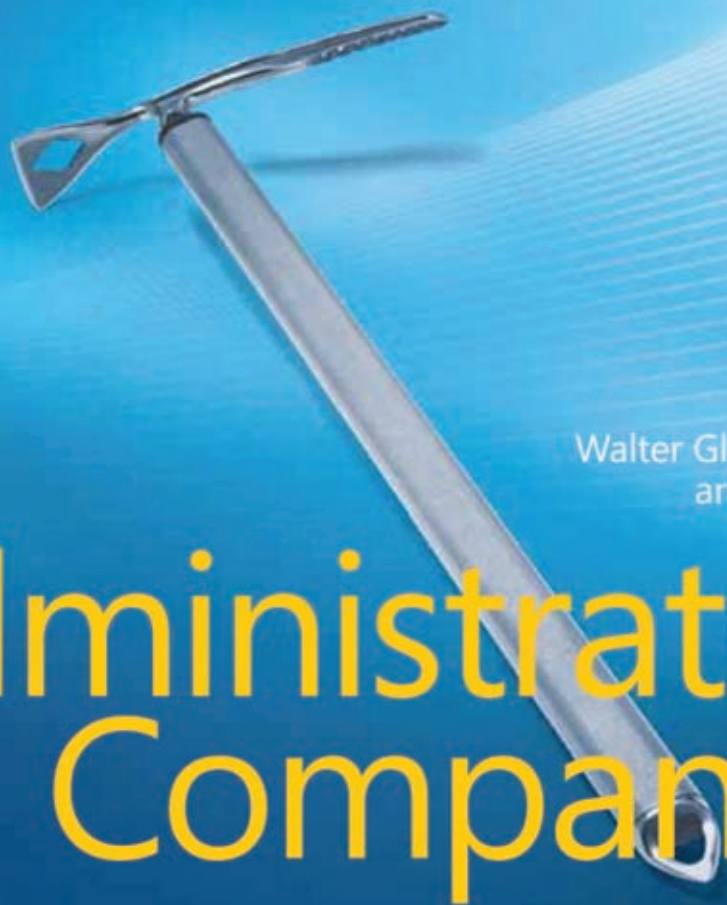
Microsoft

Updated for Service Pack 1

Microsoft® Exchange Server 2007

2

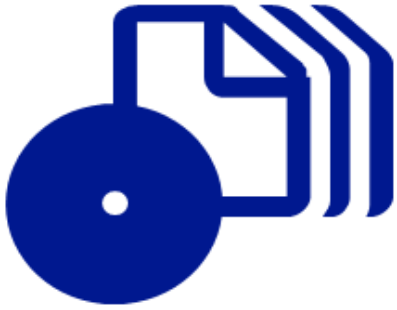
SECOND EDITION



Walter Glenn, Scott Lowe, and Joshua Maher

Administrator's Companion

How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/625907/files, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2008927277

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Acquisitions Editor: Martin DelRe
Developmental Editor: Karen Szall
Project Editor: Melissa von Tschudi-Sutton
Editorial Production: Custom Editorial Productions, Inc.
Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X14-80919

For my father, Bill English.

– Walter

For Amy. Thank you for your help and dedication in this and in everything.

– Scott

To my family for their unending support, John, Robin, Quentin, and Gabriel.

– Josh

Contents at a Glance

Part V
Maintenance

Part VI
Security

Part VII
Clients

Part VIII
Appendices

Table of Contents

Part IV
Management

Part VI
Security

Introduction

Welcome to the *Microsoft Exchange Server 2007 Administrator's Companion, Second Edition*! Whether you are an experienced Exchange administrator or just learning this product, you are going to be impressed with its new features, increased flexibility, and expanded information management capabilities. The development team at Microsoft has done an outstanding job of continuing the Exchange tradition of offering superior messaging services—Exchange Server 2007 with Service Pack 1 really is the best ever!

Microsoft Exchange Server 2007 is designed to meet the messaging and collaboration needs of businesses of all sizes. The *Microsoft Exchange Server 2007 Administrator's Companion*, *Second Edition* is designed to not only bring you up to speed in setting up the various features of Exchange Server 2007, but also to show you how these features work and why you might want to use them. We also offer advice from first-hand experience in the real world of Exchange organizations.

It's impossible to cover every element of Exchange Server 2007 in detail in one book. However, this Administrator's Companion is a great place to start as you consider implementing Exchange Server 2007 in your organization. This book can be used in several different ways. You can read it as a

- Guide to planning and deployment
- Ready reference for day-to-day questions
- Source of information needed to make decisions about the network
- Thorough introduction to the particulars of Exchange Server 2007

We assume that the reader has a fundamental understanding of networking concepts and of Microsoft Windows Server 2003. We have attempted to provide background at appropriate points as well as references to additional resources.

What's in This Book

The *Microsoft Exchange Server 2007 Administrator's Companion*, *Second Edition* is divided into multiple parts, each roughly corresponding to a stage in the implementation of an Exchange organization or covering a particular functionality.

Part I: Introduction

We begin by outlining the new features of Exchange Server 2007 and Exchange Server 2007 Service Pack 1. Then we dive in for a closer look at the program's storage and routing architecture. Chapter 1, "Overview of Microsoft Exchange Server 2007," is designed to get you up to speed quickly on what Exchange Server is and some of the features it offers. This first chapter also serves as a roadmap for the rest of the book. Chapter 2, "Active Directory for Exchange Administrators," explains the tight integration between Exchange Server 2007, Active Directory, and Windows Domain Name System (DNS). Chapter 3, "Exchange Server 2007 Architecture," details the storage and transport architecture of Exchange Server 2007.

Part II: Planning Your Deployment

Every successful implementation of a messaging system requires good planning, and Exchange Server 2007 is no exception. Two chapters are devoted to planning issues. Chapter 4, "Assessing Needs," looks at methods for taking stock of a current network and assessing the needs of users on that network prior to an Exchange Server 2007 deployment. Chapter 5, "Planning for Development," examines ways to create an actual deployment plan, based on the needs-assessment methods outlined in Chapter 4.

Part III: Installation and Deployment

After learning about the architecture of Exchange Server 2007 and how to plan for its deployment, you're ready to get your hands dirty. In this part, we outline how to install Exchange Server 2007 and how to implement its various features in the way that best suits your organization. Chapter 6, "Installing Exchange Server 2007," details the various methods of installing Exchange Server 2007. This chapter also shows how to make sure a server is ready for Exchange Server 2007 installation. Chapter 7, "Coexisting with Previous Versions of Exchange Server," shows you how to install Exchange Server 2007 into an organization that uses previous versions of Exchange Server. Chapter 8, "Transitioning to Exchange Server 2007," details how to transition an organization running a previous version of Exchange Server to using only Exchange Server 2007. Chapter 9, "High Availability in Exchange Server 2007," looks at the installation and configuration of local continuous replication, cluster continuous replication, and single copy clusters.

Part IV: Management

After learning about Exchange Server 2007 deployment, we turn our attention to issues of management. Chapter 10, "Managing Exchange Server 2007," introduces you to Microsoft Management Console (MMC)—the management interface included with Windows Server 2003. This chapter also provides a tour of the two primary interfaces for

managing Exchange Server 2007: Exchange Management Console and Exchange Management Shell.

The next group of chapters—Chapter 11, "Creating and Managing Recipients," through Chapter 14, "Unified Messaging"—covers a whole host of other topics: creation and management of recipients (users, contacts, groups, and public folders), storage groups, and configuration of the new Unified Messaging feature.

Part V: Maintenance

Every system—even Exchange Server 2007—needs maintenance. We address the most important maintenance tasks in this section. Chapter 15, "Troubleshooting Exchange Server 2007," looks at how to perform basic troubleshooting for a server. Chapter 16, "Disaster Recovery," covers the critical topic of backup and restoration of your databases. Chapter 17, "Tuning Exchange Server 2007 Performance," examines how to tune your Exchange servers for maximum performance.

Part VI: Security

Security is a primary concern of any network administrator, and Exchange Server 2007 in collaboration with Windows Server 2003 offers enhanced options for protecting your organization. Although this is another topic that could easily fill a book of its own, in this part, we offer as comprehensive a look at security as this space permits. Chapter 18, "Security Policies and Exchange Server 2007," looks at planning Exchange security policies. Chapter 19, "Exchange Server Security Basics," covers the basics of Exchange Server security. Chapter 20, "Antivirus and Anti-Spam," looks at new features in Exchange Server 2007 that help you to combat malicious software. Chapter 21, "Securing Exchange Server 2007 Messages," looks at methods for securing messaging in an Exchange organization.

Part VII: Clients

The best implementation of Exchange Server 2007 won't do your organization much good if there aren't any clients to connect to it and use it. In this section, we provide an overview of the clients for Exchange Server 2007. The topics presented here could easily be expanded into their own book, so we cover the more important topics and reference other materials where appropriate. Chapter 22, "Overview of Exchange Clients," gives a general introduction to the various types of clients that can be used to connect to an Exchange server. Chapter 23, "Deploying Microsoft Office Outlook 2007," focuses on Microsoft Office Outlook 2007 and examines the issues surrounding its deployment. Chapter 24, "Supporting Outlook Web Access," covers the use of Outlook Web Access.

Chapter 25, "Supporting Other Clients," details the configuration of basic Internet protocols: POP3 and IMAP4. We go over the basic commands of each and discuss how to use the logging features for troubleshooting purposes.

How to Use This Book

Within the chapters, we've tried to make the material accessible and readable. You'll find descriptive passages, theoretical explanations, and step-by-step examples. We've also included a generous number of graphics that make it easy to follow the written instructions. The following reader's aids are common to all books in the Administrator's Companion series.

Real World

Everyone can benefit from the experiences of others. "Real World" sidebars contain elaboration on a theme or background based on the experiences of others who used this product during the beta testing period.

Note Notes include tips, alternative ways to perform a task, or some information that needs to be highlighted.

More Info Often there are excellent sources for additional information on key topics. We use these boxes to point you to a recommended resource.

Important Boxes marked Important shouldn't be skipped. (That's why they're called Important.) Here you'll find security notes, cautions, and warnings to keep you and your network out of trouble.

Best Practices Best Practices provide advice for best practices that this book's authors have gained from our own technical experience.

Security Alert Nothing is more important than security when it comes to a computer network. Security elements should be carefully noted and acted on.

System Requirements

The following are the minimum system requirements to run the companion CD provided with this book:

- Microsoft Windows XP, with the latest service pack installed and the latest updates installed from Microsoft Update Service
- CD-ROM drive
- Internet connection
- Display monitor capable of 1024 x 768 resolution
- Microsoft Mouse or compatible pointing device
- Adobe Reader for viewing the eBook (Adobe Reader is available as a download at *http://www.adobe.com*)

About the Companion CD

The companion CD contains the fully searchable electronic version of this book. We've also included pointers to white papers, tools, webcasts, virtual labs, and other information we found useful while we were writing this book.

Support

Every effort has been made to ensure the accuracy of this book and companion CD content. Microsoft Press provides corrections to this book through the Web at the following location:

http://www.microsoft.com/learning/support

To connect directly to the Microsoft Knowledge Base and type a query regarding a question or issue that you may have, go to the following address:

http://www.microsoft.com/learning/support/search.asp

If you have comments, questions, or ideas regarding the book or companion CD content, or if you have questions that are not answered by querying the Knowledge Base, please send them to Microsoft Press using either of the following methods:

E-Mail:

mspinput@microsoft.com

Postal Mail:

Microsoft Press
Attn: *Microsoft Exchange Server 2007 Administrator's Companion, Second Edition* Editor
One Microsoft Way
Redmond, WA, 98052-6399

Please note that product support is not offered through the preceding mail addresses. For support information, please visit the Microsoft Product Support Web site at the following address:

http://support.microsoft.com

Chapter 10

Managing Exchange Server 2007

Now that you've installed Microsoft Exchange Server 2007, you're probably eager to start working with it. You'll want to begin creating mailboxes, groups, and other recipients, but first you need to know some basics of managing the Exchange system.

Exchange Server 2007 introduces a radical shift in the way you manage an Exchange server or organization. Exchange Server 2007 is built entirely upon a new command-line interface named Exchange Management Shell—a modified version of the new Windows PowerShell. You can perform just about every imaginable administrative function with Exchange Server 2007 by using shell commands called cmdlets.

The graphical management interface for Exchange Server 2007 is Exchange Management Console. It is essentially a Microsoft Management Console (MMC) snap-in that is built to run commands from the Exchange Management Shell. Whenever you configure an object in the console or run a wizard, the interface actually is using the underlying Exchange Management Shell to issue the appropriate commands. In fact, when you issue a command in the console, it even provides information about how to issue those same commands from the Exchange Management Shell, providing a friendly way to get to know the shell interface and command structure.

This chapter introduces you to the Microsoft Management Console, the Exchange Management Console, and the Exchange Management Shell. Throughout this book, you learn about ways to perform administrative functions in both interfaces. This chapter is meant to give you grounding in the two interfaces you'll be using to manage Exchange Server 2007.

Microsoft Management Console

Microsoft Management Console (MMC) provides a common environment for the management of various system and network resources. MMC is actually a framework that hosts modules called snap-ins, which provide the actual tools for managing a resource. For example, you manage Exchange Server 2007 using the Microsoft Exchange snap-in.

> **Note** The start menu icon that loads the Exchange Management Console essentially creates an MMC and loads the Microsoft Exchange snap-in, and you can do nearly all your administration by selecting this shortcut. However, you may find it useful to add the Microsoft Exchange snap-in to an MMC console you create along with other snap-ins representing common tasks you perform.

MMC itself does not provide any management functionality. Rather, the MMC environment provides for seamless integration between snap-ins. This allows administrators and other users to create custom management tools from snap-ins created by various vendors. Administrators can save the tools they have created for later use and share them with other administrators and users. This model gives administrators the ability to delegate administrative tasks by creating different tools of varying levels of complexity and giving them to the users who will perform the tasks.

The MMC User Interface

When you first load MMC, you might notice that it looks a lot like Microsoft Windows Explorer. MMC uses a multiple-document interface, meaning that you can load and display multiple console windows in the MMC parent window simultaneously. Figure 10-1 shows the MMC parent window with the Microsoft Exchange snap-in loaded. The next few sections discuss the main parts of this window.

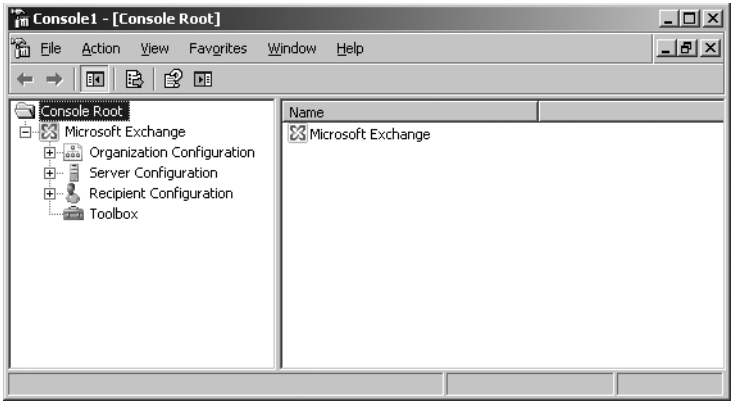


Figure 10-1 MMC window with the Microsoft Exchange snap-in loaded

MMC Toolbar

The main MMC toolbar holds six menus: File, Action, View, Favorites, Window, and Help. The View, Favorites, Window, and Help menus are pretty much what you would expect. The View menu lets you customize the columns you see in the display and turn on or off visual effects. The Favorites menu lets you add items to a list of favorites and organize that list into categories. The Favorites list can include shortcuts to tools, items in the console, or tasks. The Window menu lets you manage console windows if you have more than one window open in MMC. The Help menu lets you access general MMC Help as well as Help for the snap-ins that are currently loaded.

The Action menu provides access to commands pertinent to the object you have selected in the console. The commands on the Action menu change depending on what snap-in is loaded and what object within that snap-in is currently selected.

The File menu is where most of the action is. From this menu, you can open and save consoles and even create new ones. You can also add snap-ins to and remove them from open consoles and set general MMC options. Options you can set include the following:

- **Console Title** Specifies the console name as it appears in the MMC title bar.
- **Console Mode** Author mode grants the user full access to all MMC functionality. User mode comes in three flavors: Full Access lets the user access all MMC commands but not add or remove snap-ins or change console properties; Limited Access Multiple Window allows the user to access only the areas of the console tree that were visible when the console was saved and to open new windows; Limited Access Single Window works the same as Limited Access Multiple Window, except that users cannot open new windows.

Other options define whether users can access context menus on taskpads, save changes to the console, and customize views.

Scope Pane

The Scope pane contains a hierarchy of containers referred to as a console tree. Some containers are displayed as unique icons that graphically represent the type of items they contain. Others are displayed as folders, simply indicating that they hold other objects. Click the plus sign next to a container to expand it and display the objects inside. Click the minus sign to collapse the container.

Details Pane

The Details pane changes to show the contents of the container selected in the Scope pane. In other words, the Details pane shows the results of the currently selected scope. The Details pane can display information in a number of ways, referred to as *views*.

Note The View menu also lets you customize the columns that are shown in the scope and Details panes. In the Details pane itself, you can rearrange columns and click a column heading to reorder rows alphabetically or chronologically.

In addition to the standard views, for some snap-ins you can also create a taskpad view to show in the Details pane. A taskpad view is a dynamic HTML (DHTML) page that presents shortcuts to commands available for a selected item in the Scope pane. Each command is represented as a task that consists of an image, a label, a description, and a mechanism for instructing the snap-in to run that command. Users can run the commands by clicking a task.

You can use taskpad views to do the following things:

- Include shortcuts to all the tasks a specific user might need to perform.
- Group tasks by function or user by creating multiple taskpad views in a console.
- Create simplified lists of tasks. For example, you can add tasks to a taskpad view and then hide the console tree.
- Simplify complex tasks. For example, if a user frequently performs a given task involving several snap-ins and other tools, you can organize, in a single location, shortcuts to those tasks that run the appropriate property sheets, command lines, dialog boxes, or scripts.

Snap-in Root Container

The snap-in root container is the uppermost container in the snap-in; it is usually named based on the product or task that it is associated with. MMC supports stand-alone and extension snap-ins. A stand-alone snap-in, such as Microsoft Exchange, provides management functionality without requiring support from another snap-in. Only one snap-in root container exists for each stand-alone snap-in. An extension snap-in requires a parent snap-in above it in the console tree. Extension snap-ins extend the functionality provided by other snap-ins.

Containers and Objects

Exchange Server 2007 is a great example of an object-based, hierarchical directory environment. All the little bits and pieces that make up Exchange are objects that interact with one another to some degree. The objects you see in the Scope and Details panes can be divided into two types:

- **Containers** Containers can contain both other containers and noncontainer objects. Container objects can also appear in the Details pane. They are used to logically group all the objects that make up a management environment. An administrator uses the container objects to organize the tree and then to navigate through it.

- **Leaf Objects** A leaf object is simply an object that cannot contain other objects. Some common leaf objects with which an administrator works daily include servers and connectors.

You manage all the objects in an MMC console through the use of property sheets. A *property sheet* is a dialog box you open by selecting an object and then choosing Properties from the Action menu. It consists of one or more tabs that contain controls for setting a group of related properties. Figure 10-2 shows the property sheet for a server object in the Microsoft Exchange snap-in.

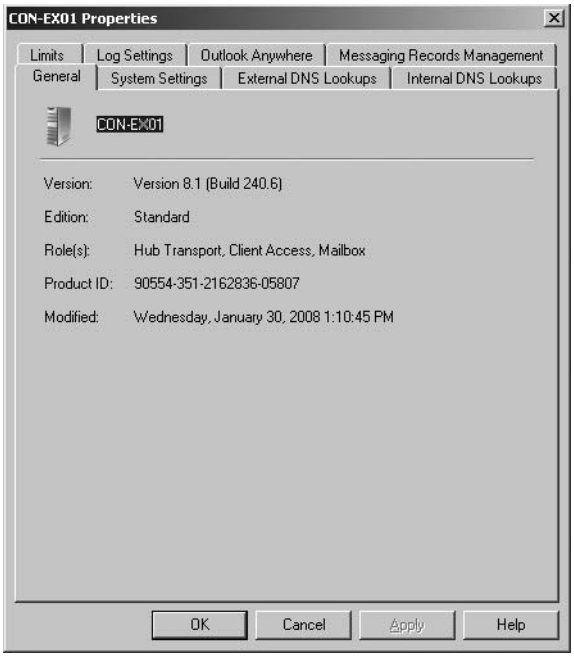


Figure 10-2 Property sheet for a server object

How MMC Works

The MMC interface permits snap-ins to integrate within a common management console. This gives all snap-ins a similar look and feel, although they might perform their tasks in different ways. The console itself offers no management functions; it merely acts as a host to the snap-ins. Snap-ins always reside in a console; they do not run by themselves.

Snap-ins

Each MMC tool is built of a collection of instances of smaller tools called MMC snap-ins. A snap-in is the smallest unit of console extension and represents one unit of manage-

ment behavior. The snap-in might call on other supporting controls and dynamic-link libraries (DLLs) to accomplish its task.

Snap-ins extend MMC by adding and enabling management behavior. They can provide this behavior in a number of ways. For example, a snap-in might add elements to the container tree, or it might extend a particular tool by adding shortcut menu items, toolbars, property sheet tabs, wizards, or Help to an existing snap-in. There are two basic types of snap-ins:

- **Stand-alone Snap-ins** Provide management functionality even if they are alone in a console with no other supporting snap-ins. They do not rely on any other snap-ins being present. The Exchange System snap-in is an example of a stand-alone snap-in.
- **Extension Snap-ins** Provide a variety of functionality, but only when used in conjunction with a parent snap-in. Some extend the console namespace, while others simply extend context menus or specific wizards.

Note Many snap-ins support both modes of operation, offering some stand-alone functionality and also extending the functionality of other snap-ins.

Packages

Snap-ins are usually shipped in groups called *packages*. For example, the Microsoft Windows operating system itself includes one or more packages of snap-ins. Additionally, other vendors might ship products composed entirely of packages of snap-ins. Grouping snap-ins into packages provides convenience for downloading and installation. It also permits several snap-ins to share core DLLs so that these DLLs do not have to be placed in every snap-in.

Custom Tools

MMC provides functionality for creating custom management tools. It allows administrators to create, save, and then delegate a customized console of multiple snap-ins tailored for specific tasks. Administrators can assemble these specific snap-ins into a tool (also called a *document*) that runs in one instance of MMC. For example, you can create a tool that manages many different aspects of the network—Active Directory, replication topology, file sharing, and so on. After assembling a tool, the administrator can save it in an .msc file and then reload the file later to instantly re-create the tool. The.msc file can also be e-mailed to another administrator, who can then load the file and use the tool.

Custom Consoles

One of the primary benefits of MMC is its support for customization of tools. You can build custom MMC consoles tailored for specific management tasks and then delegate those consoles to other administrators. These tools can focus on the particular management requirements of various administrator groups.

For example, you could create a custom console, as shown in Figure 10-3, that includes the Microsoft Exchange, Active Directory Users and Computers, Disk Management, and Event Viewer snap-ins—several tools that are important to any Exchange administrator.

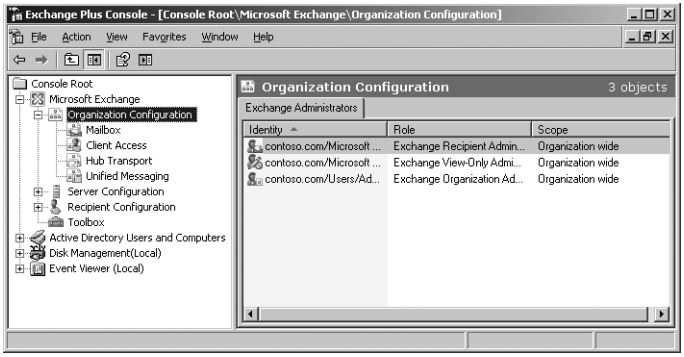


Figure 10-3 A custom console with various snap-ins

> **More Info** Obviously, there is a lot more to MMC than can be covered in a single chapter, especially when the chapter is really about using the Microsoft Exchange System snap-in. For more information about MMC, start with the Help file available from any console window.

Using the Exchange Management Console

The Exchange Management Console provides a graphical view of all the resources and components of an Exchange organization. No matter how many servers you have set up, you can manage them all from a single Exchange Management Console window. Use this window, and the property sheets of all the objects in it, to navigate the Exchange organizational hierarchy and perform the various tasks associated with Exchange administration.

You use both container and leaf objects to administer an Exchange organization. Most objects in the Exchange System console window—both container and leaf—have a property sheet that allows you to configure various parameters for that object and make it act in the way that best serves the organization's needs. You can open an object's property

sheet by selecting the object and choosing Properties from the Action menu. You can also right-click an object and choose Properties from its shortcut menu. You use property sheets to both configure and administer Exchange Server 2007.

Major Areas of the Exchange Management Console

You can start the Exchange Management Console by clicking Start, pointing to All Programs, then to Microsoft Exchange Server 2007, and then clicking Exchange Management Console. The Exchange Management Console is divided into the major areas shown in Figure 10-4. These areas include:

- **Console tree** The console tree is located on the left side of the console and is organized by containers that represent the hierarchy of the Exchange organization. The specific containers that are displayed are based on the server roles that are installed. When you select a container in the console tree, the results of that container are shown in the Results pane.
- **Results pane** The Results pane is located in the center of the console. This pane displays objects that reflect the container you have selected in the console tree. For example, if you select the Mailbox object inside the Recipient Configuration container, the Results pane shows individual mailboxes.
- **Work pane** The Work pane is located at the bottom of the Results pane. The Work pane is shown only when you select objects under the Server Configuration container, such as Mailbox, Client Access, or Unified Messaging. This pane displays objects based on the server role that is selected in the Server Configuration container. For example, if you select the Mailbox object in the Server Configuration container, the Results pane shows a list of Mailbox servers. When you select a server in the Results pane, storage groups on that server are shown in the Work pane.

> **Note** Another new feature introduced to the Exchange Management Console with Exchange Server 2007 Service Pack 1 (SP1) is the ability to export lists of objects that appear in the Results and Work panes. You can export a list as tab- or comma-delimited text files or Unicode text files.

- **Actions pane** The Actions pane is located on the right side of the console. This pane lists actions you can perform based on the object that is selected in the console tree, Results pane, or Work pane. These actions are the same actions you can take by displaying the Action menu or by right-clicking the object. For this reason, you might find it more useful to hide the Actions pane. You can do this by clicking the Show/Hide Action Pane button on the Exchange Management Console toolbar.

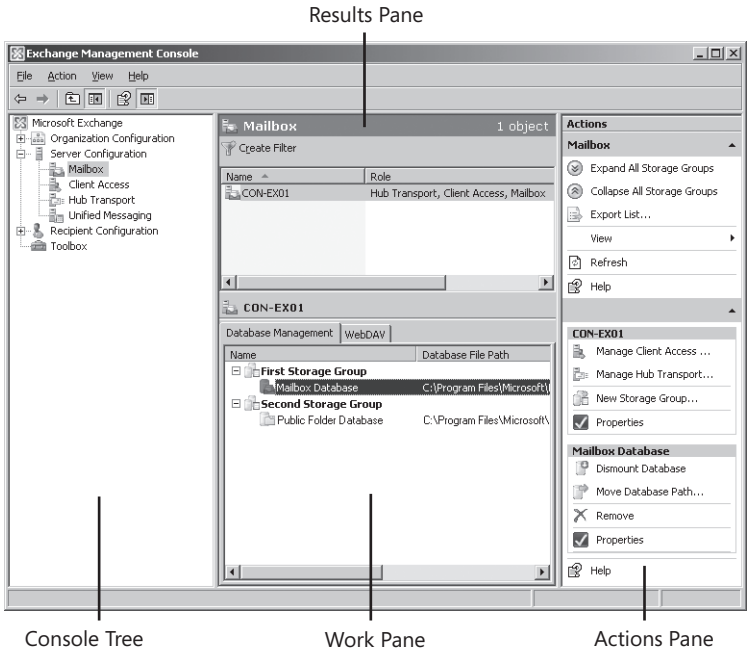


Figure 10-4 Areas of the Exchange Management Console

Real World Explore!

The sheer number of property sheets you encounter when administering Exchange Server 2007 can seem daunting, but don't let them intimidate you. Take the time to play with the program. You probably won't be able to remember exactly where to go to accomplish every administrative task in Exchange Server 2007, but it helps to think about what the task involves. If you need to manage the way all mailboxes on a server are handled, find the Mailbox container inside the Server Configuration container. If you need to manage a single mailbox, find the Mailbox container inside the Recipient Configuration container. Each component handles a different aspect of the configuration, so multiple components might be involved with a single configuration or administrative task. As you use the program and get used to the Exchange environment, it becomes easier to navigate the program and find exactly the object or objects you need to administer.

Learning the contents and layout of the various property sheets in the Exchange Management Console is a key to learning how Exchange Server 2007 works. After you know how to organize tasks that match the way Exchange Server 2007 is structured, your administrative tasks flow more easily.

To administer an Exchange environment with the Exchange Management Console, you must log on to Active Directory under a domain user account that has administrative privileges for administering the Exchange organization.

Examining the Exchange Hierarchy

The top of the hierarchy in the console tree of the Exchange Management Console is the snap-in root container that represents the Exchange organization, as shown in Figure 10-5. The snap-in root container is named Microsoft Exchange. All the Exchange containers are held within this container. Additionally, selecting the root container shows two tabbed screens in the Results pane: Finalize Deployment, which shows you tasks to perform after installation (and which is discussed in Chapter 6, "Installing Exchange Server 2007"); and End-to-End Scenario, which allows you to configure end-to-end solutions in Exchange, such as implementing best practices for disaster recovery.

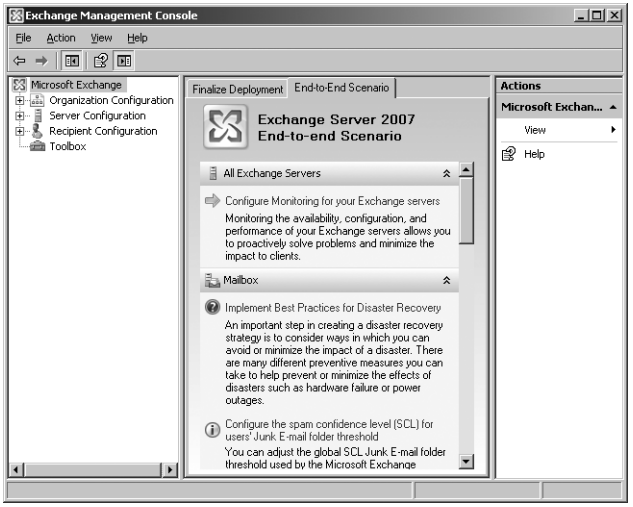


Figure 10-5 The Exchange hierarchy

There are four primary containers directly within the snap-in root container. The following sections describe each of these containers.

Organization Configuration

Selecting the Organization Configuration container itself displays all users configured as Exchange administrators and allows you to configure administrative access roles for users or groups, as shown in Figure 10-6. You must be a member of the Exchange Server Administrators group in order to view the Organization Configuration container or change the roles assigned to users.

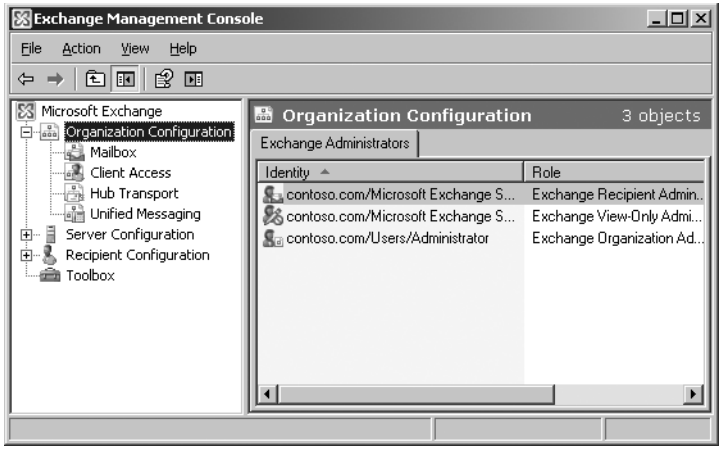


Figure 10-6 Viewing Exchange administrative roles with the Organization Configuration container

Exchange administrator roles are similar in function to Windows Server security groups. Administrator roles allow you to easily assign sets of permissions to users for the most common administrative functions in Exchange Server. Exchange administrative roles include the following:

- **Exchange Server Administrators** This role provides access to only local server Exchange configuration data, either in the Active Directory or on the physical computer on which Exchange 2007 is installed. Users who are members of the Exchange Server Administrators role have permissions to administer a particular server, but do not have permissions to perform operations that have global impact in the Exchange organization. Members assigned to this role are granted the following:
  - They are made owners of all local server configuration data. As owners, members of the role have full control over the local server configuration data.
  - They are made local administrators on the computer on which Exchange is installed.
  - They are made members of the Exchange View-Only Administrators role.
- **Exchange Organization Administrators Role** The Exchange Organization Administrators role provides administrators with full access to all Exchange properties and objects in the Exchange organization. Additionally, members assigned this role are granted the following:
  - They are made owners of the Exchange organization in the configuration container of Active Directory. As owners, members of the role have control over

the Exchange organization data in the configuration container in Active Directory and the local Exchange server Administrator group.

- They are given Read access to all domain user containers in Active Directory. Exchange grants this permission during setup of the first Exchange 2007 server in the domain, for each domain in the organization. These permissions are also granted by being a member of the Exchange Recipient Administrator role.
- They are given Write access to all Exchange-specific attributes in all domain user containers in Active Directory. Exchange 2007 grants this permission during setup of the first Exchange 2007 server in the domain, for each domain in the organization. These permissions are also granted by being a member of the Exchange Recipient Administrator role.
- They are made owners of all local server configuration data. As owners, members have full control over the local Exchange server. Exchange 2007 grants this permission during setup of each Exchange server.

- **Exchange Recipient Administrators Role** The Exchange Recipient Administrators role has permissions to modify any Exchange property on an Active Directory user, contact, group, dynamic distribution list, or public folder object. Members are granted the following:
  - They are given Read access to all the Domain User containers in Active Directory that have had Setup /PrepareDomain run in those domains.
  - They are given Write access to all the Exchange-specific attributes on the Domain User containers in Active Directory that have had Setup /PrepareDomain run in those domains.
  - They are automatically granted membership in the Exchange View-Only Administrator role.
- **Exchange View-Only Administrators Role** The Exchange View-Only Administrators role has read-only access to the entire Exchange organization tree in the Active Directory configuration container, and read-only access to all the Windows domain containers that have Exchange recipients.
- **Exchange Public Folder Administrators Role** Exchange 2007 Server Service Pack 1 (SP1) adds this new role, which allows administration of public folders. Members are automatically granted membership in the Exchange View-Only Administrator Role. Members are also given permission to modify any public folder object.

The Organization Configuration container contains the following containers:

- **Mailbox** At the organization level, the Mailbox container allows you to manage Mailbox server role settings that apply to the entire Exchange organization. You can create and manage address lists, managed custom folders, messaging records management (MRM) mailbox policies, and offline address books (OABs). You learn more about this in Chapter 11, "Creating and Managing Recipients."
- **Client Access** At the organization level, the Client Access container allows you to create and manage Exchange ActiveSync mailbox policies for mobile users. These policies apply common sets of security settings or policies to collections of users.
- **Hub Transport** At the organization level, the Hub Transport container allows you to configure features of the Hub Transport server role. The Hub Transport server role handles all internal mail flow, applies organizational message routing policies, and is responsible for delivering messages to a recipient's mailbox.
- **Unified Messaging** At the organization level, the Unified Messaging container allows you to manage Unified Messaging (UM) server role settings that apply to your entire Exchange 2007 organization. You can maintain existing or create new UM dial plans, UM IP gateways, UM mailbox policies, and UM auto attendants. For more information on Unified Messaging, see Chapter 14, "Unified Messaging."

Server Configuration

Use the Server Configuration container, shown in Figure 10-7, to view a list of all the servers in your Exchange organization and perform tasks specific to server roles. When you select the Server Configuration container itself, you can view the role, version, edition, product ID, cluster status, last modified time, and site for each server in the Results pane. For more information about how to view these columns in the Results pane, see the section, "Custom Consoles," earlier in this chapter.

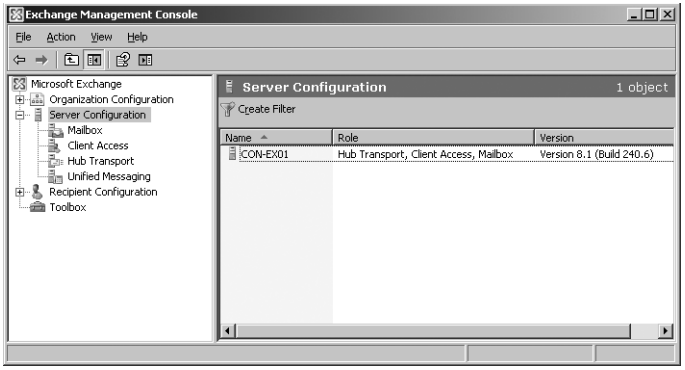


Figure 10-7 Viewing the Server Configuration container

The containers that appear under Server Configuration show only the Exchange servers that have a particular server role installed. The Server Configuration container contains the following containers:

- **Mailbox** At the server level, the Mailbox container allows you to display a list of all servers in the organization that have the Mailbox server role installed and to perform actions specific to that server role. The Database Management tab in the Work pane lists all the storage groups and databases that exist on the selected server.
- **Client Access** At the server level, the Client Access container allows you to view and maintain the settings for Microsoft Outlook Web Access (OWA), Exchange ActiveSync, and the offline address book (OAB).
- **Hub Transport** At the server level, the Hub Transport container allows you to display a list of all servers in the organization that have the Hub Transport server role installed and to perform actions specific to that server role.
- **Unified Messaging** At the server level, the Unified Messaging container allows you to configure voice messaging, fax, and e-mail messaging into one store that users can access from a telephone and a computer. Exchange 2007 Unified Messaging integrates Microsoft Exchange with telephony networks and brings the Unified Messaging features to the core of Microsoft Exchange.

Recipient Configuration

The Recipient Configuration container, shown in Figure 10-8, allows you to perform a variety of recipient management tasks. You can view all the recipients in your organization, create new recipients, and manage existing mailboxes, mail contacts, mail users, and distribution groups.

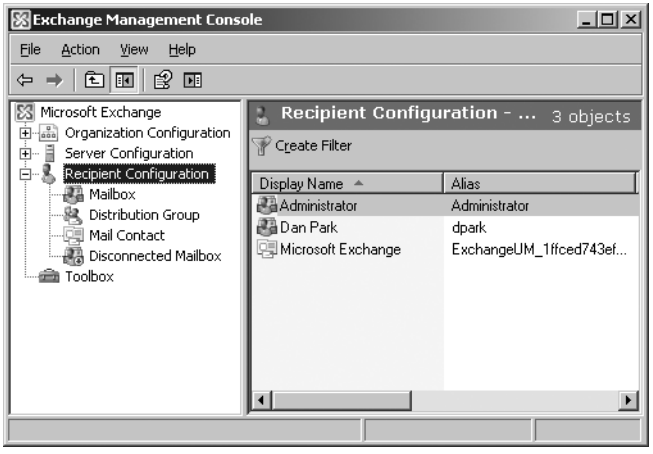


Figure 10-8 Viewing the Recipient Configuration container

The Recipient Configuration container contains the following containers:

- **Mailbox** At the recipient level, the Mailbox container allows you to manage mailbox users and resource mailboxes. Resource mailboxes include room and equipment mailboxes. You can create new mailboxes and remove, disable, or move existing mailboxes. You can also configure mailbox properties, enable and disable Unified Messaging (UM), and manage mobile devices.
- **Distribution Group** The Distribution Group container allows you to manage mail-enabled distribution groups (which include security groups) and dynamic distribution groups. You can create new distribution groups, and remove, disable, or configure existing distribution groups.
- **Mail Contact** The Mail Contact container allows you to manage mail contacts. You can create new mail contacts, and delete or configure existing mail contacts.
- **Disconnected Mailbox** The Disconnected Mailbox container allows you to view and connect disabled mailboxes. Disconnected mailboxes are retained based on the configured mailbox database limits. You will see only the mailboxes that have been disconnected within the retention period that is specified for the mailbox database.

Toolbox

The Toolbox is a collection of tools that are installed with Microsoft Exchange Server 2007. The Toolbox provides a central location for diagnostic, troubleshooting, and recovery activities using various Exchange tools.

The tools in the toolbox are divided into the following categories:

- **Configuration Management Tools** This category contains three tools. The first is the Best Practices Analyzer, which automatically examines an Exchange Server deployment and determines whether the configuration is in line with Microsoft best practices. Run the Best Practices Analyzer after installing a new Exchange server or after making any configuration changes. You learn more about this tool in Chapter 15, "Troubleshooting Exchange Server 2007."

  This category also contains the Details Templates Editor, the second tool. Details templates control how object properties (such as user information or an address list) appear in the user interface.

  The third tool in this category, Public Folder Management Console, is new to Service Pack 1, and brings public folder management to the Exchange Management Console. Before SP1, you had to manage public folders using the Exchange Management Shell. You will learn more about using this tool in Chapter 12, "Using Public Folders."

- **Disaster Recovery Tools** This category contains two tools: Database Recovery Management Tool and Database Troubleshooter. Both tools work through a set of troubleshooting steps to help identify and resolve database issues.
- **Mail Flow Tools** This category contains the following four tools:
  - **Mail Flow Troubleshooter** This tool allows you to troubleshoot common mail flow problems. After selecting a symptom of the mail flow problems you are experiencing (such as delays or non-delivery reports), the tool attempts to find a solution and then provides advice to walk you through the correct troubleshooting path. It shows an analysis of possible root causes and provides suggestions for corrective actions.
  - **Message Tracking** This tool lets you view a detailed log of all message activity as messages are transferred to and from an Exchange 2007 server that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. You can use message tracking logs for mail flow analysis, reporting, and troubleshooting.
  - **Queue Viewer** This tool allows you to monitor mail flow and inspect queues and messages. You can also perform actions to the queuing databases such as suspending or resuming a queue, or removing messages.
  - **Routing Log Viewer** Also new to SP1, this tool works on an Exchange server that has the Hub Transport or the Edge Transport server roles installed. The tool allows you to open a routing log file that contains information about how the routing topology of the network appears to the server.
- **Performance Tools** This category contains two tools: Performance Monitor and Performance Troubleshooter. Performance Monitor is a tool you can configure to collect information about the performance of your messaging system. Specifically, you can use it to monitor, create graphs, and log performance metrics for core system functions. Performance Monitor is covered in detail in Chapter 17, "Tuning Exchange Server 2007 Performance." Performance Troubleshooter helps you to locate and identify performance-related issues that could affect an Exchange server. You diagnose a problem by selecting the symptoms observed. Based on the symptoms, the tool walks you through the correct troubleshooting path. This tool is covered in Chapter 15.

Using the Exchange Management Shell

The Exchange Management Shell, shown in Figure 10-9, is based on Microsoft Windows PowerShell, which provides a powerful command-line interface for executing and automating administrative tasks. With the Exchange Management Shell, you can manage

every aspect of Exchange Server 2007, including enabling new e-mail accounts, configuring store database properties, and just about every other management task associated with Exchange Server 2007.

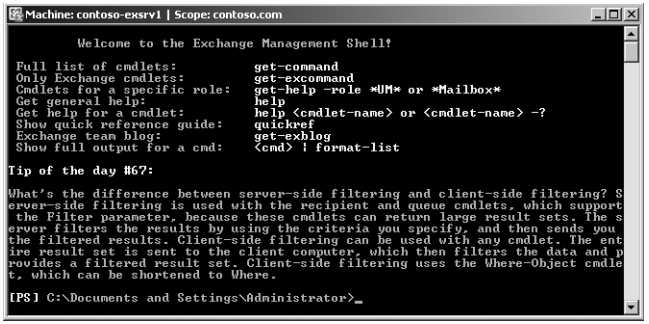


Figure 10-9 The Exchange Management Shell

In fact, you can use the Exchange Management Shell to perform every task available in the Exchange Management Console and a number of tasks that cannot be performed in the Exchange Management Console. It helps to think of it this way: the Exchange Management Console provides a graphical interface for most of the functionality of the Exchange Management Shell. When you run a command in the Exchange Management Console, the Exchange Management Shell is actually called to perform the command. When you perform a command in the Exchange Management Console, the graphic interface often even shows you the associated shell command, as shown in Figure 10-10.

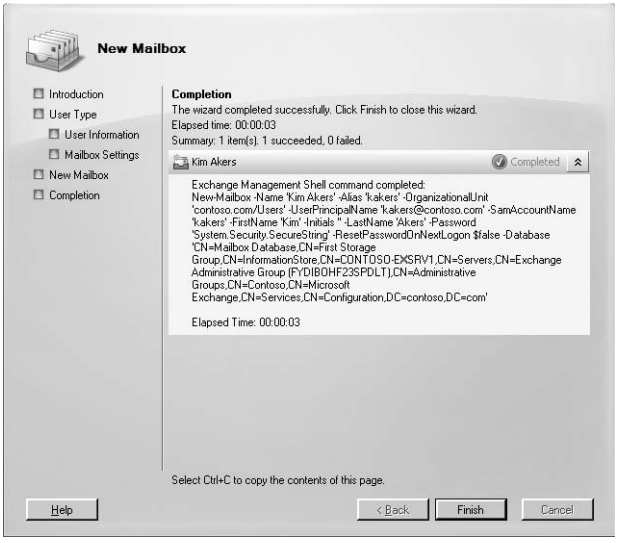


Figure 10-10 Viewing shell commands from the Exchange Management Console

So why use the shell instead of the console? Aside from the fact that some commands (such as those used to manage public folders) are only available as shell commands, the shell also offers a flexibility that can speed up and simplify common operations. For example, with a single shell command, you can get a list of recipients, filter that list according to a set of criteria, and then perform a function on only the filtered list of recipients.

Note The Exchange Management Shell also provides a robust and flexible scripting platform that can reduce the complexity of current Microsoft Visual Basic scripts. Tasks that previously required many lines in Visual Basic scripts can now be done by using as little as one line of code in the Exchange Management Shell. The Exchange Management Shell provides this flexibility because it does not use text as the basis for interaction with the system, but uses an object model that is based on the Microsoft .NET platform. This object model enables the Exchange Management Shell cmdlets to apply the output from one command to subsequent commands when they are run.

To open the Exchange Management Shell, follow these steps:

1. Click Start, point to All Programs, and then point to Microsoft Exchange Server 2007.
2. Click Exchange Management Shell.

More Info This section is intended to introduce you to the basics of using the Exchange Management Shell. Throughout this book, you find specific examples of using shell commands to complete administrative tasks. For more information on using the Exchange Management Shell, please consult the Exchange Server 2007 Help files. Help includes detailed advice on using advanced options such as `WhatIf` and comparison parameters, command output, shell variables, structured data, and scripting.

Understanding Cmdlets

At first glance, the shell may seem similar to other command-line interfaces with which you may be familiar. However, after working with the shell for just a few minutes, you see that there are dramatic differences.

In the Exchange Management Shell, a cmdlet is the smallest unit of functionality. A cmdlet is roughly analogous to a built-in command in other types of shells. You type cmdlets directly into the shell interface.

All cmdlets consist of at least two parts:

- **A verb** The verb represents the action of the command. An example of a verb is `get`, which is used to retrieve information about an object. Table 10-1 lists the most common verbs used in the Exchange Management Shell.
- **A noun** The noun represents the recipient of the verb's action. An example of a noun would be an object in the Exchange organization such as a Mailbox server. The noun in this case would be `MailboxServer`.

  Cmdlets always contain a verb and a noun separated by a hyphen. To continue the previous example, the cmdlet for getting information about a Mailbox server would be:

  ```
  Get-MailboxServer
  ```

Table 10-1 Common Verbs in the Exchange Management Shell

Verb	Function
`Disable`	Disables the specified Exchange object
`Enable`	Enables the specified Exchange object
`Get`	Retrieves information about an object
`Move`	Moves an object from one container to another
`New`	Creates a new object
`Remove`	Deletes an object
`Set`	Modifies the properties of an object

Obviously, you can't do too much with just a verb and a noun. For example, the cmdlet `Get-MailboxServer` doesn't provide enough information for the shell to do anything. You need to specify which Mailbox server and likely what information you want to get. You provide this extra information through parameters. Parameters provide information to the cmdlet, either identifying an object and its attributes to act on, or controlling how the cmdlet performs its task.

To use a parameter, type a space following the verb-noun pair and then type the parameters you need. The name of the parameter is always preceded by a hyphen (-) and the use of parameters follows this syntax:

```
Verb-Noun –ParameterName <ParameterValue>
```

For example, to get information about a specific Mailbox server (say, a server named contoso-exsrv1), add the identity parameter to the cmdlet, like this:

```
Get-MailboxServer –Identity contoso-exsrv1
```

More Info You can find a complete reference of cmdlets including parameters available in the Exchange Management Shell in the Exchange Server 2007 Help files. The cmdlets used to perform various activities are included throughout this book.

Getting Help

Obviously, it is difficult to remember all the verbs, nouns, and parameters available in the Exchange Management Shell. Fortunately, there are several ways to get help right within the shell.

Help Cmdlets

Three help cmdlets are available in the shell to help you find the information you need to perform tasks: `Get-Help`, `Get-Command`, and `Get-ExCommand`.

When you use the `Get-Help` command by itself (that is, when you type no parameters with it), the shell provides basic information about using the shell, as shown in Figure 10-11.

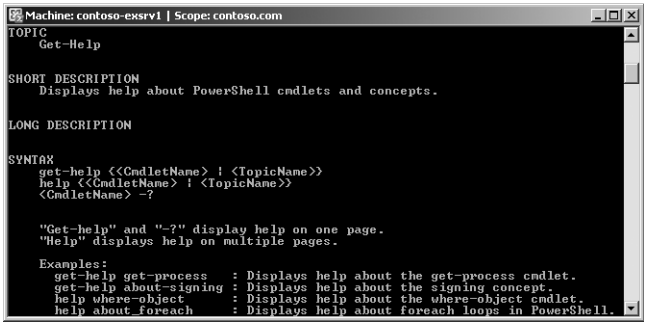


Figure 10-11 Getting help in the Exchange Management Shell

You can also use several parameters along with the `Get-Help` cmdlet to get more focused help on the task you're trying to perform. For example, you can use the name of a cmdlet as a parameter to get help on using that cmdlet. Typing the following gives you help on using the `Get-MailboxServer` cmdlet:

```
Get-Help Get-MailboxServer
```

You can even go a step further by adding additional parameters to further narrow the help you receive. Following the `Get-Help <cmdlet>` syntax, you can add the following parameters:

- **Get-Help <cmdlet> -Full** Provides full help on the specified cmdlet.

- **Get-Help <cmdlet> -Parameter <parametername>** Provides just the help view for the specific parameter of the cmdlet you name.
- **Get-Help <cmdlet> -Examples** Provides just the examples portion of the help view for the cmdlet you name.

You can use the `Get-Command` cmdlet by itself (no parameters) to view a list of all commands available in the shell. You can also add `-noun` and `-verb` parameters to the `Get-Command <commandname>` syntax to view all cmdlets with the specified noun or verb.

Also, you can use the `Get-ExCommand` cmdlet to return all the cmdlets that are specific to Exchange Server 2007. Otherwise, the `Get-Excommand` cmdlet works just like the `Get-Command` cmdlet.

Tab Completion

Tab completion helps reduce typing when using the shell. When you have typed a partial cmdlet name, just press Tab, and the Exchange Management Shell completes the cmdlet name if it finds a matching cmdlet. If it finds multiple matching cmdlets, the shell cycles through each cmdlet name as you keep pressing Tab. When you use tab completion with cmdlet names, you must supply at least the verb and the hyphen (-).

For example, you can use Tab completion to quickly view the nouns associated with the get verb. Just type `Get-` at the prompt and then keep pressing Tab to cycle through the available nouns you can use with `get`.

For another example, if you cannot remember (or just didn't want to type) a full cmdlet such as `Get-MailboxServer`, you can type `Get-Mail` and press Tab to find the correct cmdlet without having to type the full name.

Summary

This chapter provided a basic introduction to the tools used to administer an Exchange Server 2007 organization. The primary tool you use to administer Microsoft Exchange Server 2007 is the Exchange Management Console, which provides a graphical environment for configuring the various services and components of an Exchange organization. Exchange Server 2007 also features the new Exchange Management Shell, a powerful command-line interface for managing an Exchange organization. Chapter 11 begins a series of chapters that look at specific aspects of Exchange administration. In it, you learn how to create and manage the basic Exchange recipients.

Chapter 19

Exchange Server Security Basics

Security incidents, including hacking, virus attacks, spyware outbreaks, and identity theft, have rocked the computing world. Due to the e-mail server's reliance on access to the outside world, e-mail has become a target for miscreants everywhere, who try to use this medium to gain access to an organization. As such, security has become so central to the administrator's role that a large portion of this book is devoted to a discussion of it.

This chapter offers ideas about how to add complexity and create hindrances to those who wish to attack your network over port 25. It is never foolproof, but the more you invest in security, the more secure your e-mail server will be. However, if you have good strategies in place and adequate tools to assist you, you can anticipate and thwart most attacks.

Real World **Think Globally When Diagnosing a Security Problem**

Recently, a U.S. firm with national visibility in its industry was attacked by a group based outside of the U.S. The attacking group used its Exchange server to send out spam messages (in its own language) to addresses all over the world. At first, this

problem looked like a virus, but then the company realized the attackers had planted a program on the Exchange server that was launching the outgoing e-mails.

By the time the firm figured out the problem, outbound SMTP queues had nearly 100,000 messages sitting in them, ready to be sent. Besides the obvious concern that the people receiving the spam would be unhappy, there were also a multitude of other negative possible consequences that could have occurred as a result of this problem:

- **A tarnished reputation** By "allowing" this activity to take place, the company proved to those that received the spam that inadequate security measures were being taken. Whether this statement actually reflected reality would be a moot point to those whose perceptions of this company changed.
- **Lawsuits** By sending out spam, the company opened itself up to lawsuits that could prove to be costly and further harm the company's reputation.

The Scope of Security

Everyone has heard the old phrase "a chain is only as strong as its weakest link." You can easily apply that thinking to security: a network is only as secure as its least secured component. Always consider e-mail to be one of those weak links on your network because it is an obvious entry point. Attackers use e-mail to wreak havoc because it's easy: no matter how well you secure your network, chances are good that you have port 25 open on your firewall and that a Simple Mail Transport Protocol (SMTP) server is ready to work with e-mail when it comes in.

When you begin thinking about security strategies, always answer the following question: What am I securing Exchange Server 2007 against? The answers to this question are varied and can be grouped into four categories:

- Protection against social engineering attempts
- Physical security
- Administrative security
- SMTP security

You learned about social engineering in depth in Chapter 18, "Security Policies and Exchange Server 2007." In this chapter, the other three security categories are covered.

Motivations of a Criminal Hacker

Although a lot of literature has been written about the technical aspects of securing a network, not much is available about who your enemies are and what motivates them to attack. Before you can determine how to protect your organization, you must learn to think like a hacker, figure out where you're vulnerable, and then develop a game plan to reduce your exposure. If you can understand who would want to do you harm and what can be gained from such harm, you can better protect your company and your information. Make the following assumptions:

- You do have professional adversaries.
- You are on their target list.
- You will be attacked some day.
- You cannot afford to be complacent.

One of the most difficult realities for an organization to accept is the presence of adversaries who might attempt to harm it by using technology. It's also possible that you really do not have adversaries in this traditional sense. Today, attackers look for any system that has an exploitable weakness that they can turn to their advantage. Often, attackers look at weakly secured systems as bases from which to launch more sophisticated attacks.

The motivations of attackers can be varied and complex. Hackers are often motivated, in part, by their invisibleness. Today's more sophisticated hackers are often also motivated by prospect of a big payday. On the Internet, a hacker can "peek" into a company's private world—its network—and learn a lot while remaining anonymous.

Some individuals are just curious to see what they can learn about your company or individuals within your company. These hackers, sometimes referred to as "script kiddies," often don't have any malicious intent and are unaware that their actions violate security policy or criminal codes. That does not mean that these "casual hackers" are any less dangerous, however.

Others hackers are simply trying to help. You've probably been in this category once or twice yourself. In your zeal to be helpful, you bypass security policies to fix problems or accomplish emergency assignments. You might even believe that your efforts are more efficient than following established guidelines and policies. Nevertheless, the bypassing of known security policies is one element of hacking a network.

Some individuals act with malicious intent, engaging in acts of sabotage, espionage, or other criminal activities. They can become moles, stealing information to sell to competitors or foreign groups. Some simply enjoy destroying the work of others as well as their own work. Others act out of revenge for a real or perceived wrong committed against

them, or believe they are acting in line with a strongly held belief system. Still others are more methodical and hardened and turn hacking into a career: they might even take employment just to do your company harm.

How Hackers Work

Hackers start by learning that an e-mail server exists, which generic scanning tools can tell them. Coupled with the public information of your Domain Name System (DNS) records, hackers can quickly know a lot about your network.

Finding company information is easy for anyone. You can do it. Simply open a command prompt and type **nslook**. Set the type of the record you're looking for to a mail exchanger (MX) record by typing **set type=mx**. Type a domain name. This example uses Microsoft .com. Figure 19-1 shows the results.

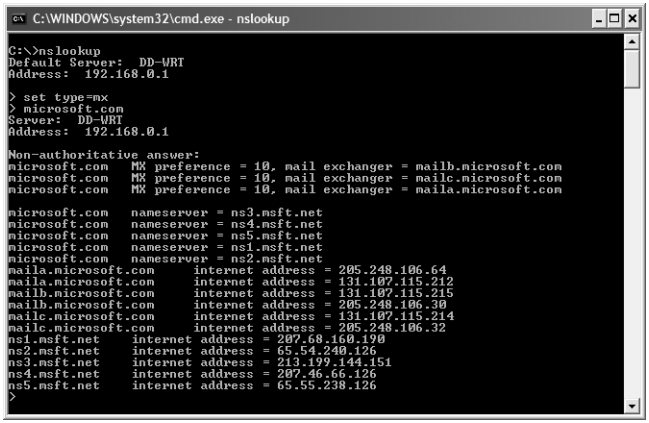


Figure 19-1 Using the NSLookup tool to find the public MX records for Microsoft.com

Next, the hacker determines the platform of your SMTP server in one of two ways. In the first approach, the hacker can use Telnet to open a session to your server over port 25 and then read the banner. Under Exchange Server 2007, the banner no longer identifies the version of Exchange Server being run, but does still indicate that the server is running the Microsoft ESMTP service. By removing the version number, Microsoft makes it harder for hackers to determine the exact version of Exchange that you are using. Note, Exchange Server 2007 is the only version that, by default, lacks this identifying information. However, a hacker can still figure out what he wants to know. It will take a couple of service packs and another major version of Exchange before this default omission really begins to bear fruit. Figure 19-2 gives you a look at an ESMTP conversation that takes place with an Exchange Server 2007 server.

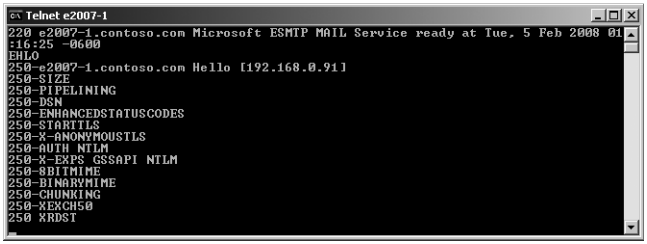


Figure 19-2 Opening a Telnet session to a server running Exchange Server 2007

Under older versions of Exchange Server, the exact version of the Exchange server being run is displayed (see Figure 19-3). The main version number, 6.0, means Exchange Server 2003. An Exchange 2000 Server registers with a main version number of 5.0. A SendMail server has its name and the version of SendMail software used by the company displayed in the header as well as the operating system (OS). Using this kind of information, a hacker can target his efforts by looking for exploits that will work for your specific system.

Figure 19-3 Opening a Telnet session to a server running Exchange Server 2003

> **More Info** Although Exchange Server 2007 is the first version of Exchange Server that, by default, does not display versioning information in a telnet window, you can manually configure older versions of Exchange Server to act the same way. Refer to *http://technet.microsoft.com/en-us/library/bb124740.aspx* for more information.

The second way to determine your e-mail server platform is to send a bogus e-mail to your server. This is accomplished by sending a message to an unlikely e-mail address such as pancake@contoso.com. The nondelivery report (NDR) that is returned has the e-mail server information located somewhere in the NDR. The following sample is a message header sent to the lab Exchange server at contoso.com. Notice that the Exchange server version is included right in the NDR's Sent by line:

```
Delivery has failed to these recipients or distribution lists:
 pancake@contoso.com
The recipient's e-mail address was not found in the recipient's e-mail system.
Microsoft Exchange will not try to redeliver this message for you.
Please check the e-mail address and try resending this message, or provide the
following diagnostic text to your system administrator.
--------------------------------------------------------------------------------
Sent by Microsoft Exchange Server 2007
Diagnostic information for administrators:
Generating server: e2007-1.contoso.com
pancake@contoso.com
#550 5.1.1 RESOLVER.ADR.RecipNotFound; not found ##
Original message headers:
Received: from e2007-1.contoso.com ([192.168.0.91]) by e2007-1.contoso.com
 ([192.168.0.91]) with mapi; Tue, 5 Feb 2008 01:25:12 -0600
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Cat Francis <cat.francis@contoso.com>
To: "pancake@contoso.com" <pancake@contoso.com>
Date: Tue, 5 Feb 2008 01:25:06 -0600
Subject: Test
Thread-Topic: Test
Thread-Index: AQHIZ8g79IUM/OhzKk2PKwL9+dATWg==
Message-ID: <1772808B96DEC14094F0236A00882DD7A43089@e2007-1.contoso.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator: <1772808B96DEC14094F0236A00882DD7A43089@e2007-
1.contoso.com>
MIME-Version: 1.0
```

Note that, even with Service Pack 1 installed, NDR messages still report just Exchange Server 2007 as the server version. By looking at just the NDR, there is no indication that SP1 is deployed on the server.

Now that the hacker knows which e-mail server software you run, he or she checks known databases to find vulnerabilities to exploit. The known vulnerabilities for Exchange Server 2007 are listed in Microsoft's Security Bulletins and can be found at *www.microsoft.com/security/default.mspx*. On older versions of Exchange, some of the vulnerabilities could involve Microsoft Internet Information Services (IIS) because IIS managed the SMTP service for Exchange. In Exchange Server 2007, SMTP is a core part of Exchange itself, which helps to reduce the attack potential on your server. Other vulnerabilities may involve Microsoft Outlook Web Access (OWA), again because of the involvement of IIS managing the HTTP connectivity to the Exchange server. At a minimum, be aware of any vulnerabilities that exist for Exchange Server 2007 and test and install the updates when they are released.

Generally speaking, the e-mail administrator can expect the following kinds of attacks:

- **Buffer overflows** Buffer overflows send a larger quantity of data to the server than is anticipated. Depending on how the overflow is executed, it could cause the server to stop working or it might run malicious code from the attacker.
- **Data processing errors** These are not common currently, but the concept is that a small program is sent directly to the server and the server runs it. More common today is sending these programs to a network though e-mail as attachments. Depending on their function and purpose, these programs can be viruses, Trojans, or worms (discussed at length later in this chapter).
- **HTML viruses** These do not require user intervention to run unattended scripts.
- **Custom programs written to run against port 25 (SMTP)** The more common types of programs that attack port 25 include e-mail flooding programs or programs that contain their own SMTP engine that use the port for their own malicious purposes.
- **Denial of Service (DoS)** A Denial of Service attack is an attack on a network that is undertaken in an effort to disrupt the services provided by a network or server.
- **Cross-site scripting** Cross-site scripting is a vulnerability whereby an attacker places malicious code into a link that appears to be from a trusted source.
- **Spam and phishing expeditions** Spam, or junk mail, is a well-known e-mail malady and affects just about everyone that uses the communication medium. A particular type of spam, called a phishing e-mail, attempts to lure unsuspecting users into clicking on unsafe web links. These links point to web forms that ask the user to provide sensitive personal information.

Here are some broad actions you can take to guard against the attacks just described, plus others:

- **Physical access to the server** Lock the doors, and use some type of biotech authentication.
- **Viruses, Trojans, and worms** Use antivirus software and regularly scan your servers and workstations. Use the Exchange Server 2007 Edge Transport server role on at least one Exchange server.
- **Loss of data** Perform regular backups.
- **Unauthorized use of user accounts** Conduct user training on information security policies and require complex passwords.
- **Denial of Service attack** Harden the TCP/IP stack and the router.
- **Platform vulnerabilities** Install all software patches and engage in service that offers minimization. Microsoft has released excellent free software for updating its patches on your servers. This software is called Windows Server Update Services (WSUS).

More Info A discussion of WSUS is outside the scope of this chapter, but you can learn more about WSUS on Microsoft's Web site at *http://www.microsoft.com/windowsserversystem/updateservices/default.mspx*

As is the case with Windows Server 2003, WSUS is not installed by default on Windows Server 2008, but is still available as a free download.

The rest of this chapter is intended to help you secure Exchange Server 2007 against these types of attacks. However, a brief discussion of physical security of your Exchange server is in order.

Physical Security

Physical security is a topic not often mentioned in many security books, particularly in books only about Exchange, but it is a topic worth mentioning. Servers can be left on desks running in a corner cubicle or in an unlocked server room. However, it is always best practice to store your servers in a secure location using door locks and, in some instances, motion detectors and/or other physical security measures.

When you limit physical access to a server, you limit who can log on locally to the server, who can use portable storage to introduce a new virus or malicious program on your network, and who can retrieve information directly from the server. Limiting physical access is one of the easiest and most elementary methods of securing your server against internal attacks that exist.

Most administrators reading this book already have these physical security measures in place. Those who haven't physically secured your servers should do so at their earliest opportunity. Limiting physical access to a server can go a long way toward protecting your information from would-be attackers.

Administrative Security

In previous versions of this book, this section talked extensively about the use of administrative groups as a way to achieve some semblance of administrative security for your Exchange organization. In Exchange Server 2007, however, Microsoft has mostly done away with administrative groups, leaving only a single administrative group named Exchange Administrative Group (FYDIBOHF23SPDLT) in which only Exchange Server 2007 servers reside. This administrative group is present only to support coexistence with legacy Exchange servers.

Note The name of the Exchange administrative group, Exchange Administrative Group (FYDIBOHF23SPDLT), is pretty convoluted. Likewise, Exchange Server

2007's legacy routing group, named Exchange Routing Group (DWBGZMFD01QNBJR), is also fairly convoluted. Have you wondered at all why Microsoft chose these particular names? First, Microsoft had to be careful that it didn't choose a name that already exists in a customer's legacy Exchange organization. Second, the Exchange team decided that a little creativity was in order. Look carefully at the two names. Both have the same number of characters with each letter and number occupying the same positions. To make a long story short, if you look at the administrative group's name, you find you can go to the previous letter (or number) in the alphabet for each character in the name and spell "EXCHANGE12ROCKS." Likewise, for the routing group, go to the next letter of the alphabet for each letter in the routing group name and you also get "EXCHANGE12ROCKS." It's really nice to see the product team having so much fun with a product that is generally considered all business!

Why did the Exchange team eliminate administrative groups from the Exchange equation? With the complete overhaul of the management interface and its new "area of responsibility" focus, administrative groups simply aren't necessary and can add to the overall complexity of managing Exchange. Figure 19-4 gives you a side-by-side look at the legacy Exchange System Manager and the Exchange Server 2007 Exchange Management console. With their absence in Exchange Server 2007, you need to use a way other than administrative groups to achieve administrative security. In this section, you learn two methods by which you can add users to act in various Exchange administrative capacities.

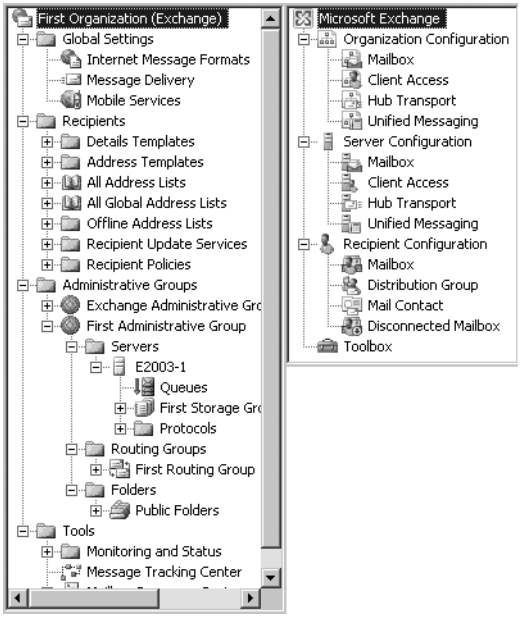


Figure 19-4 The Exchange Server 2003 Exchange System Manager is on the left and the Exchange Server 2007 Exchange Management Console is on the right.

The Built-in Exchange Administrative Groups

When you run the initial installation of Exchange Server 2007, six Active Directory universal security groups are created, each with specific rights to various parts of the Exchange organization. Five of the six groups, shown in Figure 19-5 inside Active Directory Users And Computers, pertain directly to management of the Exchange organization and are as follows:

- **Exchange View-Only Administrators** This role allows you to view configurations on all Exchange objects, but not to make any changes to those configurations.
- **Exchange Servers** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of this group have access to server-based Exchange configuration information and to the Active Directory objects that are server-related.
  - Members of this group may perform server-based administration, but cannot perform operations at the global Exchange organization level.
  - Members of this group are also members of the local Administrators group on each server on which Exchange Server 2007 is installed.
- **Exchange Recipient Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of the group are also allowed to configure any object related to recipients and public folders, including contacts, groups, public folder objects, Unified Messaging mailbox settings, Client Access mailbox settings, and any other recipient Exchange property found in Active Directory.
- **Exchange Public Folder Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of this group are also allowed to manage public folders.
- **Exchange Organization Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange Recipient Administrators, plus more.
  - Members of this group also have all of the rights of Exchange Public Folder Administrators.

- Users assigned to this group are allowed to view and administer all aspects of the Exchange organization, including servers, recipients, public folders, and organizational configuration.
- Members of the role are considered the owners of all Exchange-related Active Directory objects.
- During Exchange Server 2007 installation, this group is added to the membership of the server's local Administrators group. If you install Exchange Server 2007 on a domain controller, which is not recommended, Exchange Organization Administrators have additional rights by virtue of the local Administrators group having more rights on a domain controller.

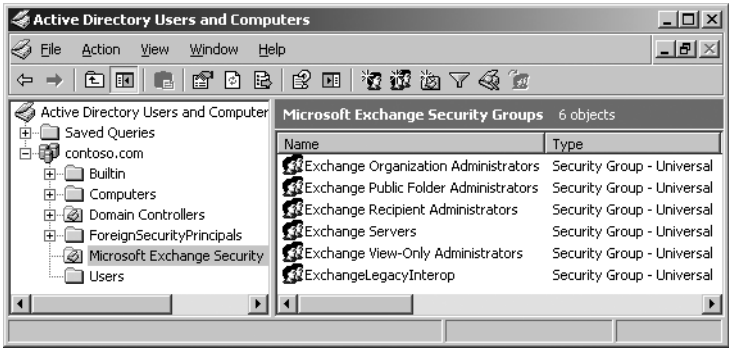


Figure 19-5 The Exchange Server 2007 built-in security groups

If you want to add a full Exchange administrator to your organization, all you have to do is add the appropriate user account to the Exchange Organization Administrators group. The same holds true for the other security groups.

The Add Exchange Administrator Wizard

Exchange Server 2007 also provides an easy way to add additional Exchange administrators with each administrator role having responsibility for only a specific part of the Exchange organization, such as a single server, a group of servers, or only able to manage recipients. You will find that this administrative delegation method is far more flexible and effective than administrative groups were in the past.

The best way to demonstrate how the Add Exchange Administrator operation works is to see it in action. To start the process, open the Exchange Management Console and select the Organization Configuration option, as shown in Figure 19-6.

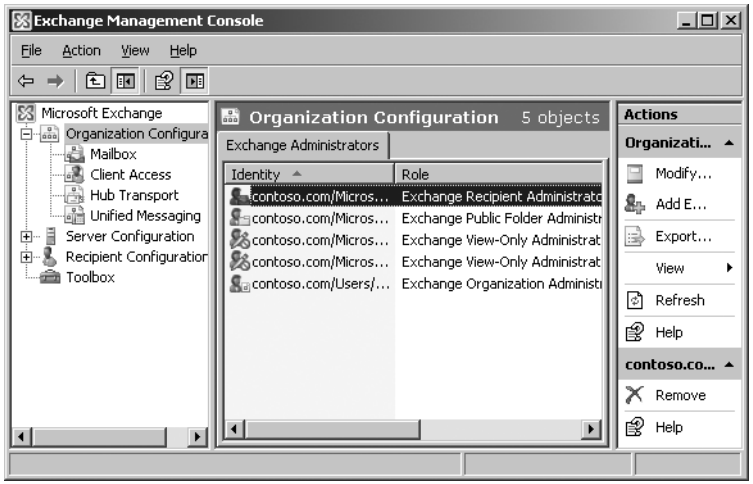


Figure 19-6 The Organization Configuration window

Note that the work pane shown in Figure 19-6 shows you the groups that already have some level of permission to the Exchange organization. To add additional Exchange administrators, from the Action pane, choose Add Exchange Administrator. This selection displays a one-page wizard, shown in Figure 19-7.

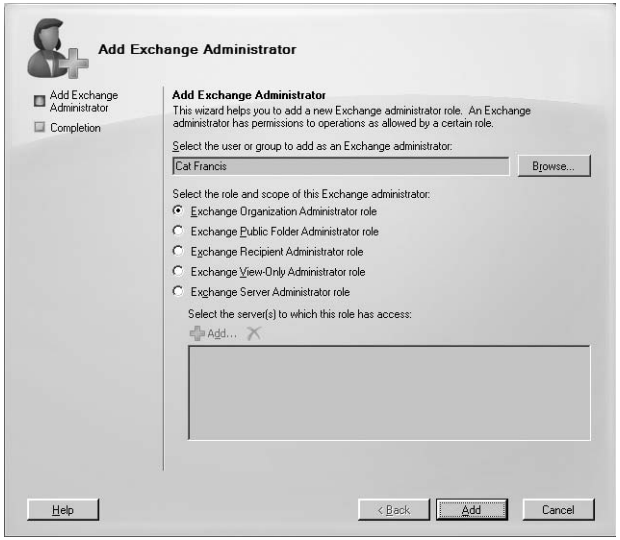


Figure 19-7 The Add Exchange Administrator Wizard

There are three selections that you must make in order to complete this wizard.

First, select the user or group to which you want to grant Exchange administrative rights. Next, select the role and scope that should apply to the new Exchange administrator. Finally, if you've selected the Exchange Server Administrator role, select at least one server to which this new user or group has access. Click Add, and from the Select Exchange Server window, choose the desired servers. Figure 19-8 shows what the screen looks like after you select the Exchange Server Administrator role and add a managed server.

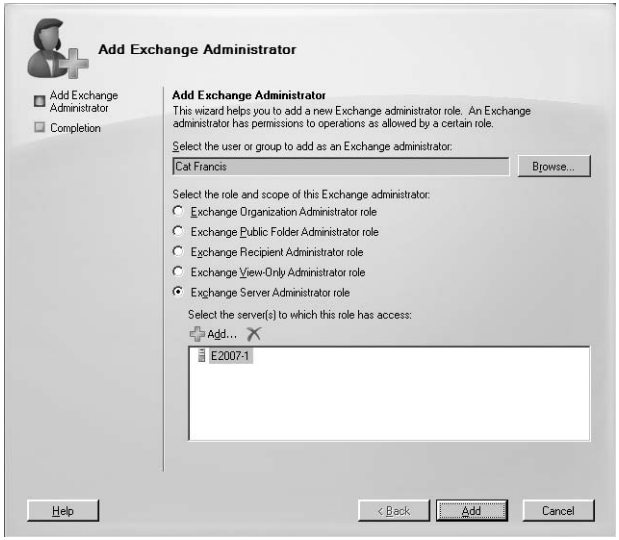


Figure 19-8 Selecting the Exchange Server Administrator role

> **Note** When you add someone to the Exchange Server Administrator role, you must manually add that user or group to each managed server's local Administrators group.

In reality, when you run the Add Exchange Administrator operation, the resulting command simply adds the selected users to one of the groups that you learned about in the section "The Built-in Exchange Administrative Groups." The only role for which this does not hold true is for the Exchange Server Administrator role. When users or groups are assigned to this role, the user or group is assigned Full Control permission on the specified server object and all child objects.

Management Shell

Adding additional users or groups to manage your Exchange organization in Exchange Server 2007 is a whole lot easier than it ever was in previous versions of Exchange Server. During the initial Exchange Server 2007 installation, a number of universal security groups are created. Each of these groups corresponds to security roles that can be granted in Exchange Server 2007 and are listed here:

- **Exchange View-Only Administrators** This role allows you to view configurations on all Exchange objects, but not to make any changes to those configurations.
- **Exchange Servers** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of this group have access to server-based Exchange configuration information and to the Active Directory objects that are server-related.
  - Members of this group may perform server-based administration, but cannot perform operations at the global Exchange organization level.
  - Members of this group are also members of the local Administrators group on each server on which Exchange Server 2007 is installed.
- **Exchange Recipient Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of the group are also allowed to configure any object related to recipients and public folders, including contacts, groups, public folder objects, Unified Messaging mailbox settings, Client Access mailbox settings, and any other recipient Exchange property found in Active Directory.
- **Exchange Public Folder Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of this group are also allowed to manage public folders.
- **Exchange Organization Administrators** This role provides the following rights:

- Members of this group have all of the rights of Exchange Recipient Administrators, plus more.
- Members of this group also have all of the rights of Exchange Public Folder Administrators.
- Users assigned to this group are allowed to view and administer all aspects of the Exchange organization, including servers, recipients, public folders, and organizational configuration.
- Members of the role are considered the owners of all Exchange-related Active Directory objects.
- During Exchange Server 2007 installation, this group is added to the membership of the server's local Administrators group. If you install Exchange Server 2007 on a domain controller, which is not recommended, Exchange Organization Administrators will have additional rights by virtue of the local Administrators group having more rights on a domain controller.

The following command adds a user account that can manage the Exchange Server 2007 server named E2007-4:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
   -Role 'ServerAdmin' -Scope 'E2007-4'
```

If you add someone using Exchange Server Administrator role, you need to manually add the selected user or group to the built-in local administrators group on the target server.

This command adds a user to the Exchange Recipient Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
   -Role 'RecipientAdmin'
```

This command adds a user to the Exchange View-Only Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
   -Role 'ViewOnlyAdmin'
```

This command adds a user to the Exchange Organization Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
   -Role 'OrgAdmin'
```

This command adds a user to the Exchange Public Folder Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
   -Role 'PublicFolderAdmin'
```

Table 19-1 comes from Microsoft's documentation on the role of roles in Exchange Server 2007 and provides a concise look at exactly what each administrative role accomplishes.

Table 19-1 Exchange Server Administrative Roles

Role	Members	Member of	Exchange permissions
Exchange Organization Administrators	Administrator, or the account that was used to install the first Exchange 2007 server	Exchange Recipient Administrator, Administrators local group of *<Server Name>*	Full control of the Microsoft Exchange container in Active Directory
Exchange Recipient Administrators	Exchange Organization Administrators	Exchange View-Only Administrators	Full control of Exchange properties on Active Directory user object
Exchange Server Administrators		Exchange View-Only Administrators, Administrators local group of *<Server Name>*	Full control of Exchange *<Server Name>*
Exchange View-Only Administrators	Exchange Recipient Administrators, Exchange Public Folder Administrators	Exchange Recipient Administrators, Exchange Server Administrators	Read access to the Microsoft Exchange container in Active Directory. Read access to all the Windows domains that have Exchange recipients.
Exchange Public Folder Administrators	Exchange Organization Administrators	Exchange View-Only Administrators	Ability to administratively manage public folders.

SMTP Security

By default, an SMTP server attempts to make a TCP port 25 connection to your Exchange server via an anonymous connection. Anonymous does not mean that a user account set up in your Active Directory proxies the connection request, as is the case with the IIS Anonymous user account, IUSR_*<machinename>*. In the SMTP world, anonymous means that no user name or password is required for the remote SMTP service to make a port 25 connection. Hence, any SMTP server on the Internet can make, by default, a port 25 connection to your Exchange server.

To make SMTP more secure, you could require either Basic or Integrated Windows Authentication (IWA) before the SMTP Virtual Server (VS) could accept an inbound connection. But this configuration isn't practical on the Internet because you can't predict

who will be connecting to your Exchange server in the future and thus can't assume that the user has an appropriate user name and password to make a connection. Moreover, not many messaging administrators are interested in implementing such a security measure at their end. So even though an anonymous connection to port 25 on your Exchange server represents a vulnerability, it is one that must be managed using a different approach than removing anonymous connections.

How do you protect against these kinds of attacks? With Exchange Server 2007, you can use an Edge Transport server that offloads the security burden from your primary Exchange servers. You learn about implementing the Edge Transport server in Chapter 20, "Antivirus and Anti-spam." This chapter also discusses how the Edge Transport server can help improve the overall security of your Exchange infrastructure. However, more traditional ways of protecting Exchange also apply even when Edge Transport servers are used.

Perhaps the most common way to protect an Exchange infrastructure is through the use of two firewalls. A dual firewall topology allows you to protect your internal Exchange servers while also filtering incoming e-mail against potential attacks. The area between the two firewalls is called the *perimeter network*. The philosophy is to put up a line of defense against potential attacks. Hence, you're willing to sacrifice your Exchange servers in the perimeter network, but not willing to sacrifice your Exchange servers on the internal network. Because the Exchange servers in the perimeter network do not host any important information—no mailboxes or public folders—they can be both sacrificed during an attack and easily rebuilt. And because they act only as relay servers, they can be used to sanitize incoming e-mail over port 25.

Take a look at Figure 19-9. Note that there are three network levels. Starting from the top, each network becomes more trusted, with the External, or Internet, zone being completely untrusted. The Perimeter network is more trusted as it resides behind at least one organizational firewall and generally houses servers that can be considered "expendable." In this diagram, the external firewall has port 25 open in order to facilitate incoming SMTP traffic. Mail is routed to the Exchange Server 2007 Edge Transport server where it is processed for viruses, checked using various spam filters, and run through various incoming transport rules. Your external MX records must point to this Edge Transport server. There is another important note in this diagram. Note that the external firewall also provides the ability to scan incoming content for viruses and spyware. When possible, always run your e-mail through a similarly configured firewall even before that mail hits the Edge Transport server's content-scanning engines. Many of today's security appliances, such as the Cisco ASA and Sonicwall's family of firewalls, provide this additional protection.

From a software perspective, also consider running Microsoft Forefront Security for Exchange Server. Forefront has the ability to scan every incoming message with up to five completely separate virus scanners. By instituting this multilayer security infrastructure, all incoming mail is scanned by many different virus scanning engines, some hardware-

based and some software-based, which results in a much higher likelihood you will be protected against even the newest viruses.

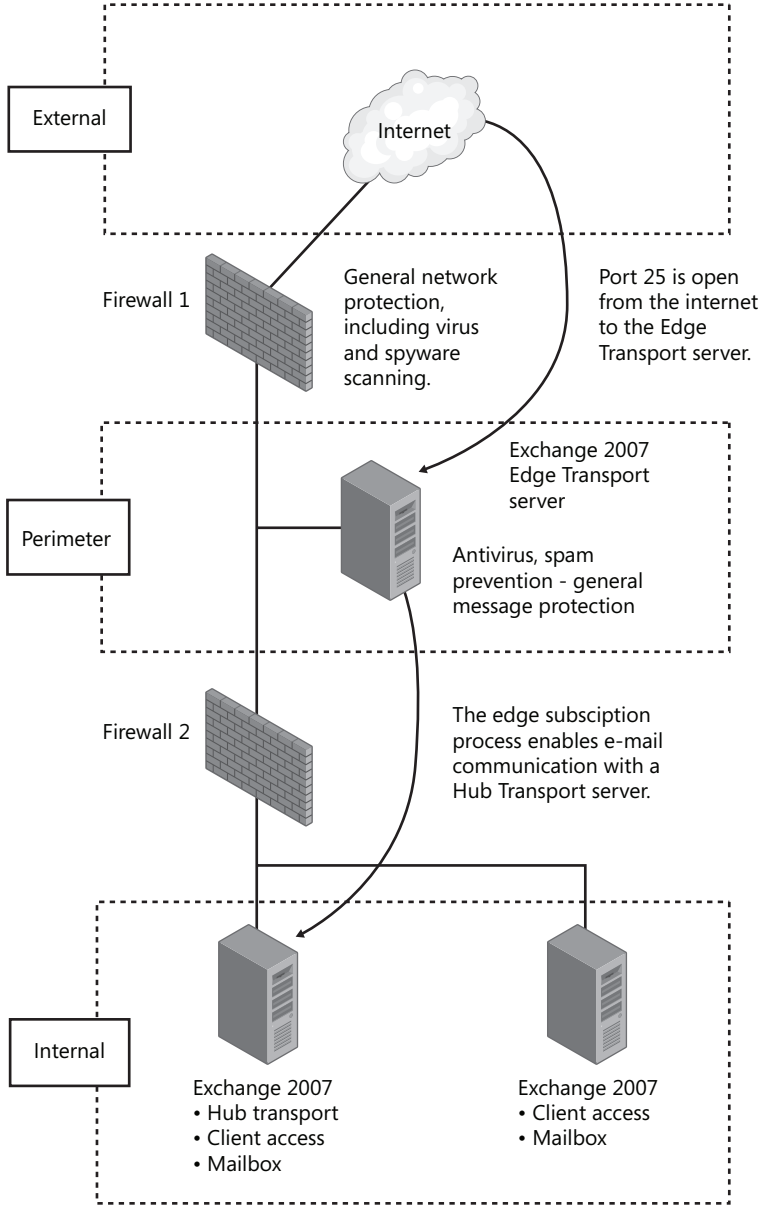


Figure 19-9 One way to secure your Exchange infrastructure

However, even the best virus-scanning infrastructure on the planet does not always protect you. Think back to some of the major viruses in the last few years, which were able to spread worldwide very quickly, usually in a matter of hours. It is almost impossible for any antivirus company to get the virus, study it, write a definition for it, and then push out the new definition for that virus before it spreads worldwide. You can tell an Edge Transport server, however, to quarantine or delete any message that contains certain types of attachments and, in effect, block most viruses based on their type of content rather than on a comparison to a virus definition file.essent.

Note Be aware of two issues regarding traditional antivirus servers. First, many products offered by the major antivirus vendors perform content scanning at the same time as the virus scanning. While there may be no problem with this method of scanning e-mail, be aware of a distinction between content scanning and antivirus scanning, which highlights the need to perform both types of scanning in the perimeter network, a capability enabled through the use of Exchange Server 2007's Edge Transport server. Second, everyone may not be able to afford to purchase everything required in order to achieve the configuration outlined in this chapter—namely, a separate Exchange server running Edge Transport as well as firewalls/security appliances that perform virus scanning functions. These ideas are presented to highlight the concepts being discussed. Other, less expensive (and potentially less secure) options include:

- Using a single firewall with multiple interfaces and creating a perimeter network using firewall rules
- Using a single firewall and running the Edge Transport server on the internal interface alongside your other Exchange servers
- Skipping the installation of the Edge Transport server and delivering mail directly to an internal Hub Transport server

Once scanned and approved, the e-mail is sent to an internal Hub Transport server. The internal Exchange Server 2007 Hub Transport server should be configured to accept inbound e-mail only from the perimeter network's Edge Transport server. Inbound mail that has been approved by the Edge Transport server also rides on the standard SMTP TCP port 25, so you need to open this port on your internal firewall as well. To do this in the most secure way possible, create a firewall rule that only allows port 25 traffic specifically between the Edge Transport server and one of your internal Hub Transport servers. Then, secure the communication tunnel using IPsec, which is discussed further in Chapter 21. The internal Exchange server should also be running its own antivirus software, preferably from a vendor that is different from the one the servers are using in the perimeter network. The whole point of implementing this model is to ensure that port 25 traffic is as well protected as possible.

In order to use an Edge Transport server, subscribe the Edge Transport server to the Active Directory domain. The subscription process establishes one-way replication of recipient and configuration information from your Active Directory into an Active Directory Application Mode (ADAM) instance running on your Edge Transport server. Further, the Edge Subscription process creates the SMTP Send connectors required to enable mail flow from your Exchange servers to the Internet through an Edge Transport server. If you are using the recipient lookup or safe list aggregation features of the Edge Transport server, subscribe the Edge Transport server to the organization.

More Info The complete process for installing, configuring, and subscribing the Edge Transport services is covered in Chapter 20, "Antivirus and Anti-spam."

No system is foolproof, but this dual firewall topology has multiple advantages:

- By passing incoming e-mail through the Edge Transport servers content filtering services, you filter for code types that virus scanners don't.
- By passing your e-mail through a virus scanner, you do your best to ensure that all known viruses are cleaned out. Not passing your e-mail through an updated antivirus scanner after running it through a content scanner is unwise because older viruses might not be caught by the content scanner.
- By passing all of your outgoing e-mail through the Exchange Server 2007 Edge Transport server, the IP address (private or public) of the internal Exchange Server 2007 server does not need to be published in the public DNS records. This means that an attacker attempting to Telnet into your server is never able to reach it directly. Also, if you configure the internal Exchange Server 2007 server to accept e-mail only from perimeter network–based Exchange servers, any attempts to make port 25 connections to the internal Exchange server from any other IP address will fail.

If a hacker decides to bring down your perimeter Exchange servers, you've really lost nothing of value other than your time in getting the servers functioning again. Your company might lose some money due to the inability to communicate via e-mail, but it hasn't lost any current data. This is an important point. The server that hosts your data is the one most protected. And the ones most exposed do not host important data. If those servers are lost, at least all the business-critical data is saved on the internal Exchange Server 2007 Server. For many companies, this is an acceptable level of risk to assume. This is the beginning stage of a defense that provides multiple layers of protection, starting with expendable services with the really important data protected in a variety of different ways.

As explained throughout this chapter, no answer is perfect, and this security scenario does have a few major holes, such as doing nothing to protect against messages sent to the Exchange server via Outlook Web Access. Port 25 is well protected but port 80 access to your Exchange server is wide open. If you want to learn more about OWA, refer to Chapter 24, "Supporting Outlook Web Access."

The second major hole in this model is one that cannot be plugged: messages are continuing to flow to your internal Exchange server. As long as a packet can reach your internal Exchange server, there is always the potential for harm. So remember the 80 percent rule: you can make your data only about 80 percent secure. But don't let that discourage you from implementing appropriate security strategies.

Computer Viruses

This section expands on computer viruses in general and discusses some implications for viruses on Exchange Server 2007.

What Is a Virus?

A *virus* is a piece of code that attaches itself to other programs or files. When these files run, the code is invoked and begins replicating itself. The replication occurs over the network. Viruses can now exploit the vulnerabilities of nearly every platform.

Some viruses reside in memory after the original program is shut down. When other programs are executed, the virus attaches itself to these new programs until the computer is shut down or turned off. Some viruses have a "dormant" phase and appear only at certain times or when certain actions are performed.

There are many types of viruses. Some overwrite existing code or data. Others include the ability to recognize whether an executable file is already infected. *Self-recognition* is required if the virus is to avoid multiple infections of a single executable, which can cause excessive growth in size of infected executables and corresponding excessive storage space, contributing to the detection of the virus.

Resident viruses install themselves as part of the operating system upon execution of an infected host program. The virus remains resident until the system is shut down. Once installed in memory, a resident virus is available to infect all suitable hosts that are accessed.

A *stealth virus* is a resident virus that attempts to evade detection by concealing its presence in infected files. For example, a stealth virus might remove the virus code from an executable when it is read (rather than executed) so that an antivirus software package sees only the noncompromised form of the executable.

Computer viruses can spread by the use of e-mail and usually appear in e-mail attachments. If the virus can find its way into the messaging stream, it uses the client capability to send and receive e-mail to replicate itself quickly and do its damage as fast as possible.

An essential aspect of protecting your messaging system against viruses is user education. Users should learn to be guarded about which attachments they are allowed to open. Your information security policies should also outline the types of e-mails and attachments that users are allowed to open. For example, users should be forbidden to open attachments in two instances: when they were not expecting the attachments, and when the attachments arrive from unrecognizable aliases.

Finally, whenever possible, consider a centralized antivirus service that updates the distributed clients from a centrally managed server. Most such solutions provide you with ways to more granularly manage each client and proactively fix problems that may take place.

Trojans

A *Trojan* (also known as a Trojan horse) is a malicious program embedded inside a normal, safe-looking program. The difference between a virus and a Trojan is that the Trojan is embedded and the virus is attached to the file or executable.

When the normal program runs, the malicious code runs as well and can cause damage or steal critical information. An example of a Trojan is a word-processing program that, when executed, allows the user to compose a document while, in the background, malicious code is running that deletes files or destroys other programs.

Trojans generally are spread through e-mail or *worms*, which are programs that run by themselves. The damage that Trojans can cause is similar to that of a virus: from nominal to critical. Trojans are particularly frightening because in most cases, users are unaware of the damage the Trojan is causing. The malicious work is being masked by the Trojan effect of the program.

Worms

As just mentioned, worms are programs that run by themselves. They do not embed or attach themselves to other programs nor do they need to do this to replicate. They can travel from computer to computer across network connections and are self-replicating. Worms might have portions of themselves running on many different computers, or the entire program might run on a single computer. Typically, worms do not change other programs, although they might carry other code that does.

The first network worms were intended to perform useful network management functions by taking advantage of operating system properties. Malicious worms exploit sys-

tem vulnerabilities for their own purposes. Release of a worm usually results in brief outbreaks, shutting down entire networks.

The damage that worms can cause, like Trojans and viruses, ranges from the nominal to the critical. The type and extent of damage must be assessed individually for each worm. However, worms can install viruses and Trojans that then run their own code.

An attack that combines a worm, Trojan, and/or virus can be a very difficult attack to survive without significant damage. The impact of viruses, Trojans, and worms on your messaging system and network should not be underestimated. Because they use e-mail to exploit system vulnerabilities, installing antivirus software is simply not enough. You must also ensure that known vulnerabilities in all your operating systems are updated. Don't focus only on your servers. Every device should be updated with the most recent updates from each vendor as soon as possible. Most environments will want to test these updates before installing them. But after they have been tested, install them.

Junk E-Mail

Junk e-mail is a huge issue. One client with whom this author recently worked installed its first e-mail filtering software and found that it had 46 percent fewer inbound e-mails.

Exchange Server 2007's new Edge Transport role has new capabilities that can help to significantly reduce the amount of junk e-mail that enters your environment. The Edge Transport role server has the following agents that help to protect your e-mail infrastructure. The information in Table 19-2 is right from Microsoft's Edge Transport server documentation.

Many of these features are discussed in the next chapter, Chapter 20, "Antivirus and Antispam," and Chapter 21, "Securing Exchange Server 2007 Messages."

Table 19-2 Edge Transport Agents

Agent name	Description
Connection Filtering Agent	Performs host IP address filtering based on IP Allow Lists, IP Allow List providers, IP Block Lists, and IP Block List providers.
Address Rewriting Inbound Agent	Modifies recipient SMTP addresses in inbound messages based on predefined address alias information. Address rewriting can be useful in scenarios where an organization wants to hide internal domains.
Edge Rule Agent	Processes all messages received over SMTP to enforce transport rules defined on the Edge Transport server.
Sender ID Agent	Determines whether the sending SMTP host is authorized to send messages for the SMTP domain of the message originator.

Table 19-2 Edge Transport Agents

Agent name	Description
Recipient Filter Agent	Verifies that the recipients specified during the SMTP session through the RCPT TO: command are valid and not on the list of blocked SMTP addresses and domains.
Sender Filter Agent	Verifies that the sender specified in the MAIL FROM: command and in the message header is valid and not on the list of blocked SMTP addresses and domains.
Content Filter Agent	Uses Microsoft SmartScreen technology to assess the contents of inbound messages in order to assign an SCL rating for junk e-mail processing based on transport and store thresholds.
Protocol Analysis Agent	Interacts with Connection Filtering, Sender Filtering, Recipient Filtering, and Sender ID agents to determine Sender Reputation Level (SRL) rating and to take action based on rating thresholds.
Attachment Filtering Agent	Filters messages based on attachment file name, file name extension, or MIME content type to block potentially harmful messages or remove critical attachments.
Address Rewriting Outbound Agent	Modifies sender SMTP addresses in outbound messages based on predefined address alias information. Address rewriting can be useful in scenarios where an organization wants to hide internal domains.
Forefront Security for Exchange Routing Agent	Responsible for connecting into the Transport stack to ensure that the scanning process scans messages prior to delivery to Hub Transport servers.

Security Tools Provided by Microsoft

In order to help you deploy and maintain the most secure Exchange infrastructure possible, Microsoft provides a number of tools designed to remove malware, make sure that your environment is properly configured, and help you configure a multitude of security settings.

- **Malicious Software Removal Tool** The Microsoft Windows Malicious Software Removal Tool checks computers running Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. On a regular basis, run the

Malicious Software Removal Tool on your Exchange server to make sure your system is free of threats.

> **More Info** To download the Microsoft Software Removal Tool, visit *http://www.microsoft.com/security/malwareremove/default.mspx*.

- **Microsoft Baseline Security Analyzer** The Microsoft Baseline Security Analyzer (MBSA) is a tool that analyzes your existing environment and, in particular, analyzes how you have configured a number of Microsoft products, including Windows 2000 SP3; Windows XP and Windows Server 2003; Office XP, 2003 and 2007; Exchange 2000, 2003 and 2007; SQL Server 2000 SP4; and SQL Server 2005. With this information, Microsoft compares your configuration against a list of best practices and provides you with a report of action items that you can take to improve the security of your environment.

> **More Info** To download the Microsoft Baseline Security Analyzer, visit *http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx*.

- **Security Configuration Wizard** Windows Server 2003 Service Pack 1 includes the Security Configuration Wizard (SCW), a tool designed to reduce the attack surface of your Windows servers. SCW helps administrators to create security policies that are consistent with the practice of least privilege. In this case, that means running the fewest possible services on a server in order to reduce the number of services that can be used to attack the computer.
- **Microsoft Exchange 2007 Anti-Spam Migration Tool** The Exchange 2007 Anti-Spam Migration Tool is designed to ease the administrative burden involved in transitioning from Exchange Server 2003 to Exchange Server 2007, particularly for those administrators who have deployed Exchange Server 2003 anti-spam services and want to maintain the service configuration under Exchange Server 2007. This tool converts the Exchange Server 2003 anti-spam service settings into PowerShell commands that can be used to appropriately configure anti-spam service settings in Exchange Server 2007

> **More Info** To download the Microsoft Exchange 2007 Anti-Spam Migration Tool, visit *http://www.microsoft.com/downloads/details.aspx?FamilyId=805EAF35-EBB3-43D4-83E4-A4CCC7D88C10&displaylang=en*.
>
> This tool is not available for use on Windows Server 2008.

Summary

This chapter discussed how hackers think, how to secure incoming SMTP e-mail, and how to secure Administrator access to your Exchange server. Also discussed were the differences between a virus, a Trojan, and a worm, and a method was outlined for securing inbound SMTP traffic. Two other areas in this book were also referenced that discuss sender filtering and securing OWA. The next chapter discusses how to secure e-mail messages using encryption and certificates.

Index

D

E

F

J

K

L

M

P

Q

R

S

T

U

V

W

X