
Microsoft[®]
Exchange Server 2007

**An Overview of
Microsoft Exchange Server 2007**
White Paper

Published: October 2006

For the latest information, please see <http://www.microsoft.com/exchange>

Contents

Introduction	1
Architectural Overview	2
Server Roles	2
Administrative Groups and Routing Groups	4
Storage Groups and Information Stores	4
The 64-Bit Advantage	4
New Features and Capabilities	6
Comprehensive Protection from Outside Threats	6
Simplified Message Security	9
Compliance	9
Maximizing Availability	12
Simplifying Exchange Management	14
Productivity Boost	18
Deploying Exchange Server 2007	21
Installing Exchange Server 2007	21
Upgrading to Exchange Server 2007	22
Conclusion	24
Appendix A – Microsoft Exchange Hosted Services	25

Introduction

April 2006 marked the 10th year that Microsoft® Exchange has been providing messaging services to organizations large and small. The release of Exchange 4.0 in April 1996 was Microsoft's first major step out of the workgroup and into the datacenter. It was Microsoft's flagship client/server application highlighting how Microsoft can provide back-office products that complement Microsoft desktop products – allowing productivity increases only possible with tightly integrated desktop and server products.

Back then, Microsoft Exchange Server was an X.400–based messaging system with an X.500–like directory. Industry messaging was simple (e-mail), and features such as shared calendaring and public folders wowed us like those fancy dance moves in the 1996 pop hit “Macarena.”

But Exchange Server continued to evolve and set pace in the messaging industry. Exchange Server 5.5 reflected Microsoft's Internet initiatives with multiple Web-based clients – offering a simple-to-use and reliable messaging system that many organizations used until recently, roughly nine years since Exchange Server 5.5 first hit the streets.

As most IT departments and datacenters continued to grow and mature, the need emerged for a more comprehensive and common platform to support a wider range of applications. This resulted in a major architectural shift in Exchange 2000 Server. The Exchange directory became the basis for the Microsoft Active Directory® directory system. Other Exchange services such as SMTP, POP3, IMAP4, and NNTP became part of the operating system. Microsoft Windows® 2000 provided a common platform for enterprise applications, with Active Directory as its backbone. Exchange 2000 Server set the stage again as the application that first fully integrated with Active Directory, storing Exchange configuration, schema, and recipient information in the directory and allowing users and administrators to realize Active Directory's potential.

Today, e-mail is a tool we use and rely on as much as the telephone – more so in some cases. Microsoft Windows Server™ 2003 and Exchange Server 2003 delivered a rich mobile user experience (device or browser) to meet the demands of a remote and mobile workforce, but are probably best known for the release that delivered significant server consolidation opportunities.

This long and dynamic history of Exchange shows how the product has evolved and set the standard for enterprise messaging along the way. Today's business requirements – such as security, disaster recovery, and mobility – are more extensive than ever before. To meet these requirements, Exchange has extended its reach beyond simple e-mail to increase user productivity and keep information close at hand, while being flexible enough to meet your organization's administrative model. This white paper delivers an overview of Exchange Server 2007 and describes how this next generation of Exchange helps increase user productivity and administrator efficiency while fulfilling your evolving business requirements.

Exchange 4.0	April 1996
Exchange 4.0 (a)	August 1996
Exchange 4.0 SP1	May 1996
Exchange 4.0 SP2	August 1996
Exchange 4.0 SP3	November 1996
Exchange 4.0 SP4	April 1997
Exchange 4.0 SP5	May 1998
Exchange 5.0	March 1997
Exchange 5.0 SP1	June 1997
Exchange 5.0 SP2	February 1998
Exchange 5.5	November 1997
Exchange 5.5 SP1	July 1998
Exchange 5.5 SP2	December 1998
Exchange 5.5 SP3	September 1999
Exchange 5.5 SP4	November 2000
Exchange 2000	October 2000
Exchange 2000 (a)	January 2001
Exchange 2000 SP1	July 2001
Exchange 2000 SP2	December 2001
Exchange 2000 SP3	August 2002
Exchange 2000 post-SP3	September 2003
Exchange 2000 post-SP3	April 2004
Exchange 2000 post-SP3	August 2004
Exchange Server 2003	October 2003
Exchange Server 2003 SP1	May 2004
Exchange Server 2003 SP2	October 2005

Architectural Overview

As a messaging system that is widely used in both large corporations and small businesses, Exchange Server has always been scalable in both directions. However, new demands on messaging – such as compliance, security, and disaster recovery – have created new challenges for delivering a messaging system that works great in small businesses and large enterprises alike. To rise to these new challenges, the architecture of Exchange Server 2007 has been updated to take advantage of 64-bit hardware, simplified administration and routing, and to enable an Exchange server to host one or more server roles.

Server Roles

Exchange Server provides a complete messaging system that can run on a single server – meaning that all Exchange services reside on one server, as with the Microsoft Small Business Server product. However, there are significant gains in deployment, management, and security that come from having a flexible, modular system that can be installed across more than one machine. This concept was first introduced in Exchange 2000 Server, where a front-end server could be configured to proxy inbound Internet client protocols to the appropriate mailbox server. Front-end servers are optional and can reduce the load on mailbox servers and simplify Microsoft Office Outlook® Web Access (OWA) and Exchange ActiveSync (EAS) user access. Having front-end servers in medium-size and large organizations made Exchange more scalable by concentrating particular tasks on a limited number of servers.

In Exchange Server 2007, role-based deployment has been expanded, allowing you to assign predefined roles to specific servers. These roles allow organizations to control mail flow, increase security, and distribute services, as shown in the following illustration.

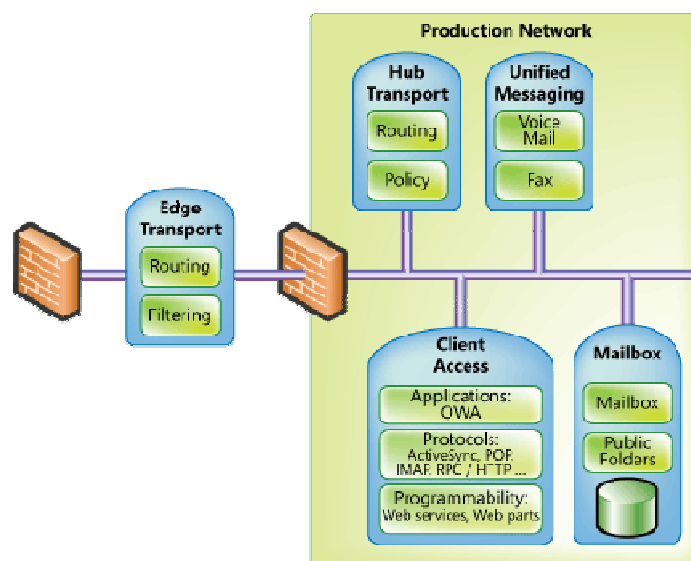


Figure 1: Exchange Server 2007 server roles

Customers would typically customize their Exchange Server 2003 installation, creating specific server roles in a very manual fashion. In Exchange Server 2007, roles are predefined and chosen during installation. The role selected during installation ensures that only the necessary services and components are installed. Not only does this simplify deployment, but it also enables more efficient management and hardware utilization over time.

- **Client Access role.** Similar to the front-end server in earlier versions of Exchange, this server proxies Internet client traffic to the correct mailbox server.
- **Mailbox role.** This role hosts user mailboxes stored in databases that can be replicated or clustered.
- **Hub Transport role.** This role provides internal routing of all messages – from Edge servers, Unified Messaging (UM) servers, or between two users on the same mailbox database. The Hub Transport role is also where messaging policy is enforced for messages moving within and outside the organization.
- **Unified Messaging role.** This role enables PBX integration to allow voice mail and fax messages delivered to Exchange mailboxes, and provides voice dial-in capabilities to Exchange Server. This role and its services are explained in more detail later in this paper.
- **Edge Transport role.** This server resides outside your internal network and provides on-premise e-mail security, antivirus, and anti-spam services for Exchange. Off-premise filtering can be provided by Exchange Hosted Filtering, discussed later.

Role Rules

With the exception of the Edge Transport role, multiple roles or all roles can be installed on a single system. This is because an Exchange server running the Edge Transport role in a perimeter network (DMZ) is not a member of Active Directory or the Exchange organization for security reasons. Another role limitation is on clustered mailbox servers, which can only be configured with the Mailbox server role.

Placing a typical Exchange server, or any other domain member server, in your perimeter network (DMZ) is not recommended because of the communication necessary with production network resources such as DNS and Active Directory. However, the perimeter network is the ideal place to analyze incoming messages and filter out unwanted or virus-infected e-mail. Exchange Server 2007 introduces the Edge Transport role, an Exchange server that is not a traditional member of the Active Directory or the Exchange organization, but analyzes incoming messages for spam and viruses.

The Edge Transport role uses a service named EdgeSync that accepts communications from the Hub Transport on your production network, so no open TCP ports are necessary from the Edge Transport inbound to the production network. A lightweight version of Active Directory named ADAM* is used by the Edge Transport role to store its configuration and other components that are normally stored in Active Directory.

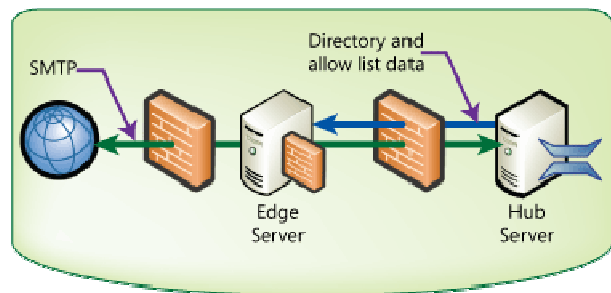


Figure 2: Edge Transport role in perimeter network

Information sent from the Hub Transport server to the Edge Transport server includes recipient lists used to verify that recipients exist before passing the inbound message along. Other information pushed out to the Edge Transport server includes user safe sender lists. A Microsoft Office Outlook® or OWA user can add SMTP addresses to a safe sender list. This list makes its way from the Hub Transport server to the Edge Transport server so that messages to that Outlook user from users on the Safe Sender list are not blocked by Exchange anti-spam components.

* <http://technet2.microsoft.com/WindowsServer/en/Library/29fb059e-544c-4577-bf7c-ba4b08df48431033.mspx?mfr=true>

Administrative Groups and Routing Groups

Administration is simplified and more flexible in Exchange Server 2007. In previous versions of Exchange, administrative groups were administrative boundaries that contained servers and other objects. While administrative groups could be created to segregate administration within your IT organization, once created they were not very flexible. (You can't move servers between administrative groups.) Exchange Server 2007 overcomes this limitation by eliminating administrative groups. Administrative rights can now be delegated from the organization down to the server. Whether your organization uses a centralized or decentralized administrative model, you can delegate permissions to more closely match that model and easily adapt to new models as your organization changes.

Routing groups have been integrated with Active Directory sites. Because the design criteria for Active Directory site boundaries are similar to the design criteria for routing groups, and are the same in most organizations, Exchange now assumes a routing topology based on Active Directory site lines. Maintaining a separate Exchange routing topology and Active Directory site topology is no longer necessary.

Storage Groups and Information Stores

Exchange Server 2007 Enterprise Edition supports up to 50 storage groups and 50 databases per server. You can configure up to five databases per storage group, up to a maximum of 50 databases. Now mailbox data can be distributed across more databases, and mailbox databases can be distributed across more storage groups, than in earlier versions of Exchange Server. Exchange Server Standard Edition supports up to five storage groups and five databases per server. Both Enterprise Edition and Standard Edition have an unlimited database size limit.

The 64-Bit Advantage

Over the last several years, Exchange servers have been rapidly growing in number and average size of mailboxes. There are several reasons for this – consolidated Exchange 5.5 sites, less expensive hardware, less expensive WAN bandwidth, increased information store size limits, and users sending more e-mail. For all of these reasons and more, organizations have implemented fewer large servers in place of several smaller distributed servers. This strategy has several cost and management benefits, but as more and more users are put on fewer and fewer servers, at some point performance becomes an issue.

Using 64-bit hardware and operating system allows for increased performance and scalability by giving Exchange considerably more resources. A 32-bit architecture only allows up to 4 GB of addressable memory, and that is split between the kernel and applications†. Increasing the server and hardware architecture to 64-bit can allow the operating system to address up to 16 Exabytes of memory. (Current hardware limitations are between 16 and 64 GB of RAM.) A 64-bit processor also has more cache capacity, or internal registers that are twice as big as 32-bit processor registers and allow applications such as Exchange to be written in such a way that more of the application resides on the processor – greatly increasing performance and allowing Exchange servers to grow along with increased messaging demands.

64-bit by the numbers

32-bit = 2^{32} or 4 GB of addressable memory

64-bit = 2^{64} or 16 Exabytes of addressable memory

Another area where 64 bit has a considerable impact on performance is in the number of input/output operations per second (IOPS). A 32-bit Exchange server with a large database can experience high IOPS if the disk subsystem is not configured correctly. This means

† With Exchange 2000 Server and Exchange Server 2003, you can give more of the 4-GB addressable memory to applications than the kernel. <http://support.microsoft.com/kb/328882/en-us>

designing your storage subsystem for performance and not capacity – using several smaller disk drives rather than fewer large disk drives, with a lot of the disk space going unused.

Early tests have shown that Exchange Server 2007 running on 64-bit hardware required roughly 75 percent fewer IOPS than Exchange Server 2003 running on the same hardware. Another way to look at this is that Exchange Server 2007 requires a quarter of the disks that Exchange Server 2003 requires for the same performance. This means that Exchange Server 2007 can support more and larger databases than earlier versions of Exchange. It also means that disk subsystem design can be planned for capacity and performance.

New Features and Capabilities

Exchange Server 2007 introduces many new features and capabilities; most organizations will find at least several that are very compelling for their environment and needs. As a stand-alone product, Exchange Server 2007 offers improvements that provide administrators with powerful new tools to do their jobs, and users with more ways to connect to a mailbox that can contain a variety of information needed throughout the day.

Comprehensive Protection from Outside Threats

The primary threat to business e-mail users comes from outside the organization in the form of unsolicited e-mail. Microsoft has two different but equally effective ways to help protect users from this real threat – onsite anti-spam and antivirus protection, and hosted anti-spam and antivirus protection.

For built in protection against spam and viruses, Exchange Server 2007 uses several methods to minimize unwanted e-mail and virus-laden messages.

Protecting your users from spam

The Exchange anti-spam framework has been expanded in Exchange Server 2007. It includes multi-tiered protection that blocks spam in several different ways. Some of the highlights include:

- **Safe-sender aggregation.** To reduce false positives, safe-sender lists created by Outlook users are transferred to Hub Transport and then Edge Transport servers (in the perimeter network) so that messages from these users are allowed into the organization regardless of their spam confidence level.
- **Outlook E-Mail Postmarks.** Outlook 2007 can create a message-specific puzzle and solution, known as a postmark, which is attached to each outgoing message. The postmark requires a number of CPU cycles to create and decipher. Spammers generally don't have time or computational resources to attach complex individual puzzles and solutions to thousands of outgoing messages, so they don't use them. Therefore, when a message with an attached postmark is received by Exchange, it verifies the puzzle and solution. The more complex the postmark, the less likely that the message is spam.
- **Spam quarantine.** In addition to the Outlook Junk E-Mail quarantine included in the Outlook and OWA clients, suspected spam messages can now be quarantined for review by the administrator. The administrator can then delete or release messages from the quarantine to the user.
- **Sender reputation.** Sender reputation is dynamically analyzed and updated. When the Edge Transport server spots specific trends from a given domain, it can impose certain actions to either quarantine or reject incoming messages.
- **Content Filtering on the Edge Transport server.** As spammers change tactics and develop new methods for avoiding detection, the spam content filter can now be automatically updated to keep spam in check, thus helping to protect your organization without adding to your workload.
- **Microsoft Forefront Security for Exchange Server.** Aside from providing complete virus protection as outlined below, this feature also updates virus signatures, IP Reputation Services and anti-spam filters several times per day.

Protecting your users from viruses

For onsite protection against viruses, antivirus software vendors and customers will benefit from the new transport agent API in Exchange Server 2007. With this API, software vendors can write antivirus agents that interact with the built-in Exchange transport agents directly. As messages are introduced into an organization through an Edge Transport server or Hub Transport server, the transports can call the antivirus agent to inspect messages and filter those that contain viruses.

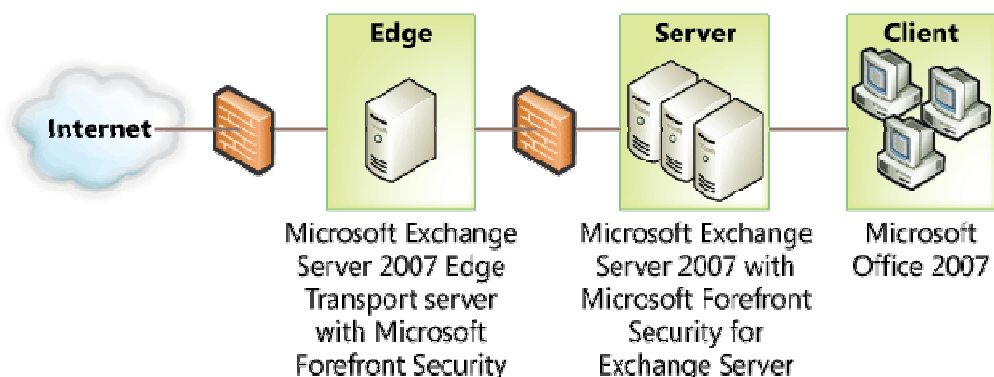


Figure 3: Virus protection using Microsoft Forefront Security for Exchange Server

In addition to this enhanced programmability, a complete antivirus solution is available with Exchange Server 2007. Forefront Security for Exchange Server[‡] delivers comprehensive on-premise antivirus protection for Exchange Edge Transport, Hub Transport and Mailbox roles. Using a multiple-scan engine with content-filtering capabilities, Forefront Security for Exchange Server offers layered protection against virus-laden messages.

Protecting against spam and viruses before they reach your organization

Microsoft can also offload spam and e-mail borne virus protection from your organization with Microsoft® Exchange Hosted Filtering Services. Part of the Microsoft® Exchange Hosted Services (see Appendix A) suite of services, with Exchange Hosted Filtering you get the same benefits of having an Edge Transport server with Forefront Security for Exchange, but management of the services is done by Microsoft. Messages are scrubbed for spam and viruses before they reach your organization.

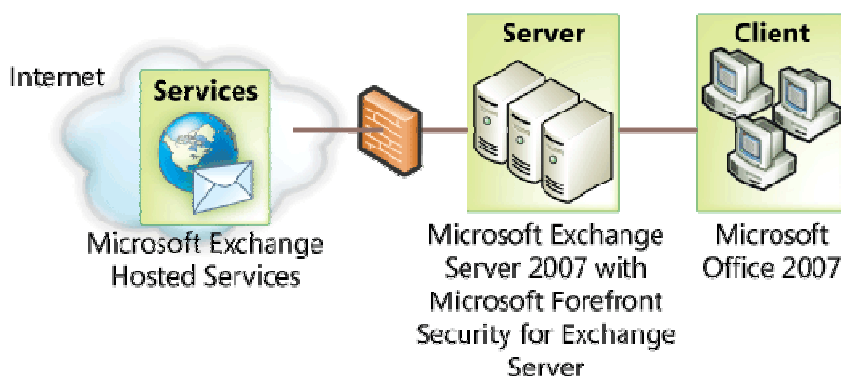


Figure 4: Spam protection using Microsoft Exchange Hosted Filtering

[‡] <http://www.microsoft.com/forefront/default.mspx>; Forefront Security is a feature of the Exchange Enterprise CAL.

Exchange Hosted Filtering uses multiple filters to proactively help protect you from spam, viruses, phishing scams, and e-mail policy violations.

Simplified Message Security

As with earlier versions of Exchange, Exchange Server 2007 uses SMTP to transport messages between Exchange servers within an organization. However, with Exchange Server 2007, all messages within an Exchange Server 2007 organization are encrypted by default. Transport Layer Security (TLS) is used for server-to-server traffic, encrypted Remote Procedure Call (RPC) is used for Outlook connections, and Secure Socket Layers (SSL) is used for Client Access traffic (Outlook Web Access, Microsoft® Exchange ActiveSync®, and Web Services). This prevents spoofing and protects message confidentiality.

Kerberos is used to authenticate, and simplified Transport Layer Security is used to encrypt. TLS is simplified in Exchange Server 2007 because it uses self-assigned SSL certificates. Because each Exchange server is automatically configured with an SSL certificate, internal Exchange servers can not only encrypt messages using SSL, but if external SMTP servers are configured to send or receive using TLS, those messages will be encrypted as well.

Transport Layer Security

With Transport Layer Security (TLS), the underlying operating system or application servers are used to handle security features. Intra-org message transfer in Exchange Server 2007 uses TLS. Secure Sockets Layer (SSL) is another common transport layer approach used to provide data encryption.

Compliance

In business today, e-mail is often both the most common and most preferred method of communication. As a corporate asset, e-mail must be protected and in some instances regulated. Governments and corporate policy makers are defining regulations that affect e-mail and the data it contains. The enforcement of these policies and regulations is known as *compliance*.

For example, the U.S. government has put regulations such as HIPAA[§] in place to protect individual privacy by requiring the secure handling of health care-related communications, including e-mail. Other such regulations, including Sarbanes-Oxley and SEC 17a-4, require financial and accounting data to be handled in particular ways, with any changes or revisions documented. Exchange Server 2007 allows enterprise, governmental, and legal regulations or policies to be enforced through a sophisticated e-mail flow control and policy engine.

Messaging Records Management explained

Within your organization, you most likely have rules, limits, and policies that define how large a mailbox can grow, how long e-mail is retained after it is deleted, and perhaps age limits on certain folders. These policies are put in place to manage e-mail within your organization. Messaging Records Management defines the life cycle of an e-mail message within your organization, based on the policies and rules you have in place.

After an e-mail message is created and the user clicks "Send", several things may happen to the message. Obviously, the

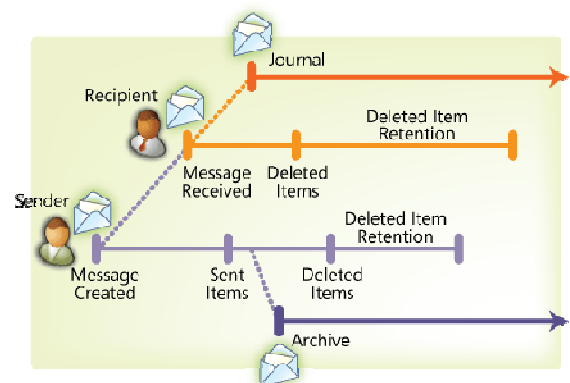


Figure 5: Simple life-cycle of an email message

[§] <http://www.hhs.gov/ocr/hipaa/>

message is delivered to its recipient(s). Beyond that, several actions may be taken with the e-mail. The illustration above shows an e-mail message sent from one user to another, and the various actions that can be taken with the message, including:

- **Sent items.** By default, a copy of each sent message is placed in the Sent items folder.
- **Deleted items.** Most messages are deleted out of the Inbox. By default, deleted messages are moved to the Deleted items folder.
- **Deleted items retention.** After a user deletes a message from the deleted items folder, the message may be stored for a period of time defined by the deleted items retention policy configured on the Exchange server. (The default is now 14 days.) After the retention period expires, the message is finally deleted from the user's mailbox.
- **Journaling during transport.** During transport, messages that meet defined criteria can be sent to any message archive that accepts SMTP e-mail. An archive contains copies of messages along with message metadata.
- **Journaling Managed Folder messages.** Messages in a Managed Folder (described later in more detail) can be sent to any message archive that accepts SMTP e-mail, such as SharePoint Server 2007.
- **Backups.** Messages are also copied during each backup. Backups are typically used for disaster recovery but can also be used to retrieve messages that have otherwise been deleted or lost.

The life cycle of an e-mail message begins when the message is created, and ends when all copies of the message are deleted. You can manage what happens to the message between these points, as defined by your organization or by government regulations. A simple life cycle is where a message is simply sent and received.

With Exchange Server 2007, you can define your e-mail life cycle for messages that touch your organization so that legal discovery and compliance policies are satisfied.

Applying policy and order using transport rules

Exchange administrators can define transport rules in Exchange Server 2007 that conform to corporate e-mail policy. During message transfer, if the message meets the transport rule criteria, an action will be taken that may affect that message. Rule criteria are based on message sender, recipient, or metadata – such as a word or phrase within the message, or the message classification. Message classification can be applied by a user or rule, such as confidential or personal.

Among the common uses of transport rules are

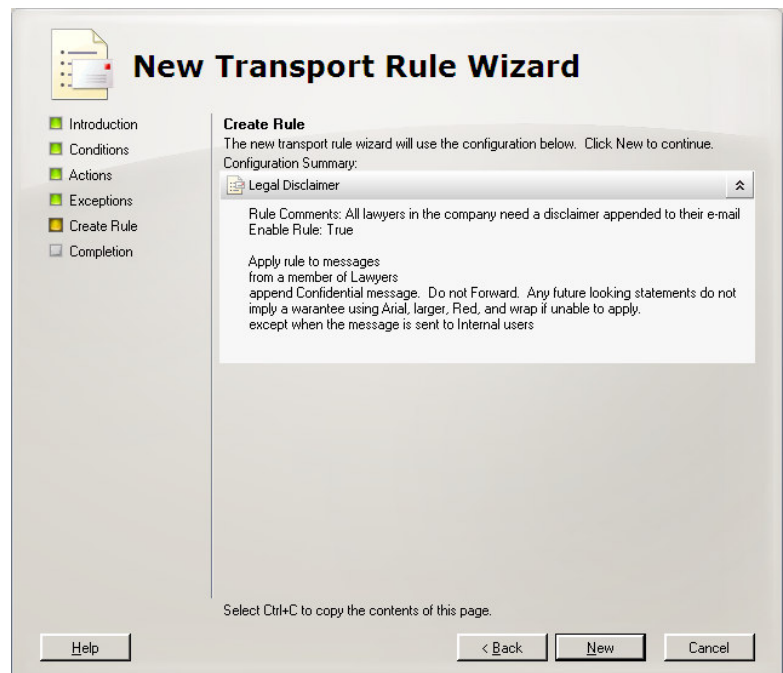


Figure 6: Transport rules can be created using a wizard

ethical walls between users within the same organization whose communication must be managed. You can define a rule where an action is taken when messages are sent between users or groups of users. Several actions can be taken: drop the message, return a non-delivery report, strip attachments, modify the message, journal the message, send a copy of the message to a compliance officer, and so on. For example, Market Analysts and Brokers within an organization – two groups whose communication should be monitored or not allowed – can be managed with a transport rule. In this example, the transport rule restricts messages being exchanged between these two groups of users.

Rules can also be defined that take action based on message classification. Users can choose from several types of message classifications within Exchange Server 2007, in addition to classifications that can be assigned by the transport rule itself. For example, all messages sent to the corporate counsel can be classified as confidential. Confidential messages can be archived differently than normal messages, or avoided during discovery searches.

Managed Folders

After a message reaches your inbox, it is outside the reach of transport rules, so policy and compliance responsibility is shifted to folder rules. Exchange Server 2007 introduces Managed Folders, useful for meeting compliance and also for general message organization.

Managed Folders are created by an Exchange administrator and appear in the mailbox folder list of a user's mailbox. They can have specific rules and age limits applied to them, but are not shared across users like Public Folders.

A compliance scenario provides a good example of how a Managed Folder might be used. Some messages within your organization may need to be retained for seven years for compliance purposes. You can create a Managed Folder that stores and archives messages for seven years. As users receive messages that require that level of compliance, they move them into the Managed Folder.

Another example of a potential Managed Folder involves customer issues. In this example, the Customer Issues alias delivers messages to the sales manager's inbox. The sales manager, along with all other managers, is configured by the administrator so that the Customer Issues folder appears in his or her mailbox. The administrator also configures the Customer Issues folder to journal all messages moved into the folder to a Microsoft® Windows SharePoint® Services-based customer service site. After the customer complaint message is moved into the Customer Issues folder by the sales manager, the Managed Folder policies apply. All managers can access the SharePoint site to review customer issue messages and their resolutions.

Journaling for compliance and retention

Together with security, compliance and retention are at the heart of most messaging regulations.

Journaling is an important part of compliance. The ability to audit all mail sent to and received by a group of users is required by several different regulations and is useful to organizations for internal policies or audits.

Messages journaled by Exchange Server 2007 can be stored in an Exchange database, on a SharePoint site, or can be sent to any external SMTP address used by third-party journaling companies.

In previous versions of Exchange, entire mailbox stores had to be journaled. In

Journaling and archives

Journaling rules associated with a given set, or scope, of users copy messages to an alternate location. The scope can be an individual, a distribution list, or the entire organization. Additionally, Managed Folders can journal messages that are moved into a folder by a user.

An archive is where journaled messages are held. An archive can be another Exchange Mailbox, a SharePoint site, or a third-party archiving solution.

Exchange Server 2007, a scope determines what messages are journaled. The scope can be as granular as a single mailbox, a Distribution List, a database, or the entire organization. Voice mail messages and missed call notifications can be excluded from the journal. Also, a detailed report on what is journaled includes information such as To:, From:, Cc:, Bcc:, and expanded distribution list information as well as other metadata from each journaled message.

Maximizing Availability

As availability requirements have increased over the years, so has the dependability of Exchange Server and the hardware it runs on.

When Exchange was first released in the mid-1990s, expectations for e-mail as a communication tool were not much different than for paper mail. But as users became more tech-savvy and dependence on e-mail grew, so too did the need to guarantee Exchange availability.

To increase messaging availability, redundancy can be built into the Exchange architecture that includes things like multiple front-end servers, multiple e-mail routes between sites and the Internet, and Public Folder replicas. However, increasing the availability of Exchange servers that host mailboxes can be challenging and costly.

One (but no longer the only) method for increasing availability for Exchange mailbox servers is to use an Exchange cluster. Using a Windows cluster of two or more nodes with Exchange provides redundant servers so that if a node or a service on a node fails, the other node can assume the Exchange services.

What is obvious here is that the Exchange services are redundant, while the Exchange mailbox databases are not. Therefore, Exchange clusters increase availability by adding redundancy to Exchange services; until now, providing database redundancy was only possible using third-party hardware or software solutions.

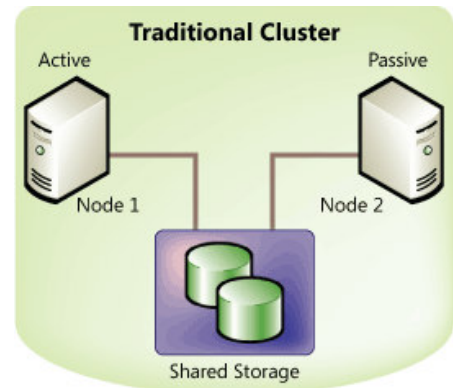


Figure 7: Traditional Cluster with shared storage

Changes to traditional clusters

Exchange Server 2007 provides the same traditional shared-storage clustering solutions as earlier versions of Exchange, except that Active/Active clustering is no longer available. Active/Active clustering was strongly discouraged in Exchange 2000 Server and Exchange Server 2003 and is now unavailable in Exchange Server 2007. For more information on why Active/Active clustering is not recommended in Exchange Server 2003, go to: <http://support.microsoft.com/kb/815180/en-us>

Exchange Server 2007 offers another clustering option that allows both services and databases to be failed over to a passive node, thereby providing both service and database redundancy. Using the same technology that replicates databases across multiple nodes, Exchange Server 2007 also allows a single server to replicate its database locally, providing an up-to-date copy of the local information stores that can be mounted if the primary database becomes corrupt.

Cluster Continuous Replication

To provide redundancy for Exchange services and information stores, Exchange Server 2007 provides Cluster Continuous Replication (CCR). Similar to clustering solutions available with earlier versions of Exchange, CCR uses Windows Clustering Services to provide virtual servers and failover capabilities. However, with CCR, shared storage is not required because each node has its own copy of the information stores. This allows customers to implement a variety of storage options such as Direct Attached Storage, Serial Attached SCSI, and Storage Area Networks. This solution uses a form of log file shipping that is found in databases such as Microsoft® SQL Server™.

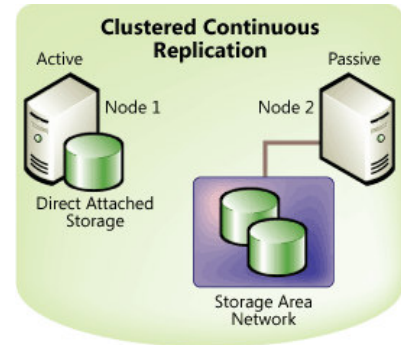


Figure 8: Clustered Continuous Replication without shared storage

On the active node, transactions are written to the transaction log. When the current transaction log is full, the passive node pulls a copy of the transaction log from the active node to the passive node. A service on the passive node then posts the transactions from the replicated transaction log into the database on the passive node.

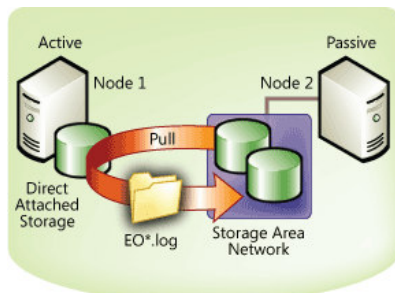


Figure 9: Passive node pulls transaction logs from active node

If the active node fails (either planned or unplanned), the cluster fails over to the passive node that mounts the databases and continues providing Exchange services. Transactions logs on the new active node are then replicated over to the new passive node as needed.

Aside from the benefits of having your databases replicated across multiple nodes, you can also back up the database and transaction logs on the passive node without impacting performance on the active node. After backup is complete on the passive node, and the proper transaction logs are deleted, the transaction logs on the active node are also deleted. The cluster nodes must be on the same subnet, but if the subnet spans physical

networks, you can place the active node and passive node in different physical locations. This means that replicating your Exchange databases to a remote disaster recovery site is now possible.

Also, since the reasons for having to restore from backup are reduced with CCR, you may be able to reduce your operating costs by reevaluating your backup strategy and decide if the same schedule, backup type, and number of tapes are needed.

Local Continuous Replication

Local Continuous Replication (LCR) takes the database replication technology from CCR and applies it to a stand-alone Exchange Server 2007 server. With LCR, databases are replicated to another location on the local server. If the database becomes corrupt or a disk fails, the Information Store can be pointed to the local copy and service can continue.

Ideal for small or medium-sized organizations, LCR allows for rapid recovery from disk or database issues and only requires an additional disk or disks to host the database replicas. While backups (with off-site storage) are a must for disaster recovery, LCR is an affordable way to provide increased availability.



Figure 10: Local Continuous Replication replicates locally

How each cluster scenario relates to the other

With more choices come more decisions – between traditional Exchange clustering with shared storage, CCR, or LCR. How shared storage clustering compares to CCR depends on whether database redundancy hardware or software solutions are in place with the shared storage. Without storage redundancy, the shared storage cluster is only providing service failover, and the databases in shared storage are a single point of failure. If the shared storage solution provides redundancy for the databases, a traditional cluster is on par with CCR.

Similar to traditional clustering but without database redundancy, LCR only provides half of a redundancy solution by not having multiple nodes for service failover. However, for organizations without the need or budget for a multi-node cluster, LCR is a good way to provide affordable redundancy that can reduce downtime in the event of a disk failure or database corruption.

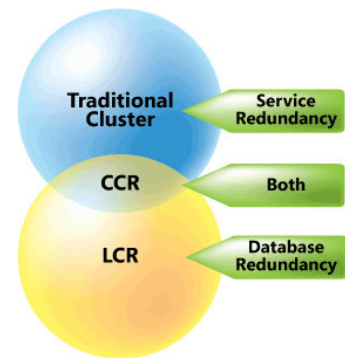


Figure 11: Cluster scenarios

Availability of other roles

Providing redundancy for a mailbox server with a cluster is only a partial high-availability solution. Other Exchange Server 2007 roles cannot be installed on a cluster but need to be made redundant by using multiple servers. When designing your Exchange Server 2007 architecture for high availability, verify that no single point of failure exists between the clients, their mailboxes, and the directory.

Simplifying Exchange Management

One of the primary goals of Exchange Server 2007 is to make an Exchange administrator's job easier and more effective. Day-to-day maintenance, monitoring, and troubleshooting can become a burden in small or large organizations. With its new tools and features, Exchange Server 2007 aims to simplify Exchange management so that Service Level Agreements can be upheld and proactive maintenance and monitoring can be achieved to prevent issues before they arise.

Tools for improved manageability

Exchange Server 2007 introduces a modular server role-based architecture to address changing messaging requirements in the enterprise. Similarly, a new graphical management tool is included with Exchange Server 2007. The Exchange Management Console is a Microsoft Management Console (MMC)-based tool that reflects changes to the architecture so that server roles can be independently managed and the new administrative model can be implemented, with no administrative or routing groups.

As shown in the following illustration, the Exchange Management Console is divided into four sections: the Console Tree, Result Pane, Work Pane, and Action Pane. Multiple panes reduce navigational confusion and provide more information at a glance.

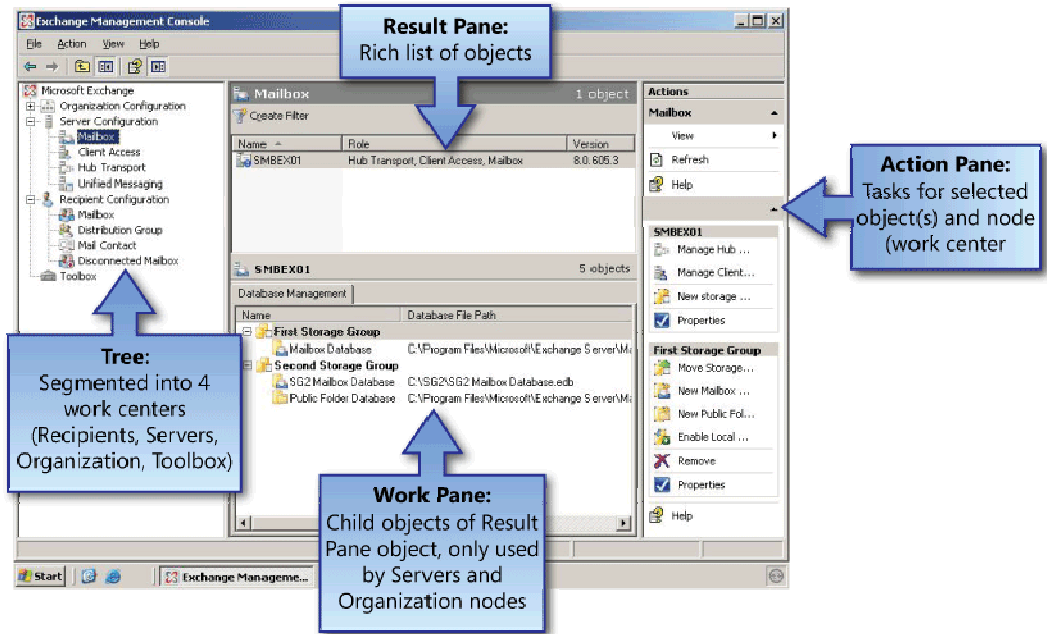


Figure 12: Exchange Management Console work centers

The four independent work centers in the Exchange Management Console Tree allow you more flexibility when delegating administrative permissions. They also let you effectively manage Exchange without having to drill down several layers to get to the object to be managed.

- **Recipient Configuration** allows you to manage the Exchange recipients.
- **Servers** allow you to manage the servers based on their roles. You can use this work center to configure all of the Exchange servers and their child objects.
- **Organization Configuration** enables you to configure Exchange global data that applies to all servers running a particular server role.
- **Toolbox** provides a central location for Exchange administrative tools and troubleshooters

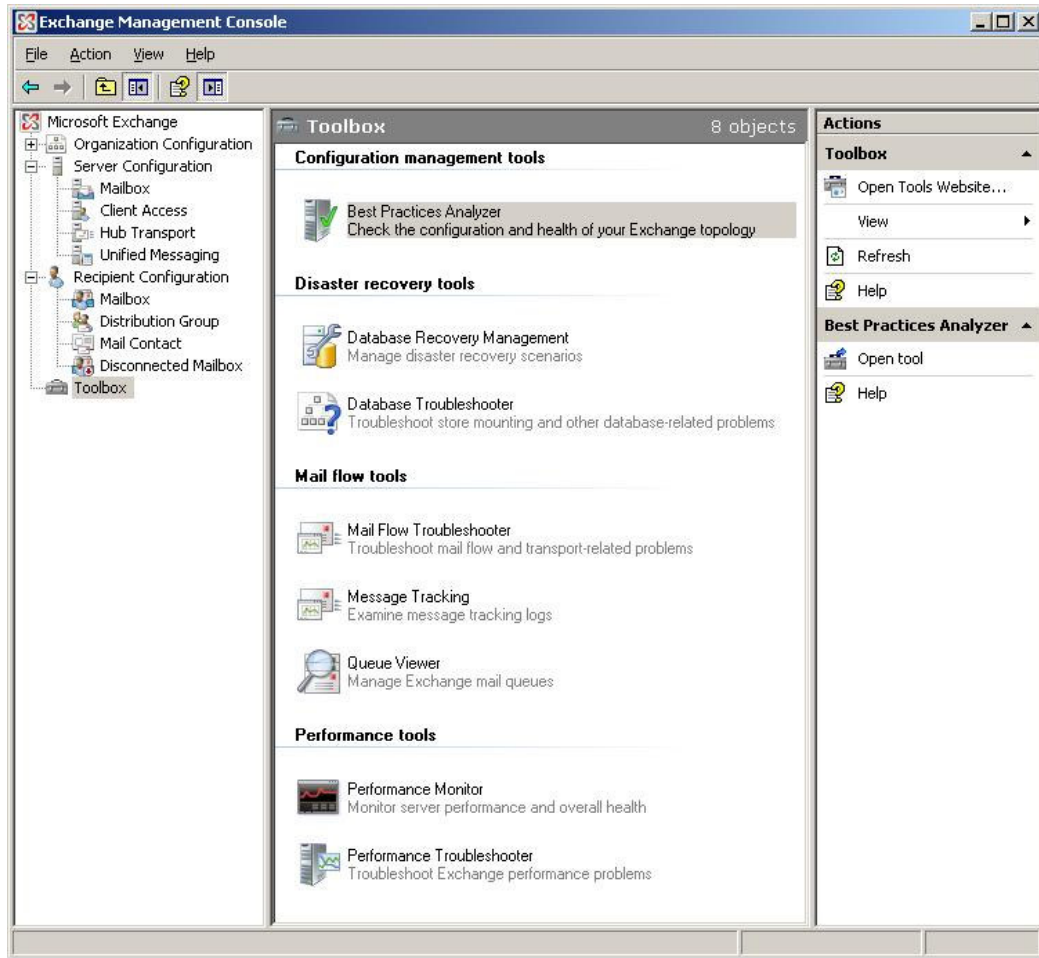


Figure 13: Exchange Management Console toolbox

A powerful scripting tool – Exchange Management Shell

The Exchange Management Console uses a powerful scripting technology named Exchange Management Shell. Based on the Windows PowerShell™, Exchange Management Shell is a command-line tool that gives you access to a very powerful set of cmdlets (pronounced "command-lets") made up of verb-noun pairs. Using PowerShell, you can script complex tasks with minimal code or run them interactively at the shell prompt. With the shell, you can execute commands that access and affect a number of different sources, including the mailbox database, registry, and Active Directory.

Every task in Exchange is made up of a particular verb attached to a noun. Because cmdlets and scripts can be manipulated as Microsoft .NET objects, applications can be built using managed code that can take advantage of the cmdlets and their output. This model is the basis for the Exchange Management Console. All functionality available from the Exchange Management Console is provided through cmdlets in the Exchange Management Shell.

To dive a little deeper into the Exchange Management Shell, the example below shows how a verb-noun pair can stand on its own. In other cases, a parameter could follow the task (verb-noun pair) in the format of the parameter name and an argument string. Alternatively, the parameter could be loaded by using a pipe from a task run earlier, or a variable set used earlier.

Scripting is made easier with an auto tab complete feature that allows you to press TAB to tab through the options as you're typing a particular cmdlet. Also, if you omit an option, the cmdlet will prompt you, rather than stopping with an error message.

In the example below, a simple shell command gets mailbox properties for a specific server.

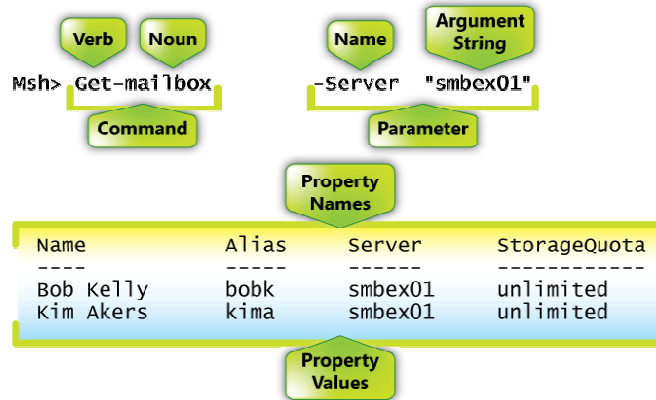


Figure 14: Exchange Management Shell command structure

Tasks associated with the Get verb return a set of property names and property values, as shown in the illustration above. Although a noun such as “mailbox” may contain a large number of property names, by default the shell only returns the most commonly used subset. Additional properties or a defined property set can be used to determine what values are returned.

Simplifying Outlook configuration with Autodiscover

In the past, Outlook profile configuration could be challenging because most users don't know the name of an Exchange server needed to resolve their profile. With the new Autodiscover feature, users only need to know their user name, password, and e-mail address to configure an Outlook profile.

Autodiscover is run when Outlook is started – periodically in the background – and if the connection to the Exchange server is lost. The process Autodiscover follows when determining profile information is:

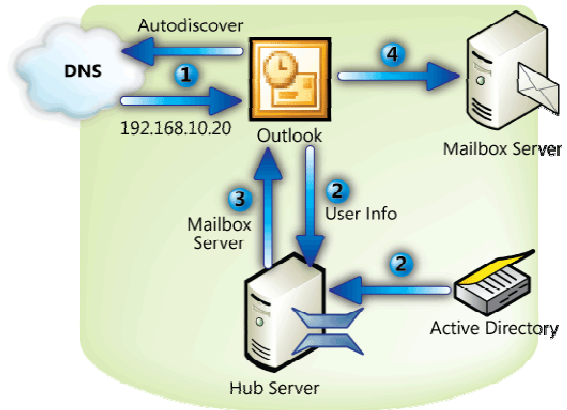


Figure 15: The Autodiscover process

1. Outlook locates an Autodiscover service on a Client Access server using DNS.
2. The Autodiscover service on the Client Access server uses configuration information from Active Directory to build a configuration template for Outlook. The configuration template includes information about Active Directory and the Exchange Server 2007 organization and topology.
3. Outlook downloads the configuration information from the Autodiscover service.
4. Outlook then connects to Exchange by using the downloaded configuration settings.

Productivity Boost

Users are becoming more and more sophisticated, and their productivity relies on their ability to find, share, and use information. Power users like these were once the exception but are now the rule. These users require centralized access to information from anywhere. With its deep integration with Office 2007, Exchange Server 2007 facilitates data sharing between data sources (Exchange, SharePoint, file shares) like never before, leading to greatly enhanced productivity.

Increase collaboration and productivity will follow

Separating employees from each other can have a major impact on productivity in most organizations. Yet with remote offices, roaming and traveling users, and organizations spread across several time zones, users are more geographically dispersed than ever before.

To bring users back together again, at least virtually, Exchange Server 2007 allows integrated access to several different sources of information using tools built for collaboration. Highlights include:

- **Unified Messaging** gives users anywhere access to all of their vital business communications, including e-mail, voice mail, and fax messages in desktop, mobile, web, or phone clients.
- **LinkAccess** allows you to access SharePoint sites and file shares through Outlook Web Access, eliminating the need to expose your internal SharePoint topology or file shares to the Internet or require a virtual private network (VPN) connection to gain access.
- **Calendar Concierge** refers to a set of features that simplify and automate scheduling people and resources
 - *Scheduling Assistant* analyzes attendee and resource schedules and suggests meeting times using a color-coded user interface based on who's available when. Users interact with it in Outlook Web Access or Outlook 2007.
 - *Calendar Attendant* runs on the Exchange 2007 server and, without any end user interaction required, marks meeting requests as tentative on recipient calendars until users act on the request, and assures that only the latest version of calendar requests are in your mailbox.
 - *Resource Booking Attendant* also runs on the Exchange 2007 server and, without any end user interaction required, manages resource availability and allows for resource policies such as available hours and scheduling permissions.
- **WebReady Document Viewing** in Outlook Web Access 2007 can transcode a variety of document types – including Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and PDF files – from their native format into HTML so that they can be viewed in a client browser even if the application that created the document is not installed on the client. This allows users to be productive from almost any machine and keeps viewed documents safe, even on kiosk machines, since HTML documents are purged by Outlook Web Access at logoff or session timeout.
- **Flexible Out of Office rules** allow you to configure a different Out of Office rule for internal users and Internet users. Each rule can also be given a start and end date.

These features help bring separated users together. If you're at an airport or trade show kiosk, you can receive e-mail, check your calendar, or review a document in SharePoint – all through the rich and familiar Outlook Web Access user interface or from your Exchange ActiveSync-enabled mobile device. Therefore coworkers at another trade show, or airport, or the office can continue their work with your valuable input or approval. This way, collaboration and productivity don't have to be put on hold while you're away.

Unified Messaging

Exchange Server 2007 marks a significant advance over previous versions of Exchange by offering Unified Messaging (UM) capabilities. *Unified Messaging* refers to the integration of various messaging media, such as voice mail and e-mail, into a messaging solution accessible from a single location - the Exchange inbox. Voicemail, faxes, and e-mail are seamlessly delivered to the mailbox, where you can access them by using familiar clients such as Outlook, the improved Outlook Web Access, and a variety of mobile devices, and even from ordinary telephones through new Outlook Voice Access with speech recognition. You can now phone into the UM server from any location and access your Exchange voice mail, e-mail, calendar, and contacts. You can also work with any of these types of communication, independent of their format and method of access.

Here is a high-level overview of how Exchange UM works:

When calls come in from phones and fax machines via the public switched telephone network, as well as from phones within your organization, they reach your PBX – either a traditional PBX or an IP-PBX system, depending on what type of infrastructure you have in place. If you have a supported IP-PBX, it can directly communicate with the UM server via Session Initiation Protocol (SIP), used to setup and terminate voice communications, and Real-time Transport Protocol (RTP), which defines a standard packet format for delivering audio and video over a given network.

If you have a traditional PBX, you will need to place a VoIP gateway between it and the UM server, situated at the same site as the PBX. The UM server does not need to be placed at the same site as the PBX but is located in your existing forest, ideally very close to the rest of your Exchange infrastructure. The UM server then communicates with the other Exchange server roles, storing messages on the mailbox server.

Additional UM User Features

In addition to the essential UM features described above, Exchange UM includes a speech recognition-enabled auto attendant that can answer an organization's internal and external phone calls and automate dialing through directory integration with the organization's Global Address List. This feature allows you to call a main switchboard number, ask for the person you want to reach, and then get transferred to their number without operator intervention.

Exchange UM also allows you to customize your voice menus. For example, you can create a custom menu that states, "Say one for sales, say two for support," and so on.

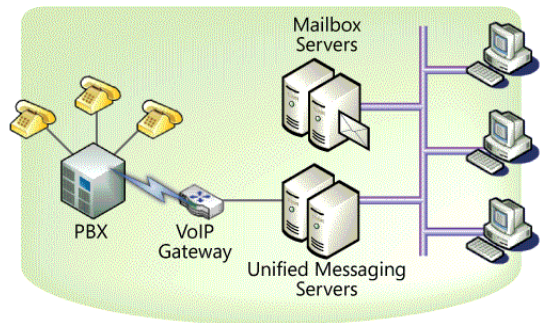


Figure 16: Unified Messaging topology

Telephony TLAs

VoIP: Voice over IP – voice calls over a data network

TDM: Time Division Multiplexing – allowing multiple calls on one line

PBX: Private Branch Exchange – a telephone switch used by organizations to share a limited number of external lines

SIP: Session Initiation Protocol – a protocol used to initiate VoIP calls

PSTN: Public Switch Telephone Network – the telephone network

IVR: Interactive Voice Response – a feature that allows Exchange users to interact with the telephone system

Unified Messaging can reduce cost by consolidating two messaging systems (electronic and voice) into one. Unified Messaging can also save time by allowing office workers to stay in Outlook to receive voice mail. Mobile workers can receive all their communications on their mobile device, which broadens access to information that helps keep them productive when on the road.

Anywhere Access

One of the other ways Exchange Server 2007 increases productivity is by providing access to Exchange data in a variety of ways. Prior to Exchange Server 2007, there were several ways to access your mailbox from the Internet or intranet. Exchange Server 2007 offers improvements to current clients and other options new to Exchange.

- **Outlook Anywhere** allows users to easily access their mailbox from any computer running Outlook that is connected to the Internet, by using the Autodiscover feature described above along with RPC/HTTP.
- **Outlook Web Access** has a new look and feel similar to Outlook 2007. Improvements to the Search feature and the Address Book make getting the information you're looking for easier. Outlook Web Access also allows you to access network resources, such as SharePoint sites and file shares. With Outlook Web Access, you can now access your mailbox and network resources without a VPN.
- **Microsoft Exchange ActiveSync®-enabled Mobile Devices** provide seamless and integrated mobile access to Exchange data. These devices include Windows Mobile® devices and devices of Exchange ActiveSync licensees, including Nokia, Sony Ericsson, DataViz, Palm and Symbian. Without any additional software or licensing, Exchange mobile users using either type of device can now manage their mobile devices using Outlook Web Access. For example, if the device is lost, the user can initiate a remote wipe of the device from Outlook Web Access, without having to contact their helpdesk or a third party. Administrators can define per-user policies, and new policies, for example allowing or disallowing message attachments. The upcoming version of Windows Mobile and some ActiveSync-enabled devices can take advantage of additional mobile features available with Exchange Server 2007, including improved calendaring, message flagging, search and more.
- **Outlook Voice Access**, a feature of Exchange Unified Messaging, gives you access to your mailbox, calendar, personal contacts and corporate directory through your phone by using speech recognition or touch tones as the interface. Going to be late to a meeting? You can now call your mailbox and have an e-mail message sent to all meeting attendees explaining that you are running 15 minutes late.

Deploying Exchange Server 2007

How Exchange Server 2007 is deployed varies slightly depending on whether you're upgrading, or transitioning, from Exchange 2000 Server or Exchange Server 2003. Note that there is no direct upgrade path from Exchange Server 5.5.

Installing Exchange Server 2007

There are two methods for installing Exchange Server 2007. The traditional method, using a graphical user interface, allows you to choose the role of the server you're installing, perform several pre-installation tests, and then perform the installation.

You can mix and match the roles you require, or install all roles on a single server for small to medium-size organizations with only a few servers. The one role that cannot be installed with the others is the Edge Transport role. This role is meant to be outside the Exchange organization (in the perimeter network) and therefore will not install with any other role.

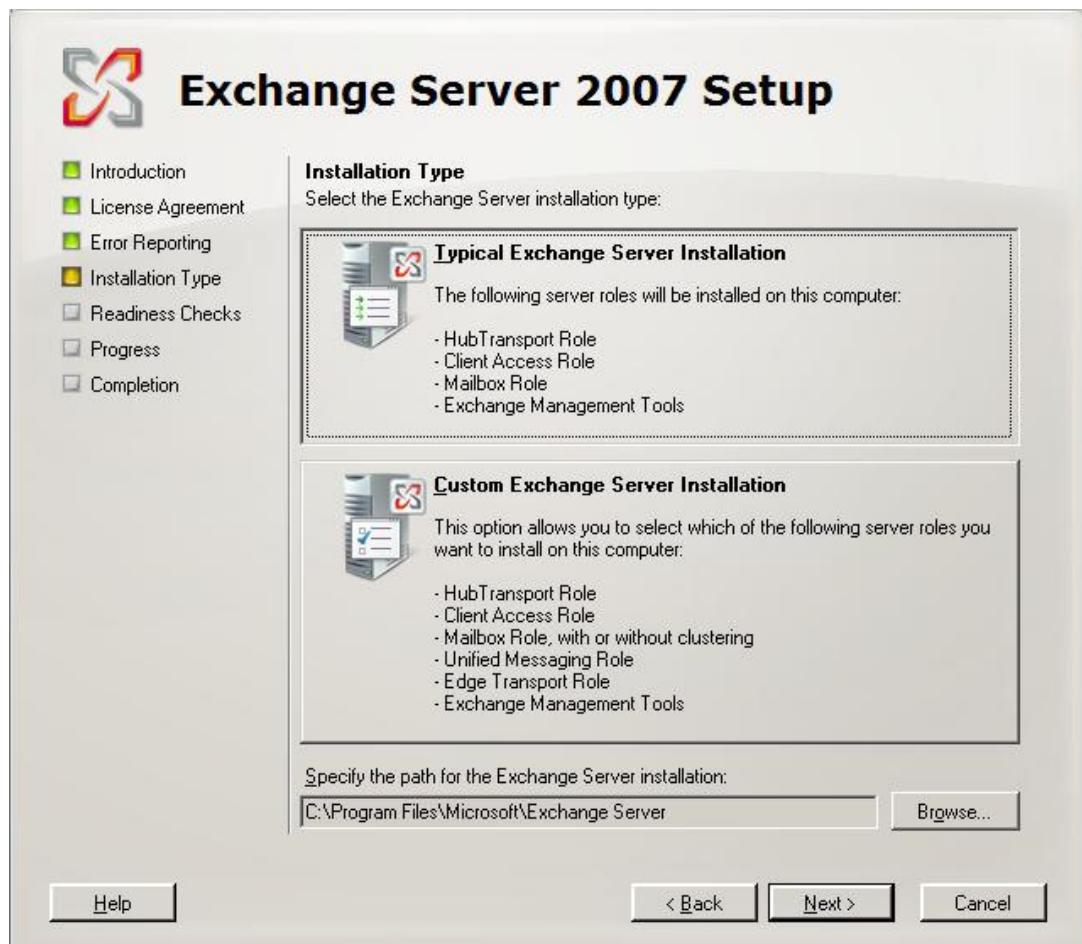
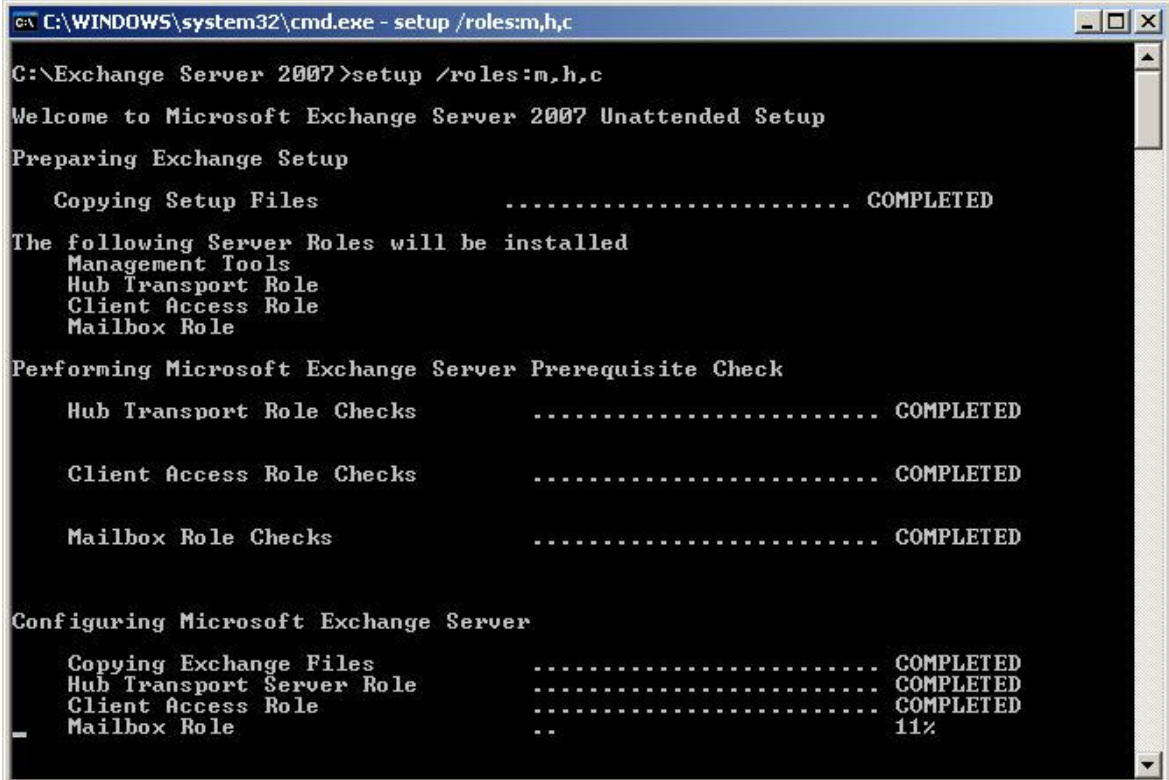


Figure 17: Exchange Server 2007 setup using the graphical user interface

The second method of installing Exchange is by using the Exchange Management Shell. A scripted installation is useful in larger organizations where standard installation options are defined and the installation is carried out remotely. This is especially useful when you can define deployment characteristics beyond just the installation. For example, after installation using the shell is complete, the script can continue on to create Storage Groups and mailbox

databases, set mailbox size limits, and so on. Therefore the scripted installation delivers a server that is not only installed, but is also configured for your organization.



```
C:\WINDOWS\system32\cmd.exe - setup /roles:m,h,c
C:\Exchange Server 2007>setup /roles:m,h,c
Welcome to Microsoft Exchange Server 2007 Unattended Setup
Preparing Exchange Setup
  Copying Setup Files ..... COMPLETED
The following Server Roles will be installed
  Management Tools
  Hub Transport Role
  Client Access Role
  Mailbox Role
Performing Microsoft Exchange Server Prerequisite Check
  Hub Transport Role Checks ..... COMPLETED
  Client Access Role Checks ..... COMPLETED
  Mailbox Role Checks ..... COMPLETED
Configuring Microsoft Exchange Server
  Copying Exchange Files ..... COMPLETED
  Hub Transport Server Role ..... COMPLETED
  Client Access Role ..... COMPLETED
  Mailbox Role .. 11%
```

Figure 18: Simple command line setup of Exchange Server 2007

Upgrading to Exchange Server 2007

Exchange 2000 Server and Exchange Server 2003 both have supported upgrade paths to Exchange Server 2007. A simplified description of the process is moving, or transitioning, data and services from Exchange 2000 Server or Exchange Server 2003 to Exchange Server 2007. During the transition, Exchange Server 2007 routes messages within an Exchange 2000 Server or Exchange Server 2003 organization. However, these previous versions of Exchange do not know how to route messages in an Exchange Server 2007 organization. All Exchange Server 2007 servers will appear in a single routing group. Therefore, it's important that Exchange Server 2007 Hub Transport servers be placed in key locations to manage routing. This involves re-homing all routing group connectors to the Exchange Server 2007 Hub Transport servers in the same location.

Upgrade path for Exchange 5.5 customers

Exchange Server 5.5 customers must first upgrade to Exchange Server 2003 and Active Directory before deploying Exchange Server 2007. For more information on upgrading from Exchange Server 5.5 to Exchange Server 2003, go to <http://www.microsoft.com/technet/prodtechnol/exchange/2003/upgrade.mspx>

Re-homing of Routing Group Connectors can take place in two phases. In the first phase, the central or hub locations will have their Routing Group Connectors re-homed to Exchange Server 2007 Hub Transport servers. In the second phase, the remote locations switch to Exchange Server 2007 Hub Transport servers. The second phase ensures that messages at

remote locations do not have to travel to a hub location and back, but instead stay at the local destination.

As routing groups are disabled during migration, it is important to review how Public Folder referrals are configured. Exchange 2000 Server and Exchange Server 2003 may automatically choose a server that is not ideal for Public Folder referrals. If this happens, Public Folder referrals can be manually defined in Exchange Server 2003.

Design considerations for legacy Exchange customers

Current Exchange 2000 Server and Exchange Server 2003 customers can prepare for Exchange Server 2007 by reviewing their existing Active Directory site design and considering how messages will be routed using that design and whether any changes will be necessary. Exchange Best Practice Analyzer 2.7** has been updated to make recommendations for preparing for Exchange Server 2007. Also, because Exchange Server 2007 requires 64-bit hardware (x64), if you are upgrading hardware in the meantime, you should purchase 64-bit hardware to prepare for the upgrade.

** Available from <http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/analyzers/default.mspx>

Conclusion

This paper reveals how Exchange Server 2007 provides services well beyond traditional e-mail. Built-in capabilities that give users an *anywhere access* platform, with more ways to access more types of information than ever before. Built-in services that, when configured, provide dependable access to information compliant with regulatory requirements. This information is supported in many formats, including e-mail, voice mail, fax, calendar, contacts, SharePoint sites, and file shares.

For administrators, Exchange Server 2007 offers a modular, role-based architecture allowing you to locate services where they're needed and delegate administration in a way that closely matches how your IT department is organized. Features like the Exchange Management Shell allow administrators to create scripted tasks that proactively manage your messaging environment. While tools like those in the Exchange Management Console bring up to date Exchange performance and troubleshooting best practice knowledge from Microsoft to your fingertips.

Exchange Server 2007 takes a hard line approach to security by stopping spam and viruses before they enter your organization. Whether you chose on-premise protection using Edge services or off-premise protection using Exchange Hosted Filtering, you'll get dynamic protection that is regularly updated as security threats change.

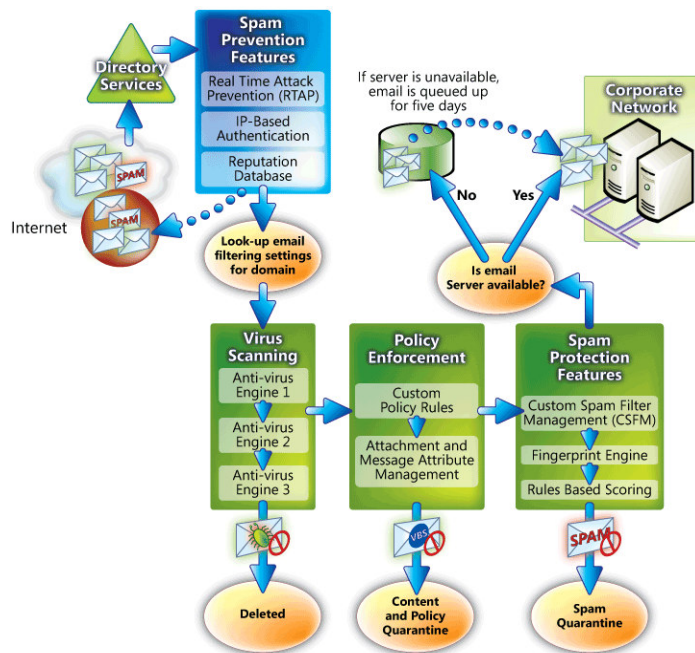
Exchange is rooted in a long history of delivering cutting-edge messaging services. Exchange Server 2007 continues that tradition by helping to make your organization more secure, your users more productive, and your job easier.

Appendix A – Microsoft Exchange Hosted Services

As mentioned above, Microsoft can offload spam and e-mail-borne virus protection from your organization with Exchange Hosted Filtering, which is just one of the services provided by Exchange Hosted Services. Beyond anti-spam and antivirus protection, Microsoft offers a comprehensive suite of other hosted services for e-mail security and management to help protect your organization against data loss due to disasters and stay compliant.

The Exchange Hosted Services suite includes four different subscription-based services. Each can be subscribed to separately:

- **Exchange Hosted Filtering** uses multiple filters to proactively help protect you from spam, viruses, phishing scams, and e-mail policy violations.
- **Exchange Hosted Archive** stores e-mail and Instant Messages to help you meet a variety of regulatory, legal, and corporate archiving requirements.
- **Exchange Hosted Continuity** stores copies of e-mail messages remotely, allowing your users to access their messages in the event of an outage or disaster by using a Web-based e-mail client similar to Outlook Web Access.
- **Exchange Hosted Encryption** helps preserve e-mail confidentiality by allowing your users to send and receive encrypted e-mail directly from their desktops.



Microsoft Exchange Hosted Services

The types of protection offered by Exchange Hosted Services can also be configured in Exchange Server 2007 with Edge Transport servers and other Exchange Server 2007 features. However, many organizations have neither the staff nor time to configure and manage this level of protection. Therefore, EHS is the ideal solution for these organizations.

For more information, go to <http://www.microsoft.com/exchange/services/default.aspx>



**Windows
Server System™
Engineered**

Windows Server System™ software is engineered with industry-leading standards and delivers better manageability, security, and integration.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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.

© 2006 Microsoft Corporation. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted 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.

Microsoft, Active Directory, Excel, Outlook, SharePoint, Windows PowerShell, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.