a set of drivers to all current and future servers in the farm. See "Replicating Printer Drivers Automatically" on page 280.

## Replicating Printer Drivers Manually

You can copy printer drivers to other servers on your farm by replicating them manually. You may want to replicate drivers manually when:

- You need a speciality driver on specific servers as opposed to all servers on your farm
- You want to ensure that all servers in your farm that use a shared printer, which is attached locally to a farm server, have the correct drivers for it

You can either manually replicate one or more drivers or replicate all drivers for a shared printer.

### To replicate one or more drivers

The destination servers must be on the same platform as the selected driver. If the destination server is not on the same platform as the driver, its name will not appear.

1. In the left pane of the Advanced Configuration tool, select **Printer Management > Drivers**. The **Drivers** tab displays a list of all drivers available from all servers in the farm.
2. Choose a server source from the drop-down list of servers.

   A list of drivers on the chosen server appears in the lower left pane. Choose **Any** for replication from any one of the servers on which the driver is installed.

   Citrix recommends setting the source to **Any** only if you are certain that all servers in your farm have the same driver version installed. If Server A has

driver version 2.0 and Server B has version 2.1, explicitly choose a driver as the source.

3. Select one or more drivers and, on the **Actions** menu, select **Printer Management > Replicate Drivers**. The drivers must be supported on the same platform.
4. Choose your replication option:
   - **Replicate to all servers on the same platform and add to the Auto-replication list**. The driver information is copied to all other servers in the farm on the same platform and is added to the autoreplication list for the farm.
   - **Choose the servers to which you want to copy the driver information**. Select the servers from the list provided.
5. To replace old drivers, select **Overwrite existing drivers**.

   If the destination server already has a driver installed with the same name, the selected driver overwrites the existing driver.

To check the progress of the driver replication, select each server in the left pane of the Advanced Configuration tool and select the **Printer Drivers** tab. After the driver is replicated, it is listed on the Printer Drivers tab. If the replication did not complete, an entry is written to the source server's event log.

#### To replicate all drivers for a shared printer

This procedure lets you replicate the drivers from a shared printer that is local to a farm server.

1. Under **Printer Management** in the left pane of the Advanced Configuration tool, select **Printers**.

   The **Printers** tab displays a list of all printers in the farm.
2. Select the shared printer from which you want to replicate the drivers. On the **Actions** menu, select **Printer Management > Replicate Drivers**.
3. Choose your replication option:
   - **Replicate to all servers on the same platform and add to the Auto-replication list**. The driver information is copied to all other servers in the farm on the same platform and is added to the autoreplication list for the farm.
   - **Choose the servers to which you want to copy the driver information**. Select the servers from the list provided.
4. To replace old drivers, select **Overwrite existing drivers**.

If the destination server already has a driver installed with the same name, the selected driver overwrites the existing driver.

5. To replace old drivers, select **Overwrite existing drivers**. By default, this option is not selected.

## Replicating Printer Drivers Automatically

You can instruct XenApp to replicate any new printer drivers you add to the farm automatically by creating an autoreplication list. This lists drivers that are replicated automatically to each server as it joins or connects to the farm.

When you edit the autoreplication 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, XenApp copies the driver from any server that is available in the farm at the time of autoreplication 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 users might not be able to print consistently.

XenApp 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 Advanced Configuration tool 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. Perform replication during low usage periods.

---

The autoreplication list is subdivided based on the server platform.

### To replicate a driver automatically to each server in the farm

1. In the left pane of the Advanced Configuration tool, select **Printer Management > Drivers**.
2. On the **Drivers** tab, select the driver you want to replicate.
3. On the **Actions** menu, select **Printer Management > Auto-replication**.
4. In the **Auto-replication** dialog box, choose the required platform from the drop-down list and click **Add**.
5. In the the **Select Drivers to Replicate** dialog box, choose the printer drivers that will be copied to all servers in the farm:

    A. Choose a server source from the drop-down list of servers to display only the printer drivers installed on the selected server.

    By default, **Any** appears in the Server list. Choose **Any** for replication from any one of the servers on which the driver is

installed. Citrix recommends setting the source to **Any** only if you are certain that all servers in your farm have exactly the same driver version installed.

B. If you want to prevent XenApp from creating duplicate drivers with the same name, select the **Overwrite existing drivers** check box.

If you select this check box and the destination server already has a driver installed with the same name, the selected driver overwrites the existing driver.

---

**Note:** To display the servers where a driver is installed, select the driver.

---

6. Click **Yes** to the warning message, if prompted.

After you add a driver, the Auto-replication dialog box displays information about each printer driver in the list under the following columns:

- **Source**. The name of the server from which the driver is copied. If you use **Any**, the driver is replicated from any one of the servers on which the driver is installed.
- **Overwrite**. If you selected Overwrite existing drivers when you added a driver to the list, a checkmark appears. Otherwise, the column is blank.

### To remove drivers from the autoreplication list

1. In the left pane of the Advanced Configuration tool, select **Printer Management > Drivers**.
2. On the **Actions** menu, select **Printer Management > Auto-replication**.
3. Choose the required platform from the drop-down list.
4. Select the driver you want to remove and click **Remove**.

# Displaying Printers

The following table summarizes where you can manage and modify print queues and display printers in a XenApp environment. To understand this table, it is critical that you understand the terms *client printing pathway* and *network printing pathway*. Client printing pathway is not synonymous with printers attached to client devices.

| | Printing Pathway | UAC Enabled? | Location |
|---|---|---|---|
| Client printers<br>(Printers attached to the client device) | Client printing pathway | On | **Print Management** snap-in in the Microsoft Management Console |
| | | Off | **Control Panel > Printers** |
| Network printers<br>(Printers on a network print server) | Client printing pathway | On | **Print Management** snap-in in the Microsoft Management Console |
| | | Off | **Control Panel > Printers** |
| Network printers<br>(Printers on a network print server) | Network printing pathway | On | Print Server > **Print Management** snap-in in the Microsoft Management Console |
| | | Off | Print Server > **Control Panel > Printers** |
| Server local printers<br>(Shared printers locally attached to a XenApp server) | N/A | On | **Control Panel > Printers** |
| | | Off | **Control Panel > Printers** |
| Local network server printers<br>(Printers from a network print server that are added to server running XenApp) | Network printing pathway | On | **Control Panel > Printers** |
| | | Off | **Control Panel > Printers** |

Related topics:

"Overview of Client and Network Printing Pathways" on page 223

# Displaying Printers Using the Network Printing Pathway

Network print server printers appear on the Network Print Servers tab when you click the Printer Management node in the Advanced Configuration tool. However, if you want to modify or manage a user's network print queue that a user printed to across the network printing pathway, you must manage it through **Control Panel > Printers** on the print server with the correct level of Windows administrator privileges. Print queues for network printers that use the network printing pathway are private and cannot be managed through XenApp.

Whenever you configure a network printing pathway and the server hosting the application does not have or cannot install the driver, by default, XenApp sends the print job along the client printing pathway. You can tell a job sent to the network printer is redirected along the client printing pathway when you see printers appearing in the Windows **Server Manager Snap-in for Printers** that has the following syntax:

***PrinterName* on *PrintServer* (from *clientname*) in session *n***

where *PrinterName* is the name of the printer being redirected and *PrintServer* is the name of the print server it is associated with, and *clientname* is the name of the client through which the print job is being rerouted. (For example, **Dell Laser Printer 1710n Ps3 on 3r41-2 (from 3R39-2) in session 2**.)

## To display a list of the network and server local printers in your farm

This procedure displays a list of all the imported print server printers and server local printers in your farm. This list does not include client printers.

1. In the Advanced Configuration tool, expand the **Printer Management** node and select **Printers**.
2. The **Printers** tab displays the following information about each printer:
    - **Shared Name**. The name of the printer available from the associated print server.
    - **Server**. The name of the print server.
    - **Driver**. The name of the driver in use by the printer. No information appears for network print servers.
    - **Platform**. The operating system for the print server. No information appears for network print servers.

## To display a list of the server local printers for a server

You can display a list of the shared local printers available on a specific server.

---

**Note:** Server local printers must be shared in Windows Server 2008 or they do not appear in XenApp Advanced Configuration tool. See “To configure server local printers” on page 262.

---

1. In the Advanced Configuration tool, select **Servers** > ***servername***.
2. Click the **Printers** tab.

    The Printers tab displays the following information about each printer:

- **Shared Name**. The name used to connect to the printer on the associated print server.
- **Driver**. The name of the driver in use by the printer. No information appears for network print servers.

# Displaying Printers Using the Client Printing Pathway

If UAC is not enabled, you can, however, display and manage redirected client print queues and server local printers through **Control Panel > Printers** of individual servers. The client printers displayed on a server fluctuate based on what sessions are active on a server because XenApp creates these printers based on the printers on the connecting client devices. You can display client printers in **Control Panel > Printers**.

## To display printers that use the client printing pathway when UAC is enabled

1. On the XenApp server that is hosting the session for which you want to display the printers, install the **Print Services** server role.
2. In **Administrative Tools**, open the **Print Management** stand-alone snap-in.
3. To display client redirected printers, in the Print Management tree, select **Print Management** > **Custom Filters** > **All Printers**.

   The **Print Management** snap-in displays the client printers redirected from all clients connected to that server. You can display and manage the print queues for these printers and select **Printers With Jobs** in the Print Management Tree to display active jobs on redirected printers.

## To display printers that use the client printing pathway without UAC enabled

On the XenApp server, open **Control Panel > Printers**.

The **Printers** screen displays the local printers mapped to the ICA session. By default, the name of the printer takes the form *printername* (from *clientname*) in session *x*; for example, "printer01 (from machine01) in session 7." *Printername* is the name of the printer on the client device, *clientname* is the unique name given to the client device or the Web Interface, and *x* is the SessionID of the user's session on the server.

# Displaying Drivers

You can display drivers on a per-server or per-farm basis in the Advanced Configuration tool.

## To display a list of the drivers on a server

This procedure displays a list of all the printer drivers on a specific server.

1. In the Advanced Configuration tool, select **Servers** > ***servername***.
2. Click the **Printer Drivers** tab.
3. In the right pane of the tab, select a driver to list the servers on which it is installed.

## To display a list of the printer drivers available from a server in your farm

1. In the left pane of the Advanced Configuration tool, select **Drivers**.
2. In the Drivers display, select a server from the **Server** drop-down list, which displays the servers in the farm. The default value is Any.
3. To display only the printer drivers installed on the selected server, select a server from the drop-down list. The selected server is used as the source for driver replication if that command is selected.

   The information about each printer driver appears under the following columns:

   - **Driver**. The name of the printer driver.
   - **Platform**. The operating system for the driver. If a server is selected, it is the operating system for the server.

   In the right pane of the tab, select a driver to list the servers on which the driver is installed.

   To replicate printer drivers, select one or more drivers and on the Actions menu, click **Printer Management > Replicate Drivers**.

# Maintaining Server Farms

A server farm is a group of servers running Citrix XenApp and managed as a single entity. The servers in the server farm share a single IMA-based data store. Using the Access Management Console and XenApp Advanced Configuration, you can manage all the servers in all your farms remotely.

Citrix recommends performing farm maintenance tasks from the data collector, assuming no applications are published on the data collector, because this updates farm data faster. Performing farm maintenance tasks from a server hosting published applications can slow down users trying to connect to published applications and take longer to update in the data store.

This topic describes how to perform the following tasks:

- “Displaying and Organizing Your Farm”
- “To configure general farm properties”
- “To search for objects in your farm”
- “Connecting to a Server”
- “Restarting Servers at Scheduled Times”
- “To repair a XenApp installation”
- “Changing XenApp Farm Membership”
- “Removing and Reinstalling XenApp”
- “Monitoring Server Performance with Health Monitoring & Recovery”
- “Using Citrix Performance Monitoring Counters”
- “Enabling SNMP Monitoring”
- “Optimizing Server Performance”
- “Managing Farm Infrastructure”
- “Updating Citrix License Server Settings”
- “Setting the Product Edition”

- "Setting the Citrix XML Service Port"

# Displaying and Organizing Your Farm

Server and farm properties are configuration settings specific to individual servers or entire farms. Using the **Farm Properties** page, you can configure a number of properties at the farm level. By default, all servers are configured to use the farm settings for a given property.

Using a **Server Properties** page, you can override farm settings and customize the configuration of individual servers. For example, if you specify a license server on a **Farm Properties** page, all servers in the farm, including servers you add later, point to that license server. To point particular servers to a different license server, use those **Server Properties** pages to specify a different license server.

---

**Important:** Interoperability of XenApp 5.0 for Windows Server 2008 with versions prior to Presentation Server 4.5 for Windows Server 2003 is no longer supported.

---

## To view farm information

You can view summary information about the server farm, published resources, servers, and sessions. Depending on the configuration of your farm, some areas may not appear.

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, click **Change display** > **Information**.

   The right, or details, pane of the console displays summary information about the farm, servers, published resources, and sessions.
3. From **Available Displays**, you can click **Alerts**, **Users**, **Offline Sessions**, **Hotfixes**, **Configured file types**, **Read-only Properties**, or **Offline users** for more detailed information about these areas.

---

**Note:** The displays that appear depend on the features you enabled in XenApp.

---

## To view server information

You can view a wide variety of summary information about each server in the farm. Depending on the configuration of your server, some areas may not appear.

1. In the left pane of the Access Management Console, select a server.

2. From the **Action** menu, select **Change display** > **Information**.

   The details pane of the console displays summary information about the product edition and version, installed service packs, server operating system, and TCP address. Click **Expand list** to view more server summary information.

3. From **Available Displays**, you can select **Alerts**, **Users**, **Sessions**, **Processes**, **Hotfixes, Published applications**, **Read-only Properties**, **View server health**, and **Trace Sessions** for more detailed information about these areas.

---

**Note:** The displays that appear depend on the features you enabled in XenApp.

---

# Organizing Your Farm Display in the Console

You can group applications or servers in folders to make navigating through their console listings easier. Folders are also useful for Object Based Delegated Administration. Grouping servers into folders can facilitate the process of delegating administrative tasks to Citrix administrators.

You can move items between folders by dragging and dropping.

---

**Important:** The folder structure within Applications is not related to, or reflected in, the folder structure for clients using Program Neighborhood.

---

## To create a folder

1. In the left pane of the Access Management Console, select **Applications** or **Servers**.

   To create a subfolder, select the folder in which you want the new folder created.

2. From the **Action** menu, select **New** > **Create folder**.

3. In the **New Folder** dialog box, type the name of the new folder, and select **Copy permissions from the parent folder** if you want the new folder to be accessed by the same administrators who have access to the parent folder.

**Note:** This is a one-time only inheritance; no updating occurs if you make permission changes to the parent folder later. If you clear the check box to disable the option, only administrators with view only or full administration privileges can access the folder. Administrators with Custom privileges cannot access the folder until they are given permission.

4. Click **OK**.

## To rename a folder

1. Select the folder in question and from the **Action** menu, select **Rename**.
2. Type the new name of the folder directly in the left pane.

## To delete a folder

1. If the folder contains applications or servers, move them to other locations.

**Note:** You can delete empty folders only.

2. Select the empty folder you want to delete.
3. From the **Action** menu, select **Delete folder**.
4. Click **Yes** to confirm the deletion.

## To move the contents of a folder

1. Select the published application, server, or folder you want to move.
2. From the **Action** menu, select **Move to folder**.
3. Select the required destination folder and click **OK**.

## To move servers to a folder

1. In the left pane, select the destination folder (under the Servers folder only) into which you want to move a server.
2. From the **Action** menu, select **All Tasks** > **Move servers to folder**.
3. Select the required server or subfolder and click **Add**.
4. Click **OK**.

**Note:** Published applications can be moved only to **Applications** or folders under **Applications**. Similarly, servers can be moved only to **Servers** or folders under **Servers**.

# To configure general farm properties

General farm properties includes settings such as broadcast response, client time zones, Citrix XML Service, and Novell Directory Services.

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Farm-wide** > **XenApp** > **General**.
4. Under **Respond to client broadcast messages**, select either of the following check boxes to respond to broadcasts from clients:
   - **Data collectors**
   - **RAS servers**
5. Under **Client time zones**, select **Use Client's local time**.

   This means that all time stamps for all applications are based on the client's time instead of the server's time.

   You can then select **Estimate local time for clients**. This time is based on the client's time zone settings.

   ---

   **Note:** Client time zone settings override similar settings that are configured in Microsoft Windows Group Policy.

   ---

   ---

   **Important:** Version 6.*x* of the Presentation Server Clients introduced the capability to send time zone information to the server. For earlier versions of clients, the client sends the local time, which could be incorrect or modified by the user, so the server's estimate of the client time zone might not be accurate.

   ---

6. Under **Citrix XML Service**, select **XML Service DNS address resolution** to allow a server to return the fully qualified domain name (FQDN) to clients using the Citrix XML Service.

   ---

   **Important:** DNS address resolution works only in server farms that contain servers running MetaFrame XP Feature Release 1 or later, and clients must be using Presentation Server Client Version 6.20.985 or later or Citrix XenApp Plugin for Hosted Apps version 11.*x*.

   ---

7. Under **Novell Directory Services**, in the **NDS preferred tree** field, enter the name of the NDS tree used to access NDS user account information and authentication.
8. Under **Published application icons**, select **Enhanced icon support** to enable additional icon color depths (32-bit) when you publish applications. To apply this setting to previously published applications, delete them and publish the applications again.

# To search for objects in your farm

XenApp provides an advanced search feature so that you can search for the objects in your farm such as discovered items, sessions or applications by user, and servers that do not have a specific hotfix applied to them.

1. From the **Tasks** pane of the Access Management Console, select **Search** > **Advanced search**.
2. In the **Advanced Search** dialog box, in the **Find** box, select one of the following:
   - **Discovered items**. Searches discovered items.
   - **Sessions By User**. Lists the sessions to which a specific user is connected. Type a user name in the **Name** box.
   - **Applications By User**. Lists the applications that the specified user is using. Type a user name in the **Name** box.
   - **Servers without hotfix**. Lets you search for all of the servers missing a specific hotfix. This feature is useful if you want to check that you applied a hotfix to all servers in your farm. Type a hotfix number in the **Name** box.
3. If desired, select one of the following locations to search in:
   - **A farm**. Displays all applications in that farm matching the search.
   - **An application folder**. Displays all applications in that folder matching the search.
   - **An application**. Displays only that application, if it matches the search.
   - **A server folder**. Displays all applications published to servers in the folder, that match the search.
   - **A server**. Displays all applications published to the server, that match the search.

- **A zone**. Displays all applications published to servers in the zone, that match the search (may be useful for zone preference and failover scenarios).
- **Any other node**. Displays all applications in all farms, that match the search.

---

**Note:** If there are multiple farms in the search scope, the **Select directory type** box contains multiple **Citrix User Selector, for farm <n>** entries. After you enter or select a complete user name, the user's account authority is checked. If you enter a user name and password that is incorrect or is not recognized by any of the farms in the search scope, the **Enter Credentials** dialog box reappears. If the user is an Active Directory Service (ADS) user, you are prompted whether or not you want to do a full ADS tree search.

After resolving the credentials, a progress dialog may appear and then your search results appear.

---

# Connecting to a Server

You can configure a XenApp server to allow other servers to access it remotely. The following topics describe how to allow remote servers to connect to the console, published desktop, or actual desktop of any server in your farm.

- "Connecting to a Server's Console"
- "Connecting to a Server's Published Desktop"
- "Connecting Directly to a Server's Desktop"
- "Limiting Connections"
- "Controlling Server Logons"
- "Enabling Content Redirection and Remote Console Connections"
- "Configuring Auto Client Reconnect"

## Connecting to a Server's Console

You can connect to a server's console; however, you must enable this option before you can connect.

---

**Note:** You must be a local administrator to log on to a remote console.

---

### To enable connections to a server's console

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **All Tasks** > **Modify server properties** > **Modify all properties**.
3. In the **Server Properties** dialog box, select **XenApp** > **Remote Console Connection**.
4. If enabled, clear the **Use farm settings** check box.
5. Select the **Remote connections to the console** check box.
6. Click **OK**.

### To connect to a server's console

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **All Tasks** > **Connect to server** > **Connect to server's console**.
3. Click **OK** to accept the default values.

   If desired, you can specify values for the **Width**, **Height**, **Colors**, and **Encryption** level for the remote console display.

   After you click **OK**, the connection progress dialog box appears. You are prompted to enter your credentials and then the console appears.

## Connecting to a Server's Published Desktop

You can access a server's desktop only if the desktop of the selected server is published, and the selected server is running XenApp 5.0 or later.

### To connect to a server's published desktop

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **All Tasks** > **Connect to server** > **Connect to server's published desktop**.
3. In the **Launch ICA Desktop Session** dialog box, choose from the following selections. The selections you make here become the new default settings.

   - **Published Desktop**. Select the published desktop from the list to which you want to connect.
   - Accept the **Width** and **Height** values or specify a different resolution.

- **Colors**. Select the color depth for the application. The available options are 16 Colors, 256 Colors, High Color (16-bit), or True Color (24-bit).
- **Encryption**. Select one of the following options from the list.
  - **Basic** encrypts the connection using a non-RC5 algorithm. Basic encryption protects the data stream from being read directly but can be decrypted.
  - **128-Bit Login Only (RC5)** encrypts the logon data with RC5 128-bit encryption and the ICA connection with basic encryption.
  - **40-Bit (RC5)** encrypts the connection with RC5 40-bit encryption.
  - **56-Bit (RC5)** encrypts the connection with RC5 56-bit encryption.
  - **128-Bit (RC5)** encrypts the connection with RC5 128-bit encryption.

4. Click **OK**.

# Connecting Directly to a Server's Desktop

**Note:** Starting with 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) using Terminal Services Configuration.

## To connect directly to a server's desktop

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **All Tasks** > **Connect to server** > **Connect directly to server's desktop**.
3. In the **Launch ICA Desktop Session** dialog box, choose from the following selections. The selections you make here become the new default settings.
   - Accept the **Width** and **Height** values or specify a different resolution.
   - **Colors**. Select the color depth for the application. The available options are 16 Colors, 256 Colors, High Color (16-bit), or True Color (24-bit).

- **Encryption**. Select one of the following options from the list.
  - **Basic** encrypts the connection using a non-RC5 algorithm. Basic encryption protects the data stream from being read directly but can be decrypted.
  - **128-Bit Login Only (RC5)** encrypts the logon data with RC5 128-bit encryption and the ICA connection with basic encryption.
  - **40-Bit (RC5)** encrypts the connection with RC5 40-bit encryption.
  - **56-Bit (RC5)** encrypts the connection with RC5 56-bit encryption.
  - **128-Bit (RC5)** encrypts the connection with RC5 128-bit encryption.

4. Click **OK**.

# Limiting Connections

When a user starts a published application, the client establishes a connection to a server in the farm and initiates a client session. If the user then starts another published application without logging off from the first application, the user has two concurrent connections to the server farm. To conserve resources, you can limit the number of concurrent connections that users can make.

## To limit connections

1. Select the farm in the left pane.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Farm-wide** > **Connection Limits**.
4. Select **Maximum connections per user** and type the numerical limit.
5. Select **Enforce limit on administrators** to extend the connection limit to Citrix administrators.

---

**Important:** Limiting connections for Citrix administrators can adversely affect their ability to shadow other users.

---

6. Select **Log over-the-limit denials** to record information about denied connection events in the server's system log.

7. Click **Apply** to implement your changes and then **OK** to close the **Farm Properties** dialog box.

# Controlling Server Logons

By default, logons are enabled for each server in a farm. You can disable logons on a per-server basis; for example, during maintenance of a server.

## To disable logons to a server

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **All Tasks** > **Disable logon**.
3. Click **Yes** to confirm.
4. Complete your maintenance work.

## To enable logons to a server

1. To make the server accessible to users again, from the **Action** menu, select **All Tasks** > **Enable logon**.
2. Click **Yes** to confirm.

# Enabling Content Redirection and Remote Console Connections

You can configure content redirection and remote console connections as a farm-wide server default setting or as an individual setting for a particular server.

Use the following procedures to enable or disable content redirection and remote console connections as a default setting for one or all the servers in your farm.

Related topics:

“Redirecting Content from Client to Server” on page 53

“Redirecting Content from Server to Client” on page 54

## To configure a content redirection setting for a farm

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **XenApp**.
4. Select **Content Redirection** to allow users to open URLs found in remote published applications in a local Web browser.

5. On the **Content Redirection** page, select **Content redirection from server to client**.

### To configure a remote console connection setting for a farm

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **XenApp**.
4. Select **Remote Console Connections** to allow administrators to connect remotely to console sessions on servers running Microsoft Windows 2003.
5. On the **Remote Console Connections** page, select **Remote connections to the console**.

### To configure a content redirection setting for a server

1. Select the server in the left pane.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **XenApp**.
4. Select **Content Redirection** to allow users to open URLs found in remote published applications in a local Web browser.
5. On the **Content Redirection** page, select **Use farm settings** (available on server level only) or **Content redirection from server to client**.

### To configure a remote console connection setting for a server

1. Select the server in the left pane.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **XenApp**.
4. Select **Remote Console Connections**.
5. Select **Use farm settings** (available on server level only) or **Remote connections to the console**.

## Configuring Auto Client Reconnect

You can configure Auto Client Reconnect as a farm-wide server default setting or as an individual setting for a particular server.

Use the following procedures to configure server reconnection settings to be used when connections between client devices and XenApp servers are broken.

## To configure a default Auto Client Reconnect setting for a farm

1. Select the farm in the left pane.
2. From the **Action** menu, select **Modify farm properties** > **Modify all properties**.
3. From the **Properties** list, select **Server Default** > **ICA** > **Auto Client Reconnect**.
4. Choose one of the following options:
   - **Require user authentication**. Select this option if you want users to be prompted for new credentials during automatic reconnection to an ICA session. Do not select this option if you want users to be reauthenticated automatically during reconnection. Settings for automatic client reconnection override similar settings configured in Microsoft Windows Group Policy.
   - **Reconnect automatically** (default setting). Select this option if you do not want users to resupply credentials. Selecting this option also allows reconnection attempts to be logged.
5. If you selected **Reconnect automatically** in Step 4, select **Log automatic reconnection attempts** to record information about successful and failed automatic reconnection events to each server's system log.
6. Click **Apply** to implement your changes and then **OK** to close the **Farm Properties** dialog box.

## To configure an Auto Client Reconnect setting for a server

1. Select the server in the left pane.
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.
3. From the **Properties** list, select **ICA** > **Auto Client Reconnect**.
4. Choose one of the following options:
   - **Use farm settings**. Select this option if you want the server to use the default farm settings.
   - **Require user authentication**. Select this option if you want users to be prompted for new credentials during automatic reconnection to an ICA session. Do not select this option if you want users to be reauthenticated automatically during reconnection. Settings for automatic client reconnection override similar settings configured in Microsoft Windows Group Policy.

- **Reconnect automatically** (default setting). Select this option if you do not want users to resupply credentials. Selecting this option also allows reconnection attempts to be logged.

5. If you selected **Reconnect automatically** in Step 4, select **Log automatic reconnection attempts** to record information about successful and failed automatic reconnection events to each server's system log.
6. Click **Apply** to implement your changes and then **OK** to close the **Server Properties** dialog box.

# Restarting Servers at Scheduled Times

To optimize performance, you can restart a server automatically at specified intervals by creating a restart schedule.

Restart schedules are based on the local time for each server to which they apply. This means that if you apply a schedule to servers that are located in more than one time zone, the restarts do not happen simultaneously; each server is restarted at the selected time in its own time zone.

When the Citrix Independent Management Architecture service starts after a restart, it establishes a connection to the data store and updates the local host cache. This update can vary from a few hundred kilobytes of data to several megabytes of data, depending on the size and configuration of the server farm.

To reduce the load on the data store and to reduce the IMA service start time, Citrix recommends maintaining restart groups of no more than 100 servers. In large server farms with hundreds of servers, or when the database hardware is not sufficient, restart servers in groups of approximately 50, with at least 10 minute intervals between groups.

## To define when multiple servers restart

1. In the left pane of the Access Management Console, select the **Servers** folder.
2. In the **Contents** display in the right pane, press the SHIFT key and select the servers to restart.
3. From the **Action** menu, select **All Tasks > Set restart options > Set restart schedule**. This starts the Set Restart Schedule wizard.
4. Use the wizard to configure your restart options.

## To define when a single server restarts

1. In the left pane of the Access Management Console, select a server.

2. From the **Action** menu, select **All Tasks** > **Modify server properties** > **Modify all properties**.
3. In the **Server Properties** dialog box, select **Restart Schedule** and configure your restart options.

### To stop restarts for a server

1. Select the servers you do not want to restart.
2. In the center pane of the Access Management Console, select **Other Tasks > Set restart options > Disable restarts**.

## To repair a XenApp installation

When you run the repair utility, XenApp overwrites all files and settings with those from the original installation. If you customized any of the files or features in your XenApp installation, running the repair utility replaces your customizations with the original files and settings.

1. Log off from all sessions and exit any applications running on the server.
2. Choose **Start > Control Panel > Programs and Features**.
3. Select **Citrix XenApp**, click **Change**, and then select **Repair** when asked to select the maintenance action you want to perform.
4. Restart the server when prompted.

## Changing XenApp Farm Membership

To change the farm to which a XenApp server belongs, use the **chfarm** command utility. You can run **chfarm** from %Program Files%\Citrix\system32\citrix\IMA, the installation media, or a network image of the media.

When you run **chfarm**, the following events occur:

- The server you specify is removed from the farm
- The IMA service stops
- The data store is configured
- The IMA server restarts

Related topics:

“CHFARM” on page 358

## To move a XenApp server to a new server farm using SQL Server Express

1. Create a named instance of SQL Server Express by installing it on the first server in the new farm. You can do this by performing the following steps:
   A. Open a text editor such as Notepad and modify the the *instance_name* parameter of the SetupSQLExpressForCPS.cmd file.
   B. Run SetupSQLExpressForCPS.cmd.
2. Run **chfarm** on the server that you want to use to create the new farm using the **/instancename:***iname* option, where *iname* is the name of the instance of SQL Server Express you created in Step 1.

---

**Note:** If you name an instance of SQL Server Express "CITRIX_METAFRAME," you do not need to use the **/instancename** option.

---

# Removing and Reinstalling XenApp

At times, you might have to remove servers from your farm or uninstall XenApp software from a server. Some tasks you might need to perform include:

- Moving a server to another farm
- Renaming a server
- Removing a server from your farm
- Uninstalling XenApp from a computer in your farm or need to force its uninstallation
- Removing a server from your farm if the hardware hosting XenApp fails

To accomplish these tasks, you might need to uninstall XenApp from its host computer, remove it from the farm or from the list of farm servers in the Access Management Console, or both depending on your situation.

**Moving a Server to a Different Farm**

If you want to *move* a XenApp server to another farm, use the Change Farm (CHFARM) command. This removes the server from the farm data store and from the lists of servers displayed in the management consoles.

### Renaming a Server

Follow the instructions in "To rename a XenApp server" on page 306 to rename a server. They contain critical steps to ensure records are not corrupted in the data store.

### Uninstalling XenApp

Citrix recommends that you uninstall XenApp by using Control Panel > Programs and Features while the server is still connected to the farm and the network. This method removes the host information from the farm data store and removes the server from the farm properties displayed in the management tools.

When uninstalling servers that connect to the data store indirectly through another farm server, uninstall the indirectly connected servers before uninstalling the directly connected server. Uninstalling the direct server first prevents the other servers from being uninstalled properly from the data store.

Citrix does not recommend uninstalling XenApp from within a Remote Desktop Connection (RDC) session because the uninstall program needs to log off all remote users as it uninstalls XenApp. If you need to uninstall XenApp remotely, you can do so using tools such as Microsoft Configuration Manager 2007 (formerly Systems Management Server (SMS)).

### Removing a Server from a Farm

If you want to remove a server from a farm, Citrix recommends that you uninstall XenApp. Then, check the server was successfully removed from the farm using the Access Management Console and reimage it, if desired. While you can remove the server from the farm using only the Access Management Console, Citrix strongly recommends using the method explained in "To remove a server from the farm" on page 305 since it is safer.

### Forcing the Uninstall of XenApp

If you cannot uninstall XenApp through the Control Panel, you can *force* the removal of the software by using the Windows Msiexec command.

### Removing a Server from a Farm Due to Hardware Failure

If the hardware for a server fails or it cannot be brought up to run the uninstall program, remove the server using the Access Management Console. Citrix recommends that you only use the Access Management Console to remove a server from the farm in cases where the server cannot be brought up to run the uninstall program.

---

**Caution:** If you remove all servers belonging to a single domain and have Citrix administrators in the domain, their user accounts cannot be enumerated by the console and appear as a question mark (?) in the list of Citrix administrators.

---

### Reinstalling XenApp Due to Hardware Failure

If the hardware for a server fails, before you connect its replacement server to your network, change its name to the same name as the failed server. Assigning the replacement server the failed server's name lets the replacement have the same properties and functionality as the failed XenApp server. The records in the data store for the old server apply to its replacement of the same name.

When you assign a replacement server the failed server's name, make sure the settings on the replacement server are identical to the failed server. This includes settings for the operating system, settings for applications made during installation or when the application was published, and any user accounts on the failed server.

### Backing Up and Restoring the XenApp Data Store

Many data store maintenance tasks, such as backing up and restoring the data store, are performed using the DSMAINT and DSCHECK commands. Some data store maintenances tasks have different instructions according to the type of database (for example, Microsoft Access). The data store maintenance instructions are in the *Citrix XenApp Installation Guide*.

---

**Note:** If the server that failed was hosting an indirect data store, create a new data store. If the new server hosting the data store has a different name than the failed server, run the CHFARM command on each server in the farm so they reference the new data store.

---

Related topics:

"CHFARM" on page 358

"DSMAINT" on page 365

"DSCHECK" on page 364

# To uninstall XenApp

For illustration purposes, this procedure assumes that you installed XenApp with all options enabled.

---

**Caution:** If you are uninstalling XenApp remotely, do not do so from within a Remote Desktop Connection (RDC) session. Using RDC to host a remote uninstall can result in you being unexpectedly disconnected from the computer with no way to reconnect or complete the uninstall.

---

1. Log off from all sessions and exit any applications running on the server.

2. Choose **Start > Control Panel > Programs and Features**.
3. Select **Citrix XenApp**, click **Uninstall**, click **Yes** when asked if you want to uninstall XenApp, and follow the instructions that appear.
4. Uninstall XenApp. If you want to uninstall only specific components of XenApp, do so in the following order:
   - Citrix Access Management Console
   - XenApp Advanced Configuration
   - Citrix XenApp
   - Citrix Web Interface
   - Citrix Licensing

**Note:** To complete the uninstall, you must restart the computer after you remove XenApp.

## To force the uninstallation of XenApp

1. If you need to force the uninstallation of XenApp from a computer, you can use msiexec on a command line to add the property:

   `CTX_MF_FORCE_SUBSYSTEM_UNINSTALL`

   Set its value to **Yes**
2. The following sample command line enables logging of the uninstallation operation and forces the removal of XenApp:

   ```
   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.

## To remove a server from the farm

1. With the server still on the network and online in the farm, uninstall XenApp from the server from Control Panel > Programs and Features by selecting Citrix XenApp 5.0 and selecting **Uninstall**.
2. Open the Access Management Console on a different server, run or rerun Discovery and check the server was removed from the farm successfully.

   If the server from which you uninstalled XenApp still appears in the Access Management Console, do the following:

   A. In the left pane of the Access Management Console, select the server.

B. From the **Action** menu, select **All Tasks** > **Remove from farm**.

3. After you ensure the server no longer appears in the farm in the Access Management Console, disconnect the server from the network.

---

**Caution:** Do not reconnect the server to the network until you reimage it or remove its XenApp software. If it reconnects to the network, it can corrupt your farm.

---

4. Run the **dscheck** command on the data store to repair any consistency errors.
5. Perform a new installation of operating system (that is, a "clean" installation and not an upgrade) and XenApp 5.0 (if you want to reuse the hardware for that server).

---

**Note:** You cannot remove a server from a farm in the Access Management Console unless you have uninstalled XenApp from the server or the server is offline.

---

# To rename a XenApp 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.

---

1. Create a Citrix local administrator account on the server you want to rename.
2. On the server you want to rename, run **chglogon /disable** to prevent users from logging into the server.
3. Open the Access Management Console on a different server, remove the server to be renamed from published applications assigned to that server.
4. On the server you want to rename, stop the Citrix Independent Management Architecture service.
5. In the Registry, set the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\IMA\RUNTIME\PSRequired registry value to 1. This value is HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\RUNTIME\PSRequired on XenApp, 32-bit Edition.

**Caution:** Not changing the PSRequired registry value to 1 can result in incomplete records in the data store. Changing this value to 1 forces the Citrix Independent Management Architecture service to communicate with the data store and create a record for the newly named server.

The value for PSRequired reverts to 0 the next time the Citrix Independent Management Architecture service restarts.

6. Change the name of the server in the server operating system and restart the server.
7. Log on to Access Management Console using the local administrator account you created.
8. Update all references to the old server to the new server name. This might require logging on to the XenApp Advanced Configuration tool as well.

**Important:** Before removing the old server name, change all objects that reference the old name to the new server name, including data collector ranking, published application references, load evaluators, and zone settings.

9. Expand the Servers folder and remove the old server name from the Access Management Console's list of servers.
10. Add the new server name to the list of configured servers for published applications.

# Monitoring Server Performance with Health Monitoring & Recovery

Health Monitoring & Recovery is a feature that is available with the Enterprise and Platinum Editions of XenApp. You can use this 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 10 tests; you have the option of importing additional tests, including custom tests that you develop. The 10 tests included with XenApp allow you to monitor several services and activities including Terminal Services, XML Service, Citrix IMA Service, and logon/logoff cycles. These tests are:

**Note:** You can update the default names of these tests. Therefore, within your organization, the tests might have different names from those specified in this topic.

- **Terminal Services test.** This test enumerates the list of sessions running on the server and the session user information, such as user name.
- **XML Service test.** This test requests a ticket from the 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 or possibly an application failure. 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. |

- **Check DNS test.** This test performs a forward DNS lookup using the local host name to query the local DNS server in the computer's environment for the computer's IP address. A failure occurs if the returned IP address does not match the IP address that is registered locally. To perform reverse DNS lookups in addition to forward DNS lookups, use the flag **/rl** when running this test.
- **Check Local Host Cache test.** This test ensures the data stored in the XenApp server's local host cache is not corrupted and that there are no duplicate entries. Because this test can be CPU-intensive, use a 24-hour test interval (86,400 seconds) and keep the default test threshold and time-out values.

Before running this test, ensure the permissions of the files and registry keys that the test accesses are set properly. To do this, run the **LHCTestACLsUtil.exe** file located in C:\Program Files (x86)\Citrix\System32 of the XenApp server. To run this utility, you must have local administrator privileges.

- **Check XML Threads test.** This test inspects the threshold of the current number of worker threads running in the Citrix XML Service. When running this test, use a single integer parameter to set the maximum allowable threshold value. The test compares the current value on the XenApp server with the input value. A failure occurs if the current value is greater than the input value.
- **Citrix Print Manager Service test.** This test enumerates session printers to determine the health of the Citrix Print Manager service. A failure occurs if the test cannot enumerate session printers.
- **Microsoft Print Spooler Service test.** This test enumerates printer drivers, printer processors, and printers to determine whether or not the Print Spooler Service in Windows Server 2008 is healthy and ready for use.
- **ICA Listener test.** This test determines whether or not the XenApp server is able to accept ICA connections. The test detects the default ICA port of the server, connects to the port, and sends test data in anticipation of a response. The test is successful when the server responds to the test with the correct data.

---

**Note:** Through the Health Monitoring & Recovery page of the **Farm Properties** and **Server Properties** dialog boxes, you can configure the feature to allow additional tests to run on your servers.

---

Use the load balancing feature of XenApp 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 and using Load Manager, see the *Load Manager Administrator's Guide*.

Related topics:

"Adding Health Monitoring & Recovery Tests" on page 312

# Enabling and Disabling Health Monitoring & Recovery

By default, Health Monitoring & Recovery is enabled on all of the servers in your farm, and the four tests that are included run on all servers, 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.

## To disable Health Monitoring & Recovery on all servers in a farm

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties > Modify all properies**.
3. In the **Farm Properties** dialog box, from the **Properties** list, select the **Server Default** > **Health Monitoring & Recovery**.
4. Clear the **Run health check tests on all servers in the farm** check box.

## To disable Health Monitoring & Recovery on a particular server

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **Modify server properties > Modify all properties**.
3. In the **Server Properties** dialog box. from the **Properties** list, select **Health Monitoring & Recovery**.
4. Clear the **Use farm settings** and **Run Health Monitoring tests on this Server** check boxes.

# Modifying Health Monitoring & Recovery Test Settings

The Health Monitoring & Recovery tests included with XenApp are configured with default settings. You can modify the settings for each test by server or across all servers in a farm through the Health Monitoring & Recovery page of the **Server Properties** or **Farm Properties** dialog box in the Access Management Console.

## Selecting Recovery Actions

When modifying the tests, you have the opportunity to choose whatever action you want XenApp to take if a test fails. Separate recovery actions can be taken for each test. The recover actions are:

- **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.

  **Note:** To restore one or more servers to load balancing, use the **enablelb** command-line utility.

- **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 is triggered before the server is restarted. After the system is restarted, the tests resumes.

**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. Although you 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.

Related topics:

“ENABLELB” on page 370

## To modify the settings of Health Monitoring & Recovery tests for a farm

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties > Modify all properties**.

3. From the **Properties** list, select **Server Default > Health Monitoring & Recovery**.
4. Select a test and click **Modify**.
5. Make the necessary modifications and click **OK**.

### To modify the settings of Health Monitoring & Recovery tests for a server

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **Modify server properties > Modify all properties**.
3. From the **Properties** list, select **Health Monitoring & Recovery**.
4. Clear the **Use farm settings** check box and ensure **Run Health Monitoring tests on this server** is selected.
5. To copy existing tests from the farm to the server, click **Copy From Farm**.
6. Select a test and click **Modify**.
7. Make the necessary modifications and click **OK**.

## Adding Health Monitoring & Recovery Tests

You can add two types of Health Monitoring & Recovery tests to your servers: tests supplied by Citrix through the Citrix Knowledge Center and custom tests developed by your organization or third parties.

### Storing Health Monitoring & Recovery Tests

Citrix recommends that you store all tests in the following location:

%Program Files%\Citrix\HealthMon\Tests\

where %Program Files% is the location in which you installed XenApp. Store Citrix-supplied tests in the Citrix folder and custom tests in the Custom folder.

---

**Note:** For information about custom tests, see "Developing Custom Health Monitoring & Recovery Tests" on page 313.

---

### To add tests to a farm

1. In the left pane of the Access Management Console, select a farm.
2. From the **Action** menu, select **Modify farm properties > Modify all properties**.
3. From the **Properties** list, select **Server Default > Health Monitoring & Recovery**.

4. Click **New**.
5. In the **New Health Monitoring & Recovery Test** dialog box, select the **Allow running custom Health Monitoring tests** check box.

   This setting is disabled by default. By selecting this check box, you can import a test by typing or navigating to the appropriate file path in the **Test file** field.

### To add tests to a server

1. In the left pane of the Access Management Console, select a server.
2. From the **Action** menu, select **Modify server properties > Modify all properties**.
3. From the **Properties** list, select **Health Monitoring & Recovery**.
4. Clear the **Use farm settings** check box and ensure **Run Health Monitoring tests on this server** is selected.
5. Click **New**.
6. In the **New Health Monitoring & Recovery Test** dialog box, select the **Allow running custom Health Monitoring tests** check box.

   This setting is disabled by default. By selecting this check box, you can import a test by typing or navigating to the appropriate file path in the **Test file** field.

## Developing Custom Health Monitoring & Recovery 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. This SDK includes a Readme file and white papers that contain information required 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 is available for download from the Citrix Knowledge Center.

Related topics:

“Adding Health Monitoring & Recovery Tests” on page 312

## Getting Health Monitoring & Recovery 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, 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.

---

**Note:** In the Advanced Edition of XenApp, 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.

Related topics:

"Modifying Health Monitoring & Recovery Test Settings" on page 310

# Using Citrix Performance Monitoring Counters

Performance monitoring counters for ICA data are installed with XenApp 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 XenApp
- Bandwidth counters for individual virtual channels within an ICA session
- Latency counters for ICA sessions

Related topics:

"Performance Counters Reference" on page 387

## To access ICA performance counters

1. Select **Start > Administrative Tools > Server Manager**.

2. In the Tree view, Select **Diagnostics > Reliability and Performance > Monitoring Tools > Performance Monitor**.
3. Click **Add**.
4. In the **Add Counters** dialog box, from the **Select counters from computer** drop-down list, ensure **Local computer** is selected.
5. In the **Avaliable counters** list, select **ICA Session**.
6. **To add all ICA counters:** In the **Avaliable counters** list, select **ICA Session**.

   **To add one or more ICA counters:** Click the plus sign next to **ICA Session** and select the individual counters to be added.
7. Select **All instances** to enable all instances of the selected ICA counters, **No instance**, or **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 see no performance data for that session until shadowing is terminated.
8. 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.

# Enabling SNMP Monitoring

The XenApp Platinum and Enterprise Editions support Simple Network Management Protocol (SNMP) monitoring and integration with third-party SNMP network management products. Using third-party applications, you can perform the following tasks remotely on XenApp servers:

- Monitor server status
- Terminate processes on servers
- Disconnect, log off, or send a message to an active session on a server

- Query operating system, process, and session information

This topic describes how to enable and configure SNMP monitoring on XenApp servers. For information about support and use of integrated third-party SNMP network management products, contact the product vendor.

Enabling SNMP monitoring comprises the following steps:

- Installing and configuring the Microsoft SNMP Service on the XenApp servers.
- From the Access Management Console, enabling the Citrix SNMP agent on the XenApp servers and enabling/disabling traps to be reported. You can enable the SNMP agent for all servers in the farm or for individual servers.

# Installing and Configuring the Microsoft SNMP Service

The Microsoft SNMP Service is included with Windows but is not installed by default.

To determine if the Microsoft SNMP Service is installed, click **Start > Administrative Tools > Server Manager,** then click **Features**. If SNMP is not listed, you must install the service.

## To install the Microsoft SNMP Services

1. Click **Start > Administrative Tools > Server Manager**.
2. Click **Features**.
3. Click **Add Features**.
4. In the Add Features Wizard, on the **Select Features** page, select **SNMP Services** (SNMP Services includes the SNMP Service and SNMP WMI Provider).
5. Follow the on-screen instructions to complete the installation.
6. Restart the computer and reinstall any service packs.

# SNMP Security Considerations

Generally, the third-party SNMP network management product administrator provides the community names to the Citrix administrator. The XenApp servers must have at least one community name in common with the computer running the SNMP network management product.

If an SNMP community on the XenApp server is configured with Read/Write permissions and the SNMP agent is enabled, users can perform potentially dangerous actions remotely (such as logging off or disconnecting a user, terminating a process, or sending a message).

To prevent unauthorized users from performing these actions, you can configure the SNMP Service to accept SNMP packets only from computers running the SNMP network management product by adding the DNS name or IP address of that computer to the list of hosts from which to accept packets.

If you have a firewall, you can prevent spoofing by configuring the firewall to block packets coming from outside the firewall that contain source IP addresses known to be inside the firewall.

Alternatively, you can disable these features completely by removing Read/Write permissions from all SNMP communities on all computers.

The Access Management Console uses Windows domain-based user authentication and is a secure method of allowing access to these actions.

See the Windows documentation for details about SNMP community security properties.

### To display or change the SNMP security properties

1. Click **Start > Administrative Tools > Server Manager**.
2. Click **Configuration > Services**.
3. Double-click **SNMP Service**.

   The **SNMP Service Properties** dialog box appears.
4. In the **SNMP Service Properties** dialog box, revise the properties as needed.
5. Click **OK**.
6. If you changed any SNMP security settings, stop and restart the SNMP Service.

## Enabling the Citrix SNMP Agent and Configuring Trap Settings

By default, the Citrix SNMP agent is not enabled on XenApp servers. You can enable the SNMP agent and configure trap settings for all servers in the farm or for individual servers.

The following table lists the supported traps.

| Check box on configuration page | Name<br>OID.trap number | Server action that triggers trap |
|---|---|---|
| - | trapMfAgentUp<br>1.3.6.1.4.1.3845.3.1.1.8 | SNMP agent starts |
| Logon | trapSessionLogon<br>1.3.6.1.4.1.3845.3.1.1.2 | User logs on |
| Logoff | trapSessionLogoff<br>1.3.6.1.4.1.3845.3.1.1.1 | User logs off |
| Disconnect | trapSessionDisconnect<br>1.3.6.1.4.1.3845.3.1.1.2 | User disconnects |
| Session limit per server | trapSessionLimitThreshold<br>1.3.6.1.4.1.3845.3.1.1.4 | Number of concurrent sessions on the server exceeds the configured session limit |
| Session limit per server | trapSessionThresholdNormal<br>1.3.6.1.4.1.3845.3.1.1.9 | Number of concurrent sessions falls below the configured session limit |

## To enable the SNMP agent and configure trap settings on all servers in a farm

1. From the Access Management Console, select the farm node in the XenApp node in the console tree.
2. From the **Action** menu, choose **Modify farm properties > Modify all properties**.
3. From the Properties tree, click **SNMP**.
4. Select the **Send session traps to selected SNMP agent on all farm servers** check box.
5. Enable these traps as desired:
   - **Logon**
   - **Logoff**
   - **Disconnect**
   - **Session limit per server**

   If you enable **Session limit per server**, choose a value.
6. Click **OK**.

By default, the **Use farm settings** check box is selected in each server's properties.

### To enable the SNMP agent and configure trap settings on an individual server

1. From the Access Management Console, select the server in the Servers node in the console tree.
2. From the **Action** menu, choose **Modify server properties > Modify all properties**.
3. From the **Properties** tree, click **SNMP**.
4. Clear the **Use farm settings** check box.
5. Select the **Send session traps to selected SNMP agent on this server** check box.
6. Enable these traps as desired:
   - **Logon**
   - **Logoff**
   - **Disconnect**
   - **Session limit per server**

   If you enable **Session limit per server**, choose a value.
7. Click **OK**.

## Troubleshooting SNMP Monitoring

If a XenApp server does not appear as an icon in the IP Internet tree of the third-party SNMP network management product display, verify that the SNMP agent is enabled on the XenApp server, and that it is configured to send traps to the computer running the SNMP network management product.

## Monitoring Traps from SNMP Network Management Products

You may be able to use one or more of the following methods to monitor traps from the third-party SNMP network management product:

- **Monitoring the event browser.** An event browser may log all traps received by the SNMP network management product; a filter may be available to display traps specific to XenApp servers.
- **Using the Citrix TrapDialog monitor.** The Citrix TrapDialog monitor displays a pop-up message when a status-change trap is received.

- **Configuring notifications.** You may be able to configure monitoring and notification procedures such as sending an email or paging individuals when traps are received. You may also be able to customize descriptions saved to the event log.

See the documentation for the SNMP network management product for details.

## Using the Citrix Management Information Base

Although support for XenApp is integrated into a number of popular third-party SNMP network management products, the Citrix Management Information Base (MIB) can be used with other SNMP network management products.

If the SNMP network management product has a MIB browser utility, you must load the MIB file before you can use the utility to query or set SNMP trap values. The MetaFrame.mib file is located in the \NetworkManager\mibs directory of the XenApp media. See the documentation for the SNMP network management product for instructions about loading these files.

The SNMP agent returns strings in Unicode format for all MIB variables except serverFarmA and serverZoneA. Depending on your query, these variables can return strings in either Unicode or multibyte format. Your SNMP network management product may not be able to handle strings in Unicode format.

# Optimizing Server Performance

XenApp provides you with a number of ways to optimize the performance of the servers in your farm. This topic includes information about:

- Assigning Load Evaluators to servers and published applications
- Using Preferential Load Balancing
- Managing CPU usage
- Managing virtual memory usage
- Enhancing the performance of remote servers
- Working with the cache
- Updating license server settings

## Assigning Load Evaluators to Servers

You can assign load evaluators previously created using Load Manager in XenApp Advanced Configuration. See the *Citrix Load Manager Administrator's Guide* for more details about creating load evaluators.

### To assign a load evaluator to a server

1. In the left pane, select the server to which you want to assign a load evaluator.
2. From the **Action** menu, select **All Tasks** > **Assign load evaluator**.
3. From the **Load Evaluator** drop-down box, select either:
   - **Advanced**. Select this option to limit memory usage, CPU utilization, and page swaps on a server.
   - **Default**. Select this option to employ user session count as a load balancing criterion.

   **Note:** If you created any custom load evaluators, they are also available for selection here.
4. Click **OK**.

   The load evaluator you specified is applied to the server.

## Assigning a Load Evaluator to a Published Application

You can assign load evaluators to one or more applications simultaneously.

### To assign a load evaluator to a published application

1. In the left pane of the console, select the published application(s) to which you want to assign a load evaluator.
2. From the **Action** menu, select **All Tasks** > **Load manage application**.
3. Select one or more servers from the **Configured servers** list and click **Edit** to change the load evaluator.

   These application load evaluators are used in addition to any server load evaluators that are applied to the server running the application.
4. Click **OK** to confirm your changes in the **Assign Load Evaluator** dialog box.

**Note:** You can create custom load evaluators using Load Manager in XenApp Advanced Configuration. You can then apply them to servers running published applications using the XenApp plugin (Access Management Console).

Related topics:

"Assigning Load Evaluators to Servers" on page 320

# Using Preferential Load Balancing

**Note:** See the *Citrix XenApp Comparative Feature Matrix* at http://www.citrix.com/xenapp/comparativematrix for information about which XenApp editions support this feature.

Preferential Load Balancing assigns importance levels (Low, Normal, or High) to specific users and applications. For example, doctors and nurses in a hospital are specified as important users and MRI scans and X-rays are specified as important applications. These important users and applications with higher levels of service connect to their sessions more quickly and have more computing resources available to them. By default, a Normal level of service is assigned to all users and applications.

Preferential Load Balancing calculates importance levels based on the *Resource Allotment* for each session. The Resource Allotment is determined by the *importance levels* of both the session and the published application that the session is running.

To enable Preferential Load Balancing, use the Access Management Console to choose **CPU sharing based on Resource Allotments** on the **CPU Utilization Managment** page.

Set the application importance level when publishing the application and use XenApp Advanced Configuration to set the session importance policy level.

Related topics:

"Resource Allotment" on page 322

"To configure application importance" on page 60

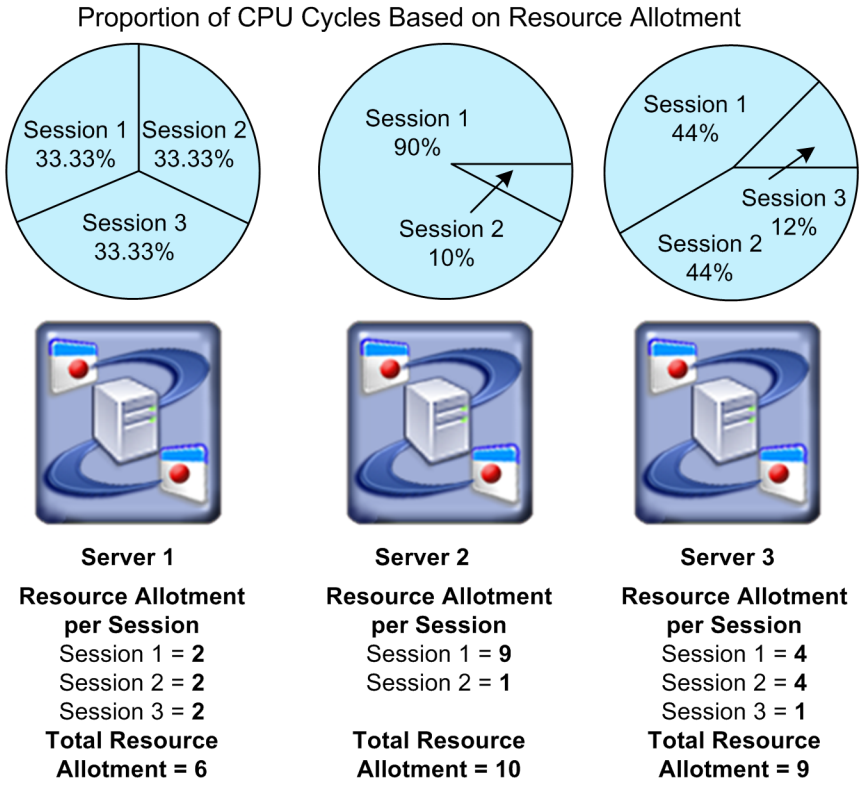
"Using CPU Utilization Management" on page 325

## Resource Allotment

Resource Allotment is calculated based on the published application importance level and the result of the XenApp policy engine for that session. The policy engine bases the session result on the session importance policy setting.

A session's Resource Allotment determines the level of service it experiences in comparison with other sessions on the same XenApp server, as well as sessions on other XenApp servers. The higher a session's Resource Allotment, the higher service it receives compared with those other sessions.

The figure illustrates a XenApp farm running sessions with different Resource Allotments. It illustrates how a session's Resource Allotment affects its competition with other sessions on the same server and on different servers. Session 1 on Server 2 has a relatively high Resource Allotment compared with all other sessions in the farm. As a result Session 1 gets the highest percentage of CPU cycles (90%) of any session running in the farm, and at the same time has to compete with fewer sessions on that server (there are only two sessions on Server 2, as opposed to three). Any new session would be assigned to Server 1 because it has the lowest Resource Allotment of the three servers.




*The session with the highest Resource Allotment gets the highest percentage of CPU cycles of any sessions running in the farm.*

The three application importance settings have Resource Allotment values associated with them, as do the three session importance policy settings. To determine the effective Resource Allotment associated with a session running the published application, multiply the application importance value by the session importance policy value. The most powerful session is one with a high importance policy setting (3) running a high importance application (3), with a total Resource Allotment of 9 (3x3). Conversely, the least powerful session is one with a low importance policy setting (1) running a low importance application (1), with a total Resource Allotment of 1 (1x1).

Use this table to help determine how to set your importance levels for applications and sessions.

| **Resource Allotments based on importance levels** | | |
|---|---|---|
| Application Importance | Session Importance (from policy) | Session Resource Allotment |
| Low (1) | Low (1) | 1 |
| Low (1) | Normal (2) | 2 |
| Low (1) | High (3) | 3 |
| Normal (2) | Low (1) | 2 |
| Normal (2) | Normal (2) | 4 |
| Normal (2) | High (3) | 6 |
| High (3) | Low (1) | 3 |
| High (3) | Normal (2) | 6 |
| High (3) | High (3) | 9 |

## Multiple Published Applications in the Same Session

Session sharing allows multiple published applications to run in the same session. During session sharing, the Resource Allotment is calculated based on the maximum application importance level setting of all the published applications running in the session multiplied by the session importance policy setting.

When an application is launched in an existing session, the importance level of the new application is compared with the maximum of all current application importance levels. If the importance level of the new application is greater, the session's Resource Allotment is recalculated and the session's CPU entitlement adjusted upwards. Similarly, when an application is closed, if the maximum importance level of the remaining applications is lower, the session's Resource Allotment is recalculated and the session's CPU entitlement adjusted downward.

# Using CPU Utilization Management

**Note:** See the *Citrix XenApp Comparative Feature Matrix* at http://www.citrix.com/xenapp/comparativematrix for information about which XenApp editions support this feature.

The CPU utilization management feature can improve the ability of a farm to manage resources and normalize CPU peaks when the farm's performance becomes limited by CPU-intensive operations.

In Windows, CPU resources are not divided equitably amongst users. By default, users running more processes get a larger percentage of a CPU's overall resources, provided those processes want to use the resource.

CPU utilization management shares processor resources equitably amongst users (*fair sharing*) and makes servers more responsive in periods with high processor loads. The effect of enabling the feature is that it can make applications respond faster than they would otherwise.

To determine if enabling CPU utilization management could be beneficial, check the CPU column and the Base Priority column in the Task Manager to see if there are processes from user sessions that consume inequitable amounts of CPU resources yet have the same priority.

You can set the CPU utilization management feature to either **Fair sharing of CPU between sessions** or **CPU sharing based on Resource Allotments**.

## Fair Sharing of CPU Between Sessions

The CPU utilization management **Fair sharing of CPU between sessions** option ensures that CPU resources are equitably shared among users by having the server allocate 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. This is accomplished by providing CPU reservation and CPU shares.

- CPU reservation is a percentage of your server's CPU resource that is available to a user. If all of a reserved allocation is not being used, other users or processes can use the available resource, as needed. Up to 20% of the work capability of a single CPU on a server is always set aside for the local system account:

  Default Local System Account CPU Reservation % = 20 / (*number of CPUs or CPU cores)*. For example, if System A has only one CPU, the local system account has a 20% reservation of the total CPU capability. If System B has two CPUs, the local system account has a 10% reservation of its total CPU capability. Reservations are available to the users who need them the most.

**Note:** If the feature is supported in your XenApp edition, Citrix recommends you use Preferential Load Balancing to allocate more CPU resources to one user over another, rather than setting CPU Shares and Reservations in the registry key associated with the CPU Utilization Management feature: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CTXCPU\Policy. If you set this registry key and enable Preferential Load Balancing, the values in this key are not used.

- CPU shares are percentages of the CPU time. By default, CPU utilization management allocates four shares for each user. If two users are logged on to a server and the local system account does not need any of the resources on the system, each user receives 50% of the CPU time. If there are four users, each user receives 25% of the CPU time.

**Important:** The minimum number of CPU shares that can be assigned to a single user is 1 and the maximum is 64. For CPU reservation, the total cannot exceed 99% of the computer's CPU capacity, where 100% represents the entire CPU resource on the computer. For example, if the local system has a 20% reservation, you can assign a reservation of 79% to a user, but not 80%.

Do not enable **Fair sharing of CPU** between sessions 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 require higher priority access to servers

### Managing Peak Utilization on Multiprocessor Servers

If you enable **Fair sharing of CPU** on a multiprocessor system and fair sharing does not occur, you might need to start the Citrix CPU Utilization Mgmt/CPU Rebalancer service.

On Windows Server 2008, there is one run queue for each CPU. To optimize cache reuse, on computers with two or more CPUs, processes tend to stay on the same run queue and, consequently, execute on the same CPU. However, on multiprocessor systems, a side effect of this behavior is that it can compromise the CPU utilization management's ability to align CPU usage with CPU entitlement.

To determine if fair sharing is occurring, check the CPU column in the Windows Task Manager to see if one or more processes is consuming one processor each.

The Citrix CPU Utilization Mgmt/CPU Rebalancer service is installed multiprocessor systems only. To use this service, start it manually. If you decide to use this service long-term, set it to **Automatic**.

Do not start the CPU rebalancer service simply because your server has multiple processors. If fair sharing is occurring, the CPU Rebalancer service can impact server performance.

---

**Note:** If throughput is more important than fair sharing, Citrix does not recommend starting the CPU rebalancer service.

---

## CPU Sharing Based on Resource Allotments

Choose **CPU sharing based on Resource Allotments** to enable Preferential Load Balancing, which determines CPU resource allotments for users based on their published application and session importance levels. Use Preferential Load Balancing when specific users and applications require higher levels of service.

Related topics:

"Using Preferential Load Balancing" on page 322

## 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 left pane of the Access Management Console, select the farm for which you want to enable CPU utilization management.
2. In the task pane under **Common Tasks**, select **Modify farm properties > Modify Memory/CPU properties**.
3. In the left pane of the **Farm Properties** dialog box, select **Memory/CPU > CPU Utilization Management**.
4. On the **CPU Utilization Management** page, make one of these choices to enable this setting for all of the servers in your farm:
   - Select **Fair sharing of CPU between sessions** to allocate an equal share of the CPU to each user
   - Select **CPU sharing based on Resource Allotments** to enable Preferential Load Balancing

### To enable or disable CPU utilization management for a server

1. In the left pane of the Access Management Console, select the server for which you want to enable CPU utilization management.

2. In the task pane under **Common Tasks**, select **Modify server properties > Modify Memory/CPU properties**.
3. In the left pane of the **Server Properties** dialog box, select **Memory/CPU > CPU Utilization Management**.
4. On the **CPU Utilization Management** page, clear the **Use farm settings** check box.
5. Select one of these choices to disable or enable this setting for this server.
    - Select **No CPU utilization management** to disable all CPU utilization management
    - Select **Fair sharing of CPU between sessions** to allocate an equal share of the CPU to each user
    - Select **CPU sharing based on Resource Allotments** to enable Preferential Load Balancing

# 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. XenApp 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 farm

1. In the left pane of the Access Management Console, select the farm for which you want to enable memory optimization.
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 > Memory Optimization**.
4. On the **Memory Optimization** page, select the appropriate check boxes.

### To enable memory optimization for a server

1. In the left 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 for when the servers can rebase DLLs.

## 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 left 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 **Farm-wide > Memory/CPU > Optimization Interval**.
4. In the **Optimization interval** area, specify when to run the optimization program to set 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 (daily is the default). If you choose to run the program weekly or monthly, specify the day of the week or month.

   **Note:** Citrix recommends that if you select **Day of month**, you do not enter a value higher than 28 in the text box. If you specify a higher value, memory optimization may not occur in some months.

5. Specify the startup time (3:00 by default) in the **Optimization time** box to set the time at which the server begins rebasing DLLs. The optimization time is specified using a 24-hour clock format.

   **Note:** If you selected to optimize at startup, this option is disabled.

6. In the **Memory optimization user** area, if you want the memory optimization program to run automatically using the local system account, select the **Use local system account** check box (enabled by default).
7. If you want to run the optimization program with a local or remote user account (for example, if you store application files on a file server or remote server that requires special access permissions, such as a domain administrator), clear the **Use local system account** check box and supply the valid user name and password of a domain or local administrator.

   **Note:** The user must have read-write permission to all the files that you want to be optimized.

8. Click **Apply** to implement your changes and then **OK** to close the **Farm Properties** dialog box.

## Excluding Applications from Memory Optimization

The following 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 exclude additional applications from memory optimization

1. In the left pane of the Access Management Console, select the farm on which you want to exclude additional applications from memory optimization.
2. From the **Action** menu, select **Modify farm properties > Modify all properties**.
3. In the **Farm Properties** dialog box, choose **Farm-wide > Memory/CPU > Exclude Applications**.

   The **Exclude Applications** page appears. This page lists the applications that memory optimization ignores. For example, some applications require a fixed DLL address. If an application was working but it stops working after enabling this feature, add the application to this list and see if the problem is resolved.
4. Click **Add**.

   The **Browse Files** dialog box listing all servers in the farm appears.
5. Navigate to the applications from each server that you would like memory optimization to ignore, clicking **OK** to add each executable to the Excl**ude Applications** page.
6. Click **Apply** to implement your changes and then **OK** to close the **Farm Properties** dialog box.

# Optimizing Simultaneous Logon Performance

You might see an improvement in simultaneous logon performance if you enable disk write caching on the server's RAID controller. The reason is the logon process is dependent on dynamic information and is handled by a data collector in the farm rather than being dependant on the data store.

# Managing Farm Infrastructure

All farms include infrastructure functions to support the servers hosting published applications. Whether you configure these functions on shared or stand-alone servers depends on your farm's size and requirements.

Farms comprise at least one *zone* or grouping of servers. Multiple zones are sometimes used to improve the performance on geographically segmented farms. Within the zone, there is a *data collector*, which contains information about other servers in the farm, and servers designated as backup data collectors. If the data store fails, each server on the farm also contains a backup of all data store information, known as the *local host cache*.

Citrix does not recommend publishing applications on infrastructure servers.

These topics contain information about data collectors, zones, and the local host cache:

- "Maintaining the Local Host Cache"
- "Data Collectors and Elections" on page 335
- "Enhancing the Performance of a Remote Group of Servers" on page 337

## Maintaining 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.

This topic comprises:

- Tuning Local Host Cache Synchronization
- Refreshing the Local Host Cache
- Recreating the Local Host Cache

## 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 by creating the following registry key on each server you want to adjust, with the value expressed in hexadecimal notation:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\IMA\
DCNChangePollingInterval (DWORD)

Value: 0x1B7740 (default 1,800,000 milliseconds)

---

**Note:** This registry key is HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\ DCNChangePollingInterval (DWORD) on XenApp, 32-bit Edition.

---

You must restart the IMA Service for this setting to take effect.

Most changes made through the Access Management Console or XenApp Advanced Configuration are written to the data store. When you open the Access Management Console or XenApp Advanced Configuration, it connects to a specified server. The Citrix Independent Management Architecture 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.

## 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. 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.

Related topics:

"DSMAINT" on page 365

## 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**. Running this command performs three actions:

- Sets the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\IMA\RUNTIME\PSRequired to 1. This key is HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IMA\RUNTIME\PSRequired to 1 on XenApp, 32-bit Edition.
- 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.

Related topics:

“DSMAINT” on page 365

# Data Collectors and Elections

A data collector is an in-memory database that maintains *dynamic information* about the servers in the zone, such as server loads, session status, published applications, users connected, and license usage.

Data collectors receive incremental data updates and queries from servers within their zone. Data collectors relay information to all other data collectors in the farm. The data collector tracks, for example, which applications are available and how many sessions are running on each server in the zone. The data collector communicates this information to the data store on behalf of the other servers in the farm. By default, in farms that communicate indirectly with the data store, the first server in the farm functions as the data collector.

Farms determine the data collector according to what level the election preference is set for a server. By default, all servers joining the farm are configured as backup data collectors. When the zone’s data collector fails, a data collector election occurs and a backup data collector replaces the failed data collector.

If the data collector fails, existing and incoming sessions connected to other servers in the farm are not affected. The data collector election process begins automatically and a new data collector is elected almost instantaneously. Data collector elections are not dependent on the data store.

**New Data Collector Election**

When communications fail between data collectors or between a server and its data collector, the process to choose or *elect* a new data collector begins. For example:

1. The data collector for Zone 1 has an unplanned failure. If the data collector shuts down correctly, it triggers the election process as it shuts down.
2. The servers in Zone 1 detect the data collector failed and start the election process. The server set to the next highest election preference is elected as the new data collector.
3. The member servers start sending their information to the new data collector for Zone 1.
4. The new Zone 1 data collector replicates this information to the other data collectors in the farm.

Sometimes, you might decide to have a dedicated data collector after your farm is in production. In general, if users experience slow connection times due to high CPU utilization on the data collector, consider dedicating a server to act solely as the zone data collector.

## Specifying Backup Data Collectors

When you create a server farm and whenever a new server joins a zone, a server is elected as the data collector for that zone. If the data collector for the zone becomes unavailable, a new data collector is elected for the zone based on a simple ranking of servers in the zone.

---

**Important:** A primary domain controller or backup domain controller must not become the data collector for a zone. This situation may arise if XenApp is installed on Windows domain controllers. Citrix does not recommend such installations.

---

### To set the data collector election preference of a server

1. In the left pane of XenApp Advanced Configuration, select the farm.
2. On the **Actions** menu, click **Properties**.
3. Select **Zones**.
4. In the list of zones and their servers, locate the server, select it, and click **Set Election Preference**.
5. Select the ranking for the server by choosing from the following election options:

---

**Important:** If you change the server name of the data collector, the new server name is added to the list of servers in the farm. The old server name is still listed as a member of your farm and must be removed using the Access Management Console. Before removing the old server name, you must update the data collector ranking for the new server name.

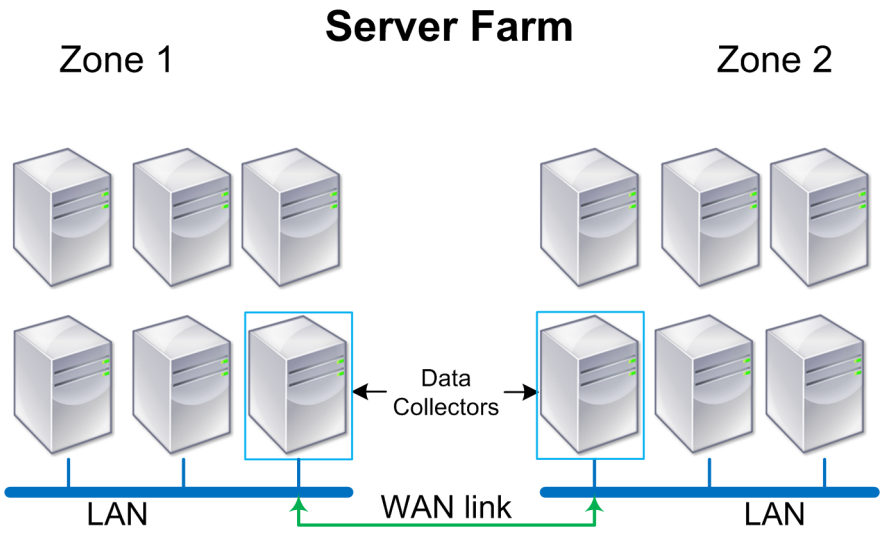
---

- **Most Preferred.** The server is always the first choice to become the data collector. It is recommended that only one server per zone be given this setting.
- **Preferred.** When electing a new data collector, XenApp elects the next collector from the Preferred servers if the Most Preferred server is not available.
- **Default Preference.** The default setting for all servers. The next collector is selected from the Default servers if neither a Most Preferred server nor a Preferred server is available.
- **Not Preferred.** Apply this setting to servers that you do not want to become the data collector for the zone. This setting means that this server becomes the data collector only when no servers are available

with any of the other three settings (Most Preferred, Preferred, Default Preference).

## Enhancing the Performance of a Remote Group of Servers

A zone is a configurable grouping of XenApp servers. All farms have at least one zone. All servers must belong to a zone. Unless otherwise specified during XenApp Setup, all servers in the farm belong to the same zone, which is named *Default Zone*.




*This illustration depicts a server farm with multiple zones. Each zone's data collector communicates with the other data collectors across the WAN link.*

In farms distributed across WANs, zones enhance performance by grouping geographically related servers together. Citrix does not recommend having more than one zone in a farm unless it has servers in geographically distributed sites. Zones are not necessary to divide large numbers of servers. There are 1000-server farms that have only one zone.

Zones have two purposes:

- Collect data from member servers in a hierarchical structure
- Efficiently distribute changes to all servers in the farm

Each zone contains a server designated as its data collector. Data collectors store information about the zone's servers and published applications. In farms with more than one zone, data collectors also act as communication gateways between zones.

Data collectors generate a lot of network traffic because they communicate with each other constantly:

- Each zone data collector has an open connection to all data collectors in the farm.
- During a zone update, member servers update the data collector with any requests and changed data.
- Data collectors relay changes to the other data collectors. Consequently, data collectors have the session information for all zones.

You can create zones during XenApp installation or after installation. This topic provides information about creating zones after Setup, moving servers between zones, and renaming zones. For design considerations for zones, including whether to zones for small groups of remote servers, see the *Citrix XenApp Installation Guide*.

For business continuity, you can specify that if all zone servers go offline, XenApp redirects user connections to a backup zone. This feature is known as *Zone Preference and Failover*; you configure it through the **User Workspace > Connections > Zone preference and failover** policy rule.

To minimize data exchanges among zones on WANs, and the ensuing network traffic, you should:

- Not configure zones to load balance across zones (share load information). By default, load balancing between zones is disabled.
- Direct requests for applications to the nearest geographic location by specifying a preferred zone connection order in the **User Workspace > Connections > Zone preference and failover** policy rule.
- Create a policy that applies to connections from a zone's location. Then, specify that zone as the Primary Group zone in the Zone preference and failover rule. This makes XenApp route incoming connection requests from users to the zone for their location first.

Zones are view-only in the Access Management Console. Use XenApp Advanced Configuration to configure zones.

## To configure zones in your farm

1. In the left pane of XenApp Advanced Configuration, select the farm.
2. On the **Actions** menu, click **Properties**.

3. Select **Zones**.

Change the configuration of the zones in your farm by selecting:

- The buttons provided.
- The **Only zone data collectors enumerate Program Neighborhood** check box to make your server farm more secure. When Program Neighborhood users browse for application sets, servers enumerate, or list, the published applications they are authorized to launch. When this option is not selected, any server in the farm can respond to client enumeration requests. For any server in the farm to enumerate users' applications, you must allow users to retain the Windows Group Policy right to log on locally to every server. When you select this option, a data collector is always used to specify which applications appear for a user in Program Neighborhood. You can then confine users' access to the servers that are or may become data collectors.

  Do not select this option if you want the fastest possible enumeration of applications to occur in Program Neighborhood and security is not a concern.

  ---

  **Important:** Servers running some earlier releases of XenApp in a mixed farm cannot access this farm setting to direct a connection for enumeration correctly. If users are directed to a server on which they are not permitted access, their applications cannot be enumerated and they will receive error messages. Citrix recommends that you maintain all servers in a farm at the same release level.

  ---

- The **Share load information across zones** check box to allow data collectors to exchange server load information across zones and ensure users are efficiently routed to the least loaded server in any zone. Enable this setting only if the following conditions are true:
  - The bandwidth capacity among zones is not limited, such as if the zones are in the same LAN
  - You are not implementing zone preference and failover policies

  Selecting this option can result in increased network traffic because every change in server load is communicated to all data collectors across all zones. Connection requests are routed to the least loaded server in the server farm, even a server located across a WAN, unless a preferred order is established using the Zone preference and failover policy rule. When you establish a preferred connection order, the zone data collectors query the preferred zones in the order you set.

### Creating New Zones

Use the **New Zone** dialog box to enter the name of the new zone.

Empty zones are not allowed. After you create a new zone, you must move one or more servers into the new zone before you click **OK** in Zones or exit Zones by making another selection in the left pane of the farm's **Properties** page.

### Renaming Zones

Use the **Rename Zone** dialog box to change the name of the zone you selected. Enter the new name of the zone in the text box provided.

If you change the server name of the data collector, the new server name is added to the list of servers in the farm. The old server name is still listed as a member of your farm and must be removed using the Access Management Console.

### Moving Servers Between Zones

Use the **Move Servers** dialog box to move the selected server to another zone. This button is available only when one or more servers is selected.

After you move one or more servers among zones, you must restart each server that was moved. This is required to update the data collector information for each zone.

### Removing Zones

Use the **Remove Zone** button to delete the selected zones. A zone cannot be removed until all the servers in the zone are moved to other zones.

# Updating Citrix License Server Settings

Use the **License Server** page in the farm's **Properties** dialog box to change the name of the license server or port number that the license server uses to communicate. You can apply the changes to either an individual server (on the **License Server** page of the server's **Properties** dialog box) or an entire farm and you can type the license server name or its IP address in the **Name** field.

License files are stored on a license server. XenApp servers must point to the license server. After you install XenApp, you can change the port number or license server name on the license server **Properties** dialog box for the farm or an individual server.

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 server other 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** dialog box 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 white paper 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 white paper in the Citrix Knowledge Center.

## To specify a default license server for a farm

Use this method to specify a default license server for all servers in your farm.

1. In the left pane of the Access Management Console, select the farm.
2. From the **Action** menu, select **Modify farm properties** > **Modify license server properties**.
3. Modify one or more of the following values:

- **Name**. You can enter either a license server name or an IP address
- **Port number (default 27000)**. Enter the license server port number

---

**Note:** 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 white paper in the Citrix Knowledge Center.

---

4. Click **Apply** to implement your changes.

## To specify a license server for individual servers

Use this method to specify a license server for individual servers in your farm.

1. In the left pane of the Access Management Console, select the server.
2. From the **Action** menu, select **Modify server properties** > **Modify license server properties**.
3. Clear the **Use farm settings** check box (selected by default).
4. Specify the following information:
   - **Name**. Because license files are tied to the license server's host name, if you change the license server name, you must ensure that you 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. Additionally, before you change the server name, ensure that there is a license server with that name on your network. Note that you cannot leave the license server name blank.
   - **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 white paper in the Citrix Knowledge Base.

For information about general licensing topics, see the *Getting Started with Citrix Licensing Guide*.

# Setting the Product Edition

The product editions of XenApp support different features. To activate the features available with a particular edition installed on each server, set the edition of the product for each server.

The product edition also determines which type of license a server requests from the license server. Make sure the editions you set match the licenses you installed.

**Important:** To apply changes to the product edition, you must restart the servers.

## To set the product edition

1. In the left pane of the Access Management Console, select the required server.
2. From the **Action** menu, select **All Tasks** > **Set server edition**.
3. Select the required edition.

   **Important:** Do not select **Other** unless you are asked to do so by Citrix Technical Support.

# Setting the Citrix XML Service Port

The Citrix XML Service is used by clients connecting over the TCP/IP+HTTP protocol and the Web Interface.

During the installation of Citrix XenApp on your server, you configured the XML Service to either share the port with your Microsoft Internet Information Server or to use a particular port.

If you chose to have the XML Service share the port, this page displays a short message to this effect.

If you chose a particular port during installation, the **TCP/IP Port** field reflects your choice. Use this field to change the XML port number if necessary.

**Note:** The port option appears only if you entered a different port number than the default **Share with IIS** during the Web Interface installation. Use this option to change the port number.

If you do not trust XML requests, certain features of XenApp are not available. Trusting requests sent to the XML Service means:

- Users can move among client devices and reconnect to all of their applications. For example, you can use workspace control to assist health-

care workers in a hospital who need to move quickly among workstations and be able to pick up where they left off in published applications.

- Users can connect to the Web Interface using pass-through authentication or smart cards to reconnect to ICA sessions. These credentials are not passed from the server running the Web Interface to the servers on which the users access their applications. Users can reconnect to their ICA sessions even though their credentials are not passed when this option is selected.
- XenApp can use the information sent in those requests by Access Gateway (Version 4.0 or later). This information includes Access Gateway filters that can be used to control access to published applications and to set XenApp session policies. If you do not trust requests sent to the XML Service, this additional information is ignored.
- Others on the network can disconnect or terminate sessions without authentication. It can also allow clients to make false security assertions.

To avoid security risks, select **Trust requests sent to the XML Service** only under the following conditions:

- Some users connecting to their ICA sessions using the Web Interface are also using pass-through authentication or smart cards.
- The same users need to move from one client device to another and still be able to pick up where they left off in published applications.
- You implemented IPSec, firewalls, or any technology that ensures that only trusted services communicate with the XML Service.
- You are selecting this setting only on servers that are contacted by the Web Interface.
- You are restricting access to the XML Service to the servers running the Web Interface. When Internet Information Services (IIS) and the XML Service share a port, you can use IIS to restrict port access to include the IP addresses of servers running the Web Interface only.

See the administrator's guides for XenApp, the Web Interface, and Access Gateway (Version 4.0 or later) for more information.

## To configure the Citrix XML Service port for a server

1. Select the server in the left pane
2. From the **Action** menu, select **Modify server properties** > **Modify all properties**.

3. From the **Properties** list, select **XML Service**.
4. Select the **Trust requests sent to the XML Service** check box if you ensured that only trusted services communicate with the XML Service.
5. Click **Apply**.

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

**Note:** This setting takes effect only after the XML Service restarts.

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 /rnn
   ```

   where *nn* is the number of the port you want to use; for example, `ctxxmlss /r88` forces the Citrix XML Service to use TCP/IP port 88.
7. At a command prompt, stop the XML Service by typing:

   ```
   net stop ctxhttp
   ```

# 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 XenApp 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.

# Citrix XenApp Commands Reference

This reference describes Citrix XenApp 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 XenApp.

| Command | Description |
|---|---|
| **acrcfg** | Configure auto-reconnect settings. |
| **altaddr** | Specify server alternate IP address. |
| **app** | Run application execution shell. |
| **auditlog** | Generate server logon/logoff reports. |
| **change client** | Change client device mapping. |
| **chfarm** | Change the server farm membership of the server, create an additional farm, and configure a replacement data store. |
| **ctxkeytool** | Generate farm key for IMA encryption. |
| **ctxxmlss** | Change the Citrix XML Service port number. |
| **dscheck** | Validate the integrity of the server farm data store. |
| **dsmaint** | Maintain 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. |
| **migratetosqlexpress** | Migrate the server farm's data store from a Microsoft Access database to a SQL Server Express database. |
| **query** | View information about server farms, processes, ICA sessions, and users. |
| **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 | /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 XenApp.

### Options

**/query, /q**

Query current settings.

**/server**

The server to be viewed or modified by the other command-line options. The server specified by *servername* must be in the same server farm as the server on which the command is run. This option and the **/farm** option are mutually exclusive. The local server is the default if neither **/server** nor **/farm** is indicated.

**/farm**

The options on the command-line after **/farm** are applied to the entire server farm.

**/inherit:on | off**

To use the 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.

**/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 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 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 plugin'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 the icaclient.adm file or an ICA file only on the Citrix XenApp Plugin for Hosted Apps 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 plugin 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

To make changes, you must be a Citrix administrator with Windows administrator privileges.

# ALTADDR

Use **altaddr** to query and set the alternate (external) IP address for a server running Citrix XenApp. 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 Citrix Independent Management Architecture 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*

### Parameters

*scriptfilename*

The name of a script file containing app commands (see script commands below).

### Script Commands

**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.

### 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.

### 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.

# 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

To run **auditlog**, you must have Windows administrator privileges.

# 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 [{/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

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 XenApp. 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 XenApp. 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

The **chfarm** utility is used to change the farm membership of a server, configure replacement data stores, and create additional farms. The utility is installed in %ProgramFiles%\citrix\system32\citrix\IMA.

To run this utility, choose **Run** from the **Start** menu and then type **chfarm**.

---

**Caution:** Be sure that the XenApp Advanced Configuration tool and the Access Management Console are closed before you run the **chfarm** command. Running **chfarm** while these tools are open can result in loss of data and functionality.

---

### Syntax for creating a new farm with an Access database

**chfarm** [**/verbose**] [**/createfarm**] [**/farmname:***name*]
[[**/admin:**[*domain*\]*username* [**/zone:***zonename*]]

### Syntax for creating a new farm with a SQL Server Express database

**chfarm** [**/verbose**] [**/createfarm**] [**/farmname:***name*]
[[**/admin:**[*domain*\]*username* [**/zone:***zonename*]] [**/instancename:***iname*]
[**/database:***dname*]

### Syntax for joining an existing farm with a direct connection to SQL, DB2, or Oracle databases

**chfarm** [**/verbose**] [**/joinfarm**] [**/ddsc:***databasetype*] [**/zone:***zonename*]
[**/odbcuser:***username*] [**/odbcpwd:***password*]
[**/dsnfile:***path_and_dsnname*] [**/quiet**]

### Syntax for joining an existing farm with an indirect connection to Access or SQL Server Express databases

**chfarm** [**/verbose**] [**/joinfarm**] [**/ldsc:***servername*] [**/zone:***zonename*]
[**/user:**[*domain*\]*username*] [**/pwd:***password*] [**/quiet**]

### Options

**/admin**:*[domain\]username*

Specifies the initial Citrix administrator account you want to use for the farm. The *domain*\ parameter is optional.

**/createfarm**

Initiates the farm creation process.

**/database**:*dname*

Specifies the name of the SQL Server Express database you want to use. The default value is MF20.

**/ddsc**:*databasetype*

Specifies the type of database used for the data store of the target farm. For example, SQL Server,

**/dsnfile**:*path_and_dsnname*

Specifies the complete path and filename of the database's file DSN.

**/farmname**:*name*

Specifies the name of the XenApp farm you want to create.

**/instancename**:*iname*

Specifies the name of the instance of SQL Server Express you want to use. The default value is CITRIX_METAFRAME.

**/joinfarm**

Initiates the join process for the farm.

**/ldsc**:*servername*

Specifies the name of the server whose farm you want to join.

**/odbcpwd**:*password*

Specifies the password for the SQL, DB2, or Oracle database connection.

**/odbcuser**:*username*

Specifies the username for the SQL, DB2, or Oracle database connection.

**/pwd**:*password*

Specifies the password for connecting to the target server.

**/quiet**

Supresses display of confirmation messages.

**/user**:*[domain\]username*

Specifies the user account needed to connect to the target server. The *domain* parameter is optional.

**/verbose**

Displays extra debugging information about the actions being performed. You can also redirect this output to a file.

**/zone**:*zonename*

The zone where you want to create or connect to the Access or SQL Server Express database.

### Remarks

**chfarm** has much of the same functionality as XenApp Setup. You can use **chfarm** when you want to move a server from its current server farm to an existing server farm or create a new server farm at the same time that you move the server.

If you did not back up your farm's data store and you need to recreate it (for example, in the event of hardware failure), running **chfarm** performs the same data store configuration tasks as XenApp Setup. You can also run the **chfarm** utility with additional command-line options to create a new farm or join an existing farm.

Citrix recommends that you back up your data store before running **chfarm**. **Chfarm** stops the Citrix Independent Management Architecture service on the server.

---

**Caution:** If **chfarm** reports any errors, continuing the process can corrupt the data store. If you cancel the data store configuration part of the Citrix XenApp Setup wizard, the server you are switching rejoins the original farm.

---

Do not remove the server hosting the data store from the farm unless all other servers are removed first. Doing so renders the farm unstable.

After the farm membership is changed or a new farm is created, restart the server.

When you run **chfarm**, the batch file JOINFARM.BAT is created in the same folder from which you run the utility. You can use this batch file to run **chfarm** with the same settings on other servers. Before using this file, you need to modify information according to the file comments; for example, passwords or the DSN file location.

### Limitations of using the command line to run CHFARM

If you choose to run the CHFARM utility from the command line instead of the Citrix XenApp Setup wizard, be aware of the following limitations:

- You can create new farms using only Access and SQL Server Express databases. You cannot create new farms using SQL Server, Oracle, or DB2 databases.
- You cannot generate or load registry keys in the HKLM\SOFTWARE\Wow6432Node\Citrix\IMA folder, or HKLM\SOFTWARE\Citrix\IMA folder on XenApp, 32-bit Edition.
- You cannot specify a license server. Instead, **chfarm** assumes the server will connect to the license server specified for the farm.
- You cannot specify a server port for an indirect connection to the farm data store. Instead, you must use port 2512.

### Important Notes for SQL Server Express Data Stores

If you want to use SQL Server Express 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 Express; you must install it separately. For more information, see "To move a server to a new server farm using SQL Server Express" on page 361.

---

**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 Express, you must either migrate to another database (Access or a third-party database) and then back to SQL Server Express, or install another named instance of SQL Server Express and then launch **chfarm** with the **/instancename** option.

---

# To move a server to a new server farm using SQL Server Express

1. Create a named instance of SQL Server Express by installing it on the first server in the new farm. You can do this by performing the following steps:

A. Open a text editor such as Notepad and modify the the *instance_name* parameter of the SetupSQLExpressForCPS.cmd file.

B. Run SetupSQLExpressForCPS.cmd.

2. Run **chfarm** on the server that you want to use to create the new farm using the **/instancename:***iname* option, where *iname* is the name of the instance of SQL Server Express you created in Step 1.

---

**Note:** If you name an instance of SQL Server Express "CITRIX_METAFRAME," you do not need to use the **/instancename** option.

---

# CTXKEYTOOL

Use **ctxkeytool** to enable and disable the IMA encryption feature and generate, load, replace, enable, disable, or back up farm key files.

### Syntax

```
ctxkeytool [generate | load | newkey | backup] filepath

ctxkeytool [enable | disable | query]
```

### Options

**generate**

Generates 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
- A new key onto a computer and the farm

**newkey**

Creates a new encryption key in the data store using the local farm key.

**backup**

Backs up the existing farm key to a file.

**enable**

Enables the IMA encryption feature for the farm.

**disable**

Disables the IMA encryption feature for the farm.

**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 has its 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.

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

You must be a Citrix administrator with local administrator privileges to run **ctxkeytool**.

# CTXXMLSS

Use **ctxxmlss** to change the Citrix XML Service port number.

### Syntax

```
ctxxmlss [/rnnn] [/u] [/knnn] [/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.

### Security Restrictions
None.

### Remarks
For more information, see the information about configuring the XML Service port in the *Citrix XenApp Installation Guide*.

# 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. **dscheck** is often used after running **dsmaint**.

### 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.

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 1 in HKLM\SOFTWARE\Wow6432Node\Citrix\IMA\RUNTIME, or HKLM\SOFTWARE\Citrix\IMA\RUNTIME on XenApp, 32-bit Edition.

**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 XenApp. 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.

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.

For data store reference information, see the *Citrix XenApp Installation Guide*.

### 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

Run the **dsmaint** on farm servers to perform XenApp data store maintenance tasks, including backing up the data store, migrating the data store to a new server, and compacting the XenApp data store or the Streaming Offline database. Not all **dsmaint** commands apply to all database types.

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** [**/user:***username*] [**/pwd:***password*] [**/dsn:***filename*]

**dsmaint backup** *destination_path*

**dsmaint failover** *direct_server* [**psserverport**=*portnumber*]

**dsmaint compactdb** [**/ds**] [**/lhc**]

```
dsmaint migrate [{/srcdsn:dsn1 /srcuser:user1 /srcpwd:pwd1}]
[{/dstdsn:dsn2 /dstuser:user2 /dstpwd:pwd2}]

dsmaint patchindex [/user:username] [/pwd:password] [/dsn:filename]

dsmaint publishsqlds {/user:username /pwd:password}

dsmaint recover

dsmaint recreatelhc

dsmaint recreaterade

dsmaint verifylhc [/autorepair]

dsmaint [/?]
```

### Parameters

*destination_path*

Path for the backup Microsoft Access data store. Do not use the same path as the original database.

*dsn1*

The name of the DSN file for the source data store.

*dsn2*

The name of of the DSN file for the destination data store.

*filename*

The name of the data store.

*direct_server*

The name of the new direct server for 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.

Enter the full path to the DSN file in quotation marks. For example,

```
C:\Program Files (x86)\Citrix\Independent Management
Architecture>dsmaint config /user:ABCnetwork\administrator
/pwd:Passw0rd101 /dsn:"C:\Program Files (x86)\Citrix\Independent
Management Architecture\mf20.dsn"
```

**/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 backup database file will be copied. This parameter cannot be used to back up Oracle or SQL data stores.

---

**Caution:** When running **dsmaint backup**, specifying the same path as the existing data store can damage it irreparably.

---

**failover**

Switches the server to use a new direct server for data store operations. Using **psserverport**, you can specify a port number when switching servers.

**compactdb**

Compacts the Access database file.

**/ds**

Specifies the database is to be compacted immediately. If the Citrix Independent Management Architecture service is running, this can be executed from the direct server or an indirect server. If the Citrix Independent Management Architecture service is not running, this can be executed only on the direct server.

**/lhc**

Compacts the local host cache on the server where this parameter is run. You might want to run **dsmaint /lhc** after your farm has been running for a long period of time as a maintenance task.

**migrate**

Migrates data from one data store database to another. Run this command on any XenApp server that has a direct connection to the data store. 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 a different type of database (for example, migrate from Access to Oracle).

To migrate the data store to a new server:

1. Prepare the new database server using the steps you did before running XenApp Setup for the first time.
2. Create a DSN file for this new database server on the server where you will be running **dsmaint migrate**.
3. Run **dsmaint migrate** on any server with a direct connection to the data store.
4. Run **dsmaint config** on each server in the farm to point it to the new 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.

**publishsqlds**

Publishes a SQL Server data store for replication.

**recover**

Restores an Access data store to its last known good state. This must be executed on the direct server while the Citrix Independent Management Architecture service is not running.

**recreatelhc**

Recreates the local host cache database. You might want to do this if prompted after running **dsmaint verifylhc**.

**recreaterade**

Recreates the Application Streaming offline database. You might want to do this as a troubleshooting step if the Citrix Independent Management Architecture service stops running and the local host cache is not corrupted.

**verifylhc**

Verifies the integrity of the 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. Alternatively, you can use **dsmaint recreatelhc** to recreate the local host cache.

**/?**

Displays the syntax and options for the utility.

### Remarks

After using **dsmaint**, Citrix recommends running **dscheck** to check the integrity of the data on the XenApp data store.

For data store reference information, see the *Citrix XenApp Installation Guide*.

**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 Citrix Independent Management Architecture 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 the "Data Store Database Reference" section of the *Citrix XenApp Installation Guide*.

---

**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.

**patchindex**

After running **dsmaint patchindex**, you must restart the Citrix Independent Management Architecture service on all servers.

**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 test, use **enablelb** to restore them to the load balance tables.

### Syntax

**enablelb** *servername* [*servername servername* …]

### Parameters

*servername*

The name of the computer running Citrix XenApp.

### 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 plugin that will connect to that server. For instructions for changing the port number on plugins, see the Administrator's Guide for the plugins 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 /port:5000
```

### Security Restrictions

Only Citrix administrators with Windows administrator privileges can run **icaport**.

# IMAPORT

Use **imaport** to query or change the IMA port.

**Important:** When you run Citrix XenApp Setup, Setup references port 2513 for communication with XenApp Advanced Configuration. If you change this port number on the first server in the farm on which you install Citrix XenApp, 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 XenApp Advanced Configuration 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 XenApp Advanced Configuration 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.

**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 XenApp installation media 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 Express 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 Express 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.

Related topics:

"Query Farm" on page 374

"Query Process" on page 376

"Query Session" on page 377

"Query Termserver" on page 378

"Query User" on page 379

# 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.

### Security Restrictions
You must be a Citrix administrator to 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.

### 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.

# TWCONFIG

Use **twconfig** to configure ICA display settings that affect graphics performance for plugins.

### 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

To run **twconfig** you must have Windows administrator privileges.

# Delegated Administration Tasks Reference

When you delegate tasks to custom Citrix administrators, you use the Access Management Console to associate custom Citrix administrator accounts with permissions to perform select tasks.

This topic includes descriptions of the tasks you can delegate to custom Citrix administrators.

Related topics:

"Delegating Tasks to Custom Administrators" on page 35

## Farm Folder Tasks

| Task | Description |
|---|---|
| Farm Management | Toggles on/off all subtasks. Allows full access to view and modify all areas of farm management. |
| Edit All Other Farm Settings | Allow 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 | Allow 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

| Task | Description |
|---|---|
| Administrators | Toggles on/off all subtasks. Allows administrators to open the XenApp Advanced Configuration Console and Web Interface Console and to view the properties of other administrators. |
| Edit centrally configured XenApp Web sites | Allow administrators to configure XenApp 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

| Task | Description |
|---|---|
| Published Applications | Toggles on/off all subtasks. Allows full access to view and edit properties for published applications in the specified folder. |
| Publish Applications and Edit Properties | Allows administrators to publish applications and edit their properties. |
| View Published Applications and Content | Allows administrators to view published applications and content. |
| Servers | Toggles on/off the Terminate Processes subtask. Allows full access to terminate processes on accessible servers. |
| 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. |
| 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. |

# Load Evaluator Folder Tasks

| Task | Description |
|---|---|
| Load Manager | Toggles on/off all subtasks. Allows full access to view and modify all areas of load management. |
| 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. |

# Policies Folder Tasks

| Task | Description |
|---|---|
| User Policies | Toggles on/off all subtasks. Allows full access to view and modify all areas of user policies. |
| 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

| Task | Description |
|---|---|
| Printers | Toggles on/off all subtasks. Allows full access to view and modify all areas of printer management. |
| 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 printer and printer drivers. |

# Servers Folder Tasks

| Task | Description |
|---|---|
| Published Applications | Allows full permissions for administering published applications on servers in the specified folder. |
| Assign Applications to Server | Allows administrators to publish applications from servers. To publish applications from a server, administrators must also have the "Publish Applications and Edit Properties" permission. |
| Servers | Toggles on/off all subtasks. Allows full access to view and modify all areas of server administration in the specified folder. |
| Edit License Server Settings | Allow 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. |
| 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 Reference

Performance monitoring counters that directly relate to the performance of ICA sessions, networking, and security are installed with Citrix XenApp. 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 XenApp-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.

Related topics:

"Using Citrix Performance Monitoring Counters" on page 314

## 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. |

| Counter | Description |
|---|---|
| CPU Reservation | The percentage of total computer CPU resource reserved for a user, should that user require it. |
| CPU Shares | The proportion of CPU resource assigned to a user. |
| 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 the XenApp 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 Enumeration/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. |
| Application Resolutions/sec | The number of resolutions completed per second. |
| DataStore Connection Failure | The number of minutes that the XenApp 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. |
| 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. |

| Counter | Description |
|---|---|
| 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 restarted. |
| Number of busy XML threads | The number of busy threads. |
| 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 XenApp 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. |
| 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. |

| Counter | Description |
|---|---|
| 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, measured in bps, used from client to server traffic on a virtual channel. |
| Latency - Last Recorded* | The last recorded latency measurement for the session. |
| 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. |

| Counter | Description |
|---|---|
| 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. |
| 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. |

| Counter | Description |
|---|---|
| Resource Shares | The total number of shares used by the session. |

# Secure Ticket Authority Counters

The following performance counters are available for the Secure Ticket Authority (STA).

| 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. |
| 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. |

# Policy Rules Reference

This is a reference topic for policy rules in XenApp. It provides:

- A quick reference table that you can use to solve problems or determine which rule you need to configure
- Details about how to configure each rule

To configure rules for a policy, right-click the policy name and select **Properties**.

Related topics:

"Creating Policies" on page 81

"Managing Policies" on page 89

## Policy Rules: Quick Reference Table

The following tables present rules you can configure within a policy. Find the task you want to perform in the left column, then locate its corresponding rule in the right column.

| **Bandwidth** | |
|---|---|
| **To limit bandwidth used for:** | **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<br>or<br>Session Limits (%) > Audio |

| **Bandwidth** | |
|---|---|
| **To limit bandwidth used for:** | **Use this policy rule:** |
| Devices connected to a local COM port | Session Limits > COM ports<br>or<br>Session Limits (%) > COM ports |
| Cut-and-paste using local clipboard | Session Limits > Clipboard<br>or<br>Session Limits (%) > Clipboard |
| Access in a session to local client drives | Session Limits > Drives<br>or<br>Session Limits (%) > Drives |
| Printers connected to the client LPT port | Session Limits > LPT Ports<br>or<br>Session Limits (%) > LPT Ports |
| Custom devices connected to the client through OEM virtual channels | Session Limits > OEM Virtual Channels<br>or<br>Session Limits (%) > OEM Virtual Channels |
| Client session | Session Limits > Overall Session |
| Printing | Session Limits > Printer<br>or<br>Session Limits (%) > Printer |
| TWAIN device (such as a camera or scanner) | Session Limits > TWAIN Redirection<br>or<br>Session Limits (%) > TWAIN Redirection |

| **Client Devices** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Control whether or not to allow audio input from client-device microphones | Resources > Audio > Microphones |
| Control client-device audio quality | Resources > Audio > Sound quality |

| **Client Devices** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Control audio mapping to client-device speakers | Resources > Audio > Turn off speakers |
| Control whether or not client-device 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 local Special Folders from appearing in sessions | Client Devices > Resources > Drivers > Special folder redirection |
| 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 |
| 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 automatic plugin updates | Maintenance > Turn off auto client update |

| **Printing** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Control creation of client printers on the client device | Client Printers > Auto-creation |
| Allow use of legacy printer names and preserve backward 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 |

| **Printing** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Control when to use the Universal Printer Driver | Drivers > Universal driver |
| Choose a printer based on a roaming user's session information | Session printers |

| **User Workspace** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| 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<br>This rule appears only in the Enterprise Edition of XenApp. |

| **Security** | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Require that connections use a specified encryption level | Encryption > SecureICA encryption |

| Service Level | |
|---|---|
| **Task:** | **Use this policy rule:** |
| Select the importance level at which the sessions run | Session Importance |

# Policy Rule Definitions

This topic provides information about the rules you can configure for a policy. The topic mirrors the structure of the rules folders in the Advanced Configuration tool. The major categories of rules are:

- Bandwidth
- Client Devices
- Printing
- User Workspace
- Security
- Service Level

All of these categories are represented by top-level folders that contain related rules.

---

**Note:** Servers running some earlier releases of XenApp in a mixed farm cannot access all these rules. Citrix recommends that you maintain all servers in a farm at the same release level.

---

## Bandwidth Folder

The Bandwidth folder contains subfolders of rules you can configure to avoid performance problems related to client session bandwidth use.

### Visual Effects Folder

The Visual Effects folder contains rules to turn off visual effects, such as desktop wallpaper, menu animations, and drag-and-drop images, to lower the bandwidth used in client connections. You can improve application performance on a WAN by limiting bandwidth usage.

#### Turn Off Desktop Wallpaper

To turn off desktop wallpaper in user sessions, set this rule to **Enabled**.

### Turn Off Menu Animations

Menu animations are a Microsoft personal preference setting that causes a menu to appear after a short delay, either by scrolling or fading in. When menu animations are on, an arrow icon appears at the bottom of the menu and the menu appears when you mouse over that arrow.

If you want to turn off menu animations in client connections, set this rule to **Enabled**.

### Turn Off Window Contents While Dragging

When you drag a window across the screen, either the entire window appears to move when you drag it or just an outline of the window moves until you drop the window. The latter occurs when you turn off window contents while dragging.

If you want to turn off window contents while dragging in user sessions, set this rule to **Enabled**.

## SpeedScreen Folder

The SpeedScreen folder contains a rule that enables you to remove or alter compression. When client connections are limited in bandwidth, downloading images without compression can be slow.

### Image Acceleration Using Lossy Compression

This rule defines ways in which images can be compressed to improve the responsiveness of graphics-intensive applications:

- Normal lossy compression
- Progressive display compression
- Heavyweight compression

If your server farm includes servers running different releases of XenApp, you may not be able to apply all of these image acceleration techniques to all of the servers in the farm. Citrix recommends that you maintain all servers in a farm at the same release level.

If this rule is not configured, SpeedScreen Image Acceleration applies image compression as follows:

- Normal lossy compression is applied with Medium compression/medium quality for all connections. This provides better session performance at the cost of a slight reduction in image quality.
- SpeedScreen Progressive Display is enabled with a threshold of 1 megabit per second.

- Heavyweight compression is disabled.

## Optimizing Image Acceleration

Citrix recommends optimizing these image acceleration settings to suit your deployment. Factors such as the type and quality of images, network configuration, and which graphics applications you use affect the user experience. Determine the optimum settings by adjusting the **Compression level**, its **Threshold value**, and by selecting **Heavyweight compression**. For example, enabling lossy compression but with no threshold can improve the display speed of high-detail bitmaps (such as photographs) over a LAN.

## Compression Level

This setting controls the normal lossy compression level used over client connections that are limited in bandwidth. In such cases, displaying images without compression can be slow. The **Compression level** setting defines the degree of lossy compression used on images. For improved responsiveness with bandwidth-intensive images, use high compression. Where preserving image data is vital; for example, when displaying X-ray images where no loss of quality is acceptable, you may not want to use lossy compression.

Enter the maximum bandwidth in kilobits per second in **Restrict compression to connections under this bandwidth**. The Compression level setting is then applied only to client connections under this bandwidth.

## SpeedScreen Progressive Display Compression Level

Slow initial download of images can be frustrating for users. The **SpeedScreen Progressive Display compression level** setting provides a less detailed but faster initial display. The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use very high or ultra high compression for improved viewing of bandwidth-intensive graphics such as photographs.

Enter the maximum bandwidth in kilobits per second in **Restrict compression to connections under this bandwidth**. The SpeedScreen Progressive Display compression level is then applied only to client connections under this bandwidth.

For this feature to be effective, the SpeedScreen Progressive Display compression level setting must be higher than the Compression level setting. By default, it is two settings higher. For example, if **Compression level** is set to medium compression, **SpeedScreen Progressive Display compression level** is set to very high compression.

**Note:** The increased level of compression associated with SpeedScreen Progressive Display also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.

### Use Heavyweight Compression

Heavyweight compression allows you to reduce bandwidth further without losing image quality by using a more advanced, but more CPU-intensive, graphical algorithm.

If enabled, heavyweight compression applies to all lossy compression settings. It is supported on the Citrix XenApp Plugin for Hosted Apps but has no effect on other plugins.

## Session Limits and Session Limits (%) Folder

The Session Limits and Session Limits (%) folders contain rules you can use to limit the bandwidth used for data transfer in client connections; for example, when accessing drives or printing. You can improve application performance on a WAN by limiting bandwidth used by competing channels for drives and printers over the same client connection or for all client connections.

If you want to limit sessions by a specific amount of kilobits per second, use the rules in the Session Limits folder. If you want to limit sessions to a percentage of the overall session bandwidth setting, use the rules in the Session Limits (%) folder. This specifies a limit for the individual virtual channels. If you use Session Limits (%) rules, you must also enable the Overall Session rule in the Session Limits folder.

If you set a fixed value and a percentage value in two parallel rules (for example, Bandwidth > Session Limits > Audio and Bandwidth > Session Limits (%) > Audio), the most restrictive rule (that is, the lower value) is the one that is applied.

### Audio

By default, users have access to audio equipment attached to their client devices when connected to a session. Applications running in a session can play sounds on the client. Client audio mapping can cause excessive load on the servers and the network.

You can limit the bandwidth consumed by audio on a client in a client connection. Limiting the amount of bandwidth consumed by audio can improve application performance. This is useful when audio and application data compete for limited bandwidth. Limiting the bandwidth used can degrade audio quality.

After enabling the rule, enter the maximum amount of bandwidth in the **Limit** box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that audio can consume in a client connection.

## Clipboard

You can limit the bandwidth consumed by a cut-and-paste data transfer between a session and the local clipboard. Limiting the amount of bandwidth consumed by using the clipboard can improve application performance. This is useful when clipboard data and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that using the clipboard can consume in a client connection.

## COM Ports

You can limit the bandwidth consumed when a client COM port is accessed in a client connection. Limiting the amount of bandwidth consumed by COM port communication can improve application performance. This is useful when the COM port virtual channel and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that COM port access can consume in a client connection.

## Drives

You can limit the bandwidth consumed when a client drive is accessed in a client connection. Limiting the amount of bandwidth consumed by client drive access can improve application performance. This is useful when mapped drive virtual channels and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that client drive access can consume in a client connection.

## LPT Ports

You can limit the bandwidth consumed by a print job using an LPT port in a single client connection. Limiting the amount of bandwidth consumed by LPT port communication can improve application performance. This is useful when the LPT port channel and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that LPT port access can consume in a client connection.

## OEM Virtual Channels

Custom (OEM) devices attached to ports on the client device can be mapped to ports on the server.

You can limit the bandwidth that a custom device's virtual channel can consume in a single client connection. Limiting the amount of bandwidth consumed by these devices can improve application performance. This is useful when custom devices and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that an OEM's virtual channel can consume in a client connection.

## Overall Session

You can limit the bandwidth used in a single client connection overall. Limiting the amount of bandwidth consumed by a client connection can improve performance when other applications outside the client connection are competing for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is in kilobits per second. This is the amount of bandwidth that a client connection can consume overall.

## Printer

You can limit the bandwidth that a print job can use in a single client connection. Limiting the amount of bandwidth consumed by print jobs can improve application performance. This is useful when printing and application data compete for limited bandwidth.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is in either kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder. This is the amount of bandwidth that a print job can consume in a client connection.

### TWAIN Redirection

Use this rule to set the maximum amount of bandwidth available to this feature in client sessions.

TWAIN devices are image acquisition devices, such as scanners and digital cameras, that use manufacturer-supplied, industry standard TWAIN drivers. TWAIN redirection (enabled by default) allows users to access client-side TWAIN devices from published image processing applications.

After enabling the rule, enter the maximum amount of bandwidth in the Limit box. The value you enter is either in kilobits per second or as a percentage of overall available bandwidth, depending on whether you choose the Session Limits folder or the Session Limits % folder.

To set a compression level for image transfers or to disable TWAIN redirection, use the rule Client Devices > Resources > Other > Configure TWAIN redirection.

## Client Devices Folder

The Client Devices folder contains subfolders of rules related to mapping various functions to client devices.

Disabling or not configuring rules that explicitly turn off device mapping does not turn device mapping on.

## Resources Folder

The Resources folder contains rules related to mapping various client devices to similar devices on a server.

Citrix XenApp Plugin for Hosted Apps for Windows supports mapping client devices to servers so they are available to users running sessions. You can restrict access to client devices depending on connection conditions.

## Audio Folder

The Audio folder contains rules you can set to permit client devices to send and receive audio in sessions without reducing performance.

## Microphones

You can allow users to record audio using devices such as microphones on the client. To record audio, the client device needs either a built-in microphone or a device that can be plugged into the microphone jack.

If audio is disabled (the default on the client), this rule has no effect.

For security, users are alerted when servers that are not trusted by their client devices try to access microphones. Users can choose to accept or not accept access. Users can disable the alert on Citrix XenApp Plugin for Hosted Apps for Windows.

To control whether or not users can record audio during their sessions, enable the rule and then choose one of the following options:

- To allow recording, select **Use client microphones for audio input**
- To turn off audio recording (for example, when bandwidth is limited), select **Do not use client microphones for audio input**

## Sound Quality

Use the projected figures for each level of sound quality to calculate the bandwidth potentially consumed in connections to specific servers. For example, if 25 users record at medium quality on one server, the bandwidth used in the connections to that server is over 200,000 bytes per second.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption is doubled.

To control sound quality, enable this rule and then choose one of the following options:

- Select **Low sound quality** for low-bandwidth connections. Sounds sent to the client are compressed up to 16Kbps. This compression results in a significant decrease in the quality of the sound but allows reasonable performance for a low-bandwidth connection.
- Select **Medium sound quality** for most LAN-based connections. Sounds sent to the client are compressed up to 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device and allows good performance.
- Select **High sound quality** for connections where bandwidth is plentiful and sound quality is important. Clients can play sound at its native rate. Sounds can use up to 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.

### Turn Off Speakers

You can allow users to receive audio from an application on a server through speakers on their client devices. Client audio mapping can cause excessive load on the servers and the network.

To turn off audio reception in connections, enable this rule.

## Drives Folder

The Drives folder contains rules relating to client drive mapping and client drive optimization.

### Connection

By default, all drives are mapped when users log on. If you want to stop drives from being mapped when users log on (for example, to prevent users from saving files to their local drive), enable this rule.

After enabling this rule, select one of the following options:

- Do Not Connect Client Drives at Logon
- Connect Client Drives at Logon

### Mappings

By default, all client drives are mapped when a user logs on and users can save files to all their client drives.

To prevent users from saving files to one or more client drives, enable this rule and select the drives that you want to prevent users from accessing:

- **Turn off Floppy disk drives**. Prevents users from accessing their floppy disk drives, such as drive A.
- **Turn off Hard drives**. Prevents users from accessing any of their hard drives, such as drive C.
- **Turn off CD-ROM drives**. Prevents users from accessing any of their CD-ROM drives.
- **Turn off Remote drives**. Prevents users from accessing any mapped network drives, such as remote drives located in the Windows Server 2008 **Computer** panel.

Disabling this rule causes the default of access to all drives to override the same rule in lower priority policies.

This rule does not turn drive mapping on for users. Use the Connection rule to stop or start mapping drives automatically when users log on.

# Optimize Folder

The Optimize folder contains rules related to improving client drive performance.

## Asynchronous Writes

Use this rule to specify asynchronous disk writes and change the speed at which physical files are transferred from server to client. Asynchronous disk writes can speed up file transfers and general writing to client disks over wide area networks (WANs), which are typically characterized by relatively high bandwidth and high latency.

However, if there is a line or disk fault, the client file or files being written may end in an undefined state. If this happens, a pop-up window informs the user of the files affected, and the user can then take remedial action, such as restarting an interrupted file transfer on reconnection or when the disk fault is corrected.

With the rule enabled, the check box for **Turn on asynchronous disk writes to client disks** is selected. This setting enables asynchronous file transfers for a connection.

Citrix recommends that you implement asynchronous disk writes only for users who need remote connectivity with good file access speed and who can easily recover files or data lost in the event of connection or disk failure.

# Special Folder Redirection

Special Folder Redirection is a XenApp feature that enables Citrix XenApp plugin and Web Interface users to see special folders, such as Documents and the Desktop, from a session. You enable this feature in the Access Management Console.

The Special folder redirection rule prevents any objects filtered through a policy from having Special Folder Redirection, regardless of which settings exist elsewhere. If you enable this rule:

- Any related settings you specified for Web Interface or Citrix XenApp Plugin in the Access Management Console are ignored, even if one of those settings enabled this feature
- Users affected by this policy cannot see their local Documents and Desktop folders from a session

To define which users can have Special Folder Redirection, enable this rule in a policy filtered on the users that you do not want to have this feature. The Special folder redirection rule overrides all other Special Folder Redirection settings throughout XenApp. For more information, see "Displaying Local Special Folders in Sessions" on page 110.

# Ports Folder

This folder contains rules for client LPT and COM port mapping.

## Turn Off COM Ports

By default, client COM ports are turned on and available for mapping to server COM ports. However, they are not mapped automaticallyat logon; you must map them manually in the session.

To make client COM ports unavailable for mapping, set the rule to **Enabled**.

---

**Note:** PDA devices are not supported in XenApp 5.0. However, in a mixed-farm environment, enabling this rule prevents PDA devices from working in client sessions initiated from pre-Windows Vista client devices.

---

## Turn Off LPT Ports

By default, the LPT ports on the client are mapped to LPT ports on the server when a user logs on to a session. However, LPT ports are used only by legacy applications that send print jobs to the LPT ports and not to the print objects on the client device. Most applications today can send print jobs to printer objects.

When this rule is enabled, users cannot print to legacy applications that print through LPT ports. This rule is necessary only for servers that host legacy applications that print to LPT ports.

To prevent data transmission to an LPT port, set the rule to **Enabled**.

# PDA Devices folder

Due to limitations in Windows Server 2008, PDA support is not available in XenApp 5.0. Users can sync PDAs only if they are running an operating system released before Windows Vista on their client device and they are syncing to an application published on a server running Citrix Presentation Server 4.0 or 4.5. The Turn on automatic virtual COM port mapping rule appears in XenApp 5.0 to let you manage servers from earlier releases; it has no effect on a server running XenApp 5.0.

This folder contains a rule for turning on virtual COM port mapping.

## Turn On Automatic Virtual Com Port Mapping

Use this rule to enable users with USB-tethered, Windows CE-based PDA devices to use USB-to-virtual-COM-port emulation in client sessions.

By default, client COM ports, both physical and virtual, are not mapped automatically at logon.

### To map virtual COM ports automatically at logon

1. On a server running Windows Server 2003 and Presentation Server 4.5, set this rule to **Enabled**.
2. Set the rule Client Devices > Resources > Ports > Turn off COM ports to **Not Configured** or **Disabled**.

## Other Folder

The Other folder contains rules related to mapping to other client resources; for example, ports to which custom devices are attached.

### Configure TWAIN Redirection

Use this rule to configure a compression level for image transfers from client to server or to disable TWAIN redirection. TWAIN redirection (enabled by default) allows users to access TWAIN devices on the client from published image processing applications.

TWAIN devices are image acquisition devices, such as scanners and digital cameras, that use manufacturer-supplied, industry-standard TWAIN drivers. This rule sets the compression level when users connect to TWAIN devices on the client with published image processing applications.

After enabling the rule, select an option:

- **Do not allow TWAIN redirection**. Prevents the use of TWAIN devices on the client from published applications.
- **Allow TWAIN redirection** (selected by default). Enables the feature and lets you configure a compression level.
- **Use lossy compression for high color images**. Allows you to select the level of compression from the list (low for best image quality, medium for good image quality, or high for lowest quality).

To limit the amount of bandwidth available to this feature in client sessions, use either the rule Bandwidth > Session Limits > TWAIN Redirection or Bandwidth > Session Limits (%) > TWAIN Redirection.

### Turn Off Clipboard Mapping

By default, clients map the client clipboard to the server clipboard.

To prevent cut-and-paste data transfer between a session and the local clipboard, set the rule to **Enabled**. Users can still cut and paste data between applications running in sessions.

### Turn Off OEM Virtual Channels

By default, custom devices attached to ports on the client device can be mapped to ports on the server.

To turn off OEM virtual channels in connections to which this policy is applied, set this rule to **Enabled**.

## Maintenance Folder

The Maintenance folder contains rules related to the maintenance of client devices.

### Turn Off Auto Client Update

You can use an Auto Client Update database to distribute the latest Delivery Client (SV) software to client devices automatically.

---

**Note:** The Auto Client Update feature is no longer supported.

---

If you are using Auto Client Update and want to turn it off; for example, in client connections to specific servers, set the rule's state to **Enabled**.

# Printing Folder

The Printing folder contains subfolders of rules for managing client printing.

# Client Printers Folder

This folder contains rules for client printers, including settings to autocreate client printers, use legacy printer names, retain printer properties, route print jobs, and turn off client printer mapping.

## Auto-Creation

Use this rule to override default client printer autocreation settings. By default, client printers are created at logon based on Terminal Services settings and users can print from sessions using these printers.

Disabling this rule causes the Terminal Services settings for autocreating client printers to override this rule in lower priority policies.

---

**Important:** This rule applies only if client printer mapping is enabled.

---

After enabling the rule, select an option:

- **Auto-create all client printers** (selected by default). Automatically creates all printers on a client device.
- **Auto-create local (non-network) client printers only**. Automatically creates only printers directly connected to the client device through an LPT, COM, USB, or other local port.
- **Auto-create the client's default printer only.** Automatically creates only the printer selected as the client's default printer.
- **Do not auto-create client printers**. Turns off autocreate for all client printers when users log on.

## Legacy Client Printers

Use this rule to allow old-style client printer names and preserve backward compatibility for users or groups using MetaFrame Presentation Server 3.0 or earlier.

After enabling the rule, select an option:

- **Create dynamic session-private client printers** (selected by default). Creates client printers that are private to each user session, and uses standard client printer names similar to those created by native Terminal Services, such as "HPLaserJet 4 from clientname in session 3."
- **Create old-style client printers**. Creates printers that can be shared between sessions and uses printer names based on the old naming conventions, such as "Client\clientname#\HPLaserjet 4." Because this option is less secure, use it only to provide backward compatibility for users or groups using MetaFrame Presentation Server 3.0 or earlier.

## Printer Properties Retention

Use this rule to choose where to store printer properties: on the client device only, in the user profile only, or a combination based on the best option for your users. Base your choice on the installed versions of Citrix XenApp and Citrix XenApp Plugin for Hosted Apps for Windows.

After enabling the rule, select an option:

- **Held in profile only if not saved on client** (selected by default). Allows the system to determine the method. Printer properties are stored on the client device if available, or, if not, in the user profile. Although this option is the most flexible, it can also slow down logon time and use extra bandwidth to perform the needed system-checking.

- **Saved on the client device only**. Stores printer properties only on the client device. Use this option if your system has a mandatory or roaming profile that you do not save.
- **Retained in user profile only**. Stores printer properties in the user profile on the server and prevents any properties exchange with the client. Use this option with installations of MetaFrame Presentation Server 3.0 or earlier and MetaFrame Presentation Server Client 8.*x* or earlier. This option is also useful if your system is constrained by bandwidth (this option reduces network traffic) and the default combination option slows down logon time.

## Print Job Routing

Use this rule to control how to route printing requests to the network print server.

After enabling the rule, select an option:

- **Connect directly to network print server if possible** (selected by default). Routes print jobs directly from the XenApp server to the network print server. Use this option if the network print server is not across a WAN from the server. Direct communication results in faster printing if the network print server and server are on the same LAN.
- **Always connect indirectly as a client printer**. Routes print jobs through the client device, where it is redirected to the network print server. Use this option if the network is across a WAN or has substantial latency or limited bandwidth. Data sent to the client is compressed, so less bandwidth is consumed as the data travels across the WAN.

  Additionally, if two network printers have the same name, the printer on the same network as the client is used.

## Turn Off Client Printer Mapping

Use this rule to disable all client printing by preventing mapping to client printers. By default, client printers are mapped to a server when a user logs on to a session.

# Drivers Folder

The Drivers folder contains rules relating to printer drivers.

# User Workspace Folder

The User Workspace folder contains subfolders of rules for maintaining a good user experience while permitting specific capabilities and without reducing server performance.

# Connections Folder

This folder contains rules for directing and limiting connections for each user.

## Limit Total Concurrent Sessions

You can restrict the number of concurrent connections (user sessions) that users can have in the server farm. This reduces the number of client connection licenses in use and conserves resources. The setting for the least connections overrides any other setting.

To limit the number of concurrent connections allowed, set the rule to **Enabled** and then type the number of concurrent connections you want to allow in the **Limit** box.

## Zone Preference and Failover

You can use zone preference and failover to direct connections to the least loaded server in the same zone or zones on the same LAN. Unless zones are arranged in a preferred connection order, users are directed to the server with the least load even if that server is in another zone across a WAN. If a zone is unavailable, the connection can be directed to other primary zones, backup zones, or zones with no preference, for business continuity.

---

**Important:** Zone preferences always take precedence over session sharing when they are in conflict.

---

This rule can be applied to users, IP addresses, and client names, but not servers.

To set the connection order for zones, set the rule to **Enabled** and then select one or more zones in **Zone preference settings**. For zones to which you want connections directed first, select **Primary Group**. For zones to which you do not want users to connect, select **Do Not Connect**.

You can select additional zones as backups. You can place zones in Backup Group 1 through Backup Group 10 in **Set connection order** for selected zones. Backup Group 10 is last in backup connection order. Zones with no preference, which is the default, are chosen for connection after zones in Backup Group 10.

# Content Redirection Folder

This folder contains rules for using content redirection from servers to plugins.

## Server to Client

By default, users open URLs embedded in remote applications using Web browsers or multimedia players running on servers. An example is a link to a multimedia URL sent in an email message. This can cause excessive load on the servers and the network. If you want the users' locally installed browser or multimedia player to play URLs, turn on server content redirection. Server content redirection is available for the plugins for Windows and the Client for Linux.

These URL types are opened locally when server content redirection is enabled:

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

To control server content redirection, set the rule to **Enabled** and then select one of the following options:

- Use Content Redirection from server to client
- Do not use Content Redirection from server to client

# Shadowing Folder

You can allow users to shadow other users. This is useful for training purposes and for viewing presentations. You can also allow help desk personnel to shadow users so they can troubleshoot user problems.

The Shadowing folder lets you configure rules for user-to-user shadowing. For user-to-user shadowing to work, you must configure both rules in this folder, as follows:

1. **Configuration**. Enable this rule to allow user-to-user shadowing in your environment. Then, configure shadowing options for connections to which this policy is applied. You must specify which users have permissions to shadow in the Permissions rule.
2. **Permissions**. Assign shadowing permissions to users you want to be able to shadow other users.

You specify the users who can be shadowed when you apply the policy through a filter. All of the filtered objects to which this policy is applied can be shadowed by anyone whose name is in the user list in the Permissions rule.

If you create multiple shadowing policies and assign priorities, enable the **Merge shadowers in multiple policies** setting on the farm's Properties page in the Access Management Console. Without this setting enabled, lower priority shadowing policies may be ignored.

You can configure shadowing during or after XenApp Setup by using policies or using Terminal Services Configuration. The most restrictive shadowing settings override all other settings.

---

**Note:** Shadowing policy rules are not supported for users who authenticate through Novell Directory Services when they log on.

---

Related topics:

"Configuring User Shadowing" on page 416

"Permissions to Shadow Users" on page 417

## Configuring User Shadowing

When you want to configure user-to-user shadowing you must enable support for it by enabling the Configuration rule. Then select the users you want to be able to shadow other users in the Permissions rule.

### To allow a user or user group to be shadowed

1. Select this rule from the policy's properties (**User Workspace** > **Shadowing** > **Configuration**).
2. Set the rule to **Enabled**.
3. Select **Allow Shadowing**.
4. If you want the user being shadowed to be notified when shadowing starts, select **Prohibit Being Shadowed Without Notification**.
5. If you do not want users to be able to take control of the mouse and keyboard of the user they are shadowing, select **Prohibit Remote Input When Being Shadowed**.
6. In the left pane of the **Property** sheet, select the rule Permissions and then select which users can shadow other users.
7. Filter the policy containing this rule based on the users you want to allow to be shadowed.

To prevent shadowing of the connections to which this policy is applied, set the rule to **Enabled** and select **Do Not Allow Shadowing**.

To default to the settings in Terminal Services Configuration or in other policies, set the rule to **Disabled**.

## Permissions to Shadow Users

To specify the users who can shadow other users, use the Permission rule. The users who can be shadowed are all of the users to which this policy is applied. You must also enable the Configuration rule in the same policy for shadowing to work.

### To allow users to shadow the connection to which this policy is applied

1. Select this rule from the policy's properties (**User Workspace** > **Shadowing** > **Permissions**).
2. Set the rule to **Enabled**.
3. Click **Configure**.
4. In the **Assign Shadowing Permissions** dialog box, specify the user or user group accounts that you want to allow to shadow:

   A. To add users or user groups, use one of the following controls :

   - **Add List of Names**. Click this button to enter user account names. Separate user names with a semicolon. The list of user accounts is added to the Configured Accounts list.
   - **Look in**. This list contains all trusted account authorities configured on the servers in the farm. These can include Novell Directory Services (NDS) trees, Windows NT domains, Windows 2000 Active Directory domains, and local servers.

   When you select an account authority, the user accounts that are part of the selected authority appear in the window below the list. By default, only user groups appear.

   To display every user in the selected domain, select **Show Users**. For NDS, alias objects also appear.

   The user accounts you selected appear in the **Configured Accounts** display. These are the users or groups allowed to shadow the connections to which this policy is applied.

   B. To deny shadowing permissions to any users in the Configured Accounts list, select **Deny**. By default, each user or group is set to **Allow**.

# Time Zones Folder

You can set the following policy rules in this folder to configure time zone rules for connections to which this policy is applied:

- **Do not estimate local time for legacy clients**. Enable this rule if you want the client's time zone to be used when that information is available from the client device, but not estimated if the client device cannot send that information. If you enable the rule Do not use Clients' local time, this rule has no effect.
- **Do not use Clients' local time**. Enable this rule if you want the server's time zone to be used for all clients.

## Do Not Estimate Local Time for Legacy Clients

By default, published applications reflect the user's local time zone in sessions. Earlier plugin versions may not send accurate time zone information to the server. In this situation, the server estimates local time zones for client devices.

If you want the server's time zone to be used for older plugins instead of an estimated local time zone that may not be accurate, set the rule to **Enabled**.

If you are using the server's time zone for all plugins because you enabled the rule Do not use Clients' local time, enabling the rule Do not estimate local time for legacy clients has no effect.

## Do Not Use Clients' Local Time

By default, published applications reflect the user's local time zone in sessions. If you want the server's time zone to be used, set this rule to **Enabled**.

# Citrix Password Manager Folder

Some environments use Citrix Password Manager to authenticate users of published applications. This folder contains policy rules for configuring and controlling the use of Password Manager.

## Central Credential Store

Central credential stores are repositories for Password Manager data. Central credential stores can be of several types, including file share and Active Directory. Use this rule to control which credential repository stores information about which users or user groups. By default, the rule is **Not Configured**. To override lower-priority policies, the rule must be **Disabled** or **Enabled**.

Because a single file share supports a maximum of 15,000 concurrent users, you may need multiple credential stores if you have more than this number of users.

Controlling which credential store users connect to allows you to:

- Assign users to geographically close central credential stores, thereby preventing that data from being sent over a WAN
- Define which central credential stores are used by specific user groups, clients, or servers

For more information about central credential stores, see the Password Manager documentation.

Enter the UNC path of the central credential store for use with this policy. Policies apply only to shared folders you configure to be Password Manager central credential stores. If you want this policy to use the central credential store specified by the Password Manager agent, leave this field blank.

---

**Important:** Server farm zone failover preferences apply only to published objects, not to central credential stores. If the user's preferred zone is not operating and the connection fails over to a backup zone, the user cannot access published objects using Password Manager if the credential store is in the failed zone.

---

### Do Not Use Citrix Password Manager

Use this policy rule to control which users can run Password Manager when they connect to servers or published applications in your farm. This allows you to:

- Deploy Password Manager gradually to user groups within zones or within the farm
- Limit use of Password Manager to subgroups who are specifically licensed to use it within zones or within the farm
- Limit use of Password Manager to specific clients or to specific servers in the farm

By default, the rule is **Not Configured**. To override lower-priority policies, set the rule to **Disabled** or **Enabled**.

## Streamed Applications Folder

This folder contains rules for configuring how streamed applications are delivered to users.

For information about the Citrix application streaming feature, see the *Citrix Application Streaming Guide*.

### Configure Delivery Protocol

This rule enables you to override the delivery of applications published as Streamed to client. You select the delivery method in the Access Management Console's Publish Application wizard.

For streamed applications published as **Accessed from a server**, this rule does not apply.

After enabling the rule, select an option:

- **Force server access** (selected by default). Users always launch streamed applications from the server:
  - If you publish a streamed application as **Streamed if possible, otherwise accessed from a server** (dual mode streaming), users launch the application from the server using the alternative method you selected
  - If you publish an application as **Streamed to client** (without dual mode), the connection fails
- **Force streamed delivery**. Client devices always stream the application from the file share location to the client desktops. Users must have the XenApp Plugin for Streamed Apps installed and they must access the application using XenApp Plugin for Hosted Apps or a Web Interface site. For example, you might use this setting to prevent the use of server resources.

If you disable the rule or do not configure it, the delivery method selected in the Publish Application wizard is used.

## Security Folder

The Security folder contains subfolders of rules related to security.

## Encryption Folder

The Encryption folder contains rules for raising encryption levels to further secure communications and message integrity for certain users.

### SecureICA Encryption

By default, the XenApp server uses basic encryption for client-server traffic. You can raise encryption levels to further secure communications and message integrity for certain users. If you create a policy to require a higher encryption level, plugins using a lower encryption level are denied a connection.

You can specify encryption levels for sessions using policies or, using the Access Management Console, in published applications. The setting configured for the highest encryption overrides all other settings.

After enabling this rule, select one of the following encryption levels:

- **Basic** encrypts the client connection using a non-RC5 algorithm. It protects the data stream from being read directly, but can be decrypted
- **RC5 (128-Bit) logon only** encrypts the logon data with RC5 128-bit encryption and the client connection using basic encryption
- **RC5 (40-bit)** encrypts the client connection with RC5 40-bit encryption
- **RC5 (56-bit)** encrypts the client connection with RC5 56-bit encryption
- **RC5 (128-bit)** encrypts the client connection with RC5 128-bit encryption

# Service Level Folder

The Service Level folder contains a rule to specify the importance level at which sessions run.

## Session Importance

This rule (along with the application importance level that you set when publishing an application) determines the relative importance of each session and has three possible values: low, normal, and high.

If CPU Utilization Management is enabled, sessions with higher importance levels (greater Resource Allotment) are allowed to use more CPU cycles than sessions with lower importance levels (lower Resource Allotment).

When Preferential Load Balancing is configured, a session with the highest Resource Allotment is directed to a server with the lowest Resource Allotment.

Related topics:

“Using Preferential Load Balancing” on page 322

“Resource Allotment” on page 322

“To configure application importance” on page 60

“Using CPU Utilization Management” on page 325