

1.0 Q: What is Exchange Server 2007?

A: Microsoft Exchange Server 2007 is the next version of Microsoft Exchange. Microsoft Exchange is the industry's leading e-mail, calendaring, and unified messaging server. The release of Exchange Server 2007 is closely aligned with the 2007 Microsoft Office release. Together, these products deliver a best-in-class enterprise messaging and collaboration solution.

2.0 Q: What's new in Exchange Server 2007?

A: Exchange 2007 provides built-in protection to keep the e-mail system up and running and protected from outside threats and lets employees work more productively from wherever they are by using a variety of clients. These clients include Microsoft Office Outlook 2007, Microsoft Office Outlook Web Access, and mobile devices. Exchange Server 2007 makes it easier for IT departments to deliver these new capabilities to their organizations by making the messaging environment easier to manage and more cost-efficient. For more information about Exchange Server 2007, see [What's New](#) in the Exchange 2007 product documentation.

3.0 Q: How does Exchange Server 2007 integrate with Microsoft Office Outlook 2007?

A: Outlook 2007 provides the most complete e-mail, calendaring, contacts, and tasks functionality available in an e-mail client that is compatible with Exchange. When Outlook 2007 is used with Exchange Server 2007, users benefit from the new Scheduling Assistant that automates time-consuming meeting and resource scheduling, the ability to plan and customize out-of-office communications, and managed e-mail folders that facilitate compliance with internal and regulatory policies. Outlook 2007 and Exchange Server 2007 also combine to enhance security by offering features that are easy to use and let users confidently send and receive sensitive business communications through e-mail. By enabling the Autodiscover service, you can reduce the complexity of client configuration and reduce administrative costs that are associated with troubleshooting connectivity issues for users.

4.0 Q: Where can I find Microsoft Exchange Server 2007 product documentation?

A: You can find Exchange Server 2007 product documentation on the [Exchange Server 2007 Technical Library](#) Web site, on the Start menu, or by clicking F1 within the product after it has been installed. You can also access product documentation from the [Microsoft Exchange Server TechCenter](#). You can visit the [Exchange Server Community](#) Web site or the [Exchange Team Blog](#) Web site for additional product information, common issues, and troubleshooting assistance.

5.0 Q: What are the Exchange Server 2007 licensing options?

A: Customers can purchase the Exchange Enterprise Client Access License (CAL) or the Exchange Standard CAL. The Exchange Enterprise CAL is sold as an add-on to the Exchange Standard CAL. Two server editions will continue to be offered: Exchange Server Enterprise Edition and Exchange Server Standard Edition. You can run either CAL together with either server edition. For more information about Exchange Server 2007 editions and Client Access Licenses, see [Exchange Server 2007 Editions and Client Access Licenses](#).

6.0 Q: What do I get with the Exchange Enterprise CAL vs. the Exchange Standard CAL?

A: In addition to the improvements and new capabilities that are available with the Exchange Standard CAL, the Exchange Enterprise CAL includes Unified Messaging, advanced compliance capabilities, and on-premises and hosted antivirus and anti-spam protection. For more information about Exchange Server 2007 editions and Client Access Licenses, see [Exchange Server 2007 Editions and Client Access Licenses](#).

7.0 Q: What are the different editions of Exchange Server 2007?

A: Exchange Server 2007 is offered in two server editions: Standard Edition and Enterprise Edition. Exchange Server 2007 Standard Edition is designed to meet the messaging and collaboration needs of small and medium organizations. It may also be appropriate for specific server roles or branch offices. Exchange Server 2007 Enterprise Edition, designed for large enterprise organizations, enables the creation of multiple storage groups and databases. For more information about Exchange Server 2007 editions and Client Access Licenses, see [Exchange Server 2007 Editions and Client Access Licenses](#).

Hardware and Software Requirements

8.0 Q: Will I have to buy new hardware to run Exchange Server 2007?

A: If you are running 64-bit hardware in your current messaging environment, you may not have to buy additional hardware. However, Exchange 2007 does require hardware and an operating system that are 64-bit. 64-bit hardware provides the system

architecture that is required to support the increased memory, storage, and enhanced security requirements in a more cost-effective manner. For more information about how to select the hardware for Exchange 2007, see [How to choose server hardware for Exchange Server 2003 that can be effectively re-used for Exchange 2007](#).

9.0 Q: Which 64-bit processors are supported by Exchange Server 2007?

A: Exchange Server 2007 supports servers that have "x64" processors. Most new servers include processors from Intel and AMD that provide this x64 support. The Intel processors are called Intel Extended Memory 64 Technology (EM64T), and the AMD processors are called AMD64. Exchange Server 2007 does not support Itanium (IA-64) processors.

10.0 Q: Should servers that are running Active Directory domain controllers and the global catalog be upgraded to 64-bit?

A: For the best performance, when an Active Directory organization contains more than 20,000 objects, you should upgrade to 64-bit. Upgrading servers that run Active Directory domain controllers and the global catalog to 64-bit improves the overall performance and scalability of your Exchange Server 2007 environment. However, 32-bit domain controllers are still supported.

Lookup and response times between the Exchange 2007 categorizer and the Active Directory directory service will improve with the use of 64-bit. The size of the Extensible Storage Engine (ESE) database that holds Active Directory can frequently be larger than 3.0 gigabytes (GB). This prevents caching of the contents of the whole database, and therefore increases lookup and response times. By using 64-bit, the available RAM for caching can be increased beyond 4.0 GB. This is large enough to cache the whole ESE database, even for large Active Directory organizations, and will improve Exchange 2007 lookup and response times.

11.0 Q: Will I need the 64-bit version of Windows Server 2003 to run Exchange Server 2007?

A: You will need the 64-bit version of Windows Server 2003 or Windows Server 2003 R2 to deploy Exchange 2007. Volume licensing customers can exchange their 32-bit version of Windows Server 2003 for the 64-bit version any time by using their media kits.

12.0 Q: How can I upgrade my current Exchange 2000 Server or Exchange Server 2003 environment?

A: When you upgrade to Exchange Server 2007, you cannot perform an in-place server upgrade on an existing Exchange server. Instead, you must install a new Exchange 2007 server into the existing organization, and then move the required data to the new Exchange server. Exchange Server 2007 supports mixed environments that include Exchange 2000 Server, Exchange Server 2003, or both. This allows for an easier and more gradual transition. For more information about how to plan and deploy Exchange Server 2007, see the [Microsoft Exchange Server 2007](#) product documentation.

Active Directory

13.0 Q: Should I map my current routing groups to my current Active Directory sites?

A: Yes. Exchange 2007 is based on Active Directory sites. If your current Microsoft Exchange environment maps as closely as possible to Active Directory sites, your interoperability and migration story will be easier. Additionally, the recommended upgrade path is to upgrade all the Exchange 2000 Server or Exchange Server 2003 servers in a single routing group before you upgrade the next routing group. This lets you fully decommission a routing group as you upgrade and reduces the complexity of your current routing topology. Mapping the Exchange 2000 Server or Exchange Server 2003 routing groups to the Exchange 2007 physical topology also makes it easier to plan for an upgrade to Exchange 2007 because the two environments are similarly organized and generally correlate to Active Directory sites.

14.0 Q: Should I create a dedicated Active Directory site for Exchange Server 2007?

A: You can deploy Exchange Server 2007 directly into your organization's existing Active Directory topology. For many organizations, deploying directly into the existing Active Directory topology greatly simplifies the overall management of the Exchange 2007 deployment. However, given the extensive access to domain controllers and global catalog servers that is required by Exchange 2007, you may decide to create dedicated sites for your organization. You might want a dedicated site if other applications in your organization must access Active Directory domain controllers and the global catalog server.

15.0 Q: Why do I have to disable link state routing?

A: Link state routing must be disabled whenever two or more routing groups are configured to send or receive mail from an Exchange 2007 computer that has the Hub Transport server role installed. (The Hub Transport server was formerly known as a

bridgehead server). This is because Exchange 2007 uses Active Directory to determine routing topology. The Exchange 2007 servers do not propagate link state updates. If link state routing is enabled and there is more than one routing group configured to send mail to or from an Exchange 2007 Hub Transport server, routing loops might occur.

16.0 Q: Why are routing groups not used in Exchange Server 2007?

A: Exchange 2007 uses Active Directory sites to replace routing groups. Using Active Directory is more efficient because it allows for site awareness and eliminates the requirement to create and maintain a routing topology that is separate from an organization's physical topology.

Exchange 2007 Server Roles

17.0 Q: Can the Exchange 2007 server roles be deployed and configured on the same physical hardware?

A: Because Exchange 2007 is role-based, you can deploy all Exchange Server 2007 server roles, except the Edge Transport server role on a single physical server. If you are clustering, you cannot deploy the Mailbox server role on the same server as the Client Access, Unified Messaging, Hub Transport, or Edge Transport server roles. When the server roles are installed on the same or shared hardware, they function as separate entities.

18.0 Q: Why must I deploy an Exchange 2007 server that has the Client Access server role installed in every Active Directory site that contains user mailboxes?

A: Installing the Client Access server role in every Active Directory site that contains user mailboxes reduces the use of corporate bandwidth by redirecting the connection to the Client Access server that is in the same Active Directory site in which the user's mailbox is contained.

19.0 Q: What if the Client Access server role is not available from the Internet?

A: You can disable redirection for the Client Access server. The Internet-accessible Client Access server will act as an HTTP proxy to the Client Access server that is located in the same site as the user's mailbox.

20.0 Q: Why must I deploy an Exchange 2007 server that has the Hub Transport server role installed in the same Active Directory site in which I deployed an Exchange 2007 server that has the Unified Messaging (UM) server role installed?

A: Unified Messaging servers submit voice mail and fax messages to a Hub Transport server by using SMTP. This can occur only if they are deployed in the same Active Directory site.

21.0 Q: Why must I deploy an Exchange 2007 server that has the Client Access server role installed in the same Active Directory site in which I deployed an Exchange 2007 server that has the Unified Messaging server role installed?

A: Unified Messaging Web services that run on the Client Access server enable full client functionality for UM-enabled users. Additionally, installing and configuring a Client Access server in the same site as the Unified Messaging servers reduces the bandwidth that is required if they are deployed in separate Active Directory sites.

22.0 Q: What is the Autodiscover service?

A: The Autodiscover service gathers the required configuration information in Active Directory to enable Outlook 2007, Office Outlook Web Access, and mobile e-mail clients to efficiently locate and connect to the appropriate Exchange 2007 Mailbox server that contains the user's mailbox. The Autodiscover service is also used to make configuring Outlook 2007 clients easier and to provision mobile devices that are used to connect to Exchange 2007. By default, the Autodiscover service is enabled.

Exchange 2007 Management

23.0 Q: Can I manage Exchange Server 2003 or Exchange 2000 Server by using Exchange Server 2007 management interfaces?

A: No. All administration of Exchange Server 2007 must be done by using the Exchange Management Console or the Exchange Management Shell. All administration of Exchange 2000 Server or Exchange Server 2003 must be done by using their respective administrative interfaces. The one exception to this rule is that you can use Exchange System Manager found in Exchange Server 2003 to perform most Exchange Server 2007 public folder administrative tasks.

24.0 Q: What is happening with public folders?

A: Public folders are similar to mailbox stores, but the information within a public folder store is contained within a dedicated database. Exchange 2007 de-emphasizes public folders. Public folders may not be included in future releases, but support for public folders will be maintained through at least 2016. Current Microsoft Exchange customers should plan to migrate to Outlook 2007 and Exchange 2007. We recommend that you investigate integrating Microsoft Windows SharePoint Services with Exchange Server 2007 if you must have an application that supports sharing documents, calendar items, contacts, and tasks and archiving distribution lists. For other customized applications that are being developed, you should use Microsoft .NET. For more information about public folders, see the [Exchange 2007 and Public Folders](#) blog.

Tell me a bit about the capabilities of Exchange Server.

- 1) Outlook Anywhere (OWA)
- 2) Mailbox Can sync with Blackberry Device.
- 3) Calender Shairing.
- 4) MAPI & POP3 Client support.

Exchange Server 2003 (v6.5) debuted on [September 28, 2003](#). Exchange Server 2003 (currently at [Service Pack 2](#)) can be run on [Windows 2000 Server](#) (only if [Service Pack 4](#) is first installed) and [32-bit Windows Server 2003](#), although some new features only work with the latter. Like Windows Server 2003, Exchange Server 2003 has many compatibility modes to allow users to slowly migrate to the new system. This is useful in large companies with distributed Exchange Server environments who cannot afford the downtime and expense that comes with a complete migration.

One of the new features in Exchange Server 2003 is enhanced disaster recovery which allows administrators to bring the server online quicker. This is done by allowing the server to send and receive mail while the message stores are being recovered from backup. Some features previously available in the Microsoft [Mobile Information Server](#) 2001/2002 products have been added to the core Exchange Server product, like [Outlook Mobile Access](#) and server-side [ActiveSync](#), while the Mobile Information Server product itself has been dropped. Better anti-virus and anti-spam protection have also been added, both by providing built-in APIs that facilitate filtering software and built-in support for the basic methods of originating IP address, [SPF](#) ("Sender ID"), and [DNSBL](#) filtering which were standard on other open source and [*nix](#)-based mail servers. Also new is the ability to drop inbound e-mail before being fully processed, thus preventing delays in the message routing system. There are also improved message and mailbox management tools, which allow administrators to execute common chores more quickly. Others, such as Instant Messaging and Exchange Conferencing Server have been extracted completely in order to form separate products. Microsoft now appears to be positioning a combination of [Microsoft Office](#), [Microsoft Office Live Communications Server](#), [Live Meeting](#) and [Sharepoint](#) as its collaboration software of choice. Exchange Server is now to be simply e-mail and calendaring.

What are the different Exchange 2003 versions?

Go to your server in Exchange System Manager, right-click your server, choose Properties, and on the General tab make a note of the version number.

Each version of Exchange Server includes a build number so that you can easily identify which version of the product you are running:

6944.4 = Exchange 2003 RTM (including SBS2003)

7226.6 = Exchange 2003 SP1

7638.2 = Exchange 2003 SP2

features are available in Exchange 2007 SP1:

The following new features for high availability and improvements to existing high availability features are available in Exchange 2007 SP1:

- Standby continuous replication (SCR)
- Support for the following features in Windows Server 2008:
 - Multiple subnet failover clusters
 - Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4)
 - IPv6
 - Exchange and failover cluster network configuration
 - New quorum models (disk and file share witness)
- Continuous replication (log shipping and seeding) over a redundant cluster network in a cluster continuous replication (CCR) environment
- Reporting and monitoring improvements
- Performance improvements
- Transport dumpster improvements
- Exchange Management Console improvements

Exchange Server 2003

(v6.5) debuted on [September 28, 2003](#). Exchange Server 2003 (currently at [Service Pack 2](#)) can be run on [Windows 2000 Server](#) (only if [Service Pack 4](#) is first installed) and [32-bit Windows Server 2003](#), although some new features only work with the latter. Like Windows Server 2003, Exchange Server 2003 has many compatibility modes to allow users to slowly migrate to the new system. This is useful in large companies with distributed Exchange Server environments who cannot afford the downtime and expense that comes with a complete migration.

One of the new features in Exchange Server 2003 is enhanced disaster recovery which allows administrators to bring the server online quicker. This is done by allowing the server to send and receive mail while the message stores are being recovered from backup. Some features previously available in the Microsoft [Mobile Information Server](#) 2001/2002 products have been added to the core Exchange Server product, like [Outlook Mobile Access](#) and server-side [ActiveSync](#), while the Mobile Information Server product itself has been dropped. Better anti-virus and anti-spam protection have also been added, both by providing built-in APIs that facilitate filtering software and built-in support for the basic methods of originating IP address, [SPF](#) ("Sender ID"), and [DNSBL](#) filtering which were standard on other open source and [*nix](#)-based mail servers. Also new is the ability to drop inbound e-mail before being fully processed, thus preventing delays in the message routing system. There are also improved message and mailbox management tools, which allow administrators to execute common chores more quickly. Others, such as Instant Messaging and Exchange Conferencing Server have been extracted completely in order to form separate products. Microsoft now appears to be positioning a combination of [Microsoft Office](#), [Microsoft Office Live Communications Server](#), [Live Meeting](#) and [Sharepoint](#) as its collaboration software of choice. Exchange Server is now to be simply e-mail and calendaring.

Exchange 2003 provides improved functionality in the following areas:

- Routing
- Support for Volume Shadow Copy service
- Support for Outlook 2003 Cached Exchange Mode
- Outlook Web Access for Exchange 2003

- Mobile Device Support for Exchange 2003
-

Checklist for Evaluating Your Current Environment

The following checklist outlines the physical and logical factors you should take into consideration when assessing your current environment before deploying Exchange.

Physical plant	
	Data center floor space
	Rack space
	Network sizing
	WAN (may need to provision higher bandwidth connections)
	Degree of separation between physical sites (latency introduced)
	LAN upgrades
	Backbone
	Modem pools or alternate dial-up
	Hardware needs
	Servers
	Memory
	Processor
	Storage
	High bandwidth network interface cards (NICs)
	Routers
	Memory
	Processor
	Switches
	Firewalls
	Power
	Power grid Service Level Agreement (SLA)
	Projected power draw
	Uninterruptible power supply (UPS) or other power-insulating device (generators, etc.)
	Designated "hot" site
Staffing	
	Training on newly introduced technologies and procedures
	Augmentation
	Administrators
	Support staff
Geography	
	Time zone issues
	Languages

WAN	
	Encapsulation upgrade (asynchronous transfer mode [ATM], etc.)
	Optimization (permanent virtual circuit [PVC] for frame relay)
	Overall quality of connections
LAN	
	Encapsulation change (token ring to Ethernet)
	Layer 2 device removal or upgrade
Network	
	TCP/IP end-to-end
	IP Hop count between endpoints
	Subnetting considerations (Microsoft® Active Directory® directory service site considerations)
	Device configuration
	Routers and open ports
	Switches
	Firewalls and open ports
	Ports and layer 4 protocols enabled on filtering or blocking devices
	All encryption and decryption operations
	All format-change operations (for example, other mail gateways and X.400 connectors)
	remote procedure call (RPC) connectivity
	network basic input/output system (NetBIOS)
	Public key infrastructure (PKI)
	Virtual private network (VPN)
	Shared dependencies between Internet Information Services (IIS), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP)
	DNS
	Windows® Internet Name Service (WINS)
Network operating system	
	Shared dependencies between DHCP, NTLM, NTLMv2, and LM
	Windows NT® Server version 4.0 domain structure: Trusts, primary domain controllers, backup domain controllers
	Windows 2000 Server or Windows Server™ 2003 Active Directory
	Forest structure
	Domain structure
	Migration
	Site structure
Security	
	Kerberos
	Migration
	Security principles
	Security identifier (SID) history

	Directories
	Migration
	Active Directory Connector
	Meta directories
	Administration
	Migration
	Permissions delegation
	Management

What are the major network infrastructure for installing Exchange 2003? What is the

Windows 2003's role in the Exchange 2003 installation

Before breaking out the Exchange CDs and actually installing Exchange 2003, you must decide your strategy and tactics. If you have not done this see [\(Check Exchange Migration Strategy here\)](#)

You may already realise that Exchange 2003 needs to extend the Active Directory schema. This makes sense when you realize that a mailbox is now an attribute of the user, hence the user object needs extra attributes which translate to tabs in the user property sheets. Best to install Exchange 2003 in an Windows Server 2003 domain, rather than a Windows 2000 domain. [\(Check Exchange Compatibility here\)](#)

If you are migrating from Exchange 5.5 to Exchange Server 2003, then remember that the old Exchange 5.5 has its own directory database (Dir.edb). As a pre-requisite to installing Exchange 2003, this account information must be transferred to Windows 2003's Active Directory. Incidentally, Exchange 2003 also relies on Windows 2003 for IIS, account security, Event Viewer and the SMTP service.



Exchange 2003 Dependencies

Exchange Server 2003 Requires the following Windows 200x services

- .NET Framework
- ASP.NET
- Internet Information Services (IIS)
- World Wide Web Publishing Service
- Simple Mail Transfer Protocol (SMTP) service
- Network News Transfer Protocol (NNTP) service

For security reasons in Windows 2003 IIS is locked down, so not only make sure that you install the services, but also that the corresponding services are set to Automatic. Finally start the service.

Beware - the two Editions of Exchange 2003

Just like its predecessors, Exchange 2003 comes in two editions. Always choose the Enterprise edition because it has no limit on the mail Store database. The standard edition should come with a warning that the 16 GB limit will be insufficient for all but the smallest organization.

As a consultant, I have had several assignments helping people when they reach the 16 GB limit. Whilst each job gave me work, I had this feeling that the problem should have been avoided, that Microsoft should place a warning on that Standard Edition - 'Beware you will be in trouble when you hit the 16 GB store limit'.

The Enterprise edition also supports multiple mailbox stores which means that you can have different backup strategies for different users. Naturally, you would need the Enterprise version of Exchange and Windows if you wished to create a cluster of Exchange servers.



Get a test machine to install Exchange 2003, then you can practice with its quirky setup interface.

Install Exchange Server 2003 in stages:

- a) Setup /forestprep
- b) Setup /domainprep
- c) Finally plain: setup

If you are new to Exchange 200x, a further difficulty is that the setup menu is quirky. Exchange has several strange drop down menus which are not seen in other Microsoft setup programs. However, once you run this setup menu a few times, you begin to understand how its mind works and configuration becomes easier.

There are two reasons why you may want to install Exchange 2003 in stages, security and the time it takes to run the first full setup. The adage: 'The more security you have the more work there will be', applies here. To install Exchange 2003 you must be not only an Administrator, but also a member of the Enterprise Admins and Schema Admins. Incidentally, consider creating a special domain account which will be used in installation, and then this account will become the first Exchange 'Full Administrator'.

What setup /forestprep does is create the Exchange Organisation name in Active Directory. So be very careful with this Organization name as you cannot change your mind later. In addition /forestprep extends the schema and modifies the users attributes to include a mailbox. In practical terms, this means that 4 new tabs will appear on the User's property sheet as viewed in Active Directory Users and Computers.



Make sure that you run /forestprep on the domain controller which is also the schema master and preferably a Global Catalog server.

Setup /domainprep creates two new security groups: Exchange Domain Servers and Exchange Enterprise Servers. You can inspect the new groups in the USERS folder of Active Directory Users and Computers. /domainprep also creates the Exchange System Objects container in Active Directory.

The other benefit of running /forestprep and /domainprep switches early in the deployment is that it will save time later; allowing ordinary administrators to install the Exchange binary files more quickly.

Now would be the time to run Exchange 2003's setup and install the binary files. Once that's completed verify the installation by checking the services, and if it were me I would be desperately keen to send my first email in my new Exchange Organization.

Unattended Install

If you have lots of servers to install, and you distrust Ghost for such an important job, you could try creating an unattended 'Answer' file by using setup /createunattend on the first, perfectly installed server. Then, use the /unattendfile switch when installing the other Exchange 2003 servers. For more details try setup /? at the command prompt.



Remember that the Strategy is Co-existence

Keep in mind that your strategy for this phase of the migration is co-existence between Exchange 5.5 and a new Exchange 2003 server. Temporarily, both generations of Exchange will be in the same site of the same organization. Eventually, you will decommission the Exchange 5.5 servers but for now both servers will be active and communicating. Remember that even if you wanted to, it is not possible to make an in-place upgrade of the Exchange 5.5 servers to Exchange 2003.

When you run setup on the Exchange 2003 server, you will need the name of an existing Exchange 5.5 server as well as the NT 4.0 service account name and password. A final complication is that you may need to be an administrator in the NT 4.0 domain and this may involve creating trusts and adding the Active Directory installation account to the NT 4.0 Administrators Local Group.



Read all menus and error messages - extra c a r e f u l l y.

Troubleshooting Installation of Exchange Server 2003

- Made sure you have enough Disk Space
- Check the Edition of Exchange Server (Enterprise is best)
- Check Active Directory, a user's property sheet is a good place to start.
- Check DNS.
- LDAP port 389 in use, so cannot connect to Exchange 5.5. Solution change and synchronise port numbers.
- If installation fails make sure you delete EXCHSRV\mbdata before trying again.
- Why does no-one ever check the Event Viewer? If there is a problem you will see a red error dot in the logs. Remember to check the Application log as well as the System log. If the messages are not self explanatory, look up the error number in TechNet.
- Check that ALL the IIS components are installed including SMTP and NNTP. Make sure that ASP.NET and .NET Framework are also installed.
- Run DCDiag or NetDiag for extra clues as to what is wrong with the server. [See more on DCDiag](#)

Introduction to Installing Exchange Server 2007

All installations reward planning; in the case of Exchange 2007, decide on the underlying operating system and then decide which Exchange roles to install. What makes setting up Exchange 2007 such a joy is the way the wizard helps you check the pre-requisites. For example, it prompts you to raise the domain level, and shows you the way to install .Net Framework 2.0

The trickiest feature of Exchange 2007 is not the installation, but the new method of creating Mailboxes from the Exchange manager. In Exchange 2007, creating mailboxes (mailbox enabled users) with Active Directory Users and Computers is fool's gold. Any objects you manage to create have no SMTP address and don't work. You simply must use the Exchange Management Console to create mailboxes.

1.1.1 Choose your Underlying Operating System

Before you install Exchange Server 2007, you need a 64-bit operating system; I choose the Windows Server 2003 R2 rather than the minimum requirement of Windows Server 2003 with SP1.

An even better option would be to install Exchange Server 2007 SP1 on Windows Server 2008, but note those three letters: SP1. Just to emphasise that for Server 2008 you need the later, slipstreamed SP1 DVD (or image), and not the original RTM disk. Furthermore, you need a clean install of Windows Server 2008 on 64-bit hardware, and not an upgrade from W2K3.

In terms of tactics, Microsoft recommend that you install Exchange 2007 on member server. Exchange on a Domain Controller is not supported, and should only be used for testing where you only have one machine. If you have already prepared your domain, then jump to [Key preparation steps](#)

1.1.2 Active Directory

Creating the Active Directory domain is not strictly a part of installing Exchange, I added here below a brief description of the most important features for the sake of completeness.

Domain Functional Level

The [Domain Function Level](#) must be at least - Windows 2000 Server Native. Fortunately, this is not a great burden as there is only one lower setting, 2000 Mixed. This is a reminder that Exchange Server 2007 has severed the umbilical cord to Exchange 5.5. Thus all those old 5.5 servers must be decommissioned and removed if you are migrating an existing organization to Exchange Server 2007.

You also need to check the Forest Functional Level, particularly where you want the advanced features of Exchange 2007. Incidentally, Functional Level is my one of my 'Litmus tests' for seeing if people have sufficient Active Directory knowledge to install Exchange 2007. If someone does not know how to find and configure Function Levels, then they are likely to need help installing Exchange 2007.

Global Catalog

Every active directory site where you install Exchange Server 2007 needs at least one Global Catalog server. As you may know, GC is a configurable role of every domain controller.

System Icon - DNS Domain Configuration

A trivial task, I appended the fully qualified domain name to the hostname. What I did was open the System Icon, Computer Name (Tab), click on the Change button.

As with Exchange 200x, the mail server relies on Active Directory. Therefore, I installed a Windows Server 2003 (RC2) member server then ran DCPROMO, from there I followed the wizard's prompting to create a new domain in a new forest.

DNS - Automatic addition of _SRV

When I installed my active directory domain, the plan was to persuade DCPROMO to install DNS using the wizard to automatically add all the _SRV records. To succeed, at the menu below, I selected the middle (automatic) option, Install and configure DNS server on this computer.

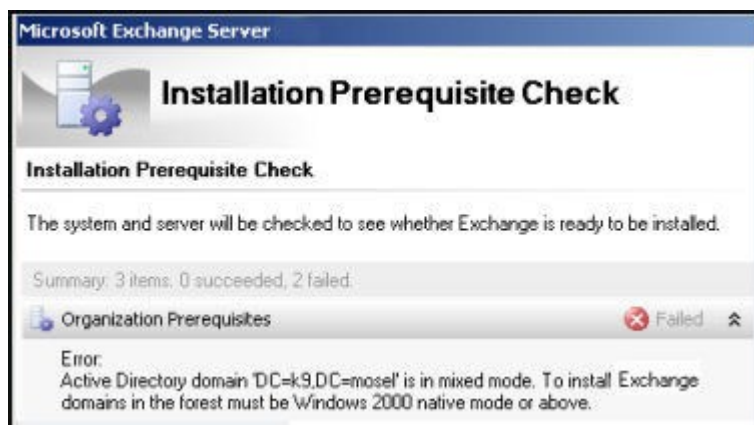


I was taken aback to get an error message, however, I allowed the DCPROMO to finish, then I went to the Services and Stopped then restarted the Netlogon Service. What followed was a magic moment, restarting the Netlogon Service triggered the creation of all the DNS records under _msdcs.

The bottom line is check that DNS has the 'A' Host record for each Exchange 2007 server.

1.1.3 Key preparation steps before you install Exchange 2007:

At every stage of installing Exchange 2007, kind friendly wizards guide you through the minefield. Here is a screen shot of the wizard checking then explaining a problem with mixed mode.



Raise Domain Level

As indicated by the wizard, I needed to Raise Domain Level 2003 (2000). What I did was launch the ADUC (Active Directory Users and Computers), right click on your domain and select, Raise Domain Function Level. As I had no old domain controllers, I chose Windows Server 2003.

Global Catalog

I would like to give a timely reminder of the importance of Global Catalog to Exchange. Insure that at least one Domain Controller on the subnet where you install Exchange 2007 has Global Catalog enabled.

.Net Framework 2.0

Exchange 2007 requires .Net Framework 2.0 (or 3.0). We need to install PowerShell before the main Exchange 2007. This is an indication of the importance of the new PowerShell / PowerShell cmdlets.

MMC v 3.0

One minor surprise, was that when I installed on Windows Server 2003, Exchange 2007 needs MMC v 3.0.

PowerShell

Once you start using Exchange Server 2007 it won't belong before you meet PowerShell. It follows therefore, that you have to add it as a 'Feature' of Windows Server 2008, else, on Windows Server 2003 install PowerShell together with .Net Framework by downloading the files from Microsoft's site.

64-bit Hardware

Production versions of Exchange 2007 require 64-bit hardware. Don't be lulled by 32-bit beta versions of Exchange 2007, they are only for testing, and for a specific preparation context. That context is to prepare Active Directory and domains for Exchange 2007 from a computer that has a 32-bit processor. Remember that Exchange 2007 will be the first Microsoft product which runs solely on 64-bit processors.

Other than this processor requirement, just use common sense and provide plenty of RAM. It's also worth spending a few minutes thought and planning on the disks sizes and partitions, particularly servers hosting the Mailbox Role. For larger organization, this would be a good time to review your SAN (Storage Area Network) needs.

No NNTP

Finally, avoid 'over-think', you do not, repeat, not need the NNTP service. The good news is that the wizard coupled with the result pane not only alerts you to the problem, but also suggests a remedy.

1.1.4 Installation Switches to Prepare Active Directory

Prerequisites, you need the Exchange Server 2007 disk or image. (SP1 would be even better) Each command is prefaced by setup. You could also try setup /? to see the full list of options, for example: /mode or /role.

Setup /PrepareAD Creates the necessary global Exchange objects and universal security groups in Active Directory. Must be run by a member of the Enterprise Admins group, run this command in both the root and current domain. You may find that if you run this command as a Schema Admin (and Enterprise Admin), there is no need to run the other commands.

/PrepareLegacyExchangePermissions This command is needed if your organization contains Exchange Server 2003 or 2000 computers. It modifies the permissions assigned to the Enterprise Exchange Servers group so that the Recipient Update Service can run. Remember to logon as a member of the Enterprise Admins group.

/PrepareSchema This prepares the Active Directory schema so that it allows Exchange Server 2007 to install. You must be a member of both the Schema Admins and Enterprise Admins. You need to run this command in the root domain, or the domain which holds the Schema Master role.

/PrepareDomain /PrepareDomain:domainname This creates a new global group in the Microsoft Exchange System Objects container called Exchange. You must be a member of both the Enterprise Admins and the Domain Admins group.

One more point, if you are using a Windows Server 2008 computer, first install the AD DS management tools.

1.1.5 Finalize Deployment Tab

Once the Exchange setup wizard finishes its tasks, there is yet more work for you. Seek out the Finalize Deployment tab, and also the End-to-End Scenarios tab.

Launch the Exchange Management Console, select Microsoft Exchange in the left tree, and now you should see the 'Finalize Deployment tab'. Most of these configuration tasks are optional, and will vary depending on which Server Role(s) you added. However, I bet that there will be at least two items that you had forgotten or not previously considered changing.

While you have the Management Console open, take the chance to investigate the End-to-End Scenarios tab. As with the previous tab, these tasks are optional and vary depending on which Exchange 2007 features you added.

1.1.6 Verification Check List

- Check the installation log at: C:\ExchangeSetupLogs. Also check the system and application event logs.
- Launch the Exchange Management Console and check your newly installed Exchange server. If this is a brand new installation check that the Organization Name is the same as you planned.
- Create a mail-enabled user and then connect to that mailbox using Outlook Web Access, or an Outlook client if you prefer.
- Once you create a Hub Server see if you can receive email from another mail-enabled account.
- For CAS servers make sure you check with OWA.
- In the case of the Edge Server send email to an external internet account.
- Check that services to see that the dozen or so Microsoft Exchange Services are running. Note they begin with Microsoft and not Exchange.
- If anything seems wrong check the Exchange files underneath: C:\Program Files\Microsoft\Exchange Server.
- When there is no quick resolution to the problem, seek the [ExBPA](#) (Exchange Server Best Practices Analyzer), then run the Exchange 2007 Readiness check. The best way is to launch the Exchange Management Console and open the Toolbox and there you will find the Exchange Server Best Practices Analyser.



1.1.7 Exchange 2007 Roles

Once I completed all the preparatory steps, I was ready for the main Exchange 2007 installation. All that remained was to decide upon the role or roles for your exchange server. As expected, you can always return to this menu to add more roles.

1.1.8 Additional Requirements for the Various Roles



Mailbox Server

This back-end server needs IIS and WWW.

Client Access Server (CAS)

The CAS server also requires ASP.Net and the WWW service. Remember that this should be the first role to implement for Exchange Server 2007. [See more on CAS](#)

Unified Messaging Server

Needs speechify. No worries, setup will automatically install as needed. This Unified Messaging role provides integration for email, calendars, voicemail and if you still use it, fax.

Bridgehead Server

No special requirements

Edge Transport Server

The Edge Transport Server (Formerly Gateway Server) must be in it's own workgroup. Just will not operate in a Domain for the obvious reason of security.

The role of Edge Transport server is to accept messages from the internet that come are addressed to your Exchange 2007 organization. After these emails are processed, the Edge server routes them to the Hub Transport servers inside your organization.

Client Requirements

Mapi clients need Outlook 2002 or later. Outlook 2007 is by far the best client. Outlook 2007 and Exchange 2007 are made for one another. [OWA \(Outlook Web Access\)](#) is a great alternative all clients need is a browser.

1.1.9 Troubleshooting Exchange 2007 SP1 Installation Problems

Problem: Public Folder Replicas

Solution: Temporarily disable the OAB, then delete the replicas or move them to another Exchange server. This task is ideal for PowerShell:

The cmdlets are

```
get-PublicFolderStatistics Check the situation
```

```
get-PublicFolder
```

```
remove-PublicFolder Dangerous if you don't know what you are doing, effective if you do.
```

```
Get-PublicFolderStatistics -Server <YourExchangeServer> | fl
```

```
Get-PublicFolder -Server <server containing the public folder database> "*" -Recurse -ResultSize:Unlimited | Remove-PublicFolder -Server <server containing the public folder database> -Recurse -ErrorAction:SilentlyContinue
```

```
Get-PublicFolder -Server <server containing the public folder database> "Non_Ipm_Subtree" -Recurse -ResultSize:Unlimited | Remove-PublicFolder -Server <server containing the public folder database> -Recurse -ErrorAction:SilentlyContinue
```

Problem: Email Address Policy

Solution: Check the Exchangesetup.log for this message:

```
[ERROR]The Exchange server Address list failed to respond- error 0x8004010f
```

Next launch the Event Viewer and check the Application log (not the system log) for Event ID: 8325. If you examine the details it will tell you precise Filter Rule that is preventing installation.

This problem occurs when you add the Mailbox role to Exchange 2007. The root cause was an incorrect filter was created in Exchange 2003.

Problem: Existing object in Active Directory

[ERROR] Active Directory operation failed on DC.YourDom.com The object 'CN=Default Global Address List,CN=All Global Address List

Solution: Launch ADSI Edit and investigate the Address Lists Container, in particular, edit the purportedSeach attribute.

Problem: DNS

Example: Unable to connect to 'YourDC' DC No Exchange Server with identity 'YourServer' was found

Solution: Check with Netdiag and Dcdiag. With luck it could just be a latency, or initial connection problem, which mysteriously disappears when you try to repeat the Exchange 2007 server install.

Problem: Windows 2000 Domain Controllers

Solution: Upgrade to Windows Server 2003. Or install a Windows Server 2003 in that child domain or site.

Problem: ADC (Active Directory Connectors)

Remove (uninstall) the ADC on the Windows 2003 servers before continuing with Exchange 2007 server install.

Problem: CAS server setup fails with a Watson MultiValuedProperty error

Solution: Launch ADSI Edit check Default Offline Address List. In particular, set the value of the MsExchVersion attribute to 4535486012416

Problem: Disabled IPv6

Windows Server 2008. Problem installation failed. Reason, I had foolishly disabled IPv6. Solution, give the NIC and IPv6 address. Extra information, I had checked the install Hub Transport role, whether this was relevant, I have not had time to research.

1.1.10 General Features of Microsoft Exchange Server 2007 SP1

I am guessing, but service pack 1's feature list looks as though Microsoft has engaged their top project manager to oversee SP1. It seems as though he has listened to customer feedback from the RTM version, trawled forums, and sat down with the Exchange 2007 team and asked, 'What could we have done better?' Then the project manager produced a list of improvements and enhancements to be delivered in SP1. This procedure is typical of service pack ones, a welcome but unspectacular list of improvements. It is only later in the development cycle when SP3 or SP4 tend to introduce brand new features.

To my way of thinking, Exchange Server 2007 SP1 will always be the 'Longhorn service pack'. Other benefits of running Exchange 2007 on Windows Server 2008 include, support for IPv6, and for high availability, Standby Continuous Replication (SCR).



1.1.11 OWA (Outlook Web Access)

OWA continues to improve as it matures as a technology. The highlights of SP1's enhancements are:

- Recover deleted items through Outlook Web Access.
- Users can create their own Personal Distribution Lists
- Users can copy folders and individual items
- Support for Public Folders through the /owa virtual directory
- For secure email there is now S/MIME
- Improved delegation so that others can access some of your folders - watch out for the Delegation Wizard

1.1.12 Improvements for the Unified Messaging Server Role

Again it is the emerging, maturing technologies that require the most tweaking, making clunky components in the RTM version work smoothly in SP1. Unified Message enhancements include:

- The ability to record high-fidelity voice messages in Exchange Unified Messaging
- Integration of missed call notification e-mail messages with Office Communicator 2007
- Users can now open their Outlook Voice Access from Microsoft Office Communicator 2007 without needing a PIN
- QoS (Quality of service) support

- You can configure Unified Messaging to use the Secure Realtime Transport Protocol (SRTP)

1.1.13 Message Transport

SP1 adds more settings to the Exchange Management Console (Formerly the Exchange System Manager), for example the ability to set additional message limits on connectors. Speaking of the Exchange Management Console, Microsoft have added new features in many areas. It's as though they pruned back too far when they reduced Exchange 2003's seven levels, to three levels in Exchange Server 2007. Now with SP1 features that were not ready or settings that were overlooked have been introduced.

One welcome new feature is the ability to import and export .pst files. Indeed, Microsoft have revamped the Move Mailbox tool to make migrations and transitions to Exchange Server 2007 that bit easier.

1.1.14 Problems with Exchange Server 2007 SP1

The bad news with every service pack these days is that it inadvertently introduces a few, often obscure problems. The good news is that there is an Update Rollup 1 to fix such problems for Exchange Server 2007 SP1. Here are some of the problems that the Rollup 1 fixes:

- The Autodiscover service fails in Outlook 2007 after you install Exchange Server 2007 Service Pack 1.
- Sundry garbled OWA messages in 'Subject' field, especially the '?'.
 - The Store.exe process hogs the CPU. You may also get: these Event IDs 9659, 8206, 8213, or 8199 in the log.
- The Microsoft Exchange Information Store service hangs.
- Email messages get stuck in the submission queue.
- An external NDR message is sent to all recipients on a distribution list.
- An application cannot run Windows PowerShell commands by impersonating a user account.
- Beware, SP1 resets Connector Receive MaxMessageSize to 10 MB.

latest Exchange 2003 Service Pack? Name a few changes in functionality in that SP.

Microsoft® Exchange Server 2003 builds on the Microsoft Exchange 2000 Server code base, providing many new features and improvements in areas such as reliability, manageability, and security.

Exchange Server 2003 is the first Exchange release designed to work with Microsoft Windows Server™ 2003. Running Exchange 2003 on Windows Server 2003 provides several benefits, such as improved memory allocation, reduced Microsoft Active Directory® directory service replication traffic, and rollback of Active Directory changes. Running Exchange 2003 on Windows Server 2003 also allows you to take advantage of new features, such as the Volume Shadow Copy service and cross-forest Kerberos authentication. Exchange 2003 also runs on Microsoft Windows® 2000 Server Service Pack 3 (SP3) or later.

Exchange 2003 works with Microsoft Office Outlook® 2003 to provide a range of improvements, such as cached mode synchronization, client-side performance monitoring, and support for RPC over HTTP (which allows users to connect directly to their Exchange server over the Internet without needing to establish a virtual private network (VPN) tunnel).

When combined with Windows Server 2003 and Outlook 2003, Exchange 2003 provides a robust, feature-rich end-to-end messaging system that is both scalable and manageable.

What are the disk considerations when installing Exchange (RAID types, locations and so on).

You got a new HP DL380 (2U) server, dual Xeon, 4GB of RAM, 7 SAS disks, 64-bit. What do you do next to install Exchange 2003? (you have AD in place)

Why not install Exchange on the same machine as a DC?

- The server must NOT be a cluster. Exchange 2003 clusters co-existing on Active Directory servers is not supported by Microsoft.
- Installing Exchange 2003 and Active Directory on the same server has a significant performance impact.
- The server **must be a Global Catalog server** (not just a DC).
- DSAcess/DSPProxy/Cat will not load-balance or fail-over to another DC/GC.

- Avoid the use of the /3GB switch, otherwise the Exchange cache might monopolize system memory. Additionally, the number of user connections should be very low, therefore the /3GB switch should not be required.
- All services run under LocalSystem so there is a greater risk of exposure should a security bug be found (e.g. a bug in AD which allows an attacker to access the AD will also allow them to access Exchange, and vice-versa)
- If Exchange administrators will be able to logon to the local server. Because they have physical console access to a DC, potentially they can elevate their permissions in the AD.
- It may take approximately 10 minutes for the server to shutdown. This is because the AD service (LSASS.EXE) shuts down before the Exchange services, and DSAccess will go through several timeouts before shutting down. The workaround for this issue is to manually stop the Exchange services (specifically the Store) before initiating a system shutdown or restart.

Exchange Migration Options

While there are many permutations of Exchange and Outlook, the best combination is Exchange 2003 (server) with Outlook 2003 (client).

The main focus of my advice is about migrating from Exchange 5.5 to Exchange 2003. However there are other upgrade scenarios:

Exchange 5.5 to Exchange 2000 - Because you have Windows 2000 not Server 2003.

Exchange 2000 to Exchange 2003 - Because you want the latest Exchange features and you have upgraded to Windows Server 2003.

Reasons to migrate to Exchange 2003

1. Clustering - 4 or 8 Node Active / Passive clustering is now a feasible option.
2. Multiple storage groups - Divide and rule for better performance and faster restore. Put the Boss and senior staff in their own mail store.
3. Multiple administrative Groups - useful for delegation.
4. OWA (Outlook **Web** Access).
5. OMA (Outlook **Mobile** Access)
6. Front end / Back end Exchange servers, used in conjunction with firewalls to improve security.
7. RPC over HTTP allows OWA clients to collect their email by only opening port 80
8. Volume Shadow Copy.
9. Query Based Distribution Groups. Let LDAP create distribution lists dynamically, based on users department or office.
10. ExDeploy and ExMerge new wizards to help you migrate and configure.
11. Better message queue management. (Also gives faster throughput)
12. Outlook Cached Mode (Laptops).
13. Junk email filtering. (Not perfect, but a step in the right direction)
14. Single mailbox restore.
15. Better support for mobile users thanks to OWA and OMA.
16. Enhanced junk mail filtering on both client and server ([see more here](#)).
17. Greater server availability.
18. Superior reliability, better manageability.
19. Reduced number of servers, less fragmentation.
20. Improved replication traffic, thanks to Windows Server 2003.

Improved Performance

My rule of thumb for Exchange 5.5 was 500 users per server, amazingly, with Exchange 2003, you can support 2000 users on the same specification machine. The latest Exchange version is so much more efficient at handling messages.

The Evolution of Exchange Server Deployment at Microsoft itself

	Exchange 4.0	Exchange 5.0	Exchange 5.5	Exchange 2000	Exchange 2003
Mailboxes per Server	305	305	1,024	3,000	4,000
Mailbox Size/User	50 MB	50 MB	50 MB	100 MB	200 MB
Restore Time per Database	12 hours	12 Hours	8 Hours	1 Hour	25 minutes
Total number of Mailboxes	32,000	40,000	50,000	71,000	85,000

How to Set the Recovery Storage Group Override Registry Key

If you restore mailbox stores without creating a Recovery Storage Group, the data will be restored directly to the original mailbox stores, as in previous versions of Exchange. If you already created a Recovery Storage Group, you can restore directly to the original mailbox stores if you set the override registry key.

Procedure

To set the Recovery Storage Group Override registry key

1. Start Registry editor (regedit).
2. In **Registry Editor**, navigate to the following registry key:

HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\Parameters\System

3. Create a new DWORD value **Recovery SG Override = 1**. After this key has been set, you can restore mailbox stores to their original locations, even though the Recovery Storage Group exists

Differences Between Exchange Server 2003 and Exchange 2000 Server

The following Microsoft® Exchange 2000 Server application development-related technologies and features were changed in Exchange Server 2003. Some technologies were enhanced, while others were removed, or are not supported in specific scenarios.

1.2 Exchange WMI Provider Changes

The Exchange Server 2003 includes new Microsoft Windows® Management Instrumentation (WMI) classes for managing Exchange Server 2003. You can read about the changes in the [WMI Changes for Exchange Server 2003](#) section.

1.3 Active Directory Schema Changes

During installation, Exchange Server 2003 changes some class and attribute definitions in Microsoft Active Directory®. For information about the schema changes that Exchange Server 2003 makes, read the [Active Directory Schema](#) section.

1.4 Managed Wrappers for SMTP Server Event Sinks

Published in June, 2003, the technical article [Writing Managed Sinks for SMTP and Transport Events](#)  provides sample code and information for both Exchange 2000 Server and Exchange Server 2003.

1.5 Anti-spam Infrastructure

Exchange Server 2003 includes a new property that can be used as a standard mechanism by message filtering applications. The property indicates how confident the filter is that a message is unsolicited commercial e-mail. For more information about how to create message filtering applications, see the [Anti-Spam](#) section.

1.6 CDO Component Names Did Not Change

In Exchange Server 2003 the CDOEX library is still named "CDO for Exchange 2000". Similarly, the CDO library that ships with Microsoft Windows Server™ 2003 is still named "CDO for Windows 2000".

Note The CDO for Exchange Management (CDOEXM) version that ships with Exchange Server 2003 must be used when accessing Exchange Server 2003. The Exchange Server 2003 CDOEXM can also be used to access Exchange 2000 Server. The CDOEXM library that ships with Exchange 2000 Server is not supported for accessing Exchange Server 2003.

1.7 Exchange 2000 Technologies not Included with Exchange 2003

The following technologies that were included in Exchange 2000 Server are not available in Exchange Server 2003.

1.7.1 M: Drive Mapping Removed

The mapped M: drive is not supported in Exchange Server 2003 and is not added in either the upgrade or fresh install of Exchange Server 2003. Microsoft FrontPage® Server Extensions are also not supported in Exchange Server 2003 because the mapped M: drive is required to upload some data to Exchange. Existing applications can no longer use the mapped M: drive functionality.

1.7.2 FrontPage Server Extensions Removed

FrontPage Server Extensions are not supported on Exchange Server 2003 because the mapped M: drive is required to upload some data to Exchange. Existing applications can no longer use this functionality.

1.7.3 Exchange Instant Messaging Removed

The Exchange 2000 Server Instant Messaging Service (IM) is no longer included in the Exchange Server 2003. Microsoft recommends migrating any applications that use Exchange 2000 Server IM to other Microsoft real-time collaboration technologies.

1.7.4 SQL Create Index Function Removed

The Structured Query Language (SQL) Create Index function is not supported in Exchange Server 2003 and has been removed. Applications should not attempt to use the function.

1.7.5 Versioning Schema Properties Removed

Versioning will not be supported in Exchange Server 2003, and the following schema properties will not be available to applications:

- dav:autoversion
- dav:checkintime
- dav:childautoversioning
- dav:childversioning

- <http://schemas.microsoft.com/exchange/defaultrevision>
- dav:isversioned
- dav:mergedfrom
- dav:revisioncomment
- dav:revisionid
- dav:revisionlabel
- dav:revisionuri
- dav:vresourceid

1.8 MAPI Technology Changes

While Extended MAPI is still used and supported with Exchange Server 2003, the following parts of Exchange MAPI are not installed, and are not supported by Exchange Server 2003. These changes affect only the MAPI system that is installed by Exchange.

- Common Messaging Calls (CMC)
- Simple MAPI
- CDOHTML

Client applications build using Simple MAPI or CMC will continue to function and be supported, provided the necessary libraries are installed on the computer where the application is running. Extended MAPI and Collaboration Data Objects (CDO) version 1.2.1 are supported with Exchange Server 2003

1.9 Visual Studio .NET Technology Support Policy

Not all Exchange technologies are supported for use in managed code applications. The Microsoft Knowledge Base article [813349](#)  provides information about which Exchange development APIs are supported in applications using Microsoft Visual Studio® .NET and the Microsoft .NET Framework.

1.10 Anonymous Access to IIS Metabase Disabled

When you send a message using `cdoSendUsingPickup` without specifying a pickup directory, CDO for Exchange 2000 Server (CDOEX) searches the Microsoft Internet Information Services (IIS) metabase and determines the pickup directory for the first active SMTP service instance. However, because anonymous access to the IIS metabase has been disabled, you need to either specify which SMTP service pickup directory you want CDOEX to use by setting the `smtpserverpickupdirectory` Field, or ensure that your application runs under an account that has read access to the IIS metabase. Note that if you set the pickup directory in your application explicitly, subsequently changing the location of the pickup directory may cause your application to fail.

1.11 Public Folders Mail-Disabled by Default

By default, all folders under `PUBLIC/NON_IPM_SUBTREE` are mail-disabled. You can, however, mail enable any of these folders as necessary. Please see the Exchange SDK for instructions about how to mail enable a public folder.

1.12 **savesentitems Field is ignored**

The savesentitems Field has no effect when you send messages using CDOEX. A copy of the message is saved to the Sent Items folder regardless of the parameter setting. This is because the Exchange OLE DB (ExOLEDB) provider provider is hard-coded to save a copy of all sent messages to the Sent Items folder.

1.13 **Exchange 5.5 Event Agent Disabled by Default**

The Exchange Server 5.5 event agent continues to be shipped with, and supported on Exchange Server 2003. However, by default the agent is disabled during installation.

1.14 **MSDAIPP Cannot be Run on the Exchange Server**

The Microsoft OLE DB Provider for Internet Publishing (MSDAIPP) is not supported on the Exchange computer. Running MSDAIPP is supported on a computer where Exchange is not installed.

Are there any other installation considerations?

How would you prepare the AD Schema in advance before installing Exchange?

To Install an new exchange on a domain that already has AD installed:

1. Make sure all the following are installed and working on the server SMTP, NNTP, ASP.NET, IIS, WWW. This can be installed windows component on Add-Remove program
2. Run Forest Preinstall Prep
3. Run Domain Prep and you are good to go.

Types of Exchange Server 2003 Backup

Full Backup

Make it your reflex to make a full backup of Exchange. Here are two killer reasons why a full backup is so much better than the alternatives; you only need one tape for a restore and a full backup purges the transaction logs.

Only resort to differential or incremental if the time taken by the full backup is unacceptable. If the duration seems too long for a full backup, try work-arounds like faster tapes, backup to disk then to tape. Anything to avoid having to use incremental or differential backups.

Differential Backup

If you have tried every trick in the book, and a full backup still takes too much time, then choose a differential rather than incremental backup. Remember that when you restore differential tapes, there must be a full backup as a reference point. Traditionally, the full backup is made at weekends, complemented by a differential backup on each weekday night. Times may vary but the guideline would be the hours of lowest user activity.

Unfortunately, differential backups do not purge or truncate the transaction logs, so not only does the differential backup get slightly bigger each day, but the logs are using up more and more disk space until you perform the next full backup.

Incremental Backup

Avoid this method. To prove my point try a test restore on a Friday. Calculate how many tapes you need and how long it will take. Realize that there is a five times greater chance of a slip up before the data is recovered, than with a full backup. Another clue that this is a poor method is that SQL and other relational databases do not allow incremental backups. Two tiny pieces of good news, incremental backups are quick and they do delete old portions of the transaction logs.

Copy Backup

This is a specialist method which is useful if you need to take a snapshot of the system without altering the archive bit. Differential and Incremental backups take their cue from the archive property of the files, so my point is that a copy backup doesn't affect other backup schedules that you have in place.

Daily Backup

This method surprised me, I thought that it would backup any file within the last 24hrs. Not so. It only backed up files that had changed since midnight, time stamp 0:00. I cannot recommend this method for Exchange 2003.

Understanding the Exchange Information Store

The Information Store is the heart and soul of Exchange Server 2000 and 2003. Understanding the fundamentals of the Information Store is important for anyone managing an Exchange server.

Note: This article is published with permission from www.msexchange.org 

Introduction

The Information Store is the heart and soul of Exchange 2000 and 2003. Understanding the fundamentals of the Information Store is important for anyone managing an Exchange server. If you don't believe me, stop the Microsoft Exchange Information Store service and count the seconds before your phone starts ringing!

Exchange 2000 and 2003 use the same Information Store but there are some differences depending on the version. Table 1 describes these differences.

Store Features	Exchange 2000* or Exchange 2003 Standard Pre-SP2	Exchange 2003 Standard /w SP2	Exchange 2000 or 2003 Enterprise
# of Storage Groups	1 + 1 RSG**	1 + 1 RSG**	4 + 1 RSG**
# of Stores	1 Mailbox store and 1 Public Folder Store per Storage Group	1 Mailbox store and 1 Public Folder Store per Storage Group	5 per Storage Group
Store Size Limit	16GB per Store	75GB per Store	16TB per Store

* Any Exchange 2000 service pack level

**RSG = Recovery Storage Group

Storage Groups and Databases

A Storage Group will contain one or more Mailbox and Public Folder stores, depending on the version and the needs of the organization. Mailbox stores contain the user and system mailboxes and the Public Folder Store contains the Public Folders and their contents. For most organizations, a single Storage Group, with one Mailbox Store and one Public Folder Store is more than enough, however as the database grows in size, splitting one large database into multiple smaller databases can ease the management of backups.

A default Exchange installation will create a Storage Group that contains a Mailbox Store and a Public Folder Store. Each Mailbox Store is made up of a database set that contains two files:

- **Priv1.ebd** is a rich-text database file that contains the email messages, text attachments and headers for the users e-mail messages
- **Priv1.stm** is a streaming file that contains multi-media data that is formatted as MIME data.

Similarly, each Public Folder Store is made up of a database set that also contains two files:

- **Pub1.ebd** is a rich-text database file that contains the messages, text attachments and headers for files stored in the Public Folder tree.
- **Pub1.stm** is a streaming file that contains multi-media data that is formatted as MIME data

For every EDB file there will be an associated STM file.

Exchange utilizes what Microsoft terms a single-instance message store. This single-instance message store works on a per database basis. What does this mean? If an e-mail message is sent to multiple mailboxes that are all in the same database, the message is stored once and each mailbox has a pointer to the message. The transaction is also logged in the transaction

logs for the Storage Group that contains the database. However, if the e-mail message is sent to multiple mailboxes that are located in different databases, the message is copied to each database and written to the transaction logs for each Storage Group the contains the database with a copy of the message.

For example, if I send 10 users a 1MB email message and all the mailboxes are located in the same database, one copy of the message is written to the database and each mailbox points to this message which will consume 1MB of disk space in total. If the 10 recipients are located in two different databases, each database will get a copy of this message which will consume 2MB of disk space. As you can see this is a much more efficient use of space as opposed to the alternative of 10 1MB messages using up 10 MB of disk space.

Aside from the database files, Storage Groups also contain system files and transaction logs. There are two system files, Tmp.edb which is a temporary database where transactions are processed, and E##.chk. The E##.chk file maintains the checkpoint for the Storage Group. The ## represents the Storage Group number with the First Storage Group file called E00.chk. This checkpoint file keeps track of the last committed transaction. If you are ever forced to perform a recovery, this file contains the point at which the replaying of transaction logs starts.

Transaction Logs

The transaction logs are some of the most crucial files when it comes to a working Exchange server. Microsoft Exchange Server uses transaction logs as a disaster recovery method that can bring a Exchange database back to a consistent state after a crash. Before anything is written to the EDB file, it is first written to a transaction log. Once the transaction has been logged, the data is written to the database when convenient.

Until a transaction is committed to the database, it is available from memory and recorded in the transaction logs. This is why you will see store.exe use up to 1GB of memory after the Exchange server has been in use for a while. After an Exchange server is brought back up after a crash, the checkpoint file points to the last committed transaction in the transaction logs which are then replayed from that point on. This form of write-ahead logging is important for you to know.

There are four types of transaction logs:

- **E##.log** is the current transaction log for the database. Once the log file reaches 5MB in size it is renamed E#####.log and a new E##.log is created. As with the checkpoint file the ## represents the Storage Group identifier. While the new E##.log file is being created you will see a file called Edbtmp.log which is a template for Exchange server log files.
- **E#####.log** are the secondary transaction logs. They are number sequentially starting with E0000001.log using the hexadecimal numbering format and are 5MB in size.
- **Res1.log** is a reserved log file that is limited to 5MB in size. When the disk has run out of space, transactions are written to this log file while you work on clearing up space on the disk.
- **Res2.log** is another reserved log with the same function as Res1.log.

Transaction logs can grow at a fast pace as each and every transaction is recorded to the log files. There are two ways to manage this growth with the recommended method being a regular full backup of the Information Store. Upon successful backup, the transactions are committed to the database and then purged.

The other method is to enable circular logging. Circular logging is disabled by default as it only allows you to recover Exchange data since the last full backup. With circular logging enabled the transaction logs are purged as the transactions are committed to the database. If you have to restore from backup, the transaction logs will not be replayed and all transactions since that backup will be lost.

The two reserved log files, Res1.log and Res2.log, are used to "save" 10MB of space on the disk in case there is no more free space. When the disk runs out of free space, the transactions are logged to the reserve logs as the Information Store shuts down gracefully. You will not be able to restart the Information Store service until you clear up some disk space.

Best Practices

As with anything there are some best practices you can follow in order to maintain a healthy Information Store.

- Locating the Exchange program files, SMTP queues, transaction logs and database files on separate disk arrays is ideal. If budget constraints will not allow for this, locating the program files, transaction logs and SMTP queues on separate partitions on one disk array and the database files on a separate disk array will still offer some performance increases at a reduced cost.
- All files should be located on redundant disk arrays. RAID 1 is the minimum recommended level, with RAID 5 offering an increase in performance and RAID 10 offering the best performance but at an increased cost.

- Perform regular, full backups of the Information Store to commit the transactions and flush the log files. This can be done with the native Windows backup tool, NTBackup, or a third party solution. Even if you live on the wild side and do not keep backups of your data, it is important to do this to prevent the disk from filling up with log files and running out of space.
- Do not use circular logging. As mentioned circular logging will not allow you to replay the transaction logs limiting you to recovering only the data from the latest full backup set.

The Information Store is the most critical component of Exchange Server 2000/2003 and a proper understanding of its structure is important to know for anyone tasked with managing and maintaining an Exchange server.

Why not install exchange on the same machine as a DC?

well, this is not a good practice to do and the reasons behind are :

1. Redundancy and Stability - if the exchange server fails then Domain Controller also fails and it concludes a big failure...

2. Overload : It may overload your existing server and that can cause a significant performance problem.

well if think there is something important that i missed please inform me via mail.

What's the main differences between exchange 5.5 and Exchange 2000/2003

Exchange 5.5 does not integrate with the NT4 domain or the Windows 2000/2003 Active Directory in a meaningful way. A single user could be associated with several different mailboxes. Exchange 2000/2003/2007 integrates tightly with Active Directory, and there is a 1:1 relationship between mailboxes and AD user accounts. There are other differences, depending on whether you have a standard or enterprise version as it relates to maximum database size, but the directory integration is probably the biggest difference.

What type or permissions do you need in order to install the first Exchange server in a forest? In a domain?

Domain admin

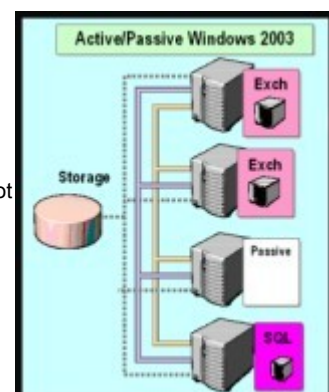
Schema admin

Enterprise admin

Clustering Terms and Concepts

The master plan is to deploy clustering and so eliminate a single point of failure. If, for whatever reason, an Exchange server is not available, then another server is firstly aware, and secondly has the capability of taking over the dead servers role. The email continues to flow!

Clustering neatly illustrates how a new Microsoft technology evolves. In the 1990's Microsoft started developing clustering for NT servers. Unfortunately, early implementations were weak, even flaky. By Windows 2000 clustering was workable if not scalable. With Windows Server 2003 and Exchange 2003 all the pieces are in place, clustering is now a feasible solution for fault tolerant mail servers.



There are two types of clustering. Active / Passive and Active / Active clustering. Always favour the Active / Passive or 'hot spare' solution. My reasoning is that you want to be sure that second server can take the full load. Where both servers are Active, at the very least there will be a performance reduction, at worst the one remaining server will not be capable of carrying the load of both servers. The Active / Passive is like having a standby engine, whereas the Active / Active is like cancelling a train and piling two loads of commuters onto one train.

The key development in Windows 2003 clustering has been to increase the nodes from 2 to 8. The idea is to always have a 'hot spare' machine to takeover, or 'failover' if any of the other 7 machines is unavailable. The passive machine would have Exchange 2003 installed and would be ready to seamlessly replace any of the regular Exchange Servers should they crash.

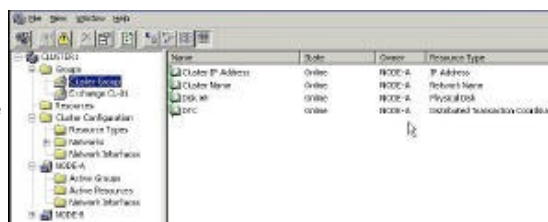
How Clustering Services work

The key to configuring clustering is to focus on the Exchange services and the concept of Virtual servers. Clustering relies on shared storage. This shared disk takes the form of SCSI or SAN. Let us say that the active node on server A is in charge of Exchange Services, for example System Attendant. If that active node fails then the passive node B (hot spare) takes over those services previously hosted by server A. As the disk containing the mail is shared between all members of the cluster there is no transfer of data, and little latency in the Exchange services failing over.

Meanwhile the clients are still connecting to the virtual server name and IP. So the email users do not notice that the services have been switched automatically from server at node A to the server at node B.

Getting Started - Cluster Configuration.

This section is only intended as an overview on configuring clustering. My best recommendation on server hardware is, pick the brains of your suppliers. They will have all the features at their finger-tips and guide you to an integrated system with components designed to work in clusters.



Those who use the HCL (Hardware compatibility list) as their Bible will be rewarded with compatible components. In particular, be sure that your RAID disks are cluster aware. Those who mix and match components could be in for a nasty shock when they get messages like STOP 0x000000B8 due to hardware which is incompatible with clustering. Talking of hardware in general and disks in particular, take the opportunity to research other [technologies like SAN](#) (Storage Area Network).

If you have to make the most of existing hardware, then the Windows Server 2003 Help and Support will guide you through preparing your server. You will need a second network card so that the cluster machines have their own private 'heartbeat' network.

Incidentally, unlike Windows 2000, the clustering service is now installed automatically in Sever 2003, there is no need to Add or Remove Programs, just run CluAdmin. The wizard will then guide you through the creating and naming of your cluster. What you will need is a service called MS DTC (Data Transaction Co-ordinator)

Always install and configure the cluster service before you install Exchange. Sounds simple, but trust me if you do it the other way around it wrecks your Exchange server. (Another reminder to always backup before you attempt something new or adventurous.)

From the client's point of view they see the cluster as a virtual entity so you must assign a unique name to the cluster. The actual names of the servers are hidden from the clients.

How would you verify that the schema was in fact updated?

What type of memory optimization changes could you do for Exchange 2003?

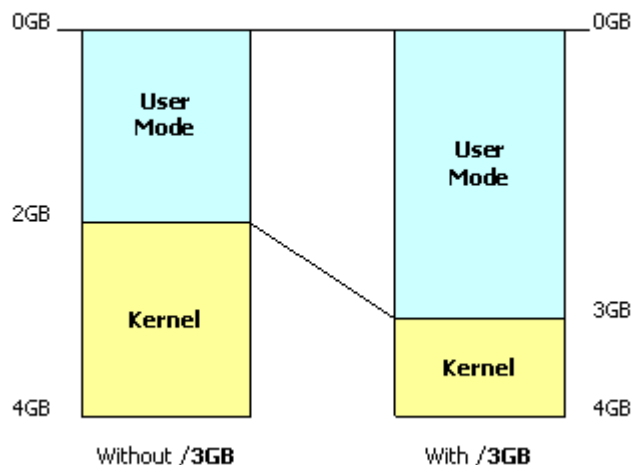
Anyone who knows Exchange has probably heard by now that Exchange is a memory eater. The store process is the main responsible for this behavior, since store.exe starts it will grab as much memory as it can possibly get. This behavior is often wrongly seen as a problem or as a memory leak, but actually it's a normal and expected operation. Besides, Exchange can return memory to the operating system using an algorithm known as Dynamic Buffer Allocation. And yes, you can limit the maximum amount of memory that Exchange uses by reducing the ESE Buffer size.

By these days, memory is not as expensive as it used to be, so it's easy to find Exchange servers with a couple of GB of RAM. But with all this memory, you'll have to give a little help to make Exchange use it wisely. If you have a server with more than 1GB of RAM, there are some configuration parameters you can change in order to optimize Exchange memory usage.

I'll describe the modifications you should do just for Exchange 2003 running on Windows 2003. There are slightly differences for Windows 2000, but I will not mention them in order to keep this article shorter (if you really want to know the differences feel free to drop me an email).

You should not make any modifications to servers that do not contain any mailboxes or public folders (front-ends or bridgeheads), neither to Exchange Server computers which are at the same time Active Directory Domain Controllers or Global Catalogs.

1. First of all you should add the switches **/3GB** and **/USERVA=3030** to boot.ini. The **/3GB** switch modifies the way virtual address space is created so that 3 gigabytes are available for user mode applications. By default, Windows reserves 2GB for kernel and another 2GB for user mode processes. The **/USERVA** switch is a more precise tuning Microsoft recommends that increases the system page table entries (PTE) by 42MB.



2. Configure the HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\HeapDeCommitFreeBlockThreshold registry value to 0x00040000. The HeapDeCommitFreeBlockThreshold registry key specifies the number of contiguous bytes above which the memory is decommitted rather than retained for reuse, thus avoiding virtual memory fragmentation.
3. If you have a server with more than 2 GB of memory, it may help to increase the size of the Store Database Cache (aka ESE buffer). Because of virtual address space limitations, this value must not be set higher than 1200 MB. You should use Windows Performance utility to monitor the memory of the server before you change this setting. To do this, monitor the following performance object and value:

Performance object: Process
Performance counter: Virtual Bytes
Instance: STORE

If you have a server that is configured with the /3GB and the virtual bytes counter is at 2.5 GB when the server is heavily loaded, you may be able to increase your maximum buffer size by about 300 MB, for a total size of 1200 MB. But keep in mind that increasing the buffer size may adversely affect server performance, so you'll have to be very careful with this setting.

To modify the ESE Buffer size you may use the ADSI Edit utility. Under Configuration Container expand CN=Services, CN=Microsoft Exchange, CN=OrganizationName, CN=Administrative Groups, CN=First Administrative Group, CN=Servers, CN=servername. Under CN=servername, right-click CN=InformationStore, and then click Properties. Find the **msExchESEParamCacheSizeMax** property and in the Edit Attribute box, type the value that you want to assign to it (make sure that you enter a value that is a multiple of 8,192). Click Set, and then click OK.

4. Verify that the HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\SystemPages registry value is set to 0.

After making all of these modifications you must restart your server for these changes to take effect.

Remember that there is no point in having a dedicated Exchange 2003 server with more than 4GB of memory. Although this may constitute a surprise for some of you, Exchange Server 2003 does not support instancing, Physical Address Extension (PAE), or Address Windowing Extensions (AWE). Therefore, 4 GB of RAM is the maximum amount of memory that an Exchange Server computer can efficiently use.

If you want to know more about Exchange Server memory usage, there are some Knowledge Base articles dedicated to this issue:

How would you check your Exchange configuration settings to see if they're right?

Microsoft made

available a Web-based diagnostic tool specifically for Exchange admins -- the Microsoft Exchange Server Best Practices Analyzer tool, or ExBPA.

The product is the brainchild of Paul Bowden, program manager for Exchange Server development, who two years ago came up with the idea of developing a tool that could programmatically check Exchange for "correct configuration and system health" and expose any critical and non-default server configurations.

The end result: the tool takes 1,200 data points from each server and generates a report that includes step-by-step instructions on how to solve any problems.

What are the Exchange management tools? How and where can you install them?

[Microsoft Exchange Troubleshooting Assistant v1.0](#)

[Mail Flow Troubleshooter in Exchange Troubleshooting Assistant \(ExTRA\) - A closer look](#)

[Exchange 2003 -- Performance Troubleshooting Analyzer Tool v1.0 \(ExPTA\)](#)

[Exchange 2003 - Disaster Recovery Analyzer Tool \(ExDRA 1.0\)](#)

1 Microsoft Exchange Server Monitoring tool

Exchange Server monitoring involves checking the availability of the following services:

• MS Exchange Information Store • MS Exchange Site Replication Store • MS Exchange MTA Stacks • MS Exchange Management • SMTP	• IMAP4 • MS Exchange System Attendant • MS Exchange Routing Engine • MS Exchange Event Service • POP3
---	--

1.15 Exchange Server Monitoring Capabilities

- Out-of-the-box management of Exchange Server.
- Monitors performance statistics such as response time, Availability.
- Based on the thresholds configured, notifications and alerts are generated if the mail server or any specified attribute within the system has problems. Actions are executed automatically based on configurations.
- Performance graphs and reports are available instantly. Reports can be grouped and displayed based on availability and health,
- Delivers both historical and current Exchange Server performance metrics, delivering insight into the performance over a period of time.

2 Microsoft Exchange Server Best Practices Analyzer tool, or ExBPA.

What types of permissions are configurable for Exchange?

How can you grant access for an administrator to access all mailboxes on a specific server?

What is the Send As permission?

Send As" allows one user to send an email as though it came from another user. The recipient will not be given any indication that the email was composed by someone other than the stated sender.

"Send As" can only be granted by a system administrator. "Send on Behalf of" may be more appropriate in many situations, it allows the recipient to be notified both who the author was and on who's behalf the email was sent. (See [How to grant Send On Behalf Of permission.](#))

The following procedure will allow system managers to grant users the ability to send as another:

1. Log onto the server running Exchange.
2. Run Active Directory Users and Computers.
3. Under the "View" menu ensure that "Advanced Features" is ticked.
4. Find the user's account that you want to be able to send as, and open up the account properties.
5. Select the "Security" tab.
6. Click [Add ...] (under "Group or user names") and add the user (users or group) that is to be granted permission to send-as this account.
7. For each account added, highlight the account under "Group or user names" and in the "Permissions for ..." window grant the account "Send As" permission.
8. Click [OK] to close the account properties dialog.

What other management tools are used to manage and control Exchange 2003? Name the tools you'd use.

What are Exchange Recipient types? Name 5.

Understanding the Recipient Types in Microsoft Exchange 2003

There is no doubt, knowledge is power. If you truly understand the names and capabilities of email objects, then you will always choose the right recipient for the right job.

Mailbox enabled user - Standard email account in Exchange Server 2003. A regular Active Directory user with a full MAPI mailbox. (90% of all email accounts are this type.)

Mail-enabled user - Tricky recipient. An Active Directory account with an email address, but no mailbox in your Exchange Organization. I call this the contractor object. Their email is delivered, not to your exchange mailstore, but to their external account, e.g. hotmail or gmail.

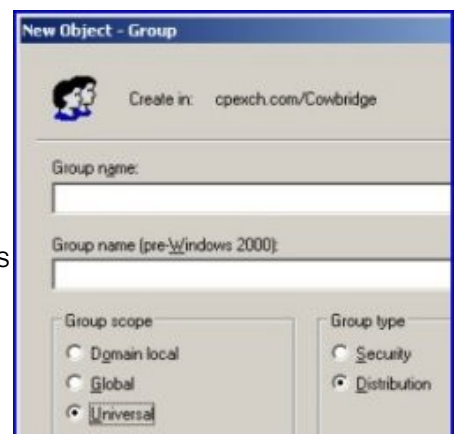
Distribution Group - The old Exchange 5.5 DL (distribution list). Big organizations may favour the Universal Distribution groups, while companies with one domain prefer Global Distribution groups.

Query-based Distribution Groups - A great new idea in Exchange 2003. You must investigate these dynamic groups which are populated by LDAP queries. [See how to manage these Query-based Distribution Groups groups here.](#)

Security Enabled Group - Where ever possible, avoid this object and use Distribution Groups instead.

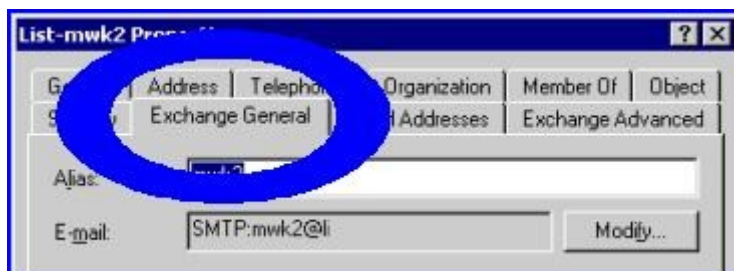
Here is my reasoning for shunning Security Enabled Groups for email recipients. Technically it takes longer to logon if users are members of lots of Security Groups - SIDS have to be checked and Universal group membership has to be verified.

However my main objection is because security groups are normally used for share permissions. I once saw an administrator add a user to a group that had access to the printer. What they forgot was that this was a mail-enabled group and the new user started receiving emails that were not meant for their eyes. (It was unpleasant because they were emails about that person's redundancy.)



Contacts - Easy recipient. These are your suppliers, customers with external email accounts. Contacts have no Active Directory account, just the email address of important people who your users regularly email. When you create a contact it appears in the Global Address List.

If there is a surprise with Contacts, it is that like User objects, Contacts have more tabs once you install Exchange, note the Exchange General and Exchange Advanced tabs.



Mail-enabled Public Folders - I think sending emails to public folders is a neat idea, however, it does not seem to have caught on at the sites that I have visited.

Creating Mail Enabled objects

Start by launching Active Directory Users and Computers (Not the Exchange System Manager). Now I love OUs (Organizational Units). So I would create the new users, groups or contacts in a suitable OU rather than in the default users container.

Tip If you get a choice of which server to create the mailbox, then choose a server physically close to the user. One company choose the server for the mailbox based on alphabetic order. This resulted in unnecessary traffic as the servers were in separate routing groups.

By default the mailbox name or alias = logon name. This makes sense and the user will soon get used to their alias. However if you have a strange rules for logon names, for example works number, then you can uncouple the alias = logon name and give the alias a more descriptive identifier

Exchange server 2007 64 bit and 32 bit details.

Microsoft Exchange Server 2007 and Exchange 2007 Service Pack 1 (SP1) are available in two server editions: Standard Edition and Enterprise Edition. For more information about these editions including descriptions and comparisons, see [Exchange Server 2007 Editions and Client Access Licenses](#). According to the Exchange Server 2007 Edition Offerings table on that Web page, the primary differences are:

- Only Enterprise Edition can scale to 50 databases per server; Standard Edition is limited to 5 databases per server.
- In a production environment, only Enterprise Edition is supported in a Microsoft Windows failover cluster; Standard Edition is not supported in a Windows failover cluster in production. Therefore, single copy clusters (SCCs) and cluster continuous replication (CCR) environments are only supported on Enterprise Edition. When you deploy Exchange 2007 in a failover cluster, an Enterprise Edition license is required for each node on which Exchange 2007 is installed.

Exchange 2007 RTM and SP1 are available in two platform versions: the 64-bit version is for live production environments and the 32-bit version is for non-production environments (such as labs, training facilities, demos, and evaluation environments). Only the 64-bit version can be purchased because you cannot run 32-bit Exchange 2007 servers in production.

There are exceptions with respect to production and non-production use of the 32-bit platform because Microsoft does allow minimal supported use of the 32-bit version in production environments:

- You can use the 32-bit version in production to extend your Active Directory directory service schema. For detailed steps about how to prepare Active Directory for Exchange 2007, see [How to Prepare Active Directory and Domains](#).
- You can use the 32-bit version of the release to manufacturing (RTM) management tools in production to administer Exchange 2007 servers from Windows Server 2003 or Windows XP.

- You can use the 32-bit version of the Service Pack 1 (SP1) management tools on Windows Server 2008 or on Windows Vista. Support for Windows Server 2008 and Windows Vista is available only with Microsoft Exchange Server 2007 SP1. However, you cannot use the SP1 management tools (32-bit or 64-bit) on Windows Vista to remotely manage a clustered mailbox server in a failover cluster. This is because:
 - Windows Server does not support cross-operating system management of failover clusters. Thus, Windows Vista cannot be used to manage a Windows Server 2003 failover cluster, and neither Windows Server 2003 nor Windows XP can be used to remotely manage a Windows Server 2008 failover cluster.
 - Remote management of a Windows Server 2008 failover cluster requires the installation of the Failover Cluster Management tools, which currently do not exist for Windows Vista. Thus, Windows Vista cannot be used to remotely manage a Windows Server 2008 failover cluster.

Let's begin

There are several components that are involved in the Mail delivery process.

Information Store (Store.exe)

The Microsoft Exchange Server Information Store (Store.exe) is the end point for e-mails sent to users on this server. It is also the start point for e-mails which are sent by MAPI clients, like Microsoft Outlook 2003, which directly connect to the MExchangeIS.

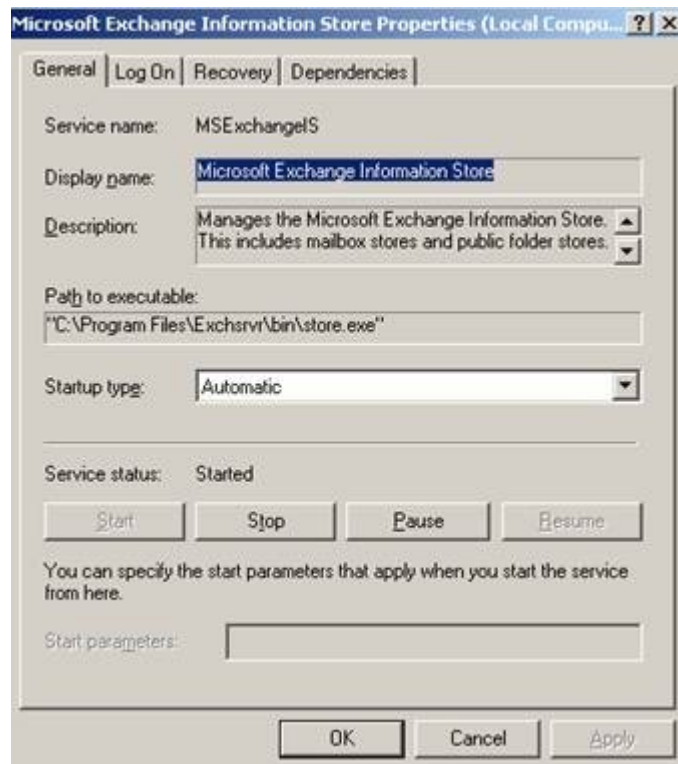


Figure 1: MExchangeIS

Exchange InterProcess Communication (EXIPC)

EXIPC is responsible for Data Transfer between Internet Information Server 6.0 (IIS) and the Microsoft Exchange Server Information Store (MExchangeIS). EXIPC provides a layered service between both components to achieve the best possible performance between IIS dependant components and the Exchange databases. As you might know, all Internet Client Access Protocols like HTTP/S, SMTP, POP3 and IMAP4 are configured and managed by IIS with some exceptions.

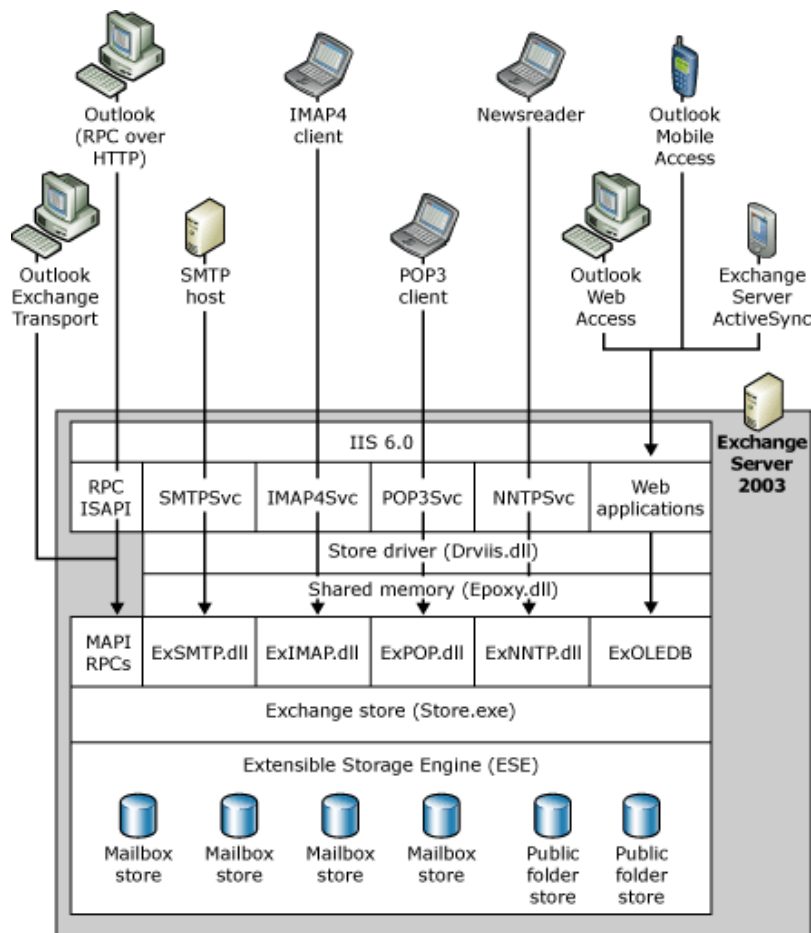


Figure 2: EXIPC Layer

This interaction allows Exchange to be in a FrontEnd, and BackEnd, Server scenario.

Through Virtual Servers, multiple configurations of the same protocol can exist on a single Exchange Server.

Advanced Queuing Engine (AQE)

The Advanced Queuing Engine (AQE) is responsible for creating and managing message queues for e-mail delivery. When AQE receives a Simple Mail Transfer Protocol (SMTP) mailmsg object, this object will be forwarded to the Message Categorizer. The Advanced Queuing Engine then queues the Mailmsg object for message delivery based on the Routing information provided by the Routing Engine process of Exchange Server 2003.

The Message Categorizer is part of the Advanced Queuing Engine and is responsible for address resolution on every Mailmsg object that flows through the AQE. The Message Categorizer is implemented as an Event Sink. The Message Categorizer is also responsible for splitting messages into RTF or MAPI.

Routing Engine

The Exchange Routing Engine uses Link State information for e-mail routing. The Routing Engine will forward this information to the Advanced Queuing Engine.

Please note:

The SMTP Stack from Windows Server 2003 will be extended through the Exchange Server installation process with several enhancements. One of these enhancements is the implementation of the XLINKSTATE protocol.

The Routing Engine creates and maintains the Link State information for every Exchange Server and is also responsible for routing the messages to inbound or outbound destinations.

SMTP Service

The SMTP Service processes incoming traffic from any SMTP host. SMTP is also used in most communications between Exchange Servers (except Exchange 5.x Servers which use RPC for message transferring). SMTP is also responsible for some advanced Exchange Server functions like Message Journaling. During the Exchange installation, the built in SMTP Service from Windows Server 2003 will be extended with several new functions. Some of the Enhancements are:

- Moving the Message Queue Directories to the Exchange installation Directory
- Providing support for the LSA (Link State Algorithm) in SMTP
- Moving SMTP Messaging from IIS to the Exchange System Manager

1.16 Message Flow

Because understanding the e-mail message flow is important, I will list some high level steps in the message flow:

- MAPI client sends a message to a remote recipient
- Information Store (Store.exe) receives the message
- The created MailMsg object is forwarded to the Advanced Queue Engine (AQE)
- The Message Categorizer from the AQE processes the MailMsg object and splits it into MIME or RTF as necessary
- The Message Categorizer expands groups and checks defined Message limits on Exchange
- The MailMsg object is then transferred to the Remote Destination Domain within the AQE
- The AQE passes the destination address to the Exchange Routing Engine
- SMTP initiates an SMTP session with the remote SMTP host
- After the SMTP session with the remote host has been established, the information store retrieves the body of the message and converts the message as necessary
- SMTP sends the Message from the Queue to the Remote Host

The following Exchange Features require the use of SMTP:

- Intra Server Message Delivery
- Inter Server Message Delivery
- Message Delivery to the Internet
- Exchange of Routing Information

Intra Server Message Delivery

SMTP will be used for Intra Server Message Delivery for several components like Message Journaling and Message categorization. Exchange Servers in the same Routing Group use SMTP to communicate with each other.

You created a mailbox for a user, yet the mailbox does not appear in ESM. Why?

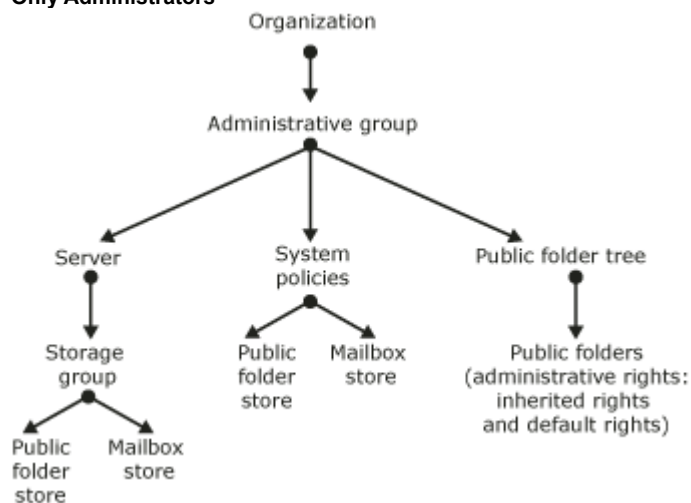
You wanted to change mailbox access permissions for a mailbox, yet you see the SELF permission alone on the permissions list. Why?

1.16.1 Permissions for the Exchange administrative roles on mailbox stores, public folder stores, and public folder trees

Role	Allowed	Denied
Exchange Full Administrator	Full Control Additional permissions in Active Directory to allow you to work with deleted items and offline address lists	Receive-As Send-As
Exchange Administrator	All except Change Permissions Additional permissions in Active Directory to allow you to work with offline address lists	Receive-As Send-As
Exchange View Only Administrator	Read List object List contents View Information Store Status	None

The following figure summarizes how mailbox stores, public folder stores, and public folder trees inherit permissions.

Direction of inheritance of permissions for Exchange Full Administrators, Exchange Administrators, or Exchange View Only Administrators



As Figure 7.1 shows, objects in the Exchange store inherit permissions from their administrative group, with the following exceptions:

- Delegating Exchange administrative roles on an administrative group gives administrators in those roles limited permissions on mailboxes—enough to create or delete mailboxes, and set options such as storage limits.
- A public folder inherits some administrative permissions from the public folder tree where it resides. It does not inherit permissions from the public folder store.
- Administrative rights on a public folder include many folder-specific permissions that are not available on the public folder tree. For example, although an Exchange Administrator cannot modify the permissions on a public folder tree, the administrator can modify permissions on a public folder in that tree.

In Exchange 2003, there are three sets of permissions that you can manage:

- Permissions for Exchange objects. These settings are stored in Active Directory and the Microsoft Internet Information Services (IIS) metabase.
- Store permissions.
- File permissions on NTFS file system volumes.

What are Query Based Distribution groups?

How Does a Query-Based Distribution Group Work?

1. An e-Mail is submitted to the submission queue of the Exchange store driver or through SMTP
2. The message categorizer determines that the recipient is a Query-based Distribution Group
3. The categorizer sends an LDAP request to an global catalog server
4. The contacted global catalog server executes the query and returns the addresses that matches the query
5. After receiving the complete set of addresses matching the query, the categorizer generates a recipient list containing all the users.
6. After the categorizer sends the complete, list of recipients to routing, the normal message delivery process continues, and the e-mail message is delivered to the users mailboxes.

1.17 Guidelines for Creating Query-Based Distribution Groups

Use the following guidelines when creating query-based distribution groups:

- You can only use query-based distribution groups in a pure Exchange 2003 environment or in a native mode environment with Exchange 2000 and Service Pack 3 and Exchange 2003.
- In multiple-domain environments you should use only universal groups as members of the query-based distribution group because only the membership of universal groups is replicated to global catalog servers.
- Index the attributes in the query because this will improve the performance of the query and reduce the time to expand the distribution group.

1.18 Combining Multiple Query-Based Distribution Groups

You can create query-based distribution groups based on the AND operator. This means you can combine two or more queries. The first query includes users who are on mailbox store X and the second query includes users who are on mailbox store Y. Then we would create a standard distribution group

7.

What type of groups would you use when configuring distribution groups in a multiple domain forest?

Name a few configuration options for Exchange recipients.

Default Recipient Policy

You can view the proxy addresses assigned to a recipient using the Active Directory Users and Computers console. Open the Properties window for the recipient and select the Email Addresses tab. Figure 5.27 shows an example.

When you install Exchange for the first time, it determines the format of the SMTP address you'll want for your users based on your organization name and the DNS name of your domain. It places the result into an Active Directory object called a **Recipient Policy**.

A service called the Recipient Update Service, or RUS, reads the proxy addresses in that default recipient policy and applies them to the mail-enabled objects in Active Directory.

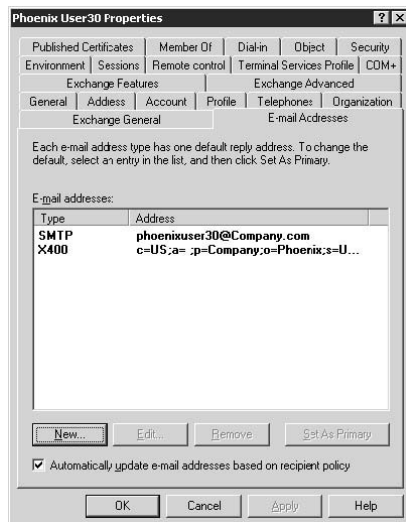


Figure 5.27 Proxy email addresses assigned based on Default Recipient Policy. (Click on image for enlarged view.)

To access recipient policies in ESM, drill down under Recipients to the Recipient Policies container, as shown in Figure 5.28.

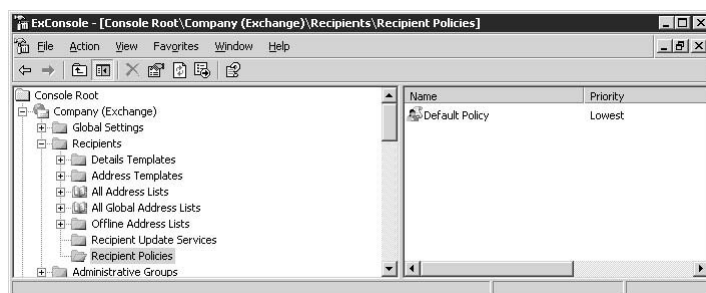


Figure 5.28 ESM console showing Recipient Policies container and Default Policy. (Click on image for enlarged view.)

To see how Exchange formulates a proxy address, open the Properties window for the Default Policy object. Figure 5.29 shows an example. If Exchange guessed wrong when formulating the default SMTP address for your organization, you can change the address as follows:

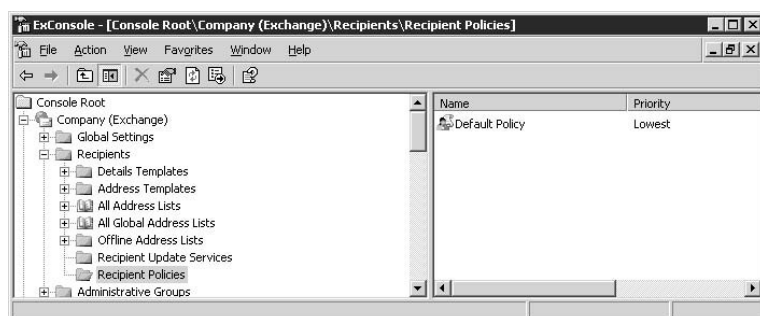


Figure 5.29 Proxy email address selection options in Default Recipient Policy. (Click on image for enlarged view.)

1. Highlight the address and click **Edit**. This opens an Edit window where you can enter a new address.
2. Enter the new SMTP address you want as the default for your organization.
3. Save the change. You'll get a warning message saying that **The email Addresses of type(s) SMTP have been modified. Do you want to update all corresponding recipient email addresses to match these new address(es)?**
4. Click **Yes** to apply the change.

In a few minutes, the Recipient Update Service will apply the change to all existing mail-enabled objects. The next time you create a new mail-enabled object, the Recipient Update Service applies the new address settings.

If you look at the Email Addresses tab of existing users and groups, you'll notice that the old address remains, relegated to a secondary SMTP address, as shown in Figure 5.30.

Exchange retains the old address just in case a user receives mail addressed to that SMTP domain. For example, if you have salespeople already getting mail addressed to `subsidiary.com` and you configure a recipient policy to give them an SMTP domain of `company.com`, you don't necessarily want mail addressed to `subsidiary.com` to bounce.

If you want the superseded addresses to go away, you must either remove the addresses manually in Active Directory Users and Computers or use an automated process of some sort. Microsoft Knowledge Base article 318774 describes how to dump the contents of the recipient's attributes using LDIFDE, and how to manipulate the ProxyAddresses attribute to get rid of the unwanted addresses to then import the result back into Active Directory. You can also write a script to replace the content of the ProxyAddresses attribute. These processes can get fairly complex, so you have to ask yourself if you *really* want those old addresses to go away.

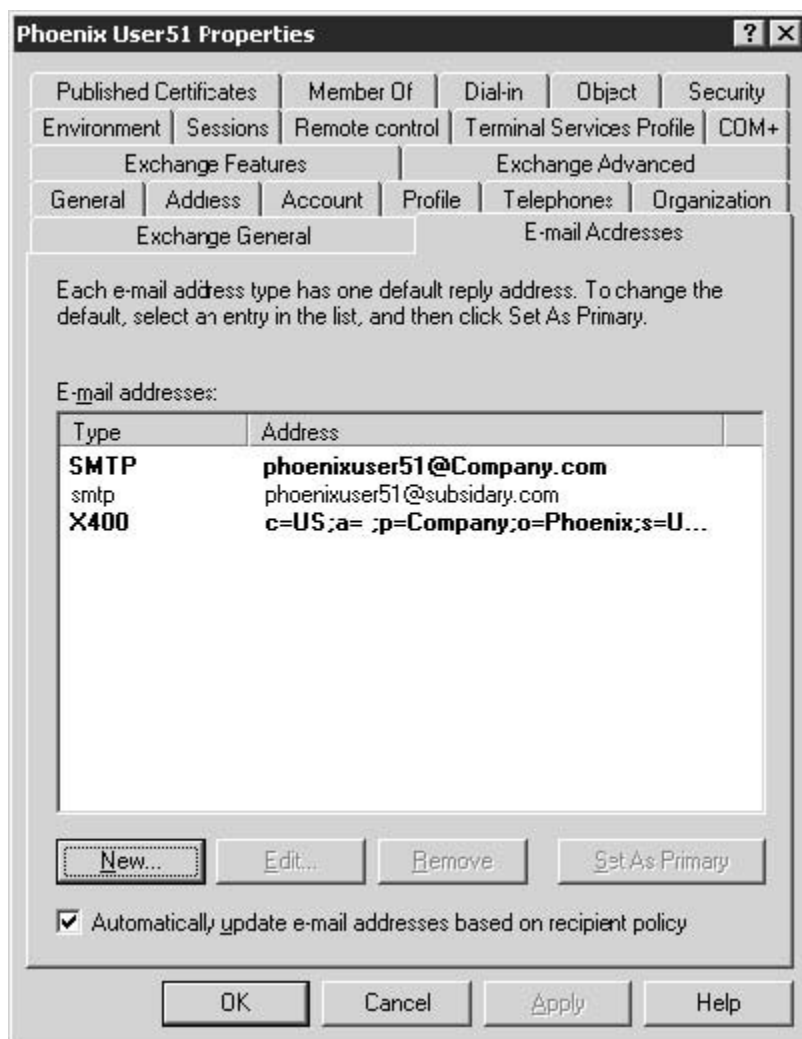


Figure 5.30 Proxy address changes done as the result of changing the Default Recipient Policy.

Policy filter

Each Recipient Policy contains an LDAP filter that defines who gets the proxy addresses contained in the policy. (Recipient policies also control the Mailbox Management feature, covered later in this chapter.)

To see the LDAP filter for a Recipient Policy, select the General tab. Figure 5.31 shows the filter for the Default Recipient Policy. Note that the default policy applies to every mail-enabled object in Active Directory via the simple expedient of searching for any object with a mailnickname attribute.

You can create a new Recipient Policy and target it to specific types of recipients via an LDAP query. For example, let's say that the Sales department manager wants potential customers to try out a new corporate identity called WhizBang.com instead of the boring old Company.com. She wants salespeople to give out their email addresses as user@whizbang.com instead of user@company.com, but she does not want them to give up their old addresses because they have made valuable contacts with those addresses.

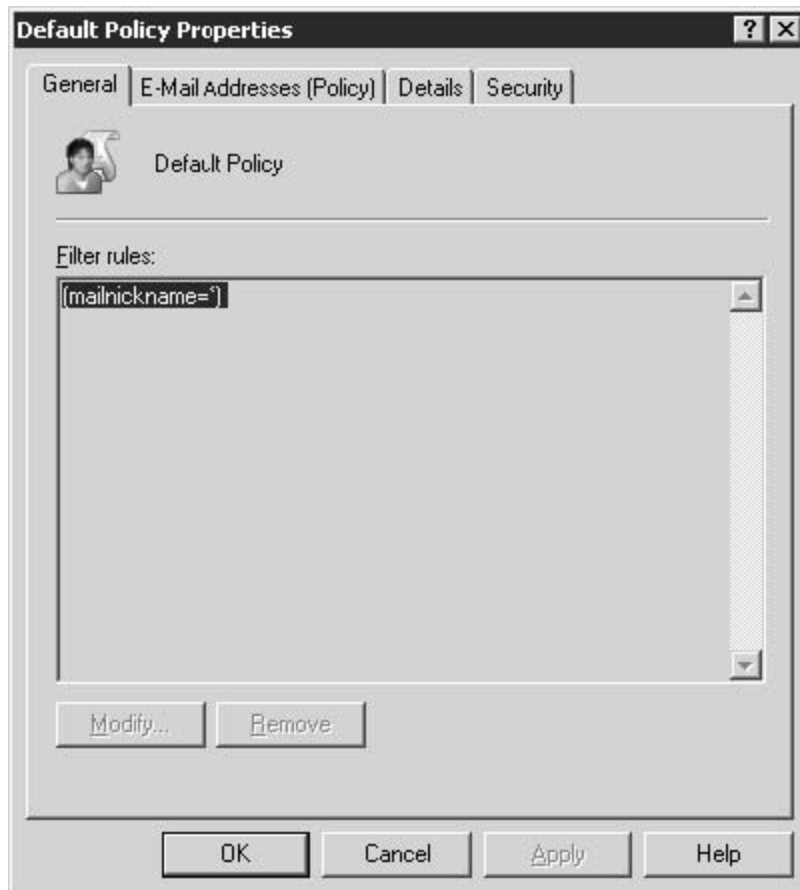


Figure 5.31 LDAP query associated with Default Recipient Policy, which selects all mail-enabled objects in Active Directory (mailnickname=*).

You work with your ISP to register the whizbang.com address and to install an MX record in the whizbang.com DNS zone so Internet clients can find the public interface of your Exchange front-end server. But if the front-end server gets an email message addressed to sally@whizbang.com, it rejects the message unless it finds that proxy address in Sally's account.

You can configure a recipient policy to assign a second SMTP address suffix of @whizbang.com to members of the Sales group using this procedure:

1. Right-click the **Recipient Policies** icon and select **New -> Recipient Policy** from the flyout menu. This opens the new Policy window, as shown in Figure 5.32.
2. Check the **Email Addresses** option and click **OK**. This opens the Properties window for the policy.
3. In the **General** tab, give the policy a name.
4. Select the **Email Addresses (Policy)** tab.
5. Click **New** to add a new email address.

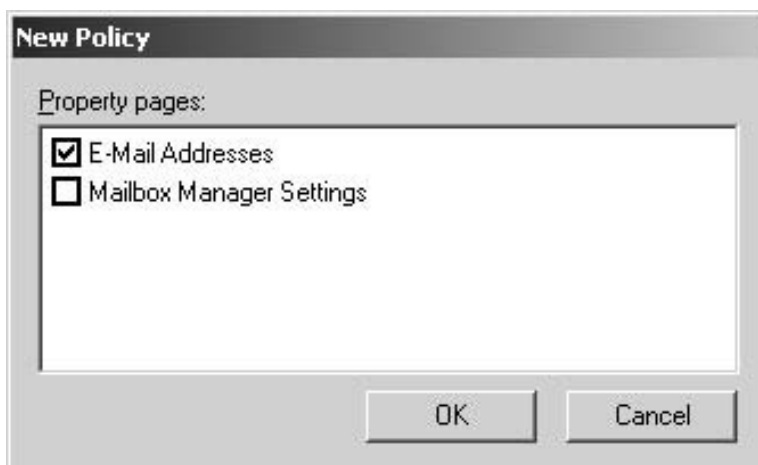


Figure 5.32 New recipient policy with selection for policy type, either Email Addresses or Mailbox Manager Settings. (Click on image for enlarged view.)

6. Select **SMTP Address** from the list of addresses and click **OK**.
7. In the SMTP Address window, enter the SMTP suffix for the domain, such as @whizbang.com. Figure 5.33 shows an example. Leave the **This Exchange Organization is responsible...** option selected.

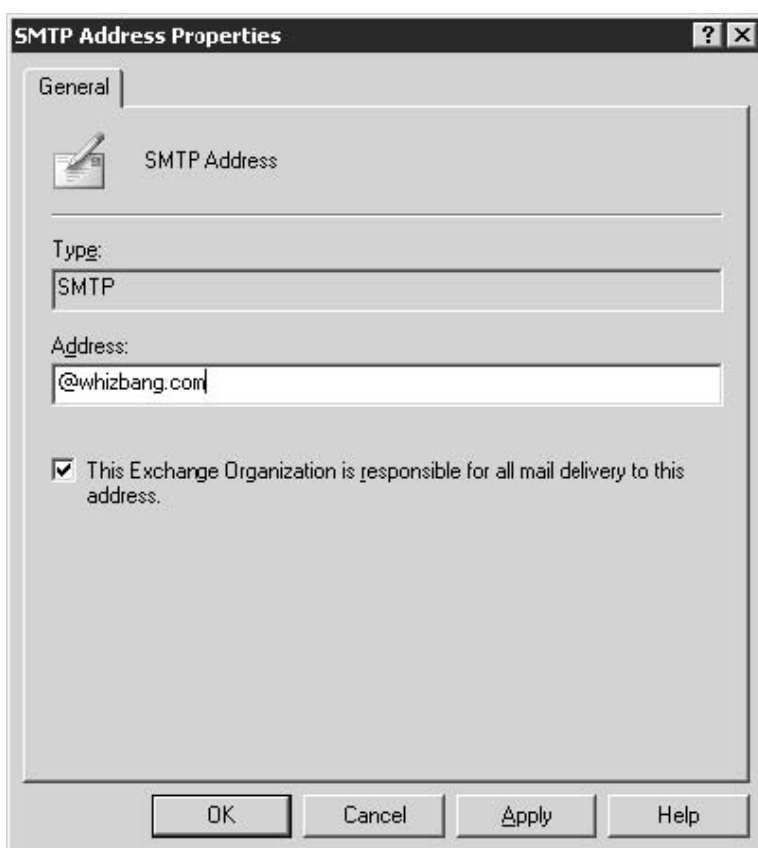


Figure 5.33 SMTP address assigned to new recipient policy. (Click on image for enlarged view.)

8. Click **OK** to save the address. The new address appears in the address list, as shown in Figure 5.34. Check the box to make the new address effective.
9. If you want the outbound mail sent by the salespeople to show company.com as the return address, highlight the address and click **Set As Primary**.
10. Click **OK** to save the new policy.
11. Double-click the new policy to open the Properties window.

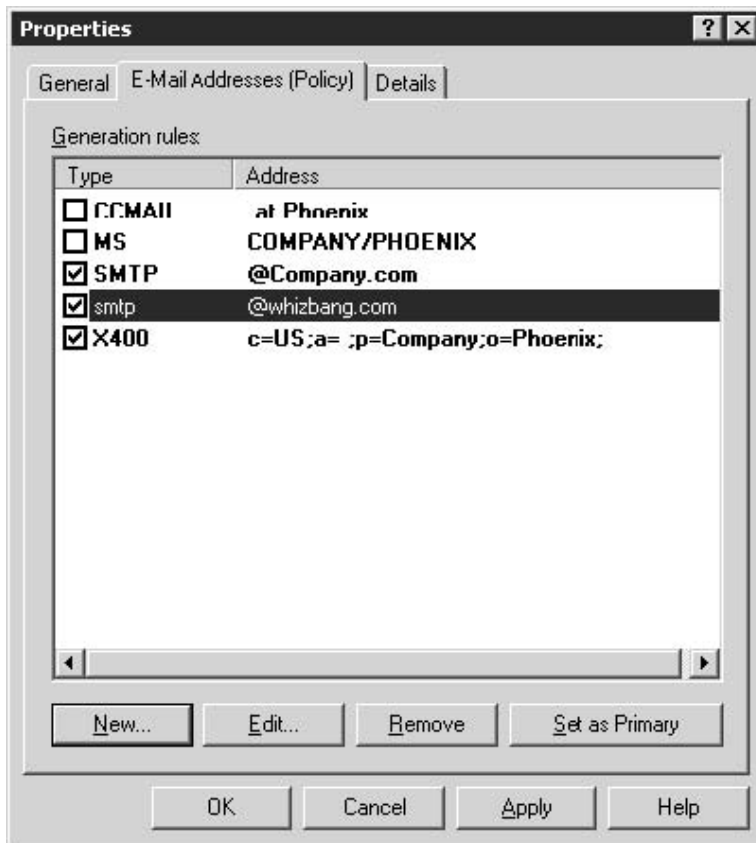


Figure 5.34 Proxy address changes done as the result of adding a new recipient policy in addition to the default policy. (Click on image for enlarged view.)

12. In the **General** tab, under **Filter Rules**, click **Modify**. This opens the Find Exchange Recipients window, as shown in Figure 5.35.

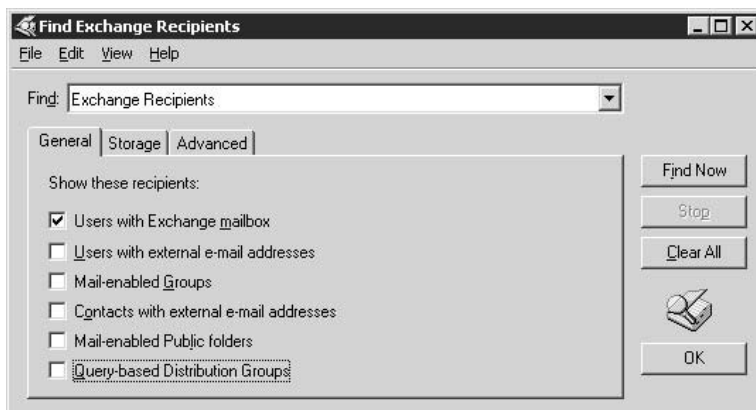


Figure 5.35 LDAP query builder limiting the selection to mailbox-enabled users. (Click on image for enlarged view.)

13. Uncheck all options except for **Users with Exchange Mailbox**.
14. Click the **Advanced** tab.
15. Click **Field** and then **Users**; then scroll down and select the **Member Of** option.
16. Leave the **Condition** field as **Is (exactly)**.
17. In the **Value** field, enter the distinguished name of the group that has members from the Sales department. You might need to create this group. For example, the entry might read

cn=sales,ou=groups,ou=phoenix,dc=company,dc=com.

(See Appendix A for information about distinguished names.)

18. Click **Add** to add this set of selection criteria under **Condition List**.
19. Click **Find Now** to check your selection criteria. The list of users in the **Search Results** field should match your expectations.
20. Click **OK** to save the filter.
21. Click **OK** to close the Properties window. You'll be prompted that the policy does not apply right away.
22. Click **OK** to acknowledge the warning and close the window.
23. Right-click the new policy and select **Apply This Policy Now** from the flyout menu.

The next time the Recipient Update Service fires, it applies the new proxy addresses on the targeted recipients and changes the existing addresses to a secondary addresses.

Multiple Recipient Policies

At this point, you should have two Recipient Policies, one you just created for the Sales group and the default. ESM displays the policies in the order that RUS evaluates them.

If you create several policies, stacked one on top of the other, RUS evaluates them in order, starting with the policy at the top of the list. If a selected target object does not fall within the LDAP filter criteria of the first policy, then RUS goes on to check the search criteria of the next policy. If the filter in the policy *does* include a particular object, though, then RUS applies that policy and no others.

You might have situations where you want to apply different email addresses to different groups of users. For example, the Sales department might want to publish email addresses using several different DNS domains, such as sales@companyinfo.com or info@newcompany.com. If you want a set of recipients to have multiple addresses, put all the required addresses into the policy that targets those users. If a recipient falls under several filter criteria, the first filter RUS finds that includes the recipient in the filter takes precedence. RUS ignores all other filter criteria for that recipient.

What happened to the M: drive?

The EXIFS (M: drive) feature has been disabled by default. If the feature is still needed, it can be assigned to an available drive letter with a registry setting.

Where's the Instant Messaging Server?

The Exchange Instant Messaging Service is being replaced by the Microsoft Office Real-Time Communications (RTC) server. It is no longer a component of the Exchange Server. For more information, see <http://www.microsoft.com/office/preview/rtcserver/>.

What is OMA?

Outlook Mobile Access and Exchange Server ActiveSync features, formerly found in Microsoft Mobile Information Server 2002, are now built-in with all Exchange Server 2003 Standard installations. Complementing the Outlook 2003 and Outlook Web Access mobile improvements, Outlook Mobile Access and Exchange Server ActiveSync help enable secure corporate e-mail on a range of mobile devices including browser-based mobile phones, Microsoft Windows Powered Pocket PC, and Microsoft Windows Powered Smartphone devices.

Adding this functionality to the core Exchange Server 2003 product reduces the need to deploy additional mobile server products in the corporate environment, thus lowering the total cost of ownership.

Why should I go to Exchange 2003 now?

There are several reasons. A few are:

1. Opportunity for Server Consolidation From Exchange 5.5 and Exchange 2000 because you can get more mailboxes on an Exchange 2003 Server.

2. Better security features. The server is secure by default and has added things like automatic logoff for an inactive OWA session, Connection filtering, and has more junk mail features like real-time blacklists.
3. Availability enhancements such as End-to-End Outlook Monitoring, Improvements in ESM, Mailbox Recovery Center, and a Recovery Storage Group.
4. Increase in Mobile device support for Pocket PC's, Pocket PC Phones and Microsoft Windows®-powered Smartphones.

What are the differences between Exchange 2000 and Exchange 2003?

Some features that are new in Exchange 2003 are:

- Volume Shadow Copy Service for Database Backups/Recovery
- Mailbox Recovery Center
- Recovery Storage Group
- Front-end and back-end Kerberos authentication
- Distribution lists are restricted to authenticated users
- Real-time Safe and Block lists
- Inbound recipient filtering
- Attachment blocking in Microsoft Office Outlook Web Access
- HTTP access from Outlook 2003
- cHTML browser support (i-Mode phones)
- xHTML (Wireless Application Protocol [WAP] 2.0) browser support
- Queues are centralized on a per-server basis
- Move log files and queue data using Exchange System Manager
- Multiple Mailbox Move tool
- Dynamic distribution lists
- 1,700 Exchange-specific events using Microsoft Operations Manager (requires Microsoft Operations Manager)
- Deployment and migration tools

For more information refer to the following resources:

What is the difference between Exchange 2003 Standard and Exchange 2003 Enterprise editions?

Standard Edition

- 16 GB database limit
- One mailbox store
- One public folder store
- NEW: Server can act as a front-end (post-Beta 2)

Enterprise Edition

- Clustering
- Up to 20 databases per server
- X.400 Connectors

Both Editions support features such as:

- Database snapshot
- OMA and ActiveSync
- AirMAPI
- Recovery Storage Group
- Exchange Management Pack for MOM
- **Note: It is not possible to in-place upgrade Exchange 2000 Enterprise Edition to Exchange 2003 Standard Edition.**

What's the difference between Exchange 2003 and Windows 2003?

Windows Server 2003 provides significant enhanced functionality that Exchange 2003 takes advantage of:

Outlook HTTP access

IIS 6.0 and Windows RPC Proxy service in Windows Server 2003 enable communication between Outlook 2003 and Exchange Server 2003 by means of HTTP. Outlook 2003 users can synchronize directly with the server running Exchange Server 2003 over a HTTP or HTTPS connection.

Internet protocol support

IIS 6.0 provides Exchange with its support for many common Internet access protocols that increase the flexibility of the operating system, such as HTTP, Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4), and Simple Mail Transfer Protocol (SMTP).

Active Directory

Windows provides Active Directory, upon which Exchange depends for user information, mail routing information, user authentication, and LDAP read and write functions.

Support for clustering

Exchange Server 2003 provides better support for clustering, which enables high availability of a company's infrastructure. Customers can choose to run up to 8-node clusters, with at least one passive node, when running Exchange 2003 on Windows Server 2003, Enterprise Edition. (In Windows 2000 Advanced Server, clustering was limited to two nodes, one active and one passive; if a company chose to run Windows 2000 Datacenter Server, clustering was limited to four nodes.)

Volume Shadow Copy service

This and Virtual Disk Service are part of a storage framework that provides heterogeneous interoperability of storage hardware, storage software, and applications. Exchange 2003 writes to the Volume Shadow Copy service on Windows Server 2003, reducing dramatically the backup and restore times for Exchange messaging environments. This enables IT departments to support greater numbers of users per server and reduces the total number of servers running Exchange in their environment.

Name a few configuration options related to mailbox stores.

Creating storage groups

Before I explain how to create additional message stores, you need to know about an architectural element that did not exist in Exchange Server 5.5 called storage groups. A storage group is designed to hold the actual database stores. Exchange 2000 and Exchange 2003 both let you have up to four different storage groups. Each of those storage groups can then contain up to five different databases, giving you a total of 20 potential databases per server.

Why you are allowed to create multiple storage groups if all they do is act as a container for the databases? The reason is that the storage groups do more than store databases. There are certain aspects of database maintenance that are performed at the storage group level rather than at the store level. Specifically, if you want to enable or disable circular logging, zero out deleted database pages or change the transaction log location or system path location, it must be done at the storage group level. The settings that you make then apply to every database within the storage group.

Because the system path and the transaction log path are both set at the storage group level, you can't just create a new store and start moving mailboxes to it should you run low on disk space. Doing so wouldn't save you any space at all because the two stores are in the same location along with the transaction logs. If you were running low on disk space you would need to create a separate storage group that's directed to a separate volume. Only then could you create a new store and start moving mailboxes to it and accomplish your goal of freeing some disk space.

To create a new storage group, open the Exchange System Manager and navigate to Administrative Groups | your administrative group | Servers | your server. Right click on the listing for your server and then select the New | Storage Group commands from the resulting shortcut menu. When you do, you will see a dialog box prompting you to enter a name for the new storage group, the system path and transaction log path. Microsoft recommends that you place the system path and the transaction log path both onto a fault tolerant RAID array, but on separate volumes. Click OK when you're done and the storage group will be created.

Next step: create a mailbox store

Next, you need to create a mailbox store within the new storage group. To do so, right click on the new storage group and select the New | Mailbox Store commands from the shortcut menu. You will see the new store's properties sheet. You will have to give the store a name. You also have the option of setting any other option that would normally be associated with a store, such as the store's policy. When you're done, click OK to create the store. When you click OK, Windows will ask you if you'd like to mount the store. Click Yes and the store will be mounted.

Now that you have created and mounted a new store, let's look at how to move a mailbox into it. Go to your original storage group and select the Mailboxes container. The System Manager will now display a list of the mailboxes that are contained within the store. Select the mailbox or mailboxes that you want to move, right click on them and select Exchange Tasks from the resulting shortcut menu.

After a brief delay, Windows will launch the Exchange Tasks Wizard. Click Next to bypass the wizard's Welcome screen. You will be asked which task you want to perform. Select Move Mailbox and click Next. You are now given the chance to select a server and a storage group / store. Make your selection and click Next.

The following screen will ask you what you want to do about any mailboxes that might be corrupt. Select the Create a Failure Report option and click Next. The wizard will prompt you for a start date and time and for a time when the operation should be terminated if it is not complete. Make your selections and click Next. Exchange will now move the selected mailboxes. When the process completes, click Finish to close the wizard.

What are System Public Folders? Where would you find them?

On the various networks that I have been involved in over the years, it always seems as though public folders are always either very heavily used or else not used at all. I've always taken this to mean that some administrators think that public folders are the greatest thing since sliced bread, while others either don't see the value in them or don't understand them.

A public folder is basically a repository for information, and can be used to store messages, files (as message attachments), calendars or contacts. The idea behind a public folder is that if your organization has information that everyone needs to access, it is sometimes easier to place that information in a public folder so that it is available through Outlook than to put it in a normal file share.

As you're probably aware, most Exchange Server-related tasks are performed through the System Manager. This isn't the case with public folders, however, which are created and accessed directly through Outlook

Create the folder

To create a public folder, open Outlook and expand the Public Folders container. Right click on the All Public Folders container and then select the New Folder command from the resulting shortcut menu. When you do, you will see a dialog box appear that asks you for three pieces of information.

First, you must enter a name for the new folder. Second, you must select the folder's contents. The folder's contents can be mail and post items, calendar items, contacts or just about any other type of data that Outlook recognizes. Finally, you must navigate through the public folder tree and select the new folder's location within the public folder hierarchy. Once you have done this, click OK and the new folder will be created.

Now that I have shown you how to create public folders, let's take a look at how you can manage a folder's permissions. Although you must create public folders through Outlook, you must set the folder's permissions through Exchange System Manager.

Set the permissions

When you open System Manager, navigate to Administrative Groups | your administrative group | Servers | your server | First Storage Group | Public Folder Store. Now, right click on the Public Folder Store container and select the Properties command from the resulting shortcut menu. When you do you will see the Public Folder Store Properties sheet. This properties sheet allows you to control the general behavior of the public information store. The main thing that I wanted to show you on this properties sheet is the Security tab. The Security tab sets up the permissions across the entire public folder store. This is where you can specify who should and should not be allowed to create or delete public folders. This is important because you don't want one of your users creating their own unauthorized public folders or deleting yours.

Although the Public Folder Store properties sheet allows you to create a broad set of permissions that apply to all public folders, you can also modify permissions on individual folders. That way, you can grant users the right to post content to one folder, but not to another.

To set the permissions on an individual public folder, expand the System Manager's Public Folder Store container and select the Public Folders container beneath it. All of the server's public folders will appear in the details pane. Now, right click on an individual public folder and then select the Properties command from the resulting shortcut menu. Doing so will open the folder's properties sheet.

Permissions over the folder are set through the properties sheet's Permissions tab. This tab contains two buttons: Client Permissions and Administrative Rights. If you click the Client Permissions button, you will be able to set up the rights that various users or groups have over the folder. Simple check boxes allow you to grant or revoke public folder specific rights such as create items, read items, create sub folder, folder owner, folder contact and folder visible.

You can also control whether users are allowed to edit and delete any items in the folder, only items that they have posted or no items at all. If this sounds a little complicated, you will be happy to know that Microsoft has created several pre-defined roles that you can select rather than applying individual permissions. For example, you can assign users the Author role, which would allow them to create and read items and to edit or delete their own posts.

As the name implies, the Administrative Rights button takes you to a dialog box that lets you control who is an administrator over the folder. There are also quite a few different advanced permissions that you can set for administrators. These permissions control the administrator's rights to do things like controlling access to the folder or modifying the folder itself. Generally speaking, these are settings that you would usually leave alone.

For the most part, working with public folders is simple. By default, Exchange admins have the right to create public folders. Everyone then has the right to post to newly created folders or to read items within the folders unless those permissions are changed.

Offline address lists use system public folders to contain the required address list information. Their associated public folders are created during the public store maintenance interval, and the content of the public folder is updated according to the **Update interval** that you specify on the **Properties** dialog box of each offline address list. By default, the Offline Address List (System) public folders are hidden from users. This procedure outlines how to view the system public folders.

Before You Begin

In a mixed environment where some users connect to Exchange 2003 or Exchange 2000 servers, and other users connect to Exchange 5.5 servers, you must have multiple address lists. Those users who connect to Exchange 5.5 need to use the offline address book that is generated by Exchange 5.5.

Procedure

To see the System public folders

1. In Exchange System Manager, expand the administrative group, and then expand the folders container.
2. Right-click the **Public Folders** container, and then click **View System Folders**.

How would you plan and configure Public Folder redundancy?

How can you immediately stop PF replication?

Exchange Public Folder Best Practices: Implementing Replication

Topic Last Modified: 2006-09-14

This article describes best practices for deploying and configuring public folder replication in Microsoft® Exchange 2000 Server and Exchange Server 2003. This article assumes that you have a good understanding of replication, the types of replication messages that Exchange Server uses, and sets of change numbers (CN sets). For a description of these concepts, see [Controlling Exchange Server 2003 Public Folder Replication](#).

Public folder replication in Exchange Server can be a resource-intensive operation. Replication requires network, CPU, and disk resources to operate. By implementing a solution that enables efficient public folder replication, especially in organizations with heavy public folder usage, you may greatly improve network, CPU, and disk load in your Exchange Server environment.

Generally, it is a best practice to minimize replication across the Exchange Server organization. By minimizing replication, you minimize the amount of data that travels over your network. You also minimize the CPU and disk resource load on your Exchange servers. Additionally, by minimizing replication, you can help ensure that multiple users are less likely to access different versions of data on multiple replicas. However, you should note that by minimizing replication, you decrease availability of the public folder data because fewer replicas of the folder are available to clients if a public folder store fails. If availability on a large scale is required for data in a specific public folder, you may require more replication.

Planning for Efficient Replication

The first step in determining a solution that enables efficient public folder replication is to understand how users use each folder in a specific hierarchy. Most of the time it makes sense to distribute the content and reduce replicas as much as you can. In this context, "distributing content" means breaking up content so that it will be aggregated on each public folder store and not replicated to the other public folder stores.

For example, consider a routing group that has four Exchange servers. If each server in that routing group contains a replica of the same folders, every time that a replication cycle runs, the changes in the content are replicated to all four servers. This replication implementation causes increased network load because of the increased SMTP traffic and increased CPU and disk

usage to process the replication messages. This replication implementation may make sense if all users in the routing group access a specific folder. However, if subsets of users access a specific folder, such replication is inefficient. In this example, you could save a significant amount of network, CPU, and disk load by distributing the content across the four Exchange servers and reducing the number of replicas.

You should note, however, that by distributing content across multiple replicas, you may increase the management overhead. In this example, load distribution will require more maintenance and monitoring than you would require for a single replica of the whole hierarchy. Therefore, be mindful of the effect on server management as you plan your replication solution.

In some organizations, the Schedule+ Free/Busy public folder is typically the most frequently accessed public folder. Therefore, you should pay special attention to how these folders are used.

In large enterprises with global facilities, it typically makes sense to replicate Schedule+ Free/Busy public folders according to region so that multiple replicas are available to local users, and large data replication traffic across wide area networks is minimized. This recommendation is optimal for organizations that have organized administrative groups according to regional local area networks.

If your Exchange Server infrastructure is not organized according to regional local area networks, a general best practice is to replicate the Schedule+ Free/Busy public folder from each administrative group to at least one server in each routing group. However, you should note that this best practice may not suit all deployments. You should always consider user access requirements and network latency when you plan your deployment.

Planning Public Folder Servers

The key question is will you have a dedicated public folder server, or whether to run the mail and public folder on the same Exchange 2003 machine? The answer depends on the size of your organization. For large companies separating public folder traffic from mailbox traffic is essential, while on small organization co-existence would be more cost effective.

Another consideration is how many public folders servers do you need? One for each of the main sites would be a good starting point. Clients at small sites could access public folders on the larger sites provided the network was fast enough.

Public Folder Migration Tool (pfMigrate)

Exchange 2003 has a new tool called pfMigrate that helps you to migrate both system folders and public folders from Exchange 5.5. The key concept is Replica. You can use pfMigrate to create replica folders on the new server. Unlike Exchange 5.5, you do not need to set a home server for a public folder in Exchange Server 2003. This is because Active Directory uses the multiple master model whereby any server has a read write copy of the public folder information.

With pfMigrate you can carry out a trial run and produce a report; if you like what you see then you can run the tool again and actually migrate the public folders.

Installing pfMigrate

pfMigrate.wsf is actually a command-line script rather than an executable. You will find the script on the ExchangeCD\Support\ExDeploy folder. Alternatively, you can run the script through the Exchange Deployment Tools which you find on the first screen of the setup menu.

Trap:

After you run pfMigrate, only the hierarchy of the system folders and public folders is migrated immediately. Be patient and wait for replication for the actual contents of the folders to be migrated.

ADC Agreements

You can use the Active Directory Connector to create agreements to synchronize and migrate public folders from Exchange 5.5 to Exchange 2003. These are the same principles that you used to make ADC agreements for mailboxes.

How can you prevent PF referral across slow WAN links?

What types of PF management tools might you use?

What are the differences between administrative permissions and client permissions in PF?

Applies to: Exchange Server 2007, Exchange Server 2007 SP1 **Topic Last Modified:** 2007-09-11

You can configure public folder permissions for both administrators of Microsoft Exchange Server 2007 or for users of client programs such as Microsoft Office Outlook 2007. Public folder permissions consist of various access rights that specify the level of control a client user or administrator has over a public folder or public folder hierarchy.

This topic includes the following information about public folder permissions:

- The access rights and predefined roles (which consist of specific access rights) that you can configure for client users. The access rights that you can configure for administrators.
- Links to the management tasks you can perform for client users and administrators.

Client User Access Rights and Roles

In Exchange 2007, you use the Exchange Management Shell to configure the permissions for the users who use client programs such as Outlook to access public folders. Whether you want to manually select the access rights or use predefined roles that contain specific access rights, you will use the **Add-PublicFolderClientPermissions** cmdlet to perform the tasks.

The following is a list of client user access rights (followed by a table that shows the predefined permission roles):

- **ReadItems** The user has the right to read items within the specified public folder.
- **CreateItems** The user has the right to create items within the specified public folder and send e-mail messages to the public folder if it is mail-enabled.
- **EditOwnedItems** The user has the right to edit the items that the user owns in the specified public folder.
- **DeleteOwnedItems** The user has the right to delete items that the user owns in the specified public folder.
- **EditAllItems** The user has the right to edit all items in the specified public folder.
- **DeleteAllItems** The user has the right to delete all items in the specified public folder.
- **CreateSubfolders** The user has the right to create subfolders in the specified public folder.
- **FolderOwner** The user is the owner of the specified public folder. The user has the right to view and move the public folder, create subfolders, and set permissions for the folder. The user cannot read items, edit items, delete items, or create items.
- **FolderContact** The user is the contact for the specified public folder.
- **FolderVisible** The user can view the specified public folder, but cannot read or edit items within the specified public folder.

The following table lists the predefined public folder client access roles and the access rights that are included in each role. The table headers reflect the access rights listed previously in this document.

 Note:										
The FolderOwner access right and the Owner role have different permissions as shown in the following table.										
Role	CreateItems	ReadItems	CreateSubfolders	FolderOwner	FolderContact	FolderVisible	EditOwnedItems	EditAllItems	DeleteOwnedItems	DeleteAllItems

None						X				
Owner	X	X	X	X	X	X	X	X	X	X
PublishingEditor	X	X	X			X	X	X	X	X
Editor	X	X				X	X	X	X	X
PublishingAuthor	X	X	X			X	X		X	X
Author	X	X				X	X		X	
Non-EditingAuthor	X	X				X				
Reviewer		X				X				
Contributor	X					X				

Administrator Access Rights

In the release to manufacturing (RTM) version of Exchange 2007, you can only use the **Add-ExchangeAdministrator** cmdlet to grant public folder administrative rights to a user.

In Exchange 2007 Service Pack 1 (SP1), there are two methods you can use to grant public folder administrative rights to a user:

- Use the **Add-ExchangeAdministrator** cmdlet or the Add Exchange Administrator wizard to add a user to the Public Folder Administrator role.
- Use the **Add-PublicFolderAdministratorPermission** cmdlet to grant or deny specific rights to public folders.

The following table describes the differences between the rights that are granted by the Public Folder Administrator role and the rights that are granted by using the **Add-PublicFolderAdministratorPermission** cmdlet.

Exchange Public Folder Administrator role	Add-PublicFolderAdministratorPermission
The user can create top-level public folders.	The user cannot create top-level public folders.
The user is granted AllExtendedRights to public folders.	The user can be granted or denied specific rights to public folders.
The user can administer any top-level public folder, child public folder, and system public folders in the public folder tree. In addition, this user's access rights cannot be revoked by using the Remove-PublicFolderAdministratorPermission cmdlet.	The user can be granted the right to administer specific top-level public folders and specific child public folders. However, the user's access rights can be revoked by using the Remove-PublicFolderAdministratorPermission cmdlet.

By default, when you create a top-level public folder, users who have permissions that are granted by specific Exchange administrator roles and Microsoft Windows security groups are automatically added as administrators to that public folder because of the group's inherited rights. The following list shows which roles and groups automatically have administrative rights to a new top-level public folder, including the specific access rights that are granted to each:

- Exchange administrator roles:
 - Exchange Public Folder Administrator (granted AllExtendedRights)

Note:

This role is available only in Exchange 2007 SP1.

- Exchange Server Administrator (granted AllExtendedRights)
- Exchange Organization Administrator (granted AllExtendedRights)
- Exchange View-Only Administrator (granted ViewInformationStore)
- Windows security groups:

- Enterprise Admins (granted AllExtendedRights)
- Administrator (granted AllExtendedRights)
- Domain Admins (granted AllExtendedRights)

The following list describes the standard set of administrative access rights that can be set on a public folder:

- **None** The administrator does not have any rights to modify public folder attributes.
- **ModifyPublicFolderACL** The administrator has the right to modify client access permissions for the specified folder.
- **ModifyPublicFolderAdminACL** The administrator has the right to modify administrator permissions for the specified public folder.
- **ModifyPublicFolderDeletedItemRetention** The administrator has the right to modify the Public Folder Deleted Item Retention attributes (*RetainDeletedItemsFor*, *UseDatabaseRetentionDefaults*).
- **ModifyPublicFolderExpiry** The administrator has the right to modify the Public Folder Expiration attributes (*AgeLimit*, *UseDatabaseAgeDefaults*).
- **ModifyPublicFolderQuotas** The administrator has the right to modify the Public Folder Quota attributes (*MaxItemSize*, *PostQuota*, *PostWarningQuota*, *UseDatabaseQuotaDefaults*).
- **ModifyPublicFolderReplicaList** The administrator has the right to modify the replica list attribute for the specified public folder (*Replicas*).
- **AdministerInformationStore** The administrator has the right to modify all other public folder properties not defined previously.
- **ViewInformationStore** The administrator has the right to view public folder properties.
- **AllExtendedRights** The administrator has the right to modify all public folder properties.

you have to distinguish the 3 different permission types for public folder.

to clarify from microsoft>

Client permissions

These settings control who can use client applications to access folders and messages. By default, all users have permissions to read and write content in the public folder. You can change permissions for all users or create different permissions for specific users. The default client permissions do not include the Exchange administrative roles (Exchange Full Administrators, Exchange Administrators, or Exchange View Only Administrators).

Depending on the type of public folder that you are working with, you may see different forms of the client permissions.

Folders in the Public Folders tree use MAPI permissions.

Folders in general-purpose public folder trees use Windows 2000 Server permissions.

Directory rights

These settings are normal Active Directory permissions, and control who can change the e-mail-related attributes of a mail-enabled public folder. Exchange stores these attributes in Active Directory, in the public folder's directory object in the Microsoft Exchange System Objects container. The default directory permissions include extensive permissions for the domain local Administrators group. Normally, any user that you have assigned to one of the Exchange administrative roles is a member of this group.

Administrative rights

These settings control who can use Exchange System Manager (or a custom administration program) to change the replication, limits, and other settings for a public folder. Some of these permissions are inherited from the public folder store and include permissions for the Exchange administrative roles. These permissions are Windows 2000 Server permissions, although they reside only in the public folder store.

How can you configure PF replication from the command prompt in Exchange 2003?

Replicating Public Folders from Exchange 2000 to Exchange Server 2003

Just as the mailboxes are migrated from one set of Exchange 2000 servers to another set of Exchange Server 2003 systems, the public folders should be replicated before retiring the old Exchange 2000 servers. Previously, this procedure involved a manual replication of folder hierarchy, which could prove to be a tedious process. Microsoft addressed this drawback with a new utility called PFMigrate, which is accessible via the Exchange Deployment Tools. PFMigrate can create public and system folder replicas on new systems, and remove them from old servers. The following procedure outlines how to use PFMigrate to migrate from an Exchange 2000 Server to an Exchange Server 2003 system:

1. Open a Command Prompt (select Start, Run; type `cmd`; and press Enter).
2. Type `cd D:\support\Exdeploy` and press Enter.
3. To create a report of current public folder replication, type the following:

```
pfmigrate.wsf /S:OLDSEVERNAME /T:NEWSEVERNAME /R /F:c:\LOGNAME.log
```

This generates a report named LOGNAME.log on the C: drive. OLDSEVERNAME should be the name of the Exchange 2000 system, and NEWSEVERNAME should be the new Exchange Server 2003 system.

Copyrights

Migrating to Exchange Server 2003 Using the Move Mailbox Method

4. To replicate System Folders from the Exchange 2000 server to the Exchange 2003 server, type the following:

```
pfmigrate.wsf /S:OLDSEVERNAME /T:NEWSEVERNAME /SF /A /N:100  
/F:c:\LOGNAME.log
```

5. To replicate Public Folders from Exchange 2000 to Exchange Server 2003, type the following:

```
pfmigrate.wsf /S:OLDSEVERNAME /T:NEWSEVERNAME /A /N:100 /F:c:\LOGNAME.log
```

6. After all public folders have replicated, the old replicas can be removed from the Exchange 2000 Servers by typing the following, as illustrated in Figure 16.11:

```
pfmigrate.wsf /S:OLDSEVERNAME /T:NEWSEVERNAME /D
```

C:\support\Exdeploy> pfmigrate.wsf

What are the message hygiene options you can use natively in Exchange 2003?

What are the configuration options in IMF?

With Exchange 2003 Service Pack 2 Microsoft introduced their spam detection tool "Intelligent Message Filter" (IMF) as a built in component of Exchange. Previously it was available as a optional extra.

This article explains how to enable the feature, and then working with the results. While it is built in, it is not enabled by default.

Note: If you are using Small Business Server with the POP3 connector, then you cannot use IMF. The POP3 connector bypasses the IMF scanner. To use IMF you will need to get your email delivered directly by SMTP.

Enabling IMF

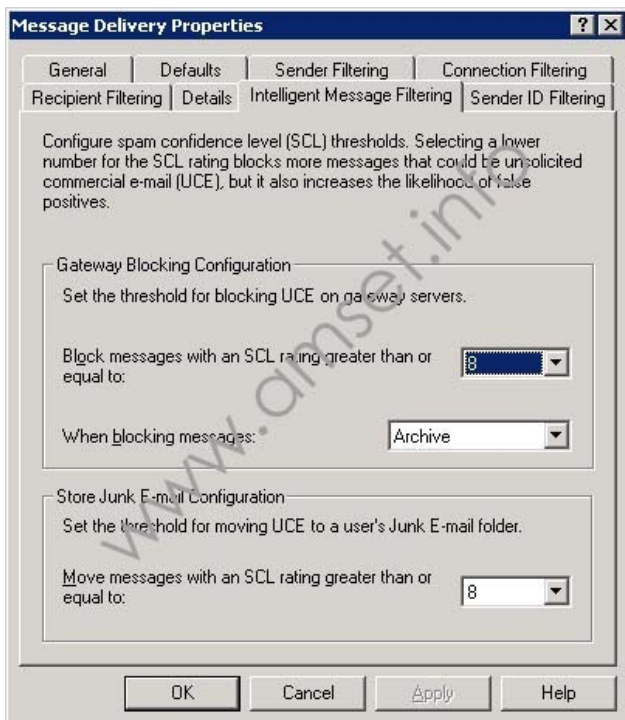
There are two steps to enable the Intelligent Message Filter. Many people carry out the first, but fail to do the second.

Step One - Enable the option in the Exchange Organisation

Exchange System Manager, Global Settings. Right click on Message Delivery and select Properties.

Click on the tab "Intelligent Message Filtering". Change the option in the middle from No Action to Archive (you should run with archive initially to ensure that it isn't catching legitimate email). Leave the other settings alone for now.

You could leave the setting to "No Action" and have the system simply record numbers. If you simply enable the option on the SMTP Virtual Server (see step 2) then you can monitor what the messages are being scored as. This will give you an idea as to whether you have a spam problem that IMF might be able to help with.



What do the numbers mean?

There are two sets of numbers.

Gateway Blocking Configuration - this is where the messages will be blocked at the server, and the users will not even see them.

Store Junk E-mail Configuration - this is where the messages will be delivered to the user's Outlook and stored in their Junk Email folder (Outlook 2003 in cached mode only, or OWA).

If you set both numbers the same, then no spam or suspected spam email will be delivered to the user's Outlook folder - it will be archived or deleted.

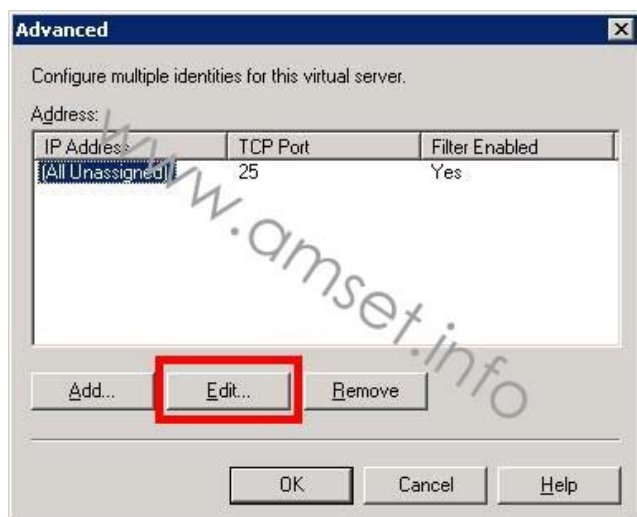
Gateway should always be higher or the same as Store Junk Email. Never lower.

Step Two - Enable the option on the SMTP Virtual Server.

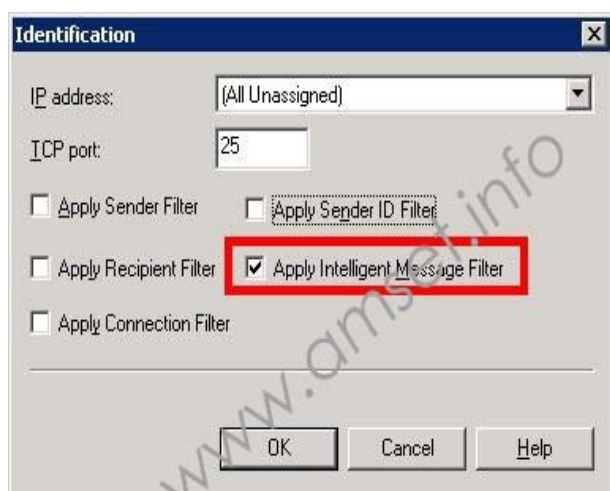
Exchange System Manager, Servers, <your server>, Protocols, SMTP. Right click on the Default SMTP Virtual Server and choose Properties. On the first tab click on "Advanced...".



On the next box, click "Edit...".



Enable the option "Apply Intelligent Message Filter".



The other options should be left alone. "Apply recipient filter" is used with the filter unknown recipients option, which is explained [here](#).

For this change to take effect, you need to restart the SMTP Service. You may want to wait and make the change to enable automatic updates first, as that requires a restart as well.

Configure IMF to Update

Like antivirus applications, a spam detection application needs to be regularly updated. IMF is not enabled by default to update automatically, but can be quickly and easily via a registry change.

Open the registry editor and move down to the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange

Create a new DWORD in the root of that location (usually by right clicking on Exchange) called ContentFilterState

Give the new DWORD key a value of 1 and close the registry editor.

The update comes down with automatic updates, however make sure that you have updated to Microsoft Update so that you get non Windows updates.

If you are using Windows Server Update Services (WSUS), then make sure that you have enabled Exchange server as a product to download updates for, and updates for IMF will be distributed through that mechanism.

Once you have made the change, restart the SMTP Service in the Services applet.

There is more information on the update process in MS KB article 907747

(<http://support.microsoft.com/default.aspx?kbid=907747>)

Monitoring the IMF

You can easily monitor how many messages the filter is blocking (or would block if no archiving settings are set) by using perfmon.

Click Start, Run and type perfmon.

The performance object that you want is "MSEExchange Intelligent Message Filter"

You can select all of the objects if you wish, however unless you are under heavy load, the top one (% of UCE Messages scanned in the last 30 minutes) and the LAST one (UCE Messages Acted Upon/sec) don't tend to provide much information of interest.

\\SERVER2	
MSExchange Intelligent Message Filter	
% UCE of Messages Scanned in the previous 30 minutes	_Total 0
% UCE out of Total Messages Scanned	23.958
Messages Scanned for UCE/sec	0.000
Total Messages Assigned an SCL Rating of 0	67
Total Messages Assigned an SCL Rating of 1	17
Total Messages Assigned an SCL Rating of 2	18
Total Messages Assigned an SCL Rating of 3	11
Total Messages Assigned an SCL Rating of 4	7
Total Messages Assigned an SCL Rating of 5	12
Total Messages Assigned an SCL Rating of 6	4
Total Messages Assigned an SCL Rating of 7	10
Total Messages Assigned an SCL Rating of 8	40
Total Messages Assigned an SCL Rating of 9	6
Total Messages Scanned for UCE	192
Total UCE Messages Acted Upon	46
UCE Messages Acted Upon/sec	0.000

Viewing the Messages in the IMF Archive

If you have set the IMF system to archive your messages, rather than block or delete them, then you need some way of checking those messages.

By default, the messages are stored in \\Exchsrvr\\Mailroot\\vsi 1\\UceArchive as msg files. These can be easily viewed via Outlook Express or dragging and dropping in to a notepad document.

However direct access like that limits your options for managing the archive. Instead you could use a third party option to provide a simpler interface.

Web Page

Originally written for the bolt on version of IMF, a set of ASP pages provides a easy to use interface to view the messages, and resubmit them for delivery to the end user. If you have already deployed an SSL certificate protected web site, then you could add these pages to the site. That would allow an administrator or other trusted person to check the messages remotely. To control access, simply put the pages on to an NTFS partition and then change the security settings of the folder to allow just those who should have access.

http://hellomate.typepad.com/exchange/2004/06/imf_archive_man.html

When you are using this application, if you get errors about "The HTTP headers are already written to the client browser" then go in to IIS Manager, find the virtual directory that has been created. On the "Application Settings" click on configuration, then the "Options" tab. Select the option "Enable Buffering" and then Apply/OK out.

Drop in to a command prompt and type IISRESET.

Utilities

There are a couple of free utilities that can be used as well. These will mean sharing the UCE folder out for remote access, or allowing access to the server.

IMF Archive Manager: <http://www.gotdotnet.com/workspaces/workspace.aspx?id=e8728572-3a4e-425a-9b26-a3fda0d06fee>

IMF Companion: <http://stoekenbroek.com/imfcompanion/default.htm> (watch for Pop ups)

More Scripts and Reporting

Glen Scales has a collection of scripts for IMF available here: <http://www.outlookexchange.com/articles/glenscales/imfrep1.asp>

View the Spam Confidence Level of Messages in the Archive

Each message is given a spam confidence level (SCL). The level is then used by Exchange to decide what to do with the message.

You can get the SCL level entered in to the header of the email messages sent in to the archive via a registry change.

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Exchange\\ContentFilter

Right click on ContentFilter and choose New and select DWORD Value.

Enter the key name as ArchiveSCL

Give the key a value of 1

To disable the option, change the value to 0 or delete the key.

Viewing the SCL Level of All Messages

Microsoft have stated that it isn't possible to expose the SCL level in the headers for all email messages as it does for messages in the archive. That isn't to say that it cannot be done.

An Outlook configuration file has been posted to the MS Exchange Team blog, which uses a custom form to expose the SCL level.

<http://msexchangeteam.com/archive/2004/05/26/142607.aspx>

This is a client side setting.

If you want server side, then you will have to look to third parties.

IVASOFT have produced ShowSCL as freeware. This allows you to see the SCL as a column in Outlook.

<http://www.ivasoft.biz/showscl.shtml>

Changing the Archive Location

If you want to store the archived messages in another location, then you can make a change to the registry to change it.

Create the folder first.

Then open your registry editor and go to HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\ContentFilter

Right click on ContentFilter and choose New, String Value.

Enter ArchiveDir as the key value.

Enter the full path to the new folder as the string data.

If you have already started using a tool to manage the archive location, don't forget to change that.

Antivirus Scanning

Ensure that your antivirus application is not scanning the archive folder. On access scanners can cause problems when it comes to viewing messages due to the way that they hold the file open. Messages with viruses may well be caught by this tool.

White Listing

One of the weaknesses of IMF is the lack of white list capability. This is where you can tell IMF to allow an email through, no matter what it scores.

The only white listing that is natively supported is via IP address. This is set elsewhere in Exchange System Manager.

Open Global Settings, then Message Delivery. Right click on Message Delivery in the left pane and choose Properties. Click on the tab Connection Filtering. The last option on that tab is the global Accept and Deny configuration. Choose the "Accept..." button and enter the IP addresses of the servers you want to bypass IMF.

If you want to white list internal resources, then a better option is to setup a second SMTP virtual server. IMF is enabled on a per virtual server basis.

Give the Exchange server an extra internal IP address. Then configure the existing SMTP virtual server to use only the original IP address. Create a new SMTP virtual server through Exchange System Manager, in Servers, <your server>, Protocols, SMTP. Right click on SMTP and choose New, Virtual server.

Fix the IP address of this new virtual server so that it doesn't conflict with the existing one.

Excluding users from IMF filtering.

Microsoft have released a hotfix for IMF to allow certain users to be excluded from IMF scanning.

This hotfix is one that you have to phone Microsoft support to get.

More information: <http://support.microsoft.com/default.aspx?kbid=912587>

Removing IMF v1.

If you had version 1 of IMF installed on your server, then it needs to be removed before installing Service Pack 2 for Exchange 2003.

There are two ways to remove IMF v1.

1. Use Add/Remove Programs.
If the tool doesn't appear in Add/Remove programs, but you have the original installation file, then you can simply reinstall it and then remove it.
It only appears in Add/Remove programs under the user account that it was originally installed by.
2. Manual removal.

Manual Removal of IMF v1

1. Stop all Exchange services, including the Information Store, System Attendant, SMTP, services, plus any Exchange antivirus applications.
2. Rename the folder "MSCFV1" in C:\Program Files\Exchsrvr\bin
3. Rename the file C:\Program Files\Exchsrvr\bin\ContentFilter.dll file
4. Open Regedit and browse to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange key.
5. Export a copy of that key for backup purposes.
6. Delete the "ControlFilterVersion" subkey from the registry.
7. Restart the server.
8. Install/Reinstall Exchange 2003 SP2.

Download: <http://www.microsoft.com/downloads/details.aspx?familyid=B1218D8C-E8B3-48FB-9208-6F75707870C2&displaylang=en>

What are virtual servers? When would you use more than one?

Introduction to Virtual Servers in Exchange Server 2003

Finding Microsoft's Virtual Servers must be one of the longest 'drill downs' in the Exchange 2003 System Manager. It's as though one of Exchange server's most important configuration settings is hidden away, rather than being visible as a top level folder.

Topics for Virtual Servers in Exchange Server 2003

- [Explaining Virtual Servers](#)
- [How to Configure a Microsoft Virtual SMTP server](#)
- [Summary](#)

Explaining Virtual Servers

Windows Exchange Servers use the word 'Virtual' in many contexts. To begin with, one physical machine can act as a server for several Virtual SMTP domains, for example ourcomp.com and mergecomp.net. Moreover, in addition to SMTP, one Exchange Server can also control Virtual servers for IMAP4, NNTP and POP3. From another point of view, you could interpret these Exchange Virtual servers as aliases for physical folders in Microsoft's IIS.

In a completely different context, the term Virtual Server is used in clustering. The Outlook clients connect not to the individual Exchange 2003 nodes, but to a Virtual server with a virtual IP address.

How to Configure a Virtual SMTP server

Opposite is a diagram to help you navigate to the various Virtual Servers folders. Once you have found your Exchange 2003 server object, expand the Protocols folder. Each protocol has its own Virtual server. SMTP for MAPI clients (Outlook), HTTP is for OWA (Outlook Web Access).

We are most interested in the Default SMTP Virtual Server. As its name suggests, this is the container where you check settings for regular SMTP mail. (See this SMTP server object at the very bottom of the screen shot.)

SMTP Virtual Server

- [General Tab](#) - For Connection Filter and Port Numbers
- [Access Tab](#) - For Permissions
- [Messages Tab](#) - For Limits
- [Delivery Tab](#) - DNS Settings

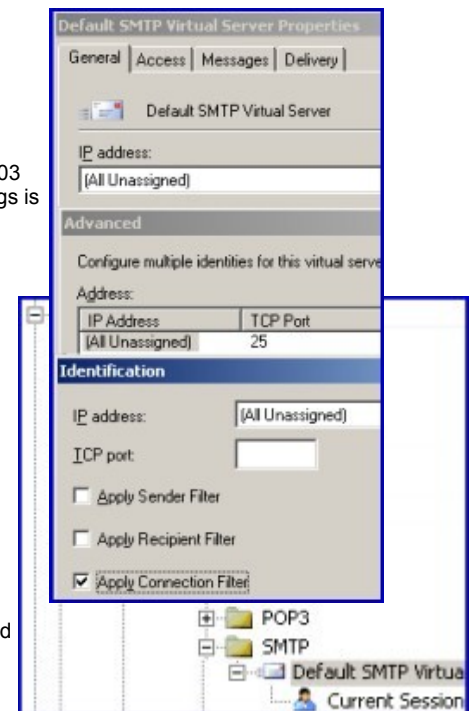
General Tab - Filter

One of the most important jobs in the Virtual Server is to configure any Filters that you set at the Global Settings, Message Delivery Tab. [See Global Settings here.](#)

To find the screen shot opposite click on the Advanced Tab next to the IP address. Select the IP address and Edit, now the Identification dialog box will appear, see diagram opposite. At last you can check: Apply Sender, Recipient or Connection Filter.

General Tab - Port Numbers

Rather like IIS, each SMTP Virtual server needs a unique combination of IP address and Port number. Here are the common Exchange port numbers:



	Default	Secure Port
HTTP	80	443
IMAP4	143	993
NNTP	119	563
POP3	110	995
SMTP	25	25

Access Tab

The access tab is where you configure authentication. Who will be allowed to use your SMTP Virtual server? Authenticated users - yes, but anonymous users? I think not, but you decide.

Messages Tab

The first section deals with setting limits - if any. For example, what would be the maximum number of recipients for your company's emails?

The lower section invites you to configure accounts to hold NDR (non deliverable reports). This is where you troubleshoot the location of the BadMail folder and the Queue directory.

Delivery Tab

As ever, DNS plays a central role in name resolution. Most likely your servers are registered on the internet as being authoritative for your email domain. This involves MX (Mail exchange) records on the InterNic servers that point to your Exchange 2003 server.

The other side of the DNS coin is that your server must be able to deliver outgoing email. If your server is (rightly) protected by a firewall delivering external email can be an extra challenge. The answer is to forward the name resolution to a Smart host on the outside of the firewall.

[See more on MX Records and DNS here.](#)

Reverse DNS

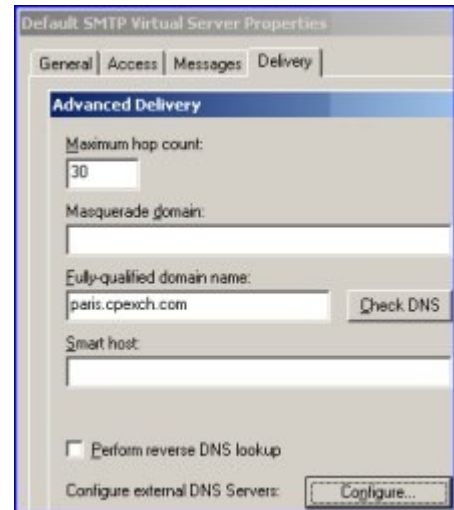
Configuring, Perform reverse DNS lookup, seems like a great idea to prevent spammers spoofing addresses in their evil emails. However, everyone that I have talked to has found that it slows down the system so much, that they put Reverse DNS lookup in that pigeon hole: 'more trouble than it's worth'.

Name some of the SMTP Virtual Server configuration options.

What is a Mail Relay? Name a few known mail relay software or hardware options.

A computer that is running Microsoft Exchange Server 2003 or Microsoft Exchange 2000 Server can be configured as a mail relay. Therefore, mail that is sent to another domain or from another domain can be forwarded to the destination by your Exchange computer. However, some issues may occur if your Exchange computer or an account on your Exchange computer is configured as an open mail relay. Additionally, some issues may occur if the mail relay is not correctly configured.

An Exchange computer that is configured as an open mail relay may be used to send unsolicited commercial e-mail, also known as spam. If other mail servers identify your Exchange computer as an unsolicited commercial e-mail server, your Exchange computer may be added to block lists. Therefore, you may have trouble when you send mail to other domains. To



resolve this issue, you must reconfigure your Exchange computer so that is not an open mail relay. Then, you must remove your Exchange computer from the block lists.

If your Exchange computer is not an open mail relay, an account on your Exchange computer may be used to send unsolicited commercial e-mail. Therefore, you must prevent someone from using the compromised account.

This article describes the symptoms of mail relay issues and includes steps to correct the configuration of your Exchange computer.

There are two parts of the Exchange that can make your Exchange server an open relay, the Default SMTP Virtual Server and SMTP connectors. You need to check both to ensure that you haven't configured them wrongly and turned your machine in to a spammers target.

Default SMTP Virtual Server

To check or correct the configuration of the Default SMTP Virtual Server:

1. Start Exchange System manager (ESM)
2. Expand Servers, <your server>, Protocols, SMTP.
3. Right click on "Default SMTP Virtual Server" and choose Properties.
4. Click on the "Access" Tab.
5. There are four buttons, click on "Relay..." at the bottom.
6. Ensure that "Only the list below" is enabled and the list is empty.
7. If you don't have users sending email through your email server with Outlook Express or another POP3 client then you can disable "Allow all users that successfully authenticate to relay regardless of the list above".
8. Apply/OK until all windows are closed.

SMTP Connections

1. Start ESM, then open Connectors.
2. Right click on each SMTP Connector in turn and choose Properties.
3. Click on the "Address Space" tab.
4. If you have a "*" in the address list, check that "Allow messages to be routed to these domains" is not enabled.
5. Apply/OK until all windows are closed.

Once you have made the changes, restart the SMTP server service and then repeat the telnet test above to ensure that you have closed everything.

Q: I don't see Admin and Routing Groups

A: The display of Admin and Routing groups isn't enabled as default. You need to enable it by hand.

Right click on your organisation name right at the top of ESM and choose Properties. Enable both boxes. Apply/OK and you should see the extra options.

Q: What happens if I don't take the * out of "Address Space".

A: All of your email is sent out via the ISP email server. While this isn't a problem, some people prefer to send most of their email direct.

Q: How can I find my ISPs Smart Host?

A: Look on their web site for the SMTP server. Another good trick is to look for their instructions for Outlook Express. This will usually have their SMTP server listed. Otherwise you may have to call them to find out what it is. While you are on the phone, check whether you need to authenticate when sending only.

Q: My ISP requires authentication to use their SMTP server

A: You need to add a username and password to the SMTP configuration. On the properties of the connector click on the "Advanced" tab. Click on the "Outbound Security" button. Change from anonymous to basic authentication. Click on the "Modify" button and enter the username and password as required.

Q: Why not specify the smart host in the SMTP virtual server?

A: While this option would work if you wanted to send all email out through the ISP email server it can cause problems. The key issue is if you have more than one Exchange server. Configuring a smart host on the SMTP virtual server breaks replication between the servers.

Q: I already have a connector to send email through our front-end server/spam server.

A: If you are using a third party server then you will need to look at the configuration to see how to direct email to another

machine.

If you already have a connector to route email through a front-end server then add the new connector as indicated above, but only add the Front-End server in "Local Bridgeheads".

Q: Is this an alternative to getting reverse DNS configured?

A: No - you should still get your ISP to make a reverse DNS entry for you if possible. This is good practise for a machine connected to the Internet. We have more information on configuring your DNS [here](#).

Q: How can I use a connector to bypass my ISPs block on SMTP traffic and use a third party SMTP Server? I don't see where I can set the port.

A: If you need to use an alternative port for SMTP traffic, then adjust the SMTP virtual server first. Another option would be to create another SMTP virtual server, on the same IP address as your main server. Then change its port. Once set, change the SMTP virtual server being used as the bridgehead in the SMTP Connector. By using an additional SMTP virtual server you can leave the default on port 25, which is good for use with additional Exchange servers.

Q: Can I use more than one SMTP Connector with the wildcard?

A: If you have access to two SMTP server that you can relay email through then you could add both on separate SMTP virtual servers. Both SMTP connectors would need to have the cost set as *. However you could also set both smart hosts on the same connector separated by a semi-colon (as indicated above).

What is a Smart Host? Where would you configure it?

How can I configure an IIS computer to be a Smart Host for my Exchange Server?

It may be necessary to configure a Windows 2000 server to relay or act as a smart host for security reasons, such as in a perimeter network scenario (also known as DMZ, demilitarized zone, and screened subnet) when you do not want to have a server that participates in domain security available on the Internet or you do not need the full functionality that an Exchange server provides to do e-mail for CDO and list serve-type applications.



1.18.1 Step 1: Verify the Installation of the SMTP Service

1. In Control Panel, open Add/Remove Programs, click Add/Remove Windows Components. Click the Internet Information Services (IIS) component, click Details, and then verify that the SMTP Service check box is selected.



If it is not selected, click to select it, click OK, and then follow the installation directions that are displayed.

1.18.2 Step 2: Configure the SMTP Service to Relay for Internal Domains

Depending on the scenario, it may be necessary to configure the SMTP service to relay inbound messages for your internal domains.

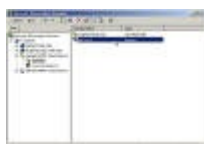
1. Click Start, point to Programs, click Administrative Tools, and then click Internet Services Manager.
2. Expand the tree under the server name, and then expand the Default SMTP Virtual Server. By default, you should have a Local (Default) domain with the fully qualified domain name of the server.



3. Configure the domain for inbound:
 - a. Right-click the Domains icon, click New, and then click Domain.



- b. Click Remote, click Next, and then type the domain name in the Name box. Click Finish.



1.18.3 Configure the domain for relay

1. In the properties for the domain that you just created, click to select the Allow the Incoming Mail to be Relayed to this Domain check box.
2. If this is being set up for a internal domain, you should specify the server that receives e-mail for the domain name by the IP address in the Route domain dialog box.



3. Click the forward all e-mail to smart host option, and then type the IP address of the server that is responsible for e-mail for that domain in square brackets. For example:

[123.123.123.123]

Note: Typing the IP address of the server in brackets is necessary so that the server recognizes this is an IP address and not to attempt a DNS lookup.

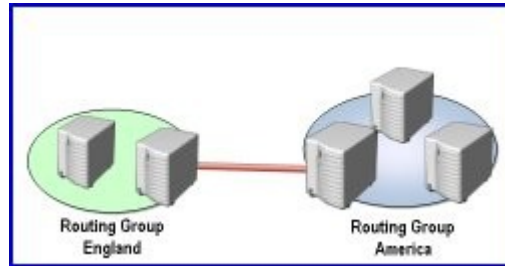
4. Click OK.

1.18.4 Step 3: Specify the Hosts That You Want to Openly Relay to All Domains

Note: Anyone can send to the domains that you specified in Step 2.

This step is for hosts, which are most likely your internal servers that would need to send to all domains on the Internet. It is not recommended to not have any restrictions because anyone can use your server as an open relay. It is recommended to only allow the minimum, necessary hosts to openly relay to all domains. To do so:

1. Open the properties of the Default SMTP Virtual Server.
2. On the Access tab, click Relay.



3. Click Only the list below, click Add, and then add the hosts that need to use this SMTP host to send e-mail.



On the dialog box that appears, you have the following options:

- Single computer: Specify one particular host that you want to relay off of this server. If you click the DNS Lookup button, you can lookup an IP address of a specific host.
- Group of computers: Specify a base IP address for the computers that you want to relay. You have to specify the octets in the IP address for hosts that you will allow to relay. For example: If the IP address is 192.68.7.21, and you want any hosts with the first two octets 192.68 to relay, specify 255.255.0.0 for the subnet mask.
- Domain: Select all of the computers in a domain by domain name that will openly relay. This option adds processing overhead, and might reduce the SMTP service performance because it includes reverse DNS lookups on all IP addresses that try to relay to verify their domain name.

1.18.5 Configure the other servers to use your relay server as a smart host

Depending on the other applications or mailers that will use your relay server, you may have a option where you can specify a smart host or SMTP relay. With Exchange 2000, you would create an SMTP connector and specify the Windows 2000 Relay server in the Forward all mail through this connector to the following smart host box.

What are Routing Groups? When would you use them?

Exchange 2003 can easily route both internal and external email. For routing email within your Exchange Organization, the best choice is a Routing Group Connector; while internet email is best served by an SMTP connector. X.400 Connectors are used to transfer email between Exchange and older types of email systems.

Topics for Microsoft Exchange 2003 Routing Groups

- [Routing Groups - Overview](#)
- [Routing Groups folder](#)
- [Types of Routing Connectors](#)
- [Exchange 2007 Hub Transport Server](#)
- [Summary](#)

Routing Groups - Overview

Both Active Directory's sites and Exchange's routing groups are physical entities. My point is that planning and configuring routing groups is separate from logical structures like OUs or even domains.

The situation with routing groups is that the Exchange servers are on different subnets, separated by routers. There is often a suspicion of a slow link, or an unreliable connection between routing groups. However, even if you have high speed links, there are benefits in organizing servers into routing groups. For example, you gain control over the message size and timing. You

can also restrict the users and addresses that can send email through that connector. Such control is not possible when all Exchange 2003 servers are in the same routing group.

Routing Groups folder

What surprises newcomers is that they cannot find the Routing Groups folder in Exchange System Manager. The reason could be that it's hidden. So check by navigating to the top of the interface, then right click Exchange Organization, properties, tick Display Routing Groups. Simply re-open the Exchange System Manager and now you should see the Routing Groups folder.



Once the Routing Group folder is visible, you are ready to create a second Routing Group. Amazingly, and slightly unnervingly, you can drag and drop an Exchange server object into the second routing group. Now the scene is set for you to create a connector. This process may sound tricky, but it is actually an easy configuration task with the Exchange System Manager. Once you join two routing groups, the email can start flowing between the servers in different routing groups.

Types of Exchange Routing Connectors

If you wish to connect two of your own Exchange 2003 servers in different routing groups, then the Routing Group Connector would be your first choice. Whereas, to transfer email to and from the internet, you need an SMTP type of connector. The only use I have for the X.400 connectors is for troubleshooting or connecting to ancient SMTP messaging systems.

Routing Group Connector

The Routing Group Connector is native to Exchange 200x. It's suspiciously like the site connector in Exchange 5.5, in fact you can transfer email to Exchange 5.5 using this connector. Technically, the Routing Group Connector is a one way street, that is why you always need a pair, one for each direction (inbound and outbound). Creating a Routing Group Connector is straightforward, and the wizard prompts you to generate a corresponding connector in the other group.

Bridgehead is a key concept where you have more than one server in each routing group. All the mail in one group is physically routed through the bridgehead server. Your bridgehead options are extremely flexible. Either you nominate one server on each side of the connector as a bridgehead, or all servers can be bridgeheads.

From the connector, click the Remote Bridgehead tab to check servers in the other group.

Exchange SMTP Connector

The SMTP connector is essential for internet email. You could also setup an SMTP connector as an alternative or backup to the Routing Group Connectors. Actually, the Virtual Server have their own built-in SMTP connector, but it's best to create a configurable connector here in the Routing Groups folder. [See much more about SMTP connectors here.](#)

X.400 Connector

X.400 connectors are reliable, but slow. My advice is to confine the X.400 to troubleshooting when all the other connectors fail to transfer the email. However, there is one other possibility, you need to connect to another (old) X.400 messaging system.

There are two flavours of Microsoft Exchange 2003 X.400 connector, TCP and X25.

What are the types of Connectors you can use in Exchange?

SMTP Connector

X.400 Connector

Why not install exchange on the same machine as a DC?

Answer well, this is not a good practice to do and the reasons

1 behind are :

1. Redundancy and Stability - if the exchange server fails then Domain Controller also fails and it concludes a big failure...
 2. Overload : It may overload your existing server and that can cause a significant performance problem.
 3. Exchange and DC use port 389 for LDAP queries. If you install both on same machine it results in port conflicts.
- For more info search for "LDAP and Exchange port conflict"

What is the cost option in Exchange connectors?

What is the Link State Table? How would you view it?

The link-state information is actually stored in memory on the Exchange Server system and isn't written to disk. The routing master in each routing group receives and maintains the link-state information (i.e., the link-state table) that routing-group members send to the routing master whenever an Exchange Server system determines that a link has changed state. The routing master is the only server that can increment the link-state version numbers in the link-state table. The routing master also sends the link-state table to routing masters in other routing groups, so that each routing group has a complete picture of the entire Exchange Server organization.

The link-state table contains information about the connectors, servers, routing groups, address spaces, link states, costs, versions, and organization to determine the most cost-effective route for a message delivery. You can use the WinRoute tool to obtain link-state information about your Exchange Server organization. Winroute.exe displays all unformatted information that's transferred from the link-state port (TCP port 691) in the bottom pane of its UI. You can find the WinRoute tool in the \support\utils\i386 folder on the Exchange 2003 or Exchange 2000 CD-ROM. You can also [download the WinRoute tool](#).

What is the Routing Group Master? Who holds that role?

How the Link State Recovers

After a link is marked as down, the original routing continues to retry the connection at 60-second intervals. Even though no message is waiting to transfer, the routing continues to try to contact the destination server. After a connection is re-established, the routing notifies the local routing group master that the connection is available, and the routing group master notifies all servers in the routing group and routing master servers in other routing groups that the connection is available.

[⬆ Back to the top](#)

Routing Group Masters

Link state information is most effective when multiple routing groups are configured in an organization, particularly if redundant paths are available. Each routing group has a master server that is fed link state information from different sources. The master keeps track of the link state data and propagates that data to the rest of the servers in the routing group. The master is normally the first server that is installed in the routing group, but you can change the master in Exchange System Manager; navigate to the routing group, click **Members**, right-click the server, and then click **Set as Master**. When a non-master server receives new link state information, the non-master server immediately transfers the link state information to the master, so that other servers can receive the information about the routing change.

[⬆ Back to the top](#)

Link Status

Only two states exist for any given link, up or down. Therefore, connection information, such as whether a link is active or in a retry state, is not propagated and is confined to the server that is involved in the message transfer.

What is DS2MB?

The Directory-service-to-Metabase-replication component (Ds2mb.dll) of the System Attendant service searches for deleted objects at a very high rate. These searches for deleted objects are overloading the Domain Controller (DC).

To resolve this problem, obtain the latest service pack for Microsoft Exchange 2000 Server. For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

XGEN: How to Obtain the Latest Exchange 2000 Server Service Pack

The English version of this fix should have the following file attributes or later:

Component:

File name	Version
Ds2mb.dll	6.0.5770.2

NOTE: Because of file dependencies, this update requires Microsoft Exchange 2000 Server Service Pack 2.

Microsoft has confirmed that this is a problem in Microsoft Exchange 2000 Server. This problem was first corrected in Microsoft Exchange 2000 Server Service Pack 3.

What is Forms Based Authentication?

Forms-based Authentication

Exchange 2003 has a snazzy new feature called Forms-based Authentication, which I'll refer to as FBA. FBA is the new logon security feature for Outlook Web Access (OWA) which is disabled by default in Exchange 2003.

Why use FBA?

There are several security benefits to running FBA:

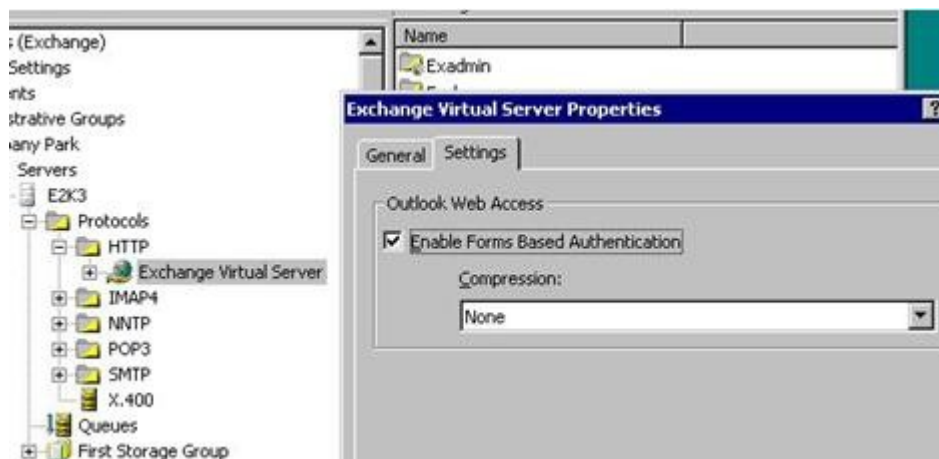
1. If the session is inactive for a period of time, the session will expire. The only way to gain access again is to re-authenticate. More on this later.
2. Users can no longer click the **Remember my password** check box in Internet Explorer.
3. Like the session inactivity setting, if you log out, you really log out. The only way to gain access again is to re-authenticate. Previously in Exchange 2000, the user had to complete the logout session by closing the browser window.

Enabling FBA

Enabling FBA is a simple process performed in Exchange System Manager. First, you should note that you need SSL enabled on the target Exchange 2003 server. When you've done that:

1. Drill down to your server object in ESM.
2. Under the server object, expand the **Protocols** container.
3. Under the Protocols container, expand **HTTP**.
4. Bring up the properties of the **Exchange Virtual Server**.
5. Click the **Settings** tab. Here you will see the option to enable FBA.

Here's what you should see. **Note that this option is greyed out on a cluster server because FBA isn't available on a cluster.** You'll need a front-end server in this scenario.



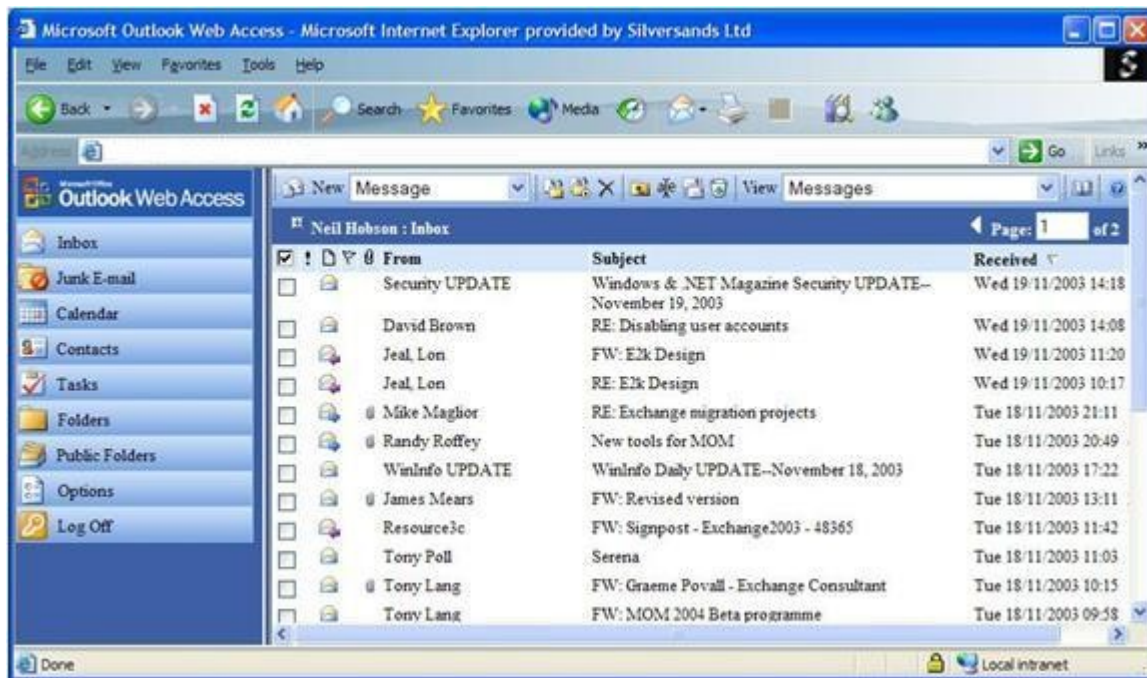
You will also note an option for compression. I'll leave that subject for another article. I've recently enabled FBA in a front-end back-end scenario here at my office. Note that FBA only needs to be enabled on the front-end server in this scenario.

If you've done everything correctly, you should get the following new OWA logon screen. Note that one difference is the fact that your users will now need to enter **domain\username** when logging on, or they can use their UPN if they prefer. There are ways around the domain/username sequence by modifying the logon.asp page, but these changes will be lost when you perform upgrades or re-installations. I think I'm going to leave this as it is for now - it's not much for users to learn, after all.



A Choice of Experience

The first option on the FBA screen is for you to select your choice of client experience: **Premium** or **Basic**. The Premium client gives you the full new OWA interface, whereas the Basic client gives you a cut-down version with less features. As you might guess, the Basic client is somewhat faster due to it offering less features. Hopefully that may help those still using dial-up connections to their OWA mailbox. If you've never seen the basic client, here's a quick screen shot.



How would you configure OWA's settings on an Exchange server?

OWA (Outlook Web Access)

In a nutshell, OWA in Exchange 2003 supports the full Outlook feature set. A sign that this version of the web client has come of age is that people are now complaining that OWA has too many features!

To connect to the Exchange 2003 server, simply type

<http://ExchangeServerName/exchange>.

I particularly appreciate having the Rules Wizard and a spell checker. The new OWA, looks and feels like Outlook. You even have navigation settings and preview - now called Reading Pane. Best of all, a right click now produces the short cut menu, just like other Windows programs.

It makes sense for administrators to configure and publicise the use of UPN (user principle names) so that OWA users can logon with their email address. For those concerned about the security of their messages or their signature OWA now supports S/MIME encryption and signature verification.

There also improvements to the calendar so that you can reply to meeting requests and receive reminders using OWA.

Note: Select the Premier version of OWA unless you have a very old browser.

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

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

Setting Up a Logon Page

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

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

Enabling Forms-Based Authentication

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

For detailed steps about enabling forms-based authentication, see

Setting the Cookie Authentication Time-Out

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

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

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

Note:

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

- For detailed steps about how to configure the public computer cookie time out value, see [How to Set the Outlook Web Access Forms-Based Authentication Public Computer Cookie Time-Out Value](#).
- For detailed steps about how to configure the trusted computer cookie time out value, see [How to Set the Outlook Web Access Forms-Based Authentication Trusted Computer Cookie Time-Out Value](#).

Configuring Client Security Options for Users

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

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

Note:

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

Note:

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

- For detailed steps about how to configure the public computer cookie time out value, see [How to Set the Outlook Web Access Forms-Based Authentication Public Computer Cookie Time-Out Value](#).
- For detailed steps about how to configure the trusted computer cookie time out value, see [How to Set the Outlook Web Access Forms-Based Authentication Trusted Computer Cookie Time-Out Value](#).

Outlook Web Access Compression

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

1.18.6 Compression settings for Outlook Web Access

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

Requirements for Outlook Web Access Compression

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

- The Exchange server that users authenticate against for Outlook Web Access must be running Windows Server 2003.
- Your users' mailboxes must be on Exchange 2003 servers. (If you have a mixed deployment of Exchange mailboxes, you can create a separate virtual server on your Exchange server just for Exchange 2003 users and enable compression on it.)
- Client computers must be running Internet Explorer version 6 or later. The client computers must also be running Microsoft® Windows® XP or Microsoft Windows® 2000 Server and have installed on them the security update that is discussed in Microsoft Security Bulletin MS02-066, "[Cumulative Patch for Internet Explorer \(Q328970\)](#)."

Note:

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

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

For detailed steps about how to enable Outlook Web Access compression, see [How to Enable Outlook Web Access Data Compression](#).

Simplifying the Outlook Web Access URL

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

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

However, users frequently request that a URL that is simpler than the default URL be made available for accessing their mailboxes. Creating this simple URL makes the URL both easier to remember and easier to enter in a Web browser. For example, <http://www.contoso1.com> is an easier URL for users to remember than <http://contosoexchange01/exchange>.

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

For detailed steps about how to simplify the Outlook Web Access URL, see [How to Simplify the Outlook Web Access URL](#).

What is DSACCESS?

DSAccess partitions the set of available directory service servers into the following three (possibly overlapping) categories: global catalog servers, domain controllers, and the configuration domain controller.

Almost all Exchange Server user-context directory service transactions target global catalogs. However, domain controllers can be used for user context requests when the requesting service has sufficient knowledge of the locality of the requested user object in the issued search. Because the directory service server used for a global catalog is also itself a domain controller, this server may be used as both types of directories. DSAccess generates a list of available global catalogs and domain controllers, which it periodically updates as directory service state changes are detected. This list can be shared out to other directory consumers that do not necessarily use DSAccess as their gateway for accessing the directory service (for example, Categorizer, DSProxy, and the System Attendant service). However, subsequent directory service state changes are left to the detection of the service that is requesting this list.

Exchange needs access to Active Directory domain controllers for a variety of reasons (see Figure 5.20):

Configuration information for the organization. Exchange stores server parameters, mailbox and public folder store parameters, public folder hierarchy, tool parameters, and much more in the Configuration naming context of Active Directory.

Recipient information in the Global Catalog. Exchange and Outlook need access to a Global Catalog server to expand group memberships for mail-enabled groups, to obtain address lists such as the GAL, and to obtain recipient information necessary for message handling and routing.

Recipient information in a domain. If Exchange can get the information it needs about a recipient from a standard domain controller in its own domain rather than a Global Catalog server, it will do so. This reduces load on the Global Catalog servers.

An Exchange service called DSAccess has the task of finding domain controllers and Global Catalog servers suitable for use by Exchange. Think of DSAccess as a nightclub owner who books stage talent. It applies a series of tests, the details of which you'll see in a minute, to determine which servers it wants to use. It then selects up to ten domain controllers and ten Global Catalog servers and puts them in a local DSAccess profile. It also selects one domain controller to use for a configuration server. This avoids replication latency issues.

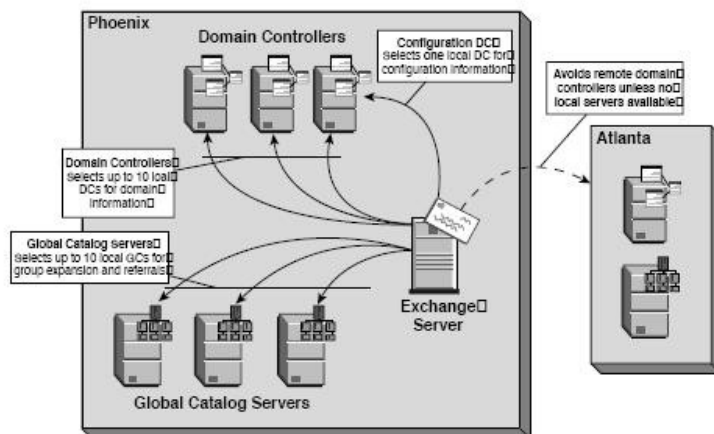


Figure 5.20 Diagram of DSAccess selection based on location. (Click on image for enlarged view.)

DSAccess keeps an open connection to each server in the DSAccess profile. This avoids the expensive chore of building up and tearing down RPC and TCP connections each time the Exchange server needs information.

Other Exchange services, such as the SMTP Routing Engine Categorizer and DSProxy, send their LDAP and NSPI requests to DSAccess, which selects a target domain controller or Global Catalog server from its profile and forwards the request to that server. It uses a round robin selection process for load balancing.

Because all LDAP queries funnel through DSAccess, Exchange dramatically improves performance by caching the query results. By default, Exchange gives 4MB of physical memory to the DSAccess cache.

Global Catalog advertising and DSAccess

DSAccess uses DNS to locate domain controllers and Global Catalog servers. Figure 5.21 shows an example DNS zone with three GC SRV records located in the `_msdcs.dc.gc._tcp` folder. Active Directory domain controllers also place copies of these SRV records into individual site folders underneath the `_msdcs.dc.gc._sites` folder. By looking in the folder corresponding to its own Active Directory site, DSAccess can locate local Global Catalog servers.

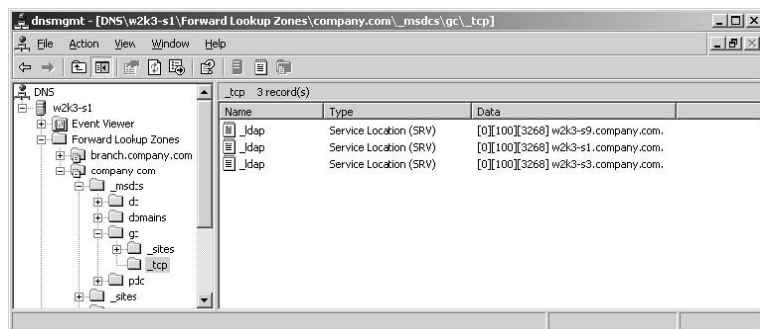


Figure 5.21 SRV records for Global Catalog servers in DNS. (Click on image for enlarged view.)

When you configure a domain controller to be a Global Catalog server, the server must replicate the Domain naming contexts from the other domains before it can answer Global Catalog lookup requests authoritatively. Once a newly promoted Global Catalog server has replicated all domain naming contexts, it places an SRV record in DNS that "advertises" itself as available. You can verify the status of the Global Catalog promotion in several ways: Look for an Event log entry saying that the GC promotion has completed (Figure 5.22 shows an example).

Look for a Registry entry called HKLM -> System -> CurrentControlSet -> Services -> NTDS -> Parameters -> Global Catalog Promotion Complete (shown in Figure 5.23.) and verify that the value is set to 1.

Dump the RootDSE contents using the LDAP Browser (LDP) from the Windows Server 2003 Support Tools and look for the isGlobalCatalogReady attribute set to TRUE.

Use the Nltest utility that comes in the Windows Server 2003 Support Tools. The following example shows that the server running Nltest was able to find a Global Catalog server in its local site (Phoenix) in its domain (Company.com):

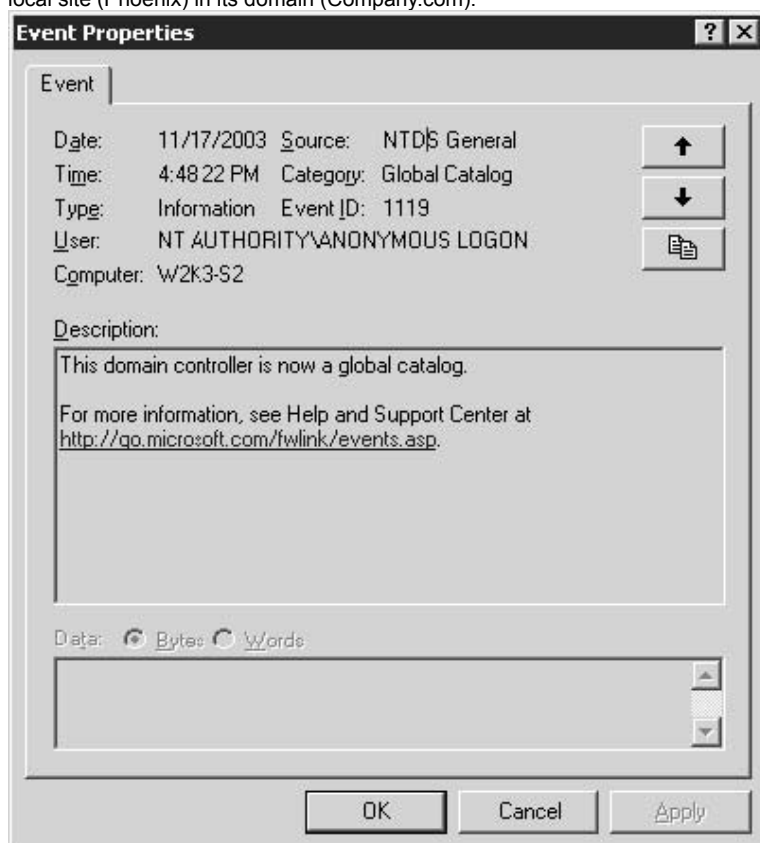


Figure 5.22 Event Log entry announcing that a domain controller has successfully begun operating as a Global Catalog server. (Click on image for enlarged view.)

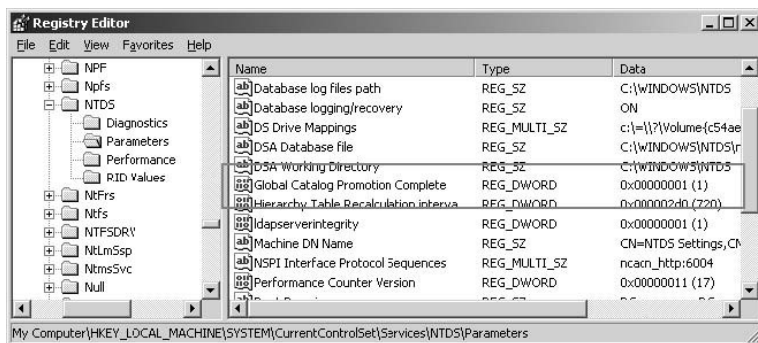


Figure 5.23 Registry entry on newly promoted Global Catalog server. (Click on image for enlarged view.)

What are Recipient Policies?

A description of the Mailbox Manager recipient policy functionality

Mailbox management recipient policies are a set of configurable rules that run on a schedule and that evaluate the mailboxes on the local server. The policy uses rules to filter all the recipient objects and to selectively apply mailbox management settings to messages in folders that go past the limit of the predefined rules.

The mailbox management process detects folders in a mailbox that contain messages larger than a certain size. If a message remains in a folder after a predefined time has passed (by default, 30 days), a number of predefined actions can be taken, including the following:

- Generate a report only and send the report to the mailbox owner.
- Move the message to the Deleted Items folder.
- Move the message to System Cleanup folders.
- Delete the message immediately.

Note Use caution when you use the **Delete the message immediately** option, because users may have to recover their messages.

If you use recipient policies, it is easy to apply or revise the rules. You do not have to reconfigure settings individually on each object. You can also change recipient policy priority levels to change the way that multiple policies are adjusted.

Note There is no default recipient policy for mailbox management (unlike the e-mail recipient policies). However, you can add the required property page to the default recipient policy if you want to create a mailbox management policy that applies to all recipients.

Policies are applied according to the schedule that you set up on each server. This prevents mailbox management from running on all servers in the organization at the same time. However, you can force a manual update if you want a recipient policy to apply immediately.

Note Like e-mail recipient policies, the highest priority recipient policy that applies to an Exchange Server object is the effective policy. Lower priority policies are no longer evaluated after a match has been made.

How would you work with multiple recipient policies?

Microsoft Exchange News:



1.0

A user who wants to get email from outside the Exchange organization needs an address that a foreign messaging system can understand. Microsoft calls this a proxy address because Exchange "stands proxy" for the foreign messaging system.

You are reading tip #7 from "15 tips in 15 minutes: Managing recipients and distribution lists," excerpted from Chapter 5 of the book Learning Exchange Server 2003, published by Addison-Wesley Professional.

Because Exchange 2003 uses Simple Mail Transfer Protocol (SMTP) for internal and external mail routing, all email objects in Active Directory get an SMTP proxy address. Exchange also assigns an X.400 proxy address, just in case you need to route messages to a legacy Exchange system. Legacy Exchange uses X.400 to route messages between sites.

You might also encounter outside messaging systems that use Lotus Notes, GroupWise, or some other application with unique addressing. These require special connectors that fall outside the scope of this book.

Default Recipient Policy

You can view the proxy addresses assigned to a recipient using the Active Directory Users and Computers console. Open the Properties window for the recipient and select the Email Addresses tab. Figure 5.27 shows an example.

When you install Exchange for the first time, it determines the format of the SMTP address you'll want for your users based on your organization name and the DNS name of your domain. It places the result into an Active Directory object called a **Recipient Policy**.

A service called the Recipient Update Service, or RUS, reads the proxy addresses in that default recipient policy and applies them to the mail-enabled objects in Active Directory.

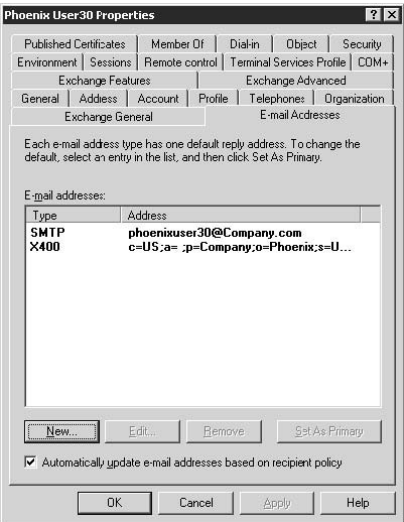


Figure 5.27 Proxy email addresses assigned based on Default Recipient Policy. (Click on image for enlarged view.)

To access recipient policies in ESM, drill down under Recipients to the Recipient Policies container, as shown in Figure 5.28.

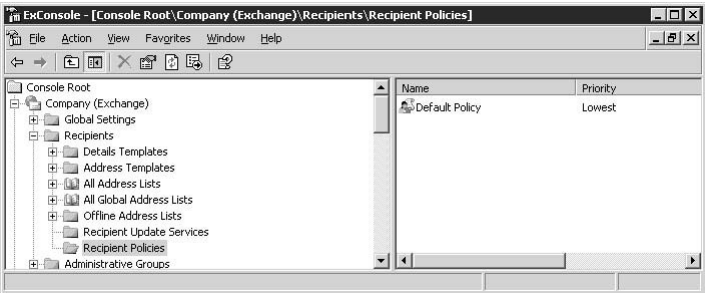


Figure 5.28 ESM console showing Recipient Policies container and Default Policy. (Click on image for enlarged view.)

To see how Exchange formulates a proxy address, open the Properties window for the Default Policy object. Figure 5.29 shows an example. If Exchange guessed wrong when formulating the default SMTP address for your organization, you can change the address as follows:



What is the "issue" with trying to remove email addresses added by recipient policies? How would you fix that?

What is the RUS?

When you perform the initial install of Exchange, the Recipient Update Service is installed and a default recipient policy is created. This policy is responsible for ensuring that all mail-enabled objects in the Exchange organization have a valid SMTP address following the username@domain.com naming format. You can create a new policy that can be configured to create each SMTP address following a different naming convention such as Firstname.Lastname@domain.com. Microsoft has a list of best practices to follow when creating and/or editing recipient policies.

- Create a new recipient policy and assign it a higher precedence rather than editing the default policy
- Keep the number of recipient policies to a minimum
- Rebuild the RUS with caution

A lack of understanding of the RUS is the major cause of issues. Often administrators apply a policy without understanding what will be changed. Exchange does not provide much warning about the impact a change will make. On top of that, organizations using a 3rd party application to create and assign SMTP addresses, through MIIS for example, can cause further damage by applying recipient policies blindly. So what do we do when RUS takes a vacation?

Verify RUS is Running

With Diagnostic Logging enabled, wait a few minutes and you should see two events show up in the Application event log with IDs 8011 and 8012. These events verify that RUS has started. If you do not get these messages, restart the Microsoft Exchange System Attendant service. Once this service is started you will see a number of new events logged, the first of which, 9006 and 9008, notify you that Abv_dg.dll is loading and then starting.

If event ID 9006 appears, but you never get event ID 9008, you are performing this task on a front-end server. On a front-end server Abv_dg.dll does not exist and RUS must be run on a back-end server.

Troubleshooting Common Issues with RUS

As previously mentioned the Recipient Update Service runs quietly in the background and requires little or no maintenance. When issues do occur there are three basic steps to troubleshooting RUS.

- Enable Diagnostic Logging
- Choose an object, or objects to monitor
- View the Application Log for errors

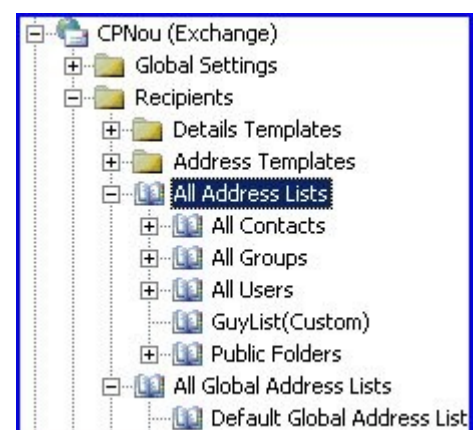
To begin troubleshooting RUS we first determine if we have more than one recipient policy, if so, set the schedule for all but one to Never Run. In the case of multiple policies, you may be required to go back and enable another policy if you find nothing wrong with the first. Just ensure that only one policy is scheduled to run at a time.

When would you need to manually create additional RUS?

What are Address Lists?

How the Exchange 2003 GAL works

All the address information is held by Active Directory. To the left of the @ is the username, to the right of the @, the email domain name. In fact, I think of the GAL as merely a fancy LDAP query which produces a list of addresses, for example guyt @ cp.com. The final piece of the address jigsaw is RUS (Recipient Update Service). RUS is the engine which generates and updates the email addresses that you see in the GAL.



If the GAL is slow to update, then look to the Global Catalog servers. Make sure that there is Windows 2003 Global Catalog server near the Exchange 2003 server running RUS. As you may know, the Global Catalog replicates a sub-set of all the user's properties, including Exchange features such as email address. So if Exchange has access to a local Global Catalog server, then its GAL will be up-to-date.

Clients

Potentially, any client who can query Active Directory can access the GAL. However, you can control who sees which list through read permission on the security tab found on the lists.

Types of Exchange 2003 Address Lists

Global Address Lists - All of Exchange's mail recipients are in the GAL. (Except hidden mailboxes). By default, everything and anything with an email address is here. The surprise is that you can have more than one, Global Address List. Multiple Global Address Lists blow my mind, so I recommend that you stick with just one GAL.

The only exception to the one GAL rule is if you manage two email domains. What I mean is that you could have a GAL for maincompany.com and another for subsidiary.com. In this case you would use security permissions to determine which users get which GAL in their Outlook clients.

Default Lists - Again, note the plural. Once you see the list names, All Users, All Contacts, All Public Folders, All Groups, then you realise that these are sub-sets of the Global Address List. Perhaps we should think of it the other way around, a Global Address List is made up of these individual lists, see diagram opposite.

Offline Address List - The idea is that for remote users, the administrator can reduce the size of the offline address book, for example, by choosing only the All Users and All Groups. (But omitting the All Public Folders). If you have more than Offline Address List, then go to the Mailbox Store, database tab, and choose which Offline Address List is associated with which Mailstore.

Custom Address List - Don't bother! Much as I usually love customizing, my own view is that you do not need anything but a list of mail objects in the main GAL. Users are getting sophisticated at searching, in my opinion they do not need the confusion of multiple lists for each department.

I fully realize that my vision of one GAL is in the minority. Most companies love to create lots of custom lists. They say, for example, if there is a John Smith in sales and John Smith in accounts then only by having a custom list for each department, can users tell who is who. I say rubbish, if they go to the properties they can see to which department the user belongs. My view is the benefits of multiple lists are offset by feeling of being overwhelmed by lots of lists.

How would you modify the filter properties of one of the default address lists?

How can you create multiple GALs and allow the users to only see the one related to them?

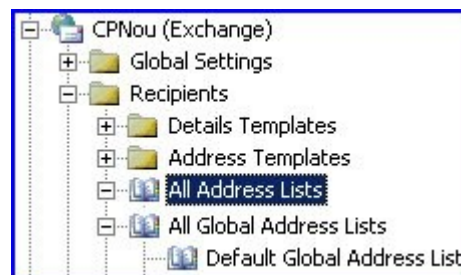
Introduction to Global Address Lists in Microsoft Exchange Server 2003

It's only natural that users try and locate each others email addresses in the GAL. But why would an administrator need to configure Exchange 2003's GAL? The most likely answers are: to check permissions, create custom lists and control how the names are displayed in the Global Address List.

Strategy for your GAL (Global Address List)

My advice for configuring the GAL is do nothing! Just go with the default GAL (Global Address List). Exchange 2003 server automatically adds every new mail recipient to the Global Address List, so, Guy says there is no more work to be done.

However, I admit that larger companies may have compelling business reasons for customizing the address book. To them I say: make changes to the GAL immediately after installing Exchange 2003 and certainly before you build the first email address.



This is the horror story. If you change the Exchange GAL display order from: Firstname Lastname, to Lastname, Firstname, it only affects new users. Here is how the display would change, Elizabeth Washington, becomes: Washington, Elizabeth [See more here](#).

Objects found in the Exchange 2003 GAL

I often say that being good at computing means being aware of subtle difference in Microsoft names. Exchange 2003's mail objects is a case in point. Pay careful attention to the difference between a mailbox enabled user and a mail-enabled user; a security group and a distribution group. Here is a list of the objects which you find the Global Address List.

- Mailbox enabled accounts. Regular users with MAPI mailboxes Active Directory accounts.
- Mail-enabled users. Contractors who have an Active Directory logon but no mailbox. (No mailbox in your Exchange Organization.)
- Contacts. Suppliers, customers, people with email address outside your organization. No Active Directory account. Thankfully, contacts have a different symbol in the GAL.
- Distribution groups. These can be Global or Universal Groups, but they are designed for email rather than security. These are sometimes referred to as DLs - Distribution lists instead of distribution groups. Pay attention to detail and examine the Members and MemberOf tabs.
- Query-based distribution groups. Well worth setting up. Again, note the different symbol from other groups. Incidentally, I wish Microsoft would use different colors for different scopes of group. Say, Red for Universal and Green for Local Groups.
- Mail-enabled groups. Security groups that have mailboxes. Guy says that unless you have a good reason, favour the classic Distribution group and avoid Mail Enabled Security Groups.
- Public Folders. Mail-enabled public folders if your users need an easy way to post.

What is a Front End server? In what scenarios would you use one?

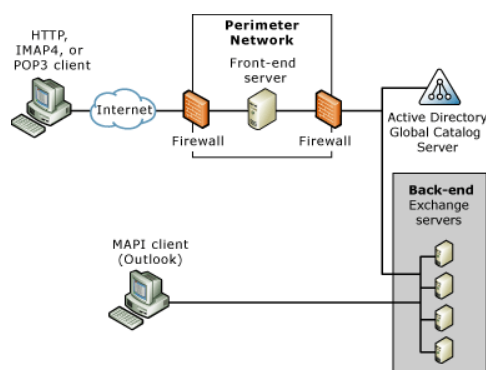
In this architecture, a front-end server accepts requests from clients and proxies them to the appropriate back-end server for processing

Front-End and Back-End Topologies Overview

Topic Last Modified: 2005-05-24

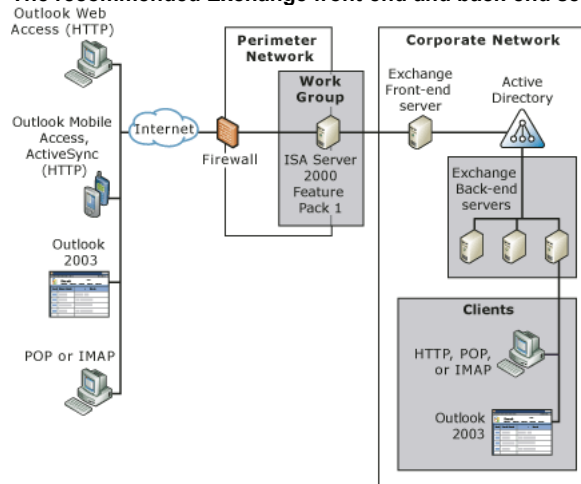
The figures in this topic describe the common implementations of the front-end and back-end server architecture. The following figure illustrates a simple Exchange front-end and back-end topology.

An Exchange front-end and back-end server architecture without an advanced firewall



The following figure illustrates the recommended scenario that uses an advanced firewall, such as Microsoft® Internet Security and Acceleration (ISA) Server with Service Pack1 (SP1) and Feature Pack1, between the Internet and the Exchange front-end server.

The recommended Exchange front-end and back-end server architecture



How to Designate a Front-End Server

Topic Last Modified: 2005-05-17

A front-end server is an Exchange server that accepts requests from clients and proxies them to the appropriate back-end server for processing.

Before You Begin

To successfully complete the procedures in this topic, confirm the following:

- The server that you will designate as a front-end server is a member of the same Microsoft® Windows® forest as the back-end servers.
- The server that you will designate as a front-end server is a member of the same Exchange organization as the back-end servers.

Procedure

To designate a front-end server

1. Install the server that will be running Exchange Server in the organization.

Note:

With Exchange 2000 Server, only Enterprise Edition servers can be configured as front-end servers. In Exchange Server 2003, both Standard Edition and Enterprise Edition can be configured as front-end servers.

2. Use **Exchange System Manager** to go to the server object, right-click the server object, and then click **Properties**.
3. Select **This is a front-end server**, and then close the page.
4. To begin using the front-end server do one of the following:
 - Restart the computer.
 - Stop and restart the HTTP, POP3, and IMAP4 services.
5. The default Exchange virtual directories have now been configured for you. However, it is recommended that you also configure SSL. For detailed instructions on how to configure SSL for POP3, IMAP4, and SMTP, see "How to Configure SSL for POP3, IMAP4, and SMTP" in the [Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide](#). For detailed instructions about how to configure SSL for HTTP, see How to Configure SSL for HTTP in the [Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Server Topology Guide](#).

How to Create a Virtual Server

Topic Last Modified: 2005-05-24

Use this procedure to create a virtual server.

Procedure

To create a virtual server

1. In Exchange System Manager, in the HTTP Protocols container for the front-end server, right-click **HTTP**, and then select **New Virtual Server**.

Note:

For a name, it is recommended that you use something following the form of "adatum.com (front-end)." Consistent naming of the new virtual servers ensures that each virtual server's purpose and associated domain can be easily determined. The name of the virtual server is used only for identification purposes and does not affect its operation.

2. Click **Mailboxes** or **Public folder**, click **Modify**, and then do one of the following:

- If the virtual server points to mailboxes, select the domain.

Note:

The list of domains in **Select SMTP Domain** is pulled from the domains of the SMTP addresses in the Exchange organization's recipient policies, so if you have more than one recipient policy for the same domain, you will see duplicates in this dialog box. It does not matter which one you choose.

- If the virtual server points to a public folder, select the appropriate public folder to act as the root public folder for this virtual server.

3. Click **Advanced**, and then add host headers that define all the names a client might use to contact this front-end server.

Note:

If a front-end server is used internally and externally, it is recommended that you list both a hostname and a fully qualified domain name.

What type of authentication is used on the front end servers?

How to Configure Authentication on a Front-End Server

Topic Last Modified: 2005-05-26

You can configure your front-end server for dual authentication or for pass-through authentication. In dual authentication, both front-end and back-end servers are configured to authenticate users. If you have a locked-down perimeter network in which RPCs are not allowed across the intranet firewall, and it is impossible for the front-end server to authenticate users, you can use pass-through authentication.

Before You Begin

To successfully complete the procedures in this topic, confirm the following:

- You use pass-through authentication only if the front-end server cannot authenticate users
- You have read [Scenarios for Deploying a Front-End and Back-End Topology](#).

Procedure

To configure authentication on a front-end server

1. Click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Go to the "Exchange" or "Public" virtual directory.
3. Right-click the "Exchange" or "Public" virtual directory and then click **Properties**.
4. Click the **Access** tab, and then click **Authentication**.

5. Do one of the following:

- To configure the front-end server to authenticate users (as in dual authentication), select the **Basic authentication** check box.
- To configure pass-through authentication, select the **Anonymous access** check box, and then clear the **Basic authentication** check box.

When would you use NLB?

How would you achieve incoming mail redundancy?

What are the 4 types of Exchange backups?

What is the Dial-Tone server scenario?

When would you use offline backup?

How do you re-install Exchange on a server that has crashed but with AD intact?

What is the dumpster?

What are the e00xxxxx.log files?

What is the e00.chk file?

What is circular logging? When would you use it?

What's the difference between online and offline defrag?

How would you know if it is time to perform an offline defrag of your Exchange stores?

How would you plan for, and perform the offline defrag?

What is the eseutil command?

What is the isinteg command?

How would you monitor Exchange's services and performance? Name 2 or 3 options.

Name all the client connection options in Exchange 2003.

What is Direct Push? What are the requirements to run it?

How would you remote wipe a PPC?

What are the issues with connecting Outlook from a remote computer to your mailbox?

How would you solve those issues? Name 2 or 3 methods

What is RPC over HTTP? What are the requirements to run it?

What is Cached Mode in OL2003/2007?

What are the benefits and "issues" when using cached mode? How would you tackle those issues?

What is S/MIME? What are the usage scenarios for S/MIME?

What are the IPSec usage scenarios for Exchange 2003?

How do you enable SSL on OWA?

What are the considerations for obtaining a digital certificate for SSL on Exchange?

Name a few 3rd-party CAs.

What do you need to consider when using a client-type AV software on an Exchange server?

What are the different clustering options in Exchange 2003? Which one would you choose and why.