CHAPTER 5

Managing Recipients and Distribution Lists

In his book, *Zen and the Art of Motorcycle Maintenance*, Robert Pirsig contends that quality is an intrinsic element of any structure. To make his point, he lays out the parts of a motorcycle on a garage floor then patiently describes, not the reassembly process, but the attitude towards Quality necessary to perform a successful reassembly. During this discussion, he draws your attention to a small sheet metal screw used to attach the oil pan cover. "If this screw gets stripped," he says, "the motorcycle cannot be ridden." Thus, the value of the smallest part on the motorcycle equals the value of the motorcycle itself. That knowledge helps you to maintain a good attitude towards the Quality inherent in every part.

This lesson comes in handy when managing recipients. You can spend weeks, even months, building a fully functional Exchange infrastructure filled with top-notch servers and redundant network connections and state-of-the-art storage systems, but all that work, every single erg of energy you expended, could go completely to waste if the users aren't happy with the result. In this chapter, you'll see how to configure Exchange in a way that gives your users a Quality experience. If they still don't appreciate your efforts, you can ask them to help you with a little blindfolded archery practice.

Security Groups and Exchange

Windows servers use groups to control access to security objects such as NTFS files and folders, Registry keys, and Active Directory objects. Exchange 2003 uses groups to control access to public folders and user mailboxes as well as to act as distribution lists.

For example, Figure 5.1 shows how you can put a Security group called Engineering on the permission list for a public folder so that only members of the Engineering group can read or contribute to the folder.

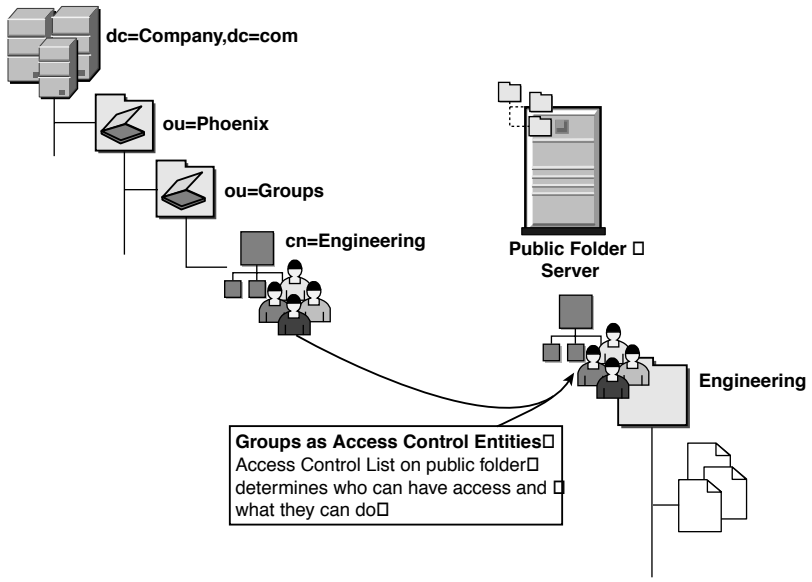

Figure 5.1 Exchange can use Active Directory Security groups to control access to resources such as public folders and mailboxes.

You can also use Security groups to control access to an individual user's private mailbox. For example, if the Forensics team wants access to the mailbox of an employee under suspicion of industrial espionage, you could create a Security group called Forensics and put that group on the permission list for the user's mailbox without the user's knowledge.

As you saw in the previous chapter, you can use Security groups to delegate administrative roles for your entire Exchange organization or for individual Administrative Groups.

Issues with Mail-enabled Security Groups

At first, using Security groups both to protect Exchange resources and to support e-mail distribution doesn't appear to present any difficulties. But the devil lies in the details, as they say, and if you don't plan your group management correctly, both your users and your Windows system administrator colleagues down the hall might not like the results.

Most Windows administrators consider the ability to create Security groups in Active Directory something of a special privilege and they tightly control that privilege, granting it only to administrators who agree to abide by a strict set of business practices or risk getting shamed at a Monday meeting.

"After all," reason the Windows administrators, "we spent a lot of time and sat down at a lot of meetings to come up with a strategy for naming and nesting groups that meets all of our users' business requirements with the fewest groups possible. We don't want outsiders coming in and messing things up."

The outsiders, in this case, include e-mail users who have an entirely different set of business practices, not to mention their own personal eccentricities, which affect their attitude towards distribution lists. E-mail users have a love affair with distribution lists. They want *lots* of them, and they want to give them all sorts of names to please executives, managers, clients, vendors, government regulators, secret agents, and just about anybody else who interacts with the messaging system in any capacity whatsoever.

And if they want a new distribution list, they want it *now*. Not tomorrow. Not by the end of the day. Not in response to filling out an online work order. *NOW!*

Because an Exchange distribution list is really an Active Directory group, and the Windows administrators don't want to see groups created willy-nilly, you might find yourself at something of an impasse. Statesmanship demands a compromise. You need a group that can act as a distribution list but cannot reside on an Access Control List where it could cause problems for Windows administrators. You need a Distribution group.

If you can get IT management and the user's managers to agree on a naming scheme, then life gets simple in this area.

Distribution Group Advantages

Distribution groups have their limits, but those limits become their strength. Windows administrators might not care about groups that can't end up on file and printer ACLs, so they can loosen the reins a bit on who can create them or modify their membership.

Okay, the Windows admins probably do care about Distribution group names, but at least the meetings to agree on Distribution group standards won't get nearly as rancorous as the meetings to agree on Security group standards.

For example, you might want junior Exchange administrators or even department gurus to create Distribution groups, with the understanding that group names such as "Executives I Loathe" had better not show up in the Global Address List (GAL). You could even grant permission to Help Desk technicians to modify the membership of Distribution groups in response to a phone call from designated users, something you would not ordinarily want to do with Security groups.

Active Directory does permit nesting a Distribution group into a Security group, but this does not assign access permissions to members of the Distribution group. For example, consider a user named TinaTurner who belongs to a Distribution group called DynamiteDivas. You nest the DynamiteDivas group into a Security group called OnStageProduction, and you grant the OnStageProduction group access permissions for an NTFS folder called LightsAndCameraControls. In this configuration, the TinaTurner account cannot access the LightsAndCameraControls folder.

Watch Out for Automatic Promotions

Your idyllic compromise to permit Exchange administrators to create Distribution groups using a different set of business practices and standards than the Windows administrators use for Security groups could get you into trouble if you don't watch out for a feature in Exchange 2003.

ESM and Outlook permit you to place a Distribution group on the permission list for a public folder or a user's mailbox, as shown in Figure 5.2.

If you take advantage of this capability, when the Exchange Information Store notices that the group appears on a permission list, it automatically promotes the Distribution group to a Security group.

Once the group becomes a Security group, it begins to appear in the Select Users and Groups control used to add security principals to Access Control Lists in Windows. Very soon after that occurs, your phone rings. It's the manager of the Windows administration team calling you to a meeting to discuss why you have violated your agreement not to create Security groups. Personally, I'd rather lock the senior representatives of the national Republican and Democratic parties in a cage for a six hour, no-holds-barred policy fight over gun control than be present at that meeting.

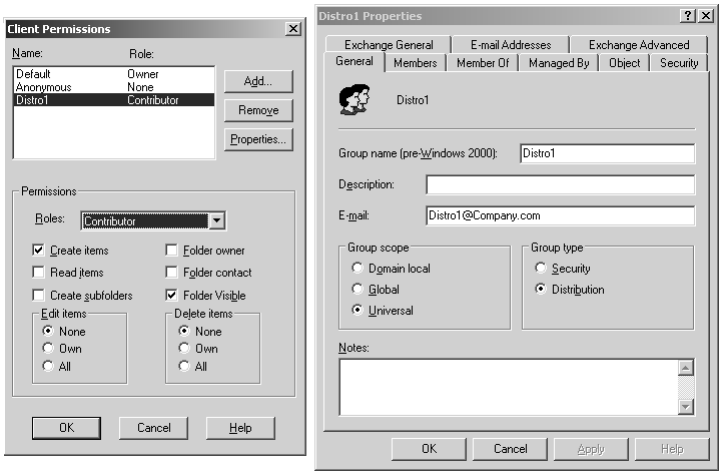

Figure 5.2 Exchange permits Distribution groups on MAPI permissions, but will subsequently promote the group to a Security group.

To avoid those situations, it's important that you make anyone with Author permissions on a public folder aware of the security group promotion feature and urge them to be absolutely sure that they only add Security groups onto a permission list.

Delegating Group Membership Management

You might decide to permit non-administrators to manage the membership of Distribution groups without allowing them to create groups, delete them, or change their scope or type. Active Directory has a "Modify Group Membership" permission intended for this purpose.

Unfortunately, Active Directory does not have a filter that applies the "Modify Group Membership" permission solely to Distribution groups. You need to collect your Distribution groups into a separate OU (Figure 5.3 shows an example) then delegate the "Modify Group Membership" permission to a Security group on the ACL of that OU. Do so as follows:

1. Right-click the **OU** icon and select **Delegate Control** from the flyout menu. This starts the Delegation of Control wizard.
2. Click **Next**. The Users and Groups window opens.
3. Click **Add** and use the object picker to select the **Distro Managers** group. The result looks like Figure 5.4.

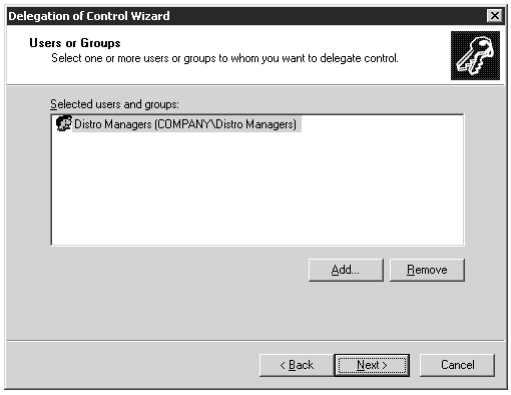

Figure 5.3 Congregate Universal Distribution Groups into their own OU to simplify delegating permission to change membership.

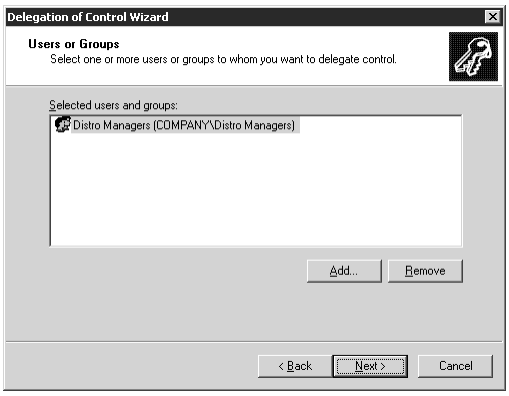

Figure 5.4 Select a group to delegate admin permissions.

4. Click **Next**. The Tasks to Delegate window opens.
5. Check the **Modify the Membership of a Group** option, as shown in Figure 5.5
6. Click **Next**. This opens a Summary window.
7. Click **Finish** to exit the wizard.

With this delegation in place, any user you put in the Distro Managers group can change the membership of a Distribution group in the Distribution Groups OU. You do not need to train those users to use Active Directory Users and Computers and you don't need to install the Adminpak.msi tools on their desktops. They can do the work via Outlook.

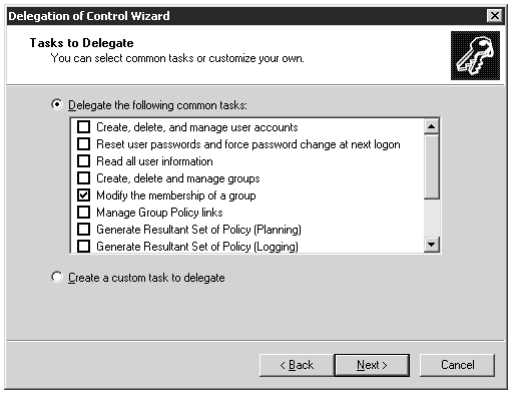

Figure 5.5 Delegation of Control wizard showing permission to assign to selected group.

Managing Distribution List Membership in Outlook

A user who has "Modify Group Membership" permissions on a group in Active Directory can use Outlook to manage members of that group. Here's the procedure:

1. From the main Outlook window, open the Address Book either by selecting **Tools | Address Book** from the main menu or by pressing **Ctrl+Shift+B**.
2. In the **Show Names** dropdown field, select **Global Address List**. Figure 5.6 shows an example.

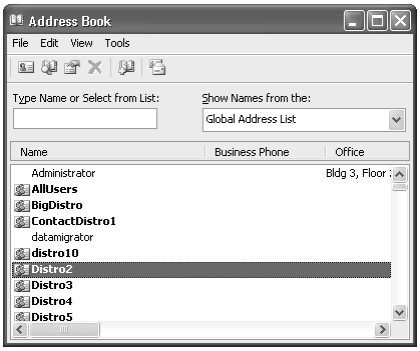

Figure 5.6 Distribution list as it appears in the GAL in Outlook.

3. Right-click a distribution list and select **Properties** from the fly-out menu. This shows the membership list of the distribution list along with information about the owner, if any. Figure 5.7 shows an example.

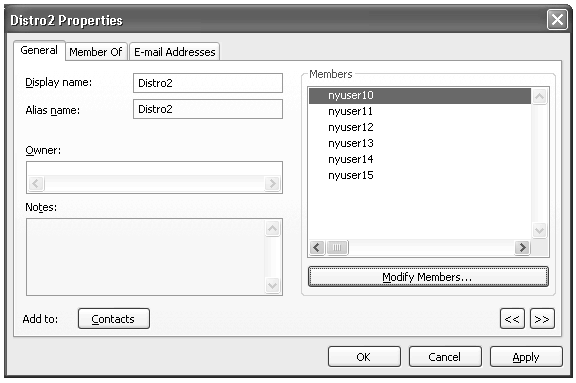

Figure 5.7 Properties of a distribution list in Outlook showing group members.

4. Click the **Modify Members** button to open a Distribution List Membership window.
5. Click **Add** to open a browse list for the GAL from which you can select new members. The member can be a user account, another group, or a contact.
6. Click **OK** then **OK** again to save the change.
7. Close the Address Book.

Group Membership Expansion

When you send a message to a mail-enabled group, the Exchange server sends a copy of the message to each mail-enabled user and contact in the group. The process of finding those mail-enabled group members is called *expansion*.

Description of Group Expansion Process

Figure 5.8 shows a diagram of the expansion process. During this discussion, I'll use the term "ultimate recipients" to mean mailbox-enabled users, mail-enabled users, and mail-enabled contacts.

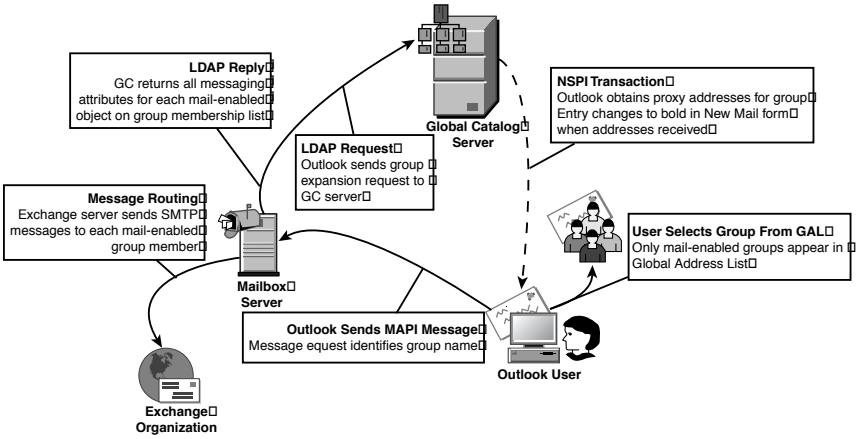

Figure 5.8 Required processes for selecting a group and sending a message to the group.

1. **User selects group from Global Address List (GAL).** The process starts when an Outlook user selects a distribution list from the GAL to be the recipient of an e-mail message. Outlook obtains the GAL via a Name Service Provider Interface (NSPI) request sent to a Global Catalog server. The user could also simply enter the distribution list name in the To field of the message.
2. **Name Server Provider Interface (NSPI) transaction.** Outlook uses NSPI to verify the group name in the Global Catalog and, if the verification succeeds, it bolds the name in the To field.
3. **MAPI Send.** When the user clicks the Send button, Outlook uses MAPI to transmit the message to the user's home Exchange server.
4. **Group Expansion.** The Exchange server sees that the recipient is a group, and it sends an LDAP query to a Global Catalog server asking for the ultimate recipients who are members of the group along with a list of e-mail attributes that it needs for each of those recipients.

The Global Catalog server obtains the names of the ultimate recipients from its copy of Active Directory along with the requested e-mail attributes. If the list includes any mail-enabled groups, the Global Catalog server expands the membership of each of those groups and repeats the process recursively until it has assembled a full list of all ultimate recipients in each of the nested groups. It returns this list to the Exchange server.

5. **Message Routing.** The Exchange server then sends a copy of the message to each of the ultimate recipients. If multiple recipients have mailboxes on the same server, the Exchange server sends a single message tagged for delivery to the recipients. This "single instance messaging" complements the "single instance storage" for messages on the target server.

This process of expanding group membership lists and returning the results to an Exchange server happens hundreds, if not thousands, of times a day. You want to support Exchange with good-quality, high-powered Global Catalog servers and you need enough of them to handle both expansion requests and the GAL requests coming from Outlook clients.

In production, start with a minimum of two Global Catalog servers for each Exchange server. To scale from there, Microsoft recommends a 4:1 ratio between the number of processors in your Exchange servers and the number of available Global Catalog servers. For example, if you have two 4-way Exchange servers in an office, you should have two Global Catalog servers in the same location.

Designating Expansion Servers

When an Outlook user sends a message to a group, the user's home Exchange server works with a local Global Catalog server to expand the group's membership. Under most circumstances, the user's home Exchange server does the expansion by working with a local Global Catalog server. The term "local," in this case, means local to the Exchange server, not necessarily local to the user. In some circumstances, you might want to specify a specific Exchange server to handle the group expansion. These circumstances include

- **Mail-enabled global groups.** If you have multiple domains in your forest, you want to use Universal groups for e-mail distribution because the Global Catalog contains the membership list. If you use a Global group instead, you should target the expansion of that group to an Exchange server in the same domain. Otherwise, if a user in another domain sends a message to the Global group, the Exchange server in that user's domain cannot expand the group membership because the Global Catalog does not contain the membership list for Global groups.
- **Localized mail delivery.** If all members of a particular Universal group reside in the Asia Pacific region, it might make sense to specify an Exchange server in Taipei as the expansion server rather than letting an Exchange server in Phoenix or Amsterdam expand the membership and send the messages.

If you decide that you need to designate an expansion server for a group, do so using Active Directory Users and Computers (ADUC). Open the group's Exchange Advanced Properties window, shown in Figure 5.9. Notice that a group is assigned to an Administrative Group. The expansion server must reside in the same Administrative Group.

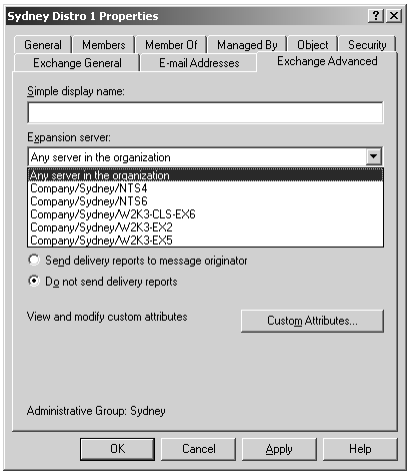

Figure 5.9 Selecting an expansion server for a group.

Single Point of Failure

If you designate an Exchange server as an expansion server for a group or groups, e-mail sent to that group does not arrive, when you take that server down for maintenance. The Exchange server will log a warning about the inability to find the expansion server, and messages queue up for delivery to the recipients. Keep this in mind as you schedule maintenance on your Exchange servers.

You might want to determine if groups have been assigned to a single expansion server. The Active Directory Users and Computers console does not have a standard query to find groups with expansion servers. You can use the Saved Query option to create a custom LDAP search using the Active Directory attribute that stores the expansion server name. This attribute is called msExchangeExpansionServerName.

The msExchangeExpansionServerName attribute stores the distinguished name of the expansion server in X.521 format; for example, o=organization,ou=site,cn=configuration,cn=servers,cn=servername. You can't just match the first few letters, so the search must use a wildcard to represent the initial part of the name. Here's the LDAP filter syntax that searches for every group that uses W2K3-EX1 as an expansion server:

```
(&(objectCategory=group)(mailnickname=*)
➥(msExchangeExpansionServerName=*w2k3-ex1)
```

If you have thousands and thousands of mail-enabled groups, this search could take a while to run because it uses a wildcard at the start of the attribute string.

Managing Group E-Mail Properties

You can control the way Exchange distributes mail to members of groups used as distribution lists. To start, select a mail-enabled group in Active Directory Users and Computers and open the Properties window. The Exchange General tab comes up first, as shown in Figure 5.10.

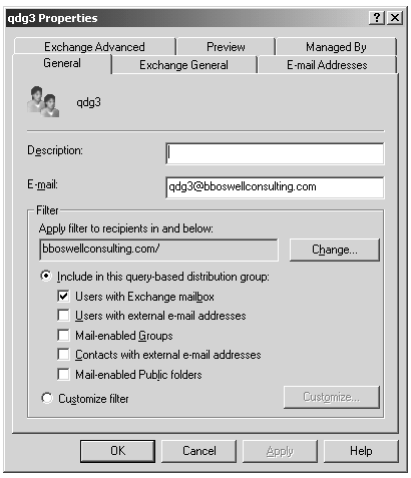

Figure 5.10 General properties for a mail-enabled group.

General Properties

In most circumstances, you don't want a user sending the latest Star Wars Kid AVI to a distribution list with thousands of recipients. In fact, you don't want users sending indiscriminate messages to any group they happen to pick from the GAL.

The Message Restrictions settings give you control over these and other situations. For example, let's say you have a group titled Corporate Executives that contains the accounts of, well, corporate executives. You probably don't want folks sending messages to this group saying, "This company *really* sucks!" unless that person has been authorized to voice such an opinion. You can set the Message Restrictions so that only members of specified groups can send messages to the Corporate Executives group.

If you don't want users from outside the company to send messages to a particular group, you can check the **From Authenticated Users Only** option. This prevents spammers from targeting a corporate distribution list on a public-facing Exchange server.

If a sender does not meet the Message Restrictions criteria, Exchange returns a Non-Delivery Report (NDR) stating that the sender does not have permission to send to this recipient.

Advanced Properties

Select the Exchange Advanced tab in the group's Properties window. Figure 5.11 shows an example. Use settings in this tab to hide groups from the GAL and to specify NDR Report handling.

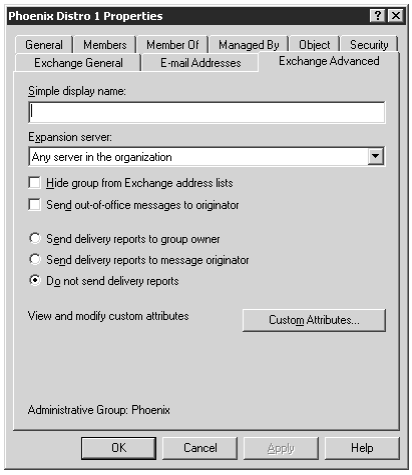

Figure 5.11 Advanced Exchange properties of a mail-enabled group.

Hiding Groups

You can help prevent users from sending inappropriate messages to a group by hiding the group from the GAL. You can still send messages to the group (or any mail-enabled object that has been hidden from the GAL) by entering the recipient's full SMTP address; for example, **executives@company.com**.

Do Not Send Delivery Reports

If the system fails to deliver a message to one or more members of a group, you might want the sender to get a NDR. Exchange disables this option by default because it exposes the distribution lists to spammers and other unauthorized persons. If you send a message to a distribution list and get an NDR for each invalid address, you now have a clue about who is and isn't in the company, both a security violation and a privacy violation.

Administrative Group Affiliation

Groups do not have mailboxes, so it might surprise you to see that a group has an Administrative Group associated with it. Exchange uses this Administrative Group to build an X.400 proxy address for mail-enabled objects. This is true even if the organization has been shifted to Exchange Native mode.

If you do not use X.400 connectors, then this requirement doesn't have an impact on production. If you do use X.400 connectors, then be sure to affiliate a mail-enabled group with the correct Administrative Group, so that messages sent to the group get routed correctly through the connector.

Hiding Group Members

When you mail-enable a group, you expose the group's membership list to MAPI clients. An Outlook user can open the GAL, right-click a group, and select **Properties** to see the group members, as shown in Figure 5.12.

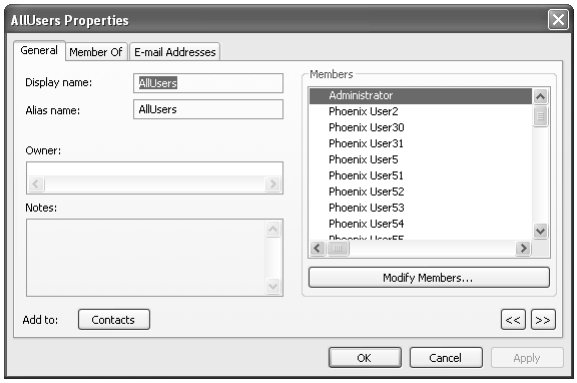

Figure 5.12 Outlook exposes members of a group, which could create a privacy or a security issue.

You might not want Outlook users to see a group's membership because of privacy concerns for the members or because the Windows administrators don't want to expose the contents of mail-enabled Security groups.

You can hide the group membership using the Exchange Tasks wizard for the group. Right-click the group in Active Directory Users and

Computers, select Exchange Tasks from the flyout menu, then select Hide Membership in the Exchange Task wizard, as shown in Figure 5.13.

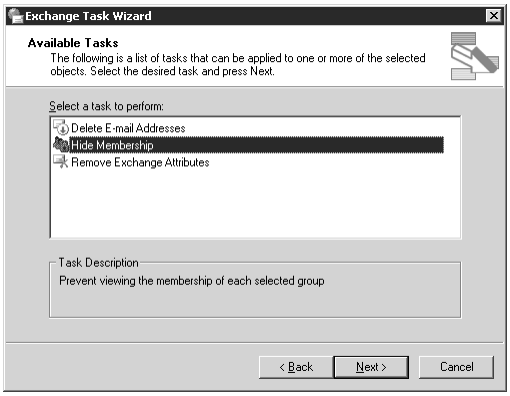

Figure 5.13 Exchange Task wizard showing the Hide Membership option.

Hiding group membership requires some fancy footwork on the part of Exchange. Here's why.

An Active Directory group object has an attribute called Member that holds the list of accounts that belong to the group. If you want to block all Outlook users from seeing the group's membership, Exchange must set a Deny Read permission on the Member attribute for the Everyone group.

But it's not that simple. An Exchange server needs to see the Member attribute so it can send e-mail to the members. That means Exchange can't simply deny access to the Everyone group, because Everyone includes the Exchange server's account.

Exchange solves this problem by changing the sort order for the Access Control List entries on a group object with hidden membership. You can see this for yourself. Use the Exchange Task wizard to hide the membership of a group then open the Properties window for that group in Active Directory Users and Computer and select the Security tab. You'll get a warning that the contents can't be modified. Acknowledge the warning and proceed.

Click **Advanced** to view the Advanced view of the Security tab, as shown in Figure 5.14. This view shows the access control entries in the order that the operating system evaluates them when determining access authorization. Each line corresponds to an Access Control Entry

(ACE), which contains the SID of a user or group and the permissions assigned to that SID. (The interface communicates with a Global Catalog server to replace the bare SIDs with their friendly names.)

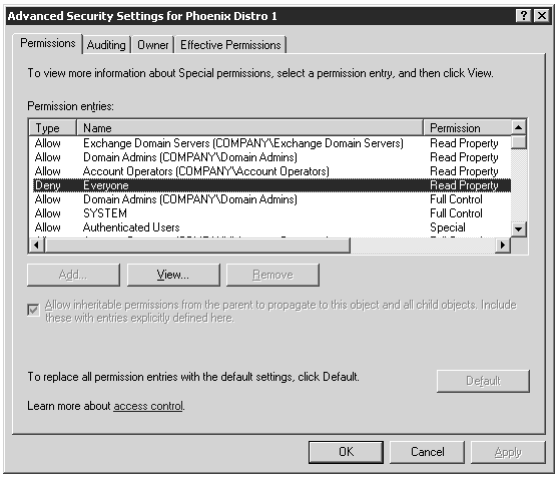

Figure 5.14 Advanced view of ACL for group with hidden membership showing non-canonical sorting of permissions.

You'll see that Exchange played a little shell game with the access list. It did indeed give the Everyone group a Deny Read on the Member attribute, but it also put an Allow Read on the same attribute for the Exchange Domain Servers group, the Domain Admins group, and the Account Operators group.

The security subsystem in Windows evaluates access control entries in the order you see them in the ACL Editor. Because the security subsystem encounters the Allow Read assigned to an Exchange server before it encounters the Deny Read assigned to the Everyone group, it gives the Exchange server access to the Member attribute while blocking users and other computers.

This is called *non-canonical sorting*. As shown in Figure 5.14, you can recognize non-canonical sorting when you see a Deny ACE placed below Allow ACEs in the same level of the hierarchy.

Because the ACL Editor always enforces canonical sorting when changing security settings, don't use the Security tab in the Properties page of a group to change the permission settings if the group has been configured to have hidden membership in Exchange.

Query-Based Distribution Groups

Exchange 2003 introduced a new group type called a Query-Based Distribution group, or QDG. Instead of a static Member attribute that you must manually populate with accounts, a QDG uses an LDAP query to build a membership list dynamically.

The power of a QDG lies in its flexibility. For example, let's say you plan to take an Exchange server down for maintenance. You want to notify users of the maintenance but you don't want to bother users on other servers.

You can create a QDG that includes an LDAP filter specifying mailbox-enabled users who have their mailbox on the designated server. You can then mail-enable the group and send it a message. The Exchange server works with a Global Catalog server to expand the group membership by executing the LDAP search.

Creating a QDG

You can use a QDG if you run Exchange 2003 on Windows 2000 or Windows Server 2003. The QDG class is added during the Forestprep stage of Exchange Setup, when new attributes and classes are added to the Active Directory schema.

> Throughout this book, the term "legacy Exchange" refers to all versions of Exchange prior to Exchange 2000.

To create a QDG, the Exchange organization must be in Native mode. Legacy Exchange servers don't know how to process QDGs. If you attempt to create a QDG in Mixed mode, you'll get an error message even though the option exists on the property menu. Create a QDG as follows:

1. Launch Active Directory Users and Computers.
2. Right-click an OU where you want to create the group and select **New | Query-based Distribution Group** from the flyout menu. This opens a New Object window as shown in Figure 5.15.
3. Enter a name for the group, such as QDG5 or Phoenix Recipients or something that reflects the nature of the LDAP query you'll be using.

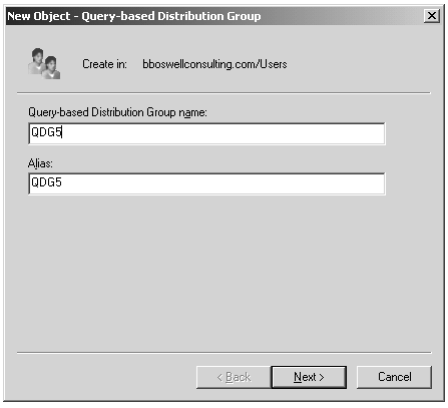

Figure 5.15 New Object window showing alias for Query-Based Distribution Group.

4. Click **Next**. A filter selection window opens, as shown in Figure 5.16.

Figure 5.16 Selecting criteria for membership in a QDG involves creating LDAP query.

5. Check the options you want to include in your search. For example, you might want just users with mailboxes, or just mail-enabled contacts.
6. If you want to be more selective, click **Customize Filter** then click **Customize** to open a Find Exchange Recipients window. Figure 5.17 shows an example with the **Storage** tab selected.

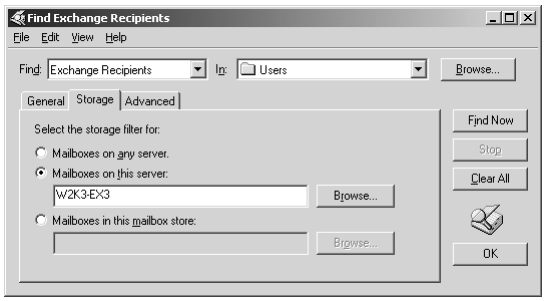

Figure 5.17 QDG selection criteria can target users on certain Exchange servers.

7. The **Advanced** tab of the Find Exchange Recipients window exposes an even more detailed set of search options, shown in Figure 5.18. You can select search criteria that include any attribute of any type of recipient—user, group, contact, or public folder. In the example, the QDG members would include all Exchange recipients (mail-enabled user, mailbox-enabled user, and mail-enabled groups, contacts, and public folders) who work in the Phoenix office. (For this query to work, you would need to have a work process that populates the Office Location field for user objects in Active Directory.)

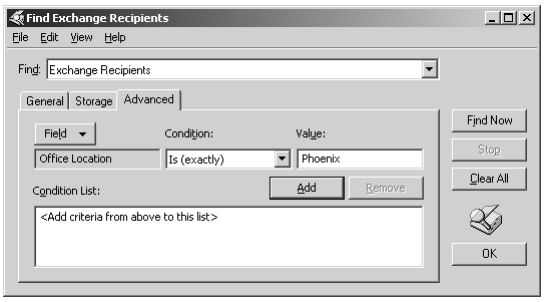

Figure 5.18 LDAP query builder showing advanced selection features that enable selecting a variety of object attributes.

8. Click **OK** then **Next** then **Finish** to create the group. Always preview the result of the LDAP query before using the group by opening the Properties window for the group and selecting the **Preview** tab, as shown in *s*Figure 5.19.

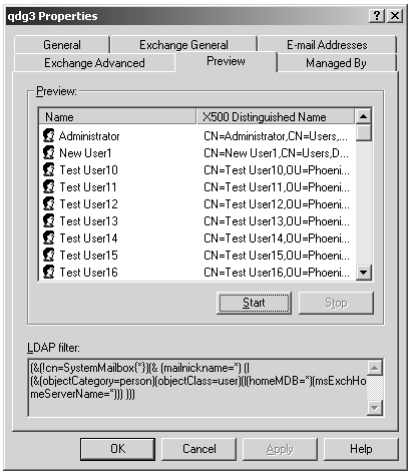

Figure 5.19 Result of an LDAP query shown in the Preview window for a QDG.

It's important that the LDAP search you define for the QDG produces at least one result. If the preview tab does not list at least one recipient, anyone sending a message to the group will get a NDR.

It's also important that you formulate the LDAP query so that only users, groups, and contacts that are able to receive e-mail get included in the result. If the query results in even one invalid recipient, Exchange cannot send a message to anyone in the group. Checking the search results in the preview window can be difficult for a large QDG, so always test the QDG by sending it an e-mail.

QDG Caveats

When a user addresses a message to a QDG, the Exchange server plucks the LDAP search criteria from the QDG definition and sends it to a Global Catalog server along with a list of e-mail attributes it needs for the group's members. The Global Catalog server executes the LDAP search, looks up the e-mail attributes for each member, and returns the result to the Exchange server. The Exchange server then sends the message to each member.

You can put fairly complex queries into a QDG, and the result could include a large number of recipients, so using a lot of QDGs could overload your Global Catalog servers. Until you get a feel for their performance impact in your system, use QDGs sparingly. You can nest QDGs

into other groups, so be on the lookout for performance and execution issues with standard groups that have QDGs as members.

If you run Exchange 2003 on Windows 2000, you'll need to adjust the SMTP service to adapt to LDAP page handling to avoid performance problems when using QDGs. This requires a Registry change (documented in Microsoft Knowledgebase article 822897):

```
Key: HKLM | SYSTEM |CurrentControlSet | Services | SMTPSVC |
Parameters
Value: DynamicDLPageSize
Data: 31 (REG_DWORD)
```

DSAccess

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.

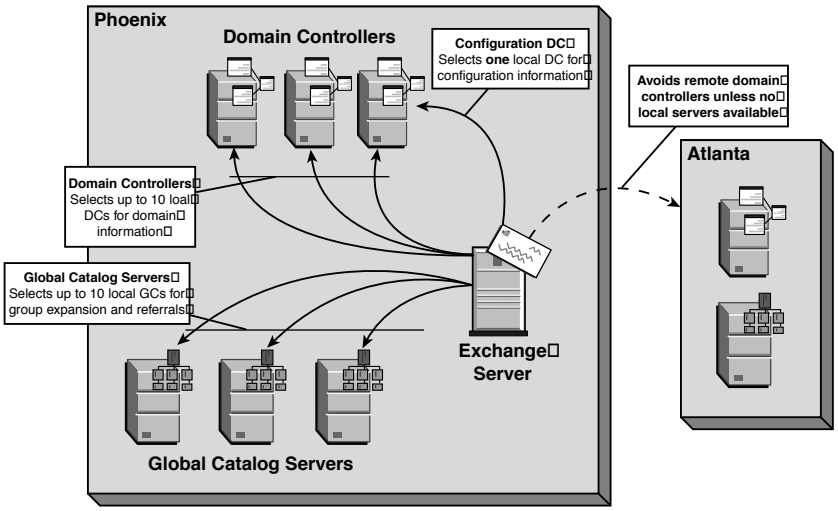

Figure 5.20 Diagram of DSAccess selection based on location.

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.

DSAccess refreshes its cache periodically. You can manually flush the cache during troubleshooting using the Dscflush utility, a free download from Microsoft.

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.

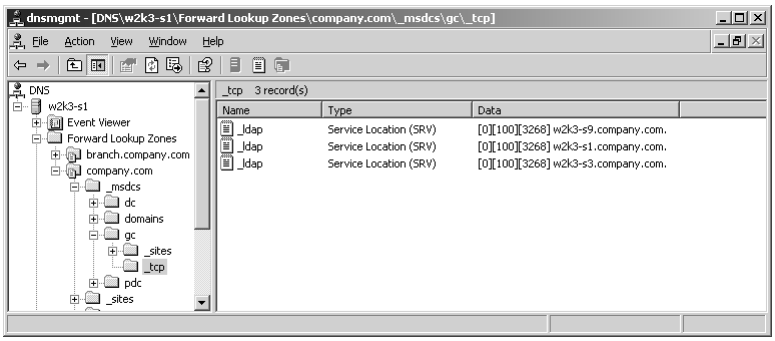

Figure 5.21 SRV records for Global Catalog servers in DNS.

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):

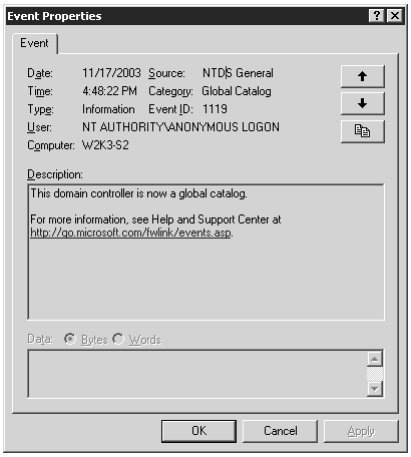

Figure 5.22 Event Log entry announcing that a domain controller has successfully begun operating as a Global Catalog server.

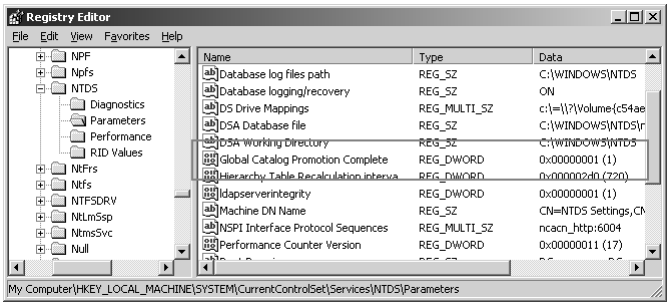

Figure 5.23 Registry entry on newly promoted Global Catalog server.

```
C:\>nltest /dsgetdc:company.com /gc
           DC: \\w2k3-s1.company.com
      Address: \\192.168.0.1
     Dom Guid: 01012378-a008-409d-9696-3c7f16bfbb62
     Dom Name: company.com
  Forest Name: company.com
 Dc Site Name: Phoenix
Our Site Name: Phoenix
        Flags: GC DS LDAP KDC TIMESERV WRITABLE DNS_DC
DNS_DOMAIN DNS_FOREST CLOSE_SITE
The command completed successfully
```

- Use the Netdiag utility that comes in the Windows Server 2003 Support Tools. The following example shows that the server running Netdiag was able to enumerate all domain controllers, it was able to find a domain controller in the local site (W2K3-S1), and it was unable to contact one of the domain controllers (W2K3-S9):

```
C:\>netdiag /test:dclist /v

    Gathering IPX configuration information.
    Querying status of the Netcard drivers... Passed
    Testing Domain membership... Passed
    Gathering NetBT configuration information.
    Gathering the list of Domain Controllers for domain
'COMPANY'

<<<intermediate tests skipped>>>

DC list test . . . . . . . . . . . : Passed

    Find DC in domain 'COMPANY':
    Found this DC in domain 'COMPANY':
        DC. . . . . . . . . . . : \\w2k3-s1.company.com
        Address . . . . . . . . : \\192.168.0.1
        Domain Guid . . . . . . : {01012378-A008-409D-9696-
3C7F16BFBB62}
        Domain Name . . . . . . : company.com
        Forest Name . . . . . . : company.com
        DC Site Name. . . . . . : Phoenix
        Our Site Name . . . . . : Phoenix
        Flags . . . . . . . . . : GC DS KDC TIMESERV WRITABLE
DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE 0x8
    List of DCs in Domain 'COMPANY':
        w2k3-s1.company.com
        W2K3-S2.company.com
        W2K3-S3.company.com
        W2K3-S4.company.com
        w2k3-s9.company.com  (this DC is down)
        [WARNING] Cannot ping 'w2k3-s9.company.com' (it may be
down).

The command completed successfully
```

DSAccess Selection Criteria

DSAccess performs a series of tests to determine the suitability of a domain controller or Global Catalog server. The first tests determine whether the domain controller or Global Catalog server can responds to Exchange queries:

- **Reachability.** The server must respond to an LDAP bind request on TCP port 389 for domain controllers and TCP port 3268 for Global Catalog servers.
- **Replication current flag.** DSAccess checks RootDSE on the domain controller to verify that the isSynchronized attribute shows TRUE.
- **Global Catalog flag.** DSAccess checks RootDSE on a Global Catalog server to verify that the isGlobalCatalogReady attribute shows TRUE.
- **Server functional test (Netlogon).** In this somewhat time-consuming test, DSAccess makes an RPC connection to the Netlogon service at the domain controller then checks available disk space, time synchronization, and whether the server participates in replication. You can disable this test for front-end servers in front of firewalls. See Chapter 11, "Deploying a Distibuted Architecture," for details.
- **Operating system version.** Exchange 2003 requires that all domain controllers used by DSAccess run at least Windows 2000 SP3 or higher.
- **Domain Exchange-Ready.** DSAccess looks to see if the Exchange Enterprise Servers group has Manage Auditing and Security Log permissions on the domain controller. This verifies that an administrator has run DomainPrep in the domain and that the changes have replicated to the target domain controller.

The Exchange Support Tools (free download from Microsoft) contains a utility called Policytest that runs the same test as DSAccess to verify that DomainPrep has fully replicated to all domain controllers. It checks see if the Exchange Enterprise Servers group has been granted the Manage Auditing And Security Logs privilege on each domain controller. You'll need Domain Admin rights to run Policytest. Here's a sample listing for three domain controllers:

```
=======================================
Local domain is "Company.com" (COMPANY)
Account is "COMPANY\Exchange Enterprise Servers"
========================
  DC      = "W2K3-S1"
  In site = "Phoenix"
  Right found:  "SeSecurityPrivilege"
========================
  DC      = "W2K3-S4"
  In site = "Sydney"
  Right found:  "SeSecurityPrivilege"
========================
  DC      = "W2K3-S9"
  In site = "SaltLakeCity"
  Right found:  "SeSecurityPrivilege"
```

The next tests determine how DSAccess distributes queries once it has assembled the servers in its profile. DSAccess looks for these configuration settings:

- Weighting in the SRV records
- FSMO (Flexible Single Master Operations) roles (See Appendix A, "Building A Stable Exchange 2003 Deployment Infrastructure," for details.)
- Site where the server resides
- LDAP query performance
- LDAP loading based on current number of connections

All things being equal, DSAccess uses round robin to share load among domain controllers and Global Catalog servers. The final checks determine if a Global Catalog server can actually give authoritative answers to queries. DSAccess verifies the following:

- Global Catalog attribute in the NTDS Settings object for the server set to TRUE
- Correct number of naming contexts

Viewing DSAccess Selection Results

Once DSAccess selects its domain controllers and Global Catalog servers, you can view the results in ESM by opening the Properties window for an Exchange server then selecting the Directory Access tab, as shown in Figure 5.24.

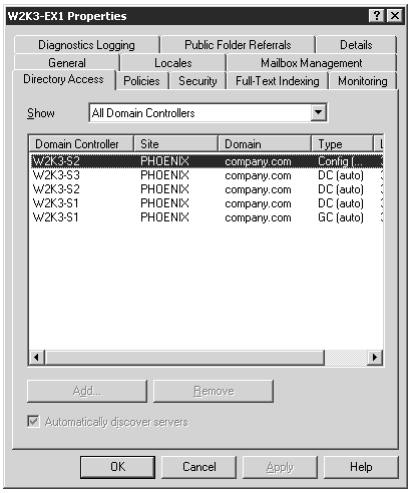

Figure 5.24 Directory Access tab in Exchange server Properties window showing selection of domain controllers and Global Catalog servers.

If you change the selection in the Show dropdown list from **All Domain Controllers** to one of the other selection options, you can uncheck the **Automatically Discover Servers** and manually select a server or servers for that operation. If you select servers manually, include more than one for fault tolerance. DSAccess does not dynamically select a server if it cannot contact any of the statically configured servers.

Event Log Entries for DSAccess Selection Results

If you enable diagnostic logging for DSAccess in the server Properties window in ESM and set the logging level to Medium, you will see a log entry Event ID 2080 from the MSExchangeDSAccess showing the result of the DSAccess evaluation. Figure 5.25 demonstrates an example.

The evaluation includes 10 tests. It's difficult to see in the Event Properties window, but the test results are displayed as columns. You can click the Copy to Clipboard button and paste the result into Notepad if you want a clearer layout. The first column, Server Name, lists the server's Fully Qualified Domain Name (FQDN). Here's a brief description of the content under each column. For more details, see Microsoft Knowledgebase article 316300.

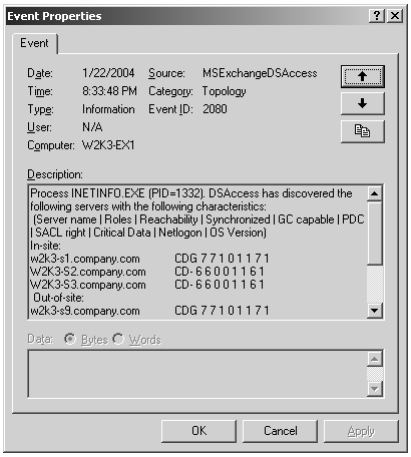

Figure 5.25 Event Log entry showing result of DSAccess domain controller evaluation.

- **Roles.** CDG stands for Configuration, Domain Controller, and Global Catalog.
- **Reachability.** DSAccess uses a numerical system to show whether it can connect to a server via TCP. A successful connection to a Global Catalog server is represented with a 1, 2 means a successful connection to a domain controller, 4 means a successful connection to a configuration domain controller, and 7 means the sum of the first three.
- **Synchronized.** Setting of isSynchronized flag in RootDSE.
- **GC Capable.** Setting of isGlobalCatalog flag in RootDSE.
- **PDC.** Result of "FSMO" check.
- **SACL Right.** Result of "Exchange Ready" check.
- **Critical Data.** Verifies that Exchange organization object exists in Configuration naming context.
- **Netlogon.** Result of "Netlogon"—numerical value must match Reachability value.
- **OS Version.** Must run at least Windows 2000 SP3 to support all features required by Exchange 2003.

DS Proxy

In a modern Exchange system, the Global Catalog servers handle requests for the GAL or a custom address list. They do so using a special service called the Name Server Provider Interface, or NSPI.

As shown in Figure 5.26, the DSProxy service on an Exchange server decides how to handle Outlook clients who need a place to send their NSPI requests.

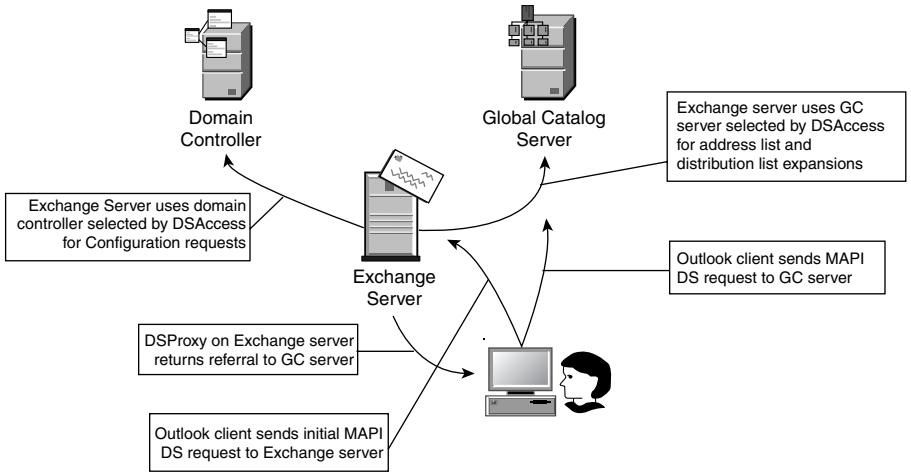

Figure 5.26 Diagram of DSProxy operation.

Name Service Provider Interface (NSPI) Service

Outlook versions older than Outlook 98 service release 2 send their NSPI requests directly to the home Exchange server of the user. The DSProxy service exposes an NSPI interface to handle these requests. The original Exchange client uses MAPI to do name service lookups. DSProxy handles these requests, as well.

When an Exchange server receives an NSPI request from a legacy client, it passes the request to a Global Catalog server for processing. The Global Catalog server determines the content of the address list and

returns the first few items to the Exchange server, which forwards the reply to the legacy Outlook client.

For reasons of security and performance, the Exchange server does not open or modify either the client's NSPI requests or the Global Catalog server's replies.

Referral (RFR)

Modern Outlook clients, Outlook 2000 SR2 and higher, know that Global Catalog servers can handle NSPI requests. These clients connect to the user's home Exchange server and send a request to the RFR service, hosted by DSProxy.

RFR works with DSAccess to determine the name of a qualified Global Catalog server and returns that name to the Outlook client. The Outlook client sends its NSPI requests directly to that Global Catalog server.

Under normal circumstances, the Global Catalog server selected by DSAccess resides in the same site as the Exchange server. But the Outlook client might reside in another location, so the DSAccess choice forces the Outlook client to send its NSPI request across the WAN.

You can set a Registry entry at the desktop running the Outlook client that tells Outlook to use a Global Catalog server in the local site and to ignore the referral from the Exchange server:

```
Key: HKCU | Software | Microsoft | Exchange | Exchange Provider
Value: Closest GC
Data: 1 (REG_DWORD)
```

You can also hardcode the FQDN of a Global Catalog in the Exchange Provider key. The Value name is **DS Server** with a REG_SZ data type. You would not ordinarily want to make this entry except for testing.

To confirm that the **Closest GC** (or **DS Server**) Registry entry worked in Outlook 2003, hold the Ctrl key, right-click the Outlook icon in the Notification Area, and select **Connection Status** from the flyout menu. This opens a Connection Status window that lists the Directory servers selected by the client. To confirm that the entry worked in earlier versions of Outlook, follow these menu items and windows: **Tools | Address Book | Tools | Options | Global Address List | Properties**. This opens a properties window that lists the Global Catalog used by Outlook.

Static DSProxy Port Mappings

If you have a firewall between your Outlook clients and a domain controller, the clients cannot send their NSPI requests directly to a Global Catalog server. You can force the clients to use the Proxy services of DSProxy rather than getting a referral to a Global Catalog server by setting a Registry entry at the Exchange server to disable referrals:

```
Key:
HKLM\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Value: No RFR Service
Data: 0x1 (REG_DWORD)
```

For this to work, you'll need to open a conduit in the firewall to allow the Exchange server to query a Global Catalog server. This requires locking down the NSPI and RFR services to use specific ports. Use the following Registry entries to assign the ports. Work with your Network Services colleagues to select the ports. You might want to use port numbers in the stratosphere of the allowable number space to avoid conflicts. Port numbers from 1024 to 65535 are allowed.

RFR

```
Key: HKLM | System | CurrentControlSet | Services | MSExchangeSA
| Parameters
Value: TCP/IP Port
Data: <port_number> (REG_DWORD)
```

NSPI

```
Key: HKLM | System | CurrentControlSet | Services | MSExchangeSA
| Parameters
Value: TCP/IP NSPI Port
Data: <port_number> (REG_DWORD)
```

Information Store

```
Key: HKLM | System | CurrentControlSet | Services | MSExchangeIS
| Parameters
Value: TCP/IP Port
Data: <port_number> (REG_DWORD)
```

Managing Recipient Policies

A user who wants to get e-mail 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.

Because Exchange 2003 uses Simple Mail Transfer Protocol (SMTP) for internal and external mail routing, all e-mail 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 E-mail 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.

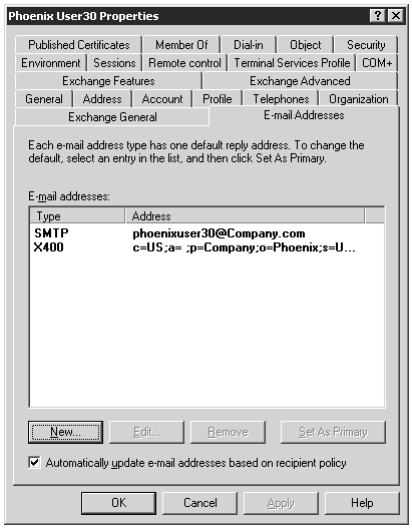

Figure 5.27 Proxy e-mail addresses assigned based on Default Recipient Policy.

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

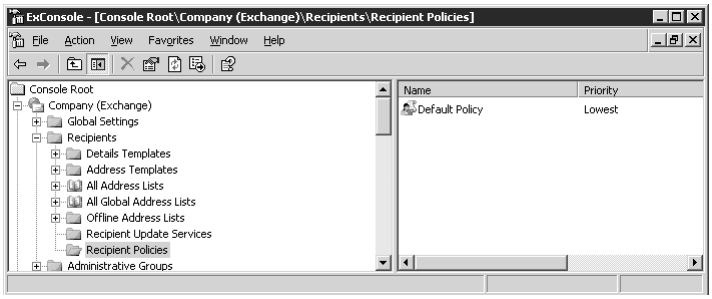

Figure 5.28 ESM console showing Recipient Policies container and Default Policy.

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:

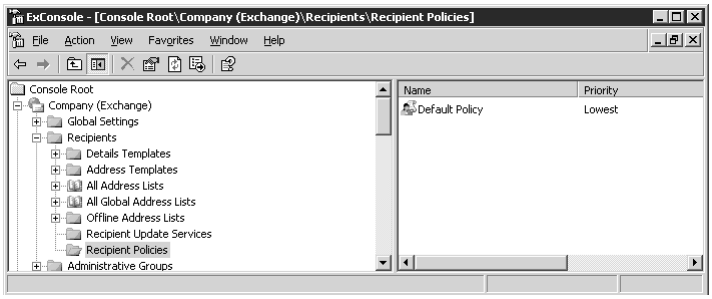

Figure 5.29 Proxy e-mail address selection options in Default Recipient Policy.

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 e-mail Addresses of type(s) SMTP have been modified. Do you want to update all corresponding recipient e-mail 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 E-mail 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 Knowledgebase 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.

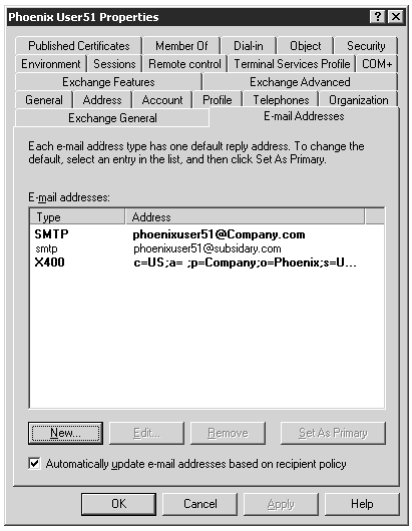

Figure 5.30 Proxy address changes done as the result of changing the Default Recipient Policy.

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 e-mail 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.

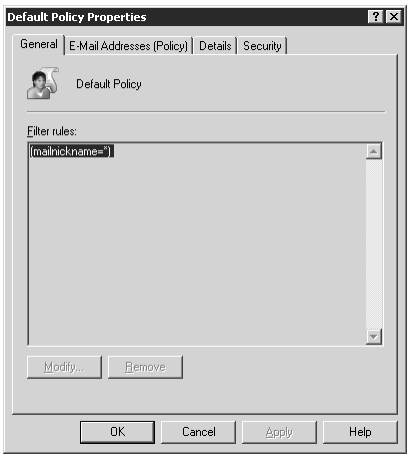

Figure 5.31 LDAP query associated with Default Recipient Policy, which selects all mail-enabled objects in Active Directory (mailnickname=*).

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 e-mail 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 **E-Mail 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 **E-Mail Addresses (Policy)** tab.
5. Click **New** to add a new e-mail address.

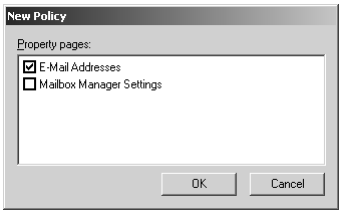

Figure 5.32 New recipient policy with selection for policy type, either E-mail Addresses or Mailbox Manager Settings.

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.

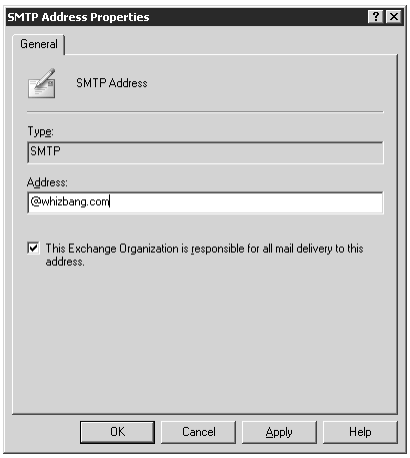

Figure 5.33 SMTP address assigned to new recipient policy.

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.

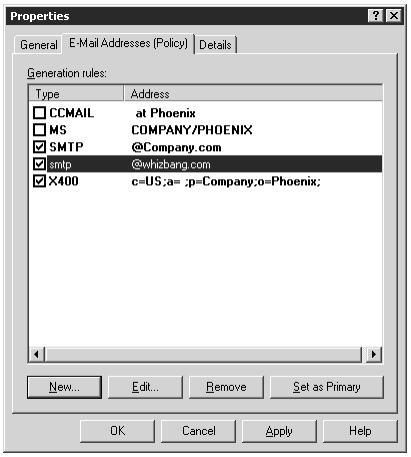

Figure 5.34 Proxy address changes done as the result of adding a new recipient policy in addition to the default policy.

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

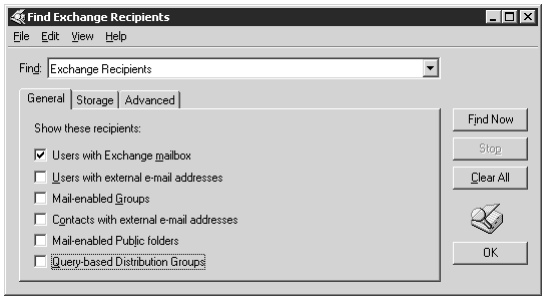

Figure 5.35 LDAP query builder limiting the selection to mailbox-enabled users.

13. Uncheck all options except for **Users with Exchange Mailbox**.
14. Click the **Advanced** tab.
15. Click **Field** 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 e-mail addresses to different groups of users. For example, the Sales department might want to publish e-mail 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.

Recipient Update Service and Proxy Addresses

The Recipient Update Service has responsibility for applying proxy addresses in Recipient Policies to target objects in Active Directory. To prevent conflicts, only one Exchange server in each domain can use RUS to perform updates. You can select this server, and configure other RUS parameters, using ESM.

Drill down under Recipients to find the Recipient Update Services folder. In the right pane you'll find at least two objects, one for Enterprise Configuration and one for each domain with an Exchange server. Figure 5.36 shows an example.

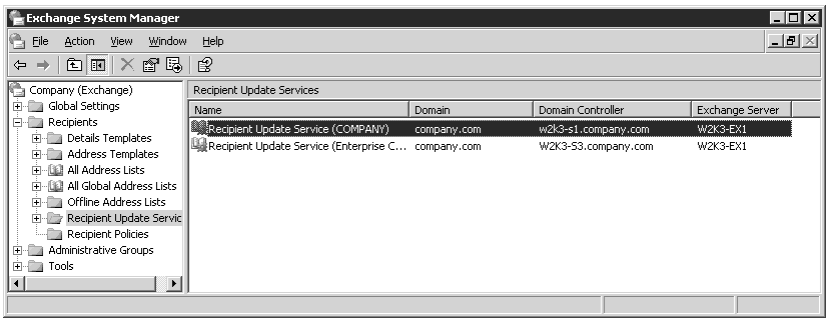

Figure 5.36 Recipient Update Service folder in ESM showing two RUS instances, one for Enterprise and one for the domain.

The Enterprise Configuration item controls the application of policies to system accounts for the Exchange servers. The domain item (or items) controls the application of policies to mail-enabled objects in the specified domain.

Note the Domain Controller and Exchange Server columns for each item. These columns list the Exchange server where RUS runs and the name of the domain controller where RUS sends its LDAP requests. Open the Properties window for the RUS instance to change the server selections and the update interval. Figure 5.37 shows an example.

Before taking an Exchange server offline, check first to see if it hosts a RUS instance. Exchange does not automatically select a new Exchange server to host RUS for a domain if the current server becomes unavailable. You must make this selection manually from the Properties window of the RUS instance. Click the Browse button next to Exchange Server and select another server that is operational and centrally located in your organization.

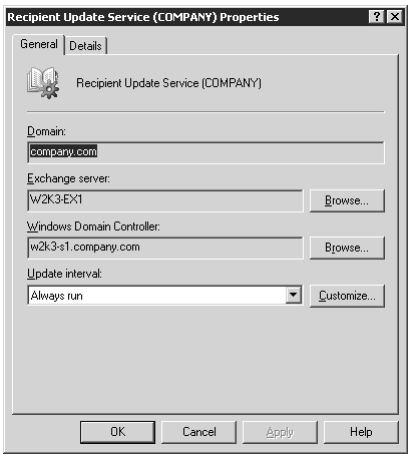

Figure 5.37 RUS instance properties showing server selected to run RUS instance, domain controller selected as the update server, and the update interval.

RUS Intervals

RUS does not wait in the wings for you to change a recipient policy so it can leap out and apply the change. It wakes up periodically, does its chores, then goes back to sleep. You can control the Update Interval using the setting in the Properties window for a RUS instance.

By default, Exchange sets the Update Interval for a RUS instance to Always Run, meaning that RUS fires once a minute.

The Always Run interval relies on an Active Directory attribute called msExchPollingInterval, which has a default value of 60 seconds.

You can select a longer update interval for RUS, but use caution. RUS has other duties in addition to applying recipient policies. For example, RUS also applies address list parameters to mail-enabled objects. If you set an Update Interval of four hours, new recipients will take quite a while to get those address list settings, which delays their appearance in the GAL.

RUS and Multiple Domains

If you have more than one domain, you'll notice that ESM shows a separate RUS icon for each domain. This relates to the way Active Directory uses naming contexts. The users, groups, and contacts you normally deal with are stored in a Domain naming context, and the Exchange server running RUS must communicate with a domain controller in that domain.

RUS can't send updates to all domains via a Global Catalog server because the partial domain replicas in the Global Catalog are read-only.

Exchange system objects reside in the Configuration naming context. The Enterprise Configuration thread of RUS takes care of updating their proxy addresses.

Forcing a Recipient Policy Update

You can force RUS to update Active Directory objects by right-clicking the RUS instance in ESM and selecting either Update Now or Rebuild from the flyout menu, shown in Figure 5.38.

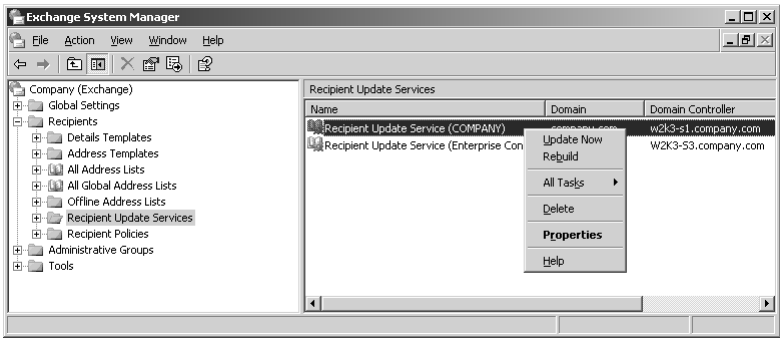

Figure 5.38 RUS instance update options, Update Now or Rebuild.

These selections look simple, but they initiate an intricate set of processes. I'm warning you about this right up front, not to scare you away, but to keep you from wondering, "Why is he making this seem so darned complicated?" It actually *is* darned complicated.

Standard Updates

Let's start with the default way RUS works. Every so often, RUS fires up and gets ready to do its thing. Remember that RUS runs on an Exchange server, so it starts by querying a domain controller for any objects that have been updated since the last time it ran.

Let's say you recently added a mail-enabled user called New User1 with a logon name of **newuser1**. RUS gets the name of that object then performs an evaluation based on the Recipient Policies. Just for the sake of argument, let's say that only the Default Policy applies to this object. RUS sends an LDAP write request to Active Directory that assigns an SMTP and an X.400 proxy address based on the policy. In this case, that would be an SMTP address of **newuser1@company.com** and an X.400 address of **c=US;a= ;p=Company;o=Phoenix;s=newuser1;g=Phoenix**. (The user is in the Phoenix OU of the domain Company.com.)

This is the behavior you get if you select the **Update Now** option from the flyout menu. RUS searches for a new or changed mail-enabled object and applies the first recipient policy that includes that object in its filter criteria. Key point: *Only new and modified objects get updated.*

Policy Changes

Remember that I said this process gets complicated. Here's where the complications begin.

Let's say you want to add a new SMTP address, such as **@companyinformation.com**, to an existing Recipient Policy. You open the Properties for the policy and add the new address and check the box next to the new address to enable it. When you click OK to save the change, a little notification window pops up telling you that the e-mail addresses have been modified and asking if you want to update all corresponding recipient e-mail addresses to match the new address[match what?].

This is an important window. If you don't click Yes, then RUS won't see any changes to apply. If you click Yes, the new proxy addresses in the policy get added to an attribute called GatewayProxy in the Recipient Update Service object, as shown in this listing:

```
gatewayProxy: {98356E20-3000-
4F1DBB4B3852C423E766}smtp:@companyinformation.com;
{98356E20-3000-4F1DBB4B3852C423E766}smtp:@company.com;
{98356E20-3000-4F1DBB4B3852C423E766} X400:c=US;a=
;p=Company;o=Phoenix;;
```

The next time RUS fires, it applies the entries in GatewayProxy to the objects targeted by the search query in the Recipient Policy. It then clears the entries from GatewayProxy.

Rebuilds

If you change the proxy addresses in a recipient policy and you want to apply the new addresses to all existing objects, select the Rebuild option. This sets a flag called msExchDoFullReplication in the Active Directory object that controls the RUS instance, which tells RUS to look at all current objects as well as any new or modified objects. You can see this flag using the ADSI Editor. Figure 5.39 shows an example.

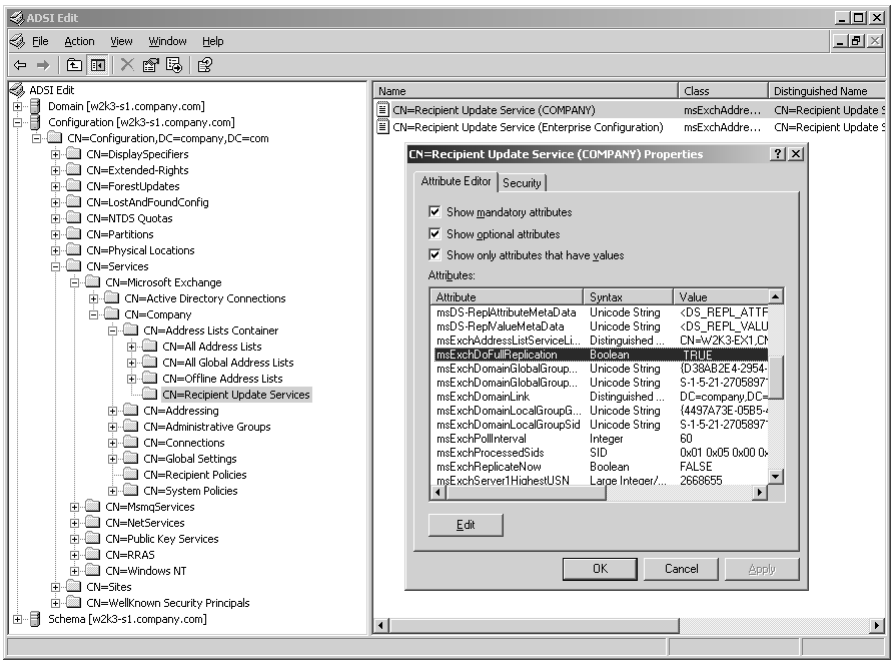

Figure 5.39 ADSI Editor showing msExchDoFullReplication attribute after setting RUS to Rebuild.

When you select Rebuild, you'll get a warning that this could take some time and that it could possibly update a significant number of objects, increasing replication traffic. But if you want to change existing objects, Rebuild is your only option.

But wait…It's not quite that simple.

The Rebuild option does not actually begin rebuild immediately. It only sets the msExchDoFullReplication flag. Nothing happens until RUS reaches its next scheduled start interval.

When RUS fires, it sees the msExchDoFullReplication flag and commences the rebuild. This happens within a minute, if you left the RUS Update Interval set for Update Always, but takes longer if you set the Update Interval to a longer period. Key point: *Rebuild uses the standard RUS update schedule.* Don't expect the changes to take effect immediately if you do a manual rebuild.

Applying Changes Right Away

If you change a proxy address and you want to apply the change to all existing mail-enabled objects, and you want the change to happen **right now**, first select Rebuild then select Update Now. The Rebuild selection primes RUS with the msExchDoFullReplication flag and the Update Now option overrides the update interval.

Policy Scope Changes

It's not over yet. Each recipient policy has a *scope* defined by the content of the LDAP filter. Let's say you define a filter that says, "apply to members of group name Executives." (You should not use group membership as filter criteria for recipient policies, and this example will eventually show you why.) You populate this policy with an SMTP suffix for use by executives and board members and the standard SMTP suffix for your organization.

Later on, you realize that the administrative assistants who work with the executives also need that executive SMTP suffix, so you expand the policy scope to include members of the Executive Admin Assistants group.

When you make a change to the scope of a recipient policy, a little warning window pops up. This window contains a different warning than the previous one, so don't just click it and go on about your business. This warning tells you that the change you just made does not take effect unless you specifically select "Apply This Policy Now" from the flyout menu of the policy. Clicking OK on this warning does not perform any action. It simply acknowledges the message.

This necessity to manually prime RUS with proxy addresses following a scope change makes it possible to have "stealth" scope changes that do not result in an update to the target objects. For example, if you add

an existing user to the Executive Administrative Assistants group, that user will not get the addresses in the Executive recipient policy because nobody has primed RUS by selecting "Apply This Policy Now."

For this reason, you should avoid defining LDAP searches that include group membership as a search criteria when formulating recipient policies or any other feature that relies on RUS. This includes Mailbox Management and Address Lists.

If you experiment with applying group policies manually and you get a result that you don't expect, I recommend using the LDP from the Support Tools to view the current GatewayProxy attribute of the RUS object as part of your troubleshooting. To view the attributes for an object, bind using a standard set of user credentials then select View | Tree and enter the distinguished name of your forest, such as `dc=company,dc=com`. Then drill down through the Configuration container and the Exchange organization container to the RUS objects.

Key Points for Managing Recipient Policies

If the preceding process descriptions make you want change professions, here are a few simple rules of thumb for RUS:

- When creating a new recipient policy, include all addresses that apply to the target recipients. Remember that RUS evaluates each policy in order of precedence. The first policy whose search scope includes a mail-enabled object is the policy that RUS applies to that object.
- When changing the content or scope of a policy, be sure to select Apply This Policy Now from the flyout menu.
- When applying a policy to existing recipients in a domain, select Rebuild followed by Update Now on the RUS service icon for that domain.
- When taking an Exchange server down for maintenance, always check to see if the server hosts a RUS instance for a particular domain or the Enterprise Configuration. If so, select another Exchange server to host that instance until you complete the maintenance.

- Avoid using group membership as a filter for a recipient policy. Only use filters that interact directly with the LDAP search, such as the Department or the Location attributes.

Restricting Mail Storage

Under normal circumstances, you want users to have as much access to your messaging system as possible. Circumstances arise, however, when users take advantage of the system by sending messages with huge attachments to hundreds of users or by storing every bit of e-mail they've received since the start of the Bush administration. (That's George H, not George W.)

In the first Matrix movie, the agent program named Smith whines to Morpheus that he, Smith, has tired of the Matrix and yearns to return to wherever programs live when they don't torture human spirits. Smith compares humanity to a virus, saying, "You move to an area and you multiply and multiply until every natural resource is consumed. The only way you can survive is to spread to another area."

I'm sure you'll agree that Smith had an ax to grind and therefore didn't exactly have an objective opinion, but to tell you the truth, when I look at storage on an Exchange server, I'm tempted to think that Smith stumbled on a bit of truth. No matter how much storage you provide to users, they quickly use it up and cry for more. If you try to draw a line and say, "You get this much storage and no more," users go around you and cry to executive management or buy their own servers and sneer at you in the lunchroom.

Putting the Brakes on Storage Expansion

Users don't appreciate, of course, that the cost of storage only starts with the spindles and RAID cages. You have to back up the store every night and restore it if something goes wrong. If you have more than 16GB of data in your Exchange store, you have to invest in Exchange Enterprise Edition, at a $2,500 price differential. And above all, you have to address concerns about stability and reliability and service level agreements when you have a server with a huge store.

So, for better or worse, in spite of their bellyaching and complaining, the time eventually comes when you have to put limits on the size of your users' mailboxes. The sooner the better, really, before they get spoiled.

You can find the worst offenders by scanning down the list of mailbox sizes shown in ESM. Drill down to a Mailbox Store and see the sizes and item count in the right pane of the console, as shown in Figure 5.40.

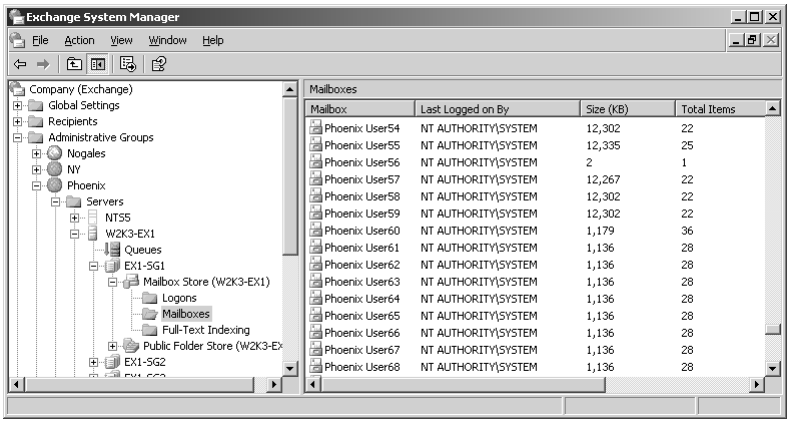

Figure 5.40 Mailbox sizes displayed in ESM. Click the Size column heading to sort the largest mailboxes to the top.

When setting mailbox size limits, select a maximum size that accommodates average use while not overloading your storage capacity. If you have 200 users and a single Exchange Standard Edition server, you would need to impose a quota of 80MB per user to stay under the maximum storage limit of 16GB. If you invest in Enterprise Edition, calculate your quotas based on the maximum size of the databases you want to back up and restore.

There are a lot of ways to decide how to apportion storage. For example, you could use a economist's approach:

- **Capitalistic.** Track the storage consumed by a set of users and charge them for it. To keep data growth in check, economically punish any department that abuses your storage guidelines. "Sure, we'll give you another 16GB of storage. It will cost you $5,000."

- **Socialistic.** Follow the dictum, "To each according to their need." The IT organization purchases spindles and backup equipment out of its own budget then carves out quotas based on the total available storage and takes requests from departments who can prove they need more than their standard allotment. (Leaving chocolate chip cookies and fresh Arabica coffee beans at the entrance to the server room helps to get an allotment increase.)

Storage Policies

You can assign storage limits on individual mailbox stores, but it makes more sense to set a System Policy then assign the policy to the mailbox stores within an Administrative Group.

For example, if you have several Enterprise Edition servers, you can create multiple mailbox stores and use them to categorize users by mailbox usage. You can have a high-quota mailbox store for users who insist on having 500MB mailboxes, and you can have moderate-quota stores for users who are happy with a 25MB limit, and you can have low-quota stores for users who infrequently use the messaging system and only need a 5MB mailbox. You would then create System Policies to enforce these limits and apply the policies to the appropriate mailbox stores.

If your account has been delegated the Exchange Administrator role in multiple Administrative Groups, or on the organization, you could create a System Policy in one Administrative Group and apply that policy to stores and servers in other Administrative Groups. In general, this does not conform to best practices. Compartmentalize your administrative settings whenever possible.

To create a System Policy to set storage limits, proceed as follows:

1. Launch ESM and drill down to the Administrative Group you want to manage.
2. Right-click the **System Policies** icon and select **New | Mailbox Store Policy** from the flyout menu. This opens the New Policy window.
3. Check the **Limits** option under **Property Pages** and click **OK**. This opens a Properties window where you can enter the name you want to apply to the policy. I'll use the name Moderate Quota User Storage Limits.

4. Select the **Limits (Policy)** tab as shown in Figure 5.41. The policy in the example issues an e-mail warning to the user when the total size of the user's mailbox store exceeds 25MB. The policy prohibits the user from sending messages after exceeding 35MB and essentially turns off the mailbox after exceeding 40MB.

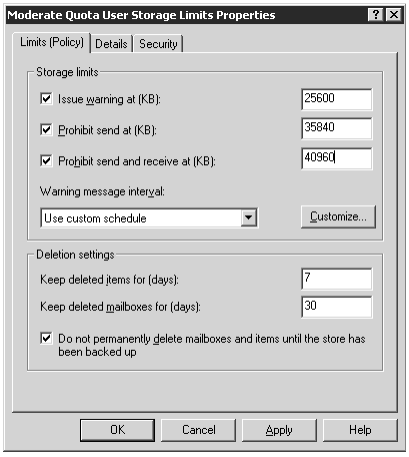

Figure 5.41 Mailbox size limits imposed by storage policy.

5. Click **OK** to save the policy. It will not affect any storage yet. You must first link the policy to a mailbox store before it takes effect.
6. Right-click the new policy in ESM and select **Add Mailbox Store** from the flyout menu.
7. Use the object picker to select the store or stores from your Administrative Group that you want to manage.
8. Click **OK** to save the change. If you want to apply the policy settings immediately, right-click the policy icon in ESM and select **Apply Now** from the flyout menu.

Of the three escalation options, prohibiting incoming mail receipt is the most drastic. Some organizations don't like to block incoming mail for any reason because an important message might get bounced. For example, if a user has exceeded the upper storage limit and has been blocked from receiving messages, a sender will get a NDR similar to the one shown in Figure 5.42.

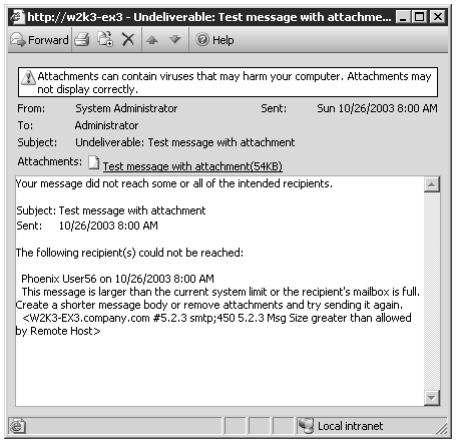

Figure 5.42 NDR sent to user when recipient's mailbox has exceeded quota.

The user gets a warning that the storage limit has been exceeded, but does not get notified when individual messages begin bouncing back to the sender. Before implementing this policy, it's a good idea to get specific approval from management. Your manager's mail could get bounced.

Local Archiving

It doesn't do any good to have quotas if you don't give users a place to put their overflow messages. The Exchange server does not have an offline storage feature for old items. Instead, each Outlook recipient keeps a repository of older messages in an *archive*.

The Outlook archive consists of a PST file called Archive.pst by default. This file contains messages placed there by an Autoarchive service that runs periodically within Outlook. I'm sure you've seen the popup message that asks, "Do you want to archive your messages now?"

To change the autoarchive settings, go to Tools | Options on the main menu then select the Other tab. Look for the second set of options, labeled AutoArchive, shown in Figure 5.43.

Click the **AutoArchive** button. This opens the AutoArchive settings window, as shown in Figure 5.44.

Figure 5.43 Outlook options showing AutoArchive button (second section).

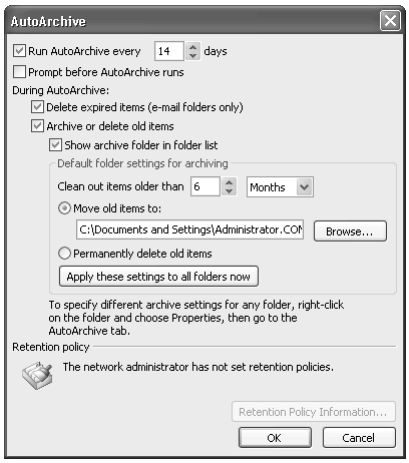

Figure 5.44 Outlook configuration for AutoArchive feature.

Every 14 days (the default interval), the autoarchive process cleans out old messages from the user's mailbox and places them into the archive.pst file. This has several ramifications for desktop support technicians:

- Archive.pst resides in the user's profile. If the technician deletes the profile, all archived messages go bye-bye.

- The archive file resides in a special section of the user's profile called Local Settings. This section does not form a part of a roaming profile. This means that roaming users see different archive contents depending on the machine they use.
- Outlook displays archived items in a separate folder, so users of older Outlook clients who do not have Folder View enabled do not see the archive folder and think their mail has disappeared.

The archive process in Outlook copies an item to Archive.pst then deletes the archived item directly from the folder where it resides. This so-called "hard" delete means that the item does not pass through the Deleted Items container. As you'll see in a bit, you can recover hard deleted items, even when deleted via archiving, if you get to them during the retention interval, seven days by default.

The option to **Prompt Before AutoArchive Runs** keeps the user informed of the archiving process but it also provides the user with the option to say "No, Don't Archive." By archiving in the background, you are more likely to achieve 100 percent compliance with your storage policy. The user can still access the archived messages, but they need to look in the archive folder. This will require a little end-user education. Make sure that any archiving/deletion policy you implement adheres to corporate information retention compliance issues.

Mailbox Management

You might want to take more sweeping enforcement action to limit mailbox sizes. If users can't do their own archiving and cleanup, you can do it for them. The Mailbox Management service cleans out old messages by either deleting them completely or moving them to a cleanup folder for eventual deletion.

The decision whether to impose automated mailbox management depends a lot on money and corporate culture. If you are an administrator in a small company where everyone likes to function with as few rules as possible, and you can convince management to buy as much storage (and backup capacity) as necessary to accommodate the users' needs, then you don't need to control mailbox size. But if you work in a company where you have to fight for every nickel to buy storage and your backup window is stretched to the limit and you can't convince your users that messages they received during the halftime of Superbowl XX can be safely deleted, then automated mailbox management starts to look pretty good.

Mailbox Manager Recipient Policies

A Mailbox Manager Recipient policy controls the selection of items that the Mailbox Management service deletes or archives. To create a Mailbox Manager policy, open ESM and drill down to the Recipients container. Right-click the Recipient Policies folder and select New | Recipient Policy from the flyout menu. This opens a New Policy window as shown in Figure 5.45.

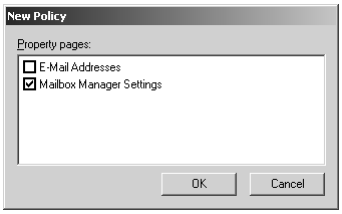

Figure 5.45 New Policy window showing option to select Mailbox Manager Settings instead of E-Mail Addresses setting.

Select the Mailbox Manager Settings option and click OK to open the Properties window for the new policy. Give the policy a name, such as Mailbox Manager Policy. Figure 5.46 shows an example of the default settings. The policy allows a user to keep all messages received in the last 30 days and to keep older messages if less than 1MB in size.

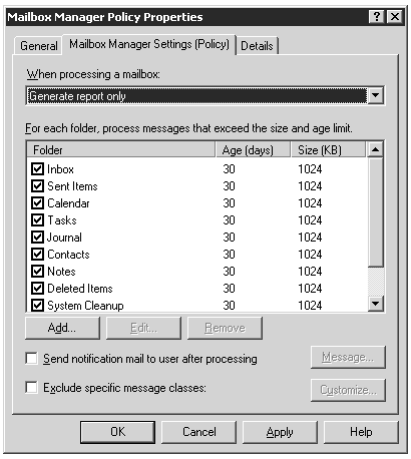

Figure 5.46 Mailbox Manager policy settings.

The **When Processing a Mailbox** dropdown box defines the following actions:

- **Generate report only.** The Mailbox Management service evaluates the content of a user's mailbox against the policy settings and e-mails a report to the user and to an administrator. It does not take any actions to move or delete the messages.
- **Move to Deleted Items folder.** The Mailbox Management service takes each item that exceeds the policy settings and moves it to the Deleted Items folder in the user's mailbox. Users must purge their Deleted Items folders occasionally for this option to have an impact on mailbox size.
- **Move to System Cleanup folders.** If you select this option, items identified by the Mailbox Management service get moved into a new folder called System Cleanup. The folder structure under System Cleanup mimics the folder structure in the user's Inbox so users can find a message quickly if they need to retrieve it. You can create another policy targeted at the System Cleanup folder with a slightly longer interval that deletes the contents.
- **Delete Immediately.** The Mailbox Management service removes the item entirely. This will get your user's attention, I guarantee.

Informing Users of Automated Mailbox Actions

When you enforce mailbox limits, be sure to configure the Mailbox Manager recipient policy to inform the user what happened. Select the **Send Notification Mail to User after Processing** option and modify the message to tell your users the purpose of the scan and the actions they should take.

If you decide to forego playing Mr. or Ms. Nice Guy, you can elect to move the items to a cleanup folder and tell the users where to look for their mail. Figure 5.47 shows an example message.

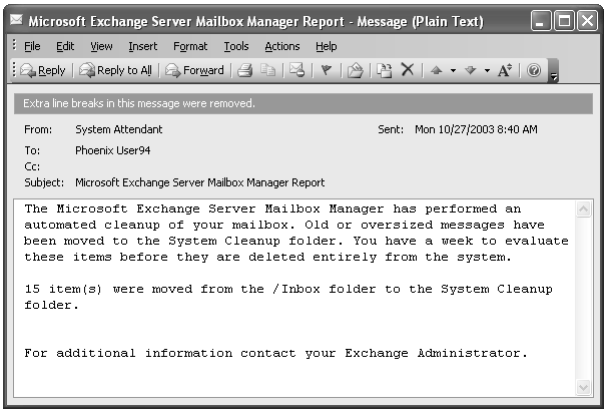

Figure 5.47 Example message sent to user following a Mailbox Manager cleanup.

Targeting Mailbox Manager Policies

You can have separate Mailbox Manager recipient policies for different types of users. For example, you can choose to simply notify some users, to move items into the System Cleanup folders for the majority of users, and to delete items completely for those users singled out as e-mail storage abusers.

To do this kind of targeting, you need to have a way to identify the recipients by a unique attribute that they share in common. The Mailbox Manager recipient policy uses an LDAP filter to identify target users, and you can use the LDAP query builder in the policy to help you create a filter.

Applying Mailbox Manager Policies

The settings you select in a Mailbox Manager policy get applied to a user's mailbox in two stages:

- In the first stage, the RUS finds users who meet the filter rule in the policy. When the RUS fires, it performs an LDAP search using the Filter Rules in the Mailbox Manager recipient policy. If it finds a user who matches the search criteria in the filter rules, it marks the user's Active Directory object with an attribute called MsExchPoliciesIncluded. This attribute contains the Globally Unique Identifier of the Mailbox Manager recipient policy. In

other words, RUS acts a little like a county code inspector who determines that a building does not comply with some statute and places a big red tag on the front door.

- In the second stage, the Mailbox Management service goes through each mailbox in a mailbox store, finds the associated user object for each mailbox, determines if RUS has flagged it with a Mailbox Manager recipient policy, then takes the action defined by the policy.

The next section describes how to configure when the Mailbox Management service runs and where to send a summary report.

Configuring the Mailbox Management Service

The Mailbox Management service runs periodically on each Exchange server with a schedule that you can configure via the Properties window for the server object in ESM. Select the Mailbox Management tab, as shown in Figure 5.48.

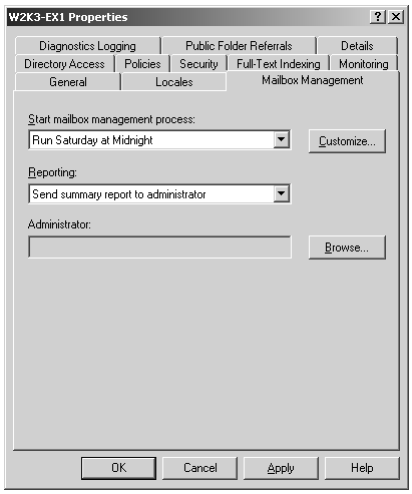

Figure 5.48 Mailbox Management settings on an Exchange server.

The default setting tells the Mailbox Management service not to not run at all. The **Start Mailbox Management Process** dropdown list has two primary options: run each **Saturday at Midnight** or each **Sunday at Midnight**. You can establish a custom schedule if those times interfere with other processes running on the server.

In the Reporting dropdown list, you can choose to send a report to a selected administrator. You have the option of a Summary or Detailed report. Figure 5.49 shows an example of a summary report. Choose the detailed report option only if you want lots and lots of data.

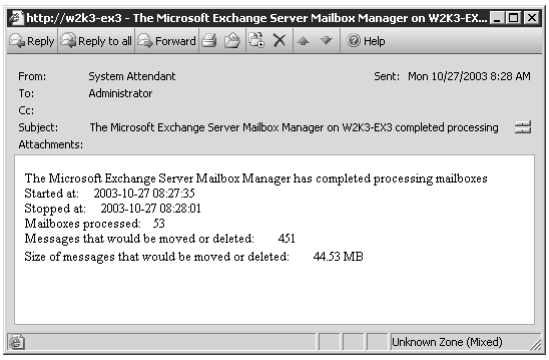

Figure 5.49 Example summary message sent to administrator at the end of a Mailbox Management session.

Manually Initiating Mailbox Management

If you want to test a new set of mailbox management policies, start by right-clicking the new Mailbox Management recipient policy and selecting Apply This Policy Now from the flyout menu. Then right-click the Recipient Update Service instance for that domain, select Update Now, then do it again and select Rebuild. This primes the Recipient Update Service with the new policy and then applies the policy to existing objects that meet the search criteria.

Once you've flagged the user objects in Active Directory using RUS, you can run the Mailbox Management service manually on a server using ESM. Right-click the server icon and select the **Start Mailbox Management Process** option as shown in Figure 5.50.

The system does not give you any progress bars or any other indication that the Mailbox Management process has completed. Instead, look for a summary report in your inbox. For troubleshooting, you can increase the diagnostics logging for the Mailbox Management item under MSExchangeSA in the properties window of an Exchange server in ESM.

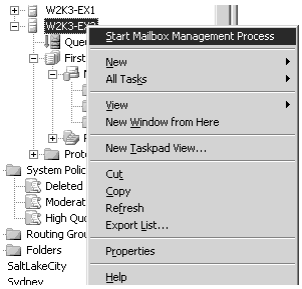

Figure 5.50 Manual initiation of Mailbox Management using Exchange server property menu.

Blocking a User's E-Mail Access

It sometimes happens that a user needs educating that access to corporate e-mail is a *privilege*, not a *right*, and that you can revoke this privilege if it gets used improperly. For example, consider a user who sends an e-mail to the entire GAL announcing that the user's manager is capable of performing certain improbable acts of personal gymnastics. If the user retains his or her job, you might want to restrict the user's e-mail access for a while. Exchange offers a variety of alternatives for temporarily or permanently removing a user's e-mail access.

Disable the User's Active Directory Account

One particularly draconian way to block a user from getting access to a mailbox is to disable the entire user account, as shown in Figure 5.51. Users who have been denied access to the network cannot access their e-mail through any client protocol, including HTTP/WebDAV (Outlook Web Access) and POP3/IMAP4.

This option has the unfortunate (depending on your perspective) result of causing Exchange to bounce any incoming messages to the user. This sometimes causes a problem when the user interacts with customers or vendors. If this is the case, use one of the other options or refer to Microsoft Knowledgebase article 278966 for hints on avoiding message bounces.

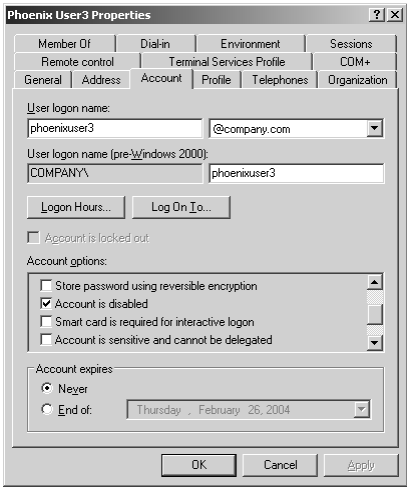

Figure 5.51 User properties in Active Directory showing Account Disabled flag.

Remove the User's Mailbox

You can remove the link between a user's object in Active Directory and the user's mailbox in Exchange by using the Delete Mailbox option in the Exchange Task wizard. Right-click the user's object in Active Directory Users and Computers, select Exchange Tasks from the flyout menu, then select Delete Mailbox from the list of tasks. (You can access this same task list from the property menu for a mailbox in Exchange System Manager.) Figure 5.52 shows an example.

The Delete Mailbox option results in the removal of the user's name from the Global Address List, the digital equivalent of banishment. Users sometimes get perturbed when you do this to them. Get written permission first.

By default, deleting a user's mailbox does not actually delete the user's messages in the mailbox store. Exchange retains a user's mailbox for 30 days, by default, before deleting the mailbox and its contents. (This value can be changed. See "Deleted Mailbox Retention" later in this chapter.) Any mail sent to the SMTP address of a deleted user gets bounced with a "Recipient Not Found" message.

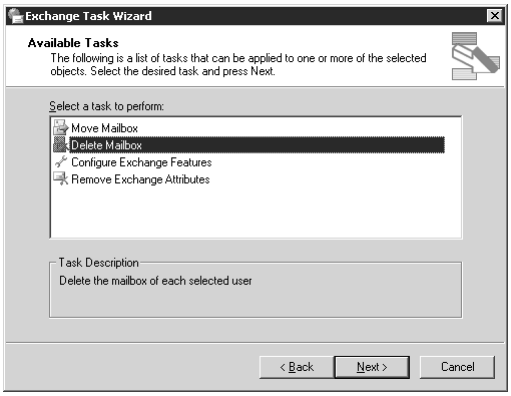

Figure 5.52 Exchange Task wizard showing option to delete user's mailbox.

Deny Access Permission to the User's Mailbox

If you want the user to continue to receive mail but you don't want the user to read that mail, you can block access using mailbox permissions.

Open the Properties window for a user, select the Exchange Advanced tab then click Mailbox Rights. The Permissions window for the selected user opens with the Mailbox Rights tab selected, as shown in Figure 5.53.

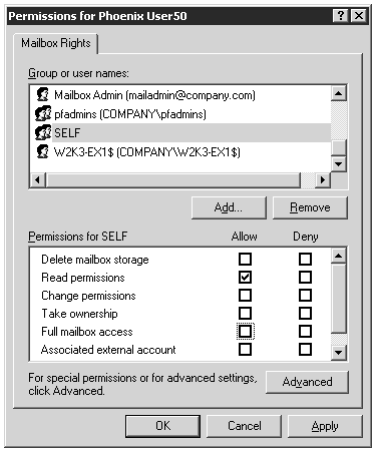

Figure 5.53 Mailbox Rights window for user mailbox showing how to remove Full Mailbox Access from user.

The permission list contains an entry called SELF. This well-known SID acts as a placeholder for the user account represented by the Active Directory object where the ACL resides.

Uncheck the Allow option for SELF and click OK to save the setting. By removing the Allow permission for SELF, the user continues to appear in the GAL and can still receive mail but the user cannot access his or her messages.

Remove Selected Access Protocols

Users can access their mailboxes using any of the supported client protocols—MAP , POP3, IMAP4, and HTTP—as long as the corresponding service has been enabled at the Exchange server. A user can always make a MAPI connection using Outlook, but you can restrict access by the other protocols.

To change the protocol setting for a user, open the user's Properties window in Active Directory Users and Computers and select the Exchange Features tab, shown in Figure 5.54.

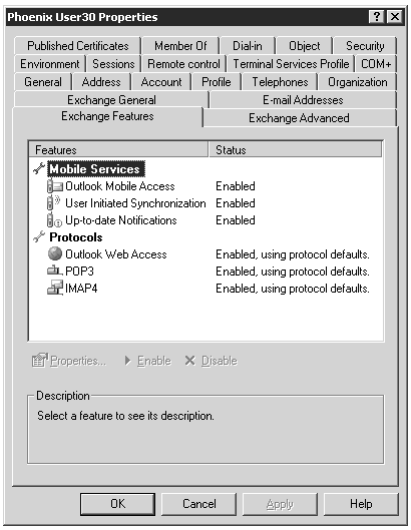

Figure 5.54 User Properties window in Active Directory showing that Exchange Features can be enabled and disabled individually.

If you only want a particular set of users to access Exchange using OWA, you can disable the protocol for all other users.

You can also use the Properties of a particular protocol to determine whether Exchange uses Multipurpose Internet Mail Extensions (MIME) with HTML message bodies or plain text. The Plain Text option prevents potentially harmful HTML content from getting delivered to a user.

Remove the User's Exchange Configuration

If you get into a situation where Exchange refuses to remove the link between a mailbox and a user account due to a configuration error, you can elect to remove all Exchange attributes from the user object using an Exchange Task wizard option called Remove Exchange Attributes (shown in Figure 5.55).

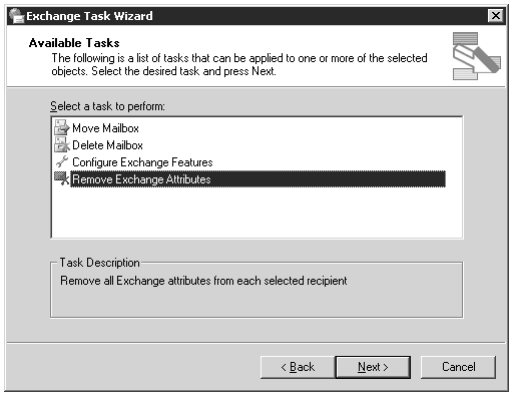

Figure 5.55 Exchange Task wizard showing option to Remove Exchange Attributes entirely.

If you take this action, the user loses mailbox access but the mailbox remains in the store where you can link it to the same or another user. Only use this option if the attempt to delete the mailbox using the Delete Mailbox option fails.

Accessing Another User's Mailbox

Situations arise when a user—maybe you—needs to access another user's mailbox. You can accomplish this in a variety of ways: The user can delegate access to you or another user, you can give access to yourself, or you can grant access to another user.

Delegating Mailbox Access

When an executive or senior manager wants her administrative assistant to screen her e-mail and handle routine items, she can use Outlook to delegate access to her inbox and calendar. Or a user might go on vacation and want some other user to monitor his messages.

An Outlook user can delegate access permissions to another user. The Outlook Options window (Tools | Options in the Outlook menu) has a Delegates tab for this purpose. Figure 5.56 shows an example.

Click Add to add a delegate. Once you select a delegate from the Global Address List, the Delegate Permissions window opens as shown in Figure 5.57.

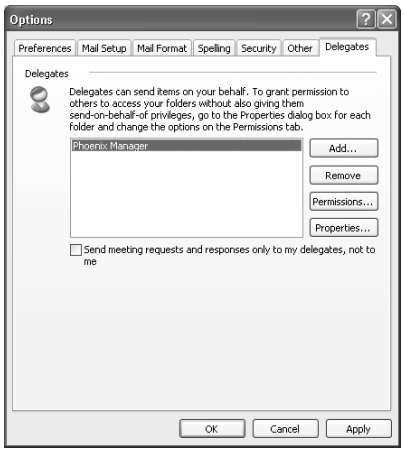

Figure 5.56 Outlook option to select a Delegate for access to user's mailbox.

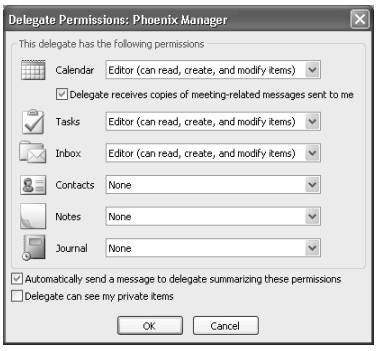

Figure 5.57 Outlook delegate options permitting access to Calendar and Tasks (the default) and to the user's inbox, which enables Send As and Receive As access.

By default, a delegate gets Editor (read, create, modify) rights only to the Calendar and Tasks folders. The user can include other folders or change the level of access using the dropdown box next to the folder.

Accessing a Delegated Mailbox

Once a user has been delegated access to another user's mailbox folders, the delegate can access the folders by selecting the File | Open | Other User's Folder option from the main menu, as shown in Figure 5.58.
If the mailbox owner delegates Editor rights for the Inbox, the delegate can use the From field in Outlook (shown in Figure 5.59) to send mail on behalf of the primary mailbox owner. This highly privileged operation should not be delegated without some thought as to the suitability (trustworthiness, maturity, and so forth) of the delegate.

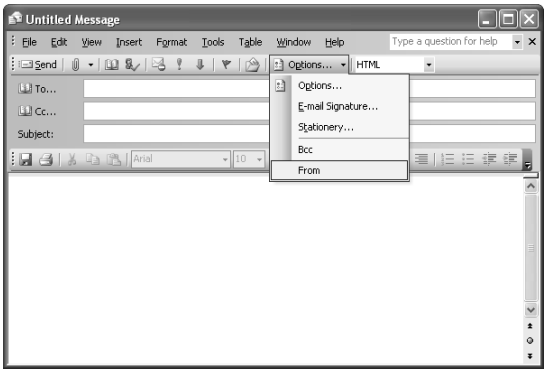

Figure 5.58 Outlook menu option for viewing another user's mailbox folders once delegation has been granted.

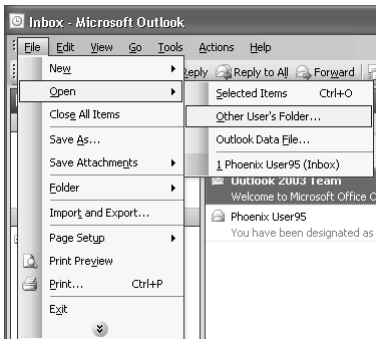

Figure 5.59 Outlook options showing the From field, which permits sending mail on behalf of another user.

Granting Access to Another User

Sometimes you don't have the opportunity to ask a user to delegate mailbox access to you or someone else. The user might have been fired or the security team has the user under investigation. Also, human nature being what it is, sometimes you'll encounter situations where a manager wants to see a subordinate's mailbox without the subordinate being aware of this access. (Don't do this in production until you have a chat with someone in your legal department. You don't want to inadvertently violate a privacy law.)

Grant a user access to another user's mailbox via Active Directory Users and Computers as follows:

1. Open the Properties window for the user's mailbox to which you want to grant access.
2. Select the **Exchange Advanced** tab, as shown in Figure 5.60.

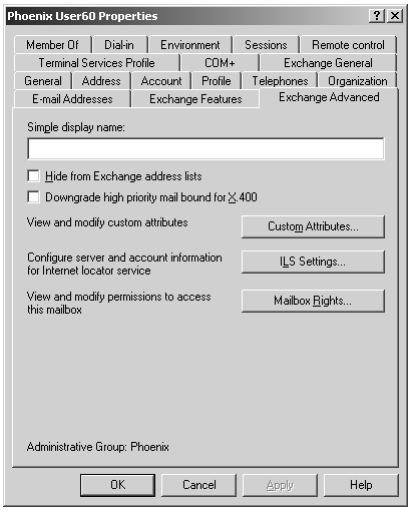

Figure 5.60 Exchange Advanced settings in Active Directory showing the Mailbox Rights button.

3. Click the **Mailbox Rights** button. This opens the Permissions window for the user's mailbox. If the permission list only has SELF, as shown in Figure 5.61, then the user has not yet received any messages and therefore does not have a mailbox. Send the user an e-mail and then the security list will include all the inherited permissions from the mailbox store.

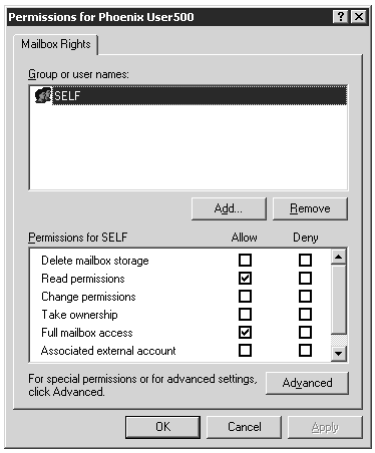

Figure 5.61 Mailbox permissions for user showing a new user that has not yet received e-mail and therefore has only the default mailbox permission settings.

4. Click **Add** and select the name of the user you want to have access to the mailbox. Give this user **Read** permission if they just want to look at the messages and **Full Mailbox Access** if they need to send messages on behalf of the user.

Once you have assigned access to another user, the user can open the mailbox in Outlook using the procedure shown in the "Accessing a Delegated Mailbox" section of this chapter.

Granting Yourself Access to a User's Mailbox

By default, Exchange denies mailbox access to any Domain Admin, Enterprise Admin, the Administrator account, and any account that has been delegated the Exchange Administrator or Exchange Full Administrator role. Figure 5.62 shows the Security tab of the Organization object in Active Directory where the Deny settings reside. If you delegate the Exchange a Full Administrator or an Exchange administrator role on an Administrative Group, then Exchange places the Deny entries on the Administrative Group object.

You can override a Deny inherited from the organization or an Administrative Group by placing an Allow permission on the mailbox itself in Active Directory Users and Computers. Because of the inheritance rules in Active Directory, an Allow applied directly to an object

takes precedence over an inherited Deny. You can grant full access to mailboxes on a per store or per server basis as well. See Microsoft Knowledgebase article 262054 for details.

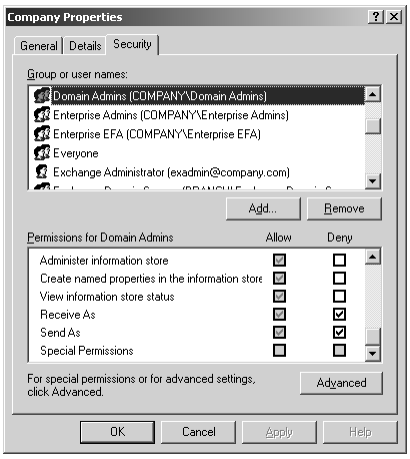

Figure 5.62 Exchange organization object showing how to override default Deny for administrators by applying an Allow for Receive As and Send As permission on mailboxes.

Mail Retention

Users call upon Exchange administrators for help with a variety of problems. Here is a brief list:

- "I deleted an important message, and you have to get it back for me right away."
- "I deleted all the stuff in my Junk Mail folder, but now I think there was an important message in there. How can I check?"
- "I cleaned out all my deleted items like you told me to and now I can't find some messages that I really, really, really need. Get them back for me."
- "I permanently deleted a message that I thought was spam but it turned out to be from a new client and I really need it back because they want me to do something, and I'm going to get fired if I don't do it. Help me out, okay?"

- "I was archiving my inbox last night and Outlook blew up and now I can't see any of my messages. This e-mail system of yours really sucks."
- Finally, one that you might hear from a colleague: "I accidentally deleted a user last night and I recreated the account, but now he can't get his e-mail."

Some of these problems seem trivial, others complex, but they all could require considerable corrective work on your part if you don't take a few precautions.

For example, recovering a user's mailbox (or recovering a single deleted message within a mailbox) involves a lengthy tape restore of the entire mailbox store followed by an extraction and import of the user's mailbox contents. Instead, you can set a retention interval for mailboxes and mailbox items and simply grab the deleted mailbox or deleted item from a hidden container in Exchange and put it back to its original location.

Do you want to do hours of work or seconds of work? Not a tough choice.

Deleted Mailbox Retention

When you delete a user from Active Directory, or remove the user's Exchange attributes by deleting a user's mailbox, Exchange does not immediately wipe the mailbox from the store. Instead, it retains the mailbox intact for a period of time to give you a chance to either change your mind or to assign the mailbox to another user.

Unless you have a regulatory or corporate policy against retaining e-mail, you should leave the deleted mailbox retention settings enabled. It is not uncommon for a user to leave the company then return, or for the user's replacement to want access to the e-mail.

Each mailbox store has a setting that determines the deleted mailbox retention interval. By default, Exchange sets a 30 day interval. You can change the interval using the Limits page of the Properties window for a mailbox store, as shown in Figure 5.63. You can also set a System Policy to manage the retention interval for all mailbox stores in an Administrative Group.

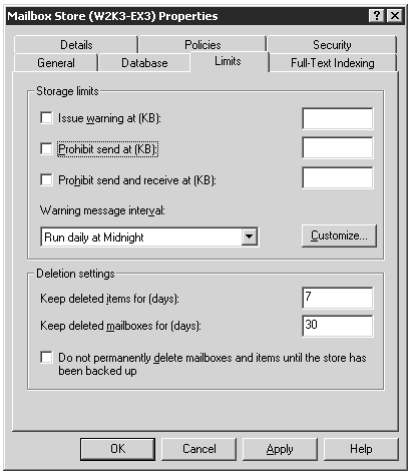

Figure 5.63 Mailbox Store Properties window showing default item and mailbox retention interval.

Deleted User Identification in ESM

Exchange periodically monitors the status of Active Directory users to make sure they still have links to their mailboxes. The Mailbox Cleanup Agent does this work.

You can manually initiate a Mailbox Cleanup Agent session from ESM. Right-click the Mailboxes icon under a mailbox store and select Run Cleanup Agent from the flyout menu, as shown in Figure 5.64.

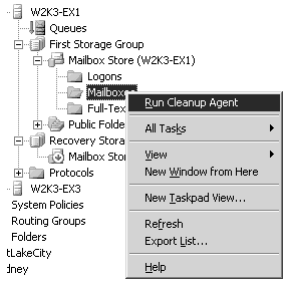

Figure 5.64 Manually initiating Cleanup Agent using Mailbox Store property menu.

If the Mailbox Cleanup Agent determines that a mailbox no longer has an owner, it flags the mailbox in ESM with a big X next to the original owner's name.

You might also notice that the "Last Logged On By" entry for the mailbox shows a bare SID, indicating that the system cannot resolve the SID to a friendly name because the user account has been removed from Active Directory.

Recovering the Deleted Mailbox

Once the Mailbox Cleanup Agent has flagged a mailbox as having no link to a User object, you can then link the mailbox to another user who does not have a mailbox.

You must see a red X on the mailbox in ESM before you can relink the mailbox. If you delete a user but you do not see a red X, manually initiate the Mailbox Cleanup agent for the mailbox store. You might need to wait a few minutes and refresh the console before the red X appears.

Right-click the mailbox in ESM and select Reconnect from the fly-out menu. Use the object picker to select a new account for the mailbox. Exchange updated the Active Directory account and the mailbox and ESM shows the selected user as the new owner after you refresh the console. The process only takes a few seconds.

You must have Exchange Full Administrator privileges to link a mailbox to another user. This gives your account permission to scan the Deleted Objects container looking for the original user. If someone with simple Exchange Administrator permissions attempts to reconnect a mailbox, the system refuses to comply and displays an error saying that the administrator does not have the rights to complete the operation.

Deleted Item Retention

Now let's deal with the users who accidentally delete a message, calendar appointment, or task item from their mailbox. Ordinarily, Outlook simply moves deleted items to the Deleted Items folder where the user can drag them back.

Things get a bit more complicated if the user empties the Deleted Items folder. You might get a panicked call when the user discovers that an important message got purged.

Exchange comes to the rescue in these situations by not actually deleting items when the user empties the Deleted Items container. Instead, Exchange gives the items a special mark that flags them as

purged so that they do not display in Outlook or an Internet client. The messages remain available for recovery for a period of time—seven days by default—and you can do the recovery in Outlook and OWA.

Recovering Purged Items from the Deleted Items Folder

You can walk a user through this process. Have the user highlight the Deleted Items container then select Tools | Recover Deleted Items from the flyout menu, as shown in Figure 5.65.

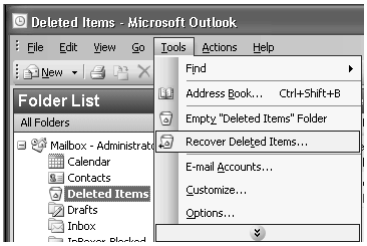

Figure 5.65 Outlook menu option showing deleted item recovery option for Deleted Items folder.

This opens a Recover Deleted Items From—Deleted Items window, as shown in Figure 5.66.

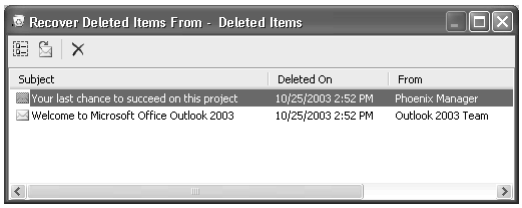

Figure 5.66 Recover Deleted Items From window showing items still marked for retention at Exchange server.

Highlight the item you want to recover and click the Recover Selected Items menu. This moves the item back into the **Deleted Items** folder where the user can then drag the item into another folder.

Deleted items obey the same single instance storage rules as any other item in the Exchange Store. If a message gets sent to 20 recipients who share the same mailbox store, only one copy of the item actually

resides in the store, whether or not the item has been flagged for purging. This means you can increase the interval from seven days without getting a tremendous increase in the size of the Exchange store.

Recovering from "Hard" Deletes

Ordinarily, deleted items pass through the Deleted Items folder on the way to oblivion, so recovering purged items from Deleted Items makes sense in most cases. Here are some exceptions:

- The user presses Shift+Del to delete the item.
- A POP3 user deletes a message, or an IMAP4 user purges a message without first deleting it.
- An offline user deletes an item then purges the Deleted Items folder before syncing with Exchange.

Microsoft calls these "hard" deletes because they don't pass through the Deleted Items folder. As it turns out, though, Exchange treats hard deletes just like any other deleted item. It simply flags the item as purged and retains it for the duration of the Deleted Item Retention period, seven days by default.

If you want to recover hard deleted items, set a Registry entry that allows Outlook to expose the Recover Deleted Items window from any folder, not just the Deleted Items folder:

```
Key: HKLM | SOFTWARE | Microsoft | Exchange | Client | Options
Value: DumpsterAlwaysOn
Data: 1 (DWORD)
```

Ordinarily, it's not a good idea to let the users believe that a "hard" delete truly lasts forever because they might recover a virus-laden message that they originally deleted using Shift+Del.

Managing Recipients with System Policies

Up to this point, you've configured recipient storage using settings on individual mailbox stores. You can avoid all that work by setting up system policies that control the same settings for all the mailbox stores on servers in an Administrative Group. These system policies override settings applied locally.

Create and manage system policies using ESM by drilling down under an Administrative Group to the System Policies folder. Figure 5.67 shows an example with a few policies already created.

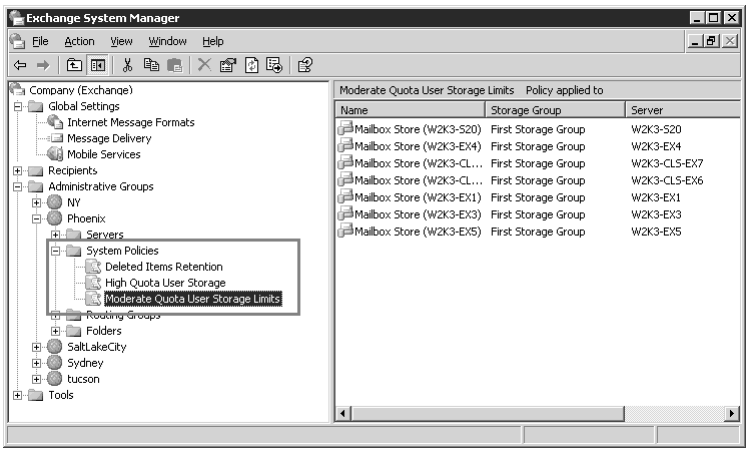

Figure 5.67 ESM showing the System Policies folder in an Administrative Group with a few policies already in place.

Creating New System Policies

To create a new system policy, right-click the System Policies folder and select New then select one of the object types to manage: Public Store Policy, Mailbox Store Policy, or Server Policy. Figure 5.68 shows the menu.

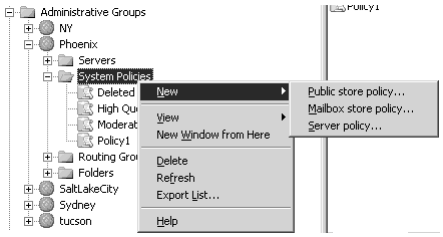

Figure 5.68 Options for creating new types of system policies in the System Policies property menu.

When you select an object type, a New Policy window opens. The window divides each policy into options that correspond to tabs on the Property window for the associated object type. For example, a Public Store policy can manage settings on the General, Database, Limits, and Full-Text Indexing tabs, as shown in Figure 5.69.

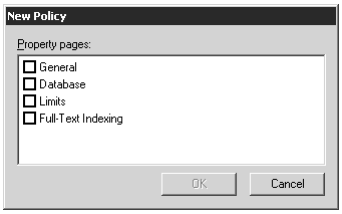

Figure 5.69 Options for property tabs to include in the new system policy. Tabs can be added after the policy has been created.

Once you select a property page or pages to include in the policy, the resultant Properties window (example in Figure 5.70) shows the associated tabs and their settings.

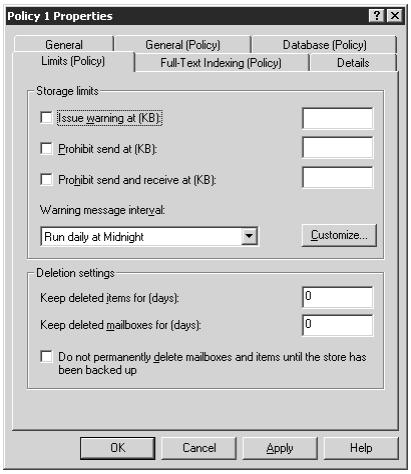

Figure 5.70 System Properties settings showing that the tab in the properties mimics the tab in the local policy.

Targeting a System Policy

System policies do not take effect until you link them to one or more mailbox stores, servers, or public folder stores. To do this, right-click the policy icon and select the Add option that matches the policy type you created. A Select Items window opens that lets you browse to the correct object type: mailbox store, public folder store, or server.

Once you link a policy to a particular object, the linked object appears under the policy icon in ESM, as shown in Figure 5.71. You can remove the linked object to return control back to the locally-controlled settings.

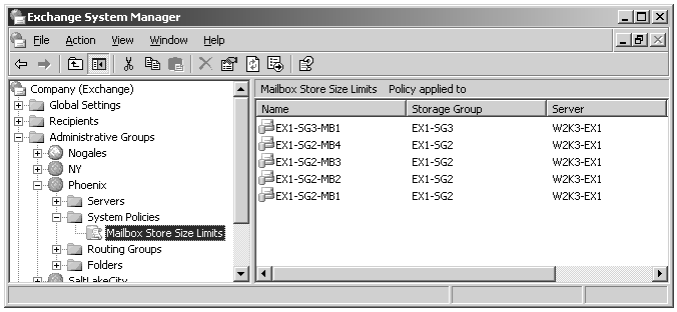

Figure 5.71 ESM showing links from a System policy to selected mailbox stores.

You can link only one property page from one policy to any given property page on a store or server. If you try to link a second, you'll get a warning that the store has already been put under the control of a conflicting policy.

When you link a policy to a property page on a store or server, ESM locks you out from changing the settings locally. If you view the local property page in ESM, you'll see the values set by the policy with the fields dimmed, indicating that you cannot make changes.

To figure out which policy has locked a particular page, click the Policies tab. This lists any policies linked to the store and the property page affected by that policy. Figure 5.72 shows an example.

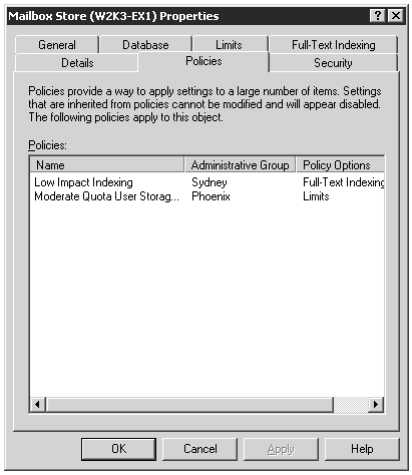

Figure 5.72 List of policies that affect the settings of a local mailbox store. The corresponding property pages would be dimmed in the local policy.

Managing Recipients with Global Settings

The system policies you've worked with so far in this chapter affect only servers and stores within an individual Administrative Group. Some settings require a more universal influence.

Exchange defines a set of *Global Settings* to control certain operations throughout an entire organization. In ESM, the Global Settings container sits right under the root of the Organization.

Exchange defines three types of global settings: Internet message formats, Message Delivery, and Mobile Services. Let's see what each one does.

Internet Message Settings

If you do business with a client from a certain SMTP domain and you want to manage the messages sent to that client, you can impose a policy for your entire organization that targets messages sent to anyone in that particular SMTP domain.

For example, you can create a Message Format policy that determines the format for messages traveling to and from that particular SMTP domain. Figure 5.73 shows an example.

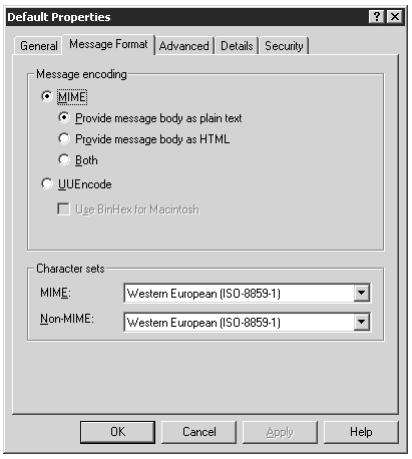

Figure 5.73 Internet Message Settings showing default message encoding and character set parameters.

Exchange Rich-Text Format

The body of a message from older Outlook client might contain Rich Text formatting rather than HTML. You can disable this formatting, forcing Exchange to remove any portions of the message that contain Rich Text features. This significantly reduces the size of the message and makes it more compatible with third party e-mail clients.

Message Text Word Wrap

This option is handy when the client application cannot word wrap a message and the line endings get truncated. The choice of 77 characters fits most text screens.

Additional Messaging Options

The automatic messaging options are disabled by default so that you do not invite spam automatically by replying to an Internet message.

You might want to disable the option to **Preserve Sender's Display Name on Message,** if you do not want the user's friendly name (LDAP display name) to show up on Internet messages. This also helps if your country of origin uses character sets that are not widely recognized. SMTP addresses are required to use ASCII, but your display name might use Unicode characters.

You should leave the delivery and non-delivery report options enabled. They provide helpful information for outside clients who might want an explanation of why their messages are not arriving. If you find that spammers use this information to gain data about your users, disable the options.

Message Delivery Settings

As shown in Figure 5.74, you can specify message size limits to discourage soaking up bandwidth with frivolously large message attachments.

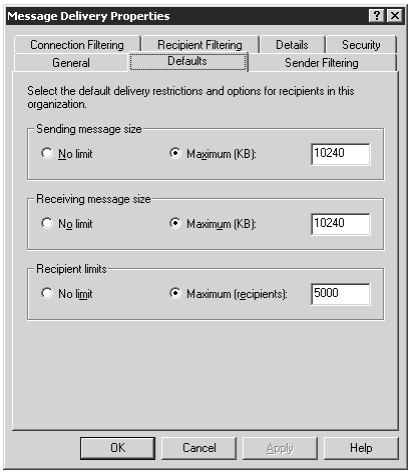

Figure 5.74 Global Message Delivery settings limiting size of mailboxes that affect all Exchange servers. Note the default setting of 10MB, which limits impact of Denial-of-Service (DoS) attacks.

The Default settings get applied to all messages. The filter settings—Sender, Recipient, and Connection—only get applied by selecting the filter at an individual SMTP virtual server or servers. See Chapter 13, "Service Continuity," for more information about using these filter options to block spam and other unwanted e-mail.

Mobile Services Settings

If you want to take advantage of the ability in Exchange 2003 to synchronize e-mail with portable devices or to provide access by handheld devices using Outlook Mobile Access, you can use the Mobile Services settings to enable the services, as shown in Figure 5.75.

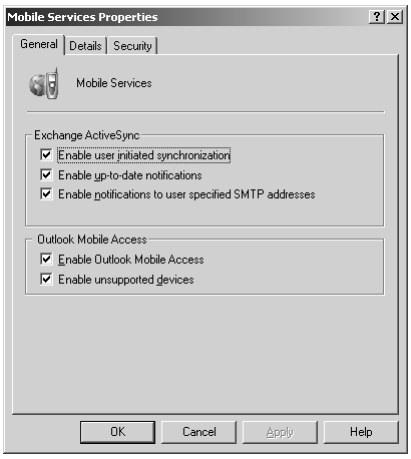

Figure 5.75 Mobile Services settings in Global Settings shown as enabled. Mobile services are disabled by default.

Looking Forward

At this point, you've given users their mailboxes without giving them complete license to dump anything they want into those mailboxes. You gave them distribution lists and a process for managing them that doesn't require an MIS degree to understand. You put a set of controls in place to guide your users towards proper e-mail practices, and you lined the route with graceful landscaping (backed up with electrified barbed wire) just in case they veer too far outside the lines.

Now you're ready to make their life even simpler by giving them a flexible set of address lists that they can access from the office and from home.