Common Criteria Evaluated Configuration Guide for Citrix XenApp 6.0 for Windows Server 2008 R2

Copyright and Trademark Notices

Use of the product documented herein is subject to your prior acceptance of the End User License Agreement. A printable copy of the End User License Agreement is included with your 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. 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.

Citrix® is a registered trademark, and Citrix Presentation Server™, Citrix XenApp™, Citrix XenApp™ for UNIX®, Citrix Access Suite™, Citrix Subscription Advantage™, are trademarks of Citrix Systems, Inc. in the United States and other countries.

Trademark Acknowledgements

RSA Encryption © 1996–1997 RSA Security Inc. All rights reserved.

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

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

Java, Sun, SunOS, Solaris, JavaServer Pages, and Sun Java System Application Server are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, MS, Windows, Windows Server, Win32, Outlook, ActiveX, Visual J#, ClearType, Excel, SQL Server, Microsoft Access, Windows Vista, .NET, Media Player, and Active Directory are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape, Netscape Navigator, and Mozilla are trademarks or registered trademarks of Netscape in the United States and other countries.

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

Document code: February 9 2011 16:28:33

Contents

1 Introduction.....7

About this Guide 7

Common Criteria Target of Evaluation 7

Citrix XenApp Documentation.....9

2 Planning for Citrix XenApp Deployment.....11

Overview 11

Common Criteria Evaluated Deployment 12

Domain Configuration 13

FIPS 140 Policies and Security Certificates 13

Authentication 14

System Requirements.....14

Evaluated Platforms 14

Operating System Updates.....15

Citrix XenApp System Requirements.....16

Installing the Server Roles.....17

Web Interface System Requirements.....18

Installing the Web Server Role.....19

Primary DNS Suffix 20

Configuring Microsoft IIS to use the Server Certificate.....20

Secure Gateway System Requirements..... 21

User Device System Requirements.....21

IPSec Configuration.....23

Policy Settings Per Server.....23

Third Party Components.....25

Firewalls 26

Firewall 1 (Public Network/DMZ) 26

Firewall 2 (DMZ/Private Network) 26

Web Browsers 26

Virus Protection Software 26

Environment Assumptions.....27

3 Installing the Citrix XenApp Components....29
Updates to Citrix Products Included in the Common Criteria Evaluated Configuration....29
Installing Citrix XenApp....30
Before Installing XenApp....30
Before Configuring XenApp....32
Installing Citrix License Server and Citrix XenApp on the Primary Server....32
Assigning Farm Administrator Credentials....32
To install Citrix XenApp on the primary server....32
To configure Citrix XenApp on the primary server....33
Securing the Secure Ticket Authority and XML Service....35
To enable communication between SQL Server Express and the secondary servers....36
Installing Citrix XenApp on the Secondary Servers....36
To install XenApp on secondary servers....37
To join secondary servers to the XenApp farm....38
To configure the data store DSN....39
Installing the Microsoft File Checksum Integrity Verifier Utility....39
Installing Web Interface....40
Installation Overview....40
Installing the Web Interface Management Console....41
To download and install the Web Interface....41
To configure the Web Interface....42
Installing Secure Gateway....43
Prerequisites....43
To install the Secure Gateway....44
To configure the Secure Gateway....45
To download and install the web plug-in....46

4 Configuring Citrix XenApp....49
Configuring the Servers Running Citrix XenApp....50
Running Discovery....50
To run Discovery using the Delivery Services Console....51
Publishing Applications....51
To publish an application....51
To remove a published application....53
Configuring the Web Interface....53
Enabling Smart Card Authentication....53
To enable the Windows Directory Service Mapper on IIS....53

To enable users to authenticate using smart cards. 54
Enabling Explicit Authentication. 54
To enable explicit authentication to the Web Interface. 54
Configuring Secure Gateway Support. 55
To configure the Web Interface to support Secure Gateway. 55
Installing Single Sign-on Components. 56

5 Securing the Deployment. 57
TLS Renegotiation Issue in Microsoft Products. 57
Updating the Evaluation Components 58
To apply the Microsoft security update. 58
To apply the Citrix hotfixes. 59
Windows Server 2008 R2 Security Configuration Wizard. 60
To install and run the Security Configuration wizard. 60
To configure the IIS Admin Service. 66
Setting Policies. 66
Domain Wide Group Policies. 66
To configure the domain policies. 66
Computer Configuration. 67
User Configuration. 70
Disabling XenApp Features with Policies. 75
Securing Executables with AppLocker. 78
Setting Group Policy Priority. 80
Secure Gateway Local Group Policies. 80
To configure the local group policies. 80
Web Plug-in Local Group Policies and Registry Settings. 83
To configure the local group policies. 83
To configure the file security preferences. 84
Removing and Disabling Citrix User Accounts 85
To remove anonymous users from the XenApp servers. 85
To disable the Citrix user accounts. 85
Using FIPS-Compliant Ciphers Between the Web Plug-in and the Web Interface 85
Securing the User Device. 86
To configure Microsoft Internet Explorer to use TLS 1.0. 86
To disable ActiveX support in Microsoft Internet Explorer 86
To enable forced downloads of ICA files. 87
Testing the Deployment. 87

6 Testing the Deployment. 89

Updates to Citrix Products Included in the Common Criteria Evaluated Configuration. . . .89
Overview. 90
To log on using explicit credentials. 90
To log on using a smart card. 90
Making Citrix XenApp Available to Users. 90
Verifying Client File Security Settings 91
To check and configure the client file security settings. 91
Ensuring Users Close Applications When Logging Off. 91
IMA Error Codes. 93

Chapter 1

Introduction

Topics:

- *Citrix XenApp Documentation*

About this Guide

The Common Criteria Evaluated Configuration Guide for Citrix XenApp 6.0 for Windows Server 2008 R2 describes the requirements and procedures for installing and configuring Citrix XenApp in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require you to deploy XenApp to match the Common Criteria Target of Evaluation configuration exactly, follow the procedures in this guide.

Note: In certain instances, this guide and the *Common Criteria Security Target for Citrix XenApp for Windows Server 2008 R2* document use differing terminology to refer to the same component. Specifically, where this guide refers to "the web plug-in," the *Common Criteria Security Target for Citrix XenApp for Windows Server 2008 R2* document refers to this component as "the online plug-in." Both terms refer to the client software installed on the user device that is used to connect to the farm servers in the evaluated deployment.

Common Criteria Target of Evaluation

This guide supplements the core documentation and details how to configure XenApp to match the Common Criteria Target of Evaluation configuration. The Target of Evaluation is a XenApp deployment comprising:

- Citrix XenApp 6.0 for Windows Server 2008 R2 (Platinum Edition license)
- Web Interface for Citrix XenApp
- Citrix Secure Gateway (for Citrix XenApp)
- Citrix Online Plug-in Web, included in the Citrix Online Plug-in 12.1 for Windows package

- Citrix Single Sign-on 4.8 (optional)

This evaluated deployment does not include the following Citrix XenApp Platinum edition components:

- Application Performance Monitoring (Citrix EdgeSight)
- Citrix Access Gateway
- Citrix Provisioning Services
- Profile Management
- Citrix XenApp Power and Capacity Management
- Smart Auditor

For further information concerning the Common Criteria evaluated deployment, see Common Criteria Evaluated Deployment on page 12.

Citrix XenApp Documentation

This guide occasionally refers to Citrix product documentation, including electronic manuals and online help. The product documentation is located on the associated product media; for example, the Citrix XenApp DVD-ROM.

Documents that are essential references when deploying Citrix XenApp in the Target of Evaluation configuration include:

- The *Citrix XenApp Administration* guide provides conceptual information and procedures for system administrators who install, configure, and maintain Citrix XenApp.
- The *Getting Started with Citrix Licensing* guide explains how to license Citrix XenApp, and describes the tasks related to deploying, maintaining, and using the licensing for Citrix products.
- The *Web Interface Administration* guide explains how to install, configure, and customize the Web Interface.
- The *Secure Gateway for Windows* guide explains how to install and configure the Secure Gateway.
- The *Online Plug-in for Windows* guide provides instructions for system administrators who deploy clients to end-users on Windows computing platforms.
- The *Citrix Single Sign-on Administration* guide provides conceptual, reference, and procedural information for system administrators responsible for installing, configuring, and maintaining Single Sign-on.
- The *Common Criteria Security Target for Citrix XenApp for Windows Server 2008 R2* guide describes the Target of Evaluation, which details assumptions such as the physical environment, the password policy used, and the rights and assumptions concerning the administrators. This document is available only on the Citrix Web site.
- The article "Additional security guidance for Citrix Presentation Server deployments" (http://support.citrix.com/article/CTX114938) describes best practices for securing Citrix XenApp environments.

The guides mentioned above are included with this guide in the downloadable archive available from the Citrix Common Criteria Certification Information Web site (http://www.citrix.com/English/SS/supportThird.asp?slID=162512&tlID=162515).

Chapter 2

Planning for Citrix XenApp Deployment

Topics:

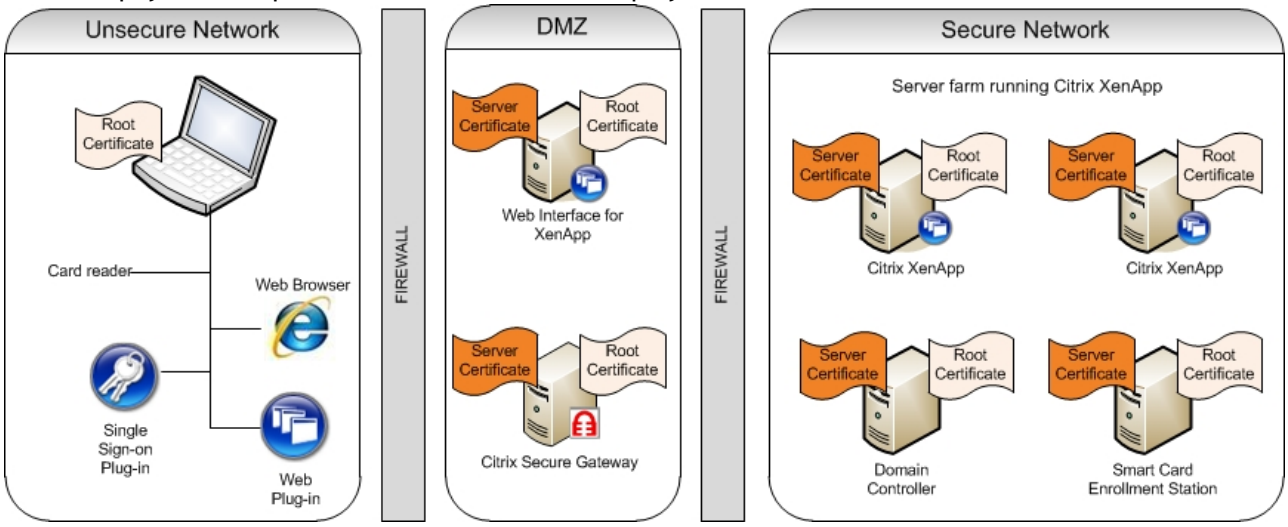
- *Common Criteria Evaluated Deployment*
- *System Requirements*

Overview

This chapter describes the Common Criteria evaluated deployment and explains what you must do before installing and deploying Citrix XenApp.

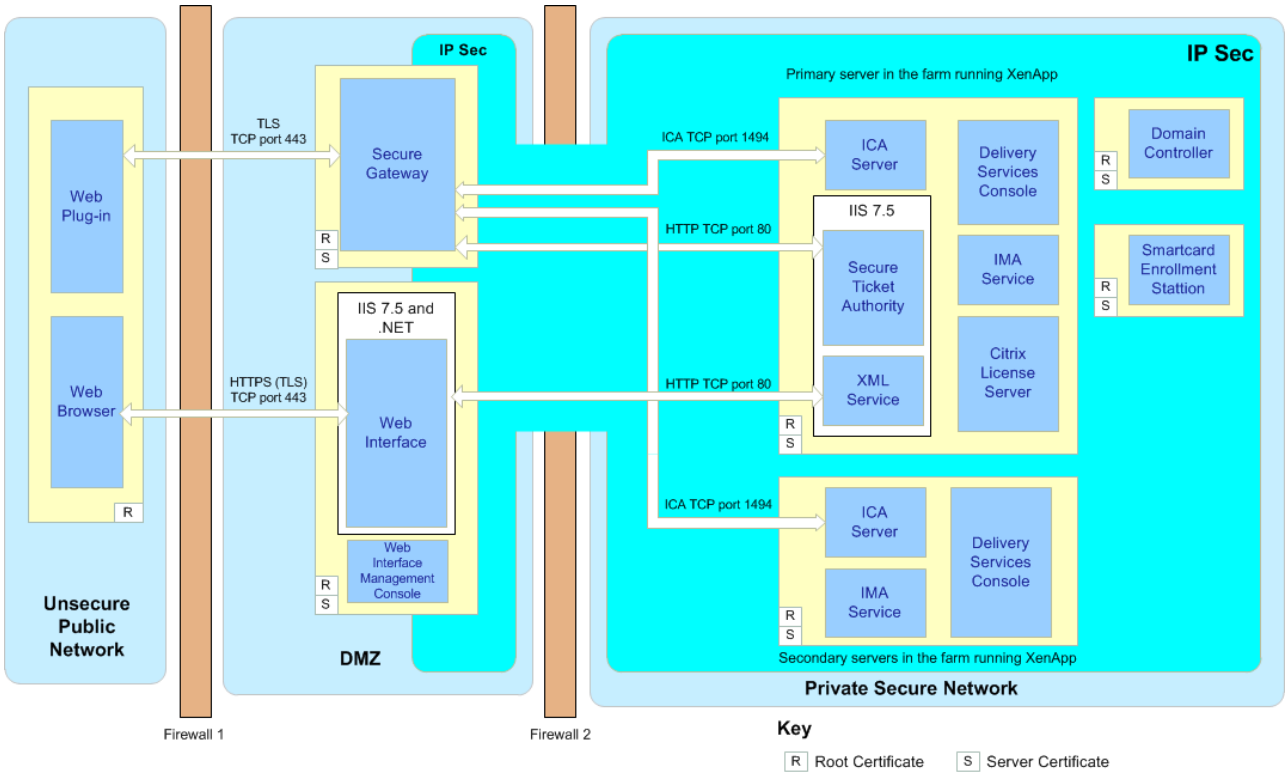
Common Criteria Evaluated Deployment

The overview of the Common Criteria evaluated deployment below illustrates the different physical computers that are used in the deployment.



Note: The domain controller and smart card enrollment station are not part of the Target of Evaluation.

A detailed view of the Common Criteria evaluated deployment is shown below. The detailed view summarizes where the server and root certificates are deployed, and the traffic that is allowed to traverse each of the firewalls.



In the detailed view above, only one of the XenApp servers has the Secure Ticket Authority (STA) enabled. This server also hosts the Citrix License Server. For clarity within this document, this server is referred to as the *primary server*.

On all of the other XenApp servers within the server farm, the STA and XML service are disabled. For clarity within this document, these servers are referred to as *secondary servers*.

Domain Configuration

The domain is a Windows Server 2008 R2 Active Directory domain. The domain is a single Active Directory domain with no trust relationship with any other domain. The following servers are located in the domain:

- The server running the Web Interface
- The primary and secondary servers
- The domain controller and smart card enrollment station

The server running the Secure Gateway is not part of the domain.

FIPS 140 Policies and Security Certificates

To ensure only FIPS 140 compliant ciphersuites and cryptographic modules are used within the deployment, you must apply FIPS 140 compliant group policies. For further

details about the deployment of the FIPS 140 compliant group policies, see Setting Policies on page 66.

Both root and server authentication certificates must be installed on all of the computers that use IPSec with certificate authentication, namely:

- The primary and secondary servers
- The server running the Web Interface
- The server running the Secure Gateway service
- The server running the domain controller
- The server running the smart card enrollment station

All of the client devices must have Certificate Authority (CA) root certificates installed that match the server authentication certificates installed on the servers running the Web Interface and Secure Gateway.

Important: Citrix recommends that customers verify that the certificate authorities trusted by client devices abide by suitable security practices to minimize the risk of issuing malformed certificates. For additional information, refer to CTX123248 in the Citrix Knowledge Center.

Authentication

The Common Criteria evaluated deployment can be configured to allow users to log on to XenApp servers using either explicit credentials (user name and password) or smart card.

Do not configure the Common Criteria evaluated deployment to allow a mix of authentication methods. Users must log on using explicit credentials or a smart card.

You set the authentication method (explicit or smart card) using the Web Interface Management console. For further details, see Configuring the Web Interface on page 53.

If the Common Criteria evaluated deployment is configured for explicit logon, note that the following components are redundant: smart card enrollment station and smart card readers and associated software. Also, the server running the Web Interface need not be in the same domain as the XenApp servers if smart card authentication is not required.

System Requirements

Evaluated Platforms

Citrix XenApp 6.0 supports Windows Server 2008 R2, which requires computers be equipped with 64-bit processors.

Operating System Updates

When installing the operating system on each computer in the evaluated configuration, ensure all applicable patches, security updates, and hotfixes are applied. In particular, ensure the following hotfixes are applied to the specified computers:

Security Bulletin Article Number	Security Bulletin Name	Security Update Name	Component of Evaluated Configuration
KB2416471	MS10-070: Description of the security update for the Microsoft .NET Framework 3.5.1 in Windows 7 and in Windows Server 2008 R2	Security Update for Microsoft .NET Framework 3.5.1, Windows 7, and Windows Server 2008 R2 for x64-based Systems (KB2416471)	◆ Primary and secondary XenApp servers ◆ Web Interface server ◆ Secure Gateway server ◆ User device
KB2271195	MS10-065: Description of the security update for Internet Information Services CGI in Windows 7 and Windows Server 2008 R2	Security Update for Windows Server 2008 R2 x64 Edition (KB2271195)	◆ Primary and secondary XenApp servers ◆ Web Interface server ◆ Secure Gateway server
KB982666	MS10-040: Vulnerability in Internet Information Services could allow remote code execution	Security Update for Windows Server 2008 R2 x64 Edition (KB982666)	◆ Primary and secondary XenApp servers ◆ Web Interface server ◆ Secure Gateway server
		Security Update for Windows 7 (KB982666)	User device

Security Bulletin Article Number	Security Bulletin Name	Security Update Name	Component of Evaluated Configuration
		Security Update for Windows Vista for x64-based Systems (KB982666)	
		Security Update for Windows Vista (KB982666)	

To verify these updates have been installed, check the Installed Updates console in Control Panel (**Start**>**Control Panel**>**Programs**>**Programs and Features**>**Installed Updates**).

Citrix XenApp System Requirements

For the evaluated deployment, the minimum system requirements for Citrix XenApp on the primary and secondary servers are shown below:

Server Hardware	Server Software
64-bit architecture-based computer with 1.4GHz or faster Intel or compatible processor, 512MB of RAM, and a hard drive with at least 32GB of free space.	Microsoft Windows Server 2008 R2 Family (either Standard Edition or Enterprise Edition). **Note:** Ensure that the Microsoft operating system is adequately patched and updated.
Additional 32MB of RAM if the XenApp server will also host connections	Internet Information Services (IIS) 7.5 Terminal Services
Additional 550MB of available hard disk space for installing XenApp. Approximately 50MB of available hard disk space for every 100 servers and 25 applications in the farm.	Smart card. If using smart cards: Smart card software including PC/SC software, Crytographic Service Provider (CSP) software, and smart card reader drivers. You may need to attach the smart card reader device to the server during the PC/SC installation. See your smartcard vendor-specific information for details.
On the primary server hosting the data store: Additional 1GB of available hard	SQL Server Express 2008 (installed with XenApp)

Server Hardware	Server Software
disk space for the SQL Server Express 2008 database.	
Network Interface Card (NIC).	

Installing the Server Roles

You must install the following server roles before you install Citrix XenApp on the primary and secondary servers:

- Application Server
- Remote Desktop Services
- Web Server (IIS)

These roles are not installed with Windows Server 2008 R2 by default. Although the XenApp installer installs some of these roles, the evaluated configuration requires additional role services that the XenApp installer does not include.

1. Log on as an administrator.
2. Launch the Server Manager (**Start**>**Administrative Tools**>**Server Manager**). The **Server Manager** screen appears.
3. From the **Server Manager** screen, under **Roles Summary**, click **Add Roles**.
4. On the **Before You Begin** page of the Add Roles Wizard, click **Next**.
5. On the **Select Server Roles** page, select the following items:
   - Application Server
   - Remote Desktop Services
   - Web Server (IIS)

   When you select the **Application Server** role, a dialog box appears notifying you that additional features are required for the role. Click **Add Required Features** to ensure the additional services are installed. Click **Next** to proceed to the next page of the Add Roles Wizard.
6. On the **Remote Desktop Services** page, click **Next**.
7. On the **Select Role Services** page, select the **Remote Desktop Session Host** check box and click **Next.**
8. On the **Uninstall and Reinstall Applications for Compatibility** page, click **Next.**
9. On the **Specify Authentication Method for Remote Desktop Session Host** page, select **Require Network Level Authentication** and click **Next.**
10. On the **Specify Licensing Mode** page, select **Per Device** and click **Next**.

11. On the **Select User Groups Allowed Access To This RD Session Host Server** page, select the users or groups that will connect to the server and click **Next.**
12. On the **Configure Client Experience** page, click **Next.**
13. On the **Application Server** page, click **Next**.
14. On the **Select Role Services** page, select **Web Server (IIS) Support**.

    Note: This role service is required for the primary server only. For the secondary server, no additional role services are required.

    A dialog box appears notifying you that additional features are required for the role service.
15. Click **Add Required Role Services** to ensure the additional features are installed.
16. Click **Next**.
17. On the **Web Server (IIS)** page, click **Next**.
18. On the **Select Role Services** page, click **Next** to accept the default selections.
19. On the **Confirm Installation Selections** page, verify the services you selected will be installed, and then click **Install.**
    A progress indicator appears while the services are installed on the server.
20. Click **Close** and then click **Yes** to let the Add Roles Wizard restart your computer.

After the server restarts, the Resume Configuration Wizard appears and finishes installing the server roles. Afterward, the wizard reports if the roles were installed successfully. Click **Close** to close the wizard.

Web Interface System Requirements

The minimum system requirements for the Web Interface are shown below:

Server Hardware	Server Software
64-bit architecture-based computer with 1.4GHz or faster Intel or compatible processor, 512MB of RAM, and a hard drive with at least 32GB of free space.	Microsoft Windows Server 2008 R2 Family (either Standard Edition or Enterprise Edition). **Note:** Ensure the Microsoft operating system is adequately patched and updated.
Two Network Interface Cards (NIC).	◆ Internet Information Services (IIS) 7.5 ◆ Visual J# .NET 2.0 Second Edition

Server Hardware	Server Software
	• Microsoft .NET Framework 3.5 with Service Pack 1 **Note:** The .NET Framework and the Visual J# .NET redistributable files are included on the Citrix XenApp DVD-ROM in the Support folder.
	Server authentication certificate stored in local computer account. IIS must be configured to use this certificate. **Note:** A corresponding root certificate must be installed on each client.
	Smart Card **Important:** If configuring the deployment toallow users to log on using smart cards, the server running the Web Interface must be in the same domain as the servers running Citrix XenApp.

Installing the Web Server Role

Before you install Web Interface, you must install the Web Server role on the server to host the Web Interface. This role installs services and features required by the Web Interface installation and configuration process.

1. Log on as an administrator.
2. Launch the Server Manager (**Start**>**Administrative Tools**>**Server Manager**). The **Server Manager** screen appears.
3. From the **Server Role Manager** screen, under **Roles Summary**, click **Add Roles**. The **Add Roles Wizard** appears.
4. On the **Before You Begin** page of the Add Roles Wizard, click **Next.**
5. On the **Select Server Roles** page, select the **Web Server (IIS)** check box.
6. On the **Web Server (IIS)** page, click **Next.**
7. On the **Select Role Services** page, click **Next** to accept the default selections.

8. On the **Confirm Installation Selections** page, verify the Web Server (IIS) role will be installed and click **Install**.
9. After the installation completes, click **Close**.

Primary DNS Suffix

Ensure the primary DNS suffix (Active Directory domain) or fully qualified DNS domain name (including the Active Directory domain) for the server is defined.

To verify correct configuration, check to see if a valid DNS suffix is present in the following registry key value data:

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.

- Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- Value: Domain

To change the primary DNS suffix using Local Area Connection Properties

1. Select **Start**>**Control Panel**>**Network and Internet**>**Network and Sharing Center**>**Local Area Connection**.
2. In the **General** tab, click **Properties**.
   The **Local Area Connection Properties** dialog box appears.
3. Select **Internet Protocol** and then click **Properties**.
   The **Internet Protocol Version Properties** dialog box appears.
4. Click **Advanced** and then click the **DNS** tab.
   You can enter the new DNS suffix in the **DNS suffix for this connection** box.

Configuring Microsoft IIS to use the Server Certificate

You must configure Microsoft IIS to use the server certificate created for the Common Criteria evaluated deployment.

1. Launch the Internet Information Services (IIS) Manager (**Start**>**All Programs**>**Administrative Tools**>**Internet Information Services (IIS) Manager**).
2. From the **Connections** pane, expand the computer node, expand the **Sites** node, and then select **Default Web Site**.
3. Right-click **Default Web Site** and select **Edit Bindings**.
   The **Site Bindings** dialog box appears.

4. Click **Add**.
   The **Add Site Binding** dialog box appears.
5. Under **Type**, select **https** and then, under **SSL Certificate**, select the required server certificate.
6. At the **Add Site Binding** dialog box, click **OK**.
7. At the **Site Bindings** dialog box, click **Close**.

Secure Gateway System Requirements

The minimum system requirements for the Secure Gateway server are shown below:

Server Hardware	Server Software
Computer with 1.4GHz or faster Intel or compatible processor, 512MB of RAM, and a 10GB hard drive with at least 4GB of free space.	Microsoft Windows Server 2008 R2. **Note:** Ensure the Microsoft operating system is adequately patched and updated.
	Server authentication certificate stored in local computer account. IIS must be configured to use this certificate. **Note:** A corresponding root certificate must beinstalled on each client.
Additional 150MB of available hard disk space.	
Two Network Interface Cards (NIC).	

Note: If the Secure Gateway cannot resolve the IP address of the primary server running Citrix XenApp using DNS, the hosts file must include an entry (IP address and FQDN) for the primary server.

User Device System Requirements

The minimum system requirements for running the web plug-in on a user device are shown below:

Client Hardware	Client Software
◆ 1GHz Pentium-compatible processor (32-bit or 64-bit) ◆ 1GB RAM (32-bit) or 2GB RAM (64-bit) ◆ 16GB of available disk space (32-bit) or 20GB of available disk space (64-bit)	◆ Microsoft Windows 7 Ultimate ◆ Microsoft Windows Vista Ultimate **Note:** Ensure that the Microsoft Windows operating system is adequately patched and updated.
	Microsoft Internet Explorer 8 **Note:** Ensure that the Internet Explorer Web browser is adequately patched, including the security updates referenced in Microsoft Security Bulletins MS07-004 and MS07-016. Microsoft Internet Explorer must be configured for TLS 1.0 communication. See Configuring Microsoft Internet Explorer to use TLS 1.0.
Microsoft mouse or 100% compatible mouse.	Trusted root (CA) certificate(s) required to connect to the Web Interface and Secure Gateway servers. **Note:** Corresponding server certificates are required on the servers running the Secure Gateway and Web Interface.
SVGA video adapter with color monitor.	Smart card. If using smart cards: Smart card software including PC/SC software, Crytographic Service Provider (CSP) software, and smart card reader drivers. You may need to attach the smart card reader device to the client device during the PC/SC installation. See your smart card vendor-specific information for details.
Suitable network connection (for example, network interface card,	

Client Hardware	Client Software
modem, and so on). For further details, see section 3 of the *Online Plug-in for Windows* guide.	

IPSec Configuration

As shown in the deployment diagrams, traffic within the private network and between the private network and the DMZ is secured using IPSec.

This section provides details for the IPSec configuration requirements. For details and procedural information, refer to the Microsoft documentation.

Note: Reverse lookup zones must be enabled in Active Directory integrated DNS for all subnets within the IPSec environment.

Policy Settings Per Server

Domain Controller and Smart Card Enrollment Station

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All IP traffic	Any IP traffic	Any IP address	Any	Any	Any	Require security: AES/ SHA-1, certificate authentication

Web Interface Policy

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All TCP/ IP traffic on port 443	Any IP address	My IP Address	TCP	Any	443	Permit

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All IP traffic	Any IP Address	Any IP Address	Any	Any	Any	Require security: AES/ SHA-1, certificate authentication

Secure Gateway Policy

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
STA traffic	My IP Address	IP Address of primary server	TCP	Any	80	Require security: AES/ SHA-1, certificate authentication
ICA traffic on port 1494 to primary server	My IP Address	IP Address of primary server	TCP	Any	1494	Require security: AES/ SHA-1, certificate authentication
ICA traffic on port 1494 to secondary servers	My IP Address	IP Address of secondary server	TCP	Any	1494	Require security: AES/ SHA-1, certificate authentication
All TCP/ IP traffic on port 443	Any IP address	My IP Address	TCP	Any	443	Permit

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All IP traffic	Any IP address	Any IP address	Any	Any	Any	Block

Primary Server Policy

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All IP traffic	Any IP address	Any IP address	Any	Any	Any	Require security: AES/ SHA-1, certificate authentication

Secondary Servers Policy

Rule	Source address	Destination address	Protocol	Source port	Destination port	Action
All IP traffic	Any IP address	Any IP address	Any	Any	Any	Require security: AES/ SHA-1, certificate authentication

Third Party Components

The Common Criteria evaluated deployment comprises various third party components including firewalls, Web browsers, virus protection software, and smart cards.

Note: For detailed configuration details, see the relevant manufacturer's documentation.

Firewalls

As shown in the deployment diagram in Common Criteria Evaluated Deployment on page 12, two firewalls are required. Firewall 1 is located between the public network and the DMZ, Firewall 2 is located between the DMZ and the private network.

Note: For details concerning how to configure your firewalls, refer to the manufacturer's documentation.

Firewall 1 (Public Network/DMZ)

Firewall 1 must be configured to allow traffic between the user devices and the servers in the DMZ (Web Interface and Secure Gateway) on TCP port 443 only. The procedure to configure the firewall is dependent on your choice of firewall. The requirements are summarized below:

- Network address translation is used to map the external IP address for the Web Interface and external IP address for the Secure Gateway to the corresponding internal IP addresses
- Allow traffic only from the public network to the DMZ servers on TCP port 443
- Allow new connections to be established only from the public network to the DMZ

Firewall 2 (DMZ/Private Network)

Firewall 2 must be configured to allow IPSec and UDP traffic between the servers in the DMZ (Web Interface and Secure Gateway) and the primary and secondary servers in the private network.

The procedure to configure the firewall is dependent on your choice of firewall. The requirements are summarized below:

- Enable IPSec - IP protocols 50 and 51
- Enable UDP on source port 500 and destination port 500
- Lock down traffic to allow the following connections only:
  - IP address of the Web Interface to/from the IP addresses of the secondary servers
  - IP address of the Web Interface to/from the IP address of the primary server
  - IP address of the Web Interface to/from the IP address of the domain controller
  - IP address of the Secure Gateway to/from the IP addresses of the secondary servers
  - IP address of the Secure Gateway to/from the IP address of the primary server

Web Browsers

A Web browser is required on the user device. The Web browser within the Common Criteria evaluated deployment is Microsoft Internet Explorer, Version 8.0.

Virus Protection Software

The computers hosting the following items must be configured with adequate antivirus software:

- Primary and secondary servers
- Web Interface
- Secure Gateway
- Web plug-in

Anti-virus software of your choice must be installed and configured within the evaluated deployment. The choice of anti-virus software may be dependent on your company's security policy.

Environment Assumptions

This Common Criteria evaluated deployment environment assumes:

- Your organization has the following items in place for all components in the evaluated configuration:
  - Authentication policies
  - File protection settings
  - Secure configuration of any third-party software
- Your organization has policies in place that prevent users from disclosing their passwords.
- Applications are not streamed.
- Applications are published and configured such that they do not act in a malicious manner. These applications do not interact with other applications or maliciously affect published application data or configuration data. This includes maintaining the security state of the published applications according to the user's risk environment.
- Published applications are configured so that it is not possible to "break out" of applications and gain access to operating system functions or other applications. For instructions on how to prevent users from launching unauthorized applications, see Securing Executables with AppLocker on page 78.
- Only administrators have physical access to the server components included in the evaluated configuration.
- Only administrators have access to configuration data on server components of the evaluated configuration.
- User devices included in the evaluated configuration have only trusted third-party software installed. This software must be configured securely according to the risks in the operational environment.
- Secure cryptographic functions used to provide IPSec and TLS are FIPS 140-2 Level 1 compliant.
- Any keys and other secret data that are generated and stored outside the evaluated configuration are managed in accordance with the level of risk.

For details concerning these and other Common Criteria evaluated deployment environment assumptions, refer to the *Common Criteria Security Target for Citrix XenApp for Windows Server 2008 R2*. This document details assumptions such as the physical environment, the password policy used, and the rights and assumptions concerning the administrators.

Chapter 3

Installing the Citrix XenApp Components

Topics:

- *Installing Citrix XenApp*
- *To download and install the web plug-in*

This chapter explains how to install and configure XenApp in the Common Criteria evaluated deployment. XenApp and the required components are installed in the following order:

1. XenApp on the primary and secondary servers
2. The Web Interface
3. The Secure Gateway
4. The web plug-in

Each component is installed on a separate computer as shown in the deployment diagram in Common Criteria Evaluated Deployment on page 12.

Important: To ensure the evaluated configuration cannot be used until all components are ready, the Web Interface and Secure Gateway should not be enabled for use until all other components are in a stable state.

Updates to Citrix Products Included in the Common Criteria Evaluated Configuration

Citrix will, from time to time, issue product updates which may correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators may also opt to subscribe to proactive email alerts about product security vulnerabilities and their associated fixes. These alerts are sent out on a regular basis whenever new fixes are available. Administrators may contact and work with Citrix Support directly if they require additional support in obtaining and deploying any fix. More information about the email alerts system can be found at http://www.citrix.com.

Installing Citrix XenApp

This section explains how to install XenApp on the primary server in the farm.

Review the XenApp Readme for late-breaking issues.

You must be in the Administrators group to install and configure the XenApp software. (Elevating your privilege to local administrator through User Account Control is not a substitute for Administrators group membership.)

Citrix does not recommend installing XenApp on a domain controller.

To ensure availability of the features and functionality of XenApp for Windows Server 2008 R2 to your users, install the most recent version of any plug-ins you use.

When installing roles or role components other than XenApp server, see the role documentation for details about information requested during installation and configuration.

Note: To prepare XenApp for server imaging and provisioning, you can use the XenApp Server Configuration Tool included on the XenApp 6 for Windows Server 2008 R2 installation media. However, the preparation process is streamlined and more effective if you use the updated XenApp Server Configuration Tool, which you can install on the server with CTX124981 (http://support.citrix.com/article/ctx124981) before installing the XenApp server role.

Before Installing XenApp

- Verify the authenticity of the installation media as follows:
  - Compare the shipping details of the Citrix Order Shipment Confirmation email notification to the details of the shipped package. Ensure the shipper tracking number and the purchase order reference number on the package match the emailed details.
  - Upon opening the shipped package, compare the packing list with the materials included in the package. Ensure all the items listed are included and that component packaging, such as shrinkwrapped product boxes or sealed disk envelopes, is intact and free of tampering. Compare the part numbers listed with the included items and ensure they match.
- Review the installation process (wizard-based or command-line) to learn what information you must provide.
- Review the system requirements for the XenApp server and for other roles you plan to install.
  - Wizard-based installations include automatic installation of prerequisite software and required Windows roles.

- For command-line installations, you must install the prerequisite software and Windows roles before initiating XenApp installation. Citrix recommends deploying prerequisites using the Microsoft ServerManagerCmd.exe command or Powershell, which Microsoft provides for Windows operating system roles.

- Ensure the Microsoft Windows Server has the latest Microsoft hotfixes and that the operating system clock has the correct time.
- Prepare for Windows Multilingual User Interface (MUI) support, if needed. The Windows MUI Pack is supported only on the English edition of Windows. Users connecting to XenApp from non-English language plug-ins or agents see their environment and applications in the language that corresponds to their setting, provided the server operating system and applications support it, and the corresponding language packs are installed on the server. While XenApp supports Windows MUI, some XenApp components and features do not display in the non-English language. Follow this sequence:
  a. Before you install XenApp, verify that the Windows Server language option is set to English. (Changing the language option after installing XenApp might cause display issues.) For information, see the Microsoft documentation.
  b. Install the English version of XenApp.
  c. Install the Windows MUI language packs you want to deliver to users, and install any applications required, MUI or native.
- **Important:** By default, the XenApp server installation process creates install logs in the user's temporary directory (%TEMP%). On Windows Server 2008 R2 servers, the session's temporary directory is deleted by default when the server restarts. If you encounter problems during installation or want to preserve those log files, use one of the following options:
  - Copy the logs from the %TEMP% location to a safe place before the server restarts.
  - Before installing the XenApp server role, change your local computer policy to prevent deletion of the temporary directories.
    i. Go to **Start**>**Run**, then type **gpedit.msc**.
    ii. Navigate to **Computer Configuration**>**Administrative Templates**>**Windows Components**>**Remote Desktop Services**>**Remote Desktop Session Host**>**Temporary folders**.
    iii. Verify that **Do not delete temp folder upon exit** is set.
    iv. Restart the server.
  - For a command-line installation, use the **/logfile:***path* option to specify an installation log file in a different directory.

Before Configuring XenApp

- Review the configuration process (wizard-based or command-line) to learn what information you must provide.
  - Decide what to name the server farm.
  - Decide which user account should be initially granted full access to all server farm management tasks.
- If you plan to use the Configuration Logging feature and encrypt the data being logged, you must load the encryption key on servers that join the farm after configuring XenApp but before restarting the server.

When you add subsequent servers to the server farm, you run Setup on the servers and join the existing farm. When you join an existing server farm, you need the name of that server and the logon credentials of a user authorized to access the database.

Installing Citrix License Server and Citrix XenApp on the Primary Server

In the Common Criteria evaluated deployment, the primary server hosts the Citrix License Server. The Citrix License Server must be installed on the primary server in addition to the XenApp server, and the appropriate license files must be installed.

Assigning Farm Administrator Credentials

Citrix administrators manage XenApp server farms. When you install the first server in a new server farm, you specify an initial farm administrator. This user account is automatically configured as a Citrix administrator with full administration rights to all farm management tasks in the Delivery Services Console.

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

You can create administrator accounts with various permission levels. However, within this guide and the Common Criteria evaluated deployment, it is assumed that all administrators have the same (full) administration rights. For more information about creating administrator accounts and assigning farm permissions, see section 2 of the *Citrix XenApp Administration* guide.

To install Citrix XenApp on the primary server

1. Ensure you are logged on to the primary server as a domain administrator and exit all applications.
2. Insert the Citrix XenApp for Microsoft Windows Server 2008 R2 DVD in the primary server's DVD-ROM drive. The Citrix XenApp autorun screen appears.

3. Select **Install XenApp Server**.
   The Server Role Manager launches and checks if any prerequisites and roles are already installed.
4. From the **Server Role Manager** screen, click **Add server roles.**
5. Select **Platinum Edition**.
6. Accept the End User License Agreement.
7. On the **Choose XenApp roles** page, select the following roles:
   - License Server
   - XenApp

   Click **Next**.
   The **Choose role subcomponents** page appears.
8. Under **XenApp**>**Optional Components**, select **XML Service IIS Integration** and then click **Next**.
   The Citrix online plug-in and Citrix offline plug-in are installed automatically when you install the XenApp role. These plug-ins do not appear in the components lists, and you cannot disable these installations during a wizard-based installation.
9. Review the prerequisites summary and then click **Next**.
10. Review the **Ready to install** summary, which lists the selected roles and subcomponents to be installed or prepared, and then click **Install**.
    A display indicates installation progress and the result.

    Important: When installing the XenApp role, the IMA Service is not started, nor are any configuration options set, such as creating or joining a farm and data store database information.

After the installation result displays and you click **Finish**, the Server Configuration Task list appears. Under **XenApp**, click **Configure** to begin the server configuration process.

To configure Citrix XenApp on the primary server

1. In the Server Role Manager task list, under **XenApp**, click **Configure**.
   The Server Configuration Tool launches.
2. Choose **Create a new server farm**.
3. On the **Enter basic Information about the new server farm** page, supply the following information:
   - Enter a farm name. Farm names can be up to 32 characters and can include spaces.
   - Specify the domain and username for a user who will be the first Citrix administrator. The administrator has full permissions to the farm and can create additional administrator accounts.

Click **Next**.

4. On the **Enter Citrix License Server information** page, enter the fully qualified address of this server, the one on which you have just installed the license server. Leave the default port at 27000 and click **Next**.
5. On the **Choose a database for the new server farm** page, select **New database**. This installs SQL Server Express 2008 as the data store database type.
6. On the **Enter database credentials and test database connection** page, specify the database credentials. Specify the user name in the form <DBMACHINE>\<USER> or <DOMAIN>\<USER>.

   SQL Server Express requires an existing Windows account, but it does not need to be a server or system administrator. The XenApp Server Configuration tool adds two database administrators to SQL Server Express: (local)\administrators and the supplied credentials for the local or domain user.

   Click **Next**.
7. On the **Configure shadowing** page, select **Prohibit shadowing of user session on this server** and click **Next**.
8. On the **Specify advanced server settings** page, click **Next** to accept the default settings for Zone, XML Service, Online plug-in, and Remote Desktop Users.
9. On the **Ready to configure** page, review the configuration information you specified and then click **Apply.**
10. After configuration completes, click **Finish**.

Before clicking **Reboot**, configure the License Server.

To configure the license server

1. Return to Citrix XenApp 6 for Windows Server 2008 R2 autorun screen, and in the Server Configuration Task list, under **License Server**, click **Configure**.
2. In the License Server Configuration tool, set your administrator password for your license server. Do not change any of the other default settings. Click **OK**.

After setting the administrator password and completing the remaining Server Configuration tasks, obtain and add your license file to your license server according to section 2.5 of the *Citrix Licensing 11.6.1* guide.

After configuring the license server, restart the primary server and perform the following tasks:

- Secure the Secure Ticket Authority and XML Service.
- Ensure the SQL Server Express database can communicate with the secondary server.
- Disable certain XenApp features using policies. See Disabling XenApp Features with Policies on page 75 for instructions.

Securing the Secure Ticket Authority and XML Service

Following the installation and configuration of XenApp on the primary server, you must change the default directory in which the STA logs are stored, so that unauthorized users cannot view STA logs. You must also restrict access to the STA and specify a log directory for the STA.

Before you begin this procedure, you must know the IP addresses for the servers on which you want to install the Secure Gateway and the Web Interface.

To change the STA log directory

1. Create a new directory, *%systemdrive%***stalog**.
2. Open the file CtxSta.config, which is stored in %systemdrive%\Inetpub\Scripts. Amend the LogDir line in the file to read:

   ```
   LogDir=C:\stalog\
   ```

   where *C:*\ = %systemdrive%\
3. Save the changes and close the file.

To restrict access to the STA and XML service

This procedure requires that the **IP Address and Domain Restrictions** role service be installed on the primary server. This role service is enabled when the **Web Server (IIS) Support** service is added, during configuration of the Application Server role. See Installing the Server Roles on page 17 for more information.

1. Launch the Internet Information Services (IIS) Manager (**Start**>**Administrative Tools**>**Internet Information Services (IIS) Manager**).
2. From the **Connections** pane, expand the primary server computer name (local computer) node and select **Sites**>**Default Web Site**>**Scripts**.
3. In the middle pane, under **IIS**, double-click **IP Address and Domain Name Restrictions**.
   The **IP Address and Domain Name Restrictions** page appears in the middle pane.
4. From the Actions pane, click **Edit Feature Settings**.
   The **Edit IP and Domain Restrictions Settings** dialog box appears.
5. In the **Access for unspecified clients** drop-down list, select **Deny** and click **OK**.
   You are returned to the **IP Address and Domain Restrictions** page of the Internet Information Services (IIS) Manager.
6. From the Actions pane, click **Add Allow Entry**.
7. At the **Add Allow Restriction Rule** dialog box, select **Specific IP address** and enter the IP address for the Web Interface server. Click **OK**.
   You are returned to the **IP Address and Domain Restrictions** page of the Internet Information Services (IIS) Manager.
8. From the Actions pane, click **Add Allow Entry**.

9. At the **Add Allow Restriction Rule** dialog box, select **Specific IP address** and enter the IP address for the Secure Gateway server. Click **OK.**
10. Close the Internet Information Services (IIS) Manager window.

Following the configuration of the STA, you can add more servers to the farm according to the procedures described in Installing Citrix XenApp on the Secondary Servers on page 36.

To enable communication between SQL Server Express and the secondary servers

1. Launch the SQL Server Configuration Manager (**Start**>**Microsoft SQL Server 2008**>**Configuration Tools**>**SQL Server Configuration Manager**).
   The **Sql Server Configuration Manager** window appears.
2. In the left pane, expand the **SQL Server Network Configuration (32bit)** node and then select the **Protocols for CITRIX_METAFRAME** node.
3. In the right pane, right-click **TCP/IP** and select **Properties**.
   The **TCP/IP Properties** dialog box appears.
4. On the **IP Addresses** tab, locate the entry for the static IPv4 Ethernet setting on the server's primary network adapter.
5. In **Enabled**, select **Yes**.
6. In **TCP Dynamic Ports**, clear all values.
7. In **TCP Port**, enter **1434**.
8. Scroll down to the **IPAll** entry and clear the values in **TCP Dynamic Ports**.
9. In **TCP Port**, enter **1434**.
10. Click **OK**.
    A warning message appears. Click **OK**.
11. In the left pane of the **Sql Server Configuration Manager** window, select the **SQL Server Services** node.
12. In the right pane, right-click **SQL Server (CITRIX_METAFRAME)** and select **Restart**.
13. Close the **Sql Server Configuration Manager** window.

Installing Citrix XenApp on the Secondary Servers

This section explains how to install Citrix XenApp on the secondary servers in the farm.

In the Common Criteria evaluated deployment, the secondary servers in the farm require XenApp only. The procedure to add more secondary servers to the farm is similar to the procedure to creating the primary server. However, you do not need to enter the farm details, install the License Server, or create the database.

The SQL Server Express database is created when you install the primary server in the farm. Additional servers connect to the first server using TCP port 2512. If you want to use another port, see sections 6.8.1 and 10.11 of the *Citrix XenApp Administration* guide.

When you add subsequent secondary servers to the server farm, you run autorun on the servers and join the existing farm. When you join an existing server farm, you need the FQDN and the farm administrator credentials, as you specified during the installation of the primary server. After you join the farm, you ensure the port used on the secondary servers is static by configuring the file DSN for the datastore.

XenApp autorun installs the Secure Ticket Authority (STA) and the XML Service automatically on all servers. However, the primary server is the only server in the farm with the STA and XML Service enabled. On the secondary servers, the STA and XML Service must be disabled by blocking traffic on port 80. This is achieved by creating a security policy that specifies only the ports required to be opened for the evaluated configuration and closing all others. For information about these ports, see the **Network Security Rules** section of Windows Server 2008 R2 Security Configuration Wizard on page 60.

To install XenApp on secondary servers

1. Ensure you are logged on to the secondary server as a domain administrator and exit all applications.
2. Insert the Citrix XenApp 6 for Microsoft Windows Server 2008 R2 DVD in the secondary server's DVD-ROM drive. The XenApp setup screen appears.
3. Click **Install XenApp Server**. The Server Role Manager launches and checks if any roles are already installed.
4. Click **Add server roles**.
5. Click **Platinum Edition**.
6. Accept the license agreement.
7. On the **Choose XenApp roles** page, choose only **XenApp**.
8. On the **Choose role subcomponents** page, ensure **XML Service IIS Integration** is selected.
9. Review the prerequisites summary, which indicates software that is automatically installed for XenApp Management.
10. Review the **Ready to install** summary and click **Install.**
    A display indicates installation progress and the result.

    Important: When installing the XenApp role, the IMA Service is not started, nor are any configuration options set, such as creating or joining a farm and data store database information.

After the installation result displays, click **Finish**. The Server Configuration Tasks list appears, allowing you to proceed with joining the server to the XenApp farm.

To join secondary servers to the XenApp farm

1. In the Server Configuration Tasks list, click **Configure**.
   The Server Configuration Tool launches.
2. Click **Join an existing farm**.
3. On the **Choose a database** page, ensure **Existing Microsoft SQL Server Express database** is selected, then click **Next.**
4. On the **Configure the connection to the existing server farm** page, type only the name of your primary XenApp server (not the FQDN) and then click **Next**. Enter the database credentials you used when you installed the primary XenApp server.
5. On the **Enter database credentials and test database connection** page, click **Test Connection**.
   - If you see the message **Test Completed Successfully**, click **OK** and then click **Next.**
   - If you do not see the message **Test Completed Successfully**, ensure your primary server is online and test again.
6. On the **Shadowing** page, select **Prohibit shadowing of user session on this server** and click **Next**.
7. On the **Specify advanced server settings** page, ensure the **Use the global farm settings for the license server** setting is selected and then click **Next**.
8. Review the **Ready to configure** summary page and then click **Apply.**
9. After configuration completes, click **Finish**.
   You are returned to the Server Configuration Tasks list.
10. On the Server Configuration Tasks list, click **Reboot** and restart the server.

After the server restarts, log on as an administrator and perform the following tasks:

- Configure the file DSN for the farm data store. See To configure the data store DSN on page 39 for instructions.
- Ensure the STA and XML Service, installed by default on the secondary servers, are disabled by blocking traffic on port 80. This is achieved by creating a security policy that specifies only the ports required to be opened for the evaluated configuration and closing all others. For information about these ports, see the **Network Security Rules** section of Windows Server 2008 R2 Security Configuration Wizard on page 60.
- Disable certain XenApp features using policies. See Disabling XenApp Features with Policies on page 75 for instructions.

To configure the data store DSN

1. Launch the ODBC Data Source Administrator (**Start**>**All Programs**>**Administrative Tools**>**Data Sources (ODBC)**).
   The **ODBC Data Source Administrator** window appears.
2. On the File DSN tab, navigate to the `%SYSTEMDRIVE%\Program Files (x86)\Citrix\Independent Management Architecture` folder.
3. Select the **mf20** file and click **Configure**.
   The **Microsoft SQL Server DSN Configuration** wizard appears.
4. On the first page of the wizard, accept the default values and click **Next**.
5. Click **Client Configuration**.
   The **Add Network Library Configuration** window appears
6. Clear the **Dynamically determine port** check box and, in the **Port number box**, enter **1434** Click **OK** to return to the wizard.
7. Click **Next** and then click **Next** again.
8. Click **Finish**.
   The **ODBC Microsoft SQL Server Setup** dialog box appears.
9. Click **Test Data Source**.
   The test completes successfully.
10. Click **OK** to close the confirmation message box.
11. Click **OK** to close the **ODBC Microsoft SQL Server Setup** dialog box.
12. Click **OK** to close the **ODBC Data Source Administrator** window.
13. Launch the **Services** console (**Start**>**All Programs**>**Administrative Tools**>**Services**).
14. Right-click the **Citrix Independent Management Architecture** service and select **Restart**.
15. Close the **Services** console.

Installing the Microsoft File Checksum Integrity Verifier Utility

Before you install the Web Interface or web plug-in components on computers in the evaluated configuration, download and install the Microsoft File Checksum Integrity Verifier utility according to the instructions in Microsoft KB article 841290 (http://support.microsoft.com/kb/841290). Citrix recommends using this tool to verify the MD5 checksums that accompany these components. Before you install the utility, be sure to check the digital signature of the downloaded file to verify its integrity.

Perform this procedure on the following computers in the evaluated configuration:

- Web Interface server

- User device

1. Ensure you are logged onto the computer as an administrator and exit all applications.
2. In Windows Explorer, create a new folder called **FCIV** in which to store the downloaded utility.
3. Launch Internet Explorer and navigate to Microsoft KB article 841290 (http://support.microsoft.com/kb/841290).
4. Scroll down to the **Introduction** section and, under **Installation**, click **Download the File Checksum Integrity Verifier utility now**.
   The **File Download** dialog box appears, prompting you to run the package installer or save the file.
5. Click **Save** and then select the FCIV folder you created.
6. When the download finishes, close the **File Download** dialog box, if open.
7. To verify the digital signature of the downloaded file, perform the following actions:
   a. In Windows Explorer, in the **FCIV** folder, right-click the file **Windows-KB841290-x86-ENU.exe** and then click **Properties**.
      The **Properties** dialog box appears.
   b. Click the **Digital Signatures** tab and then click **Details** to verify the file's digital signature information.
   c. When you are finished verifying the digital signature, click **OK** and then click **OK** again.
8. In Windows Explorer, in the **FCIV** folder, double-click the **Windows-KB841290-x86-ENU.exe** file to begin installation.
9. Click **Run** and then click **Yes** to accept the license agreement.
   The installer prompts you to select a location for the extracted files.
10. Click **Browse**, select the **FCIV** folder, and then click **OK**.
    When the installer is finished, a message appears to indicate the extraction is complete. Click **OK**.

After you install the Microsoft File Checksum Integrity Verifier utility, you can download and install the Web Interface and web plug-in components.

Installing Web Interface

Installation Overview

The evaluated configuration includes Web Interface 5.4. This component is available as a secure download from the Citrix Web site. Before installing the Web Interface, note the following prerequisites:

- If smart cards are used, the Web Interface must be in the same domain as the smart card enrollment station

- The server and root certificate must be installed on the server running the Web Interface
- The FQDN of the server running the Web Interface must match the FQDN that appears in the subject box of the server certificate installed on this computer
- Install the Web Server (IIS) server role, which includes Microsoft Internet Information Services (IIS) and ASP.NET services, on the server running the Web Interface

Note: For further information concerning the Web Interface and the installation options, see the *Web Interface Administration* guide.

Installing the Web Interface Management Console

The installation of the Web Interface requires installing the Web Interface Management console so that you can administer the sites running under the Web Interface. The Web Interface Management console snaps into the Microsoft Management Console (MMC) and provides a central location to easily manage your deployment. The Web Interface Management console is installed automatically when you install the Web Interface.

To download and install the Web Interface

Before you install Citrix Web Interface 5.4, download and install the Microsoft File Checksum Integrity Verifier utility. Citrix recommends using this tool to verify the MD5 checksum that accompanies the Web Interface package. For instructions on downloading and installing the File Checksum Integrity Verifier utility, see Installing the Microsoft File Checksum Integrity Verifier Utility on page 39.

Additionally, Web Interface 5.4 is available as a secure download from the Citrix Web site. To access the secure downloads area, be sure you have your My Citrix credentials handy.

1. Ensure you are logged on to the server as an administrator and exit all applications.
2. Launch Internet Explorer and navigate to the Citrix Downloads page (http://www.citrix.com/English/ss/downloads/index.asp).
3. In the **My Citrix** panel on the left side of the page, enter your My Citrix credentials and click **Log In**.
   The Citrix Downloads page displays the My Tools panel and the address bar displays the HTTPS URL, indicating you have entered a secure area.
4. To verify the identity of the Web site, click the lock icon next to the address bar.
   A security report appears, identifying the Web site and verifying the connection to the server is encrypted.
5. Navigate to the download page for the Web Interface 5.4 component (https://www.citrix.com/English/ss/downloads/details.asp?downloadId=2305426).
6. Locate the **Web Interface 5.4 for Windows** component and then click **Download**.
   The **Download Agreement** displays in a separate window.

7. Select the checkbox to indicate your acceptance of the agreement and then click **Accept**.
   The Citrix Download Manager appears. Click **Click to download your file now** to begin the download.
8. If the Download Manager browser add-on is not already installed on the server, perform the following actions:
   a. On the **Download Manager** window, click the Information Bar and then click **Install This Add-on for All Users on This Computer**.
   b. Click **Click to download your file now** and then click **Install** to install the Download Manager component.
9. Select a location (e.g., C:\Downloads) to save the Web Interface package and then click **Save**.
   When the download finishes, click **Exit** and then click **Yes** to close the **Download Manager** window.
10. To verify the download, perform the following actions:
    a. Locate the file **WebInterface.exe** that you just downloaded.
    b. Open a command prompt and type the following string:
       ```
       C:\FCIV\fciv.exe C:\path\to\WebInterface.exe
       ```
       where *C:\path\to* is the file location of the Web Interface package; for example, C:\Downloads\WebInterface.exe.

    The File Checksum Integrity Verifier utility generates an MD5 checksum and displays it in the **Command Prompt** window.
11. Compare the generated value with the MD5 checksum posted on the My Citrix download page to verify the integrity of the download.
12. After verifying the download, double-click the file to begin installation.
    After the installation finishes, a message appears, indicating the Web Interface has been installed successfully. Click **Finish** to close this message.

To configure the Web Interface

1. From the **Start** menu, click **All Programs**>**Citrix**>**Management Consoles**>**Citrix Web Interface Management Console**.
   The Citrix Web Interface Management console appears.
2. In the Actions pane, click **Create Site**. The **Create Site** dialog box appears.
3. On the **Select Site Type** page, select **XenApp Web**, and click **Next**.
4. On the **Specify IIS Location** page, leave the default values and click **Next**.
5. On the **Specify Point of Authentication** page, accept the default values and click **Next**.
6. On the **Confirm Settings for New Site** page, click **Next**.

A progress bar appears as the wizard creates a site.

7. When the site is successfully created, ensure the **Configure this site now** check box is selected and click **Next**.
8. On the **Specify Server Farm** page, type the name of your farm in the **Farm name** box and click **Add**. The farm name must be the same as the farm name that you specified when you installed XenApp.
9. In the **Add Server** dialog box that appears, type the FQDN of the primary server and click **OK**.
10. On the **Specify Server Farm** page, do not change the values for **XML Service port** or **Transport type**. Click **Next.**
11. On the **Configure Authentication Methods** page, accept the default values and click **Next**.
12. On the **Domain Restriction** page, ensure **Allow any domains** is selected and click **Next**.
13. On the **Specify Logon Appearance** page, select **Full** and then click **Next**.
14. On the **Select Published Resource Type** page, ensure **Online** is selected and then click **Next.**
15. On the **Confirm Settings** page, click **Finish**. The new site is listed in the Site Summary of the Web Interface Management Console.

If you configure the Web Interface site for explicit authentication, ensure that users are not allowed to change their logon passwords through the Web Interface site. For instructions, see Enabling Explicit Authentication on page 54.

Installing Secure Gateway

Installing the Secure Gateway requires performing the following tasks:

- Installing the server prerequisites
- Installing the Secure Gateway
- Configuring the Secure Gateway server after finishing installation

Configuration wizards for each Secure Gateway component are launched when installation is complete. Each configuration wizard guides you through configuration tasks and provides context-sensitive help describing the task and values you need to enter.

Prerequisites

A server authentication and root certificate must be installed on the server.

Note: The Secure Gateway is designed to discover and verify the existence of the other Secure Gateway components during configuration. When you configure the Secure Gateway, a check is performed to verify that the primary server running the STA is functional. If a required component is not found, the Secure Gateway Service

may fail to start. It is, therefore, important to follow the recommended installation sequence, as documented in this chapter.

To install the Secure Gateway

1. Ensure you are logged on to the server as an administrator and exit all applications.
2. Insert the Citrix XenApp for Microsoft Windows Server 2008 R2 DVD into the server's DVD-ROM drive. The Citrix XenApp autorun screen appears.
3. Select **Install XenApp Server**. The Server Role Manager launches and checks if any roles are already installed.
4. Select **Add Server Roles**.
5. Select **Platinum Edition**.
6. Accept the End User License Agreement.
7. On the **Choose XenApp Roles** page, select **Secure Gateway** and click **Next**. The **Choose role subcomponents** page appears.
8. Click **Next**.
9. Review the **Ready to install** summary and click **Install**. A display indicates installation progress and the result.
10. After the installation result appears, click **Finish**. The Server Configuration Tasks list appears.
11. From the Server Configuration Tasks list, under **Secure Gateway**, click **Install**.
12. On the **Welcome to the Secure Gateway 3.2 Setup** page, click **Next**.
13. On the **License Agreement** page, read the agreement, select **I accept the license agreement** and click **Next**.
14. On the **Installation Mode** page, ensure that **Secure Gateway** is selected and click **Next**.
15. On the **Destination Folder** page, accept the default settings (C:\Program Files (x86)\Citrix\Secure Gateway\) and click **Next**.
16. On the **Service Account** page, in the **Account** box, select **NETWORK SERVICE**. The **Password** box becomes unavailable.
17. Click **Next**.
18. On the **Ready to Install the Secure Gateway** page, click **Next**. An **Updating System** screen appears while the installation of Secure Gateway finishes.
19. On the **Secure Gateway has been successfully installed** page, click **Finish**. The **Launch Secure Gateway Configuration Wizard** dialog box appears.

At the **Launch Secure Gateway Configuration Wizard** dialog box, click **OK** to begin the server configuration process.

To configure the Secure Gateway

1. On the **Welcome to the Secure Gateway Configuration wizard** page, click **OK**.
2. On the **Secure Gateway configuration level** page, select **Advanced** and click **Next**.
3. On the **Select a server certificate** page, select the server certificate to be used by the Secure Gateway and click **Next**.
4. On the **Configure secure protocol settings** page, perform the following actions:
   a. Select the following options:
      - Transport Layer Security (TLSv1)
      - GOV
   b. Click **Next**.
5. On the **Configure inbound client connections** page, perform the following actions:
   a. Ensure the **Monitor all IPv4 addresses** box is selected.
   b. Leave the **TCP port** box set to **443**.
   c. Click **Next**.
6. On the **Configure outbound connections** page, ensure that **No outbound traffic restrictions** is selected and click **Next**.
7. On the **Servers running the STA** page, click **Add**.
8. At the Secure Ticket Authority (STA) details dialog box, perform the following actions:
   a. Type the FQDN of the primary server in the **FQDN** box.
   b. Leave the **Path** box value set to **/Scripts/CtxSTA.dll**.
   c. Leave the **Use default** check box selected.
   d. Click **OK**.

   A connection is made to the primary server running the STA and the dialog box closes. The **Servers running the STA** page updates with an Identifier and the FQDN of the primary server. Click **Next**.
9. On the **Connection parameters** page, ensure the **No connection timeout** and **Unlimited check boxes** are not selected and click **Next**.
10. On the **Logging exclusions** page, click **Next**.
11. On the **Details of the server running the Web Interface** page, in the **Access options** section, click **Direct** then click **Next**.
12. On the **Logging parameters** page, ensure that **Warning, error, and fatal events** is selected and click **Next**.

13. On the **Secure Gateway configuration complete** page, ensure the **Restart Secure Gateway** check box is selected and click **Finish**.
The **Secure Gateway configuration complete** page closes.

To download and install the web plug-in

Before you install the web plug-in, download and install the Microsoft File Checksum Integrity Verifier utility. Citrix recommends using this tool to verify the MD5 checksum that accompanies the web plug-in package. For instructions on downloading and installing this utility, see Installing the Microsoft File Checksum Integrity Verifier Utility on page 39.

Additionally, the web plug-in is available as a secure download from the Citrix Web site. To access the secure downloads area, be sure you have your My Citrix credentials handy.

1. Ensure you are logged onto the user device as administrator and exit all applications.
2. Launch Internet Explorer and navigate to the Citrix Downloads page (http://www.citrix.com/English/ss/downloads/index.asp).
3. In the **My Citrix** panel on the left side of the page, enter your My Citrix credentials and click **Log In**.
The Citrix Downloads page displays the My Tools panel and the address bar displays the HTTPS URL, indicating you have entered a secure area.
4. To verify the identity of the Web site, click the lock icon next to the address bar.
A security report appears, identifying the Web site and verifying the connection to the server is encrypted.
5. Navigate to the download page for the Online Plug-in 12.1 component (http://www.citrix.com/English/ss/downloads/details.asp?downloadId=2305087&productId=186&c1=sot2755).

   Note: You must be logged in to My Citrix in order to access the download page.

6. Locate the **Citrix Online plug-in - Web** component and then click **Download**.
The **Download Manager** appears in a separate window.
7. Click **Click to download your file now**.
8. If the Download Manager browser add-on is not already installed on the user device, perform the following actions:
   a. On the **Download Manager** window, click the Information Bar and then click **Install This Add-on for All Users on This Computer**.
   b. Click **Click to download your file now** and then click **Install** to install the Download Manager component.
9. Select a location (e.g., C:\Downloads) to save the web plug-in package and then click **Save**.

When the download finishes, click **Exit** and then click **Yes** to close the **Download Manager** window.

10. To verify the download, perform the following actions:
    a. Locate the file **CitrixOnlinePluginWeb.exe** that you just downloaded.
    b. Open a command prompt and type the following string:
       ```
       C:\FCIV\fciv.exe C:\path\to\CitrixOnlinePluginWeb.exe
       ```
       where *C:\path\to* is the file location of the web plug-in package; for example, C:\Downloads\CitrixOnlinePluginWeb.exe.

    The File Checksum Integrity Verifier utility generates an MD5 checksum and displays it in the **Command Prompt** window.
11. Compare the generated value with the MD5 checksum posted on the My Citrix download page to verify the integrity of the download.
12. After verifying the download, double-click **CitrixOnlinePluginWeb.exe** to begin installation.
    When the web plug-in is installed, a message appears, indicating the plug-in has been installed successfully. Click **OK** to close this message.

Chapter 4

Configuring Citrix XenApp

Topics:

- *Configuring the Servers Running Citrix XenApp*
- *Configuring the Web Interface*
- *Installing Single Sign-on Components*

This chapter describes how to configure the Common Criteria evaluated deployment. For further details concerning the procedures and products, see the relevant administrator's guides.

Configuring the Servers Running Citrix XenApp

This section describes how to configure the primary and secondary servers running Citrix XenApp. Configuring these servers requires that you perform the following set up and configuration tasks:

- Configure and run discovery in the Delivery Services Console
- Publish applications
- Remove or disable unnecessary Citrix user accounts
- Prevent users from launching unauthorized applications
- Disable redirection of client devices, audio, COM & LPT ports, virtual channels, and default printing.

The last three configurations are for security purposes. Citrix assumes that you will perform these tasks as part of your Common Criteria evaluated deployment.

This evaluated deployment includes a procedure for Removing and Disabling Citrix User Accounts on page 85. During XenApp installation, several anonymous user accounts and two generic Citrix accounts are created. This deployment requires that the anonymous accounts be removed and the generic Citrix accounts be disabled on both XenApp servers.

This evaluated deployment also includes a procedure for Securing Executables with AppLocker on page 78. This procedure stops users from launching unauthorized applications during a XenApp session. For more information, see the *Common Criteria Security Target for Citrix XenApp for Windows Server 2008 R2*.

Finally, this evaluated deployment also includes a procedure for Disabling XenApp Features with Policies on page 75. As this procedure involves applying a XenApp policy to the primary and secondary servers through Group Policy, you can perform this procedure as you are configuring the group policy for the deployment.

Note: The Common Criteria evaluated deployment covers only the publishing of applications and not the publishing of desktops, content, or streaming applications.

Running Discovery

After you start the Delivery Services Console, but before you can use it to manage the items in your deployment, you must configure and run discovery. Discovery is an important console operation that checks for items (such as devices or applications) that were added to or removed from your Citrix environment. Appropriate changes are then made to the console tree.

You must configure and run discovery on either the primary or secondary server before you can publish applications.

To run Discovery using the Delivery Services Console

1. Ensure you are logged on to the server as a domain administrator.
2. Open the Delivery Services Console (**Start > All Programs > Citrix > Management Consoles > Delivery Services Console**).
   The **Initializing the Citrix Delivery Services Console** progress dialog box appears and then the **Configure and run discovery** wizard appears.
3. On the **Welcome** page, select the **Skip this screen in future check box** and click **Next**.
4. On the **Select Products or Components** page, ensure only the following products or components selected:
   - **Citrix Resources**
   - **Citrix XenApp**

   Click **Next**.
5. On the **Select Servers** page, click **Add Local Computer** and click **Next**.
6. On the **Preview Discovery** page, click **Next**.
   The **Discovery Progress** wizard screen appears displaying a **Discovering** progress bar.
7. When the **Discovery Progress** page displays a **Discovery completed** message, click **Finish**. The **Configure and run discovery** wizard closes.

After running discovery, you can publish applications.

Publishing Applications

This section provides an overview of how to publish applications using default options. For detailed instructions and a description of the options, see section 3.1.2 of the *Citrix XenApp Administration* guide.

To publish an application

1. Verify the location of the application you want to publish.
2. In the left pane of the console, select **Citrix Delivery Services Console > Citrix Resources > XenApp**, then expand and select the node of *your farm name*.
3. Select the **Applications** node and, from the **Actions** pane, select **Publish application**. The **Publish Application** wizard opens.
4. On the **Welcome** page, select the **Skip this screen in the future** check box and click **Next**.
5. On the **Name** page, enter the **Display name** and **Application description** for the published application and click **Next**.
6. On the **Type** page, perform the following actions:

a. In the **Choose the type of application to publish** section, leave the **Application** option selected.

b. In the **Application type** section, leave the **Accessed from a server** option selected.

c. Click **Next**.

7. On the **Location** page, perform the following actions:

a. In the **Command line** area, click **Browse** and then locate the executable file (.exe) for the application you want to publish. Select the executable file and then click **Open**.
The path to the executable appears in the **Command line** box and a path for the default working directory automatically appears in the **Working directory** box. Leave the path that appears in the **Working directory** box unedited.

b. Click **Next**.

8. On the **Servers** page, click **Add**.

9. In the **Select Servers** dialog box, select the server(s) to which you want to publish the application. Click **Add** and then click **OK**.
You are returned to the **Servers** page. Click **Next**.

10. On the **Users** page, perform the following actions:

a. Leave the **Allow only configured users** option selected.

b. Leave the **Select directory type** drop-down list set to **Citrix User Selector**.

c. Click **Add**.
The **Select Users or Groups** dialog box appears.

d. Select your account authority, in this case the Windows Server 2008 Active Directory domain you created for this environment, from the **Look in** drop-down list. If prompted, enter your administrator credentials to connect to the account authority.

> **Note:** 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.

e. Select the **Show users** check box.

f. Double-click the **Users** group, select the users you want to add, if applicable, and click **Add**. Click **OK**.
The user accounts you select are listed in the **Configured users** list on the **Users** page.

11. On the **Users** page, click **Next**.

12. On the **Shortcut presentation** page, click **Next**.

13. On the **Publish immediately** page, click **Finish**.

14. Close the **Citrix Delivery Services Console** window.

To remove a published application

1. In the left pane of the Delivery Services Console, select the **Applications** node.
2. In the middle pane of the console, select the published application you want to remove.
3. From the **Actions** pane, click **Delete application**.
   A warning message appears, asking you to confirm removal of the selected application. Click **Yes**.
4. Close the **Citrix Delivery Console** window.

Configuring the Web Interface

The Common Criteria evaluated deployment can be configured to allow users to log on to Citrix XenApp using either explicit credentials (user name and password) or smart card.

Do not configure the Common Criteria evaluated deployment to allow a mix of authentication methods. Users must log on using explicit credentials or smart card.

This section describes how to configure both authentication options as well as how to enable support for the Secure Gateway.

Enabling Smart Card Authentication

You must ensure the Windows Directory Service Mapper is enabled on the computer running the Web Interface. Web Interface authentication uses Windows domain accounts; that is, user name and password credentials. However, certificates are stored on smart cards as User Principal Names (UPNs). The Directory Service Mapper uses Windows Active Directory to map a UPN to a Windows domain account.

To enable the Windows Directory Service Mapper on IIS

Before performing this task, ensure the IIS Client Certificate Mapping Authentication role service is not installed for the Web Server (IIS) role.

1. Ensure you are logged on to the server running the Web Interface as a domain administrator.
2. Launch the Internet Information Services (IIS) Manager (**Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**).
   The **Internet Information Services (IIS) Manager** window appears.
3. From the **Connections** pane, expand the ***computer name*** **(local computer)** node, expand the **Sites** node, and then select **Default Web Site**.
4. From the middle pane, under the **IIS** section, double-click **Authentication**.
5. On the **Authentication** page, enable the following authentication methods:
   - Active Directory Client Certificate Authentication

- Anonymous Authentication
- Windows Authentication

6. Close the **Internet Information Services (IIS) Manager** window.

To enable users to authenticate using smart cards

1. Ensure you are logged on to the server running the Web Interface as a domain administrator.
2. Start the Web Interface Management console (**Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management Console**).
3. In the middle pane, under **Site Summary**, select the **XenApp Web site (https://** ***FQDN of Web Interface*****/Citrix/*****Name of XenApp Web Site*****)**.
4. In the **Actions** pane, click **Configure site**.
5. In the **Actions** pane, click **Authentication Methods**.
6. At the **Configure Authentication Methods** dialog box:
   a. Clear the **Explicit** check box.
   b. Click the **Smart card** check box to allow users to authenticate to the Web Interface using a smart card.
   c. Click **OK**.
7. Close the **Citrix Web Interface Management** window.

Enabling Explicit Authentication

By default, users are required to log on explicitly to the Web Interface. Users must have a user account and supply a user name and password to log on.

You can change the explicit authentication settings using the Web Interface Management console. For example, you can configure whether or not users are allowed to change their logon passwords within a Web Interface session.

To enable explicit authentication to the Web Interface

1. Ensure you are logged on to the server running the Web Interface as a domain administrator.
2. Start the Web Interface Management console (**Start > All Programs > Citrix > Management Consoles > Citrix Web Interface Management**).
3. In the middle pane, under **Site Summary**, select the **XenApp Web site (https://** ***FQDN of Web Interface*****/Citrix/*****Name of XenApp Web Site*****)**.
4. In the **Actions** pane, click **Configure site**.
5. In the **Actions** pane, click **Authentication Methods**.
6. At the **Configure Authentication Methods** dialog box, perform the following actions:

a. Click the **Explicit** check box to force users to supply a user name and password to log on to the Web Interface.

b. Ensure the **Smart card** check box is cleared.

7. At the same **Configure Authentication Methods** dialog box, click **Properties**.
The **Properties** dialog box appears.
8. In the left pane of the **Properties** dialog box, under **Explicit**, select **Authentication Type**.
9. Ensure both of the following options are selected:
   - **Windows or NIS (UNIX)**
   - **Domain user name and UPN**
10. In the left pane of the **Properties** dialog box, select **Password Settings** and verify the **Allow users to change passwords** checkbox is cleared.
11. Click **OK**.
The **Properties** dialog box closes. You are returned to the **Configure Authentication Methods** dialog box.
12. In the **Configure Authentication Methods** dialog box, click **OK**.
The **Configure Authentication Methods** dialog box closes.
13. Close the **Citrix Web Interface Management** window.

Configuring Secure Gateway Support

You must configure the Web Interface for Secure Gateway support. This section explains configuring Secure Gateway support using the Web Interface Management console.

To configure the Web Interface to support Secure Gateway

1. Ensure you are logged on to the server running the Web Interface as a domain administrator.
2. Start the Web Interface Management console (**Start > All Programs > Citrix > Management Consoles > Web Interface Management**).
3. In the middle pane, under **Site Summary**, select the **XenApp Web site (https://** ***FQDN of Web Interface*****/Citrix/XenApp)**.
4. In the Actions pane, click **Configure Site**.
5. In the Actions pane, click **Secure Access**.
The **Edit Secure Access Settings** dialog box appears.
6. From the **Specify Access Methods** page:
   a. Select the existing **Default** entry.
   b. Click **Edit**.

c. From the **Edit the Default Route for all User Devices** dialog box, in the **Access Method** drop-down list, select **Gateway Direct** and click **OK**.

d. From the **Specify Access Methods** page, click **Next**.

7. From the **Specify Gateway Settings** page:

a. Specify the Fully Qualified Domain Name (FQDN) of the Secure Gateway server in the **Address (FQDN)** box. This must match what is on the certificate installed on the Secure Gateway server.

b. Ensure the **Port** box, which contains the Secure Gateway port number, is set to 443.

c. Ensure the **Enable session reliability** check box is cleared.

d. Click **Next**.

8. From the **Specify Secure Ticket Authority Settings** page:

a. Click **Add**.

b. In the **Add Secure Ticket Authority URL** dialog box that appears, type the STA URL for the primary server. For example: http://*FQDNServerName*/scripts/ctxsta.dll, where *FQDNServerName* is the FQDN of the primary server.

c. Click **OK**.

9. Click **Finish** to close the **Edit Secure Access Settings** dialog box.

10. Close the **Citrix Web Interface Management** window.

Installing Single Sign-on Components

If Citrix Single Sign-on is part of your deployment, install Single Sign-on components before moving on to securing the deployment, which is a requirement of this evaluated deployment. When installing these components, ensure the Single sign-on component of the Delivery Services Console is installed on the primary XenApp server. See the *Citrix Single Sign-on Administration* guide for information about installing and configuring Single Sign-on as part of this evaluated deployment. For information about securing your deployment, see Securing the Deployment on page 57.

Note: When smart card authentication is enabled, users might receive an error message when attempting to launch applications that have been configured for management by the Single Sign-on component. This error message advises the user to restart the user device and to restart the XenApp session. In this situation the user can dismiss the error message and the deployment will continue to provide access to applications as in the *Security Target*. To prevent this error from occurring, additional configuration of the Single Sign-on component might be necessary, and this is beyond the scope of this document. For more information about implementing the changes necessary to remove this error, refer to the *Citrix Single Sign-on Administration* guide.

Chapter 5

Securing the Deployment

Topics:

- *Updating the Evaluation Components*
- *Windows Server 2008 R2 Security Configuration Wizard*
- *Setting Policies*
- *Removing and Disabling Citrix User Accounts*
- *Using FIPS-Compliant Ciphers Between the Web Plug-in and the Web Interface*
- *Securing the User Device*
- *Testing the Deployment*

This chapter details the procedures necessary to secure the deployment. It covers the following topics, which must be completed in the order listed:

- Updating the Primary and Secondary XenApp Servers
- Updating the Web Interface Server
- Windows 2008 R2 Security Configuration Wizard
- Setting Policies
- Removing and Disabling Citrix User Accounts
- Using FIPS-compliant Ciphers Between the Web Plug-in and the Web Interface
- Securing the User Device

TLS Renegotiation Issue in Microsoft Products

There is a known issue with the TLS and SSL protocols implemented in several Microsoft products, both client and server, where a vulnerability in TLS/SSL could allow spoofing to occur. Microsoft has issued a security update that addresses this vulnerability. The security update is available on the Microsoft Web site, as Microsoft Security Bulletin MS10-049.

Administrators should analyze the potential impacts of the vulnerability, the impact of the security update, and apply the update if appropriate.

Updating the Evaluation Components

Apply the following software updates to components in the evaluated configuration:

Apply this software update...	...to this component in the evaluated configuration
Microsoft Security Update 2264107	◆ Primary and secondary XenApp servers ◆ Web Interface server ◆ Secure Gateway server ◆ User device
Citrix Hotfix XA600W2K8R2X64002	Primary and secondary XenApp servers
Citrix Hotfix XA600W2K8R2X64021	Primary and secondary XenApp servers

To apply the Microsoft security update

This update allows you to control how DLLs are loaded when no fully qualified path is specified. To install the update, you run the Microsoft security update package appropriate for the component's operating system. Afterward, you run the Microsoft Fix it tool which creates the required registry entry.

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.

Download the Microsoft Fix it tool (MicrosoftFixit50522.msi) and the applicable Microsoft security update packages to removable media such as a flash drive:

- For the primary and secondary XenApp servers, the Web Interface server, and the Secure Gateway server, download the **Update for Windows Server 2008 R2 x64 Edition** file (Windows6.1-KB2264107-x64.msu)
- For the user device, locate the **Update for Windows 7** (32-bit: Windows6.1-KB2264107-x86.msu; 64-bit: Windows6.1-KB2264107-x64.msu) or the **Update for Windows Vista** (32-bit: Windows6.0-KB2264107-x86.msu; 64-bit: Windows6.0-KB2264107-x64.msu) appropriate for the device's operating system.

You can download these items from http://support.microsoft.com/kb/2264107.

1. Ensure you are logged on to the server or user device as a domain administrator.
2. Insert the media to which you downloaded the update packages and Fix it tool.
3. Locate the appropriate package for the component to which you are applying the update and double-click it to begin the installation.

The Windows Update Standalone Installer appears, confirming you want to install the update. Click **Yes**.

4. After the update finishes installing, click **Restart Now**.
5. After the computer restarts, log on as a domain administrator.
6. Locate the Microsoft Fix it tool and double-click it to begin the update.
   A security warning message appears, confirming you want to run the Fix it tool. Click **Run**.
7. When the Microsoft Fix it tool End User License Agreement appears, select the **I agree** check box and then click **Next**.
8. After the Microsoft Fix it tool finishes updating, click **Close**.
9. Repeat steps 1-8 for each component in the evaluated configuration

To verify the registry entry has been created, open Registry Editor and locate `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDLLSearch`. Note the value is set to 2 which affects how DLLs are loaded system-wide.

To apply the Citrix hotfixes

Download the Citrix hotfixes from the secure URLs listed below :

Download this Citrix hotfix...	...from this URL
Citrix Hotfix XA600W2K8R2X64002 (CTX126123)	https://support.citrix.com/servlet/KbServlet/download/25193-102-648323/XA600W2K8R2X64002.msp
Citrix Hotfix XA600W2K8R2X64021 (CTX127036)	https://support.citrix.com/servlet/KbServlet/download/25193-102-648323/XA600W2K8R2X64021.msp

Be sure to install the hotfixes in sequential order on the primary and secondary servers.

1. Ensure you are logged on to the XenApp server as a domain administrator.
2. Locate the file **XA600W2K8R2X64002.msp** and double-click it to begin the installation.
3. When the installation finishes, restart the XenApp server.
4. Repeat steps 1-3 for the file **XA600W2K8R2X64021.msp**.
5. Repeat steps 1-4 for each XenApp server in the evaluated configuration.

Windows Server 2008 R2 Security Configuration Wizard

The Windows Server 2008 R2 Security Configuration wizard must be installed and run on the following computers in the Common Criteria deployment:

- Web Interface
- Secure Gateway
- Primary and secondary servers running Citrix XenApp

The Windows Server 2008 R2 Security Configuration wizard allows you to secure the computers in the Common Criteria deployment. It allows you to lock down ports used by various services and disable Windows services that are unnecessary. The options that appear while running the Windows Server 2008 R2 Security Configuration wizard vary according to the choices you make along the way. Because each computer in the Common Criteria deployment requires a different set of available Windows services and open ports (choices), the steps will vary according to the sections below.

To install and run the Security Configuration wizard

1. Log on to the server with administrator credentials.
2. Launch the Security Configuration wizard (**Start**>**Administrative Tools**>**Security Configuration Wizard**).
3. At the **Welcome to the Security Configuration Wizard** page, click **Next**.
4. At the **Configuration Action** page, ensure that **Create a new security policy** is selected and click **Next**.
5. At the **Select Server** page, leave the default value and click **Next**.
6. At the **Processing Security Configuration Database** page, wait for the system scan to complete and click **Next**.
7. At the **Role-Based Service Configuration** page, click **Next**.
   The **Select Server Roles** page appears.
8. From the **Select Server Roles** page onwards, the options you select vary according to the computer to which you are applying the Security Configuration wizard. Each of the subsequent screens require you to select different options according to the table below. The n/a (not applicable) entries either mean that you do not select any options or the screen does not exist.

Screen	Web Interface	Secure Gateway	Primary server in the farm	Secondary servers in the farm
Select Server Roles	Application server ASP .NET State Service Middle-tier application server (COM +/DTC) Web server Windows Process Activation Service	none	Middle-tier application server (COM +/DTC) Remote Desktop Session Host Web server Windows Process Activation Service	Middle-tier application server(COM+/ DTC) Remote Desktop Session Host
Select Client Features	DNS client Domain member Microsoft Networking Client Time synchronization	none	DNS client Domain member Microsoft Networking Client Time synchronization	DNS client Domain member Microsoft Networking Client Time synchronization
Select Administration and Other Options	IPsec Policy Agent	IPsec Policy Agent	IPsec Policy Agent Windows User Mode Driver Framework	IPsec Policy Agent Windows User Mode Driver Framework
Select Additional Services	n/a	Citrix Secure Gateway	Application Identity Citrix 64-bit Virtual Memory Optimization Citrix CPU Utilization	Application Identity Citrix 64-bit Virtual Memory Optimization Citrix CPU Utilization

Screen	Web Interface	Secure Gateway	Primary server in the farm	Secondary servers in the farm
			Mgmt/ Resource Mgmt Citrix Group Policy Engine Citrix Independent Management Architecture Citrix Licensing Citrix Licensing WMI Citrix MFCOM Service Citrix Smart Card Service Citrix Virtual Memory Optimization Citrix WMI Service SQL Server(CITRIX_METAFRAME)	Mgmt/ Resource Mgmt Citrix Group Policy Engine Citrix Independent Management Architecture Citrix MFCOM Service Citrix Smart Card Service Citrix Virtual Memory Optimization Citrix WMI Service
Handling Unspecified Services	Do not change the startup mode of the service	Do not change the startup mode of the service	Do not change the startup mode of the service	Do not change the startup mode of the service
Confirm Service Changes	Click **Next**	Click **Next**	Click **Next**	Click **Next**
Network Security	Leave **Skip this section**	Leave **Skip this section**	Leave **Skip this section**	Leave **Skip this section**

<table>
<tr><th>Screen</th><th>Web Interface</th><th>Secure Gateway</th><th>Primary server in the farm</th><th>Secondary servers in the farm</th></tr>
<tr><td></td><td>cleared and click Next</td><td>cleared and click Next</td><td>cleared and click Next</td><td>cleared and click Next</td></tr>
<tr><td>Network Security Rules</td><td colspan="4">Note: The port numbers listed for each server are outbound TCP ports that must be added to the security policy. To do this:
a. Click Add.
b. On the General tab, in Name, type a name for the rule.
c. In Direction, select Inbound.
d. In Action, select Allow all connections.
e. On the Protocols and Ports tab, in Protocol Type, select TCP.
f. In Local Port, select Specific Ports and enter the port number.</td></tr>
<tr><td></td><td>443 (HTTPS)</td><td>443 (TLS)</td><td>All Core Networking settings (selected by default)
80 (HTTP)
2512
27000
7279
1434</td><td>All Core Networking settings (selected by default)
2512
1494
Note: Port 80 is disabled on this server in order to disable to the STA and XML Service that XenApp installs by default. The primary</td></tr>
</table>

Screen	Web Interface	Secure Gateway	Primary server in the farm	Secondary servers in the farm
			1494	server is the only XenApp server in the farm with the STA and XML Service enabled.
Confirm Port Configuration	Click **Next**	Click **Next**	Click **Next**	Click **Next**
Registry Settings	Leave **Skip this section** cleared and click **Next**	Leave **Skip this section** cleared and click **Next**	Leave **Skip this section** cleared and click **Next**	Leave **Skip this section** cleared and click **Next**
Require SMB Security Signatures	All computers that connect to it satisfy the following minimum operating system requirements. It has surplus processor capacity that can be used to sign file and print traffic.	All computers that connect to it satisfy the following minimum operating system requirements. It has surplus processor capacity that can be used to sign file and print traffic.	All computers that connect to it satisfy the following minimum operating system requirements. It has surplus processor capacity that can be used to sign file and print traffic.	All computers that connect to it satisfy the following minimum operating system requirements. It has surplus processor capacity that can be used to sign file and print traffic.
Outbound Authentication Methods	Domain Accounts	none	Domain Accounts	Domain Accounts
Outbound Authenticatio	Clocks that are	n/a	Clocks that are	Clocks that are

Screen	Web Interface	Secure Gateway	Primary server in the farm	Secondary servers in the farm
n using Domain Accounts	synchronized with the selected server's clock Windows NT 4.0 Service Pack 6a or later operating systems		synchronized with the selected server's clock Windows NT 4.0 Service Pack 6a or later operating systems	synchronized with the selected server's clock Windows NT 4.0 Service Pack 6a or later operating systems
Inbound Authenticatio n Methods	Clear all values and click **Next**.	Clear all values and click **Next**.	Clear all values and click **Next**.	Clear all values and click **Next**.
Registry Settings Summary	Click **Next**	Click **Next**	Click **Next**	Click **Next**
Audit Policy	Select the **Skip this section** check box and click **Next**	Select the **Skip this section** check box and click **Next**	Select the **Skip this section** check box and click **Next**	Select the **Skip this section** check box and click **Next**

9. At the **Save Security Policy** page, click **Next**.
10. At the **Security Policy File Name** page, type an appropriate name in the **Security policy file name** box and click **Next**.
11. In the **Apply Security Policy** page, select **Apply Now** and click **Next**.
    An **Applying Security Policy** screen appears while the security policy is applied. This takes up to two minutes to complete.
12. In the dialog box that appears suggesting that a server restart is required, click **OK**.

    Note: The dialog box suggesting that a server restart is required does not appear on the server running the Web Interface.

13. At the **Applying Security Policy** screen, when the Security Configuration Wizard is finished applying the security policy, click **Next**.
14. At the **Completing the Security Configuration Wizard** page, click **Finish**.
15. Restart the server for the security policies to take effect.

Note: It is not necessary to restart the Web Interface server.

After running the Security Configuration wizard, configure the IIS Admin Service to start automatically on server startup.

To configure the IIS Admin Service

1. Launch the Server Manager (**Start**>**All Programs**>**Administrative Tools**>**Server Manager**).
2. In the left pane, expand the **Configuration** node and select the **Services** node.
3. Double-click the **IIS Admin Service**.
   The **IIS Admin Service Properties** dialog box appears.
4. In **Startup type**, select **Automatic**.
5. Click **OK** to save your selection and close the **IIS Admin Service Properties** dialog box.

Setting Policies

For the Common Criteria evaluated deployment, it is necessary to set various policies to ensure the servers meet the security requirements.

Domain Wide Group Policies

The group policies are configured on the domain controller. These policies are applied to all servers within the domain. Therefore, these policies will apply to:

- The server running the Web Interface
- The primary and secondary servers
- The domain controller
- The smart card enrollment station

To configure the domain policies

1. Log on to the domain controller as a domain administrator and start the MMC (Click **Start > Run**, type **mmc**, and then click **OK**). The **Console1** window appears.
2. From the **File** menu, click **Add/Remove Snap-in**.
3. At the **Add/Remove Snap-ins** dialog box, under **Available snap-ins**, select **Group Policy Management Editor** and then click **Add**.
4. At the **Select Group Policy Object** dialog box, click **Browse**.

5. At the **Browse for a Group Policy Object** dialog box, click the **Create New Group Policy Object** icon. A policy entry is added to the list. Enter the policy name, for example, CommonCriteriaPolicy and click **OK**.
6. Click **Finish**. Click **OK**. The new group policy appears in the **Console1** window.
7. Right-click the new policy and select **Properties**. At the dialog box, select the **Security** tab.
8. Select the **Domain Admins** group and ensure **Apply Group Policy** permission is set to **Deny**. Repeat this step for the enterprise admins group (for example, **Enterprise Admins**).
9. You must add the required user groups (for example, **Domain Users**). Click **Add**. The **Select Users, Computers, or Groups** dialog box appears. Type **Domain Users** in the **Enter the object names to select** box and click **OK**.
10. Select the user group (for example, **Domain Users**) and ensure **Apply Group Policy** is set to **Allow**. This ensures the group policy applies to the user group. Click **OK**.

    A **Security** dialog box appears. The dialog box confirms that Deny entries take priority over Allow entries. This is required in the Common Criteria evaluated deployment to ensure the group policy is not applied to the administrator groups. Click **Yes**.
11. Select the new group policy and configure the policy settings as detailed in the steps described in Computer Configuration on page 67 and User Configuration on page 70.

Computer Configuration

1. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Account Policies**>**Password Policy**. For each of the following settings, click the **Define this policy setting** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Enforce password history	5 passwords remembered
Maximum password age	42 days (default)
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled (default)

2. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Account Policies**>**Account Lockout Policy**. For each of the following settings, click the **Define this policy setting** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Account lockout duration	0
Account lockout threshold	3
Reset account lockout counter after	99999

3. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Local Policies**>**Audit Policy**. For each of the following settings, click the **Define this policy setting** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Audit account logon events	Enable Success and Failure
Audit account management	Enable Success and Failure
Audit directory service access	Enable Success and Failure
Audit logon events	Enable Success and Failure
Audit object access	Enable Success and Failure
Audit policy change	Enable Success and Failure
Audit privilege use	Enable Success and Failure
Audit process tracking	Enable Success and Failure
Audit system events	Enable Success and Failure

4. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Local Policies**>**User Rights Assignment**. For each of the following settings, click the **Define these policy settings** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Allow log on through Remote Desktop Services	Remote Desktop Users
Change the system time	Administrators
Deny access to this computer from the network	• Anonymous Logon • Guest
Deny log on through Remote Desktop Services	Service
Shut down the system	Administrators (this overrides Local Policy Settings)

5. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Local Policies**>**Security Options**. For each of the following settings, click the **Define this policy setting** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
Shutdown: Allow system to be shut down without having to log on	Disabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

6. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Event Log**. For each of the following settings, click the **Define this policy setting** check box and enter the corresponding setting values:

Policy Setting	Setting Value
Maximum application log size	5120
Maximum security log size	5120
Maximum system log size	5120

7. Navigate to **Computer Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Internet Explorer** and configure the following settings:

Policy Setting	Setting Value
Disable Automatic Install of Internet Explorer components	Enabled

Policy Setting	Setting Value
Disable Periodic Check for Internet Explorer software updates	Enabled
Disable software update shell notifications on program launch	Enabled

8. Navigate to **Computer Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Windows Installer** and configure the following settings:

Policy Setting	Setting Value
Logging	Disabled

9. Navigate to **Computer Configuration**>**Policies**>**Administrative Templates**>**System**>**Remote Assistance** and configure the following settings:

Policy Setting	Setting Value
Offer Remote Assistance	Disabled
Solicited Remote Assistance	Disabled

10. Navigate to **Computer Configuration**>**Policies**>**Administrative Templates**>**System**>**Internet Communication Management** and configure the following settings:

Policy Setting	Setting Value
Restrict Internet communication	Enabled

11. Navigate to **Computer Configuration**>**Policies**>**Administrative Templates**>**Printers** and configure the following settings:

Policy Setting	Setting Value
Allow printers to be published	Disabled

User Configuration

1. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**AutoPlay Policies** and configure the following setting:

Policy Setting	Setting Value
Turn off AutoPlay	Enabled, All drives

2. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Internet Explorer** and configure the following setting:

Policy Setting	Setting Value
Disable Internet Connection wizard	Enabled

3. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Internet Explorer**>**Browser Menus** and configure the following setting:

Policy Setting	Setting Value
Disable Save this program to disk option	Enabled

4. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Internet Explorer**>**Internet Control Panel** and configure the following setting:

Policy Setting	Setting Value
Disable the Advanced Page	Enabled
Disable the Connections Page	Enabled
Disable the Content Page	Enabled
Disable the General Page	Enabled
Disable the Privacy Page	Enabled
Disable the Programs Page	Enabled
Disable the Security Page	Enabled

5. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Windows Explorer** and configure the following settings:

Policy Setting	Setting Value
Hide these specified drives in My Computer	Enabled, Restrict A, B, C, and D drives only
Hides the Manage item on the Windows Explorer context menu	Enabled
No Computers Near Me in Network Locations	Enabled
No Entire Network in Network Locations	Enabled
Prevent access to drives from My Computer	Enabled, Restrict A, B, C, and D drives only

Policy Setting	Setting Value
	Note: This assumes that A, B, C and D are all server-side drives, which the client does not need to access.
Remove File menu from Windows Explorer	Enabled
Remove Hardware tab	Enabled
Remove “Map Network Drive” and “Disconnect Network Drive”	Enabled
Remove Search button from Windows Explorer	Enabled
Remove Windows Explorer’s default context menu	Enabled
Removes the Folder Options menu item from the Tools menu	Enabled
Common Open File Dialog folder > Hide the common dialog places bar	Enabled

6. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Windows Explorer**>**Explorer Frame Page** and configure the following settings:

Policy Setting	Setting Value
Turn off Details Pane	Enabled
Turn off Preview Pane	Enabled

7. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Microsoft Management Console** and configure the following setting:

Policy Setting	Setting Value
Restrict the user from entering author mode	Enabled
Restrict users to the explicitly permitted list of snap-ins	Enabled

8. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Task Scheduler** and configure the following settings:

Policy Setting	Setting Value
Prevent Task Run or End	Enabled
Prohibit New Task Creation	Enabled
Prohibit Task Deletion	Enabled

9. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Windows Components**>**Windows Update** and configure the following setting:

Policy Setting	Setting Value
Remove access to use all Windows Update features	Enabled

10. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Start Menu and Taskbar** and configure the following settings:

Policy Setting	Setting Value
Add Logoff to the Start Menu	Disabled
Add “Run in Separate Memory Space” check box to Run dialog box	Disabled
Clear history of recently opened documents on exit	Enabled
Do not keep history of recently opened documents	Enabled
Do not use the search-based method when resolving shell shortcuts	Enabled
Do not use the tracking-based method when resolving shell shortcuts	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Disabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove access to the context menus for the taskbar	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled
Remove common program groups from Start Menu	Enabled

Policy Setting	Setting Value
Remove Documents icon from Start Menu	Enabled
Remove drag-and-drop and context menus on the Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Logoff on the Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Search link from Start Menu	Enabled
Remove user's folders from the Start Menu	Enabled
Turn off personalized menus	Enabled
Turn off user tracking	Enabled

11. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Desktop**>**Desktop** and configure the following setting:

Policy Setting	Setting Value
Disable Active Desktop	Enabled

12. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Control Panel** and configure the following setting:

Policy Setting	Setting Value
Prohibit access to the Control Panel	Enabled

13. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**Control Panel**>**Printers** and configure the following setting:

Policy Setting	Setting Value
Prevent addition of printers	Enabled

14. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**System** and configure the following settings:

Policy Setting	Setting Value
Download missing COM components	Disabled
Prevent access to registry editing tools	Enabled, set **Disable regedit from running silently?** to **Yes**.
Prevent access to the command prompt	Enabled, leave **Disable the command prompt script processing also?** set to **No**.

15. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**System**>**Ctrl +Alt+Del Options** and configure the following settings:

Policy Setting	Setting Value
Remove Change Password	Enabled
Remove Logoff	Enabled
Remove Lock Computer	Enabled
Remove Task Manager	Enabled

16. Navigate to **User Configuration**>**Policies**>**Administrative Templates**>**System**>**Logon** and configure the following settings:

Policy Setting	Setting Value
Do not process the legacy run list	Enabled
Do not process the run once list	Enabled

Disabling XenApp Features with Policies

After installing XenApp on primary and secondary servers, configure XenApp policies to disable the following features:

- Redirection of client devices, ports, audio, and printers
- Client drive and clipboard mapping
- Multimedia and Flash acceleration
- Session reliability and shadowing

To disable these features for all farm servers and user sessions in the evaluated configuration, you add the appropriate policy settings to the Unfiltered computer and user policies that are included in XenApp. For the evaluated configuration, the policy

settings that govern these features are disabled. However, you can enable these features by enabling the settings in each policy.

Policy settings that are not added to a policy are considered "not configured" and are ignored by XenApp when evaluating policies to apply to user sessions. For more information about configuring XenApp policies, see section 4.3 of the *Citrix XenApp Administration* guide.

1. Ensure you are logged on to the primary server as a domain administrator.
2. Launch the Group Policy Management console (**Start**>**Administrative Tools**>**Group Policy Management**).
3. In the left pane of the console, under the forest node, select and expand the **Domains** node and then expand the node of *your domain name*.
4. Expand the **Group Policy Objects** node and locate the group policy object you created in To configure the domain policies on page 66.
5. Right-click the group policy object and select **Edit**.
   The **Group Policy Management Editor** window appears.

To create the XenApp computer policy

1. In the left pane of the editor, under **Computer Configuration**, expand the **Policies** node and then select **Citrix Policies**.
   The **Citrix Computer Policies** console appears in the right pane.
2. Select the **Unfiltered** policy from the policy list and then click the **Settings** tab near the bottom of the screen.
   The Settings list appears, with the **Active Settings** category selected.
3. In the Settings list, under **Categories**, click **All Settings**.
   The Settings section displays the complete list of policy settings.
4. Use the following table to select and configure the required policy settings. For each policy setting, click **Add** and select the required setting option.

Note: To locate settings quickly, type each setting name in the **Search All Settings** box. XenApp locates the matching settings as you type.

Setting Name	Setting Option
Auto client reconnect	Prohibited
HDX MediaStream Multimedia Acceleration	Prohibited
Multimedia conferencing	Prohibited
Session reliability connections	Prohibited
Shadowing	Prohibited

Note: To enable these policy settings, select **Allowed**.

To apply your policy changes immediately, at the command prompt, open a command prompt window and run the command **gpupdate /force**.

To create the XenApp user policy

1. In the left pane of the editor, under **User Configuration**, expand the **Policies** node and then select **Citrix Policies**.
   The **Citrix User Policies** console appears in the right pane.
2. Select the **Unfiltered** policy from the policy list and then click the **Settings** tab near the bottom of the screen.
   The Settings list appears, with the **Active Settings** category selected.
3. In the Settings list, under **Categories**, click **All Settings**.
   The Settings section displays the complete list of policy settings.
4. Use the following table to select and configure the required policy settings. For each policy setting, click **Add** and select the required option.

   Note: To locate settings quickly, type each setting name in the **Search All Settings** box. XenApp locates the matching settings as you type.

Setting Name	Setting Option
Client audio redirection	Prohibited
Client clipboard redirection	Prohibited
Client COM port redirection	Prohibited
Client drive redirection	Prohibited
Client LPT port redirection	Prohibited
Client microphone redirection	Prohibited
Client printer redirection	Prohibited
Client TWAIN device redirection	Prohibited
Client USB device redirection	Prohibited
Client USB Plug and Play device redirection	Prohibited
Flash acceleration	Disabled
OEM channels	Prohibited

Note: To enable these policy settings, select **Allowed** or **Enabled** as appropriate.

To apply your policy changes immediately, at the command prompt, open a command prompt window and run the command **gpupdate /force**.

Securing Executables with AppLocker

After installing XenApp, the primary and secondary servers need to be locked down to prevent launching of unauthorized executables. To do this, you use AppLocker to perform the following tasks:

- Create a default rule
- Create rules for non-Administrator users
- Configure the Application Identity service to start automatically on server restart

To create the Default Rule

1. Ensure you are logged on to the domain controller as a domain administrator. Verify the **Console1** MMC window you opened in To configure the domain policies on page 66 is still open and that the Group Policy Object you created is still displayed.
2. Navigate to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Application Control Policies**>**AppLocker**.
3. From the middle pane, click **Configure rule enforcement**.
   The **AppLocker Properties** dialog box appears.
4. Under **Executable Rules**, select **Configured** and then select **Enforce rules** from the drop-down list. Click **OK**.
5. From the tree view of the console, expand the **AppLocker** node, right-click **Executable Rules**, and select **Create New Rule**.
   The **Create Executable Rules** screen appears. Click **Next**.
6. On the **Permissions** page, perform the following actions:
   a. Ensure **Allow** is selected.
   b. Click **Select** and, in the **Select User or Group** dialog box, add the **Administrators** group.
   c. Click **OK** to return to the Permissions page and then click Next.
7. On the **Conditions** page, select **Path** and click **Next**.
8. On the **Path** page, type an asterisk (`*`) in the **Path** box and then click **Next**.
9. On the **Exceptions** page, click **Next**.
10. On the **Name and Description** page, type `Default rule (all files)` in the **Name** box and then click **Create**.
    A message appears prompting you to create additional default rules.
11. Click **No** to close the message without creating additional rules.

After the default rule is created, create additional rules for non-administrator users to securely access other executable files in the evaluated configuration.

To create rules for non-Administrator users

Perform the following steps to create rules for non-administrator users to access certain executable files in the evaluated configuration.

1. From the tree view of the console, expand the **AppLocker** node, right-click **Executable Rules**, and click **Create New Rule**.
   The **Create Executable Rules** screen appears. Click **Next**.
2. On the **Permissions** page, perform the following actions:
   a. Ensure **Allow** is selected.
   b. Ensure the **Everyone** group is selected.
   c. Click **Next**.
3. On the **Conditions** page, select **Path** and click **Next**.
4. On the **Path** page, type the executable path of the published application to which you want to allow access. For example, to allow access to the published Notepad application, type `%system32%\notepad.exe`. Click **Next**.
5. On the **Exceptions** page, click **Next**.
6. On the **Name and Description** page, accept the default entry in the **Name** box and then click **Create**.
7. In addition to the rules you create for published applications, repeat Steps 1-6 to create rules for each of the following paths:
   - %system32%\atbroker.exe
   - %system32%\conhost.exe
   - %system32%\dwm.exe
   - %system32%\taskhost.exe
   - %system32%\tstheme.exe
   - %system32%\userinit.exe
   - %programfiles%\citrix\ica client\ssonsvr.exe
   - %programfiles%\citrix\system32\cmstart.exe
   - %programfiles%\citrix\system32\ctxhide.exe
   - %programfiles%\citrix\system32\icast.exe
   - %programfiles%\citrix\system32\startssonsvr.exe
   - %programfiles%\citrix\system32\wfshell.exe
   - %windir%\application compatibility scripts\acregl.exe
8. Close the **Console1** window.

9. When the **Microsoft Management Console** dialog box prompts you to save console settings to Console1, click **No**.

To configure the Application Identity service

1. Launch the **Services** console (**Start**>**All Programs**>**Administrative Tools**>**Services**).
2. Right-click the **Application Identity** service and select **Properties**.
   The **Application Identity Properties** dialog box appears.
3. In **Startup type**, select **Automatic**. Click **Apply**.
4. Click **Start** to start the service. Click **OK**.
5. Close the **Services** console.

Setting Group Policy Priority

After you define the domain wide group policies above, you must ensure the group policy created for the Common Criteria evaluated deployment is set as the primary policy (it must be the first policy in the list of policies). This is necessary to ensure that other group policies do not override the Common Criteria evaluated deployment policy.

To set the group policy priority

1. Launch the Group Policy Management console (**Start > All Programs > Administrative Tools > Group Policy Management**).
   The **Group Policy Management** window appears.
2. Select the domain from the tree view.
3. On the **Linked Group Policy Objects** tab, select the Common Criteria evaluated deployment policy and click the **Move link to top** arrow.
   The policy appears at the top of the list.
4. Close the **Group Policy Management** window.

Secure Gateway Local Group Policies

You must configure the following local group policies on the server running the Secure Gateway.

Note: Because only administrators are allowed access to the server running the Secure Gateway, there are no user configuration policy settings for the Secure Gateway.

To configure the local group policies

1. Log on to the Secure Gateway as a local administrator and start the Local Group Policy Editor (Click **Start**>**Run >** , type **gpedit.msc**, and then click **OK**).
   The **Local Group Policy Editor** window appears.

2. In the left pane of the **Local Group Policy Editor** window, select the **Local Computer Policy** item and configure the policy settings as detailed in the following steps.
3. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Account Policies**>**Password Policy** and configure the following settings:

Policy Setting	Setting Value
Enforce password history	5 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled (default)

4. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Account Policies**>**Account Lockout Policy** and configure the following settings:

Policy Setting	Setting Value
Account lockout duration	0
Account lockout threshold	3
Reset account lockout counter after	99999

5. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Local Policies**>**Audit Policy** and configure the following settings:

Policy Setting	Setting Value
Audit account logon events	Enable Success and Failure
Audit account management	Enable Success and Failure
Audit directory service access	Enable Success and Failure
Audit logon events	Enable Success and Failure
Audit object access	Enable Success and Failure
Audit policy change	Enable Success and Failure
Audit privilege use	Enable Success and Failure

Policy Setting	Setting Value
Audit process tracking	Enable Success and Failure
Audit system events	Enable Success and Failure

6. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Local Policies**>**User Rights Assignment** and configure the following settings:

Policy Setting	Setting Value
Allow log on through Remote Desktop Services	Leave blank
Change the system time	Administrators
Deny access to this computer from the network	• Anonymous Logon • Guest
Shut down the system	Administrators

7. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Local Policies**>**Security Options** and configure the following settings:

Policy Setting	Setting Value
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
System cryptography: Use FIPS compliantalgorithms for encryption, hashing, and signing	Enabled

8. Navigate to **Computer Configuration**>**Administrative Templates**>**Windows Components**>**Internet Explorer** and configure the following settings:

Policy Setting	Setting Value
Disable Automatic Install of Internet Explorer Components	Enabled
Disable Periodic Check for Internet Explorer software updates	Enabled

Policy Setting	Setting Value
Disable software update shell notifications on program launch	Enabled

9. Navigate to **Computer Configuration**>**Administrative Templates**>**System**>**Remote Assistance** and configure the following settings:

Policy Setting	Setting Value
Solicited Remote Assistance	Disabled
Offer Remote Assistance	Disabled

10. Navigate to **Computer Configuration**>**Administrative Templates**>**System**>**Internet Communication Management** and configure the following setting:

Policy Setting	Setting Value
Restrict Internet communication	Enabled

11. Navigate to **Computer Configuration**>**Administrative Templates**>**Printers** and configure the following setting:

Policy Setting	Setting Value
Allow Printers to be published	Disabled

12. Close the **Local Group Policy Editor** window.

Web Plug-in Local Group Policies and Registry Settings

On each of the user devices, you must perform the following tasks:

- Configure the local group policies
- Configure the web plug-in's file security preferences

To configure the local group policies

1. Log on to the user device as a local administrator and start the Local Group Policy Editor (Click **Start**>**Run**, type **gpedit.msc**, and then click **OK**).
   The **Local Group Policy Editor** window appears.
2. In the left pane of the **Local Group Policy Editor** window, select the **Local Computer Policy** item and configure the policy settings as detailed in the following steps.
3. Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Local Policies**>**Security Options** and configure the following settings:

Policy Setting	Setting Value
Shutdown: Clear virtual memory page file	Enabled
System cryptography: Use FIPS compliantalgorithms for encryption, hashing, and signing	Enabled

4. Navigate to **User Configuration**>**Administrative Templates**>**Windows Components**>**Internet Explorer**>**Browser Menus** and configure the following settings:

Policy Setting	Setting Value
Disable Save this program to disk option	Enabled

5. Close the **Local Group Policy Editor** window.

To configure the file security preferences

When you configure the web plug-in's file security preferences, users are prevented from changing the Session Security settings through the Connection Center. Additionally, when users are prompted for explicit permission for remote applications to access local files, the **Remember these settings** check box is not displayed.

You configure these preferences by editing the Registry. To ensure all the required settings are included, use the CC_Settings.reg file appropriate for the user device's operating system. The CC_Settings file is available as a secure download from the Citrix Web site.

 **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. Log on to the user device as an administrator.
2. Launch Internet Explorer and navigate to http://support.citrix.com/article/CTX127308.
3. Click the **HTTPS Download** link to download the **CC_Settings.zip** file.
4. Locate one of the following registry files appropriate for the operating system on the user device:
   - **CC_settings_x86.reg** (for 32-bit operating systems)
   - **CC_settings_x64.reg** (for 64-bit operating systems)
5. Double-click the file to apply the registry settings.
   A message appears, confirming that you want to update the registry.
6. Click **Yes** to update the registry.

Removing and Disabling Citrix User Accounts

You can ensure that user accounts not required for your deployment are removed from primary and secondary XenApp servers. For the evaluated configuration, anonymous user accounts are removed, and the Ctx_ConfigMgr and Ctx_StreamingSvc accounts are disabled on both servers.

To remove anonymous users from the XenApp servers

Before you perform this procedure, be sure that:

- You have a copy of the sample script located at http://support.citrix.com/article/CTX121704
- The script is saved as a .vbs file (for example, deleteusers.vbs)

1. Ensure you are logged on to the XenApp server as an administrator.
2. Navigate to the location of the sample script and double-click to run it.
   The Command Prompt window appears and displays progress in deleting the anonymous user accounts.

To disable the Citrix user accounts

1. Ensure you are logged on to the XenApp server as an administrator.
2. Launch the **Server Manager** (**Start**>**Administrative Tools**>**Server Manager**).
   The **Server Manager** window appears.
3. In the left pane, expand the **Configuration** node, then expand the **Local Users and Groups** node and select **Users**.
4. Right-click the **Ctx_ConfigMgr** user account and select **Properties**.
5. On the **Properties** dialog box, select the **Account is disabled** check box and then click **OK**.
6. Repeat steps 4 and 5 for the Ctx_StreamingSvc user account.

Using FIPS-Compliant Ciphers Between the Web Plug-in and the Web Interface

To ensure the web plug-in uses FIPS-compliant ciphers when connecting through the Secure Gateway, you modify the default ICA file template settings on the server running the Web Interface.

1. On the server running the Web Interface, ensure you are logged on as an administrator.
2. Launch Windows Explorer (**Start**>**Computer**).
   The **Windows Explorer** window appears.
3. Navigate to the `C:\Inetpub\wwwroot\Citrix\XenApp\conf` folder.
4. Right-click on the **default.ica** file and select **Open with**.
   The **Open with** dialog box appears.
5. Select **Notepad** and clear the **Always use the selected program to open this kind of file** check box.
   The **Notepad** window appears, displaying the contents of the default.ica file.
6. Locate the **[WFClient]** section and insert the following line at the end of the section:
   SSLCIPHERS=GOV
7. Save the file and then close the **Notepad** window.
8. Close Windows Explorer.

Securing the User Device

To secure the user device in the evaluated configuration, perform the following tasks:

- Configure Microsoft Internet Explorer to use TLS 1.0
- Disable ActiveX support in Microsoft Internet Explorer
- Require the user device to download ICA files

To configure Microsoft Internet Explorer to use TLS 1.0

On each client device ensure Microsoft Internet Explorer is configured for TLS 1.0 communication.

1. Launch Microsoft Internet Explorer. Click **Tools**>**Internet Options**.
   The **Internet Options** dialog box appears.
2. Select the **Advanced** tab. Under **Settings**, within the **Security** section, ensure **Use TLS 1.0** is selected and ensure **Use SSL 2.0** and **Use SSL 3.0** are not selected.
3. Click **OK** to accept the changes and close the **Internet Options** dialog box.
4. Close Internet Explorer.

To disable ActiveX support in Microsoft Internet Explorer

On each client device, ensure ActiveX support in Microsoft Internet Explorer is disabled.

1. Launch Microsoft Internet Explorer. Click **Tools**>**Internet Options**.
   The **Internet Options** dialog box appears.
2. Select the **Security** tab and then click **Custom Level**.
   The **Security Settings** dialog box appears.
3. Under **ActiveX controls and plug-ins**, disable the following settings:
   - Binary and script behaviors
   - Download signed ActiveX controls
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting
4. Click **OK** to accept the changes and close the **Security Settings** dialog box.
5. Click **OK** to close the Internet Options dialog box.
6. Close Internet Explorer.

To enable forced downloads of ICA files

This procedure ensures the user device is forced to download ICA files.

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. Log on to the user device as an administrator.
2. Open the **Command Prompt** window (**Start**>**Accessories**>**Command Prompt**).

   Note: For Windows Vista and Windows 7 operating systems, click **Start**>**Accessories**. Right-click **Command Prompt** and select **Run as administrator**. At the **User Account Control** dialog box, click **Yes**.

3. Type the following:

```
reg add "HKLM\Software\Policies\Microsoft\Internet Explorer
\Restrictions" /v AlwaysPromptWhenDownload /t REG_DWORD /d
00000001
```

Testing the Deployment

Before making Citrix XenApp available to users, test the deployment as detailed in Testing the Deployment on page 89.

Chapter 6

Testing the Deployment

Topics:

- *Overview*
- *Making Citrix XenApp Available to Users*
- *Verifying Client File Security Settings*
- *Ensuring Users Close Applications When Logging Off*

This section describes how to log on and test the system.

Updates to Citrix Products Included in the Common Criteria Evaluated Configuration

Citrix will, from time to time, issue product updates which may correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators may also opt to subscribe to proactive email alerts about product security vulnerabilities and their associated fixes. These alerts are sent out on a regular basis whenever new fixes are available. Administrators may contact and work with Citrix Support directly if they require additional support in obtaining and deploying any fix. More information about the email alerts system can be found at http://www.citrix.com.

Overview

After you complete installation and configuration of the deployment, you need to test that your deployment works and is accessible through the Internet.

To log on using explicit credentials

1. After you log on to the client device, launch Microsoft Internet Explorer and open: https://*FQDN of Web Interface*/Citrix/*XenApp Web Site Name*/.
   The **Citrix XenApp - Logon** page appears.
2. Enter your user credentials and click **Log On**.
   After a brief interval, the **Applications** page containing icons for published applications appears.
3. From the **Applications** page, click the appropriate icons to verify that you can launch published applications.

To log on using a smart card

1. After you log on to the user device, insert your smart card. Launch Microsoft Internet Explorer and open: https://*FQDN of Web Interface*/Citrix/*XenApp Web Site Name*/.
   The **Choose a digital certificate** dialog box appears.
2. Select your digital certificate and click **OK**.
   A dialog box appears prompting you for your smart card PIN.
3. Enter your smart card PIN and click **OK**.
   After a brief interval, the **Applications** page containing icons for published applications appears.
4. From the **Applications** page, click an appropriate icon to verify that you can launch a published application.
   The **Log On to Windows** dialog box appears.
5. In the **Log On to Windows** dialog box, reenter your smart card PIN and click **OK**.

Making Citrix XenApp Available to Users

After you test the deployment, inform your users of the URL for the Citrix XenApp Logon page. If users want to bookmark the Logon page in their browsers, Citrix recommends that the bookmark be set to: https://*FQDN of Web Interface*/Citrix/*XenApp Web Site Name*/.

Verifying Client File Security Settings

If the Citrix XenApp administrator enabled client drive mapping, the client drives are made available to published applications running on the secondary servers in the farm. If an application attempts to use a client drive, then depending upon the client's file security settings, the web plug-in prompts the user to specify the level of access the application can have to the drive.

Note: If you have completed the steps described in To configure the file security preferences on page 84, the plug-in prompts the user only to allow remote access to local files.

The client file security settings are stored in the Windows registry. However, for the evaluated configuration, the administrator should not define these settings. In the absence of these settings, users, by default, are prompted to allow access to local files.

After an ICA session is running, the client file security settings are accessible from the Citrix Connection Center.

To check and configure the client file security settings

1. When a published application is launched from the user device, confirm the following items:
   - The **File Security** dialog box appears, prompting the user to allow remote access to local files.
   - The **File Security** dialog box does not display the **Remember these settings** check box. Instead, only the **Read files only** check box is displayed.
2. Right-click the plug-in icon that appears in the Windows notification area and select **Connection Center**.
3. In the **Connection Center** dialog box, verify that the settings under **Session Security** are disabled.
4. Click **OK** to close the **Connection Center** dialog box.

Ensuring Users Close Applications When Logging Off

When users log off from the Web Interface and close the Web browser, the user session is maintained for any published applications that remain open. Other users accessing the client device can use any applications that remain open. Therefore, administrators must warn users to close all published applications when logging off from the Web Interface.

IMA Error Codes

The items in the following table are Citrix IMA Service error codes that can appear in the Event Viewer.

Hex value	Signed value	Unsigned value	Mnemonic
00000000h	0	0	IMA_RESULT_SUCCESS
00000001h	1	1	IMA_RESULT_OPERATION_INCOMPLETE
00000002h	2	2	IMA_RESULT_CALL_NEXT_HOOK
00000003h	3	3	IMA_RESULT_DISCARD_MESSAGE
00000004h	4	4	IMA_RESULT_CREATED_NEW
00000005h	5	5	IMA_RESULT_FOUND_EXISTING
00000005h	5	5	IMA_RESULT_FINDEXIST
00000009h	9	9	IMA_RESULT_CONNECTION_IDLE
0000000Ah	10	10	IMA_RESULT_ZONE_OBJECTS_UPDATE_IMCOMPLETE
0000000Bh	11	11	IMA_RESULT_BAD_ZONE_EXISTS
0000000Ch	12	12	IMA_RESULT_WSC_RECONNECT_INCOMPLETE
0000000Dh	13	13	IMA_RESULT_APP_LAUNCH_DISALLOWED
0000000Eh	14	14	IMA_RESULT_ELECTION_IN_PROGRESS
00110202h	1114626	1114626	IMA_LOAD_THROTTLING_DISABLED
00110203h	1114627	1114627	IMA_RULE_LOAD_EXCLUDE
00130001h	1245185	1245185	IMA_RESULT_ADSI_NOT_INSTALLED
00130002h	1245186	1245186	IMA_RESULT_SECURITY_INFO_INCOMPLETE
001C0000h	1835008	1835008	IMA_RESULT_COMSRV_INHERIT_FARM_HCA
0026000Bh	2490379	2490379	IMA_RESULT_PARTIAL_SUCCESS
002D0001h	2949121	2949121	IMA_RESULT_ALREADY_MASTER
00410001h	4259841	4259841	IMA_RESULT_ImaMfRpc_USER_NOT_ADMIN

Hex value	Signed value	Unsigned value	Mnemonic
80000001h	-2147483647	2147483649	IMA_RESULT_FAILURE
80000001h	-2147483647	2147483649	IMA_RESULT_UNKNOWN_FAILURE
80000002h	-2147483646	2147483650	IMA_RESULT_NO_MEMORY
80000002h	-2147483646	2147483650	IMA_RESULT_OUT_OF_MEMORY
80000002h	-2147483646	2147483650	IMA_RESULT_ALLOCBUFFER_FAILURE
80000002h	-2147483646	2147483650	IMA_RESULT_OUT_OF_RESOURCES
80000002h	-2147483646	2147483650	IMA_RESULT_GROUP_OUT_OF_MEMORY
80000003h	-2147483645	2147483651	IMA_RESULT_INVALID_ARG
80000003h	-2147483645	2147483651	IMA_RESULT_BAD_PARAM
80000004h	-2147483644	2147483652	IMA_RESULT_UNKNOWN_MESSAGE
80000005h	-2147483643	2147483653	IMA_RESULT_DESTINATION_UNREACHABLE
80000006h	-2147483642	2147483654	IMA_RESULT_REFERENCE_COUNT_NOT_ZERO
80000007h	-2147483641	2147483655	IMA_RESULT_ENTRY_NOT_FOUND
80000008h	-2147483640	2147483656	IMA_RESULT_NETWORK_FAILURE
80000009h	-2147483639	2147483657	IMA_RESULT_NOT_IMPLEMENTED
80000009h	-2147483639	2147483657	IMA_RESULT_NOTIMPLEMENTED

Hex value	Signed value	Unsigned value	Mnemonic
8000000Ah	-2147483638	2147483658	IMA_RESULT_INVALID_MESSAGE
8000000Bh	-2147483637	2147483659	IMA_RESULT_TIMEOUT
8000000Ch	-2147483636	2147483660	IMA_RESULT_POINTER_IS_NULL
8000000Dh	-2147483635	2147483661	IMA_RESULT_UNINITIALIZED
8000000Eh	-2147483634	2147483662	IMA_RESULT_FINDITEM_FAILURE
8000000Fh	-2147483633	2147483663	IMA_RESULT_CREATEPOOL_FAILURE
80000010h	-2147483632	2147483664	IMA_RESULT_SUBSYS_NOT_FOUND
80000013h	-2147483629	2147483667	IMA_RESULT_PS_UNINITIALIZED
80000014h	-2147483628	2147483668	IMA_RESULT_REGMAPFAIL
80000015h	-2147483627	2147483669	IMA_RESULT_DEST_TOO_SMALL
80000016h	-2147483626	2147483670	IMA_RESULT_ACCESS_DENIED
80000017h	-2147483625	2147483671	IMA_RESULT_NOT_SHUTTING_DOWN
80000018h	-2147483624	2147483672	IMA_RESULT_MUSTLOAD_FAILURE
80000019h	-2147483623	2147483673	IMA_RESULT_CREATELOCK_FAILURE
8000001Ah	-2147483622	2147483674	IMA_RESULT_SHUTDOWN_FAILURE
8000001Ch	-2147483620	2147483676	IMA_RESULT_SENDWAIT_FAILURE

Hex value	Signed value	Unsigned value	Mnemonic
8000001Dh	-2147483619	2147483677	IMA_RESULT_NO_COLLECTORS
8000001Eh	-2147483618	2147483678	IMA_RESULT_UPDATED
8000001Fh	-2147483617	2147483679	IMA_RESULT_NO_CHANGE
80000020h	-2147483616	2147483680	IMA_RESULT_LEGACY_NOT_ENABLED
80000021h	-2147483615	2147483681	IMA_RESULT_VALUE_ALREADY_CREATED
80000022h	-2147483614	2147483682	IMA_RESULT_UID_EXCEEDED_BOUNDS
80000023h	-2147483613	2147483683	IMA_RESULT_NO_EVENTS
80000024h	-2147483612	2147483684	IMA_RESULT_NOT_FOUND
80000024h	-2147483612	2147483684	IMA_RESULT_MEMBER_NOT_FOUND
80000024h	-2147483612	2147483684	IMA_RESULT_GROUP_NOT_FOUND
80000025h	-2147483611	2147483685	IMA_RESULT_ALREADY_EXISTS
80000025h	-2147483611	2147483685	IMA_RESULT_MEMBER_ALREADY_EXISTS
80000026h	-2147483610	2147483686	IMA_RESULT_GROUP_ALREADY_EXISTS
80000027h	-2147483609	2147483687	IMA_RESULT_NOT_A_GROUP
80000028h	-2147483608	2147483688	IMA_RESULT_GROUP_DIR_ACCESS_FAILURE
80000029h	-2147483607	2147483689	IMA_RESULT_EOF

Hex value	Signed value	Unsigned value	Mnemonic
8000002Ah	-2147483606	2147483690	IMA_RESULT_REGISTRY_ERROR
8000002Bh	-2147483605	2147483691	IMA_RESULT_DSN_OPEN_FAILURE
8000002Ch	-2147483604	2147483692	IMA_RESULT_REMOVING_PSSERVER
8000002Dh	-2147483603	2147483693	IMA_RESULT_NO_REPLY_SENT
8000002Eh	-2147483602	2147483694	IMA_RESULT_PLUGIN_FAILED_VERIFY
8000002Fh	-2147483601	2147483695	IMA_RESULT_FILE_NOT_FOUND
80000030h	-2147483600	2147483696	IMA_RESULT_PLUGIN_ENTRY_NOT_FOUND
80000031h	-2147483599	2147483697	IMA_RESULT_CLOSED
80000032h	-2147483598	2147483698	IMA_RESULT_PATH_NAME_TOO_LONG
80000033h	-2147483597	2147483699	IMA_RESULT_CREATEMESSAGEPORT_FAILED
80000034h	-2147483596	2147483700	IMA_RESULT_ALTADDRESS_NOT_DEFINED
80000035h	-2147483595	2147483701	IMA_RESULT_WOULD_BLOCK
80000036h	-2147483594	2147483702	IMA_RESULT_ALREADY_CLOSED
80000037h	-2147483593	2147483703	IMA_RESULT_TOO_BUSY
80000038h	-2147483592	2147483704	IMA_RESULT_HOST_SHUTTING_DOWN
80000039h	-2147483591	2147483705	IMA_RESULT_PORT_IN_USE

Hex value	Signed value	Unsigned value	Mnemonic
8000003Ah	-2147483590	2147483706	IMA_RESULT_NOT_SUPPORTED
8000003Bh	-2147483589	2147483707	IMA_RESULT_NOT_TRUSTED
8000003Ch	-2147483588	2147483708	IMA_RESULT_WRITE_TO_LOG_FAILED
8000003Dh	-2147483587	2147483709	IMA_RESULT_NOT_AVAILABLE_IN_SR
8000003Eh	-2147483586	2147483710	IMA_RESULT_LOG_TESTCONN_FAILED
8000003Fh	-2147483585	2147483711	IMA_RESULT_LOG_CLEARLOG_FAILED
80000040h	-2147483584	2147483712	IMA_RESULT_IMADS_TO_XML_FAILED
80000041h	-2147483583	2147483713	IMA_RESULT_INCONSISTENT_XML_KEY_TYPE
80000042h	-2147483582	2147483714	IMA_RESULT_BAD_XML_TAG
80000043h	-2147483581	2147483715	IMA_RESULT_BAD_XML_PARAM
80000044h	-2147483580	2147483716	IMA_RESULT_INVALID_FARM_TYPE
80000047h	-2147483577	2147483719	IMA_RESULT_BAD_FARM_TYPE
80000048h	-2147483576	2147483720	IMA_RESULT_INVALID_LICENSE_SERVER
80000049h	-2147483575	2147483721	IMA_RESULT_INCOMPATIBLE_LICENSE_SERVER
8000004Ah	-2147483574	2147483722	IMA_RESULT_AUDIT_LICENSE_NOT_FOUND
8000004Bh	-2147483573	2147483723	IMA_RESULT_LOG_PARAM_INVALID

Hex value	Signed value	Unsigned value	Mnemonic
8000004Ch	-2147483572	2147483724	IMA_RESULT_LOG_WRITE_TO_IMADB_FAILED
8000004Dh	-2147483571	2147483725	IMA_RESULT_CLDB_WRITE_FAILED
8000004Eh	-2147483570	2147483726	IMA_RESULT_CLDB_FARM_NAME_MISMATCH
8000004Fh	-2147483569	2147483727	IMA_RESULT_CLDB_FARM_NOT_CONFIGURED
80000050h	-2147483568	2147483728	IMA_RESULT_CLDB_DATABASE_NOT_SUPPORTED
80000051h	-2147483567	2147483729	IMA_RESULT_CLDB_CONNECTIONPARAM_INVALID
80000052h	-2147483566	2147483730	IMA_RESULT_CLDB_IMPERSONATE_FAILED
80000053h	-2147483565	2147483731	IMA_RESULT_CLDB_OPENCONNECTION_FAILED
80000054h	-2147483564	2147483732	IMA_RESULT_ARRAY_OUTOFBOUNDS
80000055h	-2147483563	2147483733	IMA_RESULT_STRINGSID_CONVERSION_ERROR
80000056h	-2147483562	2147483734	IMA_RESULT_SUBSYSTEM_DISABLED
80040001h	-2147221503	2147745793	IMA_RESULT_FILE_OPEN_FAILURE
80040002h	-2147221502	2147745794	IMA_RESULT_SESSION_REQUEST_DENIED
80040003h	-2147221501	2147745795	IMA_RESULT_JOB_NOT_FOUND
80040004h	-2147221500	2147745796	IMA_RESULT_SESSION_NOT_FOUND
80040005h	-2147221499	2147745797	IMA_RESULT_FILE_SEEK_FAILURE

Hex value	Signed value	Unsigned value	Mnemonic
80040006h	-2147221498	2147745798	IMA_RESULT_FILE_READ_FAILURE
80040007h	-2147221497	2147745799	IMA_RESULT_FILE_WRITE_FAILURE
80040008h	-2147221496	2147745800	IMA_RESULT_JOB_CANNOT_BE_UPDATED
80040009h	-2147221495	2147745801	IMA_RESULT_NO_TARGET_HOSTS
8004000Ah	-2147221494	2147745802	IMA_RESULT_NO_SOURCE_FILES
80060001h	-2147090431	2147876865	IMA_RESULT_ATTR_NOT_FOUND
80060002h	-2147090430	2147876866	IMA_RESULT_CONTEXT_NOT_FOUND
80060003h	-2147090429	2147876867	IMA_RESULT_VALUE_NOT_FOUND
80060004h	-2147090428	2147876868	IMA_RESULT_DATA_NOT_FOUND
80060005h	-2147090427	2147876869	IMA_RESULT_ENTRY_LOCKED
80060006h	-2147090426	2147876870	IMA_RESULT_SEARCH_HASMORE
80060007h	-2147090425	2147876871	IMA_RESULT_INCOMPLETE
80060008h	-2147090424	2147876872	IMA_RESULT_READEXCEPTION
80060009h	-2147090423	2147876873	IMA_RESULT_WRITEEXCEPTION
8006000Ah	-2147090422	2147876874	IMA_RESULT_LDAP_PARTIALINSTALL
8006000Bh	-2147090421	2147876875	IMA_RESULT_LDAP_NOTREADY

Hex value	Signed value	Unsigned value	Mnemonic
8006000Ch	-2147090420	2147876876	IMA_RESULT_BUFFER_TOO_SMALL
8006000Dh	-2147090419	2147876877	IMA_RESULT_CONTAINER_NOT_EMPTY
8006000Eh	-2147090418	2147876878	IMA_RESULT_CONFIGURATION_ERROR
8006000Fh	-2147090417	2147876879	IMA_RESULT_GET_BASEOBJECT
80060010h	-2147090416	2147876880	IMA_RESULT_GET_DERIVEDOBJECT
80060011h	-2147090415	2147876881	IMA_RESULT_OBJECTCLASS_NOTMATCH
80060012h	-2147090414	2147876882	IMA_RESULT_ATTRIBUTE_NOTINDEXED
80060013h	-2147090413	2147876883	IMA_RESULT_OBJECTCLASS_VIOLATION
80060014h	-2147090412	2147876884	IMA_RESULT_ENUMFAIL
80060015h	-2147090411	2147876885	IMA_RESULT_ENUMNODATA
80060016h	-2147090410	2147876886	IMA_RESULT_DBCONNECT_FAILURE
80060017h	-2147090409	2147876887	IMA_RESULT_TRUNCATE
80060018h	-2147090408	2147876888	IMA_RESULT_DUPLICATE
80060019h	-2147090407	2147876889	IMA_RESULT_PS_NOTINITIALIZED
8006001Ah	-2147090406	2147876890	IMA_RESULT_USING_ORACLE_7
8006001Bh	-2147090405	2147876891	IMA_RESULT_USING_ORACLE_8

Hex value	Signed value	Unsigned value	Mnemonic
8006001Ch	-2147090404	2147876892	IMA_RESULT_USING_ORACLE_UNKNOWN
8006001Dh	-2147090403	2147876893	IMA_RESULT_LOAD_DAO_ENGINE_FAILED
8006001Eh	-2147090402	2147876894	IMA_RESULT_COMPACT_DB_FAILED
80060033h	-2147090381	2147876915	IMA_RESULT_ODBC_NO_CONNECTIONS_AVAILABLE
80060034h	-2147090380	2147876916	IMA_RESULT_CREATE_SQL_ENVIRONMENT_FAILED
80060035h	-2147090379	2147876917	IMA_RESULT_SQL_EXECUTE_FAILED
80060036h	-2147090378	2147876918	IMA_RESULT_SQL_FETCH_FAILED
80060037h	-2147090377	2147876919	IMA_RESULT_SQL_BIND_PARAM_FAILED
80060038h	-2147090376	2147876920	IMA_RESULT_SQL_GET_COLUMN_DATA_FAILED
80060039h	-2147090375	2147876921	IMA_RESULT_REPLICATED_DATA_CONTENTION
8006003Ah	-2147090374	2147876922	IMA_RESULT_DB_TABLE_NOT_FOUND
8006003Bh	-2147090373	2147876923	IMA_RESULT_CONNECTION_EXIST
8006003Ch	-2147090372	2147876924	IMA_RESULT_QUERY_MAX_NODEID_FAILED
8006003Dh	-2147090371	2147876925	IMA_RESULT_SQL_FUNCTION_SEQUENCE_ERROR
8006003Eh	-2147090370	2147876926	IMA_RESULT_DB_CONNECTION_TIMEOUT
8006003Fh	-2147090369	2147876927	IMA_RESULT_SQL_INVALID_TRANSACTION_STATE

Hex value	Signed value	Unsigned value	Mnemonic
80060040h	-2147090368	2147876928	IMA_RESULT_DB_NO_DISK_SPACE
80060041h	-2147090367	2147876929	IMA_RESULT_USING_ORACLE_9
80060042h	-2147090366	2147876930	IMA_RESULT_TRANSACTION_ROLLEDBACK
80060043h	-2147090365	2147876931	IMA_RESULT_OCI_STILL_EXECUTING
80060044h	-2147090364	2147876932	IMA_RESULT_DATABASE_READONLY
80060045h	-2147090363	2147876933	IMA_RESULT_INVALID_CHANGE_ID
80080001h	-2146959359	2148007937	IMA_RESULT_MFS_REGISTRY_ERROR
80080002h	-2146959358	2148007938	IMA_RESULT_MFS_LOGONUSER_ERROR
80080003h	-2146959357	2148007939	IMA_RESULT_MFS_CREATEPROCESS_ERROR
80080004h	-2146959356	2148007940	IMA_RESULT_MFS_WINSTATION_ERROR
80080005h	-2146959355	2148007941	IMA_RESULT_MFS_WINCFG_ERROR
80080006h	-2146959354	2148007942	IMA_RESULT_MFS_BUFFER_OVERFLOW
80080007h	-2146959353	2148007943	IMA_RESULT_MFS_BUSY_TRY_LATER
80080008h	-2146959352	2148007944	IMA_RESULT_MFS_UNABLE_RESTART_NFUSE_SERVICE
80080009h	-2146959351	2148007945	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_ACR
8008000Ah	-2146959350	2148007946	IMA_RESULT_MFS_SERVER_FR_LEVEL_TOO_LOW

Hex value	Signed value	Unsigned value	Mnemonic
8008000Bh	-2146959349	2148007947	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_ICAKEEPALIVE
8008000Ch	-2146959348	2148007948	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_SPEEDBROWSE
8008000Dh	-2146959347	2148007949	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_CONNECT_TO_CONSOLE
8008000Eh	-2146959346	2148007950	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_RAVE
8008000Fh	-2146959345	2148007951	IMA_RESULT_MFS_SERVER_DOES_NOT_SUPPORT_SPEEDFLASH
80080010h	-2146959344	2148007952	IMA_RESULT_MFS_VIP_RANGE_OVERLAP
80080011h	-2146959343	2148007953	IMA_RESULT_MFS_VIP_RANGE_TOOSMALL
80080012h	-2146959342	2148007954	IMA_RESULT_MFS_VIP_END_ADDRESS_SMALLER_THAN_START
80080013h	-2146959341	2148007955	IMA_RESULT_MFS_VIP_INVALID_ADDRESS
80080014h	-2146959340	2148007956	IMA_RESULT_MFS_VIP_ADDRESS_NOT_ON_SAME_SUBNET
80080015h	-2146959339	2148007957	IMA_RESULT_MFS_VIP_ERROR_SAVING
80080016h	-2146959338	2148007958	IMA_RESULT_MFS_NO_ADAPTERS_CONFIGURED
80080017h	-2146959337	2148007959	IMA_RESULT_MFS_NO_ADAPTERS_ENABLED
800D0000h	-2146631680	2148335616	IMA_RESULT_CAPPSUB_UNKNOWN_APPTYPE
800D0001h	-2146631679	2148335617	IMA_RESULT_CAPPSUB_INSUFFICIENT_VERSION
800D0002h	-2146631678	2148335618	IMA_RESULT_CAPPSUB_NON_UNIQUE_FRIENDLYNAME

Hex value	Signed value	Unsigned value	Mnemonic
800D0003h	-2146631677	2148335619	IMA_RESULT_CAPPSUB_NON_UNIQUE_BROWSERNAME
800D0006h	-2146631674	2148335622	IMA_RESULT_CAPPSUB_APPLICATION_IS_DISABLED
800D000Bh	-2146631669	2148335627	IMA_RESULT_CAPPSUB_ILLEGAL_BROWSERNAME_CHARACTERS
800D000Ch	-2146631668	2148335628	IMA_RESULT_CAPPSUB_BROWSERNAME_TOO_LONG
800D000Eh	-2146631666	2148335630	IMA_RESULT_CAPPSUB_ILLEGAL_FRIENDLYNAME_CHARACTERS
800D000Fh	-2146631665	2148335631	IMA_RESULT_CAPPSUB_FRIENDLYNAME_TOO_LONG
80100001h	-2146435071	2148532225	IMA_BROWSER_RESULT_ERROR_IO_ERROR
80100002h	-2146435070	2148532226	IMA_BROWSER_RESULT_ERROR_WINSOCK_STARTUP
80100003h	-2146435069	2148532227	IMA_BROWSER_RESULT_ERROR_TIMER_CREATE
80100004h	-2146435068	2148532228	IMA_BROWSER_RESULT_INVALID_PARAMETER
80100005h	-2146435067	2148532229	IMA_BROWSER_RESULT_ERROR_NOT_ENOUGH_MEMORY
80100006h	-2146435066	2148532230	IMA_BROWSER_RESULT_ERROR_DATABASE_LOCATE
80100007h	-2146435065	2148532231	IMA_BROWSER_RESULT_ERROR_APPLICATION_LOCATE
80100008h	-2146435064	2148532232	IMA_BROWSER_RESULT_ERROR_NEIGHBORHOOD_LOCATE
80110101h	-2146369279	2148598017	LMS_RESULT_APP_NOT_FOUND
80110102h	-2146369278	2148598018	LMS_RESULT_SERVER_NOT_FOUND

Hex value	Signed value	Unsigned value	Mnemonic
80110103h	-2146369277	2148598019	LMS_RESULT_COLLECTORDB_NOT_FOUND
80110104h	-2146369276	2148598020	LMS_RESULT_NO_SERVER_AVAILABLE
80110105h	-2146369275	2148598021	LMS_RESULT_LOADEVALNAME_ERROR
80110106h	-2146369275	2148598022	LMS_RESULT_CANNOT_DELETE_DEFAULTLE
80110106h	-2146369273	2148598023	LMS_RESULT_CANNOT_DELETE_LE_IN_USE
80110200h	-2146369024	2148598272	IMA_RESULT_FULL_SERVER_OR_APP_LOAD_REACHED
80110201h	-2146369023	2148598273	IMA_RESULT_MAX_SERVERS_LM_DISABLED_HCA
80130001h	-2146238463	2148728833	IMA_RESULT_MORE_ITEMS
80130002h	-2146238462	2148728834	IMA_RESULT_INVALID_ACCOUNT
80130003h	-2146238461	2148728835	IMA_RESULT_INVALID_PASSWORD
80130004h	-2146238460	2148728836	IMA_RESULT_EXPIRED_PASSWORD
80130005h	-2146238459	2148728837	IMA_RESULT_GROUP_IGNORED
80130006h	-2146238458	2148728838	IMA_RESULT_BUILTIN_GROUP
80130007h	-2146238457	2148728839	IMA_RESULT_DC_NOT_AVAILABLE
80130008h	-2146238456	2148728840	IMA_RESULT_NW_CLIENT_NOT_INSTALLED
80130009h	-2146238455	2148728841	IMA_RESULT_ACCOUNT_LOCKED_OUT

Hex value	Signed value	Unsigned value	Mnemonic
8013000Ah	-2146238454	2148728842	IMA_RESULT_INVALID_LOGON_HOURS
8013000Bh	-2146238453	2148728843	IMA_RESULT_ACCOUNT_DISABLED
8013000Ch	-2146238452	2148728844	IMA_RESULT_PREFERRED_TREE_NOT_SET
8013000Dh	-2146238451	2148728845	IMA_RESULT_EXPIRED_ACCOUNT
8013000Eh	-2146238450	2148728845	IMA_RESULT_ADSOPEN_FAILED
8013000Fh	-2146238449	2148728847	IMA_RESULT_ADSOPEN_FAILED_NOTREG
80160001h	-2146041855	2148925441	IMA_RESULT_NODE_NOT_FOUND
80160002h	-2146041854	2148925442	IMA_RESULT_NODE_NAME_INVALID
80160003h	-2146041853	2148925443	IMA_RESULT_NODE_NOT_EMPTY
80160004h	-2146041852	2148925444	IMA_RESULT_NODE_MOVE_DENIED
80160005h	-2146041851	2148925445	IMA_RESULT_NODE_NAME_NOT_UNIQUE
80160006h	-2146041850	2148925446	IMA_RESULT_NODE_RENAME_DENIED
80160007h	-2146041849	2148925447	IMA_RESULT_CONSTRAINT_VIOLATION
80160008h	-2146041848	2148925448	IMA_RESULT_LDAP_PROTOCOL_ERROR
80160009h	-2146041847	2148925449	IMA_RESULT_LDAP_SERVER_DOWN
8016000Ch	-2146041844	2148925452	IMA_RESULT_NODE_DELETE_DENIED

Hex value	Signed value	Unsigned value	Mnemonic
8016000Fh	-2146041841	2148925455	IMA_RESULT_CANNOTCHANGE_PASSWORD
80160010h	-2146041840	2148925456	IMA_RESULT_CANNOTCHANGE_LAST_RW
80160011h	-2146041839	2148925457	IMA_RESULT_LOGON_USER_DISABLED
80160012h	-2146041838	2148925458	IMA_RESULT_CMC_CONNECTION_DISABLED
80160013h	-2146041837	2148925459	IMA_RESULT_INSUFFICIENT_SERVER_SEC_FOR_USER
80160014h	-2146041836	2148925460	IMA_RESULT_FEATURE_LICENSE_NOT_FOUND
80160015h	-2146041835	2148925461	IMA_RESULT_DISALLOW_CMC_LOGON
801C0000h	-2145648640	2149318656	IMA_RESULT_COMSRV_UNKNOWN_TYPE
801C0001h	-2145648639	2149318657	IMA_RESULT_COMSRV_INSUFFICIENT_VERSION
801C0003h	-2145648637	2149318659	IMA_RESULT_COMSRV_UNDEFINED_PARENTFOLDER
801C0004h	-2145648636	2149318660	IMA_RESULT_COMSRV_NON_UNIQUE_SERVERNAME
801C0005h	-2145648635	2149318661	IMA_RESULT_COMSRV_SERVERNAME_NOT_FOUND
801C0008h	-2145648632	2149318664	IMA_RESULT_COMSRV_NO_NAMES_FOUND
801C000Bh	-2145648629	2149318667	IMA_RESULT_COMSRV_REGISTRY_ERROR
801C000Ch	-2145648628	2149318668	IMA_RESULT_COMSRV_LOWER_VERSION
801C000Dh	-2145648627	2149318669	IMA_RESULT_COMSRV_ILLEGAL_BROWSERNAME_CHARACTERS

Hex value	Signed value	Unsigned value	Mnemonic
801C000Eh	-2145648626	2149318670	IMA_RESULT_COMSRV_BROWSERNAME_TOO_LONG
801C000Fh	-2145648625	2149318671	IMA_RESULT_COMSRV_REMOVE_SERVER_NOT_OFFLINE
801D1100h	-2145578752	2149388544	IMA_RESULT_MFAPP_DATASIZE_TOO_LARGE
801D1101h	-2145578751	2149388545	IMA_RESULT_MFAPP_ENUM_COMPLETE
801D1102h	-2145578750	2149388546	IMA_RESULT_MFAPP_VERSION_TOO_LARGE
801D1103h	-2145578749	2149388547	IMA_RESULT_MFAPP_READONLY
801D1104h	-2145578748	2149388548	IMA_RESULT_MFAPP_INVALID_CONFIG
801D1105h	-2145578747	2149388549	IMA_RESULT_MFAPP_UNABLE_RESET_APP
801D1106h	-2145578746	2149388550	IMA_RESULT_MFAPP_BRNAME_ILLEGAL_CHARS
801D1107h	-2145578745	2149388551	IMA_RESULT_MFAPP_ENUM_HAS_NOT_STARTED
801D1108h	-2145578744	2149388552	IMA_RESULT_MFAPP_ALREADY_IN_ENUM
801D1109h	-2145578743	2149388553	IMA_RESULT_MFAPPSS_MIGRATION_UNABLE_CREATE_LOG_FILE
801D110Ah	-2145578742	2149388554	IMA_RESULT_MFAPP_WORK_DIRECTORY_ILLEGAL_CHARS
801D110Bh	-2145578741	2149388555	IMA_RESULT_MFAPP_CACHE_IRRELEVANT_APP
801D110Ch	-2145578740	2149388556	IMA_RESULT_MFAPP_IRRELEVANT_IMS_INFO
801D110Dh	-2145578739	2149388557	IMA_RESULT_MFAPP_NOT_ALL_SERVERS_ENT

Hex value	Signed value	Unsigned value	Mnemonic
80240001h	-2145124351	2149842945	IMA_RESULT_IMS_NO_CONFIG_INFO
80240002h	-2145124350	2149842946	IMA_RESULT_IMS_INSTALLER_FAILURE
80240003h	-2145124349	2149842947	IMA_RESULT_IMS_LOGON_FAILED
80240004h	-2145124348	2149842948	IMA_RESULT_IMS_DUPLICATED_PKGS
80240005h	-2145124347	2149842949	IMA_RESULTS_IMS_PACKAGE_IN_USE
80240006h	-2145124346	2149842950	IMA_RESULT_IMS_OP_NOT_ALLOWED
80240007h	-2145124345	2149842951	IMA_RESULT_IMS_NOT_A_PACKAGE
80240008h	-2145124344	2149842952	IMA_RESULT_IMS_NETWORK_BROWSER_ERROR
80260001h	-2144993279	2149974017	IMA_RESULT_NW_PRINT_SERVER_ALREADY_PRESENT
80260002h	-2144993278	2149974018	IMA_RESULT_SERVER_ALREADY_PRESENT
8026000Ah	-2144993270	2149974026	IMA_RESULT_PRINT_SPOOLER_NOT_AVAILABLE
802D0001h	-2144534527	2150432769	IMA_RESULT_TABLE_NOT_FOUND
802D0002h	-2144534526	2150432770	IMA_RESULT_NOT_TABLE_OWNER
802D0003h	-2144534525	2150432771	IMA_RESULT_INVALID_QUERY
802D0004h	-2144534524	2150432772	IMA_RESULT_TABLE_OWNER_HAS_CHANGED
802D0005h	-2144534523	2150432773	IMA_RESULT_SERVICE_NOT_AVAILABLE

Hex value	Signed value	Unsigned value	Mnemonic
802D0006h	-2144534522	2150432774	IMA_RESULT_ZONE_MASTER_UNKNOWN
802D0007h	-2144534521	2150432775	IMA_RESULT_NON_UNIQUE_HOSTID
802D0008h	-2144534520	2150432776	IMA_RESULT_REG_VALUE_NOT_FOUND
802D0009h	-2144534519	2150432777	IMA_RESULT_PARTIAL_LOAD
802D000Ah	-2144534518	2150432778	IMA_RESULT_GATEWAY_NOT_ESTABLISHED
802D000Bh	-2144534517	2150432779	IMA_RESULT_INVALID_GATEWAY
802D000Ch	-2144534516	2150432780	IMA_RESULT_SERVER_NOT_AVAILABLE
802D000Dh	-2144534515	2150432781	IMA_RESULT_MAGIC_NUMBER_MISMATCH
802D000Eh	-2144534514	2150432782	IMA_RESULT_NOT_ZONE_MASTER
802D000Fh	-2144534513	2150432783	IMA_RESULT_IMA_ENCRYPTION_ERROR
802D0010h	-2144534512	2150432784	IMA_RESULT_INVALID_RANK
802D0010h	-2144534511	2150432785	IMA_RESULT_NO_CONTROLLERS_AVAILABLE
80300001h	-2144337919	2150629377	IMA_RESULT_SERVICE_NOT_SUPPORTED
80300002h	-2144337920	2150629378	IMA_RESULT_BUILD_SD_FAILED
80300003h	-2144337921	2150629379	IMA_RESULT_RPC_USE_ENDPOINT_FAILED
80300004h	-2144337922	2150629380	IMA_RESULT_RPC_REG_INTERFACE_FAILED

Hex value	Signed value	Unsigned value	Mnemonic
80300005h	-2144337923	2150629381	IMA_RESULT_RPC_LISTEN_FAILED
80300006h	-2144337924	2150629382	IMA_RESULT_BUILD_FILTER_FAILED
80300007h	-2144337925	2150629383	IMA_RESULT_RPC_BUFFER_TOO_SMALL
80300008h	-2144337926	2150629384	IMA_RESULT_REQUEST_TICKET_FAILED
80300009h	-2144337927	2150629385	IMA_RESULT_INVALID_TICKET
8030000Ah	-2144337910	2150629386	IMA_RESULT_LOAD_TICKETDLL_FAILED
80370064h	-2143879068	2151088228	IMA_RESULT_EVENT_QUEUE_FULL
80401100h	-2143284992	2151682304	IMA_RESULT_CONTENT_DATASIZE_TOO_LARGE
80401100h	-2143284992	2141682304	IMA_RESULT_RADEAPP_DATASIZE_TOO_LARGE
80401101h	-2143284991	2151682305	IMA_RESULT_CONTENT_ENUM_COMPLETE
80401101h	-2143284991	2151682305	IMA_RESULT_RADEAPP_ENUM_COMPLETE
80401102h	-2143284990	2151682306	IMA_RESULT_CONTENT_VERSION_TOO_LARGE
80401102h	-2143284990	2151682306	IMA_RESULT_RADEAPP_VERSION_TOO_LARGE
80401103h	-2143284989	2151682307	IMA_RESULT_CONTENT_READONLY
80401103h	-2143284989	2151682307	IMA_RESULT_RADEAPP_READONLY
80401104h	-2143284988	2151682308	IMA_RESULT_CONTENT_INVALID_CONFIG

Hex value	Signed value	Unsigned value	Mnemonic
80401104h	-2143284988	2151682308	IMA_RESULT_RADEAPP_INVALID_CONFIG
80401105h	-2143284987	2151682309	IMA_RESULT_UNABLE_RESET_APP
80401105h	-2143284987	2151682309	IMA_RESULT_UNABLE_RESET_APP
80401106h	-2143284986	2151682310	IMA_RESULT_CONTENT_BRNAME_ILLEGAL_CHARS
80401106h	-2143284986	2151682310	IMA_RESULT_RADEAPP_BRNAME_ILLEGAL_CHARS
80401107h	-2143284985	2151682311	IMA_RESULT_CONTENT_ENUM_HAS_NOT_STARTED
80401107h	-2143284985	2151682311	IMA_RESULT_RADEAPP_ENUM_HAS_NOT_STARTED
80401108h	-2143284984	2151682312	IMA_RESULT_CONTENT_ALREADY_IN_ENUM
80401108h	-2143284984	2151682312	IMA_RESULT_RADEAPP_ALREADY_IN_ENUM
80401109h	-2143284983	2151682313	IMA_RESULT_CONTENT_VERSION_MISMATCH
80401109h	-2143284983	2151682313	IMA_RESULT_RADEAPP_VERSION_MISMATCH
80480001h	-2142765055	2152202241	IMA_RESULT_SESSION_GUID_CREATION_FAILED
80480002h	-2142765054	2152202242	IMA_RESULT_INVALID_SESSION_GUID
80480003h	-2142765053	2152202243	IMA_RESULT_MISMATCHED_INPUT_SESSIONS
80480004h	-2142765052	2152202244	IMA_RESULT_DISALLOWED_SESSION_OPERATION
80480005h	-2142765051	2152202245	IMA_RESULT_FAILED_TO_LOAD_DLL

Hex value	Signed value	Unsigned value	Mnemonic
80480006h	-2142765050	2152202246	IMA_RESULT_FAILED_TO_LOCATE_FUNCTION
80480007h	-2142765049	2152202247	IMA_RESULT_WRONG_TARGET_RADE_SERVER
80480008h	-2142765048	2152202248	IMA_RESULT_FAILED_TO_ACQUIRE_LICENSE
80480009h	-2142765047	2152202249	IMA_RESULT_NO_ADDON_LICENSE
8048000Ah	-2142765046	2152202250	IMA_RESULT_EVENT_NOT_SUPPORTED