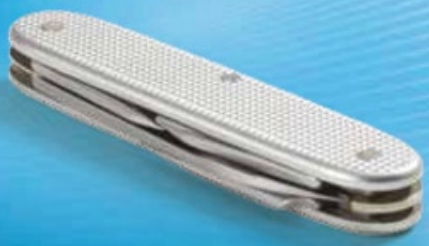
Microsoft

Microsoft®

Exchange Server 2010



William R. Stanek
Author and Series Editor

Administrator's Pocket Consultant

Sample Chapters

To learn more about this book visit Microsoft Learning at:
http://www.microsoft.com/learning/en/us/training/format-books.aspx

Contents

CHAPTER 1

Exchange Server 2010 Administration Overview

If you thought Microsoft Exchange Server 2007 was a radical departure from its predecessors, wait till you get acquainted with Microsoft Exchange Server 2010. Exchange Server 2010 completely redefines the Exchange Server messaging platform, and right up front you should know that Exchange Server 2010 does away with the concepts of storage groups, Local Continuous Replication (LCR), Single Copy Clusters (SCC), and clustered mailbox servers.

In previous releases of Exchange Server, you used storage groups to group mailbox and public folder databases into logical units of management. In Exchange Server 2010, databases are no longer associated with storage groups. For mailbox databases, database availability groups can now be used to group databases for high availability, and mailbox databases are managed at the organization level instead of at the server level. For public folder databases, database management has been moved to the organization level, but the functionality hasn't changed from how it was implemented in Exchange Server 2007.

To support these and other changes, relevant storage group functionality has been moved to the database level. Further, mailbox databases are now peers to servers in Active Directory. The Exchange store schema has been changed to remove the dependency of mailbox databases on server objects, and this reduces the Exchange store's reliance on secondary indexes maintained by the Extensible Storage Engine (ESE).

Exchange Server 2010 integrates high availability into the core architecture by enhancing aspects of Cluster Continuous Replication (CCR) and Standby Continuous Replication (SCR) and combining them into a single high-availability solution for both on-site and off-site data replication. Exchange Server 2010 also provides for automatic failover and recovery without requiring clusters when you deploy multiple mailbox servers. Because of these changes, building a high-availability mailbox server solution no longer requires cluster hardware or advanced cluster configuration. Instead, database availability groups provide the base component for high availability. Failover is automatic for mailbox databases that are part of the same database availability group.

The rules for database availability groups are simple. Each mailbox server can have multiple databases, and each database can have as many as 16 copies. A single database availability group can have up to 16 mailbox servers that provide automatic database-level recovery. Any server in a database availability group can host a copy of a mailbox database from any other server in the database availability group.

This seamless high-availability functionality is made possible because Exchange Server 2010 disconnects mailbox databases from servers and assigns the same globally unique identifier (GUID) to all copies of a mailbox database. Because storage groups no longer exist, continuous replication occurs at the database level. Transaction logs are replicated to each member of a database availability group that has a copy of a mailbox database and are replayed into the copy of the mailbox database. Failover can occur at either the database level or the server level.

Although I discuss the architectural and administrative impact of these extensive changes throughout this and other chapters of this book, you need to know this information up front because it radically changes the way you implement and manage your Exchange organization. Why? With these changes, you might not need to use Redundant Arrays Of Inexpensive Disks (RAID) for your Exchange data and you might not need to ever perform routine backups of your Exchange data. Although these are radical ideas, they are possible—especially if you implement data-retention rules as necessary for regulatory compliance and remember to rotate Exchange data to off-site storage periodically to ensure that you are protected in extreme disaster recovery scenarios.

As you get started with Exchange Server 2010, you should concentrate on the following areas:

- How Exchange Server 2010 works with your hardware
- What versions and editions of Exchange Server 2010 are available, and how they meet your needs
- How Exchange Server 2010 works with Windows–based operating systems
- How Exchange Server 2010 works with Active Directory
- What administration tools are available

Exchange Server 2010 and Your Hardware

Before you deploy Exchange Server 2010, you should carefully plan the messaging architecture. As part of your implementation planning, you need to look closely at preinstallation requirements and the hardware you will use. Exchange Server is no longer the simple messaging server that it once was. It is now a complex messaging platform with many components that work together to provide a comprehensive solution for routing, delivering, and accessing e-mail messages, voice-mail messages, faxes, contacts, and calendar information.

Successful Exchange Server administration depends on three things:

- Knowledgeable Exchange administrators
- Strong architecture
- Appropriate hardware

The first two ingredients are covered: you're the administrator, you're smart enough to buy this book to help you through the rough spots, and you've enlisted Exchange Server 2010 to provide your high-performance messaging needs. This brings us to the issue of hardware. Exchange Server 2010 should run on a system with adequate memory, processing speed, and disk space. You also need an appropriate data-protection and system-protection plan at the hardware level.

Key guidelines for choosing hardware for Exchange Server are as follows:

- **Memory** Exchange Server 2010 has been tested and developed for maximum memory configurations of 64 gigabytes (GB) for Mailbox servers and 16 GB for all other server roles except Unified Messaging. For Unified Messaging, the maximum is 8 GB. For multirole servers, the maximum is 64 GB. The minimum random access memory (RAM) is 2 GB. In most cases, you'll want to have at least twice the recommended minimum amount of memory. The primary reason for this is performance. Most of the Exchange installations I run use 4 GB of RAM as a starting point, even in small installations. In multiple Exchange server installations, the Mailbox server should have at least 2 GB of RAM plus 5 megabytes (MB) of RAM per mailbox. For all Exchange server configurations, the paging file should be at least equal to the amount of RAM in the server plus 10 MB.
- **CPU** Exchange Server 2010 runs on the x64 family of processors from AMD and Intel, including AMD64 and Intel Extended Memory 64 Technology (Intel EM64T). Exchange Server 2010 provides solid benchmark performance with Intel Xeon 3.4 GHz and higher or AMD Opteron 3.1 GHz and higher. Any of these CPUs provide good starting points for the average Exchange Server system. You can achieve significant performance improvements with a high level of processor cache. Look closely at the L1, L2, and L3 cache options available—a higher cache can yield much better performance overall. Look also at the speed of the front-side bus. The faster the bus speed, the faster the CPU can access memory.

Exchange Server 2010 runs only on 64-bit hardware. The primary advantages of 64-bit processors over 32-bit processors are related to memory limitations and data access. Because 64-bit processors can address more than 4 GB of memory at a time without physical address extension, they can store greater amounts of data in main memory, providing direct access to and faster processing of data. In addition, 64-bit processors can process data and execute instruction sets that are twice as large as 32-bit processors. Accessing 64 bits of data (versus 32 bits) offers a significant advantage when processing complex calculations that require a high level of precision.

NOTE **At the time of this writing, 64-bit versions do not support Intel Itanium.**

- **SMP** Exchange Server 2010 supports symmetric multiprocessors, and you'll see significant performance improvements if you use multiple CPUs. Microsoft tested and developed Exchange Server 2010 for use with dual-core and multicore CPUs as well. The minimum, recommended, and maximum number of CPUs—whether single core, dual core, or multicore—depends on a server's Exchange roles. (See the "Exchange Server Messaging Roles" section in Chapter 2, "Deploying Exchange Server 2010.") Still, if Exchange Server is supporting a small organization with a single domain, one CPU with multiple cores should be enough. If the server supports a medium or large organization or handles mail for multiple domains, you might want to consider adding processors. When it comes to processor cores, I prefer two 4-core processors to a single 8-core processor given current price and performance tradeoffs. An alternative is to distribute the workload across different servers based on where you locate resources.
- **Disk drives** The data storage capacity you need depends entirely on the number and size of the data that will pass through, be journaled on, or stored on the Exchange server. You need enough disk space to store all data and logs, plus workspace, system files, and virtual memory. Input/output (I/O) throughput is just as important as drive capacity. Rather than use one large drive, you should use several drives, which allow you to configure fault tolerance with RAID.
- **Data protection** You can add protection against unexpected drive failures by using RAID. For the boot and system disks, use RAID 1 on internal drives. However, because of the new high-availability features, you might not want to use RAID for Exchange data and logs. You also might not want to use expensive disk storage systems either. Instead, you might want to deploy multiple Exchange servers with each of your Exchange roles.

  If you decide to use RAID, remember that storage arrays typically already have an underlying RAID configuration and you might have to use a tool such as Storage Manager For SANs to help you distinguish between logical unit numbers (LUNs) and physical disks. For data, use RAID 0 or RAID 5.

For logs, use RAID 1. RAID 0 (disk striping without parity) offers good read/write performance, but any failed drive means that Exchange Server can't continue operation on an affected database until the drive is replaced and data is restored from backup. RAID 1 (disk mirroring) creates duplicate copies of data on separate drives; you can rebuild the RAID unit to restore full operations and can continue operations if one of the drives fails. RAID 5 (disk striping with parity) offers good protection against single drive failure, but it has poor write performance. For best performance and fault tolerance, RAID 10 (also referred to as RAID 0 + 1), which consists of disk mirroring and disk striping without parity, is also an option.

- **Uninterruptible power supply** Exchange Server 2010 is designed to maintain database integrity at all times and can recover information using transaction logs. This doesn't protect the server hardware, however, from sudden power loss or power spikes, both of which can seriously damage hardware. To prevent this, connect your server to an uninterruptible power supply (UPS). A UPS gives you time to shut down the server or servers properly in the event of a power outage. Proper shutdown is especially important on servers using write-back caching controllers. These controllers temporarily store data in cache. Without proper shutdown, this data can be lost before it is written to disk. Note that most write-back caching controllers have batteries that help ensure that changes can be written to disk after the system comes back online.

If you follow these hardware guidelines and modify them for specific messaging roles, as discussed in the next section, you'll be well on your way to success with Exchange Server 2010.

Exchange Server 2010 Editions

Several editions of Exchange Server 2010 are available, including Exchange Server 2010 Standard and Exchange Server 2010 Enterprise. The various server editions support the same core features and administration tools, which means you can use the techniques discussed throughout this book regardless of which Exchange Server 2010 edition you are using. For reference, the specific feature differences between Standard Edition and Enterprise Edition are as follows:

- **Exchange Server 2010 Standard** Designed to provide essential messaging services for small to medium-size organizations and branch office locations. This server edition supports a limited number of databases.
- **Exchange Server 2010 Enterprise** Designed to provide essential messaging services for organizations with increased availability, reliability, and manageability needs. This server edition supports up to 100 databases (including all active databases and copies of databases) on a particular server.

NOTE **Throughout this book, I refer to Exchange Server in different ways, and each has a different meaning. Typically, I refer to the software product as *Exchange Server*. If you see this term, you can take it to mean *Microsoft Exchange Server 2010*. When necessary, I use *Exchange Server 2010* to draw attention to the fact that I am discussing a feature that's new or has changed in the most recent version of the product. Each of these terms means essentially the same thing. If I refer to a previous version of Exchange Server, I always do so specifically, such as Exchange Server 2007. Finally, I often use the term *Exchange server* (note the lowercase *S* in server) to refer to an actual server computer, as in "There are eight Exchange servers in this routing group."**

REAL WORLD **Microsoft provides a single binary for x64 systems, and the same binary file is used for both the Standard and Enterprise edition. The license key provided during installation is what determines which edition is established during installation.**

You can use a valid product key to upgrade from a trial edition to the Standard edition or the Enterprise edition of Exchange Server 2010 without having to reinstall. Using a valid product key, you can also upgrade from the Standard to the Enterprise edition. You can also relicense an Exchange server by entering a new product key for the installed edition, which is useful if you accidentally used the same product key on multiple servers and want to correct the mistake.

There are several caveats. When you change the product key on a Mailbox server, you must restart the Microsoft Exchange Information Store service to apply the change. When you change the product key on an Edge Transport server, you must resubscribe the server in the Exchange organization to apply the change. Additionally, you cannot use product keys to downgrade editions. To downgrade editions, you must uninstall Exchange Server and then reinstall Exchange Server.

You can install Exchange Server 2010 on a server running Windows Server 2008 with Service Pack 2 or later as well as on a server running Windows Server 2008 Release 2. A client accessing an Exchange server requires a Client Access License (CAL). With either Exchange Server edition, the client can use a Standard CAL, an Enterprise CAL, or both. The Standard CAL allows for the use of e-mail, shared calendaring, contacts, task management, Microsoft Outlook Web App (OWA), and Exchange ActiveSync. The Enterprise CAL allows for the use of unified messaging, advanced compliance capabilities, and antivirus/antispam protection. A client must have both a Standard CAL and an Enterprise CAL to make full use of all Exchange Server features.

Beyond the editions and CALs, Exchange Server 2010 has several variants. Microsoft offers on-premises and online implementations of Exchange Server. An on-premises Exchange Server is one that you install in your organization. An online Exchange Server is delivered as a subscription service from Microsoft. In Exchange Server 2010, you can manage both on-premises and online implementations of Exchange Server using the same management tools.

When you install Exchange Server 2010, the system partition and all disk partitions used by Exchange must be formatted using the NTFS file system. Additional preinstallation requirements are as follows:

- In the Active Directory forest where you plan to install Exchange 2010, the Schema master must be running on a server with Windows Server 2003 or a later version of Windows and Active Directory must be in at least Windows Server 2003 forest functionality mode.
- In every Active Directory site where you plan to install Exchange 2010, you must have at least one global catalog server that is running Windows Server 2003 or a later version of Windows.
- For forest-to-forest delegation and free/busy availability selection across forests, you must establish a trust between the forests that have Exchange Server installed.
- The domain should be configured to use multiple-label Domain Name System (DNS) names, such as cpandl.com or adatum.local, rather than single-label DNS names, such as cpandl or adatum. However, single label names can be used.

NOTE **The full installation option of Windows Server 2008 is required for all Exchange 2010 servers. Using Active Directory with Exchange Server 2010 is covered in more detail in the "Exchange Server and Active Directory" section of this chapter and the "Integrating Exchange Server Roles with Active Directory" section of Chapter 2.**

Exchange Server 2010 requires Microsoft Management Console 3.0 or later, the Microsoft .NET Framework version 3.5.1, and Windows PowerShell Version 2.0 for the Exchange Management Shell and remote management. The Windows PowerShell remoting features are supported by the WS-Management protocol and the Windows Remote Management (WinRM) service that implements WS-Management in Windows. Computers running Windows 7 and Windows Server 2008 Release 2 and later include WinRM 2.0 or later. On computers running earlier versions of Windows, you need to install Windows Management Framework, which includes Windows PowerShell 2.0 and WinRM 2.0 or later as appropriate. Other prerequisites are role-specific and discussed in Chapter 2.

If you want to manage Exchange Server 2010 from a workstation, you need to install Windows Management Framework. Because WinRM 2.0 and Windows PowerShell 2.0 are used for remote management whether you use the GUI or the command line, you need to enable remote commands on the workstation.

You can verify the availability of WinRM 2.0 and configure Windows PowerShell for remoting by following these steps:

1. Click Start, All Programs, Accessories, Windows PowerShell. Start Windows PowerShell as an administrator by right-clicking the Windows PowerShell shortcut and selecting Run As Administrator.

2. The WinRM service is configured for manual startup by default. You must change the startup type to Automatic and start the service on each computer you want to work with. At the PowerShell prompt, you can verify that the WinRM service is running by using the following command:

   ```
   get-service winrm
   ```

   As shown in the following example, the value of the Status property in the output should be Running:

   ```
   Status   Name               DisplayName
   ------   ----               -----------
   Running  WinRM              Windows Remote Management
   ```

   If the service is stopped, enter the following command to start the service and configure it to start automatically in the future:

   ```
   set-service –name winrm –startuptype automatic –status running
   ```

3. To configure Windows PowerShell for remoting, type the following command:

   ```
   Enable-PSRemoting –force
   ```

   You can only enable remoting when your computer is connected to a domain or private network. If your computer is connected to a public network, you need to disconnect from the public network and connect to a domain or private network and then repeat this step. If one or more of your computer's connections has the Public connection type, but you are actually connected to a domain or private network, you need to change the network connection type in Network And Sharing Center and then repeat this step.

In many cases, you will be able to work with remote computers in other domains. However, if the remote computer is not in a trusted domain, the remote computer might not be able to authenticate your credentials. To enable authentication, you need to add the remote computer to the list of trusted hosts for the local computer in WinRM. To do so, type the following:

```
winrm s winrm/config/client '@{TrustedHosts="RemoteComputer"}'
```

where *RemoteComputer* is the name of the remote computer, such as:

```
winrm s winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

When you are working with computers in workgroups or homegroups, you must use HTTPS as the transport or add the remote machine to the TrustedHosts configuration settings. If you cannot connect to a remote host, verify that the service on the remote host is running and is accepting requests by running the following command on the remote host:

```
winrm quickconfig
```

This command analyzes and configures the WinRM service. If the WinRM service is set up correctly, you'll see output similar to the following:

```
WinRM already is set up to receive requests on this machine.
WinRM already is set up for remote management on this machine
```

If the WinRM service is not set up correctly, you see errors and need to respond affirmatively to several prompts that allow you to automatically configure remote management. When this process completes, WinRM should be set up correctly.

Whenever you use Windows PowerShell remoting features, you must start Windows PowerShell as an administrator by right-clicking the Windows PowerShell shortcut and selecting Run As Administrator. When starting Windows PowerShell from another program, such as the command prompt (cmd.exe), you must start that program as an administrator.

Exchange Server 2010 uses the Windows Installer (the Installer) and has a fully integrated installation process. This means you can configure Exchange Server 2010 much like you can any other application you install on the operating system. The installation can be performed remotely from a command shell as well as locally.

Chapter 2 provides detailed instructions for installing Exchange Server 2010. With an initial installation, Windows Installer first checks the system configuration to determine the status of required services and components. As part of this process, Windows Installer checks the Active Directory configuration and the availability of components, such as IIS (Internet Information Services), as well as operating system service packs, installation permissions for the default install path, memory, and hardware.

After checking the system configuration, the Installer allows you to select the roles to install. Whether you use the Standard or Enterprise edition, you have similar options. You can do any of the following:

- Install an internal messaging server by selecting the individual server roles to install and combining the Mailbox role, Client Access role, Hub Transport role, and Unified Messaging role as required for your environment. Generally, you will not want an internal Exchange server to also be configured as a domain controller with a global catalog.

  NOTE **For details on how the various server roles are used, see Chapter 2, which also provides guidelines for sizing and positioning the various server roles. Before you install the Client Access role on servers with the Mailbox role, you'll want to consider whether you want to use client access arrays. A client access array is a grouping of client access servers in a load balanced array. Servers that are members of the array cannot have the Mailbox role.**

- Install a Messaging server in a perimeter zone outside the organization's main network by selecting only the Edge Transport role. Edge Transport servers are not members of the internal Active Directory forest and are not

configured on domain controllers. They can, however, be members of an extranet Active Directory forest, which is useful for management purposes.

- Install the management tools.
- Specify the path for the Exchange Server installation files.
- Specify the path for the Exchange Server installation.

If you want to change the configuration after installation, you can use Exchange Server 2010 maintenance mode, as discussed in the "Adding, Modifying, or Uninstalling Server Roles" section in Chapter 2.

Exchange Server 2010 includes the following antispam and antivirus capabilities:

- **Connection filtering** Allows administrators to configure IP Block lists and IP Allow lists, as well as providers who can supply these lists.
- **Content filtering** Uses intelligent message filtering to scan message content and identify spam. Spam can be automatically deleted, quarantined, or filed as junk e-mail.

TIP **Using the Exchange Server management tools, administrators can manage messages sent to the quarantine mailbox and take appropriate actions, such as deleting messages, flagging them as false positives, or allowing them to be delivered as junk e-mail. Messages delivered as junk e-mail are converted to plain text to strip out any potential viruses they might contain.**

- **IP reputation service** Provides Exchange Server 2010 customers with exclusive access to an IP Block list provided by Microsoft.
- **Outlook Junk E-mail Filter list aggregation** Allows the junk e-mail filter lists of individual Outlook users to be propagated to Exchange servers.
- **Recipient filtering** Allows administrators to replicate recipient data from the enterprise to the server running the Edge Transport role. This server can then perform recipient lookups on incoming messages and block messages that are for nonexistent users, which prevents certain types of attacks and malicious attempts at information discovery.
- **Sender ID verification** Verifies that incoming e-mail messages are from the Internet domain from which they claim to come. Exchange verifies the sender ID by examining the sender's IP address and comparing it to the related security record on the sender's public DNS server.
- **Sender reputation scoring** Helps to determine the relative trustworthiness of unknown senders through sender ID verification and by examining message content and sender behavior history. A sender can then be added temporarily to the Blocked Senders list.

Although these antivirus and antispam features are extensive, they are not comprehensive in scope. For comprehensive antivirus protection, you need to install Forefront Protection for Exchange Server. Forefront Protection for Exchange Server helps protect Exchange servers from viruses, worms, and other malware using

multiple antivirus scan engines and file-filtering capabilities. Forefront Protection provides distributed protection for Exchange servers with the Mailbox server, Hub Transport server, and Edge Transport server roles. Although you can install Forefront Protection on Exchange servers with these roles to gain substantial antivirus protection, you do not need to install Forefront Protection on Exchange servers with only the Client Access server or Unified Messaging server role.

You can use the Forefront Protection Setup program to install the server and management components. The management components include the Forefront Server Security Administration Console and the Forefront Management Shell. When you are working with the console, you can configure the way real-time and scheduled scanning for viruses and spyware works. In the shell, you'll find Forefront-specific cmdlets for performing similar tasks.

Exchange Server and Windows

When you install Exchange Server and Forefront Protection for Exchange Server on a server operating system, Exchange Server and Forefront Protection make extensive modifications to the environment. These modifications include new system services, integrated authentication, and new security groups.

Services for Exchange Server

When you install Exchange Server and Forefront Protection for Exchange Server on Windows, multiple services are installed and configured on the server. Table 1-1 provides a summary of key services, how they are used, and which server components they are associated with.

TABLE 1-1 Summary of Key Services Used by Exchange Server 2010

SERVICE NAME	DESCRIPTION	SERVER ROLE
IIS Admin	Enables the server to administer the IIS metabase. The IIS metabase stores configuration information for Web applications used by Exchange. All roles need IIS for WinRM and remote Powershell. CAS needs IIS for OWA and Web services	Client Access
Microsoft Exchange Active Directory Topology	Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services will not be able to start.	Hub Transport, Mailbox, Client Access, Unified Messaging
Microsoft Exchange Address Book	Manages client address book connections for Exchange Server.	Client Access

TABLE 1-1 Summary of Key Services Used by Exchange Server 2010

SERVICE NAME	DESCRIPTION	SERVER ROLE
Microsoft Exchange Anti-Spam Update	Maintains the antispam data for Forefront Protection on an Exchange server.	Hub Transport, Edge Transport
Microsoft Exchange EdgeSync	Provides EdgeSync services between Hub and Edge servers.	Hub Transport
Microsoft Exchange File Distribution	Distributes Exchange data to other Exchange servers.	All
Microsoft Exchange Forms Based Authentication	Provides form-based authentication for Outlook Web App and the Web management interface.	Client Access
Microsoft Exchange IMAP4	Provides IMAP4 services to clients.	Client Access
Microsoft Exchange Information Store	Manages the Microsoft Exchange Information Store. This includes mailbox stores and public folder stores.	Mailbox
Microsoft Exchange Mail Submission	Submits messages from the Mailbox server to the Hub Transport servers.	Mailbox
Microsoft Exchange Mailbox Assistants	Manages assistants that are responsible for calendar updates and booking resources.	Mailbox
Microsoft Exchange Mailbox Replication	Enables online mailbox moves by processing mailbox move requests.	Client Access
Microsoft Exchange Monitoring	Provides support for monitoring and diagnostics.	All
Microsoft Exchange POP3	Provides Post Office Protocol version 3 (POP3) services to clients.	Client Access
Microsoft Exchange Protected Service Host	Provides secure host for Exchange Server services.	All
Microsoft Exchange Replication Service	Provides replication functionality used for continuous replication.	Mailbox
Microsoft Exchange RPC Client Access	Manages client remote procedure call (RPC) connections for Exchange Server.	Client Access
Microsoft Exchange Search Indexer	Controls indexing of mailboxes to improve search performance.	Mailbox

TABLE 1-1 Summary of Key Services Used by Exchange Server 2010

SERVICE NAME	DESCRIPTION	SERVER ROLE
Microsoft Exchange Server Extension for Windows Server Backup	Provides extensions for Windows Server Backup that allow you to backup and recover Exchange application data using Windows Server Backup.	All
Microsoft Exchange Service Host	Provides a host for essential Exchange services.	All
Microsoft Exchange Speech Engine	Provides speech processing services for Microsoft Exchange. If this service is stopped, speech recognition services will not be available to unified messaging clients.	Unified Messaging
Microsoft Exchange System Attendant	Provides monitoring, maintenance, and Active Directory lookup services.	Mailbox
Microsoft Exchange Throttling	Provides throttling functions to limit the rate of user operations.	Mailbox
Microsoft Exchange Transport	Provides mail transport for Exchange Server.	Hub Transport, Edge Transport
Microsoft Exchange Transport Log Search	Provides search capability for Exchange transport log files.	Hub Transport, Mailbox
Microsoft Exchange Unified Messaging	Enables voice and fax messages to be stored in Exchange and gives users telephone access to e-mail, voice mail, the calendar, contacts, or an automated attendant.	Unified Messaging
Microsoft Forefront Server Protection ADO/EWS Navigator	Navigates the objects in Active Directory for Forefront Protection by connecting with Exchange Web Services (EWS) or Exchange ActiveX Data Objects (ADO) to retrieve objects.	Forefront Protection
Microsoft Forefront Server Protection Controller	Controls the interaction between Forefront Protection and the Microsoft Exchange Information Store. Ensures that Forefront Protection initializes properly with the information store. The Microsoft Forefront Server Security Controller starts and stops scan jobs and applies engine updates.	Forefront Protection

TABLE 1-1 Summary of Key Services Used by Exchange Server 2010

SERVICE NAME	DESCRIPTION	SERVER ROLE
Microsoft Forefront Server Security Eventing Service	Processes incidents, and manages quarantine logging, performance logging, and notifications.	Forefront Protection
Microsoft Forefront Server Security for Exchange Registration Service	Ensures the Forefront Transport Agent is registered with Exchange Server.	Forefront Protection
Microsoft Forefront Server Security Mail Pickup	Provides mail pickup services for Forefront Protection.	Forefront Protection
Microsoft Forefront Server Security Monitor	Monitors the information store, SMTP/IMS, and Forefront Protection processes to ensure that Forefront Protection provides continuous protection.	Forefront Protection
Microsoft Search (Exchange)	Provides search services for mailboxes, address lists, and so on.	Hub Transport, Mailbox
Secure Socket Tunneling Protocol Service	Provides support for Secure Socket Tunneling Protocol (SSTP) for securely connecting to remote computers.	Client Access
Web Management Service	Enables remote and delegated management for the Web server, sites, and applications.	Client Access
Windows Remote Management Service	Implements the WS-Management protocol. Required for remote management using the Exchange console and Windows PowerShell.	All
World Wide Web Publishing Services	Provides Web connectivity and administration features for IIS.	Client Access

Exchange Server Authentication and Security

In Exchange Server 2010, e-mail addresses, distribution groups, and other directory resources are stored in the directory database provided by Active Directory. Active Directory is a directory service running on Windows domain controllers. When there are multiple domain controllers, the controllers automatically replicate directory data with each other using a multimaster replication model. This model allows any

domain controller to process directory changes and then replicate those changes to other domain controllers.

The first time you install Exchange Server 2010 in a Windows domain, the installation process updates and extends Active Directory to include objects and attributes used by Exchange Server 2010. Unlike Exchange Server 2003 and earlier releases of Exchange, this process does not include updates for the Active Directory Users And Computers Snap-In for Microsoft Management Console (MMC), and you do not use Active Directory Users And Computers to manage mailboxes, messaging features, messaging options, or e-mail addresses associated with user accounts. You perform these tasks using the Exchange Management tools.

Exchange Server 2010 fully supports the Windows Server security model and relies on this security mechanism to control access to directory resources. This means you can control access to mailboxes and membership in distribution groups and you can perform other Exchange security administration tasks through the standard Windows Server permission set. For example, to add a user to a distribution group, you simply make the user a member of the distribution group in Active Directory Users And Computers.

Because Exchange Server uses Windows Server security, you can't create a mailbox without first creating a user account that will use the mailbox. Every Exchange mailbox must be associated with a domain account—even those used by Exchange for general messaging tasks. For example, the SMTP and System Attendant mailboxes that Exchange Server uses are associated by default with the built-in System user. In the Exchange Management Console, you can create a new user account as part of the process of creating a new mailbox.

NOTE **To support coexistence with Exchange Server 2003, all Exchange Server 2010 servers are automatically added to a single administrative group when you install Exchange Server 2010. This administrative group is recognized in the Exchange System Manager in Exchange Server 2003 as "Exchange Administrative Group." Although Exchange Server 2003 uses administrative groups to gather Exchange objects for the purposes of delegating permission to manage those objects, Exchange Server 2007 and Exchange Server 2010 do not use administrative groups. Instead, you manage Exchange servers according to their roles and the type of information you want to manage using the Exchange Management Console. You'll learn more about this in Chapter 3, "Exchange Server 2010 Administration Essentials."**

Exchange Server Security Groups

Like Exchange Server 2007, Exchange Server 2010 uses predefined universal security groups to separate administration of Exchange permissions from administration of other permissions. When you add an administrator to one of these security groups, the administrator inherits the permissions permitted by that role.

The predefined security groups have permissions to manage the following types of Exchange data in Active Directory:

- **Organization Configuration node** This type of data is not associated with a specific server and is used to manage databases, policies, address lists, and other types of organizational configuration details.
- **Server Configuration node** This type of data is associated with a specific server and is used to manage the server's messaging configuration.
- **Recipient Configuration node** This type of data is associated with mailboxes, mail-enabled contacts, and distribution groups.

NOTE **In Exchange Server 2010, databases have been moved from the Server Configuration node to the Organization Configuration node. This change was necessary because the Exchange schema was flattened and storage groups were removed. As a result of these changes, all storage group functionality has been moved to the database level.**

The predefined groups are as follows:

- **Delegated Setup** Members of this group have permission to install and uninstall Exchange on provisioned servers.
- **Discovery Management** Members of this group can perform mailbox searches for data that meets specific criteria.
- **Exchange All Hosted Organizations** Members of this group include hosted organization mailbox groups. This group is used to apply Password Setting objects to all hosted mailboxes.
- **Exchange Servers** Members of this group are Exchange servers in the organization. This group allows Exchange servers to work together.
- **Exchange Trusted Subsystem** Members of this group are Exchange servers that run Exchange cmdlets using WinRM. Members of this group have permission to read and modify all Exchange configuration settings as well as user accounts and groups.
- **Exchange Windows Permissions** Members of this group are Exchange servers that run Exchange cmdlets using WinRM. Members of this group have permission to read and modify user accounts and groups.
- **ExchangeLegacyInterop** Members of this group are granted send-to and receive-from permissions, which are necessary for routing group connections between Exchange Server 2010 and Exchange Server 2003. Exchange Server 2003 bridgehead servers must be made members of this group to allow proper mail flow in the organization. For more information on interoperability, see Chapter 2.
- **Help Desk** Members of this group can view any property or object within the Exchange organization and have limited management permissions, including the right to change and reset passwords.
- **Hygiene Management** Members of this group can manage the antispam and antivirus features of Exchange.

- **Organization Management** Members of this group have full access to all Exchange properties and objects in the Exchange organization.
- **Public Folder Management** Members of this group can manage public folders and perform most public folder management operations.
- **Recipient Management** Members of this group have permissions to modify Exchange user attributes in Active Directory and perform most mailbox operations.
- **Records Management** Members of this group can manage compliance features, including retention policies, message classifications, and transport rules.
- **Server Management** Members of this group can manage all Exchange servers in the organization but do not have permission to perform global operations.
- **UM Management** Members of this group can manage all aspects of unified messaging, including unified messaging server configuration and unified messaging recipient configuration.
- **View-Only Organization Management** Members of this group have 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 Server and Active Directory

Like Exchange Server 2007, Exchange Server 2010 is tightly integrated with Active Directory. Not only does Exchange Server 2010 store information in Active Directory, but it also uses the Active Directory routing topology to determine how to route messages within the organization. Routing to and from the organization is handled using transport servers.

Understanding How Exchange Stores Information

Exchange stores four types of data in Active Directory: schema data (stored in the Schema partition), configuration data (stored in the Configuration partition), domain data (stored in the Domain partition), and application data (stored in application-specific partitions). In Active Directory, schema rules determine what types of objects are available and what attributes those objects have. When you install the first Exchange server in the forest, the Active Directory preparation process adds many Exchange-specific object classes and attributes to the schema partition in Active Directory. This allows Exchange-specific objects, such as agents and connectors, to be created. It also allows you to extend existing objects, such as users and groups, with new attributes, such as attributes that allow user objects to be used for sending

and receiving e-mail. Every domain controller and global catalog server in the organization has a complete copy of the Schema partition.

During the installation of the first Exchange server in the forest, Exchange configuration information is generated and stored in Active Directory. Exchange configuration information, like other configuration information, is also stored in the Configuration partition. For Active Directory, the configuration information describes the structure of the directory, and the Configuration container includes all of the domains, trees, and forests, as well as the locations of domain controllers and global catalogs. For Exchange, the configuration information is used to describe the structure of the Exchange organization. The Configuration container includes lists of templates, policies, and other global organization-level details. Every domain controller and global catalog server in the organization has a complete copy of the Configuration partition.

In Active Directory, the Domain partition stores domain-specific objects, such as users and groups, and the stored values of attributes associated with those objects. As you create, modify, or delete objects, Exchange stores the details about those objects in the Domain partition. During the installation of the first Exchange server in the forest, Exchange objects are created in the current domain. Whenever you create new recipients or modify Exchange details, the related changes are reflected in the Domain partition as well. Every domain controller has a complete copy of the Domain partition for the domain for which it is authoritative. Every global catalog server in the forest maintains information about a subset of every Domain partition in the forest.

Understanding How Exchange Routes Messages

Within the organization, Hub Transport servers use the information about sites stored in Active Directory to determine how to route messages, and they can also route messages across site links. The Hub Transport server does this by querying Active Directory about its site membership and the site membership of other servers, and then it uses the information it discovers to route messages appropriately. Because of this, when you are deploying an Exchange Server 2010 organization, no additional configuration is required to establish routing in the Active Directory forest.

For mail delivery within the organization, additional routing configuration is necessary only in these specific scenarios:

- If you deploy Exchange Server 2010 in an existing Exchange Server 2003 organization, you must configure a two-way routing group connector from the Exchange routing group to each Exchange Server 2003 routing group that communicates with Exchange Server 2010. You must also suppress link state updates for the same.

- If you deploy an Exchange Server 2010 organization with multiple forests, you must install Exchange Server 2010 in each forest and then connect the forests using appropriate cross-forest trusts. The trust allows users to see address and availability data across the forests.
- In an Exchange Server 2010 organization, if you want direct mail flow between Exchange servers in different forests, you must configure SMTP send connectors and SMTP receive connectors on the Hub Transport servers that should communicate directly with each other.

The organization's Mail Transport servers handle mail delivery outside the organization and receipt of mail from outside servers. You can use two types of Mail Transport servers: Hub Transport servers and Edge Transport servers. You deploy Hub Transport servers within the organization. You can optionally deploy Edge Transport servers in the organization's perimeter network for added security. Typically a perimeter network is a secure network set up outside the organization's private network.

With Hub Transport servers, no other special configuration is needed for message routing to external destinations. You must configure only the standard mail setup, which includes identifying DNS servers to use for lookups. With Edge Transport servers, you can optimize mail routing and delivery by configuring one-way synchronization from the internal Hub Transport servers to the perimeter network's Edge Transport servers. Beyond this, no other special configuration is required for mail routing and delivery.

Using the Graphical Administration Tools

Exchange Server 2010 provides several types of tools for administration. The graphical tools are the ones you'll use most frequently. Exchange Server and Forefront Protection for Exchange Server have separate management consoles. If you follow the instructions for installing Exchange Server in Chapter 2, you'll be able to access the Exchange tools by selecting Start, choosing All Programs, and then using the Microsoft Exchange Server 2010 menu. To access the Forefront Protection tools, select Start, choose All Programs, and then use the Microsoft Forefront Server Security menu.

Exchange Server 2010 has several graphical tools that replace or combine features of the graphical tools in Exchange Server 2003 and earlier editions. The Exchange Management Console, shown in Figure 1-1, replaces Exchange System Manager.

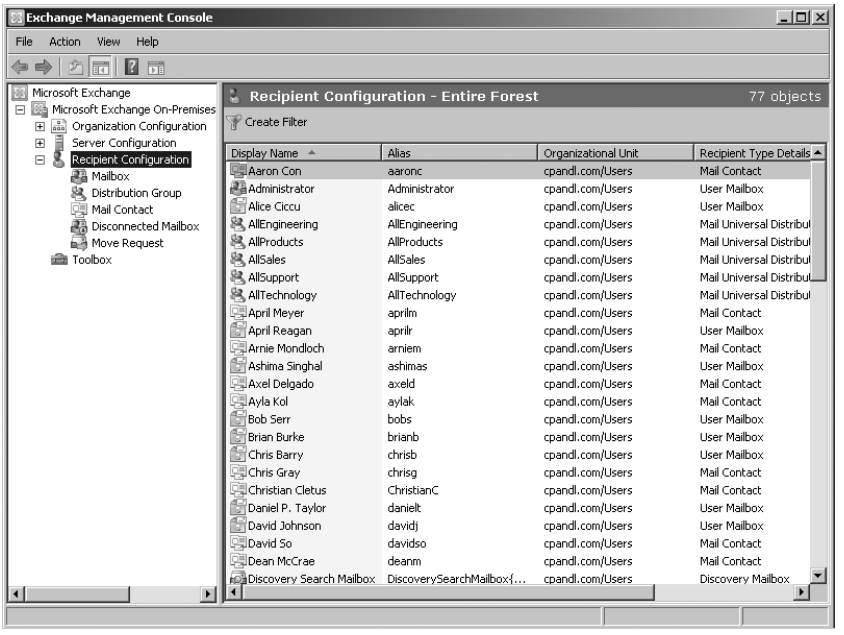


FIGURE 1-1 The Exchange Management Console.

As discussed further in Chapter 14, "Exchange Server 2010 Maintenance, Monitoring, and Queuing," and Chapter 15, "Backing Up and Restoring Exchange Server 2010," the Toolbox node in the Exchange Management Console provides access to a suite of related tools, including the following:

- **Best Practices Analyzer** Checks the configuration and health of your Exchange organization to ensure that it complies with current best practices recommended by Microsoft. Because best practices are periodically updated, the tool includes an update facility to ensure that the most current best practices are in place.
- **Details Templates Editor** Helps administrators customize client-side GUI presentation of object properties accessed through address lists. You can use this tool to customize the presentation of contacts, users, groups, public folders, and more in the client interface.
- **Mail Flow Troubleshooter** Helps troubleshoot problems related to mail flow and transport configuration by providing suggested resolutions for symptoms observed by administrators.
- **Message Tracking** Allows administrators to track messages as they are routed through the Exchange organization.
- **Performance Monitor** Allows administrators to graph system performance. Also allows administrators to create performance logs and alerts.

Wide arrays of Exchange performance objects are available for tracking performance.

- **Performance Troubleshooter** Helps troubleshoot problems related to performance by identifying possible bottlenecks and providing suggested solutions.
- **Public Folder Management Console** Allows administrators to manage public folders using a graphical interface rather than the command line.
- **Queue Viewer** Allows administrators to track message queues and mail flow. Also allows administrators to manage message queuing and remove messages.
- **Remote Connectivity Analyzer** Allows administrators to perform connectivity tests for inbound e-mail, ActiveSync, Exchange Web Services, Outlook Anywhere, and Outlook 2003 RPC over HTTP.
- **Role-Based Access Control (RBAC) User Editor** Allows administrators to assign users to RBAC groups and roles.
- **Routing Log Viewer** Helps administrators troubleshoot routing problems on transport servers by providing information about routing topology.
- **Tracking Log Explorer** Provides access to the message tracking logs for troubleshooting.

Other administration tools that you might want to use with Exchange Server are summarized in Table 1-2.

TABLE 1-2 Quick Reference Administration Tools to Use with Exchange Server 2010

ADMINISTRATIVE TOOL	PURPOSE
Computer Management	Starts and stops services, manages disks, and accesses other system management tools.
DNS	Manages the DNS service.
Event Viewer	Manages events and logs.
IIS Manager	Manages Web servers used by Exchange as well as the management service configuration.
Microsoft Network Monitor	Monitors network traffic, and troubleshoots networking problems.
Server Manager	Adds, removes, and configures roles, role services, and features.

You access most of the tools listed in Table 1-2 from the Administrative Tools program group. Click Start, point to All Programs, and then point to Administrative Tools.

Using the Command-Line Administration Tools

The graphical tools provide just about everything you need to work with Exchange Server. Still, there are many times when you might want to work from the command line, especially if you want to automate installation, administration, or maintenance with scripts. To help with all your command-line needs, Exchange Server includes the Exchange Management Shell.

The Exchange Management Shell is an extension shell for Windows PowerShell that includes a wide array of built-in commands for working with Exchange Server. Windows PowerShell commands are referred to as cmdlets (pronounced *commandlets*) to differentiate these commands from less powerful commands built into the command prompt and from more full-featured utility programs that can be invoked at the command prompt.

> ***NOTE*** **For ease of reading and reference, I'll usually refer to command prompt commands, command shell cmdlets, and command-line invoked utilities simply as commands.**

The Exchange Management Shell, shown in Figure 1-2, is accessible by selecting Start, choosing All Programs, choosing Microsoft Exchange Server 2010, and then choosing Exchange Management Shell.

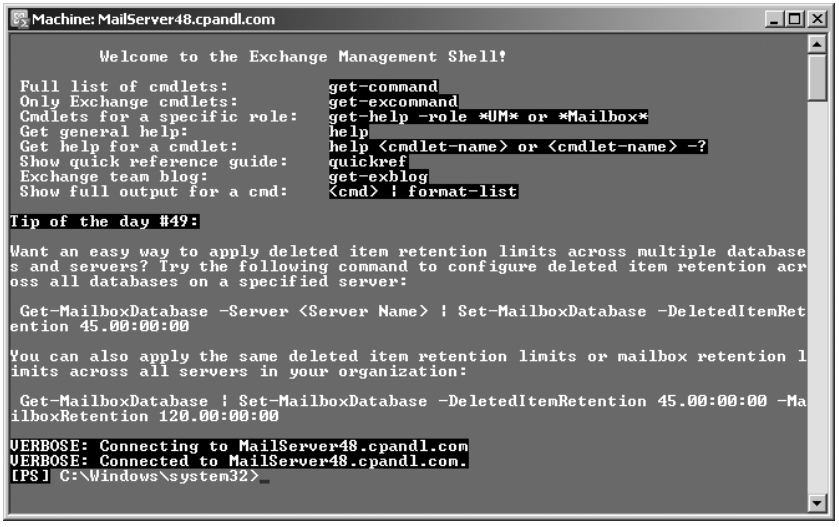


FIGURE 1-2 The Exchange Management Shell.

The basics of working with the Exchange Management Shell are straightforward:

- Type **get-command** to get a full list of all available cmdlets on the server.
- Type **get-excommand** to get a full list of all Exchange-specific cmdlets available.

- Type **help *cmdletName*** to get help information, where *cmdletName* is the name of the command you are looking up.

You'll find a comprehensive discussion of the Exchange Management Shell and Windows PowerShell in Chapter 4, "Using the Exchange Management Shell," as well as examples of using cmdlets for Exchange Server management throughout the book.

Like Exchange Server, Forefront Protection for Exchange Server has a management console and a management shell. You use the Forefront Server Security Administration console to manage Forefront Protection using a graphical interface. You use the Forefront Management Shell to manage Forefront Protection from the command line. This shell is accessible by selecting Start, choosing All Programs, choosing Microsoft Forefront Server Security, and then choosing Forefront Management Shell.

Forefront Management Shell loads extensions that allow you to manage the configuration of Forefront Protection for Exchange Server. The basics of working with the Forefront Management Shell are straightforward:

- Type **get-command** to get a full list of all available cmdlets on the server.
- Type **get-command *fse*** to get a full list of all Forefront Protection–specific cmdlets available.
- Type **help *cmdletName*** to get help information, where *cmdletName* is the name of the command you are looking up.

Because Forefront Management Shell does not load the Exchange Server cmdlets, you cannot access the Exchange-specific cmdlets from this shell by default. Because the Exchange Management Shell does not load the Forefront Protection–specific cmdlets either, you cannot access the Forefront Protection–specific cmdlets from the Exchange Management Shell by default.

CHAPTER 6

Mailbox Administration

The difference between a good Microsoft Exchange administrator and a great one is the attention he or she pays to mailbox administration. Mailboxes are private storage places for messages you've sent and received, and they are created as part of private mailbox databases in Exchange. Mailboxes have many properties that control mail delivery, permissions, and storage limits. You can configure most mailbox settings on a per-mailbox basis. However, you cannot change some settings without moving mailboxes to a different mailbox database or changing the settings of the mailbox database itself. For example, you set the storage location on the file system, the default public folder database for the mailbox, and the default offline address book on a per-mailbox-database basis. Keep this in mind when performing capacity planning and when deciding which mailbox database to use for a particular mailbox.

Creating Special-Purpose Mailboxes

Exchange Server 2010 makes it easy to create several special-purpose mailbox types, including:

- **Room mailbox** A room mailbox is a mailbox for room scheduling.
- **Equipment mailbox** An equipment mailbox is a mailbox for equipment scheduling.
- **Linked mailbox** A linked mailbox is a mailbox for a user from a separate, trusted forest.
- **Forwarding mailbox** A forwarding mailbox is a mailbox that can receive mail and forward it off-site.

- **Archive mailbox** An archive mailbox is used to store a user's messages, such as might be required for executives and needed by some managers.
- **Arbitration mailbox** An arbitration mailbox is used to manage approval requests, such as may be required for handling moderated recipients and distribution group membership approval.
- **Discovery mailbox** A discovery mailbox is the target for Discovery searches and can't be converted to another mailbox type once it's created.
- **Shared mailbox** A shared mailbox is a mailbox that is shared by multiple users, such as a general mailbox for customer inquiries.

The sections that follow discuss techniques for working with these special-purpose mailboxes.

Using Room and Equipment Mailboxes

You use room and equipment mailboxes for scheduling purposes only. You'll find that

- Room mailboxes are useful when you have conference rooms, training rooms, and other rooms for which you need to coordinate the use.
- Equipment mailboxes are useful when you have projectors, media carts, or other items of equipment for which you need to coordinate the use.

Every room and equipment mailbox must have a separate user account associated with it. Although these accounts are required so that the mailboxes can be used for scheduling, the accounts are disabled by default so that they cannot be used for logon. To ensure that the resource accounts do not get enabled accidentally, you need to coordinate closely with other administrators in your organization.

> ***NOTE*** **The Exchange Management Console doesn't show the enabled or disabled status of user accounts. The only way to check the status is to use domain administration tools.**

Because the number of scheduled rooms and amount of equipment grows as your organization grows, you'll want to carefully consider the naming conventions you use with rooms and equipment:

- With rooms, you'll typically want to use display names that clearly identify the rooms' physical locations. For example, you might have rooms named "Conference Room 28 on Fifth Floor" or "Building 83 Room 15."
- With equipment, you'll typically want to identify the type of equipment, the equipment's characteristics, and the equipment's relative location. For example, you might have equipment named "NEC HD Projector at Seattle Office" or "Fifth Floor Media Cart."

As with standard user mailboxes, room and equipment mailboxes have contact information associated with them. To make it easier to find rooms and equipment, you should provide as much information as possible. Specifically, you can make rooms easier for users to work with by using these techniques:

- If a room has a conference or call-in phone, enter this phone number as the business phone number on the Address And Phone tab of the Mailbox Properties dialog box.
- Specify the location details in the Office text box on the Organization tab of the Mailbox Properties dialog box.
- Specify the room capacity in the Resource Capacity text box on the Resource Information tab of the Mailbox Properties dialog box.

The business phone, location, and capacity are displayed in Microsoft Office Outlook.

After you've set up mailboxes for your rooms and equipment, scheduling the rooms and equipment is straightforward. In Exchange, room and equipment availability is tracked using free/busy data. In Outlook, a user who wants to reserve rooms, equipment, or both simply makes a meeting request that includes the rooms and equipment that are required for the meeting.

The steps to schedule a meeting and reserve equipment are as follows:

1. Create a meeting request:
   - In Outlook 2007, click New, and then select Meeting Request. Or press Ctrl+Shift+Q.
   - In Outlook 2010, click New Items, and then select Meeting. Or press Ctrl+Shift+Q.
2. In the To text box, invite the individuals who should attend the meeting by typing their display names, Exchange aliases, or e-mail addresses, as appropriate. (See Figure 6-1.)

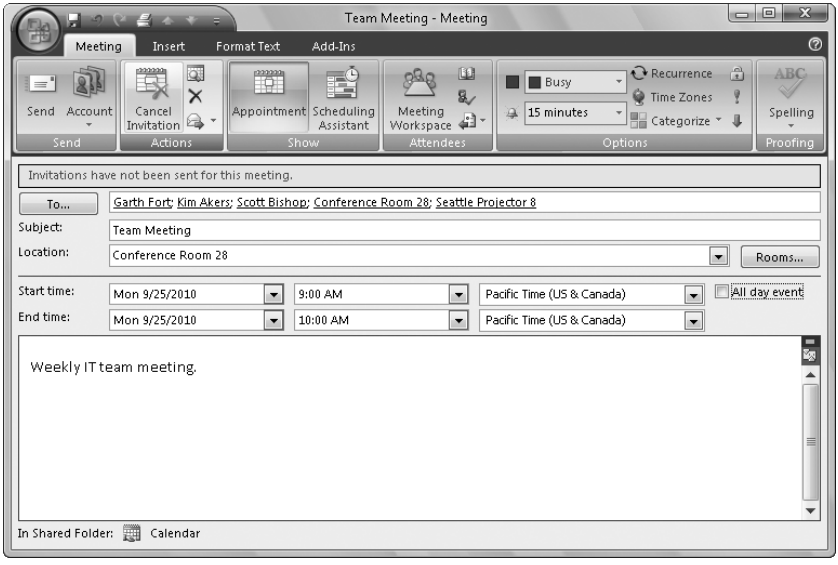


FIGURE 6-1 You can schedule a meeting that includes a reserved room and reserved equipment.

3. Type the display name, Exchange alias, or e-mail address for any equipment you need to reserve.
4. Click the Rooms button to the right of the Location text box. The Select Rooms dialog box appears, as shown in Figure 6-2. By default, the Select Rooms dialog box uses the All Rooms address book. Rooms are added to this address book automatically when you create them.
5. Double-click the room you want to use. This adds the room to the Rooms list. Click OK to close the Select Rooms dialog box.

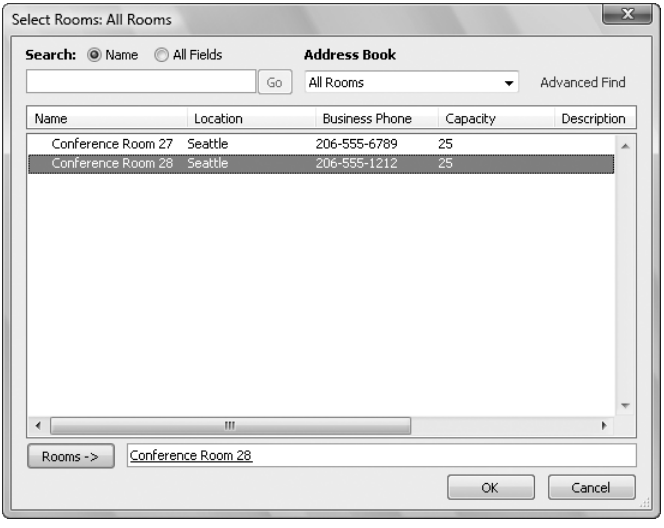


FIGURE 6-2 Select a room to use for the meeting.

6. In the Subject text box, type the meeting subject.
7. Use the Start Time and End Time options to schedule the start and end times for the meeting.
8. Click Scheduling Assistant to view the free/busy data for the invited users and the selected resources.
9. After you type a message to accompany the meeting request, click Send.

Creating Room and Equipment Mailboxes

You can create room and equipment mailboxes by completing the following steps:

1. In the Exchange Management Console, expand the Recipient Configuration node and then select the Mailbox node.

NOTE **If you want to create the user account for the room or equipment mailbox in a domain other than the current one, you first need to set the scope for the Mailbox node, as discussed in the "Finding Existing Mailboxes, Contacts, and Groups" section of Chapter 5, "User and Contact Administration."**

2. Right-click the Mailbox node, and then select New Mailbox. This starts the New Mailbox Wizard.
3. On the Introduction page, select either Room Mailbox or Equipment Mailbox, as appropriate, and then click Next.
4. On the User Type page, verify that New User is selected and then click Next. Each room or piece of equipment must have a separate user account. This is necessary to track the unique free/busy data for the room or piece of equipment.
5. On the User Information page, the Organizational Unit text box shows where in Active Directory the user account will be created. By default, this is the Users container in the current domain. Because you'll usually need to create room and equipment accounts in a specific organizational unit rather than in the Users container, select the Specify The Organizational Unit check box and then click Browse. Use the Select Organizational Unit dialog box to choose the location in which to store the account, and then click OK.
6. Type a descriptive display name in the Name text box.
7. In the User Logon Name text box, type the logon name. Use the drop-down list to select the domain with which the account is to be associated. This sets the fully qualified logon name.
8. The first 20 characters of the logon name are used to set the pre–Microsoft Windows 2000 logon name, which must be unique in the domain. If necessary, change the pre–Windows 2000 logon name.
9. Type and then confirm the password for the account. Even though the account is disabled by default, this password must follow the conventions of your organization's password policy.
10. Click Next. On the Mailbox Settings page, enter an Exchange alias. The Exchange alias is used to set the default e-mail address.
11. If you want to specify a mailbox database rather than use an automatically selected one, select the Specify Mailbox Database check box, and then click the Browse button to the right of the Mailbox Database text box. In the Select Mailbox Database dialog box, choose the mailbox database in which the mailbox should be stored. Mailbox databases are listed by name as well as by associated server.
12. If you want to create an archive mailbox for the resource, select the related check box. Items in the mailbox will be moved automatically to the archive mailbox based on the default retention policy.

13. Click Next, and then click New to create the account and the related mailbox. If an error occurs during account or mailbox creation, neither the account nor the related mailbox will be created. You need to correct the problem and repeat this procedure.
14. Click Finish. For all mailbox-enabled accounts, a Simple Mail Transfer Protocol (SMTP) e-mail address is configured automatically.

In the Exchange Management Shell, you can create a user account with a mailbox for rooms and equipment by using the New-Mailbox cmdlet. Sample 6-1 provides the syntax and usage. Although the account is disabled by default, you must enter a secure password for the account when prompted.

> ***NOTE*** **For rooms, you must use the –Room parameter. For equipment, you must use the –Equipment parameter. By default, when you use either parameter, the related value is set as $true.**

SAMPLE 6-1 Creating room and equipment mailboxes

Syntax

```
New-Mailbox -Name 'DisplayName' -Alias 'ExchangeAlias'
 -OrganizationalUnit 'OrganizationalUnit'
 -UserPrincipalName 'LogonName' -SamAccountName 'prewin2000logon'
 -FirstName '' -Initials '' -LastName ''
 -Database 'Server\MailboxDatabase'
 [-Room <$false|$true> | -Equipment <$false|$true> ]
```

Usage

```
New-Mailbox -Name 'Conference Room 27' -Alias 'room27'
 -OrganizationalUnit 'cpandl.com/Sales'
 -UserPrincipalName 'room27@cpandl.com' -SamAccountName 'room27'
 -FirstName '' -Initials '' -LastName ''
 -Database 'Sales Primary'
 -Room
```

Creating Linked Mailboxes

A linked mailbox is a mailbox that is accessed by a user in a separate, trusted forest. Typically, you use linked mailboxes when your organization's mailbox servers are in a separate resource forest and you want to ensure that users can access free/busy data across these forests.

All linked mailboxes have two user account associations:

- A unique user account in the same forest as the Mailbox server. The same forest user account is disabled automatically so that it cannot be used for logon.

- A unique user account in a separate forest for which you are creating a link. The separate forest user account is enabled so that it can be used for logon.

You can create a linked mailbox by completing the following steps:

1. In the Exchange Management Console, expand the Recipient Configuration node and then select the Mailbox node.
2. Right-click the Mailbox node, and then select New Mailbox. This starts the New Mailbox Wizard.
3. On the Introduction page, select Linked Mailbox and then click Next.
4. On the User Type page, verify that New User is selected and then click Next.
5. On the User Information page, the Organizational Unit text box shows where in Active Directory the user account will be created. By default, this is the Users container in the current domain. Select the Specify The Organizational Unit check box and then click Browse to create the new user account in a different container. Use the Select Organizational Unit dialog box to choose the location in which to store the account, and then click OK.
6. Type the user's first name, middle initial, and last name in the text boxes provided. These values are used to create the Name entry, which is the user's display name.
7. In the User Logon Name text box, type the user's logon name. Use the drop-down list to select the domain with which the account is to be associated. This sets the fully qualified logon name.
8. The first 20 characters of the logon name are used to set the pre–Windows 2000 logon name, which must be unique in the domain. If necessary, change the pre–Windows 2000 logon name.
9. Type and then confirm the password for the account. Although the account will not be used for logon, this password must follow the conventions of your organization's password policy.
10. Click Next. Enter an Exchange alias for the user. Make sure the alias matches the one used in the resource forest.
11. If you want to specify a mailbox database rather than use an automatically selected on, select the Specify Mailbox Database check box, and then click the Browse button to the right of the Mailbox Database text box. In the Select Mailbox Database dialog box, choose the mailbox database in which the mailbox should be stored. Mailbox databases are listed by name as well as by associated server.
12. Click Next. On the Master Account page, click Browse to the right of the Linked Forest text box. In the Select Trusted Forest Or Domain dialog box, select the linked forest or domain in which the user's original account is located and then click OK.

13. If you need additional administrative permissions to access the linked forest, select the Use The Following Windows Account check box. Then type the user name and password for an administrator account in this forest.
14. Click the Browse button to the right of the Linked Domain Controller text box. In the Select Domain Controller dialog box, select a domain controller in the linked forest and then click OK.
15. Click the Browse button to the right of the Linked Master Account text box. Use the options in the Select User dialog box to select the original user account in the linked forest, and then click OK.
16. Click Next, and then click New to create the account and the related mailbox. If an error occurs during account or mailbox creation, neither the account nor the related mailbox will be created. You will need to correct the problem and repeat this procedure.
17. Click Finish. For all mailbox-enabled accounts, an SMTP e-mail address is configured automatically.

In the Exchange Management Shell, you can create a user account with a linked mailbox by using the New-Mailbox cmdlet. Sample 6-2 provides the syntax and usage. You'll be prompted for two sets of credentials: one for the new user account and one for an administrator account in the linked forest.

SAMPLE 6-2 Creating linked mailboxes

Syntax

```
New-Mailbox -Name 'DisplayName' -Alias 'ExchangeAlias'
 -OrganizationalUnit 'OrganizationalUnit'
 -Database 'Database'
 -UserPrincipalName 'LogonName' -SamAccountName 'prewin2000logon'
 -FirstName 'FirstName' -Initials 'Initial' -LastName 'LastName'
 -ResetPasswordOnNextLogon State
 -LinkedDomainController 'LinkedDC'
 -LinkedMasterAccount 'domain\user'
 -LinkedCredential:(Get-Credential 'domain\administrator')
```

Usage

```
New-Mailbox -Name 'Wendy Richardson' -Alias 'wendyr'
 -OrganizationalUnit 'cpandl.com/Sales'
 -Database 'Corporate Services Primary'
 -UserPrincipalName 'wendyr@cpandl.com' -SamAccountName 'wendyr'
 -FirstName 'Wendy' -Initials '' -LastName 'Richardson'
 -ResetPasswordOnNextLogon $true
 -LinkedDomainController 'CohoDC58'
 -LinkedMasterAccount 'coho\wrichardson'
 -LinkedCredential:(Get-Credential 'coho\williams')
```

Creating Forwarding Mailboxes

Custom recipients, such as mail-enabled users and contacts, don't normally receive mail from users outside the organization because a custom recipient doesn't have an e-mail address that resolves to a specific mailbox in your organization. At times, though, you might want external users, applications, or mail systems to be able to send mail to an address within your organization and then have Exchange forward this mail to an external mailbox.

> ***TIP*** **You can send and receive text messages using Outlook Web App in Exchange 2010, or you can send text messages the old fashioned way. In my organization, I've created forwarding mailboxes for text-messaging and pager alerts. This simple solution lets managers (and monitoring systems) within the organization quickly and easily send text messages to IT personnel. Here, I've set up mail-enabled contacts for each text messaging e-mail address, such as 8085551212@adatum.com, and then created a mailbox that forwards e-mail to the custom recipient. Generally, the display name of the mail-enabled contact is in the form Alert *User Name*, such as Alert William Stanek. The display name and e-mail address for the mailbox are in the form Z *LastName* and AE-*MailAddress@myorg.com*, such as Z Stanek and AWilliamS@adatum.com, respectively. Afterward, I hide the mailbox so that it isn't displayed in the global address list or in other address lists; this way, users can see only the Alert William Stanek mailbox.**

To create a user account to receive mail and forward it off-site, follow these steps:

1. Using the Exchange Management Console, create a mail-enabled contact for the user. Name the contact Alert *User Name,* such as Alert William Stanek. Be sure to establish an external e-mail address for the contact that refers to the user's Internet address.
2. Using the Exchange Management Console, create a mailbox-enabled user account in the domain. Name the account with the appropriate display name, such as Z William Stanek. Be sure to create an Exchange mailbox for the account, but don't grant any special permission to the account. You might want to restrict the account so that the user can't log on to any servers in the domain.
3. Using the Exchange Management Console, access the Properties dialog box for the user's mailbox.
4. On the Mail Flow Settings tab, select Delivery Options and then click Properties.
5. In the Delivery Options dialog box, select the Forward To check box and then click Browse.
6. In the Select Recipient dialog box, select the mail-enabled contact you created earlier and then click OK three times. You can now use the user account to forward mail to the external mailbox.

Creating Archive Mailboxes

Each user can have an alternate mailbox for archives. An archive mailbox is used to store a user's old messages, such as might be required for executives and needed by some managers. In Outlook and Outlook Web App, users can access archive mailboxes in much the same way as they access their regular mailbox.

You can create a user's archive mailbox at the same time you create the user's standard mailbox. To create an archive mailbox, right-click the standard mailbox in the Exchange Management Console, select Enable Archive, review the dialog box, and then click Yes when prompted to confirm. Using the Exchange Management Shell, you can create an archive mailbox using Enable-Mailbox. The basic syntax is as follows:

```
Enable-Mailbox [-Identity] Identity –Archive
```

such as:

```
enable-mailbox cpandl.com/engineering/tonyg –archive
```

Because each user can have only one archive mailbox, you get an error if the user already has an archive mailbox. Items in the user's mailbox will be moved automatically to the archive mailbox based on the default retention policy. When you install Exchange Server, a default retention policy is created for all archive mailboxes.

Whether you use the Exchange Management Console or the Exchange Management Shell, several other parameters are set for archive mailboxes. The default name for the archive mailbox is set as Online Archive – *UserDisplayName,* such as Online Archive – Vamsi Kuppa. The default quota and warning quota are set as unlimited.

You can change the archive name and set quotas by using Set-Mailbox. The basic syntax is as follows:

```
Set-Mailbox [-Identity] Identity –ArchiveName Name
-ArchiveQuota Quota -ArchiveWarningQuota Quota
```

When you set a quota, specify the value with MB (for megabytes), GB (for gigabytes), or TB (for terabytes), or enter 'Unlimited' to remove the quota. Here is an example:

```
set-mailbox cpandl.com/engineering/tonyg
-ArchiveQuota '2GB' -ArchiveWarningQuota '900MB'
```

In the Exchange Management Console, you can set or remove a quota warning for an archive mailbox by right-clicking the entry for the user's standard mailbox and selecting Properties. In the Properties dialog box, on the Mailbox Settings tab, double-click Archive Quota. To set a quota warning, select Issue Warning At, and then enter a quota in megabytes. To remove a quota, clear Issue Warning At.

To disable an archive mailbox, right-click the mailbox in the Exchange Management Console, select Disable Archive, and then click Yes when prompted to confirm. In the Exchange Management Shell, you can disable an archive mailbox by using Disable-Mailbox. The basic syntax is as follows:

```
Disable-Mailbox [-Identity] Identity –Archive
```

such as:

```
disable-mailbox cpandl.com/engineering/tonyg –archive
```

Creating Arbitration Mailboxes

Exchange moderated transport requires all e-mail messages sent to specific recipients to be approved by moderators. You can configure any type of recipient as a moderated recipient, and Exchange will ensure that all messages sent to those recipients go through an approval process.

Distribution groups are the only types of recipients that use moderation by default. Membership in distribution groups can be closed, owner approved or open. While any Exchange recipient can join an open distribution group, joining a closed group requires approval. Group owners receive join and remove requests and can either approve or deny those requests.

Distribution groups can also be unmoderated or moderated. With unmoderated groups, any approved sender (which is all senders by default) can send messages to the group. With moderated groups, messages are sent to moderators for approval before being distributed to members of the group. The only exception is for a message sent by a moderator. A message from a moderator is delivered immediately because a moderator has the authority to determine what is and isn't an appropriate message.

NOTE **The default moderator for a distribution group is the group's owner.**

Arbitration mailboxes are used to store messages that are awaiting approval. When you install Exchange Server 2010, a default arbitration mailbox is created. For the purposes of load balancing or for other reasons, you can convert other mailboxes to the Arbitration mailbox type by using the Enable-Mailbox cmdlet. The basic syntax is as follows:

```
Enable-Mailbox [-Identity] Identity –Arbitration
```

such as:

```
enable-mailbox cpandl.com/users/moderatedmail –Arbitration
```

You can create an arbitration mailbox by using New-Mailbox as shown in this example:

```
New-Mailbox ModeratedMail -Arbitration -UserPrincipalName
ModeratedMail@cpandl.com
```

Creating Discovery Mailboxes

Exchange Discovery helps organizations comply with legal discovery requirements and can also be used as an aid in internal investigations or as part of regular monitoring of e-mail content. Exchange Discovery uses content indexes created by Exchange Search to speed up the search process.

> ***NOTE*** **By default, Exchange administrators do not have sufficient rights to perform Discovery searches. Only users with the Discovery Management role can perform Discovery searches.**

You use the Exchange Control Panel (ECP) to perform searches. After you log on, click Reporting in the left pane, and then click the Mailbox Searches tab. Discovery searches are performed against designated mailboxes or all mailboxes in the Exchange organization. Items in mailboxes that match the Discovery search are copied to a target mailbox. Only mailboxes specifically designated as Discovery mailboxes can be used as targets.

> ***TIP*** **By default, Discovery search does not include items that cannot be indexed by Exchange Search. To include such items in the search results, select the Include Items That Can't Be Searched check box in Exchange Control Panel.**

When you install Exchange Server 2010, a default discovery mailbox is created. You can convert other mailboxes to the Discovery mailbox type by using the Enable-Mailbox cmdlet. The basic syntax is as follows:

```
Enable-Mailbox [-Identity] Identity -Discovery
```

such as:

```
enable-mailbox cpandl.com/hr/legalsearch -discovery
```

You can create a Discovery mailbox by using New-Mailbox as shown in this example:

```
New-Mailbox LegalSearch -Discovery -UserPrincipalName
LegalSearch@cpandl.com
```

Once a Discovery mailbox is established, you can't convert it to another mailbox type. You can't use Exchange Management Console to create Discovery mailboxes.

Creating Shared Mailboxes

Shared mailboxes are mailboxes that are shared by multiple users. Although shared mailboxes must have an associated user account, this account is not used for logon in the domain and is disabled by default. Users who access the shared mailbox do so using access permissions.

You can create a shared mailbox by using New-Mailbox, as shown in this example:

```
New-Mailbox CustomerService -Shared -UserPrincipalName
customerservice@cpandl.com
```

A user account named CustomerService is created for this mailbox. This user account is disabled by default to prevent logon using this account. To share the mailbox with users who need to be able to access it, right-click the mailbox in the Exchange Management Console, select Manage Full Access Permission, and then follow the prompts.

Managing Mailboxes: The Essentials

You often need to manage mailboxes the way you do user accounts. Some of the management tasks are intuitive and others aren't. If you have questions, be sure to read the sections that follow.

You can work with multiple recipients at the same time. To select multiple resources not in sequence, hold down the Ctrl key and then click the left mouse button on each resource you want to select. To select a series of resources, select the first resource, hold down the Shift key, and then click the last resource.

The actions you can perform on multiple resources depend on the types of recipients you've selected. Generally, you'll want to work with recipients of the same type, such as either user mailboxes or room mailboxes, but not both types at the same time. The actions you can perform on multiple mailboxes include:

- Disable
- Disable Archive
- New Local Move Request
- New Remote Move Request
- Remove
- Send Mail

You also can edit the properties of multiple recipients at the same time. To do this, select the recipients you want to work with, right-click and then select Properties. Just about any property that can be set for an individual recipient can be set for multiple recipients.

TIP **If the Properties option isn't available when you right-click, you've probably selected one or more recipients of different types. For example, you might have intended to select only user mailboxes but selected a room mailbox as well.**

Viewing Current Mailbox Size, Message Count, and Last Logon

You can use the Exchange Management Console to view who last logged on to a mailbox, the last logon date and time, the mailbox size, and the message count by completing these steps:

1. Expand the Recipient Configuration node and then select the Mailbox node.
2. Double-click the mailbox with which you want to work.
3. On the General tab, the Last Logged On By text box shows who last logged on to the mailbox, and the Modified entry shows the date and time the mailbox was last modified. (See Figure 6-3.)
4. On the General tab, the Total Items and Size (KB) areas show the number of messages in the mailbox and the current mailbox size in kilobytes, respectively.

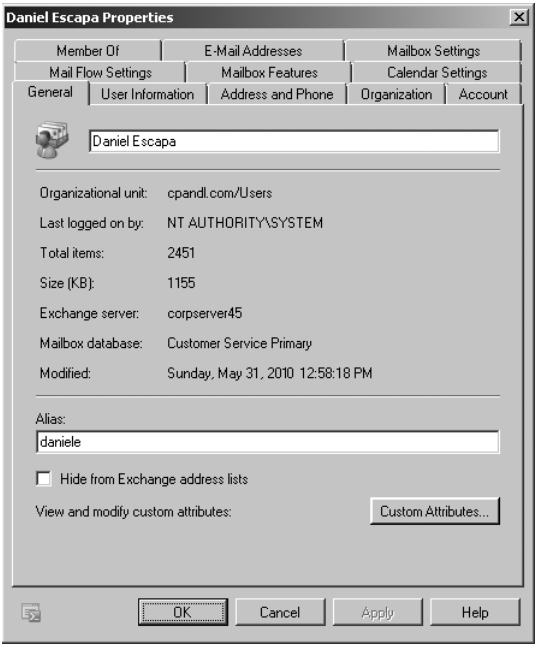


FIGURE 6-3 View mailbox statistics.

If you want to view similar information for all mailboxes on a server, the easiest way is to use the Get-MailboxStatistics cmdlet. Sample 6-3 shows examples using this cmdlet. Use the –Archive parameter to return mailbox statistics for the archive mailbox associated with a specified mailbox.

SAMPLE 6-3 Getting statistics for multiple mailboxes

Syntax

```
Get-MailboxStatistics -Identity 'Identity' [-Archive <$true|$false>]
[-DomainContoller DomainController] [-IncludeMoveHistory <$true|$false>]
[-IncludeMoveReport <$true|$false>]

Get-MailboxStatistics -Server  'Server' | -Database 'Database'
[-DomainContoller DomainController]
```

Usage

```
Get-MailboxStatistics -Server  'corpsvr127'

Get-MailboxStatistics -Database 'Engineering Primary'

Get-MailboxStatistics –Identity 'cpandl\williams'
```

When you are working with the Exchange Management Shell, the standard output won't necessarily provide all the information you are looking for. Often, you need to format the output as a list or table using Format-List or Format-Table, respectively, to get the additional information you are looking for. Format-List comes in handy when you are working with a small set of resources or want to view all the properties that are available. Once you know what properties are available for a particular resource, you can format the output as a table to view specific properties. For example, if you format the output of Get-MailboxStatistics as a list, you see all the properties that are available for mailboxes, as shown in this example and sample output:

```
get-mailboxstatistics -identity "cpandl\daniele" | format-list
```

```
AssociatedItemCount     : 2655
DeletedItemCount        : 121
DisconnectDate          :
DisplayName             : Daniel Escapa
ItemCount               : 2451
LastLoggedOnUserAccount : NT AUTHORITY\SYSTEM
LastLogoffTime          : 6/15/2010 12:58:18 PM
LastLogonTime           : 6/15/2010 12:58:14 PM
LegacyDN                : /O=FIRST ORGANIZATION/OU=EXCHANGE
ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=DANIEL ESCAPA
MailboxGuid             : d3f6ce55-fe3d-4beb-ae65-9c9f7edaf995c
```

```
ObjectClass              : Mailbox
StorageLimitStatus       : BelowLimit
TotalDeletedItemSize     : 97 KB (97,235 bytes)
TotalItemSize            : 1155.11 KB (1,155,445 bytes)
Database                 : Customer Service Primary
ServerName               : CORPSERVER45
DatabaseName             : Customer Service Primary
MoveHistory              :
IsQuarantined            : False
IsArchiveMailbox         : False
Identity                 : d3f6ce44-fe0c-4beb-ae79-9c9f8eaf123c
MapiIdentity             : d3f6ce44-fe0c-4beb-ae79-9c9f8eaf123c
OriginatingServer        : corpserver45.cpandl.com
IsValid                  : True
```

Once you know the available properties, you can format the output as a table to get exactly the information you want to see. In this example, you get information about all the mailboxes in the Engineering Primary database and format the output as a table:

```
Get-MailboxStatistics -Database 'Engineering Primary' | format-table
DisplayName, TotalItemSize, TotalDeletedItemSize, Database, ServerName
```

Setting Alternate Mailbox Display Names for Multilanguage Environments

In some cases, the full display name for a mailbox won't be available for display. This can happen when multiple language versions of the Exchange snap-in are installed on the network or when multiple language packs are installed on a system. Here, the system cannot interpret some or all of the characters in the display name and, as a result, doesn't show the display name. To correct this problem, you can set an alternate display name using a different character set. For example, you could use Cyrillic or Kanji characters instead of standard ANSI characters.

You can set an alternate display name for a mailbox by following these steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the User Information tab, type the alternate display name in the Simple Display Name text box and then click OK.

Hiding Mailboxes from Address Lists

Occasionally, you might want to hide a mailbox so that it doesn't appear in the global address list or other address lists. One reason for doing this is if you have administrative mailboxes that you use only for special purposes. To hide a mailbox from the address lists, follow these steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the General tab, select the Hide From Exchange Address Lists check box and then click OK.

Defining Custom Mailbox Attributes for Address Lists

Address lists, such as the global address list, make it easier for users and administrators to find available Exchange resources, including users, contacts, distribution groups, and public folders. The fields available for Exchange resources are based on the type of resource. If you want to add more values that should be displayed or searchable in address lists, such as an employee identification number, you can assign these values as custom attributes.

Exchange provides 15 custom attributes—labeled Customer Attribute 1, Custom Attribute 2, and so on through Custom Attribute 15. You can assign a value to a custom attribute by completing the following steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the General tab, click Custom Attributes. The Custom Attributes dialog box appears.
3. Enter attribute values in the text boxes provided, and click OK twice.

Moving Mailboxes

To complete an upgrade, balance the server load, manage drive space, or relocate mailboxes when users move to a different location, you can move mailboxes from one server or database to another server or database. Exchange Server 2010 supports online mailbox moves.

Moving Mailboxes: The Essentials

In earlier releases of Exchange, moving mailboxes while they were actively being used wasn't a good idea because it caused some disruption to the affected users. For this reason, Exchange Server 2010 performs move operations as a series of steps that allow a mailbox to remain available to a user while the move operation is being completed. When the move is completed, the user begins accessing the mailbox in the new location. Because users can continue to access their e-mail account during the move, you can perform online moves at any time.

The destination database for a move can be on the same server, on a different server, in a different domain, in a different Active Directory site, or in another forest. However, some caveats apply:

- When your source and destination Mailbox servers are running Exchange Server 2010 or Exchange Server 2007 SP2 or later and are in the same or different forests, you can use the Exchange Management Console or the

New-MoveRequest cmdlet to perform an online mailbox move. This might be necessary when you are moving mailboxes between an on-premises and an online Exchange organization. You perform the move from the Exchange 2010 Mailbox server. You can't move mailboxes from Exchange 2007 SP1 or earlier.

- When your source servers are running Exchange Server 2003 SP2 or later and your destination servers are running Exchange Server 2010, you cannot perform an online mailbox move. You need to perform an offline mailbox move instead. You do this by starting the move operation on the Exchange 2010 Mailbox server with the New-MoveRequest cmdlet. You can't move mailboxes from Exchange 2003 SP1 or earlier.

Performing online moves is a multistep process that is initiated with a Move Mailbox request that is sent to the Microsoft Exchange Mailbox Replication Service (MRS) running on a Client Access server in the source forest. The MRS queues the request for processing, handling all requests on a first-in, first-out basis. When a request is at the top of the queue, the replication service begins replicating mailbox data to the destination database. When the replication service finishes its initial replication of a mailbox, it marks the mailbox as Ready To Complete and periodically performs data synchronization between the source and destination database to ensure that the contents of a mailbox are up to date. After a mailbox has been moved, you can complete the move request and finalize the move.

In the Exchange Management Console, you can track the status of move requests by expanding Recipient Configuration and then selecting the Move Request node (see Figure 6-4). If a move request fails, you can get more information about the failure by double-clicking the move request and then clicking the View button to the right of the Failed Message entry.

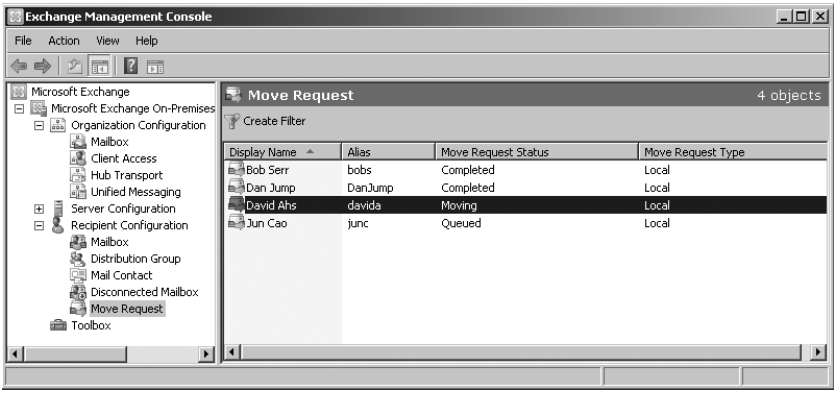


FIGURE 6-4 Check the status of move requests.

When you move mailboxes from one server to another, or even to a different database on the same sever, keep in mind that the Exchange policies of the new mailbox database might be different from the old one. Because of this, consider the following issues before you move mailboxes to a new server or database:

- **General policy** Changes to watch out for include those in the default public folder database, the offline address book, and message settings. The risk is that the users whose mailboxes you move could lose or gain access to public folders. They might have a different offline address book, which might have different entries. This address book will also have to be downloaded in its entirety the first time the user's mail client connects to Exchange after the move.
- **Database policy** Changes to watch out for pertain to the maintenance interval and automatic mounting. If Exchange performs maintenance when these users are accessing their mail, they might have slower response times. If the mailbox database is configured so that it isn't mounted at startup, restarting the Exchange services could result in the users not being able to access their mailboxes.
- **Limits** Changes to watch out for pertain to storage limits and deletion settings. Users might be prohibited from sending and receiving mail if their mailbox exceeds the storage limits of the new mailbox database. Users might notice that deleted items stay in their Deleted Items folder longer or are deleted sooner than expected if the Keep Deleted Items setting is different.

Performing Online Mailbox Moves

With online moves, you can move mailboxes between databases on the same server. You also can move mailboxes from a database on one server to a database on another server regardless of whether the servers are in a different Active Directory site or in another Active Directory forest.

Normally, when you perform online moves, the move process looks like this:

1. You create a new move request for the mailbox or mailboxes that you want to move using either the Exchange Management Console or Exchange Management Shell.
2. The move request is sent to the Mailbox Replication Service running on a Client Access server in the current Active Directory site. This server acts as the Mailbox Replication Service proxy.
3. The Mailbox Replication Service (MRS) adds the mailboxes to the Move Request queue and assigns the status Queued For Move to each mailbox. This indicates the move has been requested but the move has not started.
4. When a move request is at the top of the queue, the MRS begins replicating the related mailbox to the destination database and assigns the Move In Progress status to mailboxes being moved. By default, the replication service can move up to 5 mailboxes on a single database at one time and up to 50 mailboxes at a time in total.

5. When the MRS finishes its initial replication of the mailbox, the service assigns the Ready To Complete status to the mailbox.
6. The mailbox remains in the Ready To Complete state until you or another administrator specifies that you either want to complete the move request or cancel the move request. If you complete the move request, the MRS assigns the Completing status while it performs a final data synchronization and then marks the move as completed.
7. When the move is completed, the mailbox or mailboxes are available in the new location. Because users can continue to access their e-mail account during a move, you can perform online moves at any time.

One way to perform online mailbox moves within the same Exchange forest is by using the Exchange Management Shell. The commands for performing online mailbox moves include the following:

- **Get-MoveRequest** View the detailed status of an ongoing mailbox move that was initiated using the New-MoveRequest cmdlet.

```
Get-MoveRequest -Identity Identity [-Credential Credential]
[-DomainController FullyQualifiedName] [-Organization
OrganizationId] [-OrganizationalUnit OrganizationalUnitId]
[-ResultSize Size] [-SortBy String]


Get-MoveRequest [-BatchName BatchRequestName] [-Credential
Credential] [-DomainController FullyQualifiedName]
[-MoveStatus Status] [-Offline <$true | $false>]
[-Organization OrganizationId] [-OrganizationalUnit
OrganizationalUnitId>] [-Protect <$true | $false>]
[-RemoteHostName FullyQualifiedName] [-ResultSize Size]
[-SortBy String] [-SourceDataBase DatabaseId]
[-Suspend <$true | $false>]
[-SuspendWhenReadyToComplete <$true | $false>]
[-TargetDatabase DatabaseId]
```

- **New-MoveRequest** Start a mailbox move. You also can verify readiness to move by using the –WhatIf parameter. Use the –Protect parameter to protect the move request for tenant administrators.

```
New-MoveRequest -Identity Identity [-TargetDatabase DatabaseId]
{AddtlParams}

New-MoveRequest -Identity Identity -Remote {$true | $false}
–RemoteHostName HostName –TargetDeliveryDomain Domain
[-RemoteCredential Credential] [-RemoteGlobalCatalog GCServer]
[-RemoteTargetDatabase DatabaseID] [-TargetDatabase DatabaseID]
{AddtlParams}

New–MoveRequest –Identity Identity -RemoteGlobalCatalog GCServer
-RemoteLegacy <$true|$false> -TargetDeliveryDomain Domain
```

```
[-RemoteCredential Credential] [-RemoteTargetDatabase DatabaseID]
[-TargetDatabase DatabaseID] {AddtlParams}


{AddtlParams}
[-BadItemLimit Limit] [-BatchName BatchRequestName]
[-DomainController FullyQualifiedName] [-IgnoreRuleLimitErrors
<$true|$false>] [-MRSServer CASServer] [-Protect
<$true|$false>] [-Suspend <$true|$false>] [-SuspendComment String]
[-SuspendWhenReadyToComplete <$true|$false>]
```

- **Resume-MoveRequest** Resumes a move request that has been suspended or failed.

```
Resume-MoveRequest -Identity MoveRequestIdentity
[-DomainController FullyQualifiedName]
```

- **Set-MoveRequest** Changes a move request after it has been started.

```
Set-MoveRequest -Identity MoveRequestIdentity
[-BadItemLimit Limit] [-DomainController FullyQualifiedName]
[-IgnoreRuleLimitErrors <$true|$false>] [-Protect <$true|$false>]
[-RemoteCredential Credential] [-RemoteGlobalCatalog GCServer]
[-RemoteHostName HostName] [-SuspendWhenReadyToComplete
<$true|$false>]
```

- **Suspend-MoveRequest** Suspends a move request that has been started but has not yet been completed.

```
Suspend-MoveRequest -Identity MoveRequestIdentity
[-SuspendComment Comment]
[-DomainController FullyQualifiedName]
```

- **Remove-MoveRequest** Cancels a mailbox move initiated using the New-MoveRequest cmdlet. You can use the Remove-MoveRequest command any time after initiating the move but only if the move request is not yet complete. If the move request was initiated with the –Protect parameter, you must use the –Protect parameter to cancel the move request.

```
Remove-MoveRequest -Identity Identity [-MRSServer CASServer]
[-DomainController FullyQualifiedName] [-Protect {$true | $false}]
```

Moving Mailboxes Within a Single Forest

You perform online mailbox moves within a single forest by using the Exchange Management Shell. To verify move readiness, use New-MoveRequest with the –WhatIf parameter for each mailbox you plan to move. The following examples

show two different ways you can verify whether Garrett Vargas's mailbox can be moved:

```
New-MoveRequest -Identity 'garrettv'
-TargetDatabase "Engineering Primary" -WhatIf

'cpandl.com/users/Garrett Vargas' | New-MoveRequest –TargetDatabase
'Engineering Primary' -WhatIf
```

To initiate an online move, you use New-MoveRequest for each mailbox you want to move. The following examples show two different ways you can move Garrett Vargas's mailbox:

```
New-MoveRequest -Identity 'garrettv' –Remote –RemoteHostName
'mailserver17.cpandl.com' -mrsserver 'casserver21.cpandl.com'
-TargetDatabase "Engineering Primary"

'cpandl.com/users/Garrett Vargas' | New-MoveRequest –Remote
–RemoteHostName 'mailserver17.cpandl.com' –mrsserver
'casserver21.cpandl.com' -TargetDatabase 'Engineering Primary'
```

After you initiate a move, you can check the status of the online move using Get-MoveRequest. As shown in the following example, the key parameter to provide is the identity of the mailbox you want to check:

```
Get-MoveRequest –Identity 'garrettv'
```

By default, basic information about the move request is displayed. To get more detailed information, add the –IncludeReport parameter as shown in this example:

```
Get-MoveRequest –Identity 'garrettv' -IncludeReport
```

You can use Suspend-MoveRequest to suspend a move request that has not yet completed, and Resume-MoveRequest to resume a suspended move request. Resuming a suspended request allows it to complete.

You can cancel a move at any time prior to running the move request being completed by Exchange. To do this, run Remove-MoveRequest and specify the identity of the mailbox that shouldn't be moved. An example follows:

```
Remove-MoveRequest –Identity 'garrettv'
```

When your source and destination Mailbox servers are running Exchange Server 2010 and are in the same forest, you can move mailboxes by completing these steps:

1. In the Exchange Management Console, expand the Recipient Configuration node, and then select the related Mailbox node.

2. Right-click the mailbox, and then select New Local Move Request. This starts the New Local Move Request Wizard, as shown in Figure 6-5.

TIP **You can select and move multiple mailboxes at the same time. To select multiple users individually, hold down the Ctrl key, and then click each user account that you want to select. To select a sequence of accounts, select the first user account, hold down the Shift key, and then click the last user account.**

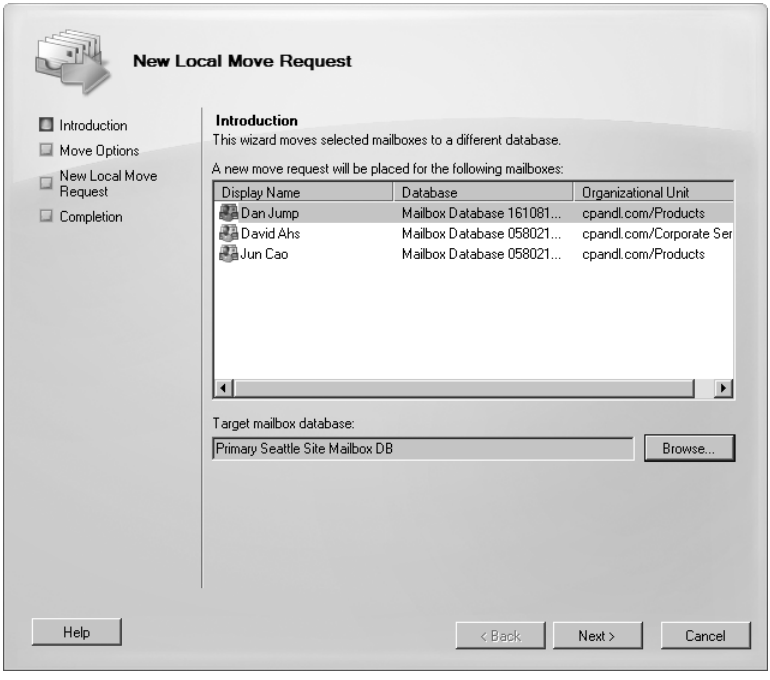


FIGURE 6-5 Use the New Local Move Request Wizard to move mailboxes.

3. Click the Browse button to the right of the Target Mailbox Database text box. In the Select Mailbox Database dialog box, choose the mailbox database to which the mailbox should be moved. Mailbox databases are listed by name as well as by associated server.
4. Click Next. If corrupted messages are found in a mailbox, specify how you would like those messages to be handled. To skip the mailbox if corrupted messages are found, select Skip The Mailbox. To skip the corrupted messages if any are found but still move the mailbox, select Skip The Corrupted Messages.
5. If you elected to skip corrupted messages, you must also specify the maximum number of corrupted messages to skip. If this value is exceeded, the mailbox will not be moved.

6. When you click Next and then click New, Exchange Server creates a new move request. Click Finish.
7. Moving mailboxes can take several hours, depending on the size of the mailboxes you are moving. You can check the status of move requests by selecting the Move Request node under Recipient Configuration. While the move request is in the Moving or Queued state, you can cancel the move request by right-clicking it and then selecting Remove Move Request.

Moving Mailboxes Between Forests

You can perform online mailbox moves between different Exchange forests using the Exchange Management Console or Exchange Management Shell. When you are moving mailboxes between forests, you'll want to verify that mailboxes are ready to be moved before you submit a move request. To verify readiness, the Microsoft Exchange Mailbox Replication service proxy in the source forest checks the status of each mailbox you are moving and also ensures you have the permissions required to move the mailboxes from the source forest to the target forest. If a user has an archive mailbox or subscriptions, you will likely need to remove the archive mailbox, the subscriptions, or both before you are able to move the mailbox.

You can verify move readiness in the Exchange Management Shell by using New-MoveRequest with the –WhatIf parameter for each mailbox you plan to move. The following examples show two different ways you can verify whether Charlie Keen's mailbox can be moved:

```
New-MoveRequest -Identity 'charliek' –Remote
–RemoteHost 'mailserver17.cpandl.com'-mrsserver 'casserver21.cpandl.com'
-TargetDatabase "Engineering Primary" -WhatIf

'cpandl.com/users/Charlie Keen' | New-MoveRequest –Remote
–RemoteHost 'mailserver17.cpandl.com' -mrsserver 'casserver21.cpandl.com'
-TargetDatabase 'Engineering Primary' -WhatIf
```

You can perform online mailbox moves between forests by following these steps:

1. In the Exchange Management Console, select the mailbox or mailboxes that you want to move. Right-click, and then select New Remote Move Request. This starts the New Remote Move Request Wizard.

   The mailboxes you selected are listed as the ones that will be moved. Click Next.
2. The source forest is the forest to which you are connected. In the Target Forest list, select the forest to which you are moving the mailboxes.
3. In the text box provided, type the fully qualified domain name of a Client Access server in the source forest that will act as the proxy server.

4. If you want to provide alternate credentials for the source forest, select the Use The Following Source Forest's Credential, type the user name, and then type the password for the account.
5. When the move request is complete, mail sent to the relocated users in the source forest will be redirected to the target forest. Enter the post-move external e-mail address for the user or users in the source forest.
6. When you click Next and then click New to initiate the move request, the Exchange Management Console calls into the shell and the shell runs New-MoveRequest for each mailbox you selected. Moving the mailboxes can take several hours, depending on the size of the mailboxes you are moving.

You can perform online moves in the Exchange Management Shell by using New-M oveRequest for each mailbox you plan to move. The following examples show two different ways you can move Bruno Denuit's mailbox:

```
New-MoveRequest -Identity 'brunod' –Remote
–RemoteHost 'mailserver17.cpandl.com'-mrsserver 'casserver21.cpandl.com'
-TargetDatabase "Engineering Primary"

'cpandl.com/users/Bruno Denuit' | New-MoveRequest –Remote
–RemoteHost 'mailserver17.cpandl.com' -mrsserver 'casserver21.cpandl.com'
-TargetDatabase 'Engineering Primary'
```

After you initiate a move, you can check the status of the online move by using Get-MoveRequest. As shown in the following example, the key parameters to provide are the identity of the mailbox you want to check and the name of the proxy server:

```
Get-MoveRequest –Identity 'brunod' -mrsserver 'casserver21.cpandl.com'
```

By default, basic information about the move request is displayed. To get more detailed information, add the –IncludeReport parameter as shown in this example:

```
Get-MoveRequest –Identity 'brunod' -mrsserver 'casserver21.cpandl.com'
-IncludeReport
```

You can use Suspend-MoveRequest to suspend a move request that is not yet complete, and Resume-MoveRequest to resume a suspended move request. Resuming a suspended request allows it to complete.

At any time prior to running the move request completing, you can cancel the move by running Remove-MoveRequest and specifying the identify of the mailbox that shouldn't be moved, such as:

```
Remove-MoveRequest –Identity 'brunod' -mrsserver 'casserver21.cpandl.com'
```

Configuring Mailbox Delivery Restrictions, Permissions, and Storage Limits

You use mailbox properties to set delivery restrictions, permissions, and storage limits. To change these configuration settings for mailboxes, follow the techniques discussed in this section.

Setting Message Size Restrictions for Contacts

You set message size restrictions for contacts in much the same way that you set size restrictions for users. Follow the steps listed in the next section.

Setting Message Size Restrictions on Delivery to and from Individual Mailboxes

Using the When The Size Of Any Attachment Is Greater Than Or Equal To Limit transport rule condition, you can set restrictions regarding the size of message attachments and specify what action to take if a message has an attachment that exceeds this limit. Sometimes, you need to set exceptions for specific users. For example, some users might need to be able to send large files as part of their job.

You set individual delivery restrictions by completing the following steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the Mail Flow Settings tab, double-click Message Size Restrictions. As shown in Figure 6-6, you can now set the following send and receive restrictions:

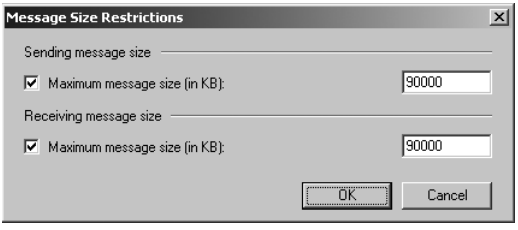


FIGURE 6-6 You can apply individual delivery restrictions on a per-user basis.

   - **Sending Message Size** Sets a limit on the size of messages the user can send. The value is set in kilobytes (KBs). If an outgoing message exceeds the limit, the message isn't sent and the user receives a non-delivery report (NDR).
   - **Receiving Message Size** Sets a limit on the size of messages the user can receive. The value is set in KBs. If an incoming message exceeds the limit, the message isn't delivered and the sender receives an NDR.
3. Click OK. The restrictions that you set override the global default settings.

Setting Send and Receive Restrictions for Contacts

You set message send and receive restrictions for contacts in the same way that you set these restrictions for users. Follow the steps listed in the next section.

Setting Message Send and Receive Restrictions on Individual Mailboxes

By default, user mailboxes are configured to accept messages from anyone. To override this behavior, you can do the following:

- Specify that only messages from the listed users, contacts, or groups be accepted.
- Specify that messages from specific users, contacts, or groups listed be rejected.
- Specify that only authenticated users—meaning users who have logged on to the Exchange system or the domain—be accepted.

You set message send and receive restrictions by completing the following steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the Mail Flow Settings tab, double-click Message Delivery Restrictions. As shown in Figure 6-7, you can now set message acceptance restrictions.

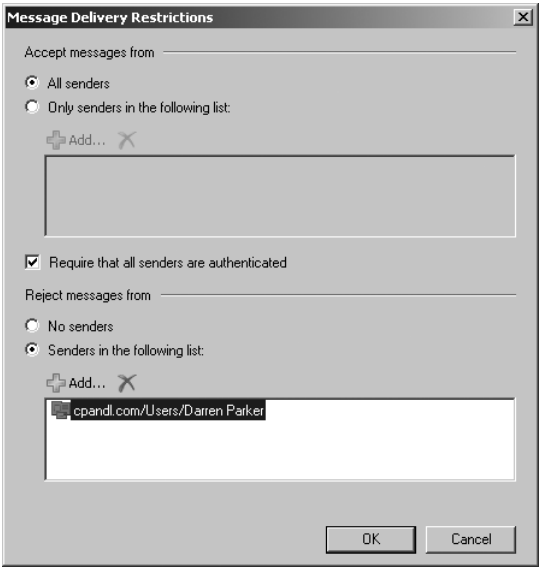


FIGURE 6-7 You can apply send and receive restrictions on messages on a per-user basis.

3. If you want to ensure that messages are accepted only from authenticated users, select the Require That All Senders Are Authenticated check box.

4. To accept messages from all e-mail addresses except those on the reject list, under Accept Messages From, select All Senders.
5. To specify that only messages from the listed users, contacts, or groups be accepted, select the Only Senders In The Following List option and then add acceptable recipients by following these steps:
   - Click Add to display the Select Recipient dialog box.
   - Select a recipient, and then click OK. Repeat as necessary.

   TIP **You can select multiple recipients at the same time. To select multiple recipients individually, hold down the Ctrl key and then click each recipient that you want to select. To select a sequence of recipients, select the first recipient, hold down the Shift key, and then click the last recipient.**

6. To specify that no recipients should be rejected, under Reject Messages From, select No Senders.
7. To reject messages from specific recipients, under Reject Messages From, select Senders In The Following List and then add unacceptable recipients by following these steps:
   - Click Add to display the Select Recipients dialog box.
   - Select a recipient, and then click OK. Repeat as necessary.
8. Click OK.

Permitting Others to Access a Mailbox

Occasionally, users need to access someone else's mailbox, and in certain situations, you should allow this. For example, if John is Susan's manager and Susan is going on vacation, John might need access to her mailbox while she's away. Another situation in which someone might need access to another mailbox is when you've set up special-purpose mailboxes, such as a mailbox for Webmaster@domain.com or a mailbox for Info@domain.com.

You can grant permissions for a mailbox in two ways:

- You can grant access to a mailbox and its content.
- You can grant the right to send messages as the mailbox owner.

If you want to grant access to a mailbox and its contents but not grant Send As permissions, use the Manage Full Access Permission Wizard. In the Exchange Management Console, right-click the mailbox you want to work with and then select Manage Full Access Permission. In the Manage Full Access Permission Wizard, click Add, and then use the Select User Or Group dialog box to choose the user or users who should have access to the mailbox. To revoke the authority to access the mailbox, select an existing user name in the Security Principal list box and then click Remove. Click Manage to set the desired access permissions.

If you want to grant Send As permissions, use the Manage Send As Permission Wizard. In the Exchange Management Console, right-click the mailbox you want

to work with and then select Manage Send As Permission. In the Manage Send As Permission Wizard, click Add, and then use the Select Recipient dialog box to choose the user or users who should have this permission. To revoke this permission, select an existing user name in the Security Principal list box and then click Remove. Click Manage to set the desired Send As permissions.

In the Exchange Management Shell, you can use the Add-MailboxPermission and Remove-MailboxPermission cmdlets to manage full access permissions. Samples 6-4 and 6-5 show examples of using these cmdlets. In these examples, the AccessRights parameter is set to FullAccess to indicate you are setting full access permissions on the mailbox.

SAMPLE 6-4 Adding full access permissions

Syntax

```
Add-MailboxPermission –Identity UserBeingGrantedPermission
 –User UserWhoseMailboxIsBeingConfigured –AccessRights 'FullAccess'
```

Usage

```
Add-MailboxPermission –Identity
'CN=Jerry Orman,OU=Engineering,DC=cpandl,DC=com'
–User 'CPANDL\boba' –AccessRights 'FullAccess'
```

SAMPLE 6-5 Removing full access permissions

Syntax

```
Remove-MailboxPermission –Identity 'UserBeingGrantedPermission'
 –User 'UserWhose'MailboxIsBeingConfigured' –AccessRights 'FullAccess'
–InheritanceType 'All'
```

Usage

```
Remove-MailboxPermission –Identity 'CN=Jerry Orman,
OU=Engineering,DC=cpandl,DC=com'
 –User 'CPANDL\boba' –AccessRights 'FullAccess' –InheritanceType 'All'
```

If you want to allow another user to send messages as the mailbox owner, you can do this using the Manage Send As Permission Wizard. In the Exchange Management Console, right-click the mailbox you want to work with and then select Manage Send As Permission. In the Manage Send As Permission Wizard, click Add, and then use the Select User Or Group dialog box to choose the user or users who should have Send As permission on the mailbox. To revoke Send As permission, select an existing user name in the Security Principal list box and then click Remove. Click Manage to set the desired access permissions.

In the Exchange Management Shell, you can use the Add-ADPermission and Remove-ADPermission cmdlets to manage Send As permissions. Samples 6-6 and 6-7 show examples using these cmdlets. In these examples, the ExtendedRights parameter is set to Send-As to indicate you are setting Send As permissions on the mailbox.

SAMPLE 6-6 Adding Send As permissions

Syntax

```
Add-ADPermission -Identity UserBeingGrantedPermission
-User UserWhoseMailboxIsBeingConfigured -ExtendedRights 'Send-As'
```

Usage

```
Add-ADPermission -Identity 'CN=Jerry
Orman,OU=Engineering,DC=cpandl,DC=com'
-User 'CPANDL\boba' -ExtendedRights 'Send-As'
```

SAMPLE 6-7 Removing Send As permissions

Syntax

```
Remove-ADPermission -Identity UserBeingRevokedPermission
-User UserWhoseMailboxIsBeingConfigured -ExtendedRights 'Send-As'
-InheritanceType 'All' -ChildObjectTypes $null
-InheritedObjectType $null -Properties $null
```

Usage

```
Remove-ADPermission -Identity 'CN=Jerry
Orman,OU=Engineering, DC=cpandl,DC=com'
 -User 'CPANDL\boba' -ExtendedRights 'Send-As' -InheritanceType 'All'
-ChildObjectTypes $null -InheritedObjectTypes $null
-Properties $null
```

NOTE **Another way to grant access permissions to mailboxes is to do so through Outlook. Using Outlook, you have more granular control over permissions. You can allow a user to log on as the mailbox owner, delegate mailbox access, and grant various levels of access. For more information on this issue, see the "Accessing Multiple Exchange Server Mailboxes" and "Granting Permission to Access Folders Without Delegating Access" sections in Chapter 16.**

Forwarding E-Mail to a New Address

Except when rights management prevents it, any messages sent to a user's mailbox can be forwarded to another recipient. This recipient can be another user or a mail-enabled contact. You can also specify that messages should be delivered to both the forwarding address and the current mailbox.

To configure mail forwarding, follow these steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the Mail Flow Settings tab, double-click Delivery Options.
3. To remove forwarding, in the Forwarding Address panel, clear the Forward To check box.
4. To add forwarding, select the Forward To check box and then click Browse. Use the Select Recipient dialog box to choose the alternate recipient.
5. If messages should go to both the alternate recipient and the current mailbox owner, select the Deliver Messages To Both Forwarding Address And Mailbox check box. (See Figure 6-8.) Click OK.

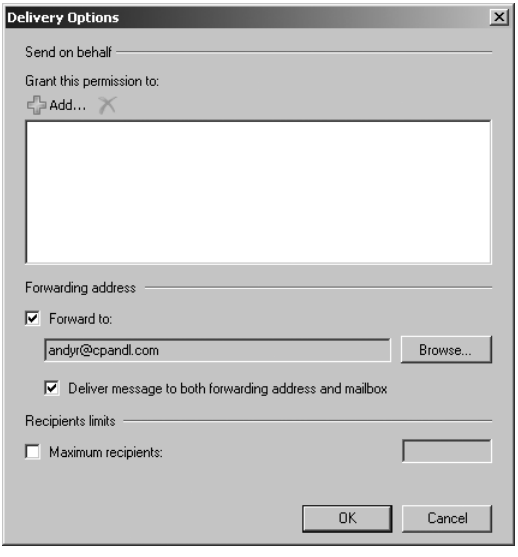


FIGURE 6-8 Using the Delivery Options dialog box, you can specify alternate recipients for mailboxes and deliver mail to the current mailbox as well.

Setting Storage Restrictions on an Individual Mailbox

You can set storage restrictions on multiple mailboxes using global settings for each mailbox database or on individual mailboxes using per-user restrictions. Global restrictions are applied when you create a mailbox and are reapplied when you define new global storage restrictions. Per-user storage restrictions are set individually for each mailbox and override the global default settings.

NOTE **Storage restrictions apply only to mailboxes stored on the server. They don't apply to personal folders. Personal folders are stored on the user's computer.**

You'll learn how to set global storage restrictions in Chapter 10, "Mailbox and Public Folder Database Administration." See the "Setting Mailbox Database Limits and Deletion Retention" section in that chapter.

You set individual storage restrictions by completing the following steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the Mailbox Settings tab, double-click Storage Quotas. This displays the Storage Quotas dialog box, shown in Figure 6-9.

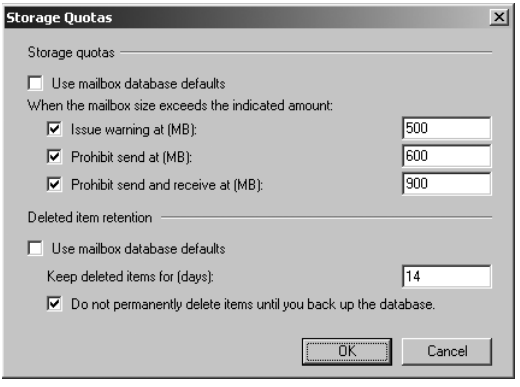


FIGURE 6-9 Using the Storage Quotas dialog box, you can specify storage limits and deleted item retention on a per-user basis when necessary.

3. To set mailbox storage limits, in the Storage Quotas panel, clear the Use Mailbox Database Defaults check box. Then set one or more of the following storage limits:
   - **Issue Warning At (MB)** This limit specifies the size, in megabytes, that a mailbox can reach before a warning is issued to the user. The warning tells the user to clean out the mailbox.
   - **Prohibit Send At (MB)** This limit specifies the size, in megabytes, that a mailbox can reach before the user is prohibited from sending any new mail. The restriction ends when the user clears out the mailbox and the mailbox size is under the limit.
   - **Prohibit Send And Receive At (MB)** This limit specifies the size, in megabytes, that a mailbox can reach before the user is prohibited from sending and receiving mail. The restriction ends when the user clears out the mailbox and the mailbox size is under the limit.

CAUTION **Prohibiting send and receive might cause the user to think they've lost e-mail. When someone sends a message to a user who is prohibited from receiving messages, an NDR is generated and delivered to the sender. The original recipient never sees the e-mail. Because of this, you should rarely prohibit send and receive.**

4. Click OK twice.

Setting Deleted Item Retention Time on Individual Mailboxes

Normally, when a user deletes a message in Microsoft Office Outlook, the message is placed in the Deleted Items folder. The message remains in the Deleted Items folder until the user deletes it manually or allows Outlook to clear out the Deleted Items folder. With personal folders, the message is then permanently deleted and you can't restore it. With server-based mailboxes, the message isn't actually deleted from the Exchange database. Instead, the message is marked as hidden and kept for a specified period of time called the *deleted item retention period*.

NOTE **The standard processes can be modified in several different ways. A user could press Shift+Delete to bypass Deleted Items. As an administrator, you can create and apply policies that prevent users from deleting items (even if they try to use Shift+Delete). You can also configure policy to retain items indefinitely.**

Default retention settings are configured for each mailbox database in the organization. You can change these settings, as described in Chapter 10 in the "Setting Mailbox Database Limits and Deletion Retention" section, or override the settings on a per-user basis by completing these steps:

1. Open the Properties dialog box for the mailbox-enabled user account by double-clicking the user name in the Exchange Management Console.
2. On the Mailbox Settings tab, double-click Storage Quotas. This displays the Storage Quotas dialog box, shown previously in Figure 6-9.
3. In the Deleted Item Retention panel, clear the Use Mailbox Database Defaults check box.
4. In the Keep Deleted Items For (Days) text box, enter the number of days to retain deleted items. An average retention period is 14 days. If you set the retention period to 0 and aren't using policies that prevent deletion, messages aren't retained and can't be recovered. If you set the retention period to 0 but are using policies that prevent deletion, the messages are retained according to the established policies.
5. You can also specify that deleted messages should not be permanently removed until the mailbox database has been backed up. This option ensures that the deleted items are archived into at least one backup set. Click OK twice.

REAL WORLD **Deleted item retention is convenient because it allows the administrator the chance to salvage accidentally deleted e-mail without restoring a user's mailbox from backup. I strongly recommend that you enable this setting, either in the mailbox database or for individual mailboxes, and configure the retention period accordingly.**