Citrix XenApp Fundamentals Administrator’s Guide
Contents

1 Introduction ................................................................. 7
   How to Use this Guide .................................................. 7
   Finding Documentation .................................................. 7
   Documentation Conventions ............................................. 7
   Getting Support and Training .......................................... 8
   Introducing XenApp Fundamentals .................................... 8
   XenApp Fundamentals Features ....................................... 9
   Accessing Centralized Applications ................................. 10
   What’s New in this Release ............................................. 11
   Support for Windows Server 2008 ..................................... 11
   Integration with Windows Essential Business Server 2008 ....... 11
   External Access with ISA Server ...................................... 11
   Full SpeedScreen Support .............................................. 12
   Planning Deployments .................................................. 12
   External Access Scenarios ............................................. 12
   Users ........................................................................... 14
   Administrators .................................................................. 15

2 Deploying XenApp Fundamentals ........................................... 17
   Before You Start ............................................................. 18
   Installation Overview ..................................................... 18
   Installing XenApp Fundamentals on a Domain Controller ........ 19
   System Requirements ..................................................... 19
   Access Gateway ............................................................. 20
   Installing XenApp Fundamentals ....................................... 23
   Removing XenApp Fundamentals ........................................ 25
   Setting Up Application Servers ...................................... 25
   Setting Up DMZ Servers .................................................. 26
   Installing XenApp Fundamentals for Windows Essential Business Server ......................................................... 26
   Quick Start Tool Overview ............................................. 27
   Essential Business Server Overview ................................. 31
Licensing XenApp Fundamentals. ................................. 33
Adding Your First License ........................................ 33
Activate Terminal Server License Server ...................... 34
Providing Access to Applications ............................... 35
Ensuring Applications Are Available ......................... 35
Publishing Applications ......................................... 35
Testing Your Internal Access Deployment ................... 36
Providing External Access ........................................ 37
Security Requirements. .......................................... 37
Using Internet Protocol ......................................... 38
External Access Direct to Server ................................. 42
External Access Using a Local Domain Certificate .......... 44
Configuring External Access for ISA Server ................. 47
External Access Using a Temporary Certificate ............ 49
External Access with a DMZ Server ............................ 51
External Access Using a VPN .................................... 52
Testing External Access ......................................... 53
Configuring Authentication ...................................... 53
Setting Up Administrator Accounts ......................... 54
Configuring Email Alerting ..................................... 55
To enable email alerting ........................................ 57
To disable email alerting ...................................... 58
Providing Access to Printers .................................... 58
Windows Managed Printers ...................................... 59
Enabling Client Printers ........................................ 60
Publishing Network Printers .................................... 60
Enabling Both Client and Published Printers ............... 61
Using Advanced Mode ........................................... 63
Setting Up Servers .............................................. 63
Setting Up Server Failover ..................................... 64
Setting Up User Profiles ....................................... 65
Managing Tasks with Essential Business Server ............ 66
Servers .......................................................... 66
Sessions ........................................................ 66
Licenses ......................................................... 67
Applications ................................................... 67
Making XenApp Fundamentals Available to Users .......... 67

3 Managing XenApp Fundamentals .............................. 69
Managing Users ................................................ 69
Managing Individual Users .......................................................... 70
  To manage access for a specific user .................................. 70
Managing User Access to Applications ........................................... 70
  To add users to or remove users from applications ................. 70
  To modify user and group access to applications .................... 71
Managing User Licenses ............................................................... 71
  Transferring Licenses ............................................................ 71
Managing Sessions ................................................................. 72
  Viewing Session Details ....................................................... 73
  Sending Messages ............................................................... 73
  Ending Sessions ..................................................................... 73
  Disconnecting Sessions .......................................................... 74
  Shadowing Sessions ............................................................... 74
Managing Published Applications .................................................. 76
  Modifying Published Application Settings .............................. 76
  Removing Published Applications .......................................... 78
  Viewing Application Information .......................................... 78
  Publishing Content ............................................................... 79
  Publishing the Desktop .......................................................... 80
Managing Licenses ........................................................................ 81
  About XenApp Fundamentals Licenses ...................................... 81
  Migrating from an Evaluation to a Retail License .................... 82
  Installing Additional Licenses ................................................. 82
Managing Administrator Accounts ................................................ 83
  Adding Administrator Accounts .............................................. 83
  Removing Administrator Accounts ......................................... 83
  Managing XenApp Fundamentals Remotely .............................. 83
Performing Server Maintenance ..................................................... 84
  To perform server maintenance .............................................. 84
  To restore a server after maintenance .................................. 85
Managing Printers ......................................................................... 85
  Setting a Default Printer ....................................................... 85
  Clearing a Default Printer .................................................... 86
  Removing a Printer ............................................................... 86
  Enabling Client Printing after Setup ...................................... 86
  Adding Published Printers .................................................... 87
Managing Certificates ................................................................... 88
  Creating and Importing a New Certificate ............................... 88
Using Advanced Application Settings .......................................... 89
  Configuring Optimization Settings ......................................... 89
4 Securing XenApp Fundamentals ................................................. 91

- Securing the Environment .................................................. 91
- Overview of Security, SSL, and Certificates ............................... 91
- The SSL Protocol .............................................................. 92
- About Cryptography .......................................................... 92
- Certificates and Certificate Authorities .................................... 92
- Obtaining a Digital Certificate .............................................. 93
- Creating a Certificate Backup .............................................. 95
- Renewing Security Certificates ............................................. 96
- User Names and Passwords .................................................. 96
- User Authentication ............................................................ 97
  - Enabling Standard Authentication ........................................ 97
  - Enabling Secure Computing SafeWord for Citrix ....................... 98
  - Enabling RSA SecurID ...................................................... 98
Introduction

This chapter introduces you to Citrix XenApp Fundamentals. Topics include:

- How to use this guide
- Key product features and benefits
- What’s new in this release
- Planning your deployment

How to Use this Guide

The *Citrix XenApp Fundamentals Administrator’s Guide* is for system administrators responsible for installing, configuring, and maintaining XenApp Fundamentals.

This is a task-based guide to help you set up XenApp Fundamentals quickly and easily. This chapter introduces the XenApp Fundamentals product. Subsequent chapters explain how to install, configure, and manage XenApp Fundamentals.

This guide assumes knowledge of basic Windows server administration.

Finding Documentation


Known issues information is included in the product readme.

Documentation Conventions

For consistency, Windows Vista and Windows Server 2008 (32-bit) terminology is used throughout the documentation set; for example, “Documents” rather than “My Documents” and “Computer” rather than “My Computer” are used.

Citrix XenApp Fundamentals documentation uses the following typographic conventions.
Getting Support and Training

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

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

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

Introducing XenApp Fundamentals

Citrix XenApp Fundamentals enables five to 75 persons to remotely use corporate Windows programs conveniently and securely over the Web. Unlike other remote access alternatives, it performs well across slow connections, strict network firewalls, and non-Windows computers without needing to rewrite applications, upgrade computers, or increase bandwidth.

Its simple role-based rules control which central resources individuals see and where they store and print sensitive information. Newly arriving Internet and internal LAN users are automatically load-balanced among available application servers, providing users application access seamlessly from anywhere at any time. The product comes with or without Microsoft Terminal Server Client Access Licenses (CALs).
XenApp Fundamentals Features

This section describes the key features and benefits of XenApp Fundamentals. A typical XenApp Fundamentals deployment is depicted below.

This centrally managed environment provides the following benefits to XenApp Fundamentals users and system administrators:

**Administrators**

- Centralized application deployment and management to minimize administrative effort
- Intuitive, wizard-driven administration, monitoring, and troubleshooting
- Role-based privileges to control who gets what
- Requires only one secure port to be open on the external firewall to gain remote access
- Automatic load-balancing across multiple application servers ensures best user access experience
- No need to rewrite applications, upgrade computers, or increase network bandwidth

**Users**

- Simple, secure, Web access to Windows applications, intranet sites, and shared files from almost anywhere using a basic Internet connection and a supported Web browser
• Responsive communications from remote offices, home, hotels, airports, customer sites, and mobile devices across firewalls even over relatively slow lines (as little as 20Kbps)

• Remote digital image capture from cameras and scanners as well as audio inputs for recording voice and dictations remotely

• Printing to central and locally attached printers

**Accessing Centralized Applications**

XenApp Fundamentals’ Web-based interface presents users with a personalized choice of applications, files, and Web sites that are centrally maintained on one or more of your internal Windows servers. Authorized persons can reach these resources from almost anywhere using a basic Internet connection and a standard Web browser, even from non-Windows computers and mobile computers. This makes it possible for them to run business applications when they are away from the main office, at home, traveling, or at a remote site, without compromising performance or security. As importantly, it helps safeguard an organization’s sensitive records by keeping them stored on internal servers rather than on a user’s PC or laptop where the files might be easily lost or stolen.

Administratively, it is also far simpler and less time consuming, particularly if you currently handhold a number of users with few computer skills through difficult software and computer upgrades. Now you can update or add applications from a server and instantly make them available to your users without needing to touch the user’s computers.

For these reasons, many customers who purchase XenApp Fundamentals to support their remote personnel soon realize that it also helps to support users working on their internal LAN.

**User Perspective**

Users connect to the XenApp Fundamentals server by pointing their Web browser to a predefined URL, where they are prompted for logon credentials. Once authenticated, they see icons corresponding to applications and files that you, as administrator, choose to make available to them based on their role in the organization.

Users simply click the relevant icon to remotely launch the required program on the server. The software takes care of redirecting screen displays and audio output back to the user over the network as if the program was running on their local computer. Keystrokes and mouse clicks are transparently sent back to the application to complete the illusion (sometimes referred to as application virtualization).
Easier to Get Started
During the initial setup, XenApp Fundamentals automatically discovers applications installed on the server and lets you quickly publish them to a group of users or to individuals. This in effect makes the applications visible only to the users whom you specified. For example, you could hide the general ledger from anyone except the accountants. You can also choose to publish specific shared files, which are referred to in the product as content.

A small piece of software called a Citrix XenApp plugin must be loaded once on each user’s computer to coordinate the remote sessions. The latest versions of the plugins can be launched automatically when users connect to your site, or they can be downloaded from http://www.citrix.com.

What’s New in this Release
Citrix XenApp Fundamentals 3.1.0 offers the following enhancements and features:

Support for Windows Server 2008

Integration with Windows Essential Business Server 2008
Most day-to-day management tasks that you perform with the Quick Start tool are now also available in the Windows Essential Business Server management console.

After installing the XenApp Fundamentals plugin, you can use the Essential Business Server console to select server groups, revoke licenses, send messages to and log off users, and modify user access to applications. Additionally, you can launch the full Quick Start tool to perform more tasks.

External Access with ISA Server
You can now configure an alternative SSL port to allow Internet Security and Acceleration Server 2006 (ISA Server) to route SSL connections directly to the server running XenApp Fundamentals.
Full SpeedScreen Support

XenApp Fundamentals now includes all SpeedScreen features, such as multimedia acceleration and flash acceleration. SpeedScreen improves the usability of any application where users need to scroll or move 2D graphics. For more information about using SpeedScreen and a description of its features, see the Citrix XenApp Administrator's Guide.

Planning Deployments

When planning your XenApp Fundamentals deployment, some points to consider are:

- How users will connect to the server
- How users will access applications
- How much control to give administrators

For more details about how to get XenApp Fundamentals up and running, see “Deploying XenApp Fundamentals” on page 17.

External Access Scenarios

XenApp Fundamentals is usually deployed in one of the following scenarios:

**Direct to server.** This is the simplest deployment. It relies only upon a firewall to separate the XenApp Fundamentals server from the public Internet. All external user sessions are secured using the built-in SSL/VPN software module known as Secure Gateway.

**DMZ.** In this scenario, a server is placed between two firewalls to constitute a demilitarized zone (DMZ). This configuration further protects the corporate LAN from external security attacks, while allowing more protocols to be used from external devices.

**VPN.** The XenApp Fundamentals server is separated from the public network using a virtual private network (VPN) device.
Deployment Scenario 1: Direct to Server
This deployment provides secure access to applications. You do not require any additional hardware or software to enable access for your external and mobile users. As shown below, external users connect to XenApp Fundamentals through a firewall.

Users enter their domain credentials (user name, password, and domain) to connect to XenApp Fundamentals through the Citrix Web Interface. For external users, you can increase security by enabling two-factor authentication (see “Configuring Authentication” on page 53).

The deployment comprises the following components:

**XenApp Fundamentals.** The XenApp Fundamentals server or servers host the published applications that users can run. The servers also provide the following:

- **Web Interface.** A built-in software module that enables applications published with XenApp Fundamentals to be accessed by users from a supported Web browser.
- **Secure Gateway.** Another built-in software module responsible for securely transmitting and routing external user sessions.
- **Quick Start tool.** Used to easily set up and manage your deployment.

**Client Device.** Users access their applications from a client device. A client device is any computer capable of running a supported plugin and a supported Web browser (see “Client Device Requirements” on page 21). Client devices include desktop PCs, laptops, mobile PCs, thin client terminals, and network computers.

Users log on, view, and access their applications using a standard Web browser. When they launch an application, a session is initiated between the XenApp Fundamentals servers and the client device.
Deployment Scenario 2: Demilitarized Zone
Combining XenApp Fundamentals with a demilitarized zone (DMZ) provides enhanced security against attacks originating in public networks. This provides secure external access to internal network resources without requiring changes to applications or the Domain Name Service (DNS).

Deployment Scenario 3: Virtual Private Network
A virtual private network (VPN) device isolates the trusted internal network (such as a corporate private LAN) from the untrusted external network (such as the Internet).

Users
When planning your deployment, you must consider how users will use the centralized resources made available by XenApp Fundamentals. You can have internal and external users:

- **Internal.** Users who access the central servers from within your trusted internal network using an internal Web interface address (URL) mapped to TCP port 80.

- **External.** Users who access the central servers from outside your trusted internal network using an external Web interface address (URL) mapped to a TCP port.
Administrators

When planning your deployment, you must determine who should be given administrator rights and what level of administrative privileges are required. There are two types of XenApp Fundamentals administrator:

- Full administrator
- Delegated administrator

Both types of administrator require background knowledge of computer and communication systems. See “Managing XenApp Fundamentals” on page 69.

**Full administrator.** Full administrators have the ability to install and configure all aspects of the deployment.

Full administrators can manage servers, publish applications, determine which users in the organization can access which published applications, configure external access, publish and manage printers, and manage licenses.

Any local administrators and Active Directory domain administrators are automatically made full administrators in XenApp Fundamentals. Similarly, when you create a full administrator, XenApp Fundamentals automatically adds them to the Administrators group on the local server.

**Delegated administrator.** Delegated administrators have access to a subset of the functions available to full administrators. The **Setup Tasks** tab in the Quick Start tool and the tasks that appear on it are not available to delegated administrators. They can monitor the server and user sessions without the authority to change the configuration. Delegated administrators can also send messages to users and shadow their sessions; however, they cannot install or configure XenApp Fundamentals. (For example, they cannot publish new applications.)
Deploying XenApp Fundamentals

This chapter explains how to install and get XenApp Fundamentals up and running quickly using the Quick Start tool, and how to use the XenApp Fundamentals features in Windows Essential Business Server 2008. Topics include:

• Installing XenApp Fundamentals
• Quick Start tool overview
• Windows Essential Business Server overview
• Licensing XenApp Fundamentals
• Providing access to applications
• Enabling secure external access
• Configuring authentication
• Setting up administrator accounts
• Configuring email alerting
• Setting up printers
• Using advanced mode
• Managing tasks with Essential Business Server
• Making XenApp Fundamentals available to users
Before You Start

Installation Overview

Before you begin your software deployment, you must determine your requirements, including:

- **Administrators.** At least one full administrator is required to install XenApp Fundamentals. The administrator installing XenApp Fundamentals is automatically assigned full administrator privileges. You must decide what other administrators (full and delegated) need to be assigned.

- **External Access and Security.** You must determine whether users will be working onsite or externally, and what sort of security is needed for external access. As well as standard authentication, you can enable two-factor authentication for external access.

- **Applications and Users.** You must determine which installed applications you want to publish, and to whom. If you run XenApp Fundamentals in advanced mode, we recommend that users use domain user accounts and not local user accounts. Because they do not have domain privileges, local user accounts may cause the profile management feature to malfunction.

**Important:** Citrix recommends that all applications be installed on the computer running XenApp Fundamentals using the Programs and Features wizard.

**Note:** With client-server applications on XenApp Fundamentals, the client portion of the implementation is installed on the XenApp Fundamentals server rather than on the user’s desktop. The file or database server portion of the installation is implemented as usual on a back-end machine.

- **Printers.** You must determine what printers need to be made available to your users.

There are two steps to your XenApp Fundamentals deployment:

- **Installation.** You install XenApp Fundamentals using the Setup utility, which runs automatically when you insert the product media in your computer or when you launch the downloaded image. This also provides an Uninstall function for future use.
• **Configuration.** You configure XenApp Fundamentals using the Quick Start tool. See “Quick Start Tool Overview” on page 27 for more information.

**Installing XenApp Fundamentals on a Domain Controller**

Domain controllers are not recommended for serving applications for security and performance reasons. If you install XenApp Fundamentals on a domain controller, consider the following points:

• Any user rights policies applied to the server also apply to any other domain controllers in the domain

• Domain controllers cannot be used as part of a multiserver XenApp Fundamentals deployment

Only install XenApp Fundamentals on a domain controller if you accept the restrictions imposed, are confident of the security of applications served from the computer, and also trust all users.

**System Requirements**

XenApp Fundamentals 3.1.0 must be installed on the server running Windows Server 2008 (Standard or Enterprise edition). Only 32-bit versions of the Windows operating system are supported.

If you are running Windows Server 2003, you must install Access Essentials 2.0. If you have servers running both operating systems, install the appropriate version of XenApp Fundamentals on each machine and manage them separately.

If you are using Active Directory, add the computer running XenApp Fundamentals to the directory before installation. XenApp Fundamentals can be part of a Windows workgroup or domain.

XenApp Fundamentals Setup checks that all required Windows system components are present on your machine. If any are missing, Setup prompts you to install the missing components. Setup also checks the Windows version and installs the appropriate version of XenApp Fundamentals.

To enable secure external access for direct to server deployments, you need to use a valid security certificate. Some certificate agencies may take several days to issue public key certificates. If required, you can generate a temporary certificate to implement external access immediately while you wait for your permanent certificate to arrive. See “External Access Direct to Server” on page 42.
Access Gateway

If the Citrix Access Gateway universal SSL VPN is part of the deployment, install and configure the VPN appliance first, as detailed in the documentation provided with this product.

Firewall Configuration

Direct to Server Deployment

If XenApp Fundamentals is configured to allow external access, a firewall must be in place between the public network and the XenApp Fundamentals server. Configure the firewall to allow access only to a specific port (HTTPS) on the server.

<table>
<thead>
<tr>
<th>Source address</th>
<th>Source TCP port</th>
<th>Incoming TCP port</th>
<th>Forward to address</th>
<th>Forward to TCP port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>443</td>
<td>Server or server group address</td>
<td>443</td>
</tr>
</tbody>
</table>

XenApp Fundamentals uses only a single active network interface card (NIC) with a single allocated IP address, even if the server is equipped with additional NICs. You are responsible for ensuring that the Fully Qualified Domain Name (FQDN) for XenApp Fundamentals (the common name in the SSL certificate) resolves to the server’s IP address. Citrix recommends using static IP addresses rather than DHCP or Automatic Private IP Addressing for XenApp Fundamentals IP address configuration.

DMZ Deployment

If XenApp Fundamentals is configured to allow external access using a DMZ, you must configure two firewalls.

<table>
<thead>
<tr>
<th>Source address</th>
<th>Source TCP port</th>
<th>Incoming TCP port</th>
<th>Forward to address</th>
<th>Forward to TCP port</th>
</tr>
</thead>
<tbody>
<tr>
<td>(External) Any</td>
<td>Any</td>
<td>Any</td>
<td>DMZ</td>
<td>443</td>
</tr>
<tr>
<td>(Internal) DMZ IP address</td>
<td>Any</td>
<td>1080</td>
<td>Server or server group address</td>
<td>1080</td>
</tr>
</tbody>
</table>

Virtual Private Network Deployment

If you are using an internal firewall and running XenApp Fundamentals in single server (basic) mode, the firewall between the VPN and the XenApp Fundamentals server must be configured as follows:
If you are running XenApp Fundamentals on multiple servers (advanced mode), each server’s NAT mappings are configured separately in the Quick Start tool. For example:

<table>
<thead>
<tr>
<th>Source address</th>
<th>Source TCP port</th>
<th>Incoming TCP port</th>
<th>Forward to address</th>
<th>Forward to TCP port</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Any</td>
<td>8080</td>
<td>XenApp Fundamentals</td>
<td>8080</td>
</tr>
<tr>
<td>VPN</td>
<td>Any</td>
<td>User Defined</td>
<td>XenApp Fundamentals</td>
<td>2598</td>
</tr>
<tr>
<td>VPN Optional: only if you want to support Remote Desktop Protocol (RDP) connections.</td>
<td>Any</td>
<td>User Defined</td>
<td>XenApp Fundamentals</td>
<td>3389</td>
</tr>
</tbody>
</table>

If you are using an external firewall, consult your VPN documentation for configuration details.

**Client Device Requirements**

After you install XenApp Fundamentals and publish your resources, users can run their applications from virtually any client device and platform with a supported Web browser.
To operate with XenApp Fundamentals, your client devices must have a supported plugin and Web browser. Compatible plugins are included on the product media and are also available for free download from the Citrix Web site.

Supported devices include:

- Java-enabled devices
- Linux and Solaris operating systems
- Windows CE handheld computers and Windows-based terminals
- MacOS X

Supported Web browsers include:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X</td>
<td>Safari 2.0</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>Mozilla 1.x</td>
</tr>
<tr>
<td>Symbian Nokia E61 and Nokia E70</td>
<td>Symbian</td>
</tr>
<tr>
<td>Windows Mobile 2005</td>
<td>Pocket IE</td>
</tr>
<tr>
<td>WinCE.NET 4.2</td>
<td>Internet Explorer 6.0</td>
</tr>
<tr>
<td>WinCE 5.0 and 6.0</td>
<td>Internet Explorer 6.0</td>
</tr>
<tr>
<td>Windows XPe with Service Pack 1</td>
<td>Internet Explorer 6.0</td>
</tr>
</tbody>
</table>
Citrix recommends that you install the latest plugins on your user’s devices to ensure that they take advantage of the latest features.

**Important:** You must install appropriate plugins on non-Windows devices before launching applications through XenApp Fundamentals. If you do not, any attempt to launch the application will likely fail.

Most Windows devices without an appropriate plugin installed invoke an automatic download of the plugin when you log on to XenApp Fundamentals. This requires the XenApp Fundamentals site to be defined as either a **Trusted site** or **Local intranet zone** in Internet Explorer (under **Tools > Internet Options > Security**).

---

**Installing XenApp Fundamentals**

You install XenApp Fundamentals using the product media or a downloaded image.

**Important:** Citrix recommends that you install XenApp Fundamentals before installing either RSA SecurID or Secure Computing SafeWord agent packages. Additionally, do not rename servers after you have installed XenApp Fundamentals. To change the server name, you must remove XenApp Fundamentals from that server, change the server name, then reinstall XenApp Fundamentals.

**Note:** You need to restart the server at least once during installation.

---

**To install XenApp Fundamentals**

1. Log on to the server as an administrator.

2. Insert the product media in the appropriate drive on the server, or locate the electronically downloaded image.

   The Citrix XenApp Fundamentals Setup screen appears.

3. Click **Install**. The License Agreement page appears.

4. Read the licensing information. Select **I accept the license agreement** if you accept the license agreement and click **Next**.

5. On the **Installation type** page, choose one of the following options and click **Next**:
• **Application server.** A full installation of XenApp Fundamentals on a server capable of publishing applications.

• **Network access (DMZ) server.** An installation on a DMZ server. If you select this option, the installation skips the remaining steps and Setup starts installing XenApp Fundamentals.

6. On the **Configure Shadowing** page, determine whether to enable or disable shadowing XenApp Fundamentals user sessions.

Shadowing enables administrators to oversee a user’s session activity from a remote device, as if they were sitting beside the user. See “Shadowing Sessions” on page 75 for more information.

- In some organizations and in some countries, shadowing is not permitted due to privacy concerns or mandates. If this is the case, select **Disable shadowing** and click **Next**.
- If you want to allow shadowing, make sure the **Disable shadowing** box is clear and click **Next**.

**Note:** If you select **Disable shadowing** and later need to enable shadowing, you must remove and then reinstall XenApp Fundamentals.

7. Setup starts installing XenApp Fundamentals automatically. The process checks that all the required software components are present on the server.

8. Restart your computer when prompted.

9. Log on using the same credentials you used to log on at the beginning of the installation.

10. When the installation is complete, click **Finish**. The Quick Start tool appears.

Use the Quick Start tool to configure your XenApp Fundamentals implementation.

**Upgrading an Existing Installation**

You cannot upgrade from Access Essentials 2.0 to XenApp Fundamentals 3.1.0. To use XenApp Fundamentals 3.1.0, you must follow the installation process in the previous section.
Removing XenApp Fundamentals

XenApp Fundamentals can be removed using the Setup tool on the installation media. This removes all components of XenApp Fundamentals except for those shared by other applications. Additionally, you can remove XenApp Fundamentals using the Programs and Features wizard.

To remove XenApp Fundamentals
1. Insert the software Setup media in the appropriate drive to run installation automatically or click on the .iso file from the downloaded image.
2. Select Uninstall from the Setup dialog box.

Setting Up Application Servers

If you selected the Application Server option during installation, the Set Up Server wizard automatically launches when you start the Quick Start tool for the first time. This allows you to configure the server in either basic or advanced mode.

Basic mode allows you to run XenApp Fundamentals on a single stand-alone server. Advanced mode allows you to run XenApp Fundamentals on multiple servers, with one server acting as a master (used for tasks such as failover, profile management, and managing server groups) and one or more servers acting as a support server. Support servers are added to the master to create server groups.

To set up the server
1. Click Next.
2. Select New single server (basic mode) or New server group (advanced mode).
3. Click Next.
4. If you selected single server (basic mode), click Finish to complete the wizard.
5. If you want the server to be the master of a server group, enter a name for the group in the Server Group Name field. Click Next.
6. Click Browse to create organizational units in Active Directory in a specified location.
7. Select the location and click OK.
8. Click Finish to complete the wizard.

You are returned to the Overview page.
Setting Up DMZ Servers

If you selected the Network access (DMZ) server option during installation, the Manage External Access Wizard automatically launches when you start the Quick Start tool for the first time.

For more information about using external access, see “Providing External Access” on page 37.

To set up the server
1. Click Next.
2. Enter the internal firewall address. If you are not using an internal firewall, enter the address of the master server. Click Next.
3. If a server certificate is not located, enter the external address of the server to generate a server certificate request. Click Next.
4. Enter your organization name and organizational unit. Click Next.
5. Enter your company’s geographical information. Click Next.
6. Specify the source of your certificate. Click Next.
7. Specify the file name and location of your root certificate. Click Next.
8. Click Finish to complete the wizard.

Installing XenApp Fundamentals for Windows Essential Business Server


To install the XenApp Fundamentals plugin
2. Click the EBSConsole.msi file.
   The Welcome page in the installation wizard appears.
3. Click Next.
   The License Agreement page appears.
4. Select I accept the terms in the License Agreement and click Next.
5. Click Install to begin the installation.
6. Click **Finish** to complete the installation and exit the Setup Wizard.

Before you launch the Essential Business Server Management Console, ensure that XenApp Fundamentals is running in advanced mode, and that all of the XenApp Fundamentals servers you want to manage are in the same domain.

**Quick Start Tool Overview**

You configure XenApp Fundamentals using the administrative functions in the Quick Start tool.

The Quick Start tool enables you to:

- License XenApp Fundamentals.
- Publish and configure applications. Publishing applications allows users to run the applications installed on the server.
- Publish content.
- Publish the server desktop.
- Grant users and groups access to published applications, content, and desktops.
- Enable and configure external access for your external users.
- Add and manage XenApp Fundamentals administrators.
- Configure email alerting.
- Define printers for use with XenApp Fundamentals.
- Manage individual servers and server groups.
- View and remove licenses from individual users.
- View and modify application settings.
- Manage user sessions.
- Access advanced management tools (such as the Access Management Console and Connection Configuration).

**Important:** Citrix recommends that you do not use advanced management tools unless you are familiar with Citrix XenApp and Windows Server administration.
Quick Start Tool Overview Screens
There is an Overview screen for each tab in the Quick Start tool. These summarize the main tasks that you can perform using the links on each tab, as shown in the example below:

**Setup**
- Links to XenApp Fundamentals configuration tasks

**Overview**
- XenApp Fundamentals status and links to tasks to get started

**Resources**
- Links to Citrix and Microsoft tools.
  - For advanced users only

**Management**
- Links to view and manage XenApp Fundamentals users, applications, licenses, and sessions.

The tabs in the Quick Start tool are:

**Setup**
This tab provides links to the tasks that full administrators need to perform after installing XenApp Fundamentals but before users can use the product. Infrequent configuration tasks are also included here. This tab is not available to delegated administrators because they are not permitted to perform these tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>Install and upgrade XenApp Fundamentals licenses and activate the Terminal Server License Server. See “Licensing XenApp Fundamentals” on page 33. This task is not available on support servers.</td>
</tr>
</tbody>
</table>
Management
This tab provides links to day-to-day management tasks and can be accessed by delegated administrators:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management</td>
<td>View and manage user application access, licenses, and sessions. See “Managing Users” on page 69.</td>
</tr>
<tr>
<td>Applications</td>
<td>Configure user and group access to applications that are already published. See “Managing User Access to Applications” on page 70.</td>
</tr>
<tr>
<td>Licensing</td>
<td>View and revoke licenses for users. See “Managing User Licenses” on page 71.</td>
</tr>
<tr>
<td>Sessions</td>
<td>View the list of users who are currently connected to applications and troubleshoot their connections. See “Managing Administrator Accounts” on page 83.</td>
</tr>
</tbody>
</table>

Resources
This tab contains links to advanced Citrix and Microsoft configuration tools.
**Important:** XenApp Fundamentals provides access to Citrix tools for advanced administrators. These tools reference modules in Citrix XenApp. The names of those management consoles are preserved for consistency. Do not attempt to use these management tools unless you are an advanced user familiar with Citrix XenApp and Windows Server administration.

The Citrix resources are as follows:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenApp Advanced Configuration</td>
<td>This starts the Citrix XenApp Advanced Configuration tool. This is for advanced users only. See “Managing XenApp Fundamentals” on page 69.</td>
</tr>
<tr>
<td>Access Management Console</td>
<td>This starts the Citrix Access Management Console. This console allows you to configure and maintain your server. This is for advanced users only.</td>
</tr>
<tr>
<td>Citrix Support</td>
<td>This link takes you to the Citrix Support Web site for information and help for XenApp Fundamentals and other Citrix products.</td>
</tr>
</tbody>
</table>

The Microsoft resources are as follows:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Configuration</td>
<td>This allows you to manage the connections between clients and XenApp Fundamentals. You can specify how different types of incoming connections are handled, and set properties for sessions launched using those connection types. This is for advanced users only.</td>
</tr>
<tr>
<td>Terminal Services Manager</td>
<td>This starts the Microsoft Terminal Services Manager. Using this tool, you can view information about sessions, users, and processes.</td>
</tr>
<tr>
<td>Terminal Services Licensing</td>
<td>This link starts the Microsoft Terminal Server Licensing tool. Microsoft Terminal Services Client Access licenses (TSCALs) are included with your Citrix licenses. The Microsoft Terminal Services License Server must be activated for correct operation.</td>
</tr>
</tbody>
</table>
Quick Start Tool Task Screens
Each task screen has a consistent format. An example **Applications** screen is shown below:

Essential Business Server Overview
XenApp Fundamentals integration with Essential Business Server combines software for management, messaging, and security in a multi-server solution designed for midsize businesses. Essential Business Server provides the following features:

- All remote sessions are coordinated with the ISA server for optimum performance and security
- Multi-server automatic load balancing and profile management take full advantage of the underlying Active Directory structure
- Built-in monitoring and alerting functions transparently communicate with the Essential Business Server Messaging Server and Exchange Server 2007
Use Windows Essential Business Server to perform a subset of the following Quick Start tasks:

- **Servers**: Use the Connect to Desktop task to open a remote desktop connection to the console for the specified server.
- **Sessions**: Use the Send Message to User task to notify the user that their session will end, and the Log Off User task to end user sessions.
- **Licenses**: Use the Revoke License task to revoke licenses from users and make them available to other users.
- **Applications**: Use the Modify Application task to add and remove users from accessing specified applications.

An example overview screen is shown below:
In the Citrix Servers Tasks area, you can use the **Change XenApp Fundamentals server group** task to select the XenApp Fundamentals server group to use, and you can launch the Quick Start tool using the **Launch Quick Start** task.

The tasks available in the Essential Business Server are performed as described for the Quick Start tool. For more information about using these features in Quick Start and descriptions of functionality, see “Managing XenApp Fundamentals” on page 69.

### Licensing XenApp Fundamentals

The Quick Start tool allows you to register your XenApp Fundamentals licenses. The product then automatically assigns licenses to users the first time they connect.

You are allowed a maximum of 75 named users of XenApp Fundamentals.

**Note:** Although there is a maximum number of users who are authorized to use an XenApp Fundamentals server, the number who can use XenApp Fundamentals at the same time depends on the limitations of your server hardware (such as total memory, processor speed, disk space, and so on).

To activate and download a license file, you need Internet access to the Citrix licensing Web site. If you do not have a license, you can run XenApp Fundamentals for 96 hours. Any configurations or changes you make during that time are preserved when you activate the license.

See “Managing Licenses” on page 81 for information about upgrading licenses.

### Adding Your First License

**To add your first license**

1. Start the Quick Start tool.
2. On the **Setup** tab, click **Licensing**.
3. Click **Install Citrix Licenses**. The Install Citrix Licenses wizard appears. You must run this wizard for each license you want to install.
4. Click **Next**. If you did not already download a license file, visit the Citrix Web site URL and follow the on-screen instructions to activate and download the file.
5. Click **Browse** to select your downloaded license file.
6. Click **Next**.
7. Review the license details and click **Finish**.

**Activate Terminal Server License Server**

The Terminal Server License server is usually activated automatically during installation; however, you can manually activate the Terminal Server License server if necessary. You do this using the Microsoft Terminal Server Licensing tool.

---

**Note:** If you are running XenApp Fundamentals without Terminal Server Client Access License (TSCAL), you do not need to activate the Terminal Server License server.

---

**To activate the Microsoft Terminal Server license server**

1. Start the Quick Start tool.
2. On the **Setup** tab, click **Licensing**.
3. Click **Activate Terminal Server License Server**.
4. Click **Start the Terminal Server License Server** to launch the Terminal Service Licensing tool.
5. Expand the list of servers under the **All servers** item. Find and select the server running XenApp Fundamentals.
6. From the **Action** menu, select **Activate Server**. Click **Next**.
7. Select the required **Connection method**. If XenApp Fundamentals has Internet access, Citrix recommends **Automatic connection**. Click **Next**.
8. Enter your name, company, and geographical information in the first **Company information** dialog box and click **Next**.
9. Enter any required specific contact information in the second **Company information** dialog box and click **Next**. This contacts the Microsoft activation server.
10. Clear **Start Terminal Server Client Licensing Wizard now** and click **Finish**.
11. From the **Action** menu of the Terminal Server Licensing console, select **Exit**.
12. In the **Microsoft Terminal Service License Server** dialog box, select **I have activated the Terminal Service License Server**.

Terminal Server Licensing is a Microsoft application. Selecting this option instructs XenApp Fundamentals that Microsoft Terminal Service License Server is activated and the Quick Start status indicates this task is complete.
13. Click **Done**.

For full details about how to activate the Terminal Server License Server, consult the Microsoft documentation.

### Providing Access to Applications

Use XenApp Fundamentals to choose the subset of installed applications that should be made available to users based on their role in the organization and their location. You can control which users or groups of users can access each published application.

Users log on to the XenApp Fundamentals server by pointing their Web browser to the preconfigured internal and external Web addresses. One Web address is provided for internal users and one is provided for external users. See “Making XenApp Fundamentals Available to Users” on page 67 for more details.

### Ensuring Applications Are Available

Make sure all the applications you and your users require are installed on the server(s) running XenApp Fundamentals. The Quick Start tool searches XenApp Fundamentals servers for available applications automatically, but you can also browse for applications that are not discovered.

### Publishing Applications

You publish applications using the Quick Start tool. You can configure the appearance of the applications on the user’s device and restrict access to applications to selected users or groups.

**To publish applications**

1. Start the Quick Start tool.
2. On the **Setup** tab, click **Applications**.
3. Click **Publish Application**.
4. Click **Next**. Select the applications to publish by clicking the checkbox next to each application’s name. You can clear selections by clicking **Clear All**. To add an application not appearing in the list, click **Add**.

Click the **Info** button to view the application’s name, description, the server on which it will be published, and the default settings. This button is available on servers running in advanced mode only.
5. Click Next. Click Add to select users to access the applications.

This page provides a flexible search for:

- **Object Types** to add users and groups
- **Locations** to select the location of the users and groups you want to add
- **Check Names** to search the domain for names entered

To remove users, select them from the list and click Remove. To publish applications to a subset of users, select only the appropriate users and groups.

6. Click Next.

7. Review your modifications and click Finish.

---

**Testing Your Internal Access Deployment**

After you publish your applications, you can test your deployment.

**To test your deployment**

1. Start your Web browser.

2. Enter the internal URL http://servername, as displayed on the Quick Start tool in the **Overview** page.

3. Log on using your user name and password.

4. The Welcome page appears. The **Applications** pane shows icons for all the applications you published.

5. Click an application icon and ensure the application launches.
Providing External Access

The type of deployment you implemented determines how you configure external access for your external users. See “Planning Deployments” on page 12 for information about the types of deployment and external access available.

Security Requirements

It is vital that you consider your security requirements in detail and implement appropriate systems.

Security is discussed in “Securing XenApp Fundamentals” on page 91. This gives you background information about the different security options available to you.

The requirements for secure access depend upon your deployment.

The minimum requirements for an XenApp Fundamentals deployment are:

- A user name and password policy. See “User Names and Passwords” on page 96.
- A valid certificate from your Certificate Authority. See “Overview of Security, SSL, and Certificates” on page 91.
- An external public IP address and a DNS name (FQDN).

For a deployment using XenApp Fundamentals and a VPN, you require a user name and password policy. See “User Names and Passwords” on page 96.

For a deployment using a DMZ, you require:

- A user and password policy.
- A valid certificate.
- An IP address and DNS name (FQDN).

Note: Citrix recommends two-factor authentication for external access to both types of deployment. See “User Authentication” on page 97.
Using Internet Protocol

XenApp Fundamentals uses both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). If you need to disable IPv6, use the following procedure.

To disable Internet Protocol 6

1. On the XenApp Fundamentals media, navigate to the Citrix>Quick Start folder.

   **Note:** Citrix recommends that you back up the configuration files before proceeding.

2. Click the `httpd.conf.template` file, and open it with a text editor such as Notepad.

3. Remove the following lines from the file:
   
   ```
   ProtocolMultiplexer [::]:[SGPORT]
   Listen [::]:[SGPORT]
   NameVirtualHost [::]:[SGPORT]
   ```

4. Remove all the lines under the second `#WI Config` heading as follows:
   
   ```
   <VirtualHost [::]:[SGPORT]>
   ServerName [ServerAddress]:[SGPORT]
   SSLEngine On
   SSLCertificateHash [CertificateHash]
   DocumentRoot "[SGPath]"
   <Directory "[SGPath]/error">
   AllowOverride None
   Options IncludesNoExec
   AddOutputFilter Includes html
   AddHandler type-map var
   LanguagePriority en ja cs de es fr it nl sv pt-br ro
   ForceLanguagePriority Prefer Fallback
   </Directory>
   ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
   ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
   ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
   ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
   ```
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 412 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 413 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 414 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
ErrorDocument 416 /error/HTTP_REQUESTENTITY_TOO_LARGE.html.var
ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 504 /error/HTTP_REQUEST_TIMEOUT.html.var
ErrorDocument 506 /error/HTTP_REQUEST_METHOD.html.var
ProxyPass /error !

<Location />
ProxyPass http://localhost:8080/
ProxyPassReverse http://localhost:8080/
<Location> 
SetEnvIf nolog ^$ LOG_HTTP=1
</VirtualHost>

5. Remove all of the lines under the second #GWY Settings - CGP section as follows:

<VirtualHost :::[SGPORT]>
ServerName [ServerAddress]:[SGPORT]
CgpProtocol On
RequireTicket On
CGPHandshakeTimeout 100000
RegisterProtocol CGP
UseConnCounter CONCURRENT_CONN_LIMIT
SSLEngine On
SSLCertificateHash [CertificateHash]
SSLProxyEngine On
<Location /destination/cgp>
Order Deny,Allow
</Location>
6. **Remove all of the lines under the second #Gwy Settings - SOCKS section as follows:**

```
<VirtualHost [::]:[SGPORT]>
  ServerName [ServerAddress]:[SGPORT]
  SocksProtocol On
  SocksHandshakeTimeout 100000
  RegisterProtocol SOCKSV5
  RequireTicket On
  UseConnCounter CONCURRENT_CONN_LIMIT
  SSLEngine On
  SSLCertificateHash [CertificateHash]
  SetEnvIf nolog ^$ LOG_SOCKS=1
</VirtualHost>
```

7. **Save and close the file.**

8. **Click the httpd.conf.dmz file, and open it with a text editor such as Notepad.**

9. **Remove the following lines from the file:**

```
ProtocolMultiplexer [::]:[SGPORT]
Listen [::]:[SGPORT]
NameVirtualHost [::]:[SGPORT]
```

10. **Remove all the lines under the second #WI Config heading as follows:**

```
<VirtualHost [::]:[SGPORT]>
  ServerName [ServerAddress]:[SGPORT]
  SSLEngine On
  SSLCertificateHash [CertificateHash]
  DocumentRoot "[SGPath]"
  <Directory "[SGPath]/error">
    AllowOverride None
    Options IncludesNoExec
    AddOutputFilter Includes html
  </Directory>
</VirtualHost>
```
AddHandler type-map var
LanguagePriority en ja cs es es fr it nl sv pt-br ro
ForceLanguagePriority Prefer Fallback
</Directory>
ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
ProxyPass /error /
<Location />
ProxyPass http://localhost:8080/
ProxyPassReverse http://localhost:8080/
</Location>
SetEnvIf nolog ^$ LOG_HTTP=1
</VirtualHost>

11. Remove all of the lines under the second #GWY Settings - CGP section as follows:

<VirtualHost [::]:[SGPORT]>
ServerName [ServerAddress]:[SGPORT]
CgpProtocol On
RequireTicket On

CGPHandshakeTimeout 100000
RegisterProtocol CGP
UseConnCounter CONCURRENT_CONN_LIMIT
SSLEngine On
SSLCertificateHash [CertificateHash]
SSLProxyEngine On
<Location /destination/cgp>
Order Deny,Allow
Deny to All
Allow to All
</Location>
SetEnvIf nolog ^$ LOG_CGP=1
</VirtualHost>

12. Remove all of the lines under the second #Gwy Settings - SOCKS section as follows:
<VirtualHost [::]:[SGPORT]>
ServerName [ServerAddress]:[SGPORT]
SocksProtocol On
SocksHandshakeTimeout 100000
RegisterProtocol SOCKSV5
RequireTicket On
UseConnCounter CONCURRENT_CONN_LIMIT
SSLEngine On
SSLCertificateHash [CertificateHash]
SetEnvIf nolog ^$ LOG_SOCKS=1
</VirtualHost>

13. Save and close the file.

**External Access Direct to Server**

See “Deployment Scenario 1: Direct to Server” on page 13 for more information about this deployment.

There are three security certificate options when providing external access using the Direct to Server deployment:

- Secure access using a public key certificate purchased from a recognized Certificate Authority. This requires an agreement with the Certificate
Authority. The certificate needs to be requested, then approved by the Certificate Authority, and then installed on the network. In most cases you do not have to install root certificates on the clients. See “Overview of Security, SSL, and Certificates” on page 91 for further information.

- Secure access using a temporary certificate. A temporary certificate can be used to provide external access while you wait for a Certificate Authority to issue a long-term certificate or when undertaking a short evaluation. This expires after thirty days, after which time external access is disabled. Root certificates need to be installed on all clients that are to use external access.

- Secure access using a certificate from a local domain. This requires a Certificate Authority to be implemented by administrators within your network domain. In this case, root certificates need to be installed on all clients that are to use external access.

**Note:** Users might be unable to install root certificates on client devices, such as Internet kiosks, that are locked down. If you do not use a recognized Certificate Authority, users might be unable to access the published applications.

---

**External Access Using a Certificate from a Certificate Authority**

To enable first-time external access direct to the XenApp Fundamentals server using a certificate from a Certificate Authority, you must:

- Generate a request for a secure certificate
- Install the certificate when you receive it

For information about certificates and security, see “Overview of Security, SSL, and Certificates” on page 91.

To ensure uninterrupted access, certificates must be renewed before they expire (typically every year). When the certificate expires or if you need to create a new certificate request (for example, from a different authority), see “Creating and Importing a New Certificate” on page 88.

**To generate a certificate request for the direct to server deployment**

1. Start the Quick Start tool.
2. On the **Setup** tab, click **External Access**.
3. Click **Manage External Access**.
4. Click **Next**. Select **Direct to this server** to access the server from the Internet using a firewall.
5. Click **Next**.
6. If a server certificate could not be located, you must request one from your Certificate Authority. To begin this process, enter the address of the server in the Public address field. Click Next and go to Step 11.

7. Enter the public (external) address of the server running XenApp Fundamentals. If enabling access from the Internet, this is your server:registered DNS domain name (for example, access-essentials.citrix.com). Click Next.

8. Type your organization’s name and organizational unit. Click Next.


10. Select Manually submit the certificate request to a Certificate Authority and click Next.

11. Specify the filename and location for your certificate request. You submit this file to your chosen Certificate Authority when you request a certificate. Click Next.

12. Review the details and click Finish to create the certificate request.

   You must contact your chosen Certificate Authority and submit your certificate request. The authority will send you your certificate after processing your request.

To install a certificate after it is issued by the Certificate Authority
1. Start the Quick Start tool.
2. Click External Access.
4. Select Enable external access and complete pending certificate request. Click Next.
5. Enter the path and file name where your certificate is located. Click Next.
6. Specify the TCP port that will be used for remote connections. You can select a standard HTTPS port, or use a custom TCP port. Click Next.
7. Review the details and click Finish to enable external access.

External Access Using a Local Domain Certificate
Administrators can create certificates for local domains. This works in a similar fashion to certificates from a recognized Certificate Authority. However, root certificates need to be installed on every client device requiring external access. After you are granted a certificate, you must save the root certificate and distribute it to your users.
The Local Domain Certificate Authority can be implemented stand-alone on the XenApp Fundamentals server, or as an enterprise Certificate Authority on a different domain server. In either case, it must be a Microsoft Certificate server.

Users must install the root certificate on their Clients for Windows device by double-clicking the file and following the Windows procedures for installation. For other client platforms, refer to your operating system or browser documentation.

To enable external access using a certificate from a local domain Certificate Authority
1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
4. Click Next.
5. Select Direct to the server. Click Next.
6. Enter the public (external) address of the server running XenApp Fundamentals. If enabling access from the Internet, this is server.registered DNS domain name (for example, xenapp-fundamentals.citrix.com). Click Next.
7. Type your organization’s name and organizational unit. Click Next.
8. Specify your geographical information. Click Next.
9. Select Submit the certificate request to a local domain based certificate authority. Quick Start searches the local domain for your local authority and displays the results in the drop-down box.

Note: If this option does not appear, submit the certificate using the Manually submit the certificate request to a Certificate Authority option.

10. Select the required local Certificate Authority and click Next.
11. Specify the TCP port that will be used for remote connections. You can select a standard HTTPS port, or use a custom TCP port. Click Next.
12. Review the details and click Finish to complete the certificate request.
To enable a local domain certificate for the direct to server deployment

The process depends upon your user credentials and the configuration of the Local Domain Certificate Authority.

- If the Local Domain Certificate Authority is configured so that you have permission to both submit and grant a certificate, the certificate will be granted automatically.

- If the Local Domain Certificate Authority is configured so that you have permission to only submit a certificate request, you are prompted to enter alternative credentials for granting the certificate request.

- If the Local Domain Certificate Authority is configured so that certificates are not delivered automatically (out of band), for example by email, you will receive a notice informing you of this situation after the certificate is granted. When you receive the notification that the certificate is granted, you must follow the procedure described in “To install a certificate after it is issued by the Certificate Authority” on page 44).

- If the Local Domain Certificate Authority is configured so that you do not have permission to either request or grant a certificate, your request will be refused.

To save the local domain root certificate

1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
3. Click Save root certificate. A Save As window appears.

   ![Note](Note: Citrix recommends that you back up your certificates. This is useful when, for example, you move servers to another domain. If the root certificate has been moved or deleted, this step is not available.)

4. Save the root certificate to a location of your choice.

To distribute the local domain root certificate to clients

1. Distribute the root certificate (for example, by email) to all users requiring external access.
2. Save the root certificate file to an appropriate location on each client device.
3. Using Windows Explorer on each client device, double-click the certificate file.
4. Follow the Windows procedure to install the root certificate on each client device.

**Note:** You can also use Active Directory Group Policy to distribute the certificate. See your Microsoft documentation for details.

### Configuring External Access for ISA Server

You can configure an alternative SSL port to allow ISA Server to route SSL connections directly to the server running XenApp Fundamentals.

To use ISA server, you:

- Export the certificate for the external access site on the server running XenApp Fundamentals
- Install the certificate in ISA Server for the external access site
- Install the Access Essential root certificate in ISA Server
- Configure port forwarding for the XenApp Fundamentals server in ISA Server
- Install the root certificate on the client device

The following procedures describe how to enable external access with ISA Server.

**To export the certificate for the external access site**

1. Launch the Microsoft Management Console.
2. Go to **File** and select **Add/Remove Snap-in**.
3. In the Standalone tab, click **Add**. Select the **Computer Account** option and click **Next**.
4. Select the **Local Computer** option, and click **Finish**. Click **Close** and **OK** to close the windows and return to the console.
5. Expand the Console Root node then the Certificates node, and click **Personal**. Double-click the Certificates folder.
   This folder contains the certificate for the external access site.
6. Right-click the certificate and select **All Tasks** and **Export**.
   The Certificate Export Wizard appears.
7. Select the format for the certificate, click **Next** and browse to the path to which the certificate will be exported. Click **Next**.
8. Click **Finish** to complete the export.

**To install the certificate for the external access site**

1. Launch the Microsoft Management Console.
2. Go to **File** and select **Add/Remove Snap-in**.
3. Select **Certificates**, click **Add**, and select the **Computer Account** option.
4. Select the **Local Computer** option and click **Finish**. Click **Close** and **OK** to close the windows and return to the console.
5. Expand the Console Root node then the Certificates node, and click **Personal**.
6. Click **Action** and select **All Tasks** and **Import**. The Certificate Import Wizard appears.
7. Click **Next** and browse to the certificate then enter a password for the certificate. Select the **Personal** option.
8. Click **Finish** to complete the import.

**To install the XenApp Fundamentals root certificate**

1. Launch the Microsoft Management Console.
2. Expand the Console Root node, then the Trusted Root Certification Authorities node, and click **Certificates**.
3. Click **Action** and select **All Tasks** and **Import**. The Certificate Import Wizard appears.
4. Browse to the XenApp Fundamentals root certificate location and click **Next**.
5. Select the **Trusted Root Certificates** option.
6. Click **Finish** to complete the import.

**To configure port forwarding for the XenApp Fundamentals server**

1. Launch the ISA Server Management console.
2. Expand the computer name node, right-click **Firewall Policy** and select **Non-Web Server Protocol Publishing Rule**.
3. Enter a name for the rule and specify the IP address of the XenApp Fundamentals server.
4. In the Selected Protocol list, select **HTTPS Server**. If you configured external access with a port other than the default (443), from the Firewall...
Ports list select **Publish on this port instead of the default port.** Enter the alternative port number.

External plug-ins must specify this port number when connecting to the external access site.

5. Select the external network for listening requests.

6. Click **Finish** to complete the wizard.

**To install the root certificate on the client device**

Use this procedure if you are using a temporary certificate generated by XenApp Fundamentals for the external access site. If you are using a certificate from a domain-based or external Certificate Authority, you must import the appropriate Certificate Authority root certificate on the client device.

1. Launch the Microsoft Management Console.

2. Expand the Console Root node, then the Trusted Root Certification Authorities node, and click **Certificates.**

3. Click **Action** and select **All Tasks** and **Import.**

4. Browse to the XenApp Fundamentals root certificate location and click **Next.**

5. Select the **Trusted Root Certificates** option.

6. Click **Finish** to complete the import.

**External Access Using a Temporary Certificate**

A temporary certificate allows you up to thirty days of secure access to test deployments and evaluate installations while you wait to receive your permanent certificate. After thirty days, you must install either a public certificate or a local domain certificate to continue offering secure external access.

After you create a temporary certificate, you must distribute the corresponding root certificate to your users. This root certificate must match the certificate on the server. Users install the root certificate on their client device by double-clicking the file and following the Windows procedures for installation.

**To enable a temporary certificate**

1. Start the Quick Start tool.

2. In the **Setup** tab, click **External Access.**

3. Click **Manage External Access.** The Manage External Access wizard appears.

4. Click **Next.**
5. Select **Direct to this server**. Click **Next**.
   This option does not appear on a DMZ server.

6. Enter the public (external) address of the server running XenApp Fundamentals. If enabling access from the Internet, this is `server.registered DNS domain name` (for example, xenapp-fundamentals.citrix.com). Click **Next**.

7. Type your organization’s name and organizational unit. Click **Next**.

8. Specify your geographical information. Click **Next**.

9. Select **Generate a temporary certificate** and click **Next**.

   **Note:** The root certificate is saved automatically in the root directory of the XenApp Fundamentals server. However, you can save the certificate to another location for distribution.

10. Specify the name and location of the root certificate. Click **Next**.

11. Specify the TCP port that will be used for remote connections. You can select a standard HTTPS port, or use a custom TCP port. Click **Next**.

12. Review the details and click **Finish** to complete the wizard.

**To save the temporary root certificate at a later date**

1. Start the Quick Start tool.

2. In the **Setup** tab, click **External Access**.

3. Click **Save root certificate**. A **Save As** window appears.

   **Note:** Citrix recommends that you back up root certificates. This is useful when, for example, you move servers to another domain. If the root certificate has been moved or deleted, this step will not be available.

4. Save the root certificate to a location of your choice.
To distribute the root certificate to client devices

1. Distribute the root certificate (for example, by email) to all the client devices requiring external access.
2. Save the root certificate file to an appropriate location on each client device.
3. Using Windows Explorer on each client, double-click the certificate file.
4. Follow the Windows procedure to install the root certificate on each client device.

**Note:** You can also use Active Directory Group Policy to distribute the certificate. See your Microsoft documentation for details.

External Access with a DMZ Server

See “Deployment Scenario 2: Demilitarized Zone” on page 14 for more information about this deployment.

To enable external access for XenApp Fundamentals DMZ deployment

1. Install and configure the DMZ server.
2. Start the Quick Start tool on the master server.
3. In the Setup tab, click **External Access**.
5. Click **Next**.
6. Select **Using a DMZ Server**. Click **Next**.
7. Review the details and click **Finish** to complete the wizard.

**Note:** When you provide the name of the master server in the Manage External Access wizard, ensure this is an IP address rather than a hostname or DNS name.
External Access Using a VPN

You can enable external access using a VPN for both basic mode (single server) or advanced mode (multiple servers). The following section describes how to do this for both modes.

See “Deployment Scenario 3: Virtual Private Network” on page 14 for more information about this deployment.

To enable external access using a VPN in basic mode
1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
4. Click Next. Select the Using a VPN option.
5. Click Next. Specify settings for the firewall between the VPN and the server running XenApp Fundamentals. Choose between:
   - **Use Network Address Translation.** This is the recommended option. Network Address Translation (NAT) allows you to enter the IP address for access through the firewall between XenApp Fundamentals and the VPN. NAT then routes access from this IP address to the multiple IPs of different users, meaning that only one IP address is presented at the firewall. Enter the IP address of the server running XenApp Fundamentals as seen by the VPN. In addition, configure the VPN to allow traffic to this address.
   - **Do not use Network Address Translation.** With this option, clients connect directly to the IP address of XenApp Fundamentals. This is not recommended.
6. Click Next.
7. Review the details and click Finish to complete the wizard.

To enable external access using a VPN in advanced mode
1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
4. Click Next. Select the Using a VPN option. Click Next.
5. Specify settings for the firewall between the VPN and the server running XenApp Fundamentals. Choose between:
• **Use Network Address Translation.** This is the recommended option.

• **Do not use Network Address Translation.** With this option, clients connect directly to the IP address of XenApp Fundamentals. This is not recommended.

6. Click **Next**. From the list provided, select a server to enter the NAT mappings on the firewall between the VPN and the server running XenApp Fundamentals. Click **Modify**.

7. Enter the IP addresses and port numbers for the ICA/CGP mapping and the RDP mapping. Click **OK**.

8. Click **Next**.

9. Verify the NAT mappings in the summary page. If you want to make any changes, click **Back**. To print this summary, click **Print**. To continue, click **Next**.

10. Review the details and click **Finish** to complete the wizard.

### Testing External Access

To test external access

1. From a client device, start your Web browser.

2. Enter the external URL as displayed on the Quick Start tool.

3. Log on using your user name and password.

4. The **Welcome** page appears. The **Applications** pane shows icons for all the applications you published.

5. Click an application icon and ensure the application launches.

### Configuring Authentication

After you configure external access, you can implement the following types of authentication:

• **Standard authentication.** Each user logs on using their user name and password defined (Windows domain) credentials. This allows secure access to applications and content published on the XenApp Fundamentals server.

• **Two-factor authentication.** This option provides enhanced security. In addition to user name and password, users also enter a time-variable code.
Two factor authentication is the most secure of these alternative options. XenApp Fundamentals supports both Secure Computing’s SafeWord for Citrix or RSA SecurID:

- **RSA SecurID** uses time-varying numbers generated by RSA SecurID tokens (tokencode) and PINs to create a passcode. Users must enter the passcode generated by their token in a specific time frame so that it matches the one generated by the server.

- **Secure Computing’s SafeWord for Citrix** uses alpha-numeric codes generated by SafeWord tokens and (optionally) PINs to create a passcode.

RSA SecurID and Secure Computing Safeword for Citrix are sold separately by their respective suppliers and must be installed to enable one of these options.

If you are using the Citrix Access Gateway, see your Access Gateway documentation for additional information about implementing two-factor authentication.

For more information about configuring authentication, see “User Authentication” on page 97.

### Setting Up Administrator Accounts

You must use only the Quick Start tool to add administrators to XenApp Fundamentals or to amend their privileges. Do not use the Citrix Access Management Console to manage administrator accounts.

**To create a full administrator**

1. Start the Quick Start tool.
2. In the **Setup** tab, click **Administrators**.
3. Click **Add Full Administrator**. The **Add Full Administrator** page appears.
4. You can either grant administrator rights to an existing user of XenApp Fundamentals (recommended because this gives more control over the details of the account created) or create a new user. Select **Grant administrator rights to an existing user** and use the **Browse** function to select a user.
   
   —Or—

   Select **Create a new local user with administrator rights** and type the name and password details for a new user.
5. Click **OK**.
To create a delegated administrator
1. Start the Quick Start tool.
2. In the Setup tab, click Administrators.
3. Click Add Delegated Administrator. The Add Delegated Administrator page appears.
4. You can either grant administrator rights to an existing user of XenApp Fundamentals (recommended because this gives more control over the details of the account created) or create a new user. Select Grant administrator rights to an existing user and use the Browse function to select a user.
   —Or—
   If the server running the Quick Start tool is in basic mode, select Create a new local user with administrator rights. If the server is in advanced mode, select Create a new domain user with administrator rights.
5. Type the name and password details for a new user, and click OK.

Configuring Email Alerting

Full administrators can set up XenApp Fundamentals so that emails are sent to specified administrators or other individuals when important system or connectivity events occur on the network that may compromise user access to applications.

Citrix recommends setting up alert emails because it makes your administrators aware of potential issues as soon as they occur, and each email contains useful troubleshooting information to resolve the particular issue. However, you may want to disable the alerts temporarily, for example when you take servers down for maintenance. Remember to restart email alerting after maintenance is complete.

The following table lists the types of alert email that XenApp Fundamentals can generate, and summarizes the events that trigger them. Full troubleshooting instructions are provided in each email.

If you have only one server running XenApp Fundamentals, note that some email types are never generated.

<table>
<thead>
<tr>
<th>Alert email type (Subject line of email)</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master server master server name unresponsive (detected by support server support server name)</td>
<td>The Citrix Independent Management Architecture service on the master server could not be contacted by the support server. This alert email type is not generated in single-server deployments.</td>
</tr>
<tr>
<td>Alert email type (Subject line of email)</td>
<td>Summary</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Master server master server name down (detected by support server support server name)</td>
<td>The master server is detected as being in a down state and unresponsive to network communications from the support server. This alert email type is not generated in single-server deployments.</td>
</tr>
<tr>
<td>Support server support server name unresponsive (detected by master server master server name)</td>
<td>The Citrix Independent Management Architecture service on the support server could not be contacted by the master server. This alert email type is not generated in single-server deployments.</td>
</tr>
<tr>
<td>Support server support server name down (detected by master server master server name)</td>
<td>The support server is detected as being in a down state and unresponsive to network communications from the master server. This alert email type is not generated in single-server deployments.</td>
</tr>
<tr>
<td>Internal Web Interface access is unavailable</td>
<td>The Web site providing users with internal Web access to their applications was detected as unavailable.</td>
</tr>
<tr>
<td>External Web Interface access is unavailable</td>
<td>The Web site providing users with external Web access to their applications was detected as unavailable.</td>
</tr>
<tr>
<td>Citrix logon component not responding on master server master server name</td>
<td>The Citrix XML Service running on the master server was unresponsive.</td>
</tr>
<tr>
<td>Unable to retrieve list of published applications</td>
<td>The master server was unable to retrieve the list of published applications from the Citrix Independent Management Architecture service.</td>
</tr>
<tr>
<td>Windows Terminal Services not operational on server server name</td>
<td>Windows’ Terminal Services service running on the server was unresponsive.</td>
</tr>
<tr>
<td>Server server name failed to locate a Terminal Server License Server</td>
<td>Windows Terminal Services are not adequately licensed.</td>
</tr>
<tr>
<td>Server server name is unable to connect to a Terminal Services License Server</td>
<td>Windows Terminal Services are not adequately licensed.</td>
</tr>
<tr>
<td>Secure Gateway external access unavailable</td>
<td>The SSL/VPN software module known as the Secure Gateway was detected as unavailable.</td>
</tr>
<tr>
<td>SSL certificate due to expire in x day(s)</td>
<td>The SSL certificate being used to provide users with secure access to their applications through the external Web Interface site is due to expire.</td>
</tr>
<tr>
<td>SSL certificate expired</td>
<td>The SSL certificate being used to provide users with secure access to their applications through the external Web Interface site has expired.</td>
</tr>
<tr>
<td>Citrix licenses due to expire in x day(s)</td>
<td>An installed Citrix evaluation license file is due to expire.</td>
</tr>
</tbody>
</table>
Note: If you are sorting alert emails in your email application, be aware that the subject lines are prefixed with the words *Citrix Alert*.

<table>
<thead>
<tr>
<th>Alert email type (Subject line of email)</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix licenses expired</td>
<td>An installed Citrix evaluation license file has expired.</td>
</tr>
<tr>
<td>Profile server <em>profile server name</em> cannot be contacted by master server <em>master server name</em></td>
<td>The profile server cannot be contacted by the master server.</td>
</tr>
<tr>
<td>Session reliability on server <em>server name</em> is not functioning</td>
<td>The Citrix XTE Server service, which provides session reliability, is not running on the server.</td>
</tr>
</tbody>
</table>

**To enable email alerting**

1. On the **Setup** tab of the Quick Start tool, click **Administrators**.
2. Click **Configure E-mail Alerting**. The Configure E-mail Alerting wizard appears.
3. Click **Next**.
4. Select **Enable alerting** and click **Next**.
5. Enter or select the name of the SMTP server that will be used to send the alert emails. You can test the connection to this server at this stage. Click **Next**.
6. If the SMTP server requires authentication, enter the user name and password. Click **Next**.
7. Enter the name or email address that will appear in the **Sender** field of the emails. Your SMTP server may require a valid email address. Citrix recommends that you use an email account with a password that will not expire and does not require logon credentials.
8. Click **Next**. The list of email recipients is displayed. By default in an Active Directory deployment (and if you have rights to access email addresses on the system), the list includes all currently configured administrators.
9. Click **Add** and enter the email address of any other individual whom you want to receive alert emails. You can enter any valid email address, not just an administrator’s. Repeat this step to add further email recipients.

You can send a test email to recipients at this stage. If you do so, ask recipients to verify that the test email has arrived.
10. Click **Next**, and check the details on the last page of the wizard.
11. Click **Finish** to confirm the configuration.

**To disable email alerting**
1. On the **Setup** tab of the Quick Start tool, click **Administrators**.
2. Click **Configure E-mail Alerting**.
3. In the Configure Email Alerting wizard, click **Next**.
4. Select **Disable alerting** and click **Next**.
5. Click **Finish** to confirm that you do not want administrators to receive alert emails.

---

**Important**: Citrix recommends that you restart email alerting as soon as possible after disabling it so that administrators are kept aware of important system events affecting users’ access to applications.

---

**Providing Access to Printers**

You can define which network printers are available for printing from published applications, and whether or not users can print to printers configured on their client devices. Use the Quick Start tool to define the types of printers available to users when running applications through XenApp Fundamentals. If you are running XenApp Fundamentals on multiple servers, printer settings are replicated across all servers in the group.

The types of printers you can use through XenApp Fundamentals are:

- **Published printers**. Published printers are network printers connected to a print server on the network. These are detected and published through the Quick Start tool.

- **Client printers**. Client printers are those printers either physically attached to the client device or mapped from the client device.

- **Windows managed printers**. Windows managed printers are those attached to the XenApp Fundamentals server, and those network printers that are available to users through their Windows profile on the server. They are always available for use with XenApp Fundamentals. However, they can be managed only by using the native Windows operating software on the server.
The following illustration depicts a possible configuration for printers with XenApp Fundamentals:

![Diagram of printer configuration]

**Windows Managed Printers**

Windows managed printers are always available for printing. They can be installed and configured only by using the Windows printer management software. You can use Quick Start to restrict printing through XenApp Fundamentals to these printers only.

**Note:** Windows managed printers can be used only on the server to which they are physically attached. When using multiserver deployments, Citrix recommends that you use published printers. For more information, see “Publishing Network Printers” on page 60.

**Restricting printing to Windows managed printers only**

1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Click Setup Printers. The Setup Printers wizard appears.
4. Click Next. The Setup Printers wizard appears.
5. Select **Use Windows managed printers only**. Click **Next**.

6. Review the details and click **Finish** to complete the wizard.

### Enabling Client Printers

You can allow users of XenApp Fundamentals to print to printers attached to or mapped from their client device, as well as to any Windows managed printers. For example, this would allow home workers to print to a printer installed in their own home.

You can enable client printing only or client printing with published printers. In both cases, Windows managed printers are available.

**To enable client printing only**

1. Start the Quick Start tool.

2. In the **Setup** tab, click **Printers**.

3. Click **Setup Printers**. The Setup Printers wizard appears.

4. Click **Next**.

5. Select **Make additional printers available through** XenApp Fundamentals.

6. Select **Client printers** from the **Type:** drop-down box.

7. Click **Next**.

8. You can change the default printer used by each client. To do this, select **Set the default printer** and select a printer from the drop-down box.

9. Click **Next**.

10. Review the details and click **Finish** to complete the wizard.

### Publishing Network Printers

Printers connected to a print server on the network can be published for use in XenApp Fundamentals as well as Windows managed printers.

**Note:** You must have appropriate administrator credentials to find and access the printers on the network. Additionally, there may be some restrictions to the printers that can be published (for example, only those within trusted domains).

**To enable published printers only**

1. Start the Quick Start tool.

2. In the **Setup** tab, click **Printers**.
3. Click **Setup Printers**. The Setup Printers wizard appears.

4. Click **Next**.

5. Select **Make additional printers available through** XenApp Fundamentals.

6. Select **Published printers** from the **Type**: drop-down box.

7. Click **Next**.

8. If your current user credentials are sufficient to locate the printers required, click **Next**. If you require different credentials, select **Use alternative account** and enter the account details.

---

**Note:** Quick Start searches for all printers on the network that can be accessed using the administrator or alternative credentials entered. In a large network, this can take considerable time. If you know the printer details you can click **Add** to add your printer manually in the **Add a Print Server** dialog box. You can do this while the Quick Start search is in progress.

9. Click **Next**.

10. Click **Select** to add the selected printers from the **Available network printers** list. Click **Unselect** to remove selected printers from the **Selected network printers** list.

11. After you add all the printers required, click **Next**.

12. Check **Set the default printer** and then select the printer you want to be the client device’s default printer from the selection box. Click **Next**.

---

**Note:** If you do not set a default printer in Quick Start, Windows sets the default printer to that defined by the Windows environment.

13. Review the details and click **Finish** to complete the wizard.

### Enabling Both Client and Published Printers

You can allow clients to use both client and published printers as well as Windows managed printers in XenApp Fundamentals.

**To enable both client and published printers**

1. Start the Quick Start tool.

2. In the **Setup** tab, click **Printers**.
3. Click **Setup Printers**. The Setup Printers wizard appears.

4. Click **Next**.

5. Select **Make additional printers available through** XenApp Fundamentals.

6. Select **Client and published printers** from the **Type** drop-down box.

7. Click **Next**.

8. If your current user credentials are sufficient to locate the printers required, click **Next**. If you require different credentials, select **Use alternative account** and enter the account details and then click **Next**.

   The **Select Printers to Publish** page appears and Quick Start searches for printers on the network.

   **Note:** Quick Start searches for all printers on the network that can be accessed using the administrator credentials entered. In a large network, this can take considerable time. If you know the printer details you can add your printer manually, as described in Step 9. You can do this while the Quick Start search is in progress.

9. Select the printers required from the **Available network printers** list, expanding nodes as needed to display the printers.

   — Or —

   Click **Add** and type the full name of the print server in the **Add a print server** box. Click **OK** to add the server.

10. Click **Select** to add the selected printers to the **Selected network printers** list. Click **Unselect** to remove selected printers from the **Selected network printers** list.

11. After you add all the printers required, click **Next**.

12. Check **Set the default printer** and then select from the box the printer you want to be the client device’s default printer. Click **Next**.

   **Note:** If you do not set a default printer in Quick Start and client printing is enabled, Windows sets the default printer to the client’s default printer.

13. Review the details and click **Finish** to complete the wizard.
Using Advanced Mode

In advanced mode, different tasks are available depending on the type of server you are running. You can add support servers to or remove them from server groups, and you can promote a support server to become the master of a server group. Master servers are used to manage server groups, and can run additional tasks such as server failover and profile management.

The following sections describe how to:

- Set up servers
- Set up failover servers
- Enable profile management

Setting Up Servers

Stand-alone servers can be added to server groups using the Quick Start tool.

To join a server group
1. Start the Quick Start tool on the server you want to join to the group.
2. In the Setup tab, click Servers.
3. Click Next.
4. On the Join Server Group page, select Existing server group to become a support server in an existing server group.
5. If you select Existing server group, the Applications Bindings page appears. On this screen, choose whether or not you want applications published on this server to be available to users. For example, if you published Notepad on the master server and it has also been installed on the support server, Notepad is launched from the support server only. If you do not want to make published applications on the support server available to users, select Make no published applications available.
6. Click Finish. The system may take a few minutes to complete this operation.

You can promote a support server to become the master server of a group if, for example, the master becomes unavailable.

To promote a support server to master
1. Start the Quick Start tool on the support server you want to promote to master.
2. In the Setup tab, click Servers.
3. Select a server from the **Servers** list and click **Become Server Group master**.

4. Click **Yes** to confirm.

**To remove a server from a server group**
1. Open the Quick Start tool on the server that you want to remove.
2. Click the **Setup** tab.
3. Click **Servers**. On the **Servers** screen, click **Leave Server Group**.

**Setting Up Server Failover**

In the event that a master server fails or is unavailable (for example, the server is taken offline), load balancing responsibilities can be transferred automatically to an alternative server. This process is called *failover*.

To use this feature, all servers must be in the same subnet and you must have an unused IP address available in the subnet.

**To set up servers for failover**
1. Start the Quick Start tool.
2. In the **Setup** tab, click **Servers**.
3. Click **Setup Failover Servers**. The Setup Failover Servers wizard appears.
4. Click **Next**.
5. To use server failover, select **Use server failover functionality**. If you do not want to use this feature, select **Do not use server failover functionality**. In this case, click **Finish** to complete the wizard. Otherwise, click **Next**.
6. Enter an unused IP address from the same subnet as the master server to use for failover and click **Test** or **Next** and Quick Start verifies the address. If the address is not valid, you must enter a valid address before proceeding to the next step.
7. Select the server(s) that will take over for the master server if the master server become unavailable. The **Server Online** column indicates which servers are currently online. The server that takes over for the master is displayed as a temporary master server in Quick Start.
8. Review the details and click **Finish** to complete the wizard.
Setting Up User Profiles

User profiles store information about accounts in multiuser networks, and ensure that users encounter the same settings regardless of which XenApp Fundamentals server they use.

To use this feature, you must have Active Directory configured on all of your servers, and at least one file server must be available to store the profile information. (A master server can be used for this purpose, but only at the expense of performance.) The profiles directory must be selected on the server in the current domain. Trusted domains are not supported.

If you run XenApp Fundamentals in advanced mode, Citrix recommends that your deployment does not include any non-domain users. Because they do not have domain privileges, non-domain users may cause the profile management feature to malfunction.

For more information about deploying Active Directory, consult your Microsoft documentation.

---

**Note:** The profiles on users’ personal computers are not affected by the user profiles that you configure with XenApp Fundamentals. Servers used for profile management must be in the same domain as the XenApp Fundamentals server group.

---

To set up user profiles

1. Start the Quick Start tool.
2. In the **Setup** tab, click **Servers**.
3. Click **Configure Profile Management**. The Configure Profile Management wizard appears.
4. Click **Next**.
5. If you are using an existing profile management solution or want to configure profile management yourself, select **Administer user profiles manually**. Otherwise, select **Profile management** and click **Next**.
6. On the **Select Profile File Server** page, select a file server that will be used to store profile data. Click **Next**.

---

**Note:** User profile data such as users’ Desktop and My Documents can be several megabytes in size. Ensure you select a server with sufficient capacity.
7. On the **Select Share Location** page, select an existing folder on the file server. Profile data will be stored in two automatically generated, shared subfolders called USER_PROFILES and USER_FOLDERS. This step is not displayed if USER_PROFILES and USER_FOLDERS subfolders already exist.

8. Click **Next**.

9. Review the details and click **Finish** to complete the wizard.

**Managing Tasks with Essential Business Server**

In the right pane of the Essential Business Server console, the following two tasks are available:

- **Change XenApp Fundamentals Server Group**: Select a server group to administer from the Essential Business Server console. Additionally, you can select **Always administer this server group** to set the default server group that is always used when Essential Business Server is launched.

- **Launch Quick Start**: To perform all administration tasks (that is, not just the subset available in the Essential Business Server console), you can launch the Quick Start tool from the Essential Business Server console.

**Note:** If a Citrix plugin is not installed, Quick Start will run in a separate window. If a plugin has been installed, Quick Start will run in seamless mode, integrated into the desktop.

**Servers**

Using the Citrix Servers tab, you can establish a remote desktop connection to the console for the selected server. To do this, click **Connect to Desktop**.

**Sessions**

Using the Citrix Sessions tab, you can perform the following tasks:

- **Send Message to User**: Select the session from the list and click **Message**, and enter a message to send to the user.

- **Log Off User**: Select the session from the list and click **Log Off**. A logoff request is sent to users, prompting users to save their work. After users save their work, they are automatically logged off.
Licenses
Using the Citrix Licenses tab, you can revoke users’ licenses. To do this, click Revoke License. Any sessions for that user end immediately.

Applications
Using the Citrix Applications tab, you can specify which users can access particular applications. To do this, click Modify Application, and either add or remove users.

Making XenApp Fundamentals Available to Users
XenApp Fundamentals users log on and access resources using an internal or external Web address:
- An internal Web address for those users accessing applications from within the trusted internal network
- An external Web address for those users accessing applications from a public network (such as the Internet)

These Web addresses appear as links on the Quick Start tool pages. Inform your users of these Web addresses so that they can access their published applications.

If users want to bookmark this page in their browsers, Citrix recommends that the bookmark be set to the path name without specifying a particular page (such as login.aspx).
Managing XenApp Fundamentals

This chapter details the management and maintenance tasks that administrators can perform after the software is installed and configured. The tasks described, and the administrator rights needed to perform them, are shown below:

<table>
<thead>
<tr>
<th>Task</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing users</td>
<td>Delegated and Full</td>
</tr>
<tr>
<td>Managing sessions</td>
<td>Delegated and Full</td>
</tr>
<tr>
<td>Managing published applications, desktops, and content</td>
<td>Full</td>
</tr>
<tr>
<td>Managing licenses</td>
<td>Full</td>
</tr>
<tr>
<td>Managing administrator accounts</td>
<td>Full</td>
</tr>
<tr>
<td>Server maintenance</td>
<td>Full</td>
</tr>
<tr>
<td>Managing printers</td>
<td>Full</td>
</tr>
<tr>
<td>Managing certificates</td>
<td>Full</td>
</tr>
<tr>
<td>Advanced application settings</td>
<td>Full</td>
</tr>
</tbody>
</table>

Managing Users

The screens on the Management tab allow you to identify the applications that users are allowed to access, their licensing status, and their sessions. However, with a large number of users you may find it quicker to locate this information for a specific user with the User Management wizard. After you specify the users, the wizard shows you whether or not they are licensed, which applications they can use, and their active sessions. If you need to, you can then modify their application access, revoke their license, or manage their sessions.

The User Management wizard allows you to troubleshoot problems quickly on a per-user basis and take any necessary corrective actions. Both full and delegated administrators can run the wizard.
Managing Individual Users

To manage access for a specific user
1. Start the Quick Start tool.
3. Enter the name of the user whose access details you want to check and click Search.
4. Select the user from the list, and click Next. The user’s applications, licensing status, and sessions are shown:
   • If you want to change any of these details for this user, select Manage this user’s application access, license, and sessions. Click Next.
   • If you do not want to make any changes, click Finish to close the wizard.
5. On the Choose a Task page, select one of the following options and follow the onscreen instructions:
   • Licensing to revoke user licenses or view a list of all licensed users
   • Sessions to send users a message, log off their sessions, shadow them, or view session details

Managing User Access to Applications

The Applications task allows you to view and modify applications and users or user groups who have access to the applications.

To add users to or remove users from applications
1. Start the Quick Start tool.
2. On the Management tab, click Applications.
3. Select the Applications option and select an application from the User/Group Access pane. Click Modify. The Configure Application wizard appears.
4. Click Next. To add a user, click Add. Locate the user and click OK. To remove a user, select the user from the list and click Remove.
5. Click Next.
6. Review the details and click Finish to complete the wizard.

**To modify user and group access to applications**

1. Start the Quick Start tool.
2. On the Management tab, click Applications.
3. Select the Groups and Users option and select a user or group from the User/Group Access pane. Click Modify. The Configure User Access wizard appears.
4. Click Next. Select the application(s) that will be available to the user or group. Click Next.
5. Review the details and click Finish to complete the wizard.

**Managing User Licenses**

Use the Licensing task to view users who are licensed to use XenApp Fundamentals and revoke licenses from users to make the license available to other users.

To view licensed users, start the Quick Start tool. From the Management tab, click Licensing. Licenses can be filtered using the Filter licensed users by field, or you can select a user from the list provided.

To revoke a license from a user, select the user from the list, click Revoke and click Yes to confirm. Any sessions for that user are ended.

**Transferring Licenses**

When you publish an application, you specify the users and groups who can access the application. XenApp Fundamentals grants licenses to users (up to the license quota) without any need for administrative intervention. However, there may be occasions when you need to transfer a license from a user who are no longer using XenApp Fundamentals (for example, when a user leaves the company or when you want to switch access rights from one user to another so that your license quota is not exceeded). The procedure below describes how to transfer licenses in such circumstances.

**To transfer an XenApp Fundamentals license**

1. Start the Quick Start tool.
2. On the Management tab, click Licensing.
3. Select the user who no longer needs access and click Revoke. The user is no longer permitted to use any application published with XenApp Fundamentals.

4. If the user is no longer with your company, disable or delete that user account.

Note: If the user is still with the company but no longer uses XenApp Fundamentals, there is no need to perform this step. However, you may want to prevent the user from accessing the XenApp Fundamentals servers by controlling membership of the Remote Desktop Users group. If you want to prevent users from inappropriately using a license (for example, if an employee changes role within the company and no longer requires access to the server), ensure that the Remote Desktop Users group on the servers includes accounts only for users allowed to use the server.

5. Ensure the new user is permitted to see the appropriate published applications from the server (depending on the users and groups each application is published to, this may be automatic, through appropriate group membership).

6. Ensure the new user is a member of the Remote Desktop Users group on the XenApp Fundamentals server (by default all users are members of this group).

7. Give instructions to the new user about how to access and log on to XenApp Fundamentals.

When the new user launches a published application, that user is granted a license.

Ensure you meet all TSCAL terms and conditions when transferring licenses. See your Microsoft documentation.

Managing Sessions

This section covers the activities a delegated or full administrator can perform to monitor or manage user sessions.

The Sessions screen in the Quick Start tool shows the published applications (but not any published content) that users have open.

If there are many sessions, locate a particular one by typing text in the Filter sessions by box. Any session property appears that matches the text you type, and the filter text is not case-sensitive. Use the buttons on the screen to perform the required operations on selected sessions, including:
• Viewing session details
• Sending messages to users
• Ending sessions
• Disconnecting sessions
• Shadowing sessions

**Viewing Session Details**

You can select a session and view detailed information about the processes, settings, client software, and client cache associated with the selected session.

**To view information about a session**
1. Start the Quick Start tool.
2. On the **Management** tab, click **Sessions**.
3. Select a session. Some details, including the session status and the names of all the applications running in the session, appears on the **Sessions** screen.
4. For further information about the session, click **Details**.

**Sending Messages**

You can send system messages to users connected to XenApp Fundamentals. You can select multiple sessions to send a message to multiple users at the same time.

**To send a message to one or more users**
1. Start the Quick Start tool.
2. On the **Management** tab, click **Sessions**.
3. Select one or more sessions. Click **Message**. The **Send Message** dialog box appears.
   If required, edit the title of the message. The title will appear in the title bar of the message window.
4. Enter the content of the message.
   If required, in **Type of message** select a symbol that indicates the severity of the message. The symbol will appear alongside the message.
5. Click **OK**. The message is sent immediately to the selected users.
Ending Sessions

You end a user’s session, and close all of the applications that are running in it, using the Log off button.

You can send a message to warn users to exit all applications if you need to log off their sessions, but, to avoid data loss, XenApp Fundamentals automatically reminds users to save their work before you do so.

To end a session
1. Start the Quick Start tool.
2. On the Management tab, click Sessions.
3. Select the session that you want to end and click Log off. The Log Off Users dialog box appears, and you are prompted to confirm the logoff request.
4. Click OK. A logoff request is immediately sent to the user asking them to save their work, and the Log Off Users dialog box lists shows you the sessions’ states. The time since the logoff request was sent is also shown.
5. After the users save their work, they are automatically logged off. If the users ignore or cancel the request to save their work, after a suitable period of time, you can end the session immediately by selecting the session and clicking Reset.

Important: Reset a session as a last resort only. Resetting sessions terminates all processes that are running in that session and can result in loss of business data.

Note: Clicking Close does not affect users: it only closes the Log Off Users dialog box.

Disconnecting Sessions

You can disconnect a session to close the connection between a user’s computer and an XenApp Fundamentals server. However, this does not log off the user, and programs that were running in the session are still running on the server. If the user then connects to the server (by selecting a published application), the disconnected session is reconnected to the client.

You disconnect sessions using the Access Management Console, a Citrix tool that you can access from the Resources tab of the Quick Start tool.
If you used the Access Management Console to reset a disconnected session, the word Disconnected appears in the **Status** column on the **Sessions** screen in the Quick Start tool. When you refresh the console display or when the next automatic refresh occurs, the session no longer appears on that screen.

**Shadowing Sessions**

You can remotely monitor and control the actions of users by shadowing their sessions. A shadowed session appears in a separate window on the administrator’s computer, and the administrator is referred to as the shadower.

Shadowing a session provides a powerful tool for you to assist and monitor users. Shadowing is a useful option for your Help desk staff, who can use it to aid users who have trouble using an application. Help desk personnel can follow a user’s actions to troubleshoot problems and can demonstrate correct procedures. You can also use shadowing for remote diagnosis and as a teaching tool.

A shadower can also remotely control a shadowed session through the shadower’s mouse and keyboard.

If **Disable shadowing** was selected during installation, you must reinstall XenApp Fundamentals if you later want to allow shadowing. See “Installing XenApp Fundamentals” on page 23.

The user who will be shadowed is asked to accept or deny the request to shadow the session.

**To shadow a session**

1. Start the Quick Start tool.
2. On the **Management** tab, click **Sessions**.
3. Select the session that you want to shadow and click **Shadow**. The **Shadow** dialog box appears and displays the key sequence that you will use to end shadowing.
4. If you would prefer to use an alternative key sequence to end shadowing, select a modifier key and a final key.
5. Click **Shadow Now**. The **Remote Control Request** appears on the user’s computer.
6. When the user accepts the request to be shadowed (the user must accept within 30 seconds), you are prompted to log on to their computer. Enter your administrator credentials. At this point:
   - The user’s session appears in a new window on your computer.
   - The Shadow Indicator dialog box appears on the user’s computer. This dialog box includes a Stop shadowing button that the user can click to stop shadowing and end the session at any time.

7. To stop shadowing the session, press the key sequence. By default, this is CTRL+*.

Managing Published Applications

You use the Quick Start tool to modify application settings, remove applications, and publish desktops and content.

Modifying Published Application Settings

If you are a full administrator, you can modify the settings of applications previously published in XenApp Fundamentals using the Quick Start tool. See “Providing Access to Applications” on page 35 for instructions about how to publish applications.

To modify published application settings
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Select the application you want to modify and click Modify. The Modify Application wizard appears.
4. Click Next.
5. If required, in the Application path field, enter the path or click Browse to locate the executable file for the application. In the Working directory field, enter the directory or click Browse to select the directory.
6. Click Next.
7. To specify different application path settings on each server, click Edit Paths. The Edit Application Path dialog box appears. Select Use custom application settings to enter the information in the fields provided. Click OK.
8. Click Next.
9. If required, amend the application details for **Display Name**, **Application Name**, and **Description**. Click **Change icon** to navigate to and select the icon to be displayed to users for the published application. Click **Next**.

10. If required, specify the application’s display size and color depth. Click **Next**.

---

**Note:** **Display size** is applicable only when publishing the desktop. It is not applicable to published applications.

11. Click **Add** if necessary to select additional users to access the applications.

   This page provides a flexible search for:

   - **Object Types** to add users and groups to the list for the application
   - **Location** to select the location of the users and groups you want to add
   - **Check Names** to search for object names entered

   To remove users, select the user from the list and click **Remove**.

12. Click **Next**.

13. If required, select one of the following options:

   - **Limit the number of instances running concurrently on the server group** to specify the number of instances of the application that can run at the same time. **This helps you to protect your application licensing agreements.** Select the number using the arrows.
   - **Allow only one instance of the application to be run by each user** to only allow one instance of the application per user. This stops users from accidentally launching multiple instances of an application by clicking too often on the application icon.

14. Click **Next**.

15. Some applications can be launched using various programs. If applicable, select the file type from the list provided to associate with the application. To view the file types, click **Refresh**. Click **Next**.

16. Review your modifications and click **Finish**.
Removing Published Applications

You can remove applications previously published in XenApp Fundamentals using the Quick Start tool.

Note: This procedure does not remove the application from the server. It removes it from the list of applications accessible to XenApp Fundamentals users.

To remove a published application
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Select the application from the list and click Remove.
4. Click Yes to confirm the removal of the selected application.
   The application is no longer available to users and is removed from the Published Applications list.

Viewing Application Information

Published application information appears on the Applications page. To view more details about an application, use the Application Information dialog box.

To view application information
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Select an application from the Published Applications list and click Info.
   The application’s name and description, the server(s) on which it is published, and its default settings appear.
Publishing Content
You can define what shared files and intranet sites are available externally and internally through XenApp Fundamentals. These resources are referred to as content. You can publish content (for example, word processing documents, spreadsheets, and intranet sites) for selected users. The content is presented in the Web interface for an end user to use, as they would use a published application.

Published content can be launched using:

- A local instance associated with the content
- A published application associated with the content

Note: Users must have access to the content you specify.

To publish content launched locally
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Click Publish Content. The Welcome to the Publish Content wizard appears.
4. Click Next.
5. Click Add File. Type the content name to display to your users in the Display name field, and the URL or Universal Naming Convention (UNC) path name for your content in the Location field. Click OK.
6. Click Next. The Modify Servers page appears. Select one or more servers from the Servers list on which the application will be published.
7. Click Next.
8. Click Add if necessary to display the Select Users or Groups search page. This provides a flexible search for:
   - Object Types to add users and/or groups to the list for the application
   - Location to select the location of the users and/or groups you want to add
   - Names to search for object names entered
   To remove users from the list, select the user and click Remove. Click Next.
9. Review your modifications and click Finish.
To publish content launched using a published application
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Click Publish Application. The Publish Application wizard appears.
4. Click Next.
5. Select the application associated with the content you want to publish. Click Next.
6. Follow the steps described in “Publishing Applications” on page 35 to publish an instance of the application associated with the content and complete the wizard.
7. In the Applications page, select the application you just published.
8. Click Modify. The Modify Application wizard appears.
9. Click Next.
10. Append the Universal Naming Convention (UNC) path name or the URL of the content to be associated with this instance to the application path, enclosed in inverted commas. For example:

   C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE “c:\Desktop\Test.xls”

11. Click Next. The Modify Servers page appears. Select one or more servers from the Servers list on which the application will be published.
12. Click Next. The Modify the Application Details page appears.
13. Amend the Display Name to a relevant name for the published content (for example, January Accounts).
14. Click Next. Complete the wizard as described in “Modifying Published Application Settings” on page 76.

Publishing the Desktop
Publishing the desktop allows selected users to access the entire server desktop. This allows you to configure a standard desktop for selected users, restricting applications where necessary and ensuring that users work using standard tools.

To publish the desktop
1. Start the Quick Start tool.
2. On the Setup tab, click Applications.
3. Click Publish Application. The Publish Application wizard appears.
4. Click **Next**.

5. Select the desktop (this is the first item in the list). Click **Next**.

6. Define how the application appears to your users by selecting the display size and color depth:
   - **Displayed size.** Choose between:
     - **Fixed window.** This sets the application screen size to always display at the size you define (in pixels).
     - **Relative.** This displays the application at the ratio defined in the % of screen size box.
     - **Full screen.** This displays the application at full screen.
   - **Color Depth.** Select the required color depth for the display from the drop-down list.

7. Click **Next**.

8. Click **Add** if necessary to display the **Select users or groups** search page.
   This page provides a flexible search for:
   - **Object Types** to add users and/or groups to the list for the application
   - **Location** to select the location of the users and/or groups you want to add
   - **Names** to search for object names entered
     Find and select your users and click **Next**.

9. Review the details and click **Finish**.

### Managing Licenses

#### About XenApp Fundamentals Licenses

There are three types of Citrix licenses for XenApp Fundamentals:

- **Retail** license: A full retail license for XenApp Fundamentals, allowing up to 75 users of XenApp Fundamentals.
- **Not-for-Resale (NFR)** license: Reserved for Citrix and Citrix partners for non-production demonstrations.
Important: You cannot install a license file that brings your total user numbers to over 75.

Licenses are controlled using license files you install and manage through the Quick Start tool. See “Adding Your First License” on page 33 and “Transferring Licenses” on page 71.

**Migrating from an Evaluation to a Retail License**

If you purchased and installed an evaluation license, you must migrate to a retail license for full and continued use of XenApp Fundamentals.

**To migrate to a retail license**
1. Start the Quick Start tool.
2. In the **Setup** tab, click **Licensing**.
3. Click **Migrate to Citrix Retail Licenses**. The **Migrate to Citrix Retail Licenses wizard** appears.
4. Click **Next**. If you did not already download a license file, visit the Citrix Web site and follow the on-screen instructions to activate and download the file.
5. Click **Browse** to select your downloaded license file.
6. Click **Next**.
7. Review the license details and click **Finish**.

**Installing Additional Licenses**

Adding licenses lets you increase the number of users who can use XenApp Fundamentals.

**To install an additional license**
1. Start the Quick Start tool.
2. In the **Setup** tab, click **Licensing**.
3. Click **Add Citrix licenses**. The **Add Citrix Licenses wizard** appears.
4. Click **Next**. If you did not already download a license file, visit the Citrix Web site and follow the on-screen instructions to activate and download the file.
5. Click **Browse** to select your downloaded license file.
6. Click **Next**.
7. Review your details and click **Finish**.

**Managing Administrator Accounts**

**Adding Administrator Accounts**
Use the Quick Start tool to add new administrators. See “Setting Up Administrator Accounts” on page 54.

**Removing Administrator Accounts**
You may need to remove administrator accounts, for example, to accommodate changes to personnel. Only full administrators can remove other XenApp Fundamentals administrator accounts.

**Important:** If only one full administrator remains on the list, you are prevented from removing it. Also, you cannot remove the built-in administrator account, local server administrators, or your own account.

**To remove an administrator account**
1. Start the Quick Start tool.
2. In the **Setup** tab, click **Administrators**.
3. Select the administrator you want to remove and click **Remove**.
4. Click **Yes** to confirm removal of the selected administrator.

**Managing XenApp Fundamentals Remotely**
XenApp Fundamentals can be managed remotely. Citrix recommends that you create a delegated administrator account to manage XenApp Fundamentals remotely. After the remote connection is made, this delegated administrator then logs on as a full administrator to provide full administrative functions.

**To log on remotely as an administrator**
1. Start a Web browser and visit the remote URL for XenApp Fundamentals.
2. Log on using the delegated administrator credentials.
3. Click **Administrator tools**.
4. Locate the icon for the server you want to manage, then click **Server Console for that server**. You are connected to the XenApp Fundamentals server and the Windows logon dialog box appears.

5. Log on using full administrator credentials.

You can then perform administrative functions remotely.

### Performing Server Maintenance

In some instances, servers need to be taken offline for maintenance tasks such as hardware or software upgrades. You may also be advised in alert emails to reboot servers in order to solve some server issues. In these cases, you should perform the reboot using the server maintenance procedure in this section.

Before the server becomes unavailable to users, you can opt to advise users of any consequences.

**To perform server maintenance**

1. Start the Quick Start tool.
2. In the **Setup** tab, click **Servers**.
3. In the **Servers** pane, select the server to take offline for maintenance. Click **Maintain**. The Server Maintenance wizard appears.
4. Click **Next**. The server is put in maintenance mode and sessions are redirected to other servers.
5. Select one of the following options:
   - **Log off all users** to log users off XenApp Fundamentals. Users will still have time to save their work.
   - **Send a message to all users** to inform them that their sessions may become unstable.
   - **Do nothing** to keep user sessions active without sending a warning about session stability.
6. Review the details and click **Finish** to complete the wizard.
To restore a server after maintenance

1. Start the Quick Start tool.
2. In the Setup tab, click Servers.
3. In the Servers pane, select the server taken offline for maintenance. Click Restore.
4. Click Yes to confirm.

The server is restored from maintenance mode.

Managing Printers

After you set up your XenApp Fundamentals printers, you can modify the settings using the Printers page in the Quick Start tool.

Setting a Default Printer

You can set a printer to be the default printer for all clients’ use.

To set a default printer

1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Select the required printer in the Printers pane.
4. Click Set Default.

Note: If you do not set a default printer in Quick Start and client printing is enabled, Windows sets the default printer to the client’s default printer. If client printing is not enabled, Windows sets the default printer to that defined by the Windows environment.
Clearing a Default Printer
You can clear the default printer so that you have no default printer defined in Quick Start.

To clear a default printer
1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Select the required printer in the Printers pane.
4. Click Clear Default.

Removing a Printer
You can remove client and published printers using Quick Start. To remove Windows managed printers, you must use the Windows print management software on the XenApp Fundamentals server.

To remove a printer
1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Select the required printer in the Printers pane.
4. Click Remove.
5. Confirm that you want to remove the selected printer.

Enabling Client Printing after Setup
You can enable client printing even after your initial setup using Quick Start.

To enable client printing after initial setup
1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Click Enable client printers in the Other Tasks menu.
4. Click Yes at the confirmation dialog box.
Adding Published Printers
You can publish network printers after initial configuration using Quick Start.

To add published printers
1. Start the Quick Start tool.
2. In the Setup tab, click Printers.
3. Click Manage published printers in the Other Tasks menu. The Manage Published Printers wizard appears. Click Next.
4. The Network Printer Credentials page appears.
5. If your current credentials are sufficient to locate the printers required, click Next. If you require different credentials, select Use alternative account and enter the account details. The Select Printers to Publish page appears and Quick Start searches for printers on the network.

Note: Quick Start searches for all printers on the network that can be accessed using the administrator credentials entered. In a large network, this can take considerable time.

6. Select the printers required from the Available network printers list, expanding nodes as needed to display the printers.
   —Or—
   Click Add and type the full name of the print server in the Add a Print Server box. Click OK to add the server.
7. Click Select to add the selected printers to the Selected network printers list. Click Unselect to remove unwanted printers from the Selected network printers list.
8. After you add all the printers required, click Next. The Select default printer page appears.
9. If a default printer is required, check Set the default printer and then select the printer you want to be the client device’s default printer. Click Next.
10. The Published Printers Summary page appears. Click Finish to publish your selected printers or Back to make any changes.
Managing Certificates

To maintain external access to published applications you must create new certificates or renew your current ones when they expire.

After you implement external access, you can create new certificate requests to renew existing certificates, or to obtain a certificate from a different Certificate Authority.

Creating and Importing a New Certificate

To create a new certificate request
1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
4. Enter the public (external) address of the server running XenApp Fundamentals. If enabling access from the Internet, this is server.registered DNS domain name (for example xenapp-fundamentals.citrix.com). Click Next.
5. Type your organization’s name and organizational unit. Click Next.
7. Select Manually submit the certificate request to a Certificate Authority and click Next.
8. Specify the file name and location for your certificate request. You submit this file to your chosen Certificate Authority when you request a certificate. Click Next.
9. Review the details and click Finish to create the certificate request.

You must contact your chosen Certificate Authority and submit your certificate request. The authority sends you your certificate after processing your request.

To enable a new certificate
1. Start the Quick Start tool.
2. In the Setup tab, click External Access.
3. Click Import requested certificate. The Certificate Import wizard appears. Click Next.
4. Enter the path and file name of your Certificate Authority’s response. Click Next.
5. Specify the TCP port that will be used for remote connections. You can select a standard HTTPS port, or use a custom TCP port. Click Next.

6. Review the details and click Finish to import the certificate.

Using Advanced Application Settings

Using the Applications task in Quick Start, you can configure optimization settings to maximize performance, and enable dictation quality audio to enable sound in client sessions.

Configuring Optimization Settings

There are two optimization settings you can configure using Quick Start. CPU optimization increases the number of users who can use XenApp Fundamentals at any one time, and improves its ability to manage resources during periods of most use. During optimization, XenApp Fundamentals allocates an equal share of the CPU to each user. This prevents one user from affecting the productivity of other users and allows more users to connect to XenApp Fundamentals at the same time.

Memory optimization improves system speed and performance. This is especially useful when user demand exceeds available random access memory (RAM), causing system performance to degrade.

Note: Citrix recommends that you use the default application optimization settings as indicated below:

- Enable CPU optimization—on
- Enable memory optimization—off

Enable memory optimization is off by default to accommodate applications that are not compatible with this technology.

After upgrading from earlier versions of XenApp Fundamentals, the application optimization settings in the previous deployment are retained. Application optimization is not applicable to digitally signed applications, such as some of Microsoft Office.

To modify memory optimization performance settings

1. Start the Quick Start tool.
2. In the Setup tab, click Applications.
3. Select Advanced Settings.
4. Select the option you want to disable/enable (Enable memory optimization, or Enable CPU optimization).

5. Click OK.

Enabling Dictation Quality Audio

Dictation quality audio enables high quality sound in client sessions. This is particularly useful for users of dictation software. Enabling dictation audio quality gives all applications full access to sound streaming (for example, applications playing music or videos).

If you enable dictation quality audio in Quick Start, you must instruct your users to change their Web Interface settings to activate it on their clients. To use this feature, each user must log on to XenApp Fundamentals and change the Web interface audio settings to High Quality on each client device they use. High quality audio requires high bandwidth connections. Therefore, Citrix recommends you advise users not to enable High Quality audio for external client devices, unless they are using a high bandwidth connection.

To enable dictation quality audio

1. Start the Quick Start tool.
2. In the Setup tab, click Applications.
3. Select Advanced Settings.
4. Select Enable Dictation quality audio.
5. Click OK.

Note: This enables dictation quality audio for all client devices.

To change Web Interface settings for dictation quality audio

1. Log on to XenApp Fundamentals on a client device.
2. Select Customize User Interface > Connection Preferences > Performance.
3. Set Audio Quality to High quality.
4. Click OK.
This chapter explains how to secure your XenApp Fundamentals deployment. Topics include:

- General security guidelines.
- General information about security and cryptography, for readers new to this field. This is particularly relevant to single server deployments.
- Guidelines for the use of user names and passwords.
- Information for two–factor authentication.

**Securing the Environment**

It is vitally important that you:

- Review your system to ensure that the file permissions are appropriate for your user and security requirements.
- Install a commercially recognized virus checker on the server running XenApp Fundamentals, and keep the virus definitions up to date.
- Ensure that you keep the server running XenApp Fundamentals up to date with all relevant Microsoft updates and patches.
- Follow Microsoft recommendations for system integrity and security.

**Overview of Security, SSL, and Certificates**

Direct to server deployments rely on the use of digital certificates to ensure secure remote access across public networks. This section describes the security protocols, such as SSL (Secure Sockets Layer), used by certificates and the concepts of cryptography on which these protocols are based. The section also discusses what the main threats to secure communications are and how SSL is designed to tackle these threats.
The SSL Protocol

The SSL protocol provides the ability to secure data communications across networks. SSL provides server authentication, encryption of the data stream, and message integrity checks. SSL uses cryptography to encode messages, authenticate their identity, and ensure the integrity of their contents. This guards against risks such as eavesdropping, misrouting, and data manipulation. SSL relies on public key certificates, issued by certificate authorities, to ensure proof of identity.

About Cryptography

SSL uses cryptography to secure communications. Cryptography provides the ability to encode messages to ensure confidentiality. Cryptography is also used to authenticate the identity of a message and to ensure the integrity of its contents.

Certificates and Certificate Authorities

SSL uses public key Certificates and Certificate Authorities.

A certificate is a digital file issued by a trusted organization known as a Certificate Authority (CA). A certificate is basically “proof of identity.” Certificates generally have a common format, usually based on ITU standards. The certificate contains information that includes the:

- **Issuer.** This is the organization that issues the certificates.
- **Period of validity.** The certificate’s start date and expiration date.
- **Public key.** A secret key used to encrypt data.
- **Issuer’s signature.** The CA digitally signs the certificate to guarantee its authenticity.
- **Subject.** The name of the entity that the certificate identifies; for example, the name of the computer running XenApp Fundamentals.

A number of companies and organizations currently act as Certificate Authorities, including VeriSign and their affiliates.

Certificate Revocation Lists

From time to time, CAs issue Certificate Revocation Lists (CRLs). CRLs contain information about certificates that can no longer be trusted—for example, because the private key is compromised. Therefore, before trusting a public key, your client software checks that its certificate is not revoked.
Obtaining a Digital Certificate

Obtaining a digital certificate can be an involved process; it is important first to accurately estimate how many digital certificates you require and then to allow enough time for the process of obtaining them.

This section helps you identify the number and type of certificates you will require and the considerations to keep in mind when deciding from where to obtain certificates.

Determining the Certificates Required

There are two main types of digital certificate:

- **Identity certificate**: This identifies a specific server—for example, the computer running XenApp Fundamentals. The type of identity certificate that is required by XenApp Fundamentals is called a Server Certificate.

- **Root certificate**: This identifies the CA that signed the identity certificate. The root certificate belongs to the CA.

For SSL to work, you require a server certificate at one end of the connection and a root certificate at the other end. Therefore:

- A server certificate must be installed on the computer running XenApp Fundamentals.

- A root certificate must be installed on the client device when using local domain certificates and temporary certificates. However, with recognized Certificate Authorities the root certificate is usually part of the Web browser itself (the majority of Web browsers and Web servers support SSL). With a certificate from a Certificate Authority, there is no need to obtain and install a root certificate on the client devices.

Obtaining Certificates

After you identify the number and type of certificates required to secure your software deployment, you must decide where to obtain the certificates. This depends on a number of factors, including:

- Whether or not your organization has already established a business relationship with a public Certificate Authority (CA)

- The cost of certificates, the reputation of a particular public CA, and so on

- The size of your deployment

You can obtain your certificates from a public CA, such as VeriSign. For example, you can use the following certificates with XenApp Fundamentals:

• A 128-bit SSL server certificate from beTRUSTed

You may want to consider running your own CA, using the free Microsoft Certification Services option. Note that, if you issue your own certificates, you need to install the root certificate on all client devices. For more information about this, see the Microsoft documentation.

Temporary certificates can be implemented using XenApp Fundamentals. These expire after 30 days, and are designed to enable external access while a request from a Certificate Authority is being processed, or for evaluation and test use. If you use a temporary certificate, you need to install the root certificate on all client devices.

About the Verification Process

Obtaining a digital certificate from a public CA involves a complex verification process in which:

• Your organization provides corporate information so that the CA can verify that your organization is who it claims to be. This may involve other departments in your organization, such as Accounts, to provide Letters of Incorporation or similar legal documents.

• Individuals with the appropriate authority in your organization are required to sign legal agreements provided by the CA.

• The CA verifies your organization as a purchaser; your purchasing department is likely to be involved.

• You provide the CA with contact details of suitable individuals whom they can call if there are queries.

Generating a Certificate Signing Request (CSR) File

After you decide which Certificate Authority to get your certificates from, the next step is to create a certificate signing request (CSR) file that you can send to the authority. You can easily generate a CSR file using the External Access task provided in the Quick Start tool.

After you receive a server certificate from the authority, you install this on the server running XenApp Fundamentals. Again, you do this using the External Access task in the Quick Start tool. The certificate must originate from a CSR created with the External Access wizard. See “External Access Direct to Server” on page 42.

For more information about creating a CSR file, submitting a request to a Certificate Authority, and installing a certificate, see “External Access Direct to Server” on page 42.
Creating a Certificate Backup

After you receive your certificate, it is important to make a backup copy in case of system corruption.

You use the Microsoft Management Console (MMC) to create a backup of your certificate. To do this you need to add the Certificates snap-in to the console.

**To add the Certificates snap-in to the MMC**

1. From your Desktop click **Start** and then click **Run**.
2. Type `mmc` and click **OK**. This starts the Microsoft Management Console.
3. On the **File** menu, click **Add/Remove Snap-in** and then click **Add**.
4. Select **Certificates** and click **Add**. The **Certificates snap-in** dialog box appears.
5. Select **Computer account** and click **Next**. The **Select Computer** dialog box appears.
6. Select **Local computer** and click **Finish**.
7. Click **Close**.
8. Click **OK**.

The Certificates snap-in is added to the console.

**To create a certificate backup using the MMC**

1. Start the Microsoft Management Console.
2. Select **Certificates (Local Computer) > Personal > Certificates**.
3. Select the certificate for backup.
4. From the right-mouse menu, select **All Tasks > Export**. This starts the Certificate Export wizard. Click **Next**.
5. Select **Yes, export the private key**. Click **Next**.
6. Under **Personal Information Exchange - PKCS #12 (.PFX)** select **Enable strong protection**. Ensure **Delete the private key if the export is successful** is not selected. Click **Next**.
7. Type and confirm a password to protect the private key information. Click **Next**.
8. Specify the filename and location for the export. Click **Next**.
9. Review the details and click **Finish**.
To import a certificate backup using the MMC
1. Start the Microsoft Management Console.
2. Select Certificates (Local Computer) > Personal > Certificates.
3. From the right-mouse menu, select All Tasks > Import. The Certificate Import Wizard appears. Click Next.
4. Locate and select the file to import. Click Next.
5. Type the password for the certificate and click Next.
6. Select Place all certificates in the following store and select Personal. Click Next.
7. Review the details and click Finish.

Renewing Security Certificates
When the license for your current certificate expires, you must renew your security certificate from your Certificate Authority.

Renewing an expired certificate follows the same process as installing a new one. See “To generate a certificate request for the direct to server deployment” on page 43.

When a certificate expires, you can use a different authority, rather than renewing the existing certificate.

For more information about renewing certificates, go to your authority’s Web site.

User Names and Passwords
Your users’ Windows user names and passwords provide a vital component to your system security. The combination of user name and password is the first barrier to unauthorized access from the Internet. Be aware that any user with a weak password could expose your network to unauthorized access.

Citrix strongly recommends that a strict password policy is applied to your network, particularly if you are not using two-factor authentication (see “User Authentication” on page 97).

An example policy is:
• Passwords should be at least eight characters in length and should contain a combination of uppercase and lowercase letters and at least one non-alphanumeric character.
• A password should never be a word that can be looked up in a dictionary, a modified dictionary word, or related to any name or user ID.
• The best passwords contain a mixture of letters, numbers, and punctuation (for example, laK5dog%, whoOlCsh2?, su$$Pp*er8, Big3pig!!). The first characters of a memorable phrase, with additional numbers and punctuation thrown in, make a good password; for example, Mary had a little lamb: 5mhall!

• Avoid any names, words, numbers, or abbreviations that can be found in your personal data (for example social security numbers, maiden names, names of relatives, or any memorable dates).

• Avoid passwords that can be guessed by knowing something personal about you, such as nicknames, names of pets, or significant others.

• Avoid simple variants or permutations of any of the above (for example, an S replaced by a 5; an E replaced by a 3).

• Change a user name’s password immediately if you think it may no longer be secret.

• Passwords should be changed regularly.

User Authentication

The following types of user authentication are supported in XenApp Fundamentals:

• **Standard authentication.** Each user has a unique name and password as their Windows domain credentials. This combination allows access to XenApp Fundamentals and to applications.

• **Two-factor authentication.** This is the recommended and most secure option for external access. In addition to the user name and password (or domain credentials), each user has a unique password-generated code that allows precise identification of the user. You can implement either Secure Computing SafeWord for Citrix or RSA SecurID, provided the appropriate software is installed.

You can enable user authentication after external access is enabled.

Enabling Standard Authentication

Standard authentication is the minimum security requirement for external access. If no other authentication method is installed, standard authentication is enabled by default.

**To manually enable standard authentication**

1. Start the Quick Start tool.
2. In the **Setup** tab, click **External Access**.
3. Click **Configure authentication**. Click **Next**.
4. Select **Standard authentication (user name and password)**. Click **Next**.
5. Click **Finish** to enable standard authentication. Click **Back** to make any changes.

**Enabling Secure Computing SafeWord for Citrix**

Citrix recommends that XenApp Fundamentals is installed **before** installing the SafeWord Agent on the same server.

Install SafeWord server software on the primary domain controller. See your SafeWord documentation for how to install the system.

**To enable Secure Computing SafeWord for Citrix**

1. Start the Quick Start tool.
2. In the **Setup** tab, click **External Access**.
3. Click **Configure authentication**. The Configure External Access Authentication wizard appears. Click **Next**.
4. Select **Safeword for Citrix**. Click **Next**.
5. Click **Finish** to enable Safeword for Citrix. Click **Back** to make any changes.

**Enabling RSA SecurID**


You enable RSA SecurID using the Quick Start tool; see “Providing Access to Applications” on page 35.

This section describes the requirements for RSA SecurID and how to configure the software.

**SecurID Requirements**

Citrix recommends that XenApp Fundamentals is installed before installing the ACE/Agent on the same server

---

**Note:** During installation of the ACE/Agent, select Common Shared Files and User Documentation, and ensure that these components are installed. The RSA ACE/Agent can be downloaded from the RSA site at [http://www.rsasecurity.com/](http://www.rsasecurity.com/)
The ACE/Agent must be installed on the XenApp Fundamentals server. See your RSA SecurID documentation for how to install the system.

The ACE server must be installed on a machine different from the one running XenApp Fundamentals.

User Names
User names in the RSA ACE/Server database need to be in the simple form of username (for example, BWayne). Do not include the domain name in user names.

See your RSA SecurID documentation for more information about populating the ACE database.

Adding the Computer Running XenApp Fundamentals as an Agent Host
You must create an Agent Host for XenApp Fundamentals in the RSA ACE/Server database, so that the RSA ACE/Server recognizes and accepts authentication requests from XenApp Fundamentals. When creating an Agent Host, select Net OS Agent from the Agent type list.

Copying the Sdconf.rec File
Locate (or if necessary, create) the Sdconf.rec file on the RSA ACE/Server and copy it to the Windows\System32 directory on the computer running XenApp Fundamentals. This file provides the server with the information necessary to connect to the RSA ACE/Server.

Node Secret Registry Key Considerations
The node secret is used to ensure secure communication between XenApp Fundamentals and the RSA ACE/Server.

The node secret can become out of synchronization between these two servers in the following circumstances:

- If the operating system on the computer running XenApp Fundamentals is reinstalled
- If the Agent Host record for the server running XenApp Fundamentals is deleted and then added again
- If the Sent Node Secret box is not selected in the Edit Agent Host dialog box on the RSA server
- If the RSA server is reinstalled
- If the node secret registry key is deleted on the computer running XenApp Fundamentals
If the node secret on the computer running XenApp Fundamentals and the RSA ACE/Server do not match, RSA SecurID fails. You must reset the node secret on the computer running XenApp Fundamentals and the RSA ACE/Server.

**Important:** Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk and always make a backup of your registry before attempting any edits.

To reset the node secret on the computer running XenApp Fundamentals
1. In the system registry, navigate to:
   
   HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT

2. Delete the NodeSecret key.

**Note:** Reinstalling XenApp Fundamentals does not delete the node secret key. If the Agent Host entry remains unchanged on the RSA server, the node secret can be reused.

To enable RSA SecurID
1. Start the Quick Start tool.
2. In the **Setup** tab, click **External Access**.
3. Click **Configure authentication**. The **Reconfigure External Access Authentication wizard** appears. Click **Next**.
4. Select **RSA SecurID**. Click **Next**.
5. Click **Finish** to enable RSA SecurID. Click **Back** to make any changes.
Index

A
administrators
  adding accounts 83
  creating delegated 55
  creating full 54
  delegated 15
  full 15
  removing accounts 83
advanced application settings 89
advanced mode
  overview 63
application servers
  setting up 25
applications
  advanced settings 89
  changing access to 71
  managing 76
  managing users 70
  modifying settings 76
  providing access to 35
  publishing 35
  removing 78
  viewing information 78
audio
  bandwidth limitations 90
  dictation quality 90
authentication
  configuring 53
  RSA SecurID 54
  SafeWord for Citrix 54
  standard 53, 97
  two-factor 53, 97

B
browsers, supported 22

C
Certificate Revocation Lists 92
Certificate Signing Requests 94
certificates
  creating 88
  creating backups 95
  enabling 44
  generating Certificate Signing Requests 94
  generating requests 43
  importing 88
  local 44
  renewing 96
  revocation lists 92
  root 93
  server 93
  temporary 49
  types of 93
Citrix resources 30
Citrix Web Interface 13
clients
  device requirements 21
content
  publishing 79
CRL. See Certificate Revocation Lists
cryptography
  overview 92

d
delegated administrator 15
deployments
  direct to server 13
  DMZ 14
  planning 12
  scenarios 12
desktop
  publishing 80
dictation quality audio 90
DMZ. See demilitarized zone
DNS. See Domain Name Service
domain controllers, installing on 19
domain credentials 13
Domain Name Service 14

E
email alerting
configuring 55
disabling 58
enabling 57

Essential Business Server 26
changing server groups 33
installing 26
launching Quick Start 33
managing applications 32
managing sessions 32
overview 31
revoking licenses 32
tasks 32
working with servers 32

external access
configuring 37
enabling DMZ servers 51
enabling VPNs 52
testing 53

F
failover
configuring 64
features 9
firewall configuration
direct to server 20
firewalls
DMZ 20
TCP port settings 20
VPN 20
full administrator 15

I
identity certificates 93
installation
system requirements 19
uninstalling 25
installing
on a domain controller 19
overview 18
internal access
testing 36
Internet Protocol
disabling version 6 38
IPv4 38
IPv6
disabling 38
ISA Server 47
configuring SSL ports for 47

L
licenses
adding 82
adding first 33
evaluation 81
maximum number 33
migrating 82
not-for-resale 81
retail 81
transferring 71
licensing
overview 33

M
management tasks 29
messages
sending 73
sending to users 73
Microsoft resources 30

N
NAT. See Network Address Translation
Network Address Translation 52
Network Interface Card 20
NIC. See Network Interface Card

O
optimization
CPU 89
virtual memory 89

P
passwords
policies 96
printers 58
  adding published printers 87
  clearing default 86
  client 58, 60
  client and published 61
  enabling client printing 86
  managing 85
  network 60
  providing access 58
  published 58
  removing 86
  setting default 85
  Windows managed 58–59
public certificate authority 93
publishing content 79

Q
Quick Start tool
  interface 28
  overview 27
  Overview screen 28
  tasks 31

R
remote administration 83
Removing. See uninstalling
Resources tab 29
Root certificates
  distributing to clients 46, 51
  saving 50
root certificates 93
  saving 46
RSA SecurID 54
tokens 54

S
SafeWord for Citrix 54
Secure Gateway 13
Secure Sockets Layer 91
  overview 92
security
  minimum requirements 37
  user authentication 97
security requirements
  external access 37
server certificates 93
server failover 64
server groups
  joining 63
  removing servers from 64
server maintenance 84
servers
  maintenance 84
  promoting to master 63
  removing from server groups 64
  restoring after maintenance 85
  setting up 63
  setting up failover 64
sessions
  disconnecting 74
  ending 74
  overview 72
  sending messages 73
  shadowing 75
  viewing details 73
setup tasks 28
shadowing
  disabling 75
  enabling 24
shadowing sessions 75
SpeedScreen 12
SSL. See Secure Sockets Layer
system requirements 19

T
Terminal Server License servers
  activating 34
  testing external access 36, 53
tokens 54

U
uninstalling 25
user applications 70
user licenses 71
user management 69
user profiles
  overview 65
  setting up 65
users
  adding to applications 70
  licenses 71
  managing 69
  managing individual 70
  modifying access to applications 71
  removing from applications 70
  sending messages to 73
W

Web address
  internal users 67
  remote users 67
Windows Essential Business Server 26

X

XenApp Fundamentals
  features 9
  introduction 8