Microsoft

Microsoft®

Exchange Server 2010

Microsoft prePress

William R. Stanek

Author and Series Editor

Administrator's Pocket Consultant

Microsoft prePress is early content, straight from the source. What makes it “prePress”? These book chapters come fresh from the minds and laptops of our respected authors, and before we’ve edited and debugged the content. It’s a great way to get cutting-edge information right now, just when you need it!

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice**.** The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

Microsoft, Microsoft Press, Access, Active Directory, ActiveSync, ActiveX, Forefront, Outlook, Windows, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Table of Contents

CHAPTER 1

Microsoft Exchange Server 2010 Administration Overview

If you thought Exchange Server 2007 was a radical departure from its predecessors, wait till you get acquainted with 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 since it was implemented in Exchange Server 2007.

To support these and other changes, all storage group functionality has been moved to the database level. Further, mailbox databases are now peers to servers in the Exchange store schema—a change which removes the dependency of mailbox databases to server objects and reduces the Exchange store's reliance on secondary indices maintained by the Extensible Storage Engine (ESE).

Exchange Server 2010 integrates high availability into the core architecture by combining Cluster Continuous Replication (CCR) and Standby Continuous Replication (SCR) into a single high availability solution for both on-site and off-site data replication. Exchange Server 2010 also adds automatic failover and recovery of any Exchange Server role when you deploy multiple Exchange servers. Because of these changes, building a high availability solution no longer requires cluster hardware or advanced cluster configuration. Instead, you simply install multiple servers running Exchange Server 2010 with whatever roles you'd like to use in the same Exchange organization and high availability is enabled automatically. While role failover is automatic, you manage failover for mailbox databases using Database Availability

Groups. 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 up to 50 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 assigned 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 members of a Database Availability Group and replayed into the copy of the mailbox database that is stored on a particular server. Failover can occur at either the database level or the server level.

While I was discuss the architectural and administration impact of these extensive changes throughout this and other chapters of this book, you need to know this information right up front because it radically changes the way you will 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 backup-less and RAID-less Exchange implementations are radical ideas, it is possible, especially if you implement data retention rules as may be necessary for regulatory compliance and remember to rotate Exchange data to offsite storage periodically to ensure you are protected in extreme disaster recovery scenarios.

As you get started with Exchange Server 2010, you should concentrate on these 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-mails, voice mails, faxes, contacts, and calendar information.

Successful Exchange Server administration depends on three things:

- Good 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-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, 16 GB for all other server roles except Unified Messaging. For Unified Messaging, the maximum is 8 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 have to do with memory limitations and data access. Because 64-bit processors can exceed the 4-GB memory limit of 32-bit processors, 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 "Exchange Server Messaging Roles" in Chapter 2, "Deploying Microsoft 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 four-core processors to a single 8-core processor given current price/performance tradeoffs. An alternative would be 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. In most cases, small computer system interface (SCSI) drives are faster than integrated device electronics/enhanced integrated drive electronics (IDE/EIDE) and are, therefore, recommended. Rather than use one large drive, you should use several drives, which allow you to configure fault tolerance with redundant array of independent disks (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 may not want to use RAID for Exchange data and logs. You also may not want to use expensive disk storage systems either. Instead, you may 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, and you can rebuild the RAID unit to restore full operations. RAID 5 (disk striping with parity) offers good protection against single drive failure, but has poor write performance. For best performance and fault tolerance, 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.

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.

Microsoft Exchange Server 2010 Editions

Several editions of Exchange Server 2010 are available, including Exchange Server 2010 Standard Edition and Exchange Server 2010 Enterprise Edition. 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 Edition Designed to provide essential messaging services for small to medium-sized organizations and branch office locations. This server edition supports limited number of databases. Each database is limited to a maximum size of 16 terabytes (TB)—limited only by hardware.
- Exchange Server 2010 Enterprise Edition Designed to provide essential messaging services for organizations with increased availability, reliability, and manageability needs. This server edition supports up to 50 databases in

total on a particular server. Each database is limited to a maximum size of 16 terabytes (TB)—limited only by hardware.

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 files is used for both the Standard and the Enterprise editions. The license key provided during installation is what determines which edition is established during installation.

You can use a valid product key to go from a trial edition to a Standard Edition or Enterprise Edition of Exchange Server 2010 without having to reinstall. Using a valid product key, you can also upgrade from Standard Edition to 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.

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, Outlook Web Access, and Exchange Active Sync. 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-premise 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.

Exchange Server 2010 runs on Windows Server 2008 with Service Pack 2 or later and Windows Server 2008 Release 2. To install Exchange Server 2010, the system partition and all disk partitions used by Exchange must be formatted using the NT file system (NTFS). Additional preinstallation requirements are as follows:

- The domain controller with the Schema Master role must be running at least Windows Server 2003 Service Pack 1 (SP1).
- All domains in the Active Directory forest where Exchange Server 2010 will be installed or in which recipients will be hosted must have the domain functional level set to Windows 2000 Server native or higher.
- 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, and the minimum forest functional level for these forests must be Windows Server 2003.
- The domain must be configured to use multiple label DNS names, such as cpandl.com or adatum.local, rather than single-label DNS names, such as cpandl or adatum.

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 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, Windows Server 2008 Release 2 and later include WinRM 2.0 or later. On computers running earlier versions of Windows, you'll need to install 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'll need to install Microsoft .NET Framework version 3.5.1, WinRM 2.0, and Windows PowerShell 2.0. As WinRM 2.0 and PowerShell 2.0 are used for remote management whether you use the GUI or the command-line, you'll 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. 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 WinRM service is running 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
   ```

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

   ```
   Enable-PSRemoting –force
   ```

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, enter:

```
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 either 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'll see errors and will 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.

To use 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 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 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 will first check the system configuration to determine the status of required services and components, which include checking the Active Directory configuration and the availability of components, such as IIS (Internet Information Server), 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:

- 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.

- 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 Active Directory forest and are not configured on domain controllers.
- 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 "Adding, Modifying, or Uninstalling Server Roles" 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.
- 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 domain name system (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 fairly extensive, they are not comprehensive in scope. For comprehensive antivirus protection, you'll need to install Forefront Security for Exchange Server. Forefront Security for Exchange Server helps protect Exchange servers from viruses, worms, and other malware using multiple antivirus scan engines and file filtering capabilities. Forefront Security provides distributed protection for Exchange servers with the Mailbox server, Hub Transport server, and Edge Transport server roles. Although you can install Forefront Security on Exchange servers with these roles to gain substantial antivirus protection, you do not need to install Forefront Security on Exchange servers with only the Client Access Server or Unified Messaging Server role.

You can use the Forefront Security 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 Security for Exchange Server on a server operating system, Exchange Server and Forefront Security 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 Security 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 with which server components they are associated.

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 the SMTP and FTP services.	Client Access
Microsoft Exchange Active Directory Topology	Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange servers 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.	Edge Transport
Microsoft Exchange Anti-Spam Update	Maintains the antispam data for Forefront Security on an Exchange server.	

Microsoft Exchange EdgeSync	Provides EdgeSync services between Hub and Edge servers.	Hub Transport, Edge Transport
Microsoft Exchange File Distribution	Distributes Exchange data to other Exchange servers.	
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 Monitoring	Provides support for monitoring and diagnostics.	
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.	
Microsoft Exchange Replication	Provides replication functions for continuous replication.	Mailbox

Microsoft Exchange Replication Service	Provides replication functionality used for continuous replication.	Mailbox
Microsoft Exchange RPC Client Access	Manages client RPC connections for Exchange Server.	Client Access
Microsoft Exchange Search Indexer	Controls indexing of mailboxes to improve search performance.	Mailbox
Microsoft Exchange Service Host	Provides a host for essential Exchange services.	
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, Client Access
Microsoft Exchange Throttling	Provides throttling functions to limit the rate of user operations.	Client Access
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, Edge Transport

Microsoft Exchange Unified Messaging	Enables voice and fax messages to be stored in Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an automated attendant.	Unified Messaging
Microsoft Forefront Server Security ADO/EWS Navigator	Navigates the objects in Active Directory for Forefront Security by connecting with Exchange Web Services (EWS) or Exchange ActiveX Directory Objects (ADO) to retrieve objects.	Forefront Security
Microsoft Forefront Server Security Controller	Controls interaction between Forefront Security and the Microsoft Exchange Information Store. Ensures that Forefront initializes properly with the information store. Controller starts and stops scan jobs and applies engine updates.	Forefront Security
Microsoft Forefront Server Security Eventing Service	Processes incidents and manages quarantine logging, performance logging and notifications.	Forefront Security
Microsoft Forefront Server Security for Exchange Registration Service	Ensures the Forefront Transport Agent is registered with Exchange Server.	Forefront Security
Microsoft Forefront Server Security Mail Pickup	Provides mail pickup services for Forefront.	Forefront Security
Microsoft Forefront Server Security Monitor	Monitors the information store, SMTP/IMS, and Forefront processes to ensure that Forefront provides continuous protection.	Forefront Security

Microsoft Search (Exchange)	Provides search services for mailboxes, address lists and so on.	Mailbox
Secure Socket Tunneling Protocol Service	Provides support for Secure Socket Tunneling Protocol (SSTP) for securely connecting to remove 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 PowerShell.	
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 in the Exchange Management Console only.

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 2000 Server and 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 2000 Server and Exchange Server 2003 use 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 5, "Microsoft 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, database 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:

- Exchange All Hosted Organizations   Members of this group include hosted organization mailboxes groups. This group is used to apply Password Setting objects to all hosted mailboxes.
- Exchange Organization Administrators   Members of this group have full access to all Exchange properties and objects in the Exchange organization.
- Exchange Public Folder Administrators   Members of this group can manage public folders and perform most public folder management operations.
- Exchange Recipient Administrators   Members of this group have permissions to modify Exchange user attributes in Active Directory and perform most mailbox operations.
- Exchange Self-Service Users   Members of this group include all mailboxes in the Exchange organization. This group is used to apply RBAC self-service permissions to 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.
- Exchange View-Only Administrators   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.
- 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 2000 Server or Exchange Server 2003. Exchange 2000 Server and 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.

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 those 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 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 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 only necessary in these specific scenarios:

- If you deploy Exchange Server 2010 in an existing Exchange 2000 Server or 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.

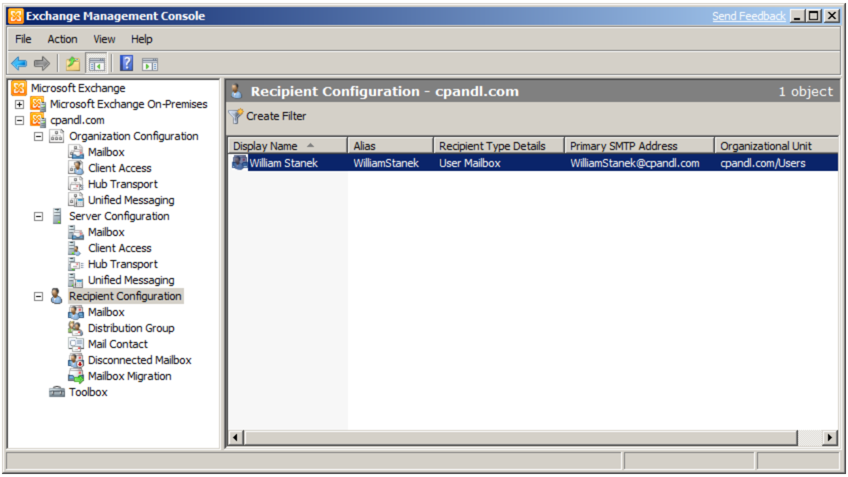
The organization's Mail Transport servers handle mail delivery outside the organization and receipt of mail from outside servers. You can use two types of Mail Transport servers: Hub Transport servers and Edge Transport servers. You deploy Hub Transport servers within the organization. You can optionally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

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 Security for Exchange 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 Security 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. As discussed further in Chapter 15, "Microsoft Exchange Server 2010 Maintenance, Monitoring, and Queuing," and Chapter 16, "Backing Up and Restoring Microsoft Exchange Server 2010," the Toolbox node in the Exchange Management Console provides access to a suite of related tools, including:



Display Name	Alias	Recipient Type Details	Primary SMTP Address	Organizational Unit
William Stanek	WilliamStanek	User Mailbox	WilliamStanek@cpandl.com	cpandl.com/Users

Figure 1-1 The Exchange Management Console.

- 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.

- Database Recovery Management Assists administrators in restoring server availability. Also provides step-by-step recovery procedures,
- Database Troubleshooter Helps troubleshoot problems related to mounting data stores as well as other problems related to Exchange databases and transaction logs that prevent recovery.
- 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.
- 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.
- 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.
- Routing Log Viewer Helps administrators troubleshoot routing problems on transport servers by providing information about routing topology.

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	Start and stop services, manage disks, and access other system management tools.

Configure Your Server	Add, remove, and configure Windows services for the network. Windows Server 2003 only.
DNS	Manage the DNS service.
Event Viewer	Manage events and logs.
IIS Manager	Manage Web servers used by Exchange as well as the management service configuration.
Microsoft Network Monitor	Monitor network traffic and troubleshoot networking problems.
Server Manager	Add, remove, and configure roles, role services, and features. Windows Server 2008 only.

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

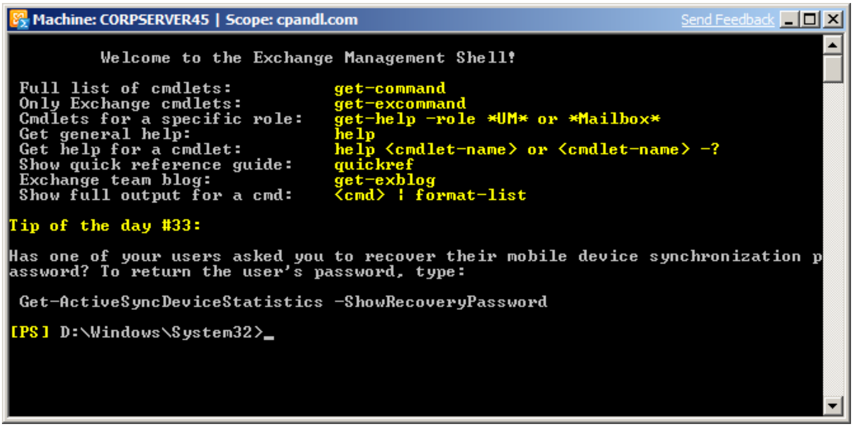
Using the Command-Line Administration Tools

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. 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 Programs or All Programs, choosing Microsoft Exchange Server 2010, and then choosing Exchange Management Shell or Exchange Management Shell (Local PowerShell). You'll use the local PowerShell option when you are logged on to the Exchange server. You'll use the standard option when you are logged on to your management computer and want to remotely manage Exchange servers.



```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #33:

Has one of your users asked you to recover their mobile device synchronization p
assword? To return the user's password, type:

 Get-ActiveSyncDeviceStatistics -ShowRecoveryPassword

[PS] D:\Windows\System32>_
```

Figure 1-2 The Exchange Management Shell.

The basics of working with the Exchange Management Shell are fairly 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 Exchange Management Shell," as well as examples of using cmdlets for Exchange Server management throughout the book.

Like Exchange Server, Forefront Security for Exchange has a management console and a management shell. You use the Forefront Server Security Administration console to manage Forefront Security using a graphical interface. You'll use the Forefront Management Shell to manage Forefront Security from the command line. This shell is accessible by selecting Start, choosing Programs or 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 Security for Exchange. The basics of working with the Forefront Management Shell are fairly 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-specific cmdlets available.
- Type **help *cmdletName*** to get help information, where *cmdletName* is the name of the command you are looking up.

As Forefront Management Shell does not load the Exchange Server cmdlets, you cannot access the Exchange-specific cmdlets from this shell by default. As the Exchange Management Shell does not load the Forefront-specific cmdlets either, you cannot access the Forefront-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 sending and receiving mail, 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 old messages, such as may be required for executives and needed by some managers.

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'll 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 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 "5th 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:

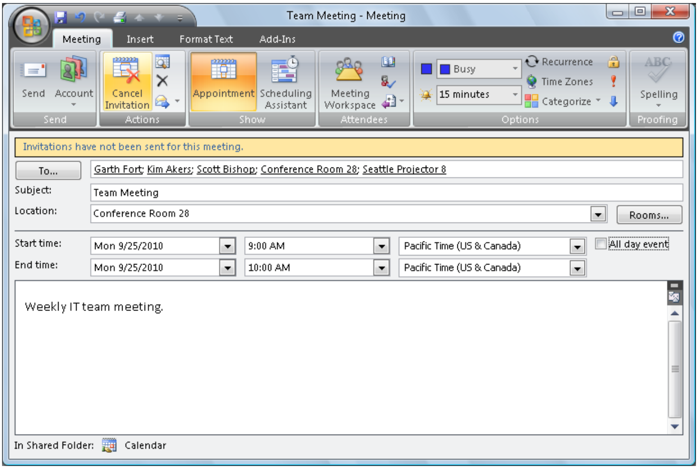
- If a room has a conference or call-in phone, enter this phone number as the business phone number on the Address And Phone tab of the Mailbox Properties dialog box.
- Specify the location details in the Office text box on the Organization tab of the Mailbox Properties dialog box.
- Specify the room 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 fairly 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. In Outlook 2007, click New, and then select Meeting Request. 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).



Invitations have not been sent for this meeting.

To... Garth Fort; Kim Akers; Scott Bishop; Conference Room 28; Seattle Projector 8

Subject: Team Meeting

Location: Conference Room 28

Busy

15 minutes

Start time: Mon 9/25/2010 9:00 AM Pacific Time (US & Canada) □ All day event

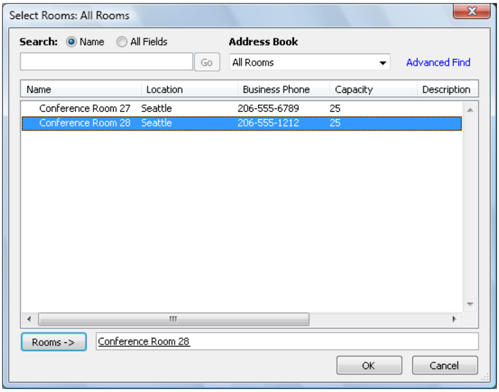
End time: Mon 9/25/2010 10:00 AM Pacific Time (US & Canada)

Weekly IT team meeting.

In Shared Folder: Calendar

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



Search: ● Name ○ All Fields

Address Book: All Rooms

Name	Location	Business Phone	Capacity	Description
Conference Room 27	Seattle	206-555-6789	25	
Conference Room 28	Seattle	206-555-1212	25	

Rooms -> Conference Room 28

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

Creating Room and Equipment Mailboxes

In the Exchange Management Console, you can create room and equipment mailboxes by completing the following steps:

1. In Exchange Management Console, expand the Recipient Configuration node and then select the related 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'll 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 equipment must have a separate user account. This is necessary to track the unique free/busy data for the room or equipment.
5. On the Mailbox 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. As you'll usually need to create room and equipment accounts in a specific organizational unit rather than the Users container, 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, the Exchange alias is set to the logon name by default. You can change this value by entering a new alias. The Exchange alias is used to set the user's e-mail address.
11. 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, 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.
13. 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 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 Note that 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'll 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.

In the Exchange Management Console, you can create a linked mailbox by completing the following steps:

1. In Exchange Management Console, expand the Recipient Configuration node and then select the related 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 Mailbox 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. 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. The Exchange alias is set to the logon name by default. Make sure the alias matches the one used in the resource forest.
11. 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 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'
 -LinkedCredentials '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'
 -LinkedCredentials '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 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, so users can see only the Alert William Stanek mailbox.**

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

1. Using 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 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 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 may be required for executives and needed by some managers. In Outlook, Outlook Web Access and other clients, users can access archive mailboxes in much the same way as they access their regular mailbox.

In Exchange Management Shell, the commands you can use to create and work with archive mailboxes include:

- Get-AlternateMailbox   Gets the properties associated with an alternate mailbox.

```
Get-AlternateMailbox [-Identity Identity]
[-DomainController FullyQualifiedName]
```

- New-AlternateMailbox   Creates an alternate mailbox for an existing mailbox user. The mailbox can be for an archive of old messages or subscriptions.

```
New-AlternateMailbox -Name NewMailboxName -Mailbox CurrentMailboxId
-Type <"Archive" | "Subscription"> [-DomainController
FullyQualifiedName]
[-RetentionPolicyEnabled <$true | $false>] [-UserDisplayName
DisplayName]
```

- Remove-AlternateMailbox   Removes a specified alternate mailbox.

```
Remove-AlternateMailbox -Identity Identity
[-DomainController FullyQualifiedName]
```

- Set-AlternateMailbox   Modifies the properties of an alternate mailbox.

```
Set-AlternateMailbox -Identity Identity [-DomainController
FullyQualifiedName]
[-Name MailboxName] [-RetentionPolicyEnabled <$true | $false>]
[-UserDisplayName DisplayName]
```

You create archive mailboxes using New-AlternateMailbox. This command has three required parameters:

- –Name   Sets the name of the alternate mailbox.
- –Mailbox   Specifies the mailbox to associate the archive with.
- -Type   Sets the type of the alternate mailbox.

In the following example, you create an archive mailbox for Daniel Escapa whose mailbox alias is daniele:

```
new-alternatemailbox -name "Dan's Archive" –mailbox "daniele" –type
"archive"
```

As each user can have only one archive mailbox, you get an error if the user already has an archive mailbox. Once you create an archive mailbox for a user, you can get information about the archive mailbox using the Get-AlternateMailbox command. In the following example, you get information about Daniel's archive mailbox:

```
get-alternatemailbox –identity "daniele"
```

Managing Mailboxes: The Essentials

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

You can work with multiple recipients at a 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 at once, hold down the SHIFT key, select the first resource, 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
- Export Mailbox
- Import Mailbox
- Move Mailbox

- New Move Request
- Remove
- Send Mail
- Verify Move Readiness

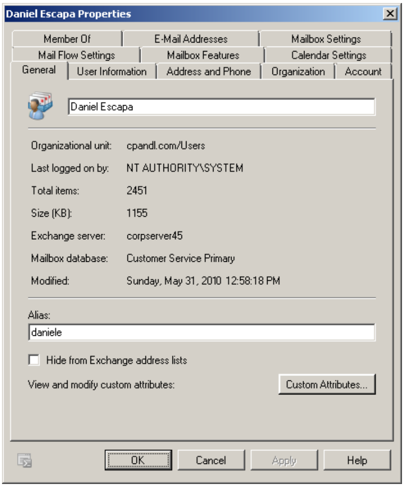
You also can edit the properties of multiple recipients at the same time. To do this, select the recipients you want to work with, right-click and then select Properties. Just about any property that can be set for an individual recipient can be set for multiple recipients.

> **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 may have intended to select only user mailboxes but may have 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, last logon date and time, mailbox size, and message count by completing these steps:

1. In Exchange Management Console, expand the Recipient Configuration node and then select the related 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 last logon date and time (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.



Daniel Escapa

Organizational unit: cpandl.com/Users
Last logged on by: NT AUTHORITY\SYSTEM
Total items: 2451
Size (KB): 1155
Exchange server: corpserver45
Mailbox database: Customer Service Primary
Modified: Sunday, May 31, 2010 12:58:18 PM

Alias: daniele

□ Hide from Exchange address lists

View and modify custom attributes:

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.

Sample 6-3 Getting statistics for multiple mailboxes

Syntax

```
Get-MailboxStatistics [-Server  'Server' | -Identity 'Identity'
 | -Database 'Database']
```

Usage

```
Get-MailboxStatistics -Server  'corpsvr127'

Get-MailboxStatistics -Database 'Engineering Primary'

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

When you are working with Exchange Management Shell, the standard output won't necessarily provide all the information you are looking for. Often, you'll need to format the output as a table or list 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
(FYDIBOHF23SPDLT)/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              :
Identity                 : d3f6ce44-fe0c-4beb-ae79-9c9f8eaf123c
IsValid                  : True
OriginatingServer        : corpserver45.cpandl.com
```

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 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 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 additional 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 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 both offline and online mailbox moves. Typically, you'll perform bulk mailbox moves offline while performing online moves of select mailboxes.

The sections that follow discuss how to perform both offline and online mailbox moves as well as how to perform related tasks.

Moving Mailboxes: The Essentials

Moving mailboxes while they are actively being used isn't a good idea, as it causes some disruption to the affected users. For this reason, Exchange Server 2010 gives you two options for moving mailboxes. You can:

- **Perform an offline, synchronous move** With an offline move, Exchange logs into both the source database and the destination database and moves the mailbox from one location to another. As users may not be able to access their email account during the move, you'll want to perform offline moves at a time when mailboxes are less likely to be in use. You can use the move scheduling features in Exchange Server 2010 to do this when you use the Exchange Management Console.
- **Perform an online, asynchronous move** With an online move, Exchange performs the move operation as a series of steps that allow the 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. As users can continue to access their email account during the move, you perform online moves at any time.

The destination database for an offline or online 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. With offline moves, keep the following in mind:

- When your source and destination Mailbox servers are running Exchange Server 2010 and are in the same forest, you can use the Exchange Management Console or the Move-Mailbox cmdlet to perform an offline mailbox move. This might be necessary when you are seeking to balance the load on a particular server.
- When your source servers are running Exchange 2000 Server, Exchange Server 2003, or Exchange Server 2007 and your destination servers are running Exchange Server 2010, you can use the Move-Mailbox cmdlet to perform an offline mailbox move. This might be necessary when you are upgrading to Exchange Server 2010.
- When your source and destination Mailbox servers are running Exchange Server 2010 and are in the different forests, you can use the Move-Mailbox cmdlet to perform an offline mailbox move. This might be necessary if you

are implementing an Exchange resource forest or establishing a new forest.

With online moves, keep the following in mind:

- When your source and destination Mailbox servers are running Exchange Server 2010 and are in the same forest, you can use the New-MoveRequest cmdlet to perform an online mailbox move. This might be necessary when you are seeking to move mailboxes while they are being used.
- When your source and destination Mailbox servers are running Exchange Server 2010 and are in 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 on-line Exchange organization.
- When your source servers are running Exchange 2000 Server, Exchange Server 2003, or Exchange Server2007 and your destination servers are running Exchange Server 2010, you cannot perform an online mailbox move. You will need to perform an offline mailbox move instead.

Performing online moves is a multi-step process that is initiated with a Move Mailbox request that is sent to the Mailbox Replication Service running on a Client Access server in the source forest. The Mailbox Replication Service 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 the contents of a mailbox are up to date. Once a mailbox has been moved, you can complete the move request and finalize the move.

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 may 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.

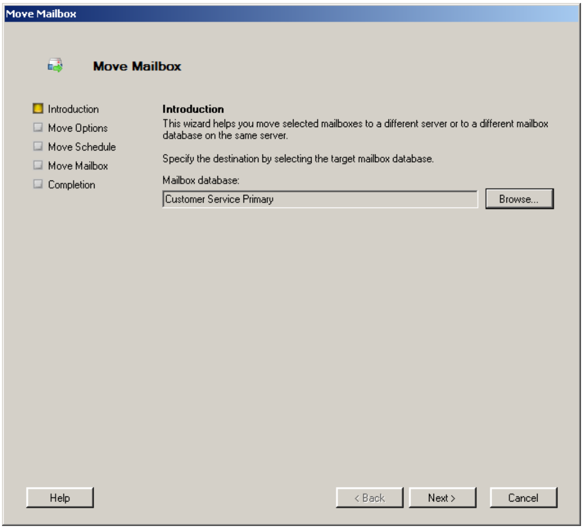
- Limits Changes to watch out for pertain to storage limits and deletion settings. Users might be prohibited from sending and receiving mail if their mailbox exceeds the storage limits of the new mailbox database. Users might notice that deleted items stay in their Deleted Items folder longer or are deleted sooner than expected if the Keep Deleted Items setting is different.

Performing Offline Mailbox Moves

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 Exchange Management Console, expand the Recipient Configuration node and then select the related Mailbox node.
2. Right-click the mailbox, and then select Move Mailbox. This starts the Move Mailbox Wizard, as shown in Figure 6-4.

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, hold down the Shift key, select the first user account, and then click the last user account.



Introduction

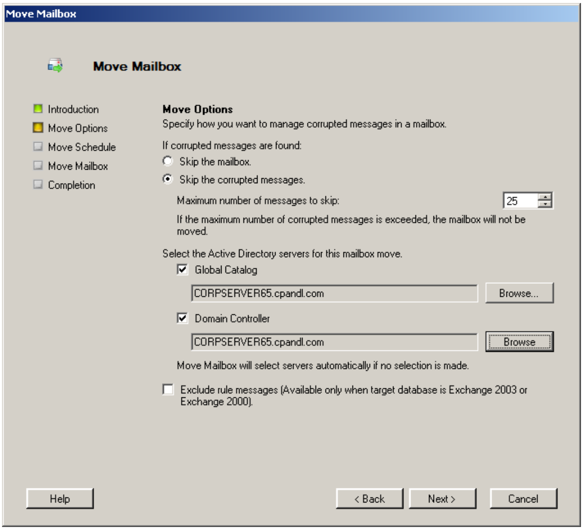
This wizard helps you move selected mailboxes to a different server or to a different mailbox database on the same server.

Specify the destination by selecting the target mailbox database.

Mailbox database: Customer Service Primary

Figure 6-4 Use the Move Mailbox Wizard to move mailboxes.

3. Click the Browse button to the right of the 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'd like those messages to be handled (see Figure 6-5). To skip the mailbox if corrupted messages are found, select Skip The Mailbox. To skip the corrupted messages if they 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. Optionally, select the Global Catalog and Domain Controller check boxes and then use the Browse buttons to set the related servers to use for this mailbox move.



Move Options

Specify how you want to manage corrupted messages in a mailbox.

If corrupted messages are found:

○ Skip the mailbox.

● Skip the corrupted messages.

Maximum number of messages to skip: 25

If the maximum number of corrupted messages is exceeded, the mailbox will not be moved.

Select the Active Directory servers for this mailbox move.

☑ Global Catalog

CORPSERVER65.cpandl.com

☑ Domain Controller

CORPSERVER65.cpandl.com

Move Mailbox will select servers automatically if no selection is made.

☐ Exclude rule messages (Available only when target database is Exchange 2003 or Exchange 2000).

Figure 6-5 Set the options for moving the mailbox.

7. Click Next. If you want to move the mailboxes right away, select Immediately. To schedule the mailbox move, select At The Following Time, and then set the move date and time.
8. To specify the maximum length of time that the mailbox move can run, select the Cancel Tasks That Are Still Running After (Hours) check box, and then set the maximum number of hours the move task can run.

Note Cancelling a move after a maximum number of hours is designed to ensure that move tasks that are blocked or not proceeding as expected are cancelled. Most move operations should be completed in eight hours or less, but the exact duration depends on the number of mailboxes being moved, the size of the mailboxes, and the connection speed of the link connecting the source and destination mail servers.

9. When you click Next and then click Move, Exchange Server attempts to move the mailbox. If a problem occurs, you'll see an Error dialog box that lets you retry or cancel the operation.

Note In the Exchange Management Console, you can't move mailboxes between forests. To move mailboxes among servers, the servers must be in the same forest.

In the Exchange Management Shell, you can move individual mailboxes using the Move-Mailbox cmdlet. Sample 6-4 provides the syntax and usage for using Move-Mailbox to move a specific mailbox from one server or database to another. Because the –Identity parameter accepts input from the pipeline, you can either explicitly specify the identity you are working with or pass in one or more identities from the pipeline as shown in the second example.

Sample 6-4 Moving individual mailboxes

Syntax

```
Move-Mailbox -Identity Identity [-IgnoreRuleLimitErrors {$true | $false}]
[-Arbitration {$true | $false}] [-OnlineMove {$true | $false}]
{AddtlParams}

Move-Mailbox -Identity Identity -ConfigurationOnly {$true | $false}
[-Arbitration {$true | $false}] {AddtlParams}

Move-Mailbox -Identity Identity {AddtlParams} {ExtendedParams}

{AddtlParams}
[-BadItemLimit Limit] [-DomainController FullyQualifiedName]
[-GlobalCatalog FullyQualifiedName] [-IgnorePolicyMatch {$true | $false}]
[-MaxThreads MaxThreads] [-ReportFile LocalPath] [-TargetDatabase
DatabaseId]
[-ValidateOnly {$true | $false}]

{ExtendedParams}
[-AllContentKeywords Keywords] [-AllowMerge {$true | $false}] [-
AttachmentFilenames
Files] [-BadItemLimit Limit] [-ContentKeywords Keywords] [-EndDate
DateTime]
[-ExcludeFolders MapiFolderPaths] [-IgnoreRuleLimitErrors {$true |
$false}]
[-IncludeFolders MapiFolderPaths] [-Locale Locale] [-NTAccountOU OUName]
[-OnlineMove {$true | $false}] [-PreserveMailboxSizeLimit {$true |
$false}]
[-RecipientKeywords Keywords] [-RetryInterval TimeSpan] [-RetryTimeout
TimeSpan]
[-SenderKeywords Keywords] [-SourceForestCredential Credential]
[-SourceForestGlobalCatalog FullyQualifiedName] [-
SourceMailboxCleanupOptions <None |
DeleteSourceMailbox | DeleteSourceNTAccount | MailEnableSourceAccount |
CreateSourceContact>] [-StartDate DateTime] [-SubjectKeywords Keywords]
[-TargetForestCredential Credential]
```

Usage

```
Move-Mailbox –Identity 'cpandl\daniele'
 -TargetDatabase 'Corporate Services'
-BadItemLimit 50 -IgnorePolicyMatch $true
 -RetryTimeout '8:00:00' -RetryInterval '5:00'

'cpandl.com/users/Charlie Keen' | Move-Mailbox -TargetDatabase
'Engineering Primary'
-BadItemLimit 50 -IgnorePolicyMatch $true
 -RetryTimeout '8:00:00' -RetryInterval '5:00'
```

If you want to move all mailboxes from one database to another, you can use the Get-Mailbox and Move-Mailbox cmdlets together, as shown in Sample 6-5.

Sample 6-5 Moving all mailboxes in a database

Syntax

```
Get-Mailbox -Database Database | Move-Mailbox -TargetDatabase DatabaseId
```

Usage

```
Get-Mailbox -Database 'Technology Primary' | Move-Mailbox
-TargetDatabase 'Engineering Primary'
 -BadItemLimit 50 -IgnorePolicyMatch $true
-RetryTimeout '8:00:00' -RetryInterval '5:00'
```

If you are moving mailboxes between domains, you'll want to specify a domain controller and Global Catalog to use in the target domain, as shown in Sample 6-6. This ensures that performance and replication issues don't cause problems when moving mailboxes across domains.

Sample 6-6 Moving mailboxes across domains

Syntax

```
Move-Mailbox -Identity Identity -TargetDatabase Database
 [-DomainController TargetDCName] [-GlobalCatalog TargetGCName]
 [-BadItemLimit Number] [-DomainController DCName]
 [-IgnorePolicyMatch {$true | $false}] [-RetryTimeout TimeSpan]
 [-RetryInterval TimeSpan]
```

Usage

```
Move-Mailbox –Identity 'cpandl\williams'  -TargetDatabase 'Engineering
Primary'
 -DomainController 'CorpServer65.cpandl.com' -GlobalCatalog '
CorpServer37.cpandl.com '
 -BadItemLimit 50 -IgnorePolicyMatch $true
```

If you are moving mailboxes across forests, you must specify Global Catalogs to use in both the source and target forests, as shown in Sample 6-7. You must also specify the NT account organizational unit. When you perform the move mailbox task, you'll be prompted for administrator credentials to connect to the target database in the target forest. You must provide the account name and password for an administrator account in the target forest.

Sample 6-7 Moving mailboxes across forests

Syntax

```
Move-Mailbox -Identity Identity -TargetDatabase Database
[-DomainController TargetDCName] [-GlobalCatalog TargetGCName]
[-BadItemLimit Number] [-IgnorePolicyMatch {$true | $false}]
[-SourceForestCredential Credential] [-SourceForestGlobalCatalog
FullyQualifiedName]
[-SourceMailboxCleanupOptions <None | DeleteSourceMailbox |
DeleteSourceNTAccount |
MailEnableSourceAccount | CreateSourceContact>] [-StartDate DateTime]
[-SubjectKeywords Keywords] [-TargetForestCredential Credential]
[-RetryTimeout TimeSpan] [-RetryInterval TimeSpan]
```

Usage

```
Move-Mailbox –Identity 'cpandl\kathyh' -TargetDatabase 'Engineering
Primary'
-DomainController 'Server14.adatum.com' -GlobalCatalog
'Server12.adatum.com'
-SourceForestGlobalCatalog 'CorpServer32.cpandl.com' -BadItemLimit 5
-IgnorePolicyMatch $true
```

Performing Online Mailbox Moves

With an online move, Exchange performs the move operation as a series of steps that allow the mailbox to remain available while the move operation is being completed. 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 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 replication service 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 replication service 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 replication service finishes its initial replication of the mailbox, the service assigns the Ready To Complete status to the mailbox and periodically performs incremental synchronization between the source and destination database to ensure the contents are up to date. By default, the replication service performs incremental synchronization approximately every 5 minutes.
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 replication services 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. As users can continue to access their email account during a move, you can perform online moves at any time.

The Mailbox Replication Service proxy runs as a Web application on a Client Access Server and is installed as part of the Client Access role. The proxy tracks two different types of moves:

- Initial moves An initial move occurs when the proxy begins replicating data and the mailbox has a status of Move In Progess.
- Incremental moves Incremental moves occur when the proxy synchronizes the mailbox data after an initial move and the mailbox has a status of Ready

To Complete.

The configuration settings for the service come from the Microsoft.Exchange.ServiceHost.exe.config file. You can modify the default settings by editing this file and changing the value of the following properties:

- MaxOngoingInitialMovesPerMDB   Sets the number of initial mailbox moves on a single database at one time. The default value is 5 concurrent moves.
- MaxOngoingInitialMovesPerMRSInstance   Sets the number of initial mailbox moves by a single instance of the Mailbox Replication Service. The default value is 50 concurrent moves.
- MaxOngoingTotalMovesPerMDB   Sets the total number of initial and incremental moves on a single database at one time. The default value is 5 concurrent moves.
- MaxOngoingTotalMovesPerMRSInstance   Sets total number of initial and incremental moves by a single instance of the Mailbox Replication Service. The default value is 50 concurrent moves.
- MinIncrementalSyncInterval   Sets the minimum interval between incremental synchronizations for a mailbox. Default is 5 minutes. Minimum is 1 minute. 0 indicates never to perform incremental synchronizations (and in which case the mailbox will be synchronized only as part of the move finalization process).

These settings are designed to ensure the Client Access server acting as the proxy can continue to perform other activities while moving databases. Before you change any of the configuration settings, you should carefully evaluate current server loads and perform capacity planning. The average size of mailboxes in your organization and network bandwidth availability should also be a part of your decision making process. If most mailboxes in your organization are over 500 Megabytes, you'll likely want to restrict the number of concurrent and total moves even further than the default settings. If most mailboxes in your organization are under 100 Megabytes, you'll likely want to increase the number of concurrent and total moves allowed. However, you would need to ensure network bandwidth is available and that you don't saturate the network.

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

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

```
Get-MoveRequest -Identity Identity [-MRSServer FullyQualifiedName]
[-DomainController FullyQualifiedName] [-IncludeReport {$true |
$false}]
```

- 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 -Local {$true | $false} [-
TargetDatabase DatabaseId] [-MRSServer FullyQualifiedName] [-
Protect {$true | $false}]
[-BadItemLimit Limit] [-DomainController FullyQualifiedName]

New-MoveRequest -Identity Identity -Remote {$true | $false} –
RemoteHostName
HostName [-MRSServer FullyQualifiedName] [-RemoteCredential
Credential]
[-TargetDatabase DatabaseId] [-BadItemLimit Limit] [-
DomainController
FullyQualifiedName] [-Protect {$true | $false}]
```

- Complete-MoveRequest Finish a request that was initiated by using the New-MoveRequest command. If the move request was initiated with the –Protect parameter, you must use the –Protect parameter to complete the move request.

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

- 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 before completing the move with the Complete-MoveRequest command. 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
FullyQualifiedName]
[-DomainController FullyQualifiedName] [-Protect {$true | $false}]
```

Moving Mailboxes Within Forests

You perform online mailbox moves within forests using 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 could verify whether Garrett Vargas's mailbox can be moved:

```
New-MoveRequest -Identity 'garrettv' –Local -TargetDatabase "Engineering
Primary"
```

```
-WhatIf

'cpandl.com/users/Garrett Vargas' | New-MoveRequest -Local
-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 could move Garrett Vargas's mailbox:

```
New-MoveRequest -Identity 'garrettv' –Remote –RemoteHost
'mailserver17.cpandl.com'
-mrsserver 'caserver21.cpandl.com' -TargetDatabase "Engineering Primary"

'cpandl.com/users/Garrett Vargas' | New-MoveRequest –Remote –RemoteHost
'mailserver17.cpandl.com' -mrsserver 'caserver21.cpandl.com' -
TargetDatabase
'Engineering Primary'
```

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

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

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

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

When the mailbox or maiboxes are in the Ready To Complete state, you can finalize the move using Complete-MoveRequest. An example follows:

```
Complete-MoveRequest –Identity 'garrettv'
```

You can cancle a move at any time prior to running Complete-MoveRequest. To do this, run Remove-MoveRequest and specify the identify of the mailbox that shouldn't be moved. An example follows:

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

Moving Mailboxes Between Forests

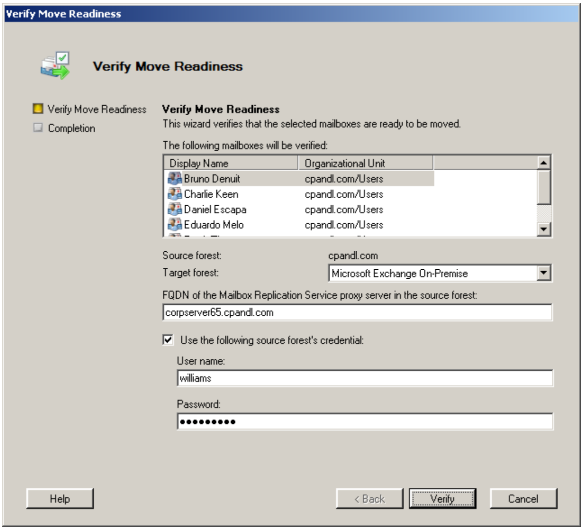
You can perform online mailbox moves between different Exchange forests using the Exchange Management Console or Exchange Management Shell. When you are moving mailboxes between forests, you'll want to verify that mailboxes are ready to be moved before you submit a move request. To verify readiness, the 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.

VERIFYING MOVE READINESS

You can verify move readiness in Exchange Management Console by following these steps:

1. In Exchange Management Console, select the mailbox or mailboxes that you are planning on moving. Right-click and then select Verify Move Readiness. This starts the Verify Move Readiness wizard.
2. On the Verify Move Readiness page, the mailboxes you selected are listed as the ones that will be verified, as shown in Figure 6-6. The source forest is the current forest you to which you are connected.



Verify Move Readiness

This wizard verifies that the selected mailboxes are ready to be moved.

The following mailboxes will be verified:

Display Name	Organizational Unit
Bruno Denuit	cpandl.com/Users
Charlie Keen	cpandl.com/Users
Daniel Escapa	cpandl.com/Users
Eduardo Melo	cpandl.com/Users

Source forest: cpandl.com

Target forest: Microsoft Exchange On-Premise

FQDN of the Mailbox Replication Service proxy server in the source forest: corpserver65.cpandl.com

☑ Use the following source forest's credential:

User name: williams

Password: ••••••••••

Figure 6-6 Verify the mailboxes are ready to be moved.

3. In the Target Forest list, select the forest to which you are moving mailboxes.
4. In the text box provided, enter the fully qualified domain name of a Client Access server in the source forest that will act as the proxy server.
5. If you want to provide alternate credentials for the source forest, select the Use The Following Source Forest's Credential, enter the user name, and then type the password for the account.

6. When you click Verify to begin the verification process, Exchange Management Console runs New-MoveRequest with the –WhatIf parameter for each mailbox you selected and displays the results on the Completion page. Note any errors and corrective actions that are required. For example, you may need to remove a user's archive mailbox before you can perform an online move. You can copy the results to the Windows clipboard for pasting into a document by pressing Ctrl+C. Click Finish.

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

```
New-MoveRequest -Identity 'charliek' –Remote –RemoteHost
'mailserver17.cpandl.com'
-mrsserver 'caserver21.cpandl.com' -TargetDatabase "Engineering Primary"
-WhatIf

'cpandl.com/users/Charlie Keen' | New-MoveRequest –Remote –RemoteHost
'mailserver17.cpandl.com' -mrsserver 'caserver21.cpandl.com' -
TargetDatabase
'Engineering Primary' -WhatIf
```

PERFORMING THE MOVE BETWEEN FORESTS

You can perform online mailbox moves between forests in Exchange Management Console by following these steps:

1. In Exchange Management Console, select the mailbox or mailboxes that you want to move. Right-click and then select New Move Request. This starts the New Move Request wizard.
2. On the New Move Request page, the mailboxes you selected are listed as the ones that will be moved. The source forest is the current forest you to which you are connected.
3. In the Target Forest list, select the forest to which you are moving mailboxes.
4. In the text box provided, enter the fully qualified domain name of a Client Access server in the source forest that will act as the proxy server.
5. If you want to provide alternate credentials for the source forest, select the Use The Following Source Forest's Credential, enter the user name, and then type the password for the account.
6. When you click New to initiate the move request, Exchange Management Console 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.

7. When the move is completed, you can either:
   - Complete the move request and finalize the move. The mailbox or mailboxes you moved are then available in the new location.
   - Cancel the move request and void the move. The mailbox or mailboxes you moved are then available in the original location.

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

```
New-MoveRequest -Identity 'brunod' –Remote –RemoteHost
'mailserver17.cpandl.com'
-mrsserver 'caserver21.cpandl.com' -TargetDatabase "Engineering Primary"

'cpandl.com/users/Bruno Denuit' | New-MoveRequest –Remote –RemoteHost
'mailserver17.cpandl.com' -mrsserver 'caserver21.cpandl.com' -
TargetDatabase
'Engineering Primary'
```

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

```
Get-MoveRequest –Identity 'brunod' -mrsserver 'caserver21.cpandl.com'
```

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

```
Get-MoveRequest –Identity 'brunod' -mrsserver 'caserver21.cpandl.com' –
IncludeReport
```

When the mailbox or maiboxes are in the Ready To Complete state, you can finalize the move using Complete-MoveRequest. An example follows:

```
Complete-MoveRequest –Identity 'brunod' -mrsserver
'caserver21.cpandl.com'
```

At any time prior to running Complete-MoveRequest, 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 'caserver21.cpandl.com'
```

Importing and Exporting Mailbox Data

As discussed in detail in Chapter 17, “Managing Microsoft Exchange Server 2010

Clients," Exchange mail can be configured to use the following: server mailboxes, server mailboxes with local copies, or personal folders. Users who travel often may prefer to have personal folders where their mail is stored locally in .pst files. However, from an administration perspective, you'll find that mailboxes are easier to manage and protect when users have either server mailboxes or server mailboxes with local copies.

When you are working with the Exchange Management Shell, you can use the Import-Mailbox cmdlet to import mailbox data from a .pst file and the Export-Mailbox cmdlet to export mailbox data to a .pst file. Import and export operations are similar to mailbox move operations.

Sample 6-8 shows the syntax and usage for Import-Mailbox. The only required parameters are Identity and PstFolderPath. Most other parameters serve to limit what you are importing. For import operations, you'll typically want to create a copy of the user's .pst file and make this copy accessible on a desktop running a 32-bit operating system where the 32-bit Exchange management tools are installed. Once you've installed the 32-bit Exchange management tools on a desktop computer running a 32-bit operating system, you can access the Exchange Management Shell on the user's desktop and run this cmdlet. With Windows Vista, the default location of a .pst file is *%LocalAppData%*\Microsoft\Outlook, where *%LocalAppData%* is a user-specific environment variable that points to a user's local application data.

Sample 6-8 Import-Mailbox cmdlet syntax and usage

Syntax

```
Import-Mailbox -Identity DestMailboxIdentifier
 -PSTFolderPath PSTLocalPath
[-AllowContentKeywords AllowedValues]
[-AllowDuplicates {$true | $false}]
[-AttachmentFilenames AllowedValues]
[-BadItemLimit Limit] [-ContentKeywords BodyOrAttachmentValues]
[-EndDate DateTime] [-ExcludeFolders MapiFoldePath]
[-GlobalCatalog GCName] [-IncludeFolders MapiFolderPath]
[-Locale Value] [-MaxThreads Num]
[-RecipientKeywords Values] [-ReportFile LocalPath]
[-SenderKeywords Values] [-StartDate DateTime]
[-SubjectKeywords Values] [-ValidateOnly <$false|$true>]
```

Usage

```
Import-Mailbox -Identity 'cpandl.com/Engineering/williams'
 -PSTFolderPath 'c:\temp\william.pst'
```

Sample 6-9 shows the syntax and usage for Export-Mailbox. The only required parameters are Identity and PstFolderPath. Most other parameters serve to limit what you are exporting. When you are exporting to a .pst file, you'll want to run the command on a desktop running a 32-bit operating system where the 32-bit Exchange management tools are installed. Once you've installed the 32-bit Exchange management tools on a desktop computer running a 32-bit operating system, you can access the Exchange Management Shell on the user's desktop and run this cmdlet to store the exported data in a .pst file.

Sample 6-9 Export-Mailbox cmdlet syntax and usage

Syntax

```
Export-Mailbox -Identity SourceMailboxIdentifier -PSTFolderPath
PSTLocalPath
{AddtlParams}

{AddtlParams}
[-AllowContentKeywords AllowedValues] [-AttachmentFilenames
AllowedValues]
[-BadItemLimit Limit] [-ContentKeywords BodyOrAttachmentValues]
[-DeleteAssociatedMessages <$false|$true>] [-DeleteContent
<$false|$true>]
[-EndDate DateTime] [-ExcludeFolders MapiFoldePath] [-GlobalCatalog
GCName]
[-IncludeAssociatedMessages {$true | $false}] [-IncludeFolders
MapiFolderPath]
[-Locale Value] [-MaxThreads Num] [-RecipientKeywords Values] [-
ReportFile LocalPath]
[-SenderKeywords Values] [-StartDate DateTime] [-SubjectKeywords Values]
[-ValidateOnly <$false|$true>]
```

Usage

```
Export-Mailbox -Identity 'cpandl.com/Engineering/williams'
 -PSTFolderPath 'c:\temp\william.pst'
```

Export-Mailbox has alternative syntax that allows you to export a mailbox or a subset of mail or folders and import it directly into a Recovered – Data subfolder of a specified folder in a specified mailbox. For example, you could use this technique to export the mail in Andy Carothers's mailbox into a SavedMail folder in Scotty Seely's mailbox. For this type of export operation, you do not have to run the cmdlet on a desktop running a 32-bit operating system where the 32-bit Exchange management tools are installed. Sample 6-10 provides the syntax and usage for an export/import.

Sample 6-10 Exporting and then importing Mailbox data

Syntax

```
Export-Mailbox -Identity SourceMailboxIdentifier -TargetFolder LocalPath
```

```
-TargetMailbox TargetMailboxId [-AllowMerge {$true | $false}]
{AddtlParams}

{AddtlParams}
[-AllowContentKeywords AllowedValues] [-AttachmentFilenames
AllowedValues]
[-BadItemLimit Limit] [-ContentKeywords BodyOrAttachmentValues]
[-DeleteAssociatedMessages <$false|$true>] [-DeleteContent
<$false|$true>]
[-EndDate DateTime] [-ExcludeFolders MapiFoldePath] [-GlobalCatalog
GCName]
[-IncludeFolders MapiFolderPath] [-Locale Value] [-MaxThreads Num]
[-RecipientKeywords Values] [-ReportFile LocalPath] [-SenderKeywords
Values]
[-StartDate DateTime] [-SubjectKeywords Values] [-ValidateOnly
<$false|$true>]
```

Usage

```
Export-Mailbox -Identity 'cpandl.com/Engineering/andyc'
-TargetFolder 'SavedMail' -TargetMailbox
' cpandl.com/Engineering/andyc'
```

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

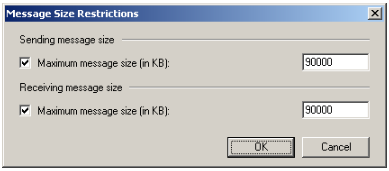
You set message size restrictions for contacts in much the same way that you set size restrictions for users. Follow the steps listed in the section of this chapter entitled “Setting Message Size Restrictions on Delivery to and from Individual Mailboxes.”

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 should a message have an attachment that exceeds this limit. Sometimes, you'll need to set exceptions for specific users. For example, some users may 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 Exchange Management Console.
2. On the Mail Flow Settings tab, double-click Message Size Restrictions. As shown in Figure 6-7, you can now set the following send and receive restrictions:



Message Size Restrictions

Sending message size

☑ Maximum message size (in KB): 90000

Receiving message size

☑ Maximum message size (in KB): 90000

Figure 6-7 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. If an outgoing message exceeds the limit, the message isn't sent and the user receives a nondelivery report (NDR).
- Receiving Message Size Sets a limit on the size of messages the user can receive. The value is set in Kilobytes. 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 section of this chapter entitled "Setting Message Send and Receive Restrictions on Individual Mailboxes."

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:

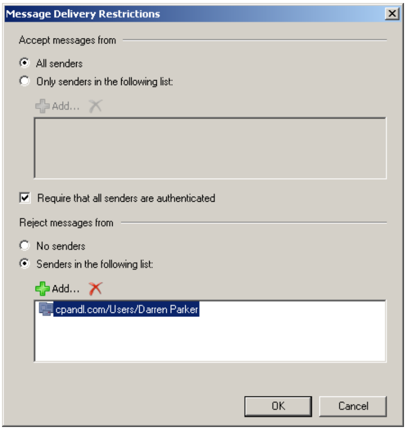
- Specify that only messages from the listed users, contacts, or groups be accepted.
- Specify that messages from specific users, contacts, or groups listed be rejected.
- Specify that only authenticated users—meaning users who have logged on to the Exchange system or the domain—be accepted.

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 Exchange Management Console.

2. On the Mail Flow Settings tab, double-click Message Delivery Restrictions. As shown in Figure 6-8, you can now set message acceptance restrictions.
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.



Message Delivery Restrictions

Accept messages from

● All senders

○ Only senders in the following list:

☑ Require that all senders are authenticated

Reject messages from

○ No senders

● Senders in the following list:

cpandl.com/Users/Darren Parker

Figure 6-8 You can apply send and receive restrictions on messages on a per-user basis.

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:
   - 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, hold down the Shift key, select the first recipient, 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.
   - 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 will 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 way:

- 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 Recipient 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 6-11 and 6-12 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 6-11 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 6-12 Removing full access permissions

Syntax

```
Remove-MailboxPermission -Identity 'UserBeingGrantedPermission'
 -User 'UserWhoseMailboxIsBeingConfigure' -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 Recipient 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. Sample 6-13 and 6-14 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 6-13 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 6-14 Removing Send As permissions

Syntax

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

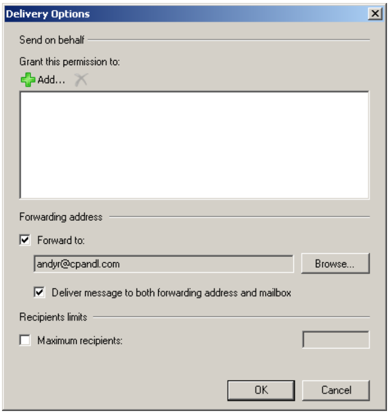
Note Another way to grant access permissions to mailboxes is to do so through Outlook. Using Outlook, you have more granular control over permissions. You can allow a user to log on as the mailbox owner, delegate mailbox access, and grant various levels of access. For more information on this issue, see the sections of Chapter 17, "Managing Microsoft Exchange Server 2010 Clients," entitled "Accessing Multiple Exchange Server Mailboxes" and "Granting Permission to Access Folders Without Delegating Access."

Forwarding E-mail to a New Address

Any messages sent to a user's mailbox can be forwarded to another recipient. This recipient could 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 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 6-9). Click OK.



Grant this permission to:

☑ Forward to: andyr@cpandl.com

☑ Deliver message to both forwarding address and mailbox

□ Maximum recipients:

Figure 6-9 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

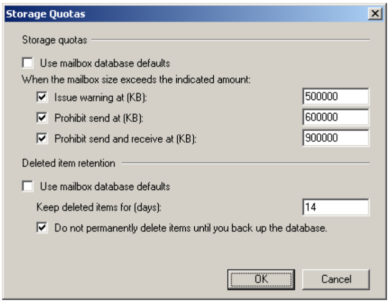
You can set storage restrictions on multiple mailboxes using global settings for each mailbox database or on individual mailboxes using per-user restrictions. Global restrictions are applied when you create a mailbox and are reapplied when you define new global storage restrictions. Per-user storage 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 12, "Mailbox and Public Folder Database Administration." See the section of that chapter entitled "Setting Mailbox Database Limits and Deletion Retention."

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 Exchange Management Console.
2. On the Mailbox Settings tab, double-click Storage Quotas. This displays the Storage Quotas dialog box, shown in Figure 6-10.



Storage Quotas

Storage quotas

☐ Use mailbox database defaults

When the mailbox size exceeds the indicated amount:

☑ Issue warning at (KB): 500000

☑ Prohibit send at (KB): 600000

☑ Prohibit send and receive at (KB): 900000

Deleted item retention

☐ Use mailbox database defaults

Keep deleted items for (days): 14

☑ Do not permanently delete items until you back up the database.

Figure 6-10 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 (KB) This limit specifies the size, in kilobytes, 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 (KB) This limit specifies the size, in kilobytes, 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 (KB) This limit specifies the size, in kilobytes, 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 lose 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

When a user deletes a message in Microsoft Office Outlook 2007, 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 information store. Instead, the message is marked as hidden and kept for a specified period of time called the *deleted item retention period*.

Default retention settings are configured for each mailbox database in the organization. You can change these settings, as described in the section of Chapter 12 entitled “Setting Mailbox Database Limits and Deletion Retention,” 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 Exchange Management Console.
2. On the Mailbox Settings tab, double-click Storage Quotas. This displays the Storage Quotas dialog box, shown previously in Figure 6-10.
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, messages aren’t retained and can’t be recovered.
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.