



Exchange Server 2003 Client Access Guide



Valid Until:
Product Version:
Reviewed By:
Latest Content:
Author:

September 7, 2004
Exchange Server 2003
Exchange Product Development
www.microsoft.com/exchange/library
Joey Masterson





Exchange Server 2003 Client Access Guide

Joey Masterson

Published: April 2004

Applies To: Exchange Server 2003

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2004 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveSync, ActiveX, Microsoft Press, MSDN, MSN, Outlook, Windows, Windows NT, Windows Server, Windows 95, and Windows 98 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Acknowledgments

Project Editor: Diane Forsyth

Technical Reviewers: Exchange Product Team

Graphic Design: Kristie Smith

Production: Joe Orzech, Sean Pohtilla

Table of Contents

Introduction	1
Who Should Read This Guide?	1
How Is This Guide Structured?	1
Hardware Requirements.....	2
Software Requirements.....	2
Chapter 1	
Understanding Exchange Server 2003 and Client Access.....	3
New Features for Exchange 2003 and Outlook 2003.....	3
Improvements in Outlook Web Access 2003	4
Mobile Services for Exchange	6
Exchange ActiveSync	6
Outlook Mobile Access.....	7
Planning Your Exchange Client Access Infrastructure	7
Chapter 2	
Configuring Exchange Server 2003 for Client Access	9
Securing Your Exchange Messaging Environment.....	9
Updating Your Server Software	9
Securing the Exchange Messaging Environment.....	9
Securing Communications.....	10
Deploying the Exchange Server Architecture.....	15
Configuring a Front-End Server	15
Configuring Exchange for Client Access.....	15
Configuring Outlook 2003 Features	16
Configuring Mobile Device Support.....	16
Configuring Outlook Mobile Access.....	19
Configuring Outlook Web Access	20
Configuring POP3 and IMAP4 Virtual Servers	24
Chapter 3	
Managing Client Access to Exchange Server 2003	25
Managing Protocols	25
Enabling a Virtual Server	25
Assigning Ports and an IP Address to a Virtual Server.....	26
Setting Connection Limits.....	27

Starting, Pausing, or Stopping a Virtual Server	28
Disconnecting Users	28
Managing Calendaring Options for the POP3 and IMAP4 Virtual Servers	28
Managing the HTTP Virtual Server	29
Working with IMAP4-Specific Settings	30
Configuring NNTP Posting Limits and Moderation Settings	30
Managing Outlook Web Access	32
Enabling and Disabling Outlook Web Access for Internal Clients Only	32
Using Browser Language Settings	33
Blocking Web Beacons	34
Configuring Attachment Handling	34
Blocking Attachments	35
Specifying Front-End Servers That Allow for Attachment Handling.....	35
Filtering Junk E-Mail Messages	36
Managing Exchange ActiveSync	36
Enabling Exchange ActiveSync for Your Organization	36
Enabling Up-to-Date Notifications for Your Organization	37
Managing Outlook Mobile Access	39
Configuring Exchange to Use Outlook Mobile Access	39
Enabling Outlook Mobile Access for Your Organization	39

Appendix A

Resources	42
Resources Cited in This Guide	42
Exchange Server 2003	42
Windows 2000	42
Other Web Sites	42
Additional Resources	42
Web Sites.....	43
Exchange Server 2003 Books.....	43
Resource Kits	43
Accessibility	43

Introduction

This guide provides essential information about working with Microsoft® Exchange Server™ 2003 and client access. This guide describes the new features for Exchange 2003 and Microsoft Office Outlook® 2003, in addition to improvements in Microsoft Office Outlook Web Access 2003. It contains configuration information, such as how to secure your messaging environment, deploy the server architecture, and configure the Exchange servers for your supported client access methods. Finally, this guide describes how to manage protocols, the Exchange Virtual Server, Outlook Web Access, Exchange ActiveSync®, and Microsoft Outlook Mobile Access.

Who Should Read This Guide?

Anyone with a technical background can benefit from reading this guide; however, it is designed to produce maximum benefits for the following professionals:

Systems Architects

Those individuals responsible for planning and crafting overall business strategies and solutions

Enterprise Exchange Administrators

Those individuals responsible for installation, maintenance, and administration of software in the enterprise

Exchange User Account Managers

Those individuals responsible for setting up individual e-mail accounts and modifying individual Exchange accounts in the Microsoft Active Directory® directory service

Messaging Supports

Those individuals who specialize in troubleshooting the causes of problems that end-users have with their messaging environment

Helpdesk Operators

Those individuals who help end-users with a variety of hardware and software issues, including simple messaging issues

How Is This Guide Structured?

This guide has three chapters and one appendix. For best results, review these chapters in order because each chapter builds on the concepts discussed in previous chapters.

Chapter 1, "Understanding Exchange Server 2003 and Client Access"

This chapter presents an overview of the new features in Exchange 2003 and Outlook 2003.

Chapter 2, "Configuring Exchange Server 2003 for Client Access"

This chapter provides information about configuring Exchange 2003 for client access. It covers securing the Exchange messaging environment, deploying the server architecture, and configuring the Exchange servers for your supported client access methods.

Chapter 3, "Managing Client Access to Exchange Server 2003"

This chapter describes how to manage the client access settings for the protocols and clients supported in your organization.

Appendix, "Resources"

This section contains links to resources that will help you maximize your understanding of Exchange Server clients.

Hardware Requirements

You need the following hardware to do the procedures in this guide. This list does not include your general Exchange servers, storage hardware, and so on. It includes only security-specific hardware requirements:

- Two firewalls (or routers)
 - RSA SecurID PIN generators (for each mobile client)
 - A minimum of one front-end server running Internet Security and Acceleration (ISA) Server
-

Software Requirements

You need the following software to do the procedures in this guide:

- Microsoft Exchange Server 2003 Enterprise Edition
- Microsoft Internet Security and Acceleration (ISA) Server
- Microsoft Windows 2000 Advanced Server
- RSA SecurID Server version 1.x

Understanding Exchange Server 2003 and Client Access

Exchange 2003 provides users with increased client messaging functionality. Exchange 2003 builds on the technologies of earlier versions of Exchange and now includes several significant messaging capabilities. New for Exchange 2003 are the following:

- Outlook 2003 cached mode
- Outlook 2003 using RPC over HTTP
- Mobile device support using Outlook Mobile Access and Exchange ActiveSync
- Improved Outlook Web Access for Exchange 2003

The new and improved clients enable you to provide your users with a simplified remote access, more access options, and an improved user experience. The following sections briefly describe the new and improved clients and client messaging technologies for Exchange 2003.

New Features for Exchange 2003 and Outlook 2003

The following sections describe the new features in Exchange 2003 and Outlook 2003 that make your messaging and information management tasks easier to perform.

Exchange server access through the Internet (RPC over HTTP)

Outlook can now connect to Exchange 2003 through the Internet without the need to use slow and sometimes unavailable virtual private network (VPN) connections. This feature enables you to access your Exchange 2003 account from the Internet when you are working outside your organization's firewall without any special connections or hardware, such as smart cards and security tokens. For more information about configuring Exchange 2003 to use RPC over HTTP, see the article *Exchange Server 2003 RPC over HTTP Deployment Scenarios* (<http://go.microsoft.com/fwlink/?linkid=24823>).

Synchronization Improvements

To reduce the amount of information that is sent between the Outlook 2003 client and Exchange 2003 servers, Exchange 2003 performs data compression. Exchange 2003 also reduces the total requests for information between the client and server, thereby optimizing the communication between the client and the server.

New Data File Type (.pst)

Outlook introduces a new file format for personal folder (.pst) files that offers greater storage capacity for items and folders and support for multilingual Unicode data.

Note A file created with the new Outlook .pst file format is not compatible with earlier versions of Outlook. For compatibility with earlier versions of Outlook, create files by using the .pst file format for Outlook 97 through Outlook 2002. Outlook 2003 can view and create files of either type.

Kerberos authentication protocol

Exchange 2003 allows Outlook 2003 clients to authenticate to Exchange 2003 servers by using Kerberos authentication.

Cached Exchange Mode

The addition of Cached Exchange Mode, combined with the synchronization and optimization improvements, significantly enhances the remote end-user's experience with Outlook. For example, in earlier versions of Outlook, dialog boxes would display requests for information from an Exchange server; however, in Outlook 2003, these requests no longer appear on a user's Outlook client because the user works primarily from their local Exchange mailbox data file (this functionality also reduces the total load on your Exchange servers). More importantly, if network connectivity is lost between the Outlook client and the network, Outlook 2003 will operate without interruption.

Improvements in Outlook Web Access 2003

The new version of Outlook Web Access in Exchange 2003 contains improvements such as forms-based authentication, rules, spell checking, and the ability to send and receive digitally signed and encrypted e-mail messages. The user interface has also been redesigned to provide a user experience that is similar to that provided with Outlook 2003, including a right preview pane and improved navigation pane.

Outlook Web Access for Exchange 2003 can perform faster, especially over slow connections, and therefore will be more responsive to user interactions.

The following list briefly describes some of the new features for Outlook Web Access for Exchange 2003:

Bytes over the wire

The speed of Outlook Web Access has been improved by reducing the amount of information that must travel from the server to the browser. Fewer bytes are sent over the wire from server to browser. However, be aware that the logon process involves more bytes than the logon process in Outlook 2003.

Compression support

Administrators can configure compression support for Outlook Web Access, which improves performance on slow network connections and provides increased performance for most actions on slow network connections. Outlook Web Access compression works by compressing either static or dynamic or both types of Web pages, depending on the compression setting you are using. You can enable compression from Exchange System Manager.

Forms -based authentication

You can enable a new logon page for Outlook Web Access that will store the user's name and password in a cookie instead of in the browser. When a user closes the browser, the cookie is cleared. Additionally, after a period of inactivity, the cookie is cleared automatically. The new logon page requires users to enter their domain, user name, and password, or their full user principal name (UPN) e-mail address and password. To enable the Outlook Web Access logon page, you must enable forms-based authentication on the server.

S/MIME support

Secure/Multipurpose Internet Mail Extensions (S/MIME) increases the security of Internet e-mail by enabling digital signing of messages, in addition to message encryption. Digital signatures provide authentication, non-repudiation, and data integrity. Message encryption provides confidentiality and data integrity.

Outlook Web Access in Exchange 2000 did not support signed and encrypted e-mail. Now, with the new Microsoft Outlook Web Access S/MIME ActiveX® control, users can digitally sign and encrypt e-mail messages. The S/MIME control works with any X.509 v3-based public key infrastructure (PKI) to provide the signing and encryption capabilities.

For more information about S/MIME support in Outlook Web Access, see *What's New in Exchange Server 2003* (<http://go.microsoft.com/fwlink/?linkid=21765>).

The improvements in features, functionality, and performance may affect decisions about which client your users should primarily use to access their Exchange information. In remote sites, Outlook Web Access may be the primary choice, which is a consideration when planning WAN connections and server placement.

Increased browser support

Table 1.1 shows the new level of browser support for the operating systems offered by Outlook Web Access for Exchange 2003.

Table 1.1 Browser support for Outlook Web Access for Microsoft operating systems

	Windows 98 Second Edition	Windows ME	Windows 2000	Windows XP	Windows Server 2003
Internet Explorer 5.1	B,P	None	B,P	None	None
Internet Explorer 5.5 SP2	B,P	B,P	B,P	None	None
Internet Explorer 6	B,P	B,P	B,P	B,P	None
Internet Explorer 6 SP1	B,P	B,P	B,P	B,P	B,P
MSN® version 8 and later	None	None	None	B,P	B,P
Netscape Navigator 4.8	B	B	B	B	B
Netscape Navigator 7	B	B	B	B	B

Table 1.2 shows the level of functionality for the operating systems and browsers for Outlook Web Access.

Key

- B - Basic version of Outlook Web Access supported
- B,P - Both the Basic and Premium versions of Outlook Web Access are supported
- None - Neither the Basic nor Premium versions of Outlook Web Access are supported

Table 1.2 Browser support for Outlook Web Access with other operating systems

	Apple OS 9.x	Apple OS 10.1 and later	Sun Microsystems Solaris HP/UX
Internet Explorer 5.0 and later for Apple	B	B	N/A
Internet Explorer 5.5 SP2	None	None	None
Internet Explorer 6	None	None	None

	Apple OS 9.x	Apple OS 10.1 and later	Sun Microsystems Solaris HP/UX
Internet Explorer 6 SP1	None	None	None
MSN version 8 and later	None	None	None
Netscape Navigator 4.8	B	B	B
Netscape Navigator 6.2	B	B	B
Netscape Navigator 7	B	B	B

Key

- B - Basic version of Outlook Web Access supported
- B,P - Both the Basic and Premium versions of Outlook Web Access are supported
- None - Neither the Basic nor Premium versions of Outlook Web Access are supported

Additionally, support for the following browsers and operating systems has been discontinued for Exchange 2003:

- Microsoft Internet Explorer 4.5
- Internet Explorer 5 on all versions of Microsoft Windows
- Internet Explorer 5 for UNIX 6.0
- Internet Explorer 4.57 for Apple OS 9 and later
- Microsoft Windows® 95
- Microsoft Windows® 98
- Microsoft Windows NT® 4.08
- Apple OS 8.17

For more information about the new features for Outlook Web Access, see *What's New in Exchange Server 2003* (<http://go.microsoft.com/fwlink/?linkid=21765>).

Mobile Services for Exchange

Exchange Server 2003 supports mobile access by using the synchronization and browse capabilities of mobile devices. You can deploy mobile services to enable your users to access their Exchange information from mobile devices such as the Microsoft Pocket PC 2002 Phone Edition device, or any mobile device with a mobile browser.

Exchange ActiveSync

Exchange 2003 now includes the ability to use Pocket PC 2002 devices to synchronize Exchange data with Exchange ActiveSync®. By default, when you install Exchange, all your users are enabled for synchronization.

By synchronizing a device to an Exchange server, your users can access their Exchange information without having to be always connected to a mobile network. Specifically, users can use their mobile carrier connection to synchronize their Exchange information to their Pocket PC Phone Edition or Smartphone device and then access this information while offline.

Outlook Mobile Access

Exchange 2003 now includes the Outlook Mobile Access application, which enables users to use mobile devices to access their e-mail, Contacts, Calendar, and Tasks folders. Outlook Mobile Access can be used with a mobile device that has a mobile browser. The mobile browser must support one of the following markup languages: HTML, xHTML, or cHTML. To deploy your Exchange server to use Outlook Mobile Access, follow the same steps involved in deploying an Exchange server to use Outlook Web Access.

Understanding Outlook Mobile Access Security Requirements

When you enable Outlook Mobile Access for your users, a security issue exists when using Mobile Operators that use Wireless Application Protocol (WAP) 1.x gateways. These gateways translate secure traffic from Internet protocols to wireless protocols. Because of this translation, a WAP 1.x gateway terminates an SSL session over TCP/IP, re-encrypts the data using Wireless Transport Layer Security (WTLS), and then sends the information over the wireless network using Wireless Session Protocol (WSP). During this translation at the WAP gateway, all data will be briefly unencrypted as it is decrypted from the SSL session and re-encrypted again as part of the WTLS session. This security issue affects your messaging infrastructure if your corporation is not hosting your own WAP gateway within the perimeter network.

Outlook Mobile Access for Exchange 2003 supports WAP 2.0 devices only. However, this does not rule out the possibility of certain devices being able to use a WAP 1.x gateway. Therefore, the security issue exists whenever a WAP 2.0 device, that can use a WAP 1.x gateway, uses a Mobile Operator with WAP 1.x gateways deployed.

To resolve this issue, you can purchase and install your own corporate WAP gateway. This solution requires you to situate a WAP gateway within your perimeter network and limit your mobile users to use this gateway alone.

Alternatively, you can choose to provide only WAP 2.0 devices that use only carriers that have WAP 2.0 gateways deployed. WAP 2.0 gateways allow SSL sessions to be passed through directly to WAP 2.0 devices that support SSL without decrypting and re-encrypting the session.

Planning Your Exchange Client Access Infrastructure

To plan your Exchange client access infrastructure, you must first identify the technical requirements for your Exchange messaging system. After you understand your technical requirements, you can perform a gap analysis and determine what changes must be made to your existing environment, including network infrastructure, hardware, and software upgrades. Additionally, you must understand the basic concepts behind the factors that you need to consider when planning your Exchange infrastructure. Some of these factors are:

- Security
- Topological boundaries and limitations
- Centralized vs. distributed messaging systems
- Routing design
- Server design and placement
- Server sizing and tuning
- User requirements

All these factors help you to design the client access infrastructure to meet your messaging requirements. For more information about designing and planning your messaging system, see *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>).

CHAPTER 2

Configuring Exchange Server 2003 for Client Access

This chapter provides information about configuring the Exchange Server 2003 features for client access. Before you deploy the client access features, take time to review the affect that these features will have on your messaging environment. Additionally, deploying client features for Exchange 2003 involves the following activities:

- Securing your Exchange messaging environment
- Deploying your server architecture
- Configuring the Exchange servers for your supported client access methods

Securing Your Exchange Messaging Environment

Follow these steps to secure your Exchange messaging environment:

1. Update your server software.
2. Secure the messaging environment.
3. Secure communications.

To secure your messaging system, complete these steps in the order given.

Updating Your Server Software

After you install Exchange 2003, you should update the server software on your Exchange servers and any other server that Exchange communicates with, such as global catalog servers and domain controllers. For more information about updating your software with the latest security updates, see the Microsoft Exchange Server Security Center Web site (<http://go.microsoft.com/fwlink/?linkid=18412>). For more information about Microsoft security, see the Microsoft Security Web site (<http://go.microsoft.com/fwlink/?linkid=21633>).

Securing the Exchange Messaging Environment

An alternative best practice to placing your front-end Exchange 2003 servers in the perimeter network is to deploy Microsoft Internet Security and Acceleration (ISA) Server 2000. ISA Server acts as advanced firewalls that control Internet traffic entering your network. When you use this configuration, you put all your Exchange 2003 servers in your corporate network and use ISA Server as the advanced firewall server exposed to Internet traffic in your perimeter network.

Securing the messaging environment also involves configuring the front-end servers in a manner that disables the features and settings for the front-end server that are not necessary in a front-end and back-end server architecture. For more information about how to configure a front-end server for the front-end and back-end server architecture, see the *Using Microsoft Exchange 2000 Front-end Servers* (<http://go.microsoft.com/fwlink/?linkid=12055>).

All inbound Internet traffic bound to your Exchange servers (such as Outlook Web Access, RPC over HTTP communication from Outlook 2003 clients, Outlook Mobile Access, Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4rev1 (IMAP4), and so on) is processed by the ISA Server. When ISA Server receives a request for an Exchange server, ISA Server proxies the requests to the appropriate Exchange servers on your internal network. The internal Exchange servers return the requested data to the ISA Server, and then ISA Server sends the information to the client through the Internet. Figure 2.1 shows an example of a recommended ISA Server deployment.

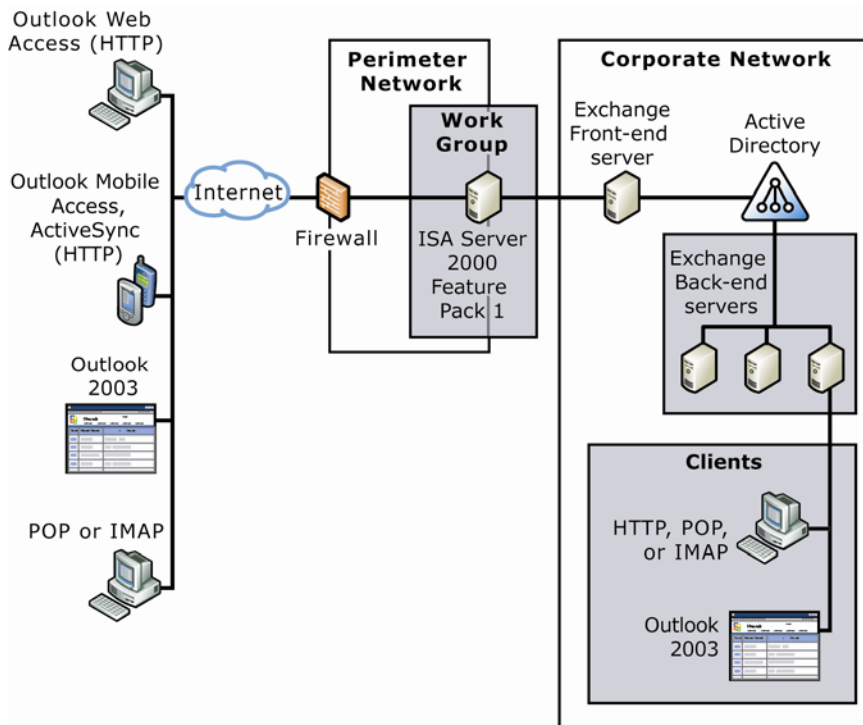


Figure 2.1 Deploying Exchange 2003 behind ISA Server

Securing Communications

To secure communications for your Exchange messaging environment, you need to do the following tasks:

- Secure the communications between the client messaging applications and the Exchange front-end server.
- Secure the communications between the Exchange front-end server and the internal network.

The following sections include information about securing communications for these two situations.

Securing Communications Between the Client and Exchange Front-End Server

To secure data transmitted between the client and the front-end server, it is highly recommended that you enable the front-end server to use Secure Sockets Layer (SSL). Additionally, to ensure that user data is always secure, you should configure the front-end server to require SSL (you can set this option in the SSL configuration). When using basic authentication, it is critical to protect the network traffic by using SSL to protect user passwords from network packet sniffing.

Warning If you do not use SSL between clients and the front-end server, HTTP data transmission to your front-end server will not be secure. It is highly recommended that you configure the front-end server to require SSL.

It is recommended that you obtain an SSL certificate by purchasing a certificate from a third-party certification authority (CA). Purchasing a certificate from a certification authority is the preferred method because most browsers trust many of these certification authorities.

As an alternative, you can use Certificate Services to install your own certification authorities. Although installing your own certification authority may be less expensive, browsers will not trust your certificate, and users will receive a warning message indicating that the certificate is not trusted. For more information about SSL, see Microsoft Knowledge Base article 320291, "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=320291>).

Using Secure Sockets Layer

To protect outbound and inbound mail, deploy SSL to encrypt messaging traffic. You can configure SSL security features on an Exchange server to verify the integrity of your content, verify the identity of users, and encrypt network transmissions. Exchange, like any Web server, requires a valid server certificate to establish SSL communications. You can use the Web Server Certificate Wizard to either generate a certificate request file (NewKeyRq.txt, by default) that you can send to a certification authority, or to generate a request for an online certification authority, such as Microsoft Certificate Services.

If you are not using Certificate Services to issue your own server certificates, a third-party certification authority must approve your request and issue your server certificate. For more information about server certificates, see "Obtaining and Installing Server Certificates" later in this chapter. Depending on the level of identification assurance offered by your server certificate, you can expect to wait several days to several months for the certification authority to approve your request and send you a certificate file. You can have only one server certificate for each Web site.

After you receive a server certificate file, use the Web Server Certificate Wizard to install it. The installation process attaches (or binds) your certificate to a Web site.

Important You must be a member of the Administrators group on the local computer to perform the following procedure, or you must have been delegated the appropriate authority. As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run Internet Information Services (IIS) Manager as an administrator. At the command prompt, type the following command:

```
runas /user:administrative_accountname
"mmc%systemroot%\system32\inetsrv\iis.msc"
```

To set up SSL on a server

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder. Right-click the Web site or file that you want to protect with SSL, and then click **Properties**.
2. Under **Web site identification**, click **Advanced**.
3. In the **Advanced Web site identification** box, under **Multiple identities for this Web site**, verify that the Web site IP address is assigned to port 443 (the default port for secure communications), and then click **OK**. Optionally, to configure more SSL ports for this Web site, click **Add** under **Multiple identities of this Web site**, and then click **OK**.
4. On the **Directory Security** tab, under **Secure communications**, click **Edit**.
5. In the **Secure Communications** box, select the **Require secure channel (SSL)** check box.

If you require 128-bit key encryption, your users must use Web browsers that support 128-bit encryption. For more information about upgrading to 128-bit encryption capability, see the Microsoft Product Support Services Web site (<http://go.microsoft.com/fwlink/?linkid=14898>).

Obtaining and Installing Server Certificates

You can obtain server certificates from an outside CA, or you can issue your own server certificates by using Microsoft Certificate Services. After you obtain a server certificate, you can install it. When you use the Web Server Certificate Wizard to obtain and install a server certificate, the process is referred to as creating and assigning a server certificate.

This section explains the issues to consider when deciding whether to obtain your server certificates from an outside CA or to issue your own server certificates. This section includes the following information:

- Obtaining server certificates from a CA
- Issuing your own server certificates
- Installing server certificates
- Backing up server certificates

Obtaining Server Certificates from a Certification Authority

If you are replacing your current server certificate, IIS continues to use that certificate until the new request has been completed. When you are selecting a CA, consider the following questions:

- Will the CA be able to issue a certificate that is compatible with all the browsers used to access my server?
- Is the CA a recognized and trusted organization?
- How will the CA provide verification of my identity?
- Does the CA have a system for receiving online certificate requests, such as requests generated by the Web Server Certificate Wizard?
- How much will the certificate cost initially, and how much will renewal or other services cost?
- Is the CA familiar with my organization or my company's business interests?

To obtain a server certificate from a certification authority

1. Use the Web Server Certificate Wizard to create a certificate request.
2. In the Web Server Certificate Wizard, on the **Delayed or Immediate Request** page, click **Prepare the request now, but send it later**.
3. Use the Web Server Certificate Wizard to send the request to the certification authority. The CA will process the request and then send you the certificate.
4. Finish using the Web Server Certificate Wizard.

Note Some certification authorities require that you prove your identity before they will process your request or issue a certificate.

Issuing Your Own Server Certificates

When deciding whether to issue your own server certificates, consider the following:

- Understand that Microsoft Certificate Services accommodates different certificate formats and provides for auditing and logging of certificate-related activity.
- Compare the cost of issuing your own certificates against the cost of buying a certificate from a certification authority.
- Remember that your organization will require an initial adjustment period to learn, implement, and integrate Certificate Services with existing security systems and policies.
- Assess the willingness of your connecting clients to trust your organization as a certificate supplier.

Use Certificate Services to create a customizable service for issuing and managing certificates. You can create server certificates for the Internet or for corporate intranets, which gives your organization complete control over certificate management policies. For more information about using Certificate Services, see "Certificate Services" in Microsoft Windows Server 2003 Help.

Online requests for server certificates can be made only to local and remote Enterprise Certificate Services and remote stand-alone Certificate Services. The Web Server Certificate Wizard does not recognize a stand-alone

installation of Certificate Services on the same computer when requesting a certificate. If you need to use Web Server Certificate Wizard on the same computer as a stand-alone Certificate Services installation, use the offline certificate request to save the request to a file and then process it as an offline request. For more information about using Certificate Services, see "Certificate Services" in Microsoft Windows Server 2003 Help.

Note If you open a Server Gated Cryptography (SGC) certificate, you may receive the following notice on the **General** tab:

The certificate has failed to verify for all its intended purposes.

This notice is issued because of how SGC certificates interact with Windows and does not necessarily indicate that the certificate does not work correctly.

Installing Server Certificates

After you obtain a server certificate from a CA, or after you issue your own server certificate by using Certificate Services, use the Web Server Certificate Wizard to install it.

Backing Up Server Certificates

You can use the Web Server Certificate Wizard to back up server certificates. Because IIS works closely with Windows, you can use Certificate Manager, which is called **Certificates** in Microsoft Management Console (MMC), to export and back up your server certificates.

Note If you do not have Certificate Manager installed in MMC, use the **To add Certificate Manager to the MMC** procedure that follows to add Certificate Manager to the MMC.

To add Certificate Manager to the MMC

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **mmc**, and then click **OK**.
3. In the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** box, click **Add**.
5. In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**.
6. Click **Computer Account**, and then click **Next**.
7. Click the **Local computer** (the computer this console is running on) option, and then click **Finish**.
8. Click **Close**, and then click **OK**.

After you install Certificate Manager, you can back up your certificate.

To back up your server certificate

1. Locate the correct certificate store. This store is typically the **Local Computer** store in Certificate Manager.

Note When you have Certificate Manager installed, it points to the correct **Local Computer** certificate store.
2. In the **Personal** store, click the certificate that you want to back up.
3. On the **Action** menu, point to **All tasks**, and then click **Export**.
4. In the Certificate Manager Export Wizard, click **Yes, export the private key**.
5. Follow the wizard default settings, and enter a password for the certificate backup file when prompted.

Note Do not select **Delete the private key if export is successful** because this option disables your current server certificate.
6. Complete the wizard to export a backup copy of your server certificate.

After you configure your network to issue server certificates, you need to secure your Exchange front-end server and the services for your Exchange server by requiring SSL communication to the Exchange front-end server. The following section describes how to enable SSL for your default Web site.

Enabling SSL for the Default Web Site

After you obtain an SSL certificate to use either with your Exchange front-end server on the default Web site or on the site where you host the \RPC, \OMA, \Microsoft-Server-ActiveSync, \Exchange, \Exchweb, and \Public virtual directories, you can the default Web site to require SSL.

Note The \Exchange, \Exchweb, \Public, \OMA, and \Microsoft-Server-ActiveSync virtual directories are installed by default on any Exchange 2003 installation. The \RPC virtual directory for RPC over HTTP communication is installed manually when you configure Exchange to support RPC over HTTP. For more information about how to set up Exchange to use RPC over HTTP, see "Configuring RPC over HTTP for Outlook 2003" later in this chapter.

To configure virtual directories to use SSL

1. In **Internet Information Services (IIS)**, select the **Default Web site** or the Web site where you are hosting your Exchange services, and then click **Properties**.
2. On the **Directory Security** tab, in **Secure Communications**, click **Edit**.
3. In **Secure Communications**, click the **Require Secure Channel (SSL)** check box.
4. After you complete this procedure, all virtual directories on the Exchange front-end server on the default Web site are configured to use SSL.

Securing Communications Between Exchange Front-End Server and Other Servers

After you secure your communications between the client computers and the Exchange servers, you must secure the communications between the Exchange server and other servers in your organization. HTTP, POP, and IMAP communications between the front-end server and any server with which the front-end server communicates (such as back-end servers, domain controllers, and global catalog servers) is not encrypted. When the front-end and back-end servers are in a trusted physical or switched network, this lack of encryption is not an issue. However, if front-end and back-end servers are kept in separate subnets, network traffic may pass over nonsecure areas of the network. The security risk increases when there is greater physical distance between the front-end and back-end servers. In this case, it is recommended that this traffic be encrypted to protect passwords and data.

Using IPSec to Encrypt IP Traffic

Windows 2000 supports Internet Protocol security (IPSec), which is an Internet standard that allows a server to encrypt any IP traffic, except traffic that uses broadcast or multicast IP addresses. Generally, you use IPSec to encrypt HTTP traffic; however, you can also use IPSec to encrypt Lightweight Directory Access Protocol (LDAP), RPC, POP, and IMAP traffic. With IPSec you can:

- Configure two servers running Windows 2000 to require trusted network access.
- Transfer data that is protected from modification (using a cryptographic checksum on every packet).
- Encrypt any traffic between the two servers at the IP layer.

In a front-end and back-end topology, you can use IPSec to encrypt traffic between the front-end and back-end servers that would otherwise not be encrypted. For more information about configuring IPSec with firewalls, see Microsoft Knowledge Base article 233256, "How to Enable IPSec Traffic Through a Firewall" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=233256>).

Deploying the Exchange Server Architecture

After you secure your Exchange messaging environment, you can deploy the Exchange front-end and back-end server architecture. For more information about the Exchange front-end and back-end server architecture, see "Protocols" in the book *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>).

To configure the Exchange front-end and back-end server architecture, you need to configure one Exchange server as a front-end server. Make sure you review your deployment options before you continue with the installation process. The following section helps you decide if you want to deploy Exchange 2003 in a front-end and back-end server configuration.

A front-end and back-end configuration is recommended for multiple-server organizations that use Outlook Web Access, POP, or IMAP and for organizations that want to provide HTTP, POP, or IMAP access to their employees.

Configuring a Front-End Server

A front-end server is an ordinary Exchange server until it is configured as a front-end server. A front-end server must not host any users or public folders and must be a member of the same Exchange 2003 organization as the back-end servers (therefore, a member of the same Windows 2000 Server or Windows Server 2003 forest). Servers that are running either Exchange Server 2003 Enterprise Edition or Exchange Server 2003 Standard Edition can be configured as front-end servers.

To designate a front-end server

1. Start Exchange System Manager.
2. In the console tree, expand **Servers**, right-click the server you want to designate as a front-end server, and then click **Properties**.
3. In **Server Name Properties**, on the **General** tab, select the **This is a front-end server** check box.
4. Click **Apply**, and then click **OK**.

To begin using your server as a front-end server, restart the server. For more information about front-end and back-end scenarios, configurations, and installation, see the following books:

- *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>)
- *Using Microsoft Exchange 2000 Front-End Servers* (<http://go.microsoft.com/fwlink/?linkid=12055>)

Configuring Exchange for Client Access

Configuring Exchange for client access involves configuring Exchange to handle the protocols and clients that you want to support. The following section describes how to enable the client protocols supported by Exchange on the Exchange server. This section includes the following sections:

- Configuring Outlook 2003 Features
- Configuring Mobile Device Support
- Configuring Outlook Web Access
- Enabling POP3 and IMAP4 Virtual Servers

Configuring Outlook 2003 Features

Outlook 2003 enables you to use the Windows RPC over HTTP feature to provide remote access to Exchange for your users. Combined with Cached Exchange Mode, which enables your users to use a copy of their Exchange mailbox on their local computer, your users will be able to access Exchange from environments in which network connectivity is slow, inconsistent, or non-existent. The following sections describe how to configure Exchange to take advantage of these features.

Configuring RPC over HTTP for Outlook 2003

Deploying RPC over HTTP to support your Outlook 2003 clients for remote access to Exchange requires that you carefully follow the steps necessary to deploy this feature. For more information about how to deploy this feature and configure your users with Outlook 2003, see the technical article *Exchange Server 2003 RPC over HTTP Deployment Scenarios* (<http://go.microsoft.com/fwlink/?linkid=24823>).

Configuring Mobile Device Support

Perform the following activities to configure mobile device support for Exchange 2003:

- Configure synchronization.
- Configure Exchange ActiveSync to use RSA SecurID.
- Enable Outlook Mobile Access.

Configuring Synchronization

When you install Exchange, synchronization access to Exchange is enabled by default for all users in your organization. You can also use the Active Directory Users and Computers snap-in to enable individual users for synchronization access.

Configuring Exchange ActiveSync

The following procedure explains how to configure Exchange ActiveSync in your organization.

To configure your Exchange 2003 organization for Exchange ActiveSync

1. Start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. Under **Exchange ActiveSync**, select from the following check boxes:
 - Select the **Enable user initiated synchronization** check box to allow users to use Pocket PC 2002 devices to synchronize their Exchange data.
 - Select the **Enable up-to-date notifications** check box to enable users to receive notifications that are sent from the Exchange server to devices that allow notifications.
 - Select the **Enable notifications to user specified SMTP addresses** check box to enable users to use their own SMTP carrier for notifications.

Note With this feature enabled, when a new message arrives in a user's mailbox, up-to-date notifications allows synchronization to occur on a user's device. Enable this feature if you have users who are using mobile devices to synchronize, and you do not want to specify the carrier.

4. Click **Apply**, and then click **OK**.

The following procedure explains how to configure a mobile device such as a Pocket PC Phone Edition device to use Exchange ActiveSync. Perform this procedure on each mobile device in your organization. As an alternative, you can instruct your users how to configure their own devices.

To configure Pocket PC Phone Edition devices to use Exchange ActiveSync

1. On the mobile device, from the **Today** screen, tap **Start**, and then tap **ActiveSync**.
2. Tap **Tools**, tap **Options**, and then tap the **Server** tab.
3. Select the check box next to each type of information that you want to synchronize with the server.
4. To configure synchronization options for each type of information, select the type of information, and then tap **Settings**.
5. In the **Server Name** field, enter the address or name of the server to connect to when synchronizing Exchange data.
6. Tap **Advanced**.
7. On the **Connection** tab, enter the user name, password, and domain name.
8. On the **Rules** tab, select the rule that best applies to you, for how you want synchronization to work whenever information about your device and your Exchange server have both been changed.
9. Tap **OK** to accept the changes you made to ActiveSync.
10. Repeat this procedure for each of your users' Pocket PC Phone Edition devices. As an alternative, instruct your users about how to configure their devices for use with Exchange ActiveSync.

Configuring Exchange ActiveSync to Use RSA SecurID

As an added level of security, you can use Microsoft Windows Mobile devices with Exchange ActiveSync with RSA SecurID two-factor authentication.

Note No additional device configuration is required to support RSA SecurID. The device presents the appropriate authentication automatically when synchronizing with an Exchange ActiveSync server protected by RSA SecurID.

Follow these steps to use RSA SecurID with Exchange ActiveSync:

1. Set up the RSA SecurID server components.
2. Configure IIS to use RSA SecurID.
3. Set up user accounts.

Setting Up the RSA SecurID Server Components

To configure the RSA SecurID server components, you need to:

- **Set up the RSA ACE/Server** The RSA ACE/Server is the RSA server that stores and manages authentication tickets and credentials for your users. To set up the RSA ACE/Server, follow the procedures as outlined in the RSA SecurID documentation provided by RSA Security Inc.
- **Set up the RSA ACE/Agent on the front-end server** The RSA ACE/Agent is the Internet Server Application Programming Interface (ISAPI) filter that performs authentication and communicates to the ACE/Server to retrieve SecurID credentials. To set up the RSA ACE/Agent, follow the procedures as outlined in the RSA documentation provided by RSA Security Inc.

Configuring IIS to Use RSA SecurID

Perform the following procedures to configure IIS for RSA and Exchange ActiveSync:

1. Protect the Exchange ActiveSync virtual directories.
2. Customizing the HTTP response headers for devices.
3. Install SecurID screens (optional). For information about installing these screens, see the RSA SecurID documentation provided by RSA Security Inc.

The following sections provide more information about completing these steps to correctly configure IIS for SecurID and Exchange ActiveSync operations.

Protecting the Exchange ActiveSync Virtual Directories

The first step to configure IIS is to protect the virtual directories that your users access when they use Exchange ActiveSync. Exchange Server 2003 uses the \Microsoft-Server-ActiveSync virtual directory.

You can protect this virtual directory in one of the following two ways:

- **Protect the entire Web server (recommended)** In this option, you protect all virtual roots on the IIS server with RSA ACE/Agent, including any other services implemented by the front-end server. For example, you may have configured your front-end Exchange server as an access point for Outlook Mobile Access or for Outlook Web Access.
- **Protect only the Exchange ActiveSync virtual directories** In this option, you configure the RSA ACE/Agent so that SecurID protects only Exchange ActiveSync. Use this option if you intend to enable additional services, such as Outlook Web Access and Outlook Mobile Access, on the same server without protecting those services with SecurID.

By default, the ACE/Agent is configured to protect the entire Web server. You can use the following procedure to verify this configuration.

To verify ACE/Agent is configured to protect the entire Web server

1. In the Internet Information Services snap-in for MMC, right-click the default Web server and select **Properties**.
2. Click the **RSA SecurID** tab, and verify that the **Protect This Resource** check box is selected.

Use the following procedure to configure the front-end server so that RSA SecurID authentication is limited to Exchange ActiveSync.

To limit SecurID authentication to the Microsoft-Exchange-ActiveSync virtual directory

1. To disable server-wide protection, in the IIS snap-in, right-click the default Web server, and then click **Properties**.
2. Click the **RSA SecurID** tab, and then clear the **Protect This Resource** check box. (This step ensures that RSA SecurID is not enabled for the entire server, but rather only for the virtual roots that you specify.)
3. To enable protection for the virtual directories, in the IIS snap-in, right-click the **Microsoft-Server-ActiveSync** virtual directory, and then click **Properties**.
4. Select the **RSA SecurID** tab, and then select the **Protect This Resource** check box.

Note If the check box is selected and shaded, this means that the virtual directory is inheriting its setting from the parent directory. Inspect the properties for the parent directory, and clear the **Protect This Resource** check box if you do not want the parent directory to be protected. Then, return to the child directory and make sure the check box is selected.

Customizing the HTTP Response Headers for Devices

The ActiveSync client on the Microsoft Windows Mobile device must be able to distinguish between RSA SecurID authentication and Exchange ActiveSync responses. To enable this capability, you need to configure custom HTTP response headers on the WebID virtual root that contains the HTML forms configured by RSA ACE/Agent.

To configure custom HTTP responses for devices

1. In the IIS snap-in for MMC, locate the WebID virtual directory on the front-end server. This virtual directory is created by SecurID and contains the SecurID authentication forms and responses.
2. Right-click the WebID virtual directory, and then click **Properties** to open the properties for this virtual directory.

- Click the **HTTP Headers** tab, click the **Add** button, and then enter the following header information.

Note The following value is case sensitive and must be entered on one line.

```
Custom Header Name: MSAS-TwoFactorAuth Custom Header Value: True Custom Header Name:
MS-ASProtocolVersions Custom Header Value: 1.0,2.0 Custom Header Name: MS-
ASProtocolCommands Custom Header Value:
Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,CreateCollection,Delet
eCollection,MoveCollection,FolderSync,FolderCreate,FolderDelete,FolderUpdate,MoveItems,
GetItemEstimate,MeetingResponse
```

Setting Up User Accounts

User accounts for SecurID should be set up by the administrator as recommended by the RSA SecurID product documentation, with the following restriction:

- For all users, SecurID user IDs must be selected to match the Windows account name. Exchange ActiveSync with SecurID does not function for users who have a distinct RSA user ID that does not match their Windows account name.

Configuring Outlook Mobile Access

By default, all users are enabled for Exchange ActiveSync and Outlook Mobile Access. However, only Exchange ActiveSync is enabled on the Exchange server; by default, Outlook Mobile Access is disabled. This section describes how to enable Outlook Mobile Access on your Exchange server.

Follow these steps to enable your Exchange 2003 users to use Outlook Mobile Access.

- Configure your Exchange 2003 front-end server for Outlook Mobile Access.
- Enable Outlook Mobile Access on the Exchange server.
- Configure user devices to use a mobile connection.
- Instruct your users about how to use Outlook Mobile Access.

Configuring Your Exchange 2003 Front-End Server for Outlook Mobile Access

By default, the Outlook Mobile Access virtual directory (which allows your users to access Exchange from a mobile device) is installed with Exchange 2003. This virtual directory has the same configuration settings as the Outlook Web Access virtual directory. When you configure a server to use Outlook Mobile Access, you should configure the server in the same way you configure a server for Outlook Web Access. For more information about how to configure your Exchange 2003 servers to use Outlook Web Access, see *Using Microsoft Exchange 2000 Front-End Servers* (<http://go.microsoft.com/fwlink/?linkid=12055>).

Enabling Outlook Mobile Access on the Exchange Server

After you configure your front-end server to use Outlook Mobile Access, you need to enable Outlook Mobile Access on your Exchange servers.

To enable Outlook Mobile Access for your organization

- Log on as an Exchange administrator to the Exchange server where the user's mailbox is located, and start Exchange System Manager.
- Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
- On the **Mobile Services** properties page, in **Outlook Mobile Access**, select **Enable Outlook Mobile Access**.

4. To enable users to use unsupported devices, select the **Enable unsupported devices** check box.

Note For more information about supported devices for Exchange and planning for mobile device support with Exchange, see *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>).

5. Click **OK**.

After you enable Outlook Mobile Access, you can modify the Outlook Mobile Access settings for users or groups of users by using the Active Directory Users and Computers snap-in.

Configuring Users' Devices to Use a Mobile Connection

To access Exchange 2003 using Outlook Mobile Access, users must have a mobile device from a mobile operator who has an established data network for mobile data. Before your users connect to Exchange 2003 and use Outlook Mobile Access or Exchange ActiveSync over a mobile connection, instruct them about how to configure their devices to use a mobile network, or provide them with resources that explain how to do so. For more information about configuring mobile devices and Exchange ActiveSync, see "To configure Pocket PC Phone Edition devices to use Exchange ActiveSync" earlier in this chapter.

Instructing Your Users About How to Use Outlook Mobile Access

After you configure Exchange 2003 for Outlook Mobile Access, and your users have mobile devices that can use a mobile network to access Exchange 2003 servers, they need to know how to access their Exchange server and use Outlook Mobile Access. The following procedure describes how to use Outlook Mobile Access on a Pocket PC Phone Edition device.

To configure a Pocket PC Phone Edition device to use Outlook Mobile Access

1. On the device, from the **Today** screen, tap **Start**, and then tap **Internet Explorer**.
2. On the **Internet Explorer** screen, tap **View**, and then tap **Address Bar** to open the address bar in your browser window.
3. Tap anywhere inside the address bar, enter the following URL, and then tap the **Go** button:
`https://ExchangeServerName/oma`, where *ExchangeServerName* is the name of your Exchange server running Outlook Mobile Access.

Note If a connection bubble does not appear, you may have to connect to your network manually.
4. At the **Network Log On** screen, enter the user name, password, and domain in the spaces provided, and then tap **OK**.
5. Repeat this procedure for each of your users' Pocket PC Phone Edition devices. As an alternative, instruct your users about how to configure their devices for use with Exchange ActiveSync.

Configuring Outlook Web Access

By default, Outlook Web Access is enabled for all your users after you install Exchange 2003. However, you can enable the following features for Outlook Web Access:

- Set up a logon page.
- Configure authentication.
- Configure security options.
- Configure Outlook Web Access compression.
- Simplify the Outlook Web Access URL.

Setting Up a Logon Page

You can enable a new logon page for Outlook Web Access that stores the user's name and password in a cookie instead of in the browser. When a user closes a browser, the cookie is cleared. Additionally, after a period of inactivity, the cookie is cleared automatically. The new logon page requires the user to enter a domain, user name, and password, or a full user principal name (UPN) e-mail address and password, to access e-mail.

To enable this logon page, you must first enable forms-based authentication on the server, and then secure the logon page by setting the cookie time-out period and adjusting client-side security settings.

Enabling Forms-Based Authentication

To enable the Outlook Web Access logon page, you must enable forms-based authentication on the server.

To enable forms-based authentication

1. On the Exchange server, log on with the Exchange administrator account, and then start Exchange System Manager.
2. In the console tree, expand **Servers**.
3. Expand the server for which you want to enable forms-based authentication, and then expand **Protocols**.
4. Expand **HTTP**, right-click **Exchange Virtual Server**, and then click **Properties**.
5. In the **Exchange Virtual Server Properties** dialog box, on the **Settings** tab, in the Outlook Web Access pane, select the **Enable Forms Based Authentication** option.
6. Click **Apply**, and then click **OK**.

Setting the Cookie Authentication Time-Out

In Exchange 2003, Outlook Web Access user credentials are stored in a cookie. When the user logs off Outlook Web Access, the cookie is cleared and it is no longer valid for authentication. Additionally, by default, if your user is using a public computer, and selects the **Public or shared computer** option on the Outlook Web Access logon screen, the cookie on this computer expires automatically after 15 minutes of user inactivity.

The automatic time-out is valuable because it helps protect a user's account from unauthorized access. However, although the automatic time-out greatly reduces the risk of unauthorized access, it does not completely eliminate the possibility that an unauthorized user might access an Outlook Web Access account if a session is left running on a public computer. Therefore, make sure that you educate users about precautions to take to avoid risks.

To match the security requirements of your organization, an administrator can configure the inactivity time-out values on the Exchange front-end server. To configure the time-out value, you must modify the registry settings on the server.

Warning Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To set the Outlook Web Access forms-based authentication public computer cookie time-out value

1. On the Exchange front-end server, log on with the Exchange administrator account, and then start Registry Editor (**regedit**).
2. In Registry Editor, locate the following registry key:


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
```
3. On the Edit menu, point to **New**, and then click **DWORD Value**.
4. In the details pane, name the new value **PublicClientTimeout**.

5. Right-click the **PublicClientTimeout** DWORD value, and then click **Modify**.
6. In **Edit DWORD Value**, under **Base**, click **Decimal**.
7. In the **Value Data** box, type a value (in minutes) between 1 and 432,000.
8. Click **OK**.

Configuring Client Security Options for Users

The Outlook Web Access logon page enables the user to select the security option that best fits their requirements. The **Public or shared computer** option (selected by default) provides a short default time-out option of 15 minutes. Users should select the **Private computer** option only if the user is the sole operator of the computer, and the computer adheres to that user's organizational security policies. When selected, the **Private computer** option allows for a much longer period of inactivity before automatically ending the session—its internal default value is 24 hours. Essentially, this option is intended to benefit Outlook Web Access users who are using personal computers in their office or home.

To match the security requirements of your organization, an administrator can configure the inactivity time-out values.

Note The default value for the public computer cookie time-out is fifteen minutes. To change this, you must modify the registry settings on the server.

Warning Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To set the Outlook Web Access forms based authentication public cookie time-out value

1. Start Registry Editor (**regedit**).
2. Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\  
Services\MSExchangeWeb\OWA
```
3. On the Edit menu, point to **New**, and then click **DWORD Value**.
4. In the details pane, name the new value **PublicClientTimeout**.
5. Right-click the **PublicClientTimeout** Dword value, and then click **Modify**.
6. In **Edit DWORD Value**, under **Base**, click **Decimal**.
7. In the **Value Data** box, type a value (in minutes) between 1 and 432,000.
8. Click **OK**.

To set the Outlook Web Access forms-based authentication trusted client cookie time-out value

1. Start Registry Editor (**regedit**).
2. Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\  
Services\MSExchangeWeb\OWA
```
3. On the Edit menu, point to **New**, and then click **DWORD Value**.
4. In the details pane, name the new value **TrustedClientTimeout**.
5. Right-click the **TrustedClientTimeout** Dword value, and then click **Modify**.
6. In **Edit DWORD Value**, under **Base**, click **Decimal**.
7. In the **Value Data** box, type a value (in minutes) between 1 and 432,000.
8. Click **OK**.

Outlook Web Access Compression

Outlook Web Access supports data compression, which is optimal for slow network connections. Depending on the compression setting you use, Outlook Web Access compresses static Web pages, dynamic Web pages, or both. Table 2.1 lists the compression settings that are available in Exchange Server 2003 for Outlook Web Access.

Table 2.1 Compression settings for Outlook Web Access

Compression setting	Description
High	Compresses both static and dynamic pages.
Low	Compresses only static pages.
None	No compression is used.

Requirements for Outlook Web Access Compression

To use data compression for Outlook Web Access in Exchange Server 2003, verify that your organization meets the following prerequisites:

- The Exchange server that users authenticate against for Outlook Web Access must be running Windows Server 2003.
- Your users' mailboxes must be on Exchange 2003 servers. (If you have a mixed deployment of Exchange mailboxes, you can create a separate virtual server on your Exchange server just for Exchange 2003 users and enable compression on it.)
- Client computers must be running Internet Explorer version 6 or later. The client computers must also be running Windows XP or Windows 2000 and have installed on them the security update that is discussed in Microsoft Security Bulletin MS02-066, "Cumulative Patch for Internet Explorer (328970)" (<http://go.microsoft.com/fwlink/?LinkId=16694>).

Note If a user does not have a supported browser for compression, the client computer still operates normally.

- You may need to enable HTTP 1.1 support through proxy servers for some dial-up connections. (HTTP 1.1 support is required for compression to function correctly.)

To enable Outlook Web Access data compression

1. Start Exchange System Manager.
2. In the details pane, expand **Servers**, expand the server you want, and then expand **Protocols**.
3. Expand **HTTP**, right-click **Exchange Virtual Server**, and then click **Properties**.
4. In **Exchange Virtual Server Properties**, on the **Settings** tab, under **Outlook Web Access**, use the **Compression** list to select the compression level you want (**None**, **Low**, or **High**).
5. Click **Apply**, and then click **OK**.

Simplifying the Outlook Web Access URL

The HTTP virtual server that is created by Exchange during installation has the following URLs for user access:

- **http://server_name/public** This URL provides access to public folders.
- **http://server_name/exchange/mailbox_name** This URL provides access to mailboxes.

However, users frequently request that a URL that is simpler than the default URL be made available for accessing their mailboxes. Creating this simple URL makes the URL both easier to remember and easier to

enter in a Web browser. For example, <http://www.contoso1.com> is an easier URL for users to remember than <http://contosoexchange01/exchange>.

The following procedure provides a method for simplifying the URL that is used to access Outlook Web Access. This procedure configures a request sent to the root directory of the Web server (http://server_name/) to redirect to the Exchange virtual directory. For example, a request to http://server_name/ is directed to http://server_name/exchange/, which then triggers implicit logon.

To simplify the Outlook Web Access URL

1. Using Internet Services Manager, open the properties for the default Web site.
2. Click the **Home Directory** tab, and then select **A redirection to a URL**.
3. In **Redirect to**, type */directory name*, and then click **A directory below URL entered**.
For example, to redirect <http://mail/> requests to <http://mail/exchange>, in **Redirect to**, you would type */exchange*.
4. To require users to use Secure Sockets Layer (SSL), in **Redirect to**, type <https://mail/directory name>, and then click **The exact URL above** option.
This setting hard codes the name of the server. Therefore, if you redirect client requests to <https://mail/>, the client must be able to resolve the name "mail."

For more information about another method for redirecting clients to SSL, see Microsoft Knowledge Base article 279681, "How to Force SSL Encryption for an Outlook Web Access 2000 Client" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=279681>).

Configuring POP3 and IMAP4 Virtual Servers

By default, the POP3 and IMAP4 virtual servers are disabled on a new installation of Exchange Server 2003. To enable the POP3 and IMAP4 virtual servers, you must first use the Services snap-in to MMC and set the services to start automatically. If you set the services to start automatically and then need to start, pause, or stop the services, use Exchange System Manager.

To start, pause, or stop the virtual server

1. In Exchange System Manager, right-click the IMAP4 or POP3 virtual server.
2. Select one of the following options:
 - **Start** Starts the virtual server.
 - **Pause** Changes the server status to paused, and an icon appears next to the server name in the console tree. To restart the server, select **Pause** again.
 - **Stop** Changes the server status to stopped, and an icon appears next to the server name in the console tree.

CHAPTER 3

Managing Client Access to Exchange Server 2003

This chapter describes how to manage the client access settings for the protocols and clients that you support. This chapter also reviews basic client access concepts, and how you manage the protocols that are used by the individual clients that access Microsoft® Exchange Server 2003 and the front-end and back-end server architecture.

Note To correctly manage client access to Exchange 2003, you must first understand how Microsoft Windows® technologies, such as Internet Information Services (IIS) and Microsoft Active Directory® directory service, interact with Exchange. You must also understand protocols such as HTTP and MAPI, and how client applications such as Exchange ActiveSync® and Microsoft Office Outlook® 2003 use these respective protocols to interact with Exchange.

Managing Protocols

In your Exchange messaging deployment configuration, you use Exchange System Manager to manage the protocols that you support. When you use Exchange System Manager to manage protocols, you handle settings on the individual virtual servers for the protocol that is to be configured. The virtual servers that are associated with the various protocols, such as the Exchange Virtual Server and the Internet Message Access Protocol version 4rev1 (IMAP4) virtual server, contain settings based on the capabilities and use of the specific protocol. For example, the Exchange Virtual Server, which manages HTTP access to Exchange, provides settings for Microsoft Office Outlook 2003 Web Access, such as gzip compression support.

Generally, managing the virtual server for one protocol is the same as managing a virtual server for a different protocol. The common management tasks include enabling a virtual server, assigning ports, setting connection limits, starting or stopping a virtual server, and disconnecting users. However, there are some server-specific management tasks. The following sections describe the common tasks for all virtual servers associated with protocols and the server-specific tasks for the Exchange Virtual Server, IMAP4 virtual server, and the Network News Transfer Protocol (NNTP) virtual server.

Note To manage individual Exchange client access settings, use Active Directory Users and Computers.

Enabling a Virtual Server

When you install Exchange, the services that are necessary to support clients such as Outlook 2003, Outlook Web Access, and Exchange ActiveSync are enabled by default. For example, Exchange enables the SMTP service because it is the underlying protocol used to route messages internally within an Exchange organization and externally to messaging systems outside an Exchange organization. Similarly, Exchange enables HTTP because it is the underlying protocol for all Internet communication.

Note Although Outlook Mobile Access uses the HTTP protocol, Outlook Mobile Access is disabled by default and must be enabled by using Exchange System Manager.

However, Exchange installs, but does not enable services for Post Office Protocol version 3 (POP3), IMAP4, and NNTP. If your client access model relies on communications that use POP3, IMAP4, or NNTP, you must manually enable them.

To enable either the POP3 or IMAP4 service, you use the Services snap-in to set the service to start automatically. Then, you start the service by using Exchange System Manager. To enable NNTP, use the Services snap-in to set the NNTP service to start automatically, and then use Exchange System Manager to start the service.

To enable a POP3 or IMAP4 virtual server to start automatically

1. In the **Services** snap-in, in the console tree, click **Services (Local)**.
2. In the details pane, right-click **Microsoft Exchange POP3** or **Microsoft Exchange IMAP4**, and then click **Properties**.
3. On the **General** tab, under **Startup type**, select **Automatic**, and then click **Apply**.
4. Under **Service status**, click **Start**, and then click **OK**.
5. Repeat this procedure on all nodes that will be running the POP3 or IMAP4 virtual server.

To enable an NNTP virtual server

1. In the **Services** snap-in, in the console tree, click **Services (Local)**.
2. In the details pane, right-click **Network News Transfer Protocol (NNTP)**, and then click **Properties**.
3. On the **General** tab in **Startup type**, select **Automatic**, and then click **OK**.

To start a POP3, IMAP4, or NNTP virtual server

1. In Exchange System Manager, expand **Protocols**, expand the appropriate protocol (**POP3**, **IMAP4**, or **NNTP**), right-click the appropriate default virtual server (**Default POP3 Virtual Server** and **Default NNTP Virtual Server**), and then click **Start**.

Assigning Ports and an IP Address to a Virtual Server

When you create a virtual server for a protocol, you have the option of using the default port assignments and Internet Protocol (IP) address for the server. Table 3.1 shows the default port assignments associated with the protocols. The default IP address is (**All Unassigned**), which means that a specific IP address has not been assigned and the virtual server will use the IP address of the Exchange server that is currently hosting the virtual server. These default values provide a virtual server with automatic discovery—the server can immediately receive incoming connections by using the default IP address and ports.

Table 3.1 Default port assignments

Protocols	TCP port	Secure Sockets Layer (SSL) port
SMTP	25	Not available
IMAP4	143	993
POP3	110	995
NNTP	119	563

Important If you do not use the recommended port assignments, some clients may be not able to connect. You may also have to reconfigure your client software manually to connect to the new port assignments.

Note To fully enable SSL on the POP3 virtual server, you must request and install a certificate. You must do this even if you leave the default SSL port set at 995 on the POP3 virtual server. For more information about installing certificates, see "Securing Communications" and "Configuring Exchange Server 2003 for Client Access" in the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

Although it is highly recommended that you use the default port assignments, you do not have to use the default IP address. You can use the IP address from any available network card as the IP address for the virtual server.

If you plan to create multiple virtual servers, each virtual server must have a unique combination of ports and IP address. Because the port settings are standard and should not be changed, you will need to provide each virtual server with a unique IP address.

Besides creating a unique combination of ports and IP address for each virtual server, you can also configure multiple identities for your virtual server. Multiple identities enable you to associate multiple host or domain names with a single virtual server.

Use the following procedure to either assign a unique IP address to a virtual server or to assign multiple identities to a virtual server.

To assign an IP address or an identity to a virtual server

1. Log on the Exchange server where the virtual server is running using the Exchange administrator account that has local Administrator permissions and Exchange Full Administrator permissions.
2. In Exchange System Manager, expand **Protocols**, right-click the protocol that is to be assigned a new IP address or to which you want to add a new identity, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. In the **Advanced** dialog box, click **Edit** to change the IP address to a unique value, or click **Add** to add a new identity (that is, a new IP address and port combination).

Setting Connection Limits

A virtual server can accept an unlimited number of inbound connections and is limited only by the resources of the computer where the virtual server is running. To prevent a computer from becoming overloaded, you can limit the number of connections that can be made to the virtual server at the same time. By default, Exchange does not limit the number of incoming connections.

After users are connected, you can also limit the length of time that idle connections remain logged on to the server. By default, Exchange disconnects idle sessions after 10 minutes.

In topologies that contain Exchange front-end and back-end servers, the connection time-out setting varies based on server role. On back-end servers, the connection time-out setting limits the length of time clients can be connected to the server without performing any activity. However, on front-end servers, the connection time-out setting limits the total length of the client session, regardless of client activity. Therefore, in front-end and back-end server environments, you should configure the time-out value on your front-end servers high enough so that users can download the maximum message size that is permitted over the slowest connection speed that you want to support. Setting this value high enough ensures that clients are not disconnected while they are downloading messages. For more information about configuring your Exchange front-end and back-end server architecture, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

Warning Setting the connection time-out setting too low can cause clients to be unexpectedly disconnected from the server and possibly receive error messages. Thirty minutes is the lowest recommended connection time-out setting.

To set connection limits

1. Log on to the Exchange server where the virtual server is running using the Exchange administrator account that has local Administrator permissions and Exchange Full Administrator permissions.
2. In Exchange System Manager, expand **Protocols**, right-click the protocol for which you want to change connection limits, and then click **Properties**.
3. On the **General** tab, set the appropriate connection limits.

Starting, Pausing, or Stopping a Virtual Server

Managing virtual servers frequently requires you to start, pause, or stop Exchange services. You manage Exchange services through the Computer Management console and Exchange System Manager.

To start, pause, or stop a virtual server

1. In Exchange System Manager, right-click the virtual server that you want to manage, and do one of the following:
2. To start the service, click **Start**.
3. To change the server status to paused or to restart a server that has previously been paused, click **Pause**.
Note When a server is paused, an icon indicating that the server is paused appears next to the server name in the console tree.
4. To change the server status to stopped, click **Stop**.
Note When a server is stopped, an icon indicating that the server is stopped appears next to the server name in the console tree.

Disconnecting Users

You can immediately disconnect a single user or all users if they are accessing the virtual server without permission.

To disconnect users

1. In Exchange System Manager, expand **SMTP**, **IMAP4**, or **POP3**, and then double-click the virtual server where you want to disconnect users.
2. To disconnect users from the **Current Sessions** node under the virtual server, use one of the following methods:
 - To disconnect a single user, click **Terminate**.
 - To disconnect all users, click **Terminate all**.

Managing Calendaring Options for the POP3 and IMAP4 Virtual Servers

You can configure a URL for access to calendaring information for your POP3 and IMAP4 messaging clients. This functionality enables you to use a POP3 or IMAP4 messaging client and Outlook Web Access to manage your calendar. The options that you select for this feature control the format of the URL.

Note In topologies that contain Exchange front-end and back-end servers, configure the URL that is used to access calendaring information about the back-end server. Exchange does not recognize any URL settings that you configure on the front-end servers.

When downloading meeting requests through POP3 and IMAP4, a URL to the meeting request in Outlook Web Access is added to the plain text/HTML part of the message. Users click the URL to access the meeting request, and then accept or decline the request. (Some IMAP4 and POP3 messaging clients include a graphical user interface that allows those clients to accept or decline meetings without having to click the URL.) If users accept the request, Exchange automatically adds it to their calendar.

Note The URL to the meeting request does not work for POP3 clients that are configured to download messages from the server. This situation occurs because the message is downloaded to the client. As a result, the URL points to a message that is no longer on the server.

To configure the calendaring options for a POP3 or IMAP4 virtual server

1. In Exchange System Manager, expand the **First Administrative Group**, expand the **Servers** node, and then expand the Exchange server for which you want to manage POP3 or IMAP4 calendaring options.

2. Expand the **Protocols** node, and then right-click the POP3 or IMAP4 protocol and select **Properties**.
3. On the **Calendar** tab, select the server where recipients download meeting requests:

- To designate the recipient's home server as the server where the recipient downloads meeting requests, select **Use recipient's server**.

This is the default setting. If you select this option, the URL has the following format:

```
http://<HomeServerName>/Exchange/Username/Inbox/Team%20Meeting.eml
```

- To designate a front-end server as the server where recipients download meeting requests, select **Use front-end server**.

This option is useful if you have configured your Outlook Web Access users to access their mailboxes through a front-end server. If you select this option, the URL has the following format:

```
http://<FQDomainName>/Exchange/Username/Inbox/Team%20Meeting.eml
```

4. To use SSL to connect to the Exchange servers, select **Use SSL connections**.
 - **Note** If you select this option, the URL syntax includes https:// instead of http://.
5. Click **OK** to save your settings.

Managing the HTTP Virtual Server

Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync rely on the HTTP protocol to access Exchange information. These clients also use the WebDAV protocol, a set of rules that enable computers to exchange information and execute instructions through the Exchange front-end server, as well as retrieve and handle information in the Exchange store. By supporting both HTTP and WebDAV, Exchange 2003 can provide more data access functionality to users. For example, users of Outlook Web Access can do calendar request operations and can store Microsoft Office files, such as Microsoft Office Word documents, in the Exchange store.

Exchange provides support for both HTTP and WebDAV through the HTTP virtual server. When you install Exchange, Exchange automatically installs and configures an HTTP virtual server. You administer this default server only from IIS.

However, to provide for several collaboration scenarios and to supplement the access to folders that is provided by the default Web site in IIS, you can create new HTTP virtual servers in Exchange System Manager. As with any virtual server, each new HTTP virtual server that you create requires a unique combination of IP address, TCP port, SSL port, and host name. Furthermore, for each virtual server that you create, you must define one virtual directory as the root directory of the server for publishing content.

Note The folder contents displayed by the HTTP virtual server are converted to Web pages and sent to a user's browser by IIS.

To create a new HTTP virtual server

1. In Exchange System Manager, expand the **First Administrative Group**, expand the **Servers** node, and then expand the Exchange server where you want to create a new HTTP virtual directory.
2. Expand the **Protocols** node, right-click the HTTP protocol, select **New** and then click **HTTP Virtual Server**.
3. In the **Properties** dialog box for the new HTTP virtual server, configure the settings for your new Exchange virtual directory.

Managing the Exchange Virtual Server

The Exchange Virtual Server contains the virtual directories that provide access to Exchange for the HTTP clients that Exchange supports, such as Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync. Although you enable settings for Outlook Web Access, including forms-based authentication and

gzip compression, by using the Exchange Virtual Server, you manage most settings for the Exchange virtual directories in the IIS snap-in.

Specifically, in Exchange 2003, if you need to configure authentication settings to your Exchange virtual directories, use the IIS snap-in. To configure access control for the \Exchange, \Public, and \Exadmin virtual directories, use Exchange System Manager instead.

Working with IMAP4-Specific Settings

The IMAP4 virtual server has two protocol-specific settings:

- **Include all public folders when a folder is requested** Unlike POP3, which allows clients to access only mail messages, IMAP4 clients have access to folders other than the Inbox folder. However, this ability to access other folders must be enabled on the virtual server.
- **Enable fast message retrieval** Fast message retrieval improves performance by approximating message size, as opposed to actually calculating the message size. Performance improves because less processor work is required.

You select these settings on the **General** tab in the **Default IMAP4 Virtual Server Properties** dialog box (Figure 3.1).

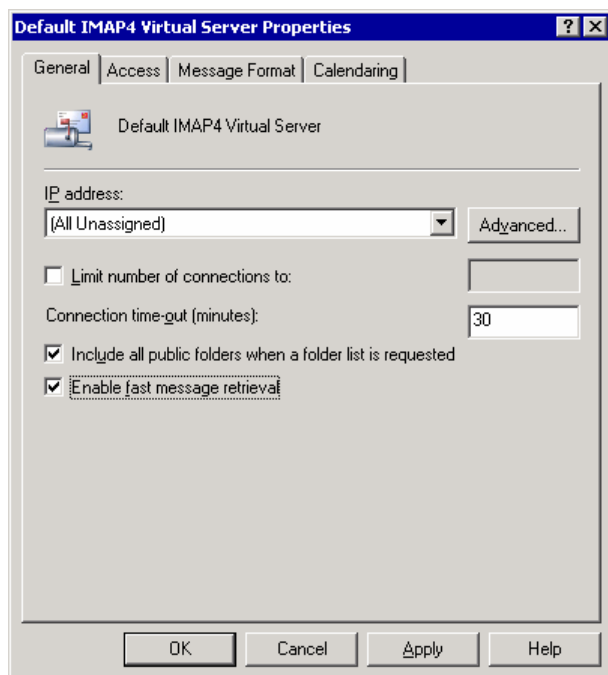


Figure 3.1 The **General** tab in the **Default IMAP4 Virtual Server Properties** dialog box

Configuring NNTP Posting Limits and Moderation Settings

Exchange Server 2003 uses NNTP to enable users to participate in newsgroup discussions. Exchange also enables users who are running client applications that support NNTP to access newsgroup public folders on computers that are running Exchange. Users can read and post items, such as messages and documents, to NNTP newsgroups that are represented in Exchange as public folders. For example, users can share information by posting messages to a newsgroup public folder in their area of interest. Other users can read and respond to items in the newsgroup. Items in newsgroups can be replicated to USENET host computers through newsfeeds.

A newsfeed is the flow of items from one USENET site to another. Newsfeeds enable users of different news sites to read and post articles to newsgroups as though they are using one news site. A news site is a collection of related newsgroups. An article posted to one news site is sent to other news sites where it can be read. You need to create a newsfeed to each remote server to which you want to distribute news articles.

Because the reason for using newsgroups is to post and share information, you will likely need to manage the size of these postings in relation to the resources available on the NNTP virtual server. Accepting articles that are too large or accepting too much data during one connection can cause increased traffic, overload your network, and quickly fill your hard disk. Be sure to set a size limit that matches your server's capabilities.

To configure posting limits and moderation settings for an NNTP virtual server

1. Log on to the Exchange server where the virtual server is running using the Exchange administrator account that has local Administrator permissions and Exchange Full Administrator permissions.
2. In Exchange System Manager, expand **Protocols**, right-click the protocol for which you want to change connection limits, and then click **Properties**.
3. On the **Settings** tab (Figure 3.2), select from the following options:
 - To allow clients to post articles to newsgroups on this NNTP virtual server, select **Allow client posting**. This option permits users to post and read articles in newsgroups that they can access, unless the newsgroup is set to read-only. You can also limit the size of the article that clients post in addition to the size of the connection.
 - To allow clients to post articles to newsfeeds on the NNTP virtual server, select **Allow feed posting**. You can limit the size of articles that are posted by using the **Limit post size** check box. You can limit the amount of data that is sent to a newsfeed during a single connection by using the **Limit connection size** check box.

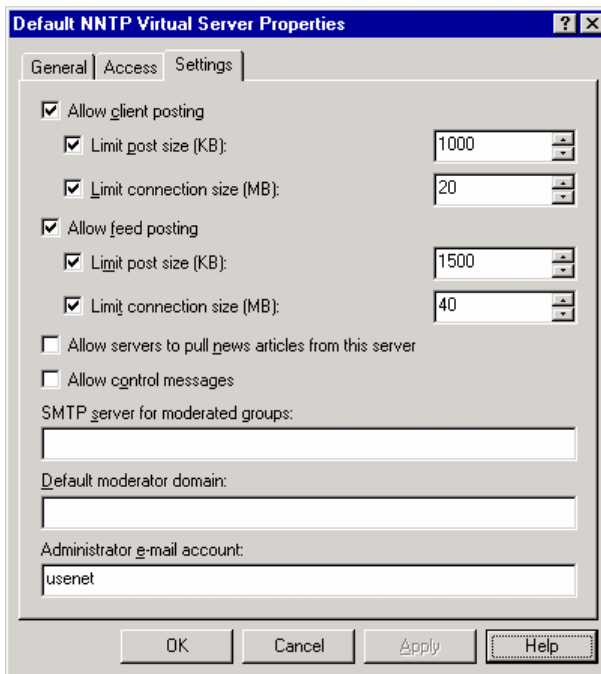


Figure 3.2 The Settings tab in the Default NNTP Virtual Server Properties dialog box

Note For more information about configuring NNTP, see the Exchange Server 2003 Help.

Managing Outlook Web Access

Outlook Web Access for Exchange 2003 includes significant improvements related to the user interface and administration. For information about the user experience improvements in Outlook Web Access, see "Client Features" in *What's New in Exchange Server 2003* (<http://go.microsoft.com/fwlink/?linkid=21765>).

You use both Exchange System Manager and the IIS snap-in to manage Outlook Web Access. Use:

- Exchange System Manager to modify settings for access control to Outlook Web Access.
- The IIS snap-in to control the authentication settings for the virtual directories for Outlook Web Access, including \Exchange, \Exchweb, and \Public.
- The IIS snap-in to enable SSL for Outlook Web Access. For more information about using SSL with Outlook Web Access, see "Configuring Exchange Server 2003 for Client Access" in the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

The following sections show how to use Exchange System Manager and the IIS snap-in to do management tasks associated with Outlook Web Access.

Enabling and Disabling Outlook Web Access for Internal Clients Only

You can enable users in your corporate network to access Outlook Web Access, while at the same time denying access to external clients. The key to this approach is a combination of a recipient policy and a special HTTP virtual server. The steps for this approach are as follows:

1. Create a recipient policy with an SMTP domain name. Users who are connecting to an HTTP virtual server must have an e-mail address with the same SMTP domain as the virtual server. Creation of a recipient policy is an efficient way to apply the same SMTP domain to multiple users.
 - **Note** Outlook Web Access users do not have to know the name of the SMTP domain.
2. Apply the recipient policy to the user accounts for which you want to enable access.
3. Then, on the front-end server, create a new HTTP virtual server that specifies the domain that is used in the recipient policy.

After you complete these steps, users whose e-mail addresses do not have the same SMTP domain as the HTTP virtual server will not be able to log on and access Outlook Web Access. Also, as long as you do not use the SMTP domain as the default domain, external users cannot determine what the SMTP domain is because the domain does not appear in the **From** field when users send e-mail messages outside the organization.

■ **Note** For more information about users with mailboxes that have an SMTP address that is not related to the address specified in the default recipient policy, see Microsoft Knowledge Base article 257891, "XWEB: 'The Page Could Not Be Found' Error Message When You Use OWA" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=257891>).

Besides enabling Outlook Web Access for users in your corporate network, you can also prevent specific internal users from accessing Outlook Web Access. You do this by disabling the HTTP and NNTP protocols for those users.

To prevent an internal user from accessing Outlook Web Access

1. In Active Directory Users and Computers, open the user's **Properties** dialog box.
2. On the **Exchange Features** tab, clear the settings for HTTP and NNTP.

Using Browser Language Settings

When using Microsoft Internet Explorer 5 or later to access Outlook Web Access, new installations and upgrades to Exchange 2003 use the browser's language settings to determine the character set to use to encode information, such as e-mail messages and meeting requests.

If you upgrade a server running Exchange 2000 that was modified to use a browser's language setting, Exchange 2003 continues to function in the same manner. Table 3.2 lists the language groups and respective character sets.

Table 3.2 Outlook Web Access language group and character sets

Language group	Character set
Arabic	Windows 1256
Baltic	iso-8859-4
Chinese (Simplified)	Gb2131
Chinese (Traditional)	Big5
Cyrillic	koi8-r
Eastern European	iso-8859-2
Greek	iso-8859-7
Hebrew	windows-1255
Japanese	iso-2022-jp
Korean	ks_c_5601-1987
Thai	windows-874
Turkish	iso-8859-9
Vietnamese	windows-1258
Western European	iso-8859-1

If you expect Outlook Web Access users in your organization to send mail frequently, you can modify registry settings so that users who are running Internet Explorer 5 or later can use UTF-8 encoded Unicode characters to send mail.

Warning Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To modify the default language setting for Outlook Web Access

1. On the Exchange server, log on with the Exchange administrator account, and start Registry Editor (**regedit**).

2. In Registry Editor, locate the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\  
MSExchangeWEB\OWA\UseRegionalCharset
```

3. Create a DWORD value named **UseRegionalCharset**.
4. Right-click the **UseRegionalCharset** DWORD value, and then click **Modify**.
5. In **Edit DWORD Value**, in the **Value data** box, type **1**, and then click **OK**.
6. Close Registry Editor to save your changes.

Blocking Web Beacons

In Exchange 2003, Outlook Web Access makes it more difficult for people who send junk e-mail messages to use beacons to retrieve e-mail addresses. Beacons frequently come in the form of images that are downloaded to a user's computer when the user opens a junk e-mail item. After the images download, a beacon notification is sent to the sender of the junk e-mail informing the sender that the e-mail address of your user is valid. The result is that the user will receive junk e-mail more frequently because the junk e-mail sender now knows that the e-mail address is valid.

In Outlook Web Access, an incoming message with any content that can be used as a beacon, regardless of whether the message actually contains a beacon, prompts Outlook Web Access to display the following warning message:

To help protect your privacy, links to images, sounds, or other external content in this message have been blocked. [Click here to unblock content.](#)

If users know that a message is legitimate, they can click the **Click here to unblock content** link in the warning message and unblock the content. If your users do not recognize the sender or the message, they can open the message without unblocking the content and then delete the message without triggering beacons. If your organization does not want to use this feature, you can disable the blocking option for Outlook Web Access.

To disable the blocking option

- On the user's Outlook Web Access **Options** page, under **Privacy and Junk E-mail Prevention**, clear the **Block external content in HTML e-mail messages** check box.

Configuring Attachment Handling

Outlook Web Access can be configured to handle e-mail attachments as your organization requires. You have three options for how your Exchange servers handle attachments:

1. Do not allow attachments
2. Allow attachments (pending file-type filtering)
3. Allow attachment access only through specific back-end servers

Additionally, you can specify a list of front-end servers that are exceptions to the "Allow attachment access through backend servers" option thereby allowing the users that connect through the specified front-end servers to be able to accept attachments. Note that if you set the server to "Allow all attachments" or "Don't allow any attachments," this value is ignored. Also, if a request is through a front-end server specified in this list of front-end servers that can accept attachments, the attachments must still pass Level 1 and 2 restrictions.

Blocking Attachments

With Outlook Web Access, you can block users from opening, sending, or receiving specified attachment types. In particular, you can:

- **Prevent users from accessing certain file type attachments** By default, all new Exchange 2003 installations block attachments of Levels 1 and 2 file types, and Levels 1 and 2 MIME types. This feature is particularly useful in stopping Outlook Web Access users from opening attachments at public Internet terminals, which could potentially compromise corporate security. If an attachment is blocked, a warning message indicating that the user cannot open the attachment appears in the InfoBar of the e-mail message. Outlook Web Access users who are working in their offices or connected to the corporate network from home can open and read attachments. You can enable full intranet access to attachments by providing the URL to the back-end servers and allowing attachments on the Exchange back-end servers.
- **Prevent users from sending or receiving attachments with specific file extensions that could contain viruses** This feature in Outlook Web Access matches the attachment blocking functionality in Outlook. For received messages, a warning message indicating that an attachment is blocked appears in the InfoBar of the e-mail message. For sent messages, users cannot upload any files with extensions that appear on the block list.

To change the attachment blocking settings, you must modify the registry settings on the server.

Warning Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To modify the attachment blocking settings on an Exchange server

1. Log on to the Exchange server using the Exchange administrator account, and then start Registry Editor (**regedit**).
2. In Registry Editor, locate the following registry key:


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
```
3. On the Edit menu, point to **New**, and then click **DWORD Value**.
4. In the details pane, name the new value **DisableAttachments**.
5. Right-click **DisableAttachments**, and then click **Modify**.
6. Under **Base**, in **Edit DWORD Value**, click **Decimal**.
7. In the **Value data** box, type one of the following numbers:
 - To allow all attachments, type **0**.
 - To disallow all attachments, type **1**.
 - To allow attachments from back-end servers only, type **2**.
8. Click **OK**.

Specifying Front-End Servers That Allow for Attachment Handling

You can specify a list of front-end servers that are exceptions to the "Allow attachment access through backend servers" option thereby allowing the users that connect through the specified front-end servers to be able to accept attachments. Note that if you set the server to "Allow all attachments" or "Don't allow any attachments," this value is ignored. Also, if a request is through a front-end server specified in this list of front-end servers that can accept attachments, the attachments must still pass Level 1 and 2 restrictions.

To configure attachment handling for Outlook Web Access

1. Log on to the Exchange server using the Exchange administrator account, and then start Registry Editor (**regedit**).
2. In Registry Editor, locate the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
```
3. On the Edit menu, point to **New**, and then click **String Value**.
4. In the details pane, name the new value **AcceptedAttachmentFrontEnds**.
5. Right-click **AcceptedAttachmentFrontEnds**, and then click **Modify**.
6. In **Edit String Value**, under **Value Data**, enter the names of the front-end servers that you want to allow attachments.
7. Click **OK**.

Filtering Junk E-Mail Messages

You can control how Exchange 2003 manages junk e-mail for your organization. To do this, you need to enable filtering, and then configure sender, recipient, and connection filtering. For more information about controlling junk e-mail with Exchange 2003, see "Configuring Filtering and Controlling Spam" in the *Exchange Server 2003 Transport and Routing Guide* (<http://go.microsoft.com/fwlink/?linkid=26041>).

Managing Exchange ActiveSync

By using Exchange ActiveSync, users with a Windows-powered mobile device with the desktop ActiveSync software can synchronize their devices with their Exchange servers over the Internet. Users connect across the Internet to their Exchange front-end server and request information from their Exchange mailbox server. When you enable access to Exchange using Exchange ActiveSync, follow these steps.

1. Use the front-end and back-end server architecture to provide a single namespace for users to connect to your network (recommended). For more information, see *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>).
2. Install an SSL certificate on the front-end server. For more information, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).
3. Inform users how to connect to the Internet from their device and use ActiveSync on their device to connect to their Exchange server. For more information, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

The following sections provide information about how to manage Exchange ActiveSync for your organization, including how to enable and disable the Exchange ActiveSync application, and how to enable ActiveSync for your users.

Enabling Exchange ActiveSync for Your Organization

By default, Exchange ActiveSync is enabled for all the users in your organization. If your users have mobile devices that are powered by Windows, you can inform them how to configure their devices to use Exchange ActiveSync. For more information about informing your users how to use Exchange ActiveSync, see "Configuring Exchange Server 2003 for Client Access" in the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

To enable and disable Exchange ActiveSync for your organization, use Exchange System Manager. However, when you add new users to your organization and you want to enable them to use Exchange ActiveSync to

access Exchange with a mobile device that is powered by Windows, use Active Directory Users and Computers to modify the settings for a user or groups of users. The following procedures describe how to enable or disable the Exchange ActiveSync application for your organization and how to modify Exchange ActiveSync settings to handle new users.

To enable or disable Exchange ActiveSync for your organization

1. On the Exchange front-end server that is running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. On the **Mobile Services Properties** page, in the Exchange ActiveSync pane, select or clear the check box next to **Enable user initiated synchronization**.
4. Click **OK**.

To modify Exchange ActiveSync settings

1. On the Exchange server with the user's mailbox, log on with the Exchange administrator account, and then start Active Directory Users and Computers.
2. Expand the domain, and then open the location for the users that you want to manage.
3. Right-click the user or users whose Exchange ActiveSync settings you want to modify, and then select **Exchange Tasks**.
4. In Exchange Task Wizard, on the **Available Tasks** page, select **Configure Exchange Features**, and then click **Next**.
5. On the **Configure Exchange Features** page, select **User initiated synchronization**, and then select one of the following:
 - To permit users to use Exchange ActiveSync to synchronize their Exchange mailbox with their mobile devices, select **Enable**.
 - To prevent users from using Exchange ActiveSync, select **Disable**.
 - To prevent the users' settings from being modified when you have selected more than one user, select **Do not modify**.
6. Click **Next** to apply your changes.
7. Click **Finish**.

Note To view a detailed report of the settings and the changes you made to users, select **View detailed report when this wizard closes**.

Enabling Up-to-Date Notifications for Your Organization

After you configure your organization to use Exchange ActiveSync, you can configure your Exchange 2003 servers so that users can receive up-to-date notifications to keep their devices current with the changes that occur when a new item arrives in their Exchange mailbox. This notification prompts the user's device to synchronize the device with the Exchange mailbox automatically.

To enable up-to-date notifications for your organization

1. On the Exchange front-end server running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. On the **Mobile Services Properties** page, in the Exchange ActiveSync pane, select **Enable up-to-date notifications**.
4. Click **OK**.

To modify up-to-date notifications settings for your users

1. On the Exchange server with the user's mailbox, log on with the Exchange administrator account, and then start Active Directory Users and Computers.

2. Expand the domain, and then open the location for the users whose settings that you want to modify.
3. Right-click the user or users whose up-to-date notifications settings you want to modify, and then select **Exchange Tasks**.
4. In Exchange Task Wizard, on the **Available Tasks** page, select **Configure Exchange Features**, and then click **Next**.
5. On the **Configure Exchange Features** page, select **Up-to-date notifications**, and then select one of the following:
 - To allow users to use up-to-date notifications, select **Enable**.
 - To prevent users from using up-to-date notifications, select **Disable**.
 - To prevent the users' settings from being modified when you have selected more than one user, select **Do not modify**.

Enabling Users to Use a Mobile Operator to Receive Notifications

If you enable the Exchange ActiveSync up-to-date notifications feature, your users use a mobile operator to deliver messages from the corporate network to their devices. You can enable your users to receive notification in two ways:

Option 1: Specify a mobile operator for your users

To specify a mobile operator for your users, disable the **Enable notifications to user specified SMTP addresses** on the Exchange server that has the mailboxes for these users. If you select this option, you need to inform your users how to set their devices to use the mobile operator that you specify for up-to-date notifications.

Option 2: Allow users to use their own mobile operators

If your users have their own mobile devices that are powered by Windows, you can allow them to use their own mobile operators to deliver notifications to their devices. If you select this option, you need to inform your users how to set their devices to use the mobile operators that they want to use for up-to-date notifications.

The following two procedures describe how to configure these options. The first procedure describes how to set the **Enable notifications to user specified SMTP address** option, and the second procedure describes how to set the mobile operator on a user's device.

To set the **Enable notifications to user-specified SMTP address** option for your organization

1. On the Exchange front-end server that is running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. On the **Mobile Services Properties** page, in the Exchange ActiveSync pane, set the **Enable notifications to user specified SMTP address** option as follows:
 - If you want to specify a mobile operator for your user, clear **Enable notifications to user specified SMTP address**.
 - If you want to allow your users to specify their own mobile operators, select **Enable notifications to user specified SMTP address**.
4. Click **OK**.

To specify a mobile operator for up-to-date notifications on a device

1. In ActiveSync, on a mobile device that is powered by Windows, tap **Tools**, and then tap **Options**.
2. On the **Server** tab, tap **Options**.
3. On the **Server Synchronization Options** screen, tap **Device Address**.

4. On the **Device Address** screen, do one of the following:
 - If your users are using a mobile operator that you specify, select **Corporate Service Provider**, and then enter the **Device Phone Number** and **Service Provider Name** in the fields that are provided.
 - If your users are using their own mobile operators, select **Device SMS Address**, and then enter the device address in the field provided.

Managing Outlook Mobile Access

By using Outlook Mobile Access, users can browse their Exchange mailbox using a device such as a Smartphone that is powered by Windows, or a cHTML-capable device. You can also enable users to use devices that are not officially supported by Microsoft, but which are likely to function correctly with only minor compatibility issues by enabling unsupported devices to use Outlook Mobile Access.

The following sections provide information about how to manage Outlook Mobile Access for your organization, including how to enable the Outlook Mobile Access application for your organization and how to enable users for Outlook Mobile Access.

Configuring Exchange to Use Outlook Mobile Access

By default, Outlook Mobile Access is disabled when you install Exchange 2003. For users to use Outlook Mobile Access, you must first enable it. When you enable access to Exchange by using Outlook Mobile Access, you should do the following:

1. Use the front-end and back-end server architecture to provide a single namespace for users to connect to your network. For more information, see *Using Microsoft Exchange 2000 Front-End Servers* at (<http://go.microsoft.com/fwlink/?linkid=12055>).
2. Install an SSL certificate on the front-end server. For more information, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).
3. Inform users how to connect to the Internet from their devices and how to use Outlook Mobile Access to access their Exchange information. For more information, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).

Enabling Outlook Mobile Access for Your Organization

To enable Outlook Mobile Access for your organization, use Exchange System Manager. After you enable Outlook Mobile Access, you can use Active Directory Users and Computers to modify the Outlook Mobile Access settings for users or groups of users.

To enable Outlook Mobile Access for your organization

1. Log on as an Exchange administrator to the Exchange server with the user's mailbox, and then start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. On the **Mobile Services Properties** page, in the Outlook Mobile Access pane, select **Enable Outlook Mobile Access**.
4. To enable users to use unsupported devices, select **Enable unsupported devices**.
 - Note** For information about supported devices for Exchange and planning for mobile device support with Exchange, see *Planning an Exchange Server 2003 Messaging System* (<http://go.microsoft.com/fwlink/?linkid=21766>).
5. Click **OK**.

To modify Outlook Mobile Access settings

1. Log on as an Exchange administrator to the Exchange server with the user's mailbox, and then start Active Directory Users and Computers.
2. Expand the domain, and then open the location for the users whose settings that you want to modify.
3. Right-click the user or users whose Outlook Mobile Access settings you want to modify, and then select **Exchange Tasks**.
4. In Exchange Task Wizard, on the **Available Tasks** page, select **Configure Exchange Features**, and then click **Next**.
5. On the **Configure Exchange Features** page, select **Outlook Mobile Access**, and then select one of the following:
 - To allow users to use Outlook Mobile Access, select **Enable**.
 - To prevent users from using Outlook Mobile Access, select **Disable**.
 - To prevent the users' settings from being modified when you have selected more than one user, select **Do not Modify**.
6. Click **Next** to apply your changes.
7. Click **Finish**.

Appendix



Resources

Resources Cited in This Guide

Exchange Server 2003

Technical Papers

- *Exchange Server 2003 RPC over HTTP Deployment Scenarios*
(<http://go.microsoft.com/fwlink/?linkid=24823>)
- *Using Microsoft Exchange 2000 Front-End Servers*
(<http://go.microsoft.com/fwlink/?linkid=12055>)

Microsoft Knowledge Base Articles

The following Microsoft Knowledge Base articles are available on the Web at
<http://go.microsoft.com/fwlink/?linkid=14898>

- 320291, "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access"
(<http://go.microsoft.com/fwlink/?linkid=3052&kbid=320291>)
- 257891, "XWEB: The 'Page Could Not Be Found' Error Message When You Use OWA"
(<http://go.microsoft.com/fwlink/?linkid=3052&kbid=257891>)
- 279681, "How to Force SSL Encryption for an Outlook Web Access 2000 Client"
(<http://go.microsoft.com/fwlink/?linkid=3052&kbid=279681>)

Windows 2000

Microsoft Knowledge Base Article

- 233256, "How to Enable IPSec Traffic Through a Firewall"
(<http://go.microsoft.com/fwlink/?linkid=3052&kbid=233256>)

Other Web Sites

- Microsoft Exchange Server Security Center
(<http://go.microsoft.com/fwlink/?linkid=18412>)

Additional Resources

In addition to the resources cited in this guide, you may find the following resources useful in your implementation of Microsoft® Exchange Server 2003.

Web Sites

- Exchange 2003 Compatibility with Mobile Devices
(<http://go.microsoft.com/fwlink/?linkid=24847>)
- Exchange Server 2003 Technical Documentation Library
(<http://go.microsoft.com/fwlink/?linkid=21277>)
- Exchange Server 2003 Tools and Updates
(<http://go.microsoft.com/fwlink/?linkid=25097>)
- Exchange Server 2003 Glossary
(<http://go.microsoft.com/fwlink/?linkid=24625>)
- Microsoft Developer Network (MSDN®)
(<http://go.microsoft.com/fwlink/?linkid=21574>)
- Cumulative Patch for Internet Explorer (328970)
(<http://go.microsoft.com/fwlink/?linkid=16694>)
- Microsoft Security Web site
(<http://go.microsoft.com/fwlink/?linkid=21633>)
- TechNet Security Web site
(<http://go.microsoft.com/fwlink/?LinkID=5936>)
- Microsoft Product Support Services Web site
(<http://go.microsoft.com/fwlink/?linkid=14898>)

Exchange Server 2003 Books

- *What's New in Exchange Server 2003*
(<http://go.microsoft.com/fwlink/?linkid=21765>)
- *Planning An Exchange Server 2003 Messaging System*
(<http://go.microsoft.com/fwlink/?linkid=21766>)
- *Exchange Server 2003 Deployment Guide*
(<http://go.microsoft.com/fwlink/?linkid=21768>)
- *Exchange Server 2003 Transport and Routing Guide*
(<http://go.microsoft.com/fwlink/?linkid=26041>)

Resource Kits

- *Microsoft Exchange 2000 Server Resource Kit*
(<http://go.microsoft.com/fwlink/?linkid=12058>)
Note You can order a copy of the *Microsoft Exchange 2000 Server Resource Kit* from Microsoft Press® at <http://go.microsoft.com/fwlink/?LinkId=6544>.
- *Windows 2000 Resource Kits*
(<http://go.microsoft.com/fwlink/?LinkId=6545>)
Note You can order a copy of *Microsoft Windows 2000 Server Resource Kit* from Microsoft Press at <http://go.microsoft.com/fwlink/?LinkId=6546>.

Accessibility

For information about accessibility for people with disabilities, see the Microsoft Accessibility Web site (<http://go.microsoft.com/fwlink/?linkid=22010>).