

realtimepublishers.comtm

The Definitive Guidetm To

Windows 2000 and Exchange 2000 Migration

Archie Reed

[**Editor's Note:** The following excerpt is from Chapter 8 of the free eBook *The Definitive Guide to Windows 2000 and Exchange 2000 Migration* (Realtimedpublishers.com) written by Archie Reed and available at <http://cc.realtimedpublishers.com/publicationhome.asp?pid=23>.]

Chapter 8: Finalizing the Migration to Exchange 2000

My discussion of migrating to E2K is now in its final stages. In this chapter, we'll describe the final steps of your migration implementation. Going back to the 4DS planning method that I outlined in Chapter 2, you're continuing the Deploy stage and beginning the Sustain, or maintenance, stage.

We'll begin by discussing the remaining steps you need to take to migrate to E2K:

- Moving mailboxes between systems and stores
- Managing mailbox accounts
- Creating contacts
- Creating groups
- Managing administrative and routing groups
- Creating public folder hierarchies
- Deploying OWA
- Implementing clustering
- Decommissioning the Exchange 5.5 organization

Then we'll describe some important management tasks:

- Managing E2K performance
- Providing security for your new E2K environment

Moving Mailboxes between Systems and Stores

In Chapter 7, we talked about upgrading Exchange servers and some considerations for the new storage system in E2K. Both of these issues will play an important role as you move remaining mailboxes from Exchange 5.5 to E2K or as you move mailboxes out of an existing store (database) into a newly created one on your new E2K Server. This procedure is an important process that you need to give careful consideration.

No doubt part of the reason that you're migrating to E2K is to take advantage of the multiple stores in E2K and thus reduce the large, difficult-to-recover, single, private IS of Exchange 5.5 to several more manageable stores. These stores are illustrated in Figure 8.1.

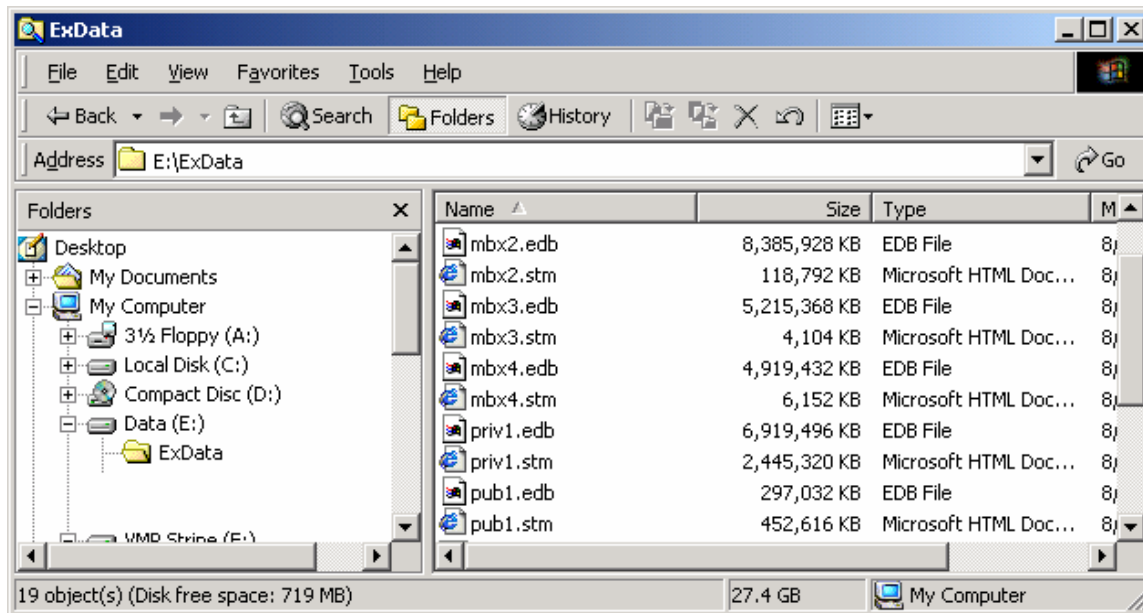


Figure 8.1: Viewing the multiple, more manageable stores in E2K.

Whether you're moving mailboxes between two stores in E2K or from an Exchange 5.5 Server to E2K, the process is the same: You use the Active Directory Users and Computers MMC snap-in, then select the Move Mailbox task; this selection displays the Move Mailbox wizard.

⚠ Although installing E2K allows you to install Exchange Administrator during setup, don't use it to manage an E2K server. The E2K server might respond to Exchange Administrator when it's running in mixed mode, but it won't work correctly. A useful adage is "manage like with like."

A disadvantage of moving mailboxes around is that it breaks the single-instance ratio (in which only one copy of a message sent to several users on the same store is kept in the IS database). If, instead, you upgrade the Exchange 5.5 store in place, single-instance is retained. So make sure to account for this factor when you plan your migration and allow ample disk space for moving users to a new store. If you plan to split apart a large IS, you'll want to look at the Performance Monitor for single-instance ratio, as shown in Figure 8.2.

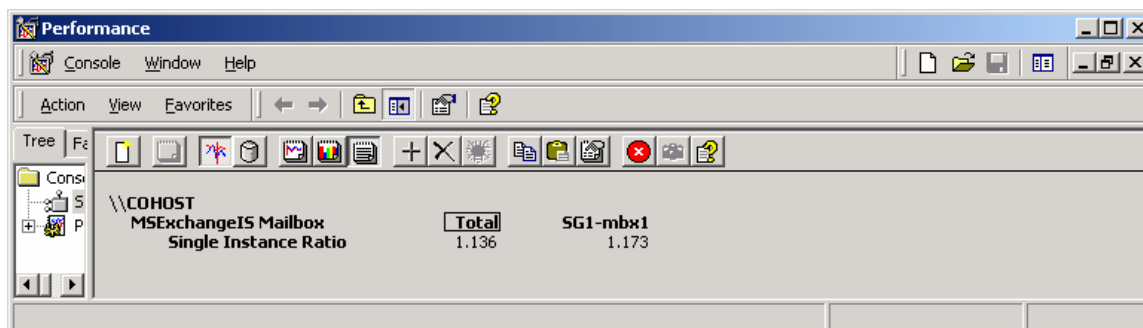



Figure 8.2: Viewing the Performance Monitor counter for single-instance ratio.

The counter should be above 1.0 (meaning that there is no benefit from single-instance storage) and most likely close to 2.0. The higher the counter, the more additional disk space you'll need when you split the store. For example, you may find that moving mailboxes from a 30GB store

into two smaller stores results in two 18GB stores. Even using the Performance Monitor single-instance ratio counter can give you an exact estimate of the impact: The counter is merely the number of messages with multiple pointer references in the store and doesn't take into account the relative size of attachments for those messages; thus, it isn't a weighted average.

One other point of interest about the Active Directory Users and Computers Move Mailbox wizard is that it processes only one mailbox at a time, even though your Exchange servers can process many mailboxes at once. So if you want to speed up the process of moving mailboxes (for example, to complete your migration overnight or over the weekend), you need to set up multiple workstations and move the mailboxes simultaneously.

 Before you take advantage of the additional mailbox stores that E2K supports, consider the impact on performance. Creating a new storage group requires additional Virtual Memory, and it also creates an additional set of transaction logs. Microsoft recommends that you use all available mailbox stores in the storage group before creating a new storage group (unless you want to create the new storage group to maintain separate storage group properties). Creating a new mailbox store breaks message single-instance and thus increases the number of writes to the disk; this behavior definitely affects performance. Splitting the store also affects transaction logs because a transaction is logged for each store.

Managing Mailbox Accounts

Exchange has always had the management tools to look after your Exchange mailbox accounts. As I mentioned in Chapter 7, the E2K System Administrator MMC snap-in is now used for looking after your mailbox accounts, and you should use it to ensure that you maintain consistent control over your Exchange environment. You use the Active Directory Users and Computers MMC snap-in to manage the usual tasks of adding, modifying, and deleting user accounts.

Confusion often arises when you look for user accounts in the mailboxes part of a mailbox store from ESM and don't find them. Mailboxes don't appear until they've been used in some way—either by someone logging in to them or by messages being sent to them. This behavior is unfortunate if you want to manage them in some way, so if you need mailboxes to appear, consider automatically generating a message to new users (mailboxes) as they're created.

Another issue is that for a mailbox to exist, a user object needs to be created; otherwise, the mailbox is considered an orphan and is removed during normal mailbox cleanup. This user object might be a temporary user account, simply created to instantiate the mailbox, but it must be created nonetheless. To minimize any potential security issue, you may want to disable the user object but grant other objects Receive As and Send As permissions to the mailbox, as Figure 8.3 shows. Here the example scenario is that John Smythe is an executive and JTom is an assistant who regularly needs to access the mailbox and who also sends out messages on behalf of John.

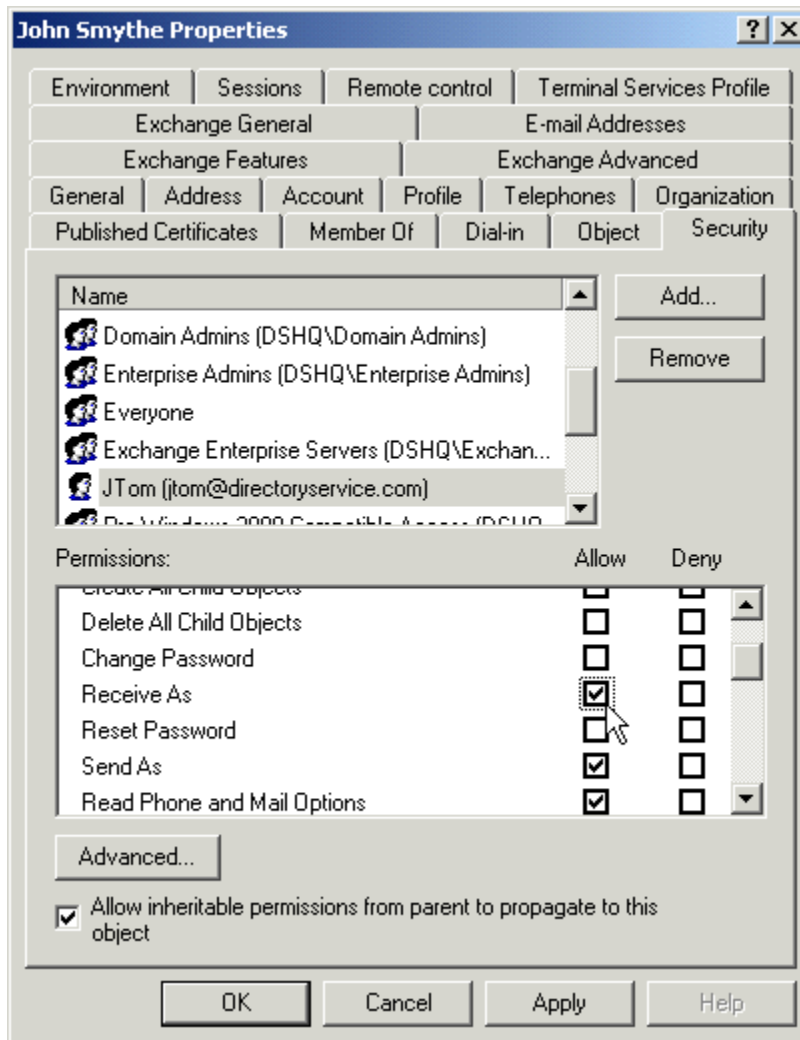


Figure 8.3: Assigning the Receive As and Send As permissions on a mailbox-enabled user object.

Giving a user object the Receive As permission allows the user object to open the associated mailbox. Giving a user object the Send As permission allows the user object to send mail messages as if it were the owner of the mailbox.

You manage permissions such as these primarily in the Active Directory Users and Computers MMC snap-in. To control these permissions, you must first switch to Advanced Features mode. To do so, right-click the domain you want to view, then choose Advanced Features from the shortcut menu, as Figure 8.4 shows.

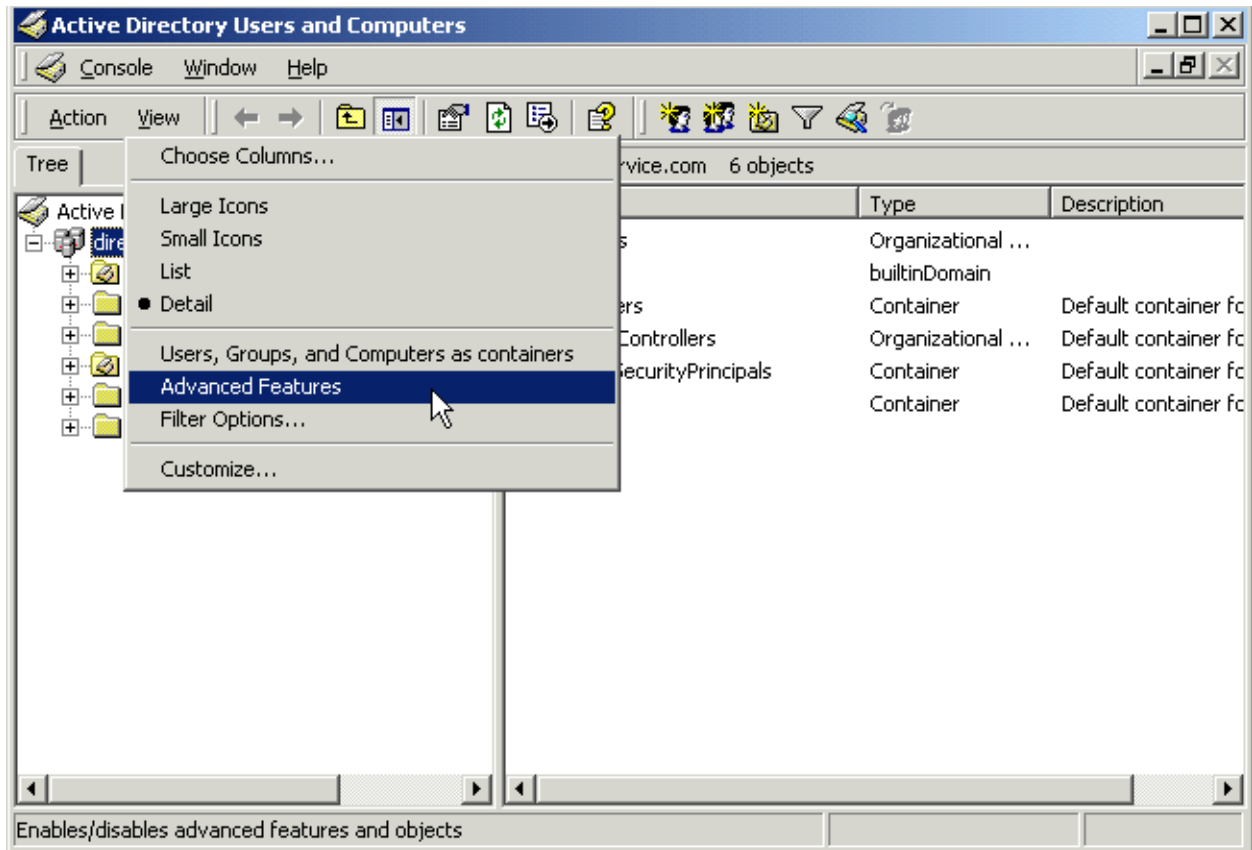


Figure 8.4: Switching to Advanced Features mode.

The Properties dialog box appears, with the Exchange Advanced tab, amongst others, added to it, as shown in Figure 8.5. To manage permissions, click Mailbox Rights.

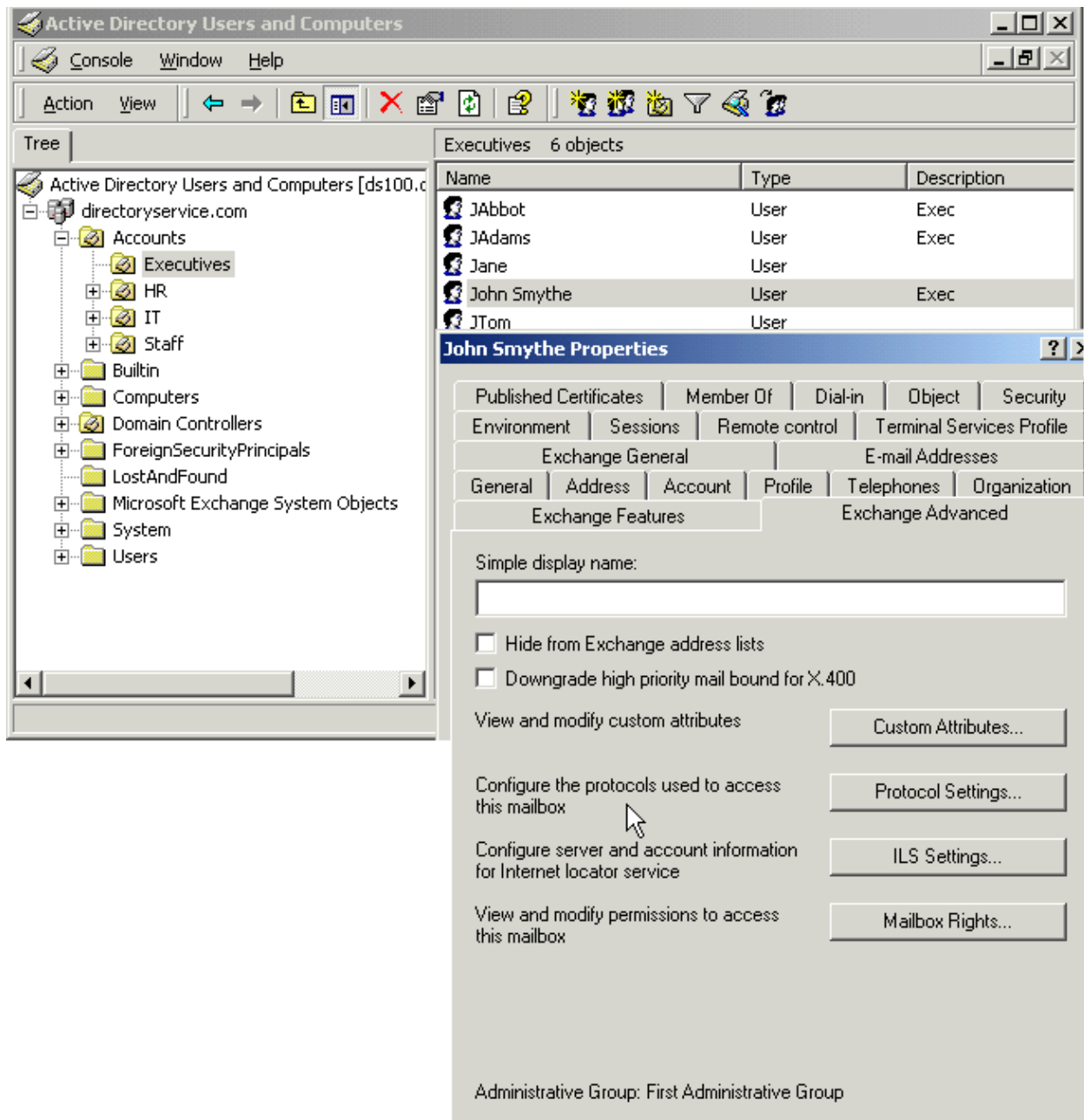


Figure 8.5: Using the Exchange Advanced page of the User Properties dialog box.

- ❗ There is a potential security issue whereby Send As permissions are granted by default to the local Administrators and Domain Admins groups when E2K is installed. If users are members of either the local Administrators or Domain Admins group on the Exchange server on which their mailboxes reside, they may be able to send mail representing anyone in the organization. You can find more information about the reasons for this default setting in Microsoft article <http://support.microsoft.com/support/kb/articles/Q303/7/09.ASP>.

Using the Latest Migration Wizard

As discussed later in this chapter, SP1 adds a number of important capabilities to support many aspects of your environment. One feature that you can use immediately in your migration is the Exchange Migration Wizard.

While the Exchange Migration Wizard was primarily used to migrate from other environments to Exchange, the latest update offers Exchange-specific migration support. For example, if you've installed E2K into its own organization without linking to an existing Exchange 5.5 organization, this release of Exchange Migration Wizard helps migrate from that organization. As a result, don't expect to throw away all the other tools I've discussed (such as Move Mailbox), although it could also help if you need to assimilate another organization at some time—such as one that's been acquired.

The Exchange Migration Wizard allows you to select mailboxes from a separate Exchange 5.5 environment, then select the E2K server, storage group, and mailbox store to which you want to move the mailboxes. The Exchange Migration Wizard also has a command-line mode, which is useful for developing scripted solutions—for example, to move a number of mailboxes at once. It is, however, limited in controls and error reporting.

Creating Contacts

In E2K and AD, *contacts* are directory objects that are *mail-enabled* but not *mailbox-enabled* (as I defined in Chapter 6). Thus, they have email addresses but no AD accounts or mailboxes in the E2K system. You can create contacts to keep track of email addresses for external contractors or consultants, for example; mail is then directed to their external email addresses. Contacts appear in address lists so that your email users can find them easily.

The concept of contacts is quite different than mail-enabled user accounts in AD, which can be used to apply permissions in AD even though the user mailbox resides on another messaging system. You can create a contact using the standard process, as shown in Figure 8.6, then choose not to create an Exchange mailbox.

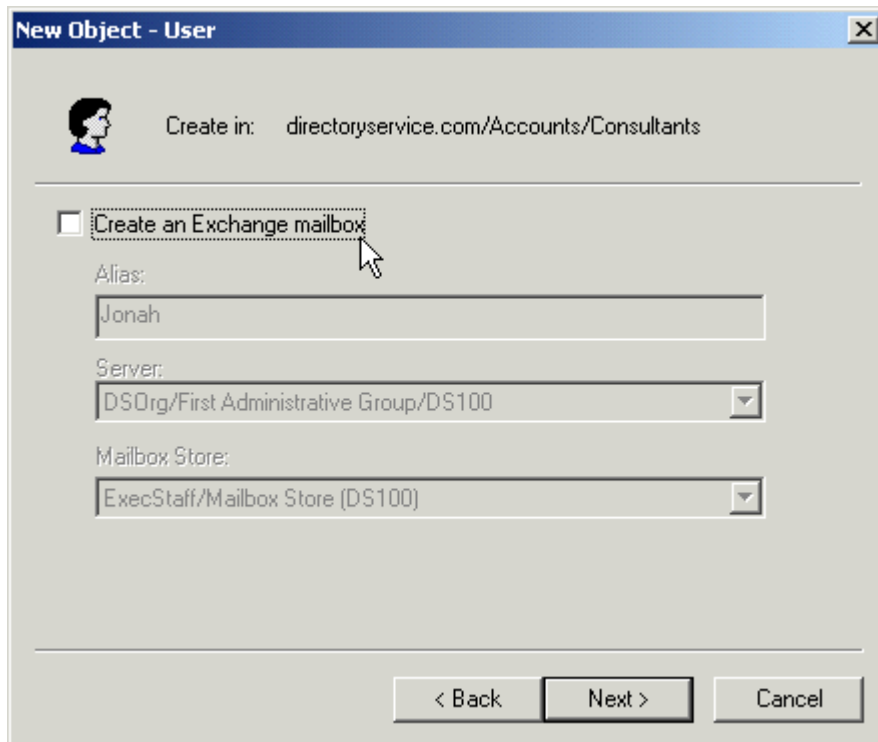


Figure 8.6: Creating a contact and choosing not to create an Exchange mailbox.

You can then add one or more email addresses by editing the user object. Alternatively, you can right-click the user object, then choose Exchange Tasks from the shortcut menu, as shown in Figure 8.7, to use the Exchange Task Wizard.

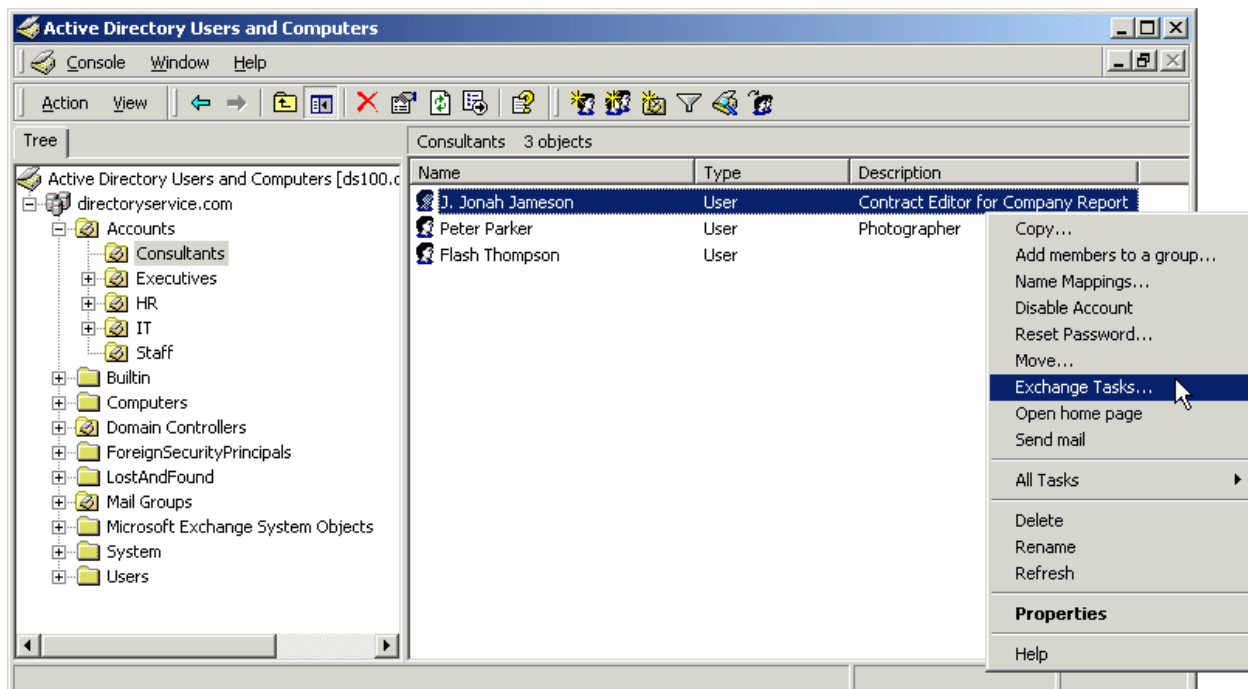


Figure 8.7: Choosing Exchange Tasks from the user object shortcut menu.

The Exchange Task Wizard allows you to add any required addresses to the user object, as shown in Figure 8.8.

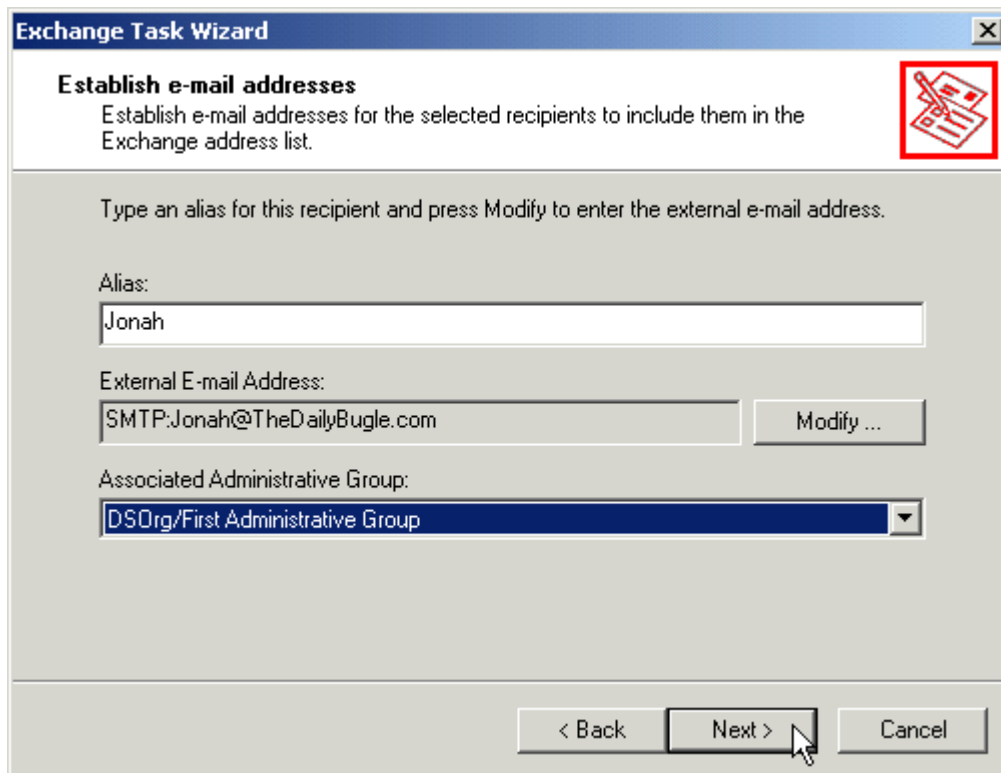


Figure 8.8: Using the Exchange Task Wizard to add an external email address to a user object.

Creating Groups

There are two types of groups in E2K, and this can be confusing. Win2K uses two group types: security groups and distribution groups, as shown in Figure 8.9. The group type determines whether the group is used to set ACLs on objects. If you create a group as a security group, you can also mail-enable it; however, you cannot use distribution groups for security purposes.

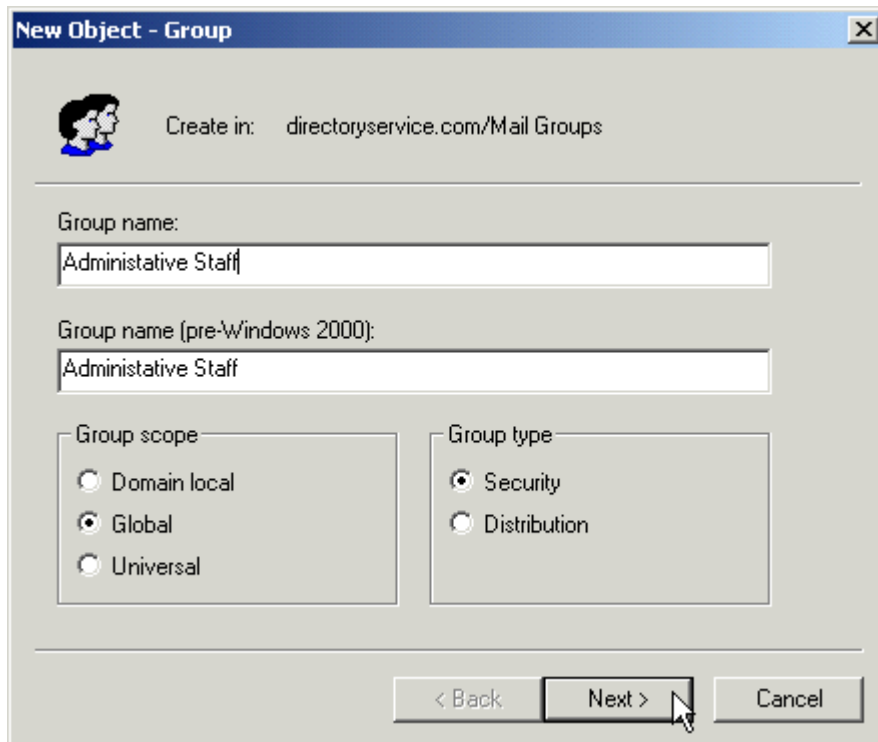


Figure 8.9: Creating a new group.

After you create a group, you can change its group type. However, as shown in Figure 8.10, if the group has been used to grant access to resources, moving from a security group to a distribution group can have undesired consequences for your security model.

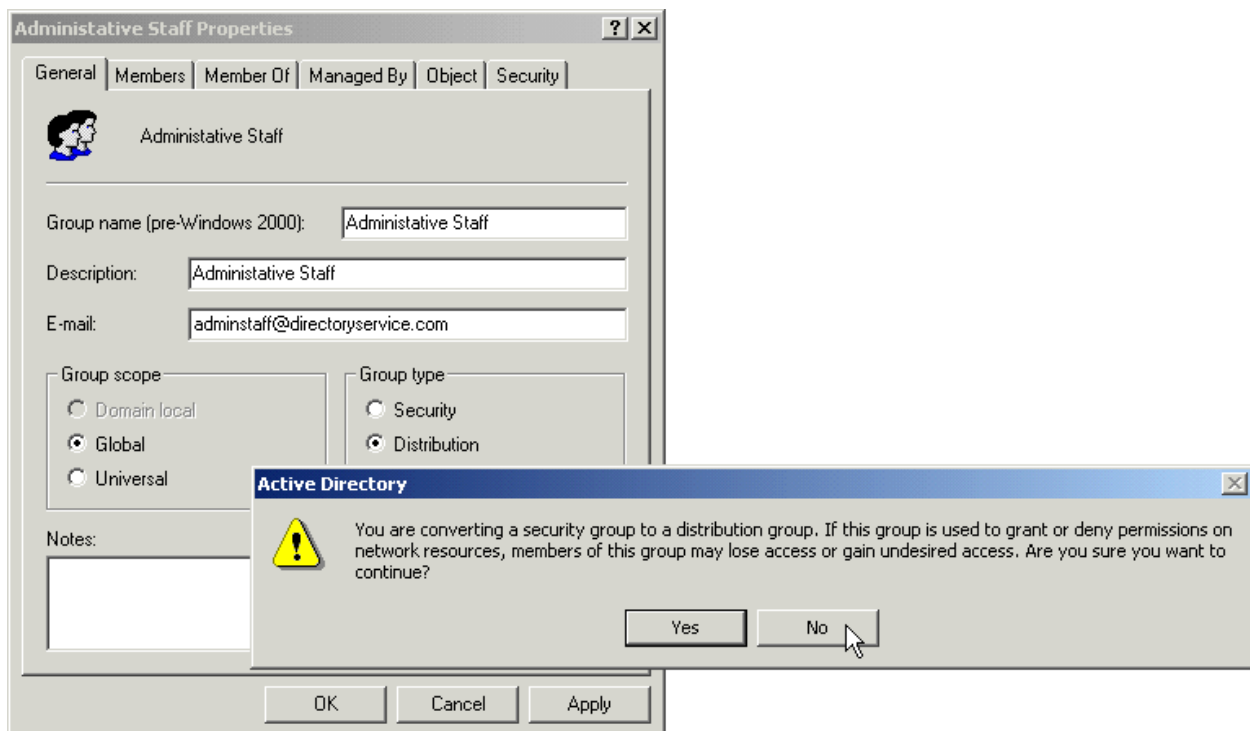


Figure 8.10: Changing group type.

Groups can contain other groups, so this allows for a degree of dynamic administration in your environment. However, as distinct from address lists, groups are not dynamically created. Instead, an administrator of a group selects specific entries to be used. This is unfortunate because by allowing a query to also make up group entries, the combination could be highly beneficial and efficient for you. The only other way to deal with potentially changing group memberships is to delegate administration, then include other groups (subgroups) in a master list.

Managing Administrative and Routing Groups

One of the final key areas of migration deployment that requires your attention is managing routing groups. Only one E2K organization can exist in a forest. Similarly, E2K cannot span multiple forests. It's bounded by the extent of the GC, which now defines all of the objects in the forest. Because of this, routing groups are very important to your overall management strategy. In Win2K, delegation of administration can be managed using OUs in AD, as discussed in Chapters 3 and 4; in E2K, administrative and routing groups are used.

Sites in Exchange 5.5

Before I begin this discussion, I want to provide some context by reviewing the model used by earlier versions of Exchange. Most of you will be familiar with an Exchange 5.5 definition of a site, which is essentially a set of well-connected Exchange servers defined by boundaries of high-speed connectivity and defining a logical boundary for administration, routing, and security. A Routing Information Daemon runs on the first server in the site (unless otherwise assigned), and it runs periodically according to a set schedule to create the GWART—although it can also be run manually.

Each site stores a knowledge base of all the other servers in the site and also what servers are used to connect to specific domains or other sites. Sites also define an administration boundary that is hard to break. Objects below the site level generally inherit permissions from the site, so anyone with administrative privileges in the site can, perhaps obviously, administer anything in the site. Although you can play with the basic permission properties in Exchange Administrator, this is an uncommon approach, and security is generally wide open from the site level down, including servers, settings, and configurations.

Because of the limitation of earlier versions of Exchange, the requirement for mixed mode is to support legacy Exchange Server computers using a combination of one administrative group and one routing group to represent a site. As discussed in Chapter 7, you can't change the site structure until you move the organization to Exchange native mode.

The E2K Model

I'll now introduce a broader understanding of administrative and routing groups in E2K. Administrative groups are what E2K uses to determine who can manage servers and what policies are applicable to servers in that group, managed according to a common policy. Unlike the predefined structure imposed by Exchange 5.5 and earlier, administrative groups allow you to define a logical structure for your Exchange organization. This allows you to group together in the directory objects that need to be logically managed together.

A default, or *first administrative group*, is created when you install Exchange. If your organization is small enough, or if it has a highly centralized administration model, you don't need to use more than that.

When you create an administrative group with assigned permissions, any object added to that group inherits those permissions. Administrative groups can contain any objects—for example, servers, policies, public folder trees, conferencing services, and routing groups.

As I discussed in Chapter 7, routing groups define how messages are routed among servers and across organizational boundaries, and they appear to be very similar in concept to the earlier Exchange concept of a site. However, the permissions that you assign to routing groups are independent of those you might assign to an administrative group, which may contain the same servers as are defined in a routing group. There is an implicit assumption that servers in a routing group share persistent connectivity and therefore can share a common routing infrastructure.

The primary difference between the earlier concept of sites and E2K's routing groups is that E2K uses SMTP instead of RPCs to handle connections among servers. In mixed mode, the following processes are used:

- **Exchange 5.5**—MTA/RPC
- **Exchange 5.5**—E2K uses MTA/RPC
- **E2K**—SMTP

In E2K, routing groups also form a minimal boundary for deploying GC servers related to your E2K deployment. You should deploy at least one GC server in each routing group to support lookups and performance, especially for routing across groups. Beyond that, the general understanding is to deploy at least one GC for each four to five Exchange servers and at least one GC per physical site.

Using both administrative and routing groups, you can fine-tune your management of your Exchange environment. To display these groups in ESM, if it's not already running, right-click the organization you want, then choose Properties from the shortcut menu. In the Properties dialog box, select the groups you want to display. (See Figure 8.11.)

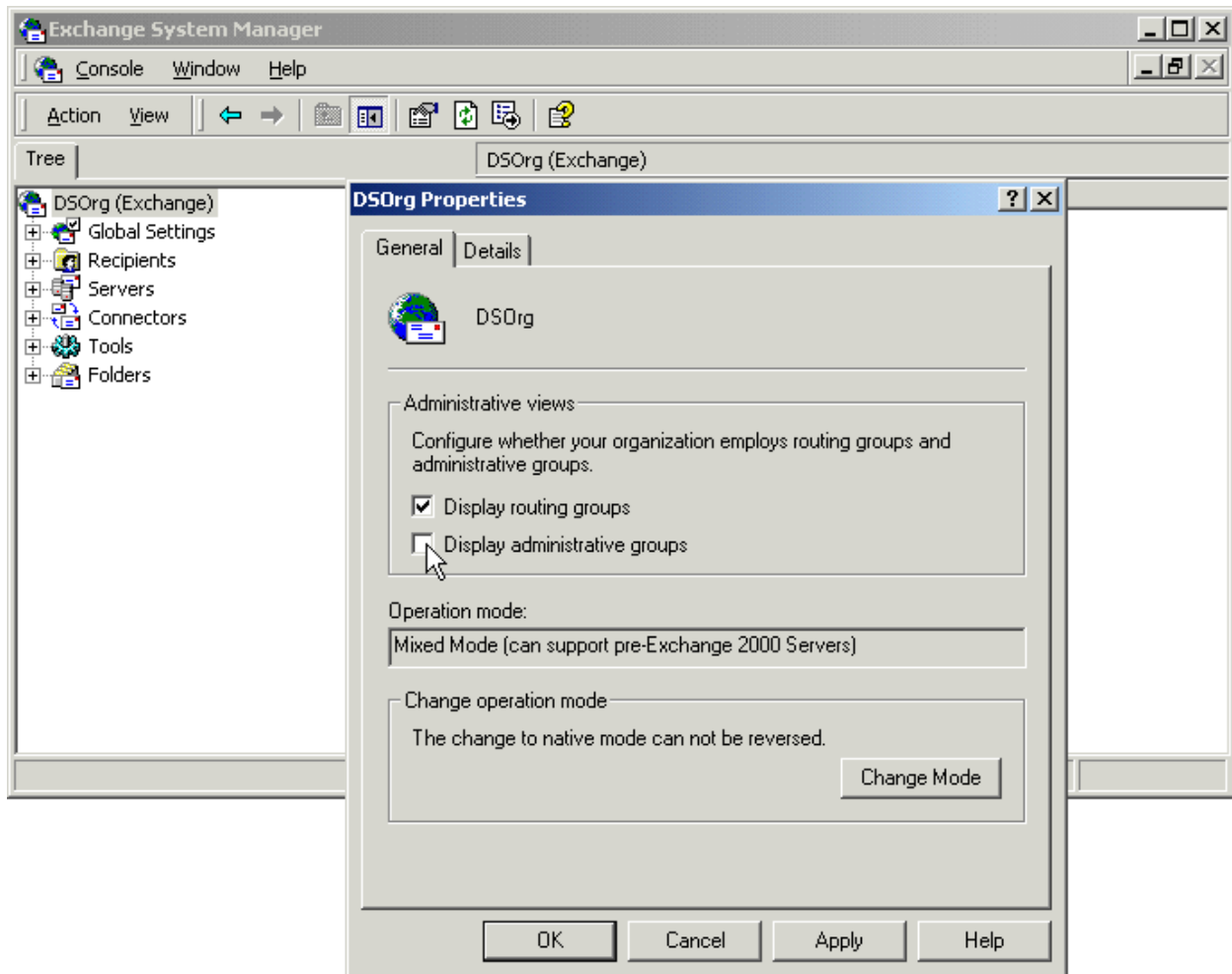


Figure 8.11: Using ESM to display administrative and routing groups.

Choosing to display administrative and routing groups changes the display in ESM, as shown below in Figure 8.12.

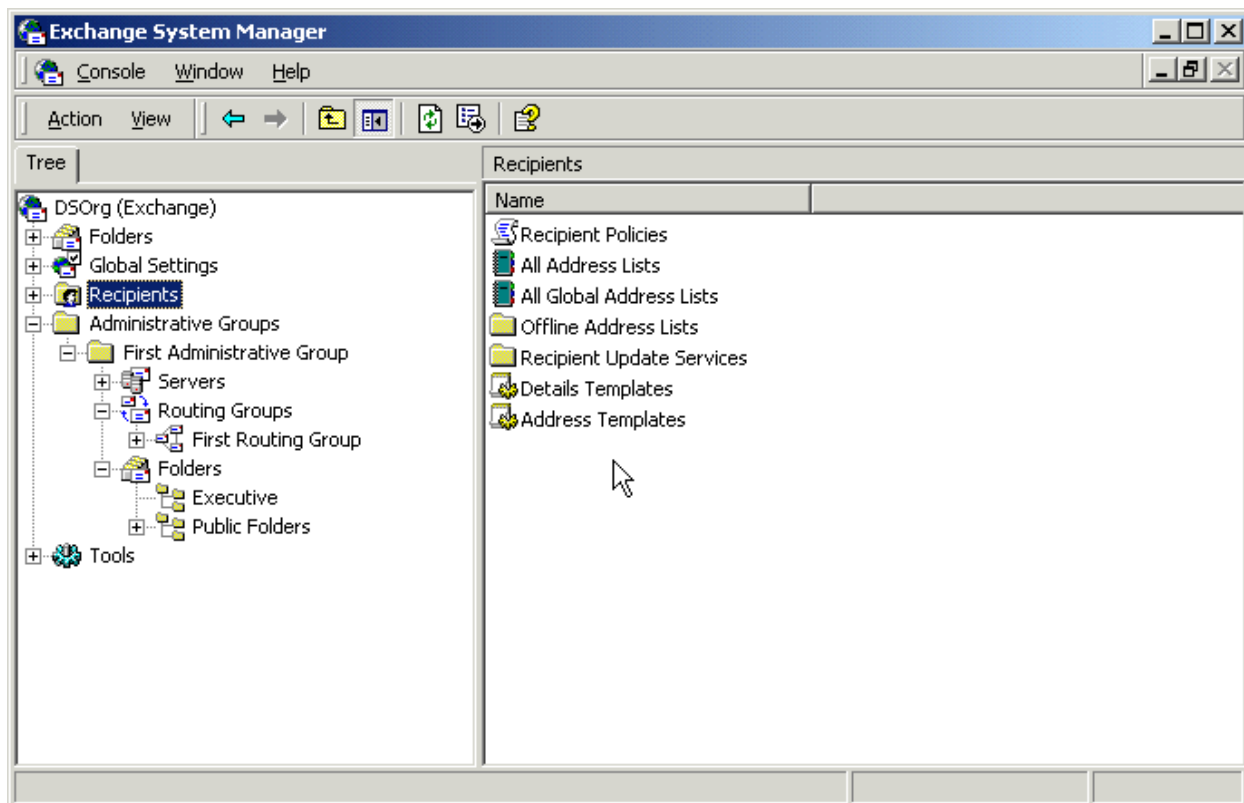


Figure 8.12: Viewing administrative and routing groups in ESM.

If you're not in Exchange native mode, perhaps confusingly, routing groups cannot be created in ESM. Because of the way in which Exchange mixed mode needs to operate, each administrative group has only one routing group. Furthermore, in mixed mode, you cannot move mailboxes from a server in one administrative group to a server in another administrative group.

Creating Public Folder Hierarchies


As with earlier versions of Exchange, installing E2K creates a default public folder tree, or *public folder hierarchy*, which is automatically replicated to all Exchange servers. Unlike earlier versions of Exchange, however, E2K allows you to create multiple public folder trees. Each new public folder hierarchy maintains its own replication configuration; this means that you must manually configure it. That is, a new hierarchy isn't automatically replicated, so you need to configure it.

In E2K, you also have the ability to precisely control folder-replication schedules and levels of administration as you require them for your environment. This can range from maintaining a public folder on a single server to replicating the folder to all servers in your E2K environment. There are a few reasons to create multiple public folder hierarchies.

- Your default public folder hierarchy is becoming too large.
- You need to delegate administration of folders or replications.
- You need to define a different security model on a specific set of public folders.

Creating multiple public folder hierarchies can help you manage your E2K environment, but it introduces other issues. For example, one common misunderstanding is that using versions of Microsoft Outlook earlier than Outlook version 2002 allows you to see multiple public folder hierarchies. However, this isn't a permissions problem but rather a compatibility issue because earlier versions of Outlook allow you to see only the default public folder root. Outlook version 2002 and later can use multiple hierarchies, so you may choose to upgrade your clients to this version. Alternatively, you can direct users to view the public folder hierarchy over the Web until an upgrade is possible. I described sharing public folders over the Web in Chapter 7.

You also have the option of moving public folder trees from one store to another by cutting and pasting them. First select the root of the public folder tree you want to move, right-click it, and choose Cut from the shortcut menu. Then select the new public folder root you want to move to, right-click it, then choose Paste from the shortcut menu.

 Moving a public folder tree immediately disconnects users who are connected anywhere in the public folder hierarchy. This ensures that users cannot change data in the hierarchy while you're moving the public folder tree. However, unless users reconnect themselves, they can lose changes they've made to documents in the public folders.

Applying Recipient Policies

A *recipient* is an AD object that can receive mail. Recipients can include users, contacts, groups, and other resources. As discussed briefly in chapters 6 and 7, a recipient can be either mailbox-enabled or mail-enabled. The following clarifies the distinction between these two options:

- **Mailbox-enabled recipients**—Have security principals (accounts) and mailboxes for sending and receiving email messages.
- **Mail-enabled recipients**—Are contacts and groups that have email addresses but no mailboxes. As a result, they appear in an organization's address list, and they receive messages, but they cannot send them from within the E2K organization.

E2K improves over earlier versions of Exchange by adding *recipient policies*, which define the assignment of addresses to mail-enabled objects (for example, contacts, public folders, connectors, and email-gateways).

The default recipient policy is generated during installation, and you cannot delete it. While it provides the policy for all mail-enabled objects, it's also the only policy used specifically for connectors and email gateways. If you need to change the way in which email addresses are assigned, you can create new policies or modify the default recipient policy. (Although you cannot delete it, you can modify it.)

Policies are located under Recipients\Recipients Policy in the E2K management tree. Editing the policy is similar to earlier Exchange address management, and it allows you to add, modify, and delete specific types of email addressing, including SMTP, Microsoft Mail, and X.400 addresses. Other types of addressing are available if connectors are installed.

Editing the policy allows you to immediately apply the change to all objects that match the search criteria for that policy. If this is the first time you're managing policies for your organization, you'll see the default recipient policy, which is assigned a priority of Lowest. When multiple recipient policies exist, the default recipient policy is applied only if the others aren't. In other words, if other recipient policies have been created, they're applied first.

Policies are applied using filters. For example, the default recipient policy filter returns all mail-enabled objects. Figure 8.13 shows a sample filter assignment for recipient policies.

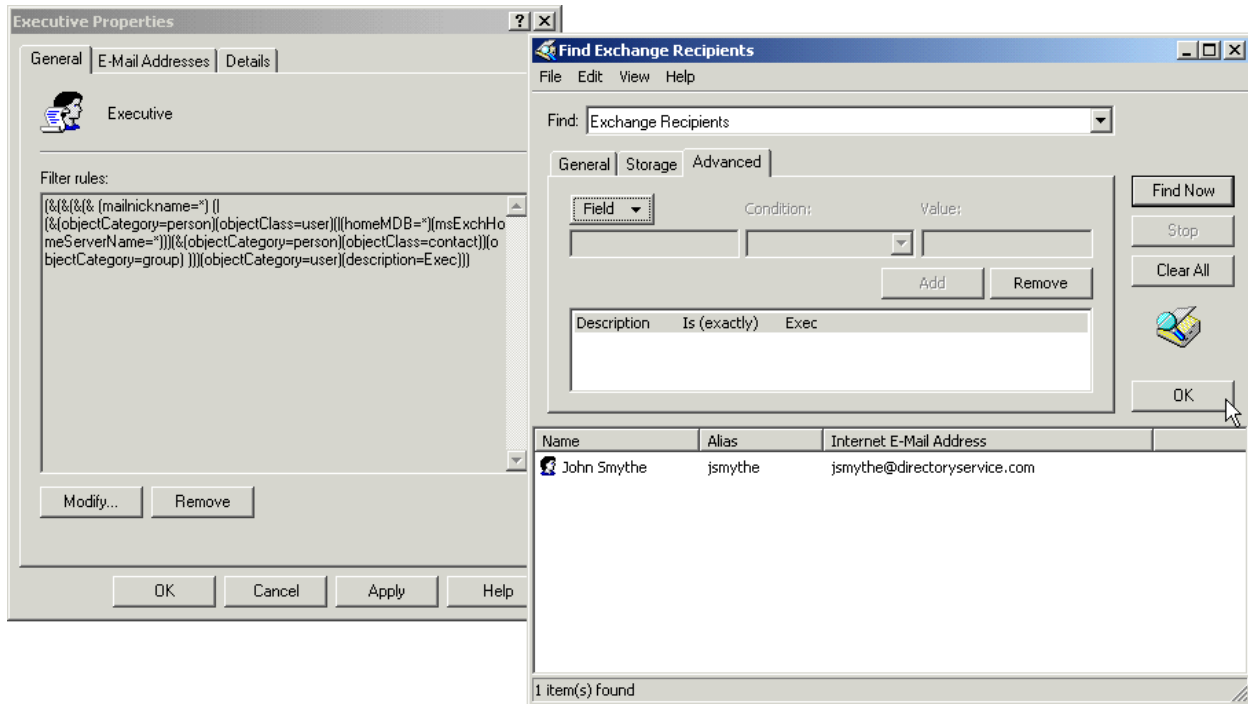


Figure 8.13: Viewing the recipient policy filter assignment for recipient policies.

Once you've set up the policy, you're asked whether you want to apply it immediately. If you select Yes, a process starts that searches for objects that match the criteria; if it finds objects, it applies the policy. When you change a policy filter, you receive the notification shown in Figure 8.14.

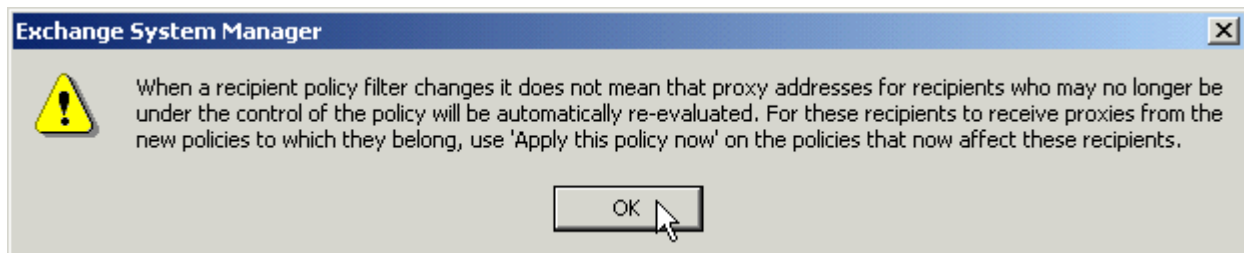


Figure 8.14: The notification that appears when you change a policy filter.

The only real consideration at this stage is that your environment matches your requirements. For example, if you add additional SMTP addressing, make sure that your DNS architecture is set up to deal with the new addresses using the appropriate routing or MX records.

The final consideration when dealing with recipient policies is the format of the name. When you look at the default policy, you'll see that it doesn't specify the front part of the name but instead relies on a default name. You can use Help, but for reference, you can still use the same options you used in Exchange 5.5, so check the Help files.

⚠ Watch out for these common problems with E2K. Having a connector to another mail system in your organization that shares the same addressing scheme (for example, user@company.com). E2K doesn't properly handle this routing between the two systems. You must perform the workaround described in the Microsoft article Q278838, "XCON: Cannot Send Mail to SMTP Domain That Is the Same as the Local Exchange Organization Domain," located at <http://support.microsoft.com/support/kb/articles/q278/8/38.asp>.

Creating a recipient policy that results in two accounts resolving to the same SMTP address. This can happen as a result of two templates generating the same SMTP address. For information on resolving this issue, see the Microsoft article Q271339, "XADM: Cannot Mount Database and Event ID 9546 Occurs," available at <http://support.microsoft.com/support/kb/articles/q271/3/39.asp>.

Creating Address Lists

Address lists determine what a user sees in their client under the Address Book for the GAL. This makes it easier to find recipients and resources (for example, room calendars) when you're trying to collaborate. E2K automatically creates a number of address lists. The most familiar is the default GAL, and its behavior is pretty similar to that in earlier versions of Exchange.

GALs are found under the Recipients node of the domain tree. You can also create your own address lists, as shown in Figure 8.15.

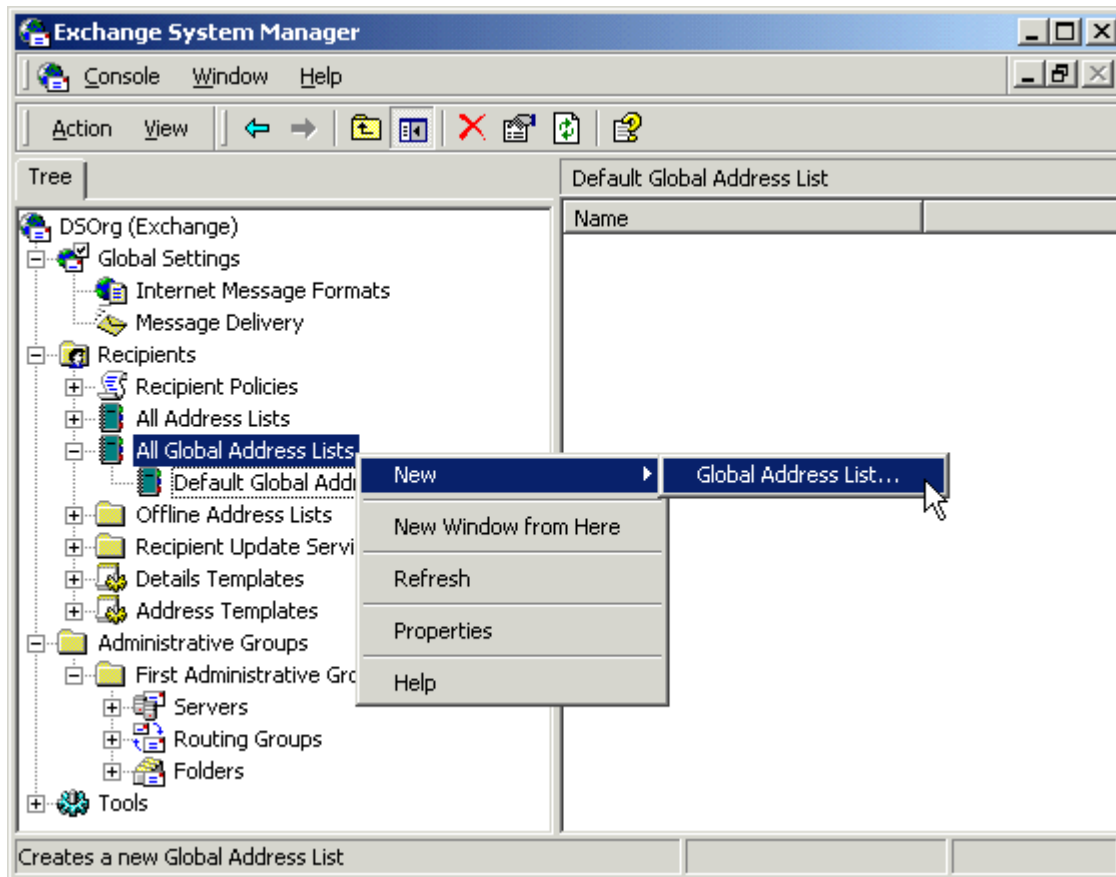


Figure 8.15: Creating an address list.

In E2K, you create address lists using LDAP queries. You can then apply permissions to the address lists to ensure that the correct clients see them or not, as appropriate, as Figure 8.16 shows.

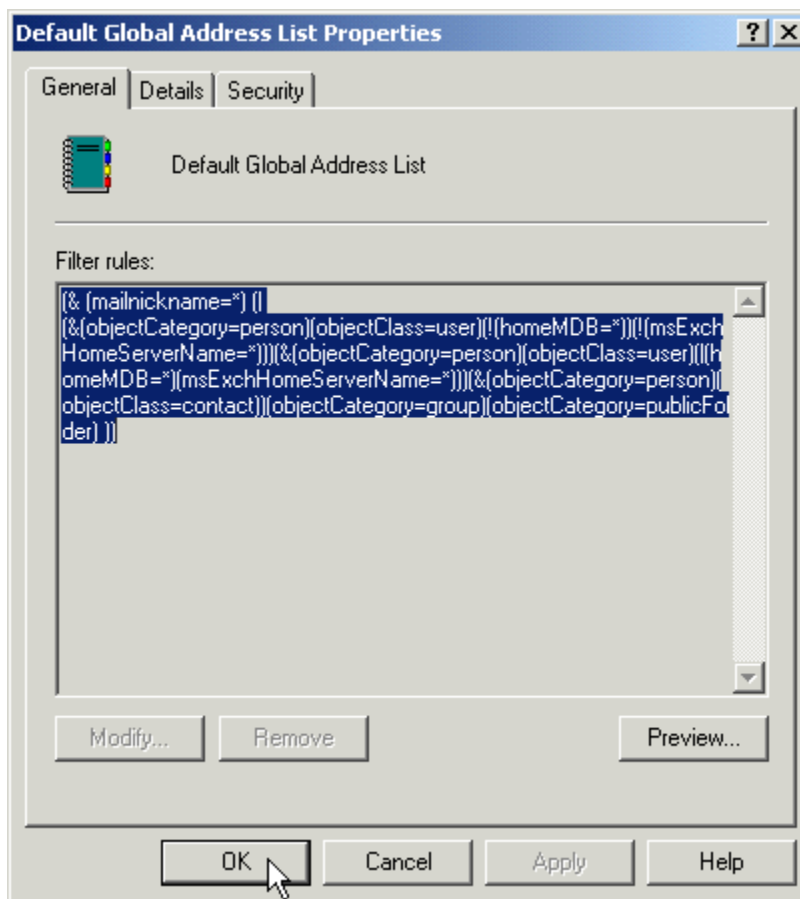


Figure 8.16: Displaying the rule for the default GAL filter.

That said, what is the default address list that a client sees? This is determined by the answers to the questions below.

- Which address list do you have permissions to see?
- Which address list contains your mailbox object as an entry?
- If your mailbox appears as an object in more than one address list, which of the remaining address lists contains more entries?

Templates define how an object's information (for example, recipients, groups, contacts, and so on) is shown in the Address Book. While default templates are normally used, you can also modify or create templates for your own requirements. You can see the template stores located under the Recipients node in Figure 8.15.

Deploying OWA

Microsoft suggests that a primary reason for migrating to E2K is to use OWA. Because E2K's OWA solution is built directly into the store technology, performance is greatly increased, and

use of resources can be more finely managed and tuned—for example, using front- and back-end designs, as discussed in Chapter 6.

I discussed OWA access in detail in Chapter 7, but I want to talk about a couple of other items that are important in deploying this new OWA solution.

Managing OWA

When you manage OWA, you carry out a number of activities: accessing Exchange 5.5 mailboxes, creating RTF messages, taking advantage of enhancements in Service Pack 1, and managing passwords.

Accessing Exchange 5.5 Mailboxes

As I noted earlier, while you can use the Exchange 5.5 implementation of OWA to access an E2K mailbox, you cannot access an Exchange 5.5 mailbox from an E2K OWA installation. Because the E2K OWA solution is intimately tied to the store technology, you cannot use it to allow Web access to an Exchange 5.5 server. That is, if you point a browser at a front-end server and your mailbox is on Exchange 5.5, you gain access. But if you point a browser at an Exchange 5.5 server, you gain access only if OWA is installed and the correct permissions are in place.

Creating Rich Text Format Messages

The points above are the client requirements for E2K OWA access, but I haven't discussed using the Exchange Multimedia ActiveX Control, which allows users to create RTF messages in OWA. If your browser allows it, you can download the control using the Options icon in the left-hand pane, as shown in Figure 8.17.

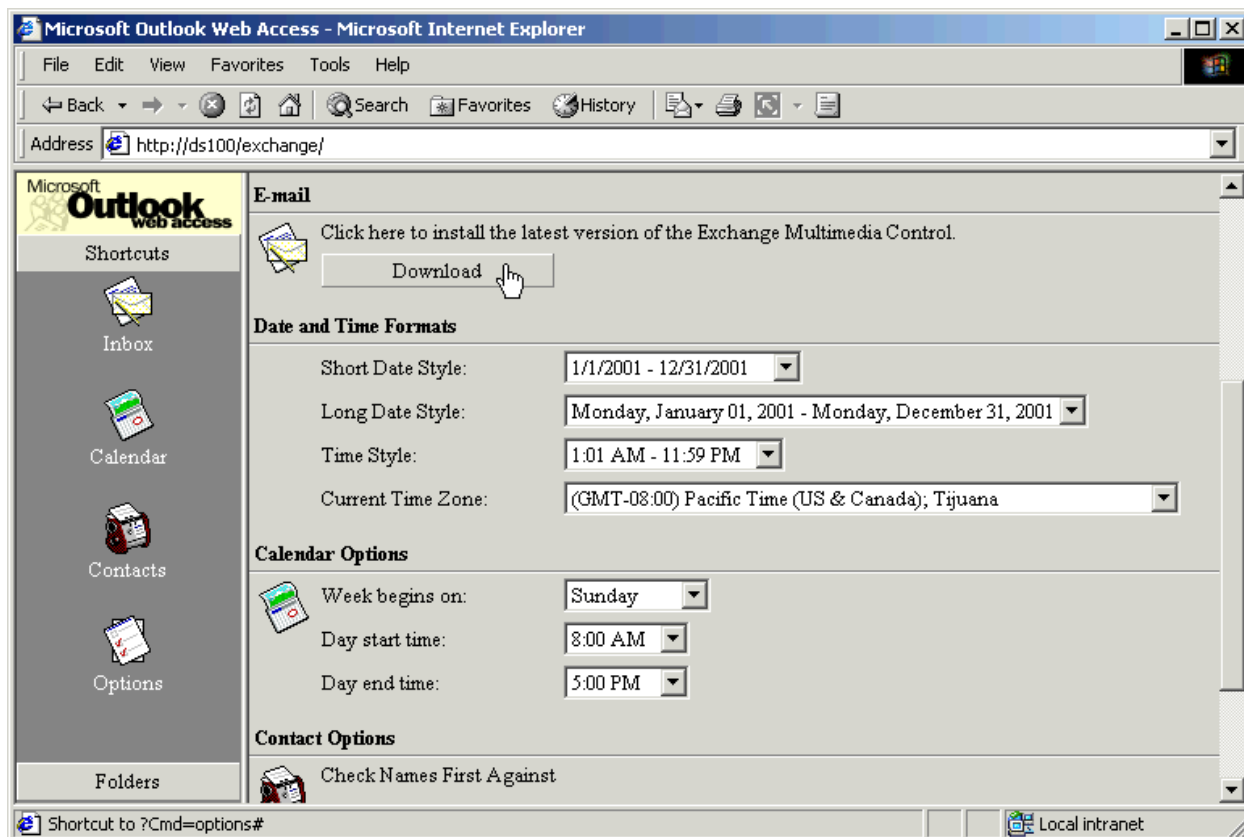


Figure 8.17: Downloading the Exchange Multimedia Control.

Taking Advantage of Enhancements in SP1

Along with bug fixes, E2K SP1 offers several enhancements to OWA, including:

- New language support.
- Recovering deleted items—In E2K, you cannot access the Deleted Items recovery area in OWA. SP1 adds a new view to the Deleted Items folder that makes this possible.
- Uploading files to a public folder—With SP1 installed, OWA allows users to upload documents or other item types to any folder in E2K. From there, users can collaborate on the document by either modifying or discussing it.
- Improved support for Microsoft IE on UNIX—In E2K, users of IE 5.01 for UNIX on Solaris and HP-UX receive the down-level OWA client. When they install SP1, they receive the full IE 5.x rich client.

Managing Passwords

One of the issues with earlier implementations of Exchange was managing passwords. If you had a password policy that required users to change passwords periodically using password expiration, you couldn't offer OWA as the only way for remote users to access email. Essentially, there was no way for users to use OWA to change their passwords. Thus, users would have to change their passwords by connecting to the network environment at some point, essentially negating OWA's potential simplicity.

E2K's OWA allows users to change passwords over the Internet, but this isn't the default behavior. To enable this capability, you first need to enable your OWA site to use SSL. The Microsoft article "XWEB: How to Change OWA Passwords Through IIS," located at <http://support.microsoft.com/support/kb/articles/q267/5/96.asp>, describes how to make the changes necessary to support this capability.

Securing OWA Communications

Of course, before you allow users to change passwords over the Internet, you'll want to secure communications with the server to ensure that any changes to passwords cannot be intercepted. This could be devastating. Let's look at how to secure OWA communications.

Whether you use OWA only for internal access or as a solution for Internet access to corporate email, you should enable SSL. To do so, you need to obtain a certificate for your server. To manage these services, you need to have both the Exchange Key Management Service (KMS) and Win2K's Certificate Services installed on the same server. If you haven't done this, you can run the original Win2K setup and install them.

The process of creating a certificate, or importing from an external Certificate Authority (CA), is made simple in E2K using the IIS Web Server Certificate Wizard, accessible from the IIS MMC snap-in. Select the site you want to create the certificate for, right-click it, then choose Properties from the shortcut menu. In the Properties dialog box, click the Directory Security tab, then click Server Certificate. The wizard guides you through the steps necessary to create a certificate signing request (CSR), which you use to obtain a third-party certificate. You then submit the CSR to your chosen CA to generate the certificate. You can then enable SSL on the Web site you use to access OWA.

It's fine to say that you can use OWA over SSL, but to ensure security, you may also want to specify that no one can access OWA if they don't use SSL. To do this, follow the steps above to display the Directory Security page for a Web site, then edit the Secure Communications option group and select Require Secure Channel (SSL). This ensures that users must use Hypertext Transfer Protocol Secure (HTTPS) to access OWA. If they try to use standard HTTP, they receive an error message.

SSL does exact a price for performing the secure encryption, however, and immediately degrades the performance of the IIS server. If you haven't already calculated the impact of this performance hit, you need to determine your expected connections, then determine the number of servers required to support them. Experience says that performance degrades at least 50 percent using SSL. Because the process of encrypting and decrypting data is processor-intensive, monitor processor use or use an SSL accelerator to offload the processing from the server CPU. Finally, you need a certificate for each front-end server you use to support SSL connectivity.

Implementing Clustering

Clustering, which is easier in Win2K because it offers more hardware solutions, is still a specialized solution. Unless you already have a cluster in place and are intimately familiar with the solutions, the first place to check for information on Win2K clustering is <http://www.microsoft.com/windows2000/technologies/clustering/default.asp>. You'll find more specific information on E2K clustering at <http://www.microsoft.com/exchange/evaluation/features/Clustering.asp>.

While you can upgrade a clustered Exchange 5.5 environment to E2K, discussing it is outside the scope of this chapter. Have a look at the process documentation on the E2K CD. It describes the steps you need to take to perform such an upgrade—essentially advising that you set up another cluster and migrate your mailboxes to it. You need to test clustering extensively, potentially with the support of your hardware vendor.

Decommissioning the Exchange 5.5 Organization

By this point, you should be ready to switch over to E2K. This involves carrying out the following tasks:

- Removing the ADC
- Removing the SRS


Removing the ADC and SRS

Of all the standard software packages that Microsoft offers, the ADC and SRS are the ones that you'll encounter most often. You still need these services and the fundamental directory synchronization functionality they offer, even if you use third-party solutions from ISVs such as NetIQ, Quest Software, BindView, Aelita Software, and others. (For more information about the ADC and SRS, see Chapter 6.)


The direct link between AD and Exchange means that only one Exchange organization can exist in an AD forest. While this constraint may be removed in future versions, it may affect your ability to support separate development domains. (You may have done this using earlier versions of Exchange; NT 4.0 and Exchange 5.x separated the security principals from the actual Exchange directory.)

Before you remove the ADC, make sure that you move over all of your users from the Exchange 5.5 servers. Then you can remove the last Exchange 5.5 server. Use Exchange Administrator to delete the directory replication connectors, which are located in the tree under Org, Site, Configuration, Connections.

At the same time, you need to remove the SRS. This allows you to remove your Exchange 5.5 server from the SRS database. In Exchange Administrator, connect to the E2K SRS server. Under Administrative Groups, select the Exchange 5.5 server to remove, then click Delete.

 The Microsoft article Q284148, "XADM: How to Remove the Last Exchange Server 5.5 Computer from an Exchange 2000 Administrative Group" (available at support.microsoft.com/support/kb/articles/Q284/1/48.ASP) notes the following: "You cannot delete an Exchange 5.5 server if you are connected to it with Exchange Administrator program. Use Connect to Server to connect to a different Exchange server first. Also, Exchange Administrator will not allow you to delete the server if Exchange services are still running on it."

Using the ADC Management tool, select `Config_CA_SRS_Server_Name`, right-click it, then choose Replicate Now from the shortcut menu. When the replication has completed, Exchange Administrator removes the Exchange 5.5 server from the SRS database. The `Config_CA` object "reads" this delete, then replicates it to AD. Once this process is complete, you need to log in to your E2K system using an account that has Schema Admin privileges, then delete the ADC from the E2K side.

 If you don't remove the Exchange 5.5 connector before removing the final Exchange 5.5 server, you'll likely see a series of errors and warning messages in the Application log on your E2K server along the lines of "LDAP Bind was unsuccessful" to the server that you just removed. Unfortunately, you cannot simply remove the ADC installation because you'll receive the error message "Setup is unable to continue as it has detected that there are one or more Connection Agreement(s) associated with this ADC." Before attempting to remove this connector service, you must delete the Connection Agreement(s) or configure them to run under a different connector service.

If you cannot assign the connector to another service, you must remove the ADC forcefully from your E2K environment. You cannot use the E2K System Administrator MMC snap-in, but you can use the Active Directory Sites and Services MMC snap-in. The ADC can be found in the AD Sites and Services MMC snap-in under Sites, Servers. *servername*, Exchange Settings. After you delete the ADC, you can reinstall it by selecting Microsoft ADC in the Control Panel Add/Remove Programs applet and clicking Reinstall.

Setting Up and Migrating Accounts

If you used the ADMT, you need to clean up after the migration. As described in Chapter 4, ADMT allows you to set up and migrate accounts (as well as domains, printers, and many other types of objects).

Decommissioning the First Exchange 5.5 Server

As discussed in Chapter 6, you need to keep track of important servers in your existing environment, such as the first Exchange 5.5 server. As you start to close down your Exchange 5.5 servers, you need to ensure, perhaps paradoxically, that the first Exchange 5.5 server is the last server you actually retire. Consider also that this step is essentially acknowledging that you've completed the bulk of your migration; once all Exchange 5.5 servers are retired, there is essentially no reason to remain in either Win2K or Exchange mixed mode.

Switching to E2K Native Mode

One of the last steps you'll take in migrating to E2K is switching to E2K native mode. (For details on this process, see Chapter 6.) I also noted there that running in Exchange native mode offers the following benefits:

- It supports multiple routing groups, separate from administrative groups.
- Routing groups can consist of servers from numerous administrative groups.
- E2K uses SMTP as the default routing protocol.
- You can move servers among routing groups.

Completing Other Migration Tasks

Finally, there are a few other migration tasks that you need to care of:

- As I discussed earlier in the section about planning your migration, you need to perform an accurate audit of your environment. It's essential for managing the scope of your migration planning.

- I also said that it was important to continually document the migration process. You now need to ensure that your documentation is up to date by going through an evaluation stage. You might consider this to be the next step in rolling into another plan, if necessary, but it's important nevertheless.
- While evaluating your migration can be a final step, you can do it at any time to ensure that you've accomplished all of your original goals.

Managing E2K Performance

Like many subjects in this book, this is a huge topic, one on which an entire book has been written, so I'll discuss only the fundamentals here and make some comparisons with Exchange 5.5 methods.

There are many ways to ensure that your Exchange environment is running optimally. One is monitoring the important areas of your environment. Another is developing a tested and approved plan for dealing with the results. Let's discuss the aspects of monitoring your Exchange environment; however, be aware that you will need to deal with the results on your own.

Monitoring Your Exchange Environment

As I said during my discussion in Chapter 5 on monitoring Win2K, it's vital that you actively manage your Exchange environment. This allows you to act proactively rather than react to events as they occur—but of course, this depends on what processes you use. I'll first examine some of the tools native to E2K, then review some of the third-party applications available.

Exchange offers minimal server and link monitoring tools. While they're useful for one or two servers, they do little to help large-scale installations perform trend analysis and diagnostics. At the very least, until you have a more complete monitoring solution in place, set up monitoring and notification for critical E2K services.

One of the simplest and commonly overlooked areas for monitoring information is the event logs. For example, the Application log stores MTA information, backup events, and access errors. Third-party applications often register events in this log as well. However, manually reviewing logs isn't a useful active monitoring solution. While the logs help significantly when you're tracking down a specific issue, in larger environments, you need to consider consolidating logs; otherwise, you have to wade through the logs at each server.

One of the updated capabilities that Microsoft offers is Web-Based Enterprise Management. WBEM forms the basis of many of the new management monitoring tools used by Microsoft, so it's worth understanding how it works.

☞ For an introduction to WBEM, read the paper located at <http://www.microsoft.com/windows2000/techinfo/howitworks/management/wmioverview.asp>. It also describes how the Microsoft implementation of WBEM-compatible technologies—Windows Management Instrumentation (WMI)—and the latest enhancements to the COM work together to simplify systems management while providing a better-managed environment.

While you may decide to use a third-party product to manage and monitor your network infrastructure, Exchange has always provided basic server-status and link-status monitoring capabilities.

Core Exchange Services

Table 8.1 describes the core Exchange services that manage and monitor E2K.

Service	Description
Event logs	Logs event informational, warning, and error messages issued by Exchange and other applications.
IIS Admin Service	Allows you to administer the Exchange HTTP virtual server in the IIS snap-in—although the recommendation is to use ESM for IIS administration of Exchange services.
Microsoft Exchange Event	Monitors folders and generates events for Exchange 5.5 applications.
Microsoft Exchange IMAP4	Provides Exchange IMAP4 services.
Microsoft Exchange IS	Manages Exchange IS. To see how much memory the ESE is using, you can use the Database Cache Size (Information Store) counter on the Performance Monitor's database object. The amount of virtual memory that the ESE uses increases as you load more storage groups and databases.
Microsoft Exchange MTA Stacks	Provides Exchange X.400 services.
Microsoft Exchange POP3	Provides Exchange POP3 services.
Microsoft Exchange Routing Engine	Processes Exchange message routing and link-state information.
Microsoft Exchange Site Replication Service	Replicates Exchange information in the organization.
Microsoft Exchange System Attendant	Monitors Exchange and provides essential services.
NNTP	Transports newsgroup messages across the network.
SMTP	Transports email across the network.
World Wide Web Publishing Service	Provides HTTP services for Microsoft Exchange and IIS.

Table 8.1: The core Exchange services that manage and monitor E2K.

Hardware Components

You also need to monitor the underlying hardware components of E2K and its OS environment. There are many aspects to creating a high-performance Exchange installation. A number of underlying hardware components form a shell within which Exchange operates; they all vie with each other to be the most important, but none of them win. To ensure that you're using them optimally and dealing with saturation points as they occur, you need to monitor them all. (See Table 8.2.)

Component	Description
CPU status	As I mentioned earlier, many services affect the raw performance of your server, such as SSL and Full-Text Indexing. To monitor CPU performance

Component	Description
	for peaks, you need to look for sustained levels of usage. Multiple CPUs have a noticeable impact on Exchange performance. Reports from Microsoft, Compaq, and Dell suggest a generally linear increase in performance up to four and possibly even eight processors.
Memory status	Memory is often cited as the first thing to look at when there are performance issues because it gives the application high-speed working room to perform. As an example, the ESE uses RAM to cache database pages in memory. When RAM is unavailable, the ESE uses disk caching to store pages on the local storage system. This causes a strain on those resources, which are forced to provide increased operations. This is why it's important to monitor storage system performance to ensure that data is being accessed optimally and to identify any need to upgrade either the storage solution itself or the I/O subsystem or even to redistribute your data locations across your storage subsystem. Remember of course that increasing RAM to maximum capacity is much more cost effective. It's important to monitor the Page Reads and Page Writes performance counters for the Memory object because they help to identify hard page faults that result in a disk access. The intent is to maximize the use of memory while minimizing access to the storage subsystem. The sum of these two values shouldn't exceed 80 milliseconds (that is, roughly the I/O limit for one disk drive). If the sum exceeds 80 milliseconds, you should add more physical memory to your server and possibly locate the pagefile on a separate, fast drive (although doing the latter is less efficient than adding memory).
Network connectivity	<p>When network connectivity is saturated, you have several options.</p> <ul style="list-style-type: none"> • Check that the network connection is running at the highest speed and is connected to a switch. • If network throughput is still a problem, install multiple network cards. • Match the cards to the highest-speed switched subnets.
Storage subsystem	<p>The cumulative count of read and write operations is important. General practice suggests that queue length should be less than half the number of disks in the volume. If queues remain consistently high, consider redesigning your data distribution and storage subsystem. E2K relies heavily on several different forms of databases, so it needs a high-performance storage subsystem to support the sometimes-contradictory requirements of these data types. I discussed this in Chapter 6, but now you need to monitor the load and stresses on both disk and controller components. When you need to look at storage performance, use the Performance Monitor counters based on the physical disk:</p> <ul style="list-style-type: none"> • Avg. disk sec/Read • Avg. disk sec/Write • Avg. disk sec/Transfer

Table 8.2: The hardware components requiring monitoring for E2K servers.

Key Indicators

Now that you have an idea of what to monitor and what thresholds you need to consider when monitoring your Exchange and supporting services, you can determine how best to distribute

your hardware for best results. As with any hardware improvements, adding capacity in one area helps only if the rest of the hardware can support it. Having enough storage to support 1,000 users with 50MB mailboxes and OWA support gets you only so far if you only have one CPU and 256MB of memory.

Microsoft provides a table of key indicators for E2K, shown in Table 8.3. (The source for this table is Microsoft Job Aid #5 “Key Exchange Server Performance Indicators,” located at <http://www.microsoft.com/technet/itsolutions/guide/jobaidhl.asp>.)

Object	Counter	Instance
Processor	% Processor Time	0 – n
	% Processor Time	inetinfo
	% Processor Time	EMSMTA
	% Processor Time	STORE
	% Processor Time	MAD
MSExchangeIS Mailbox	Messages Delivered/min	_Total
	Messages Sent/min	_Total
MSExchangeMTA	Messages/Sec	
	Work Queue Length	
MSExchangeMTA Connections	Queue Length	SMTP <ServerName>
SMTP Server	Local Queue Length	_Total
	Local Retry Queue Length	_Total

Table 8.3: Microsoft’s key indicators for E2K.

As you consider your migration environment, you’re likely already monitoring your Exchange 5.5 environment. Because adding E2K can have an impact on your existing environment, I also include in Table 8.4 (the source for this table is Microsoft Job Aid #5: “Key Exchange Server Performance Indicators,” located at <http://www.microsoft.com/technet/itsolutions/guide/jobaidhl.asp>) some of the key performance indicators of Exchange 5.5 servers that you should review during migration.

Object	Counter	Description	Recommendation
Database	Cache Hit %	Percentage of database file page requests that were fulfilled by the IS buffer pool without incurring disk input/output (I/O).	If <85 percent, add more memory.

Object	Counter	Description	Recommendation
	Cache Size	The amount of system memory in bytes that the IS buffer pool is using.	Based on available memory. Use dynamic buffer allocator (DBA) for optimal use of memory. DBA monitors the level of activity on a server and adjusts the amount of virtual memory that Exchange Server's ESE uses. Exchange Server implements DBA as part of the Information Store (IS), so the Store process can adjust quite dramatically when a server experiences periods of heavy demand. Other applications running on the same server can also impact the available memory and the DBA and cache are similarly affected.
	Table Open Cache %	Percentage of database schema information opened from Open Table Cache.	If <75%, add more memory.
MSExchangeIS	RPC Operations/sec	The rate at which Exchange Server RPC operations are occurring.	Establish performance baseline for your deployment.
	Connection Count	The number of client processes connected to the IS.	Establish performance baseline for your deployment.
MSExchangeIS Private	Send Queue Size	The number of messages in the IS's send queue.	Queue should grow and recover to near-zero state but shouldn't build over time. Shouldn't exceed 0.5 percent to 1.0 percent of connected users.
	Receive Queue Size	The number of messages in the IS's receive queue.	Queue should grow and recover to near-zero state but shouldn't build over time.
	Messages Submitted	Total number of messages submitted by clients since service (IS) startup.	Establish performance baseline for your deployment.
MSExchangeMTA	Work Queue Length	The number of outstanding messages in the MTA work queue waiting to be processed.	Queue should grow and recover to near-zero state but shouldn't build over time. Shouldn't exceed 0.5 percent to 1.0 percent of connected users.
MSExchangeIMS	Queued Inbound	The number of queued messages received from the Internet.	Queue should grow and recover to near-zero state but shouldn't build over time.
	Queued Outbound	The number of queued messages queued for delivery to the Internet.	Queue should grow and recover to near-zero state but shouldn't build over time.
	Queued MTS-IN	The number of messages awaiting final delivery to Exchange Server (IS).	Queue should grow and recover to near-zero state but shouldn't build over time.

Object	Counter	Description	Recommendation
	Queued MTS-OUT	The number of messages waiting to be converted to Internet Mail format.	Queue should grow and recover to near-zero state but shouldn't build over time.
MSExchangeMTA Connections	Queue Length	The number of outstanding messages queued for transfer to a remote entity (MTA and so on).	Queue should grow and recover to near-zero state but shouldn't build over time.

Table 8.4: The key performance indicators of Exchange 5.5 servers.

Providing Security in E2K

As an owner of an Exchange environment, you face many potential security issues; if you manage the Win2K and networking environment as well, you face even more. Throughout this book, I've discussed many aspects of security, including setup constraints and SSL issues. Other areas that you need to be concerned about in your security strategy are:

- Controlling viruses
- Controlling spam
- Applying the latest patches

Controlling Viruses

While Microsoft has provided an improved API in E2K to give virus scanners access to messages flowing through the service, you still need to purchase third-party products to do anything useful. Common providers are Trend-Micro, Symantec, Network Associates, Brightmail, and Elron.

Controlling Spam


There are several limited spam controls that you can use in E2K. However, unwanted email, also known as spam or Unsolicited Commercial Email (UCE), seems to be an increasing problem that is continually getting around such controls.

There are two sides to the spam issue.

1. The first is someone sending spam to your users. A number of sites can help you deal with this problem, and they're provided in Appendix A.
2. The second is someone using your servers as a relay to send spam to others. This is known as *being a mail-relay*. Unfortunately, it's easy to put a badly configured Exchange server onto the Internet that allows others to hide their tracks and send email through your server that appears to come from you. In some cases, this capability is important for your own services. However, if you put your Exchange server on the Internet, you need to understand how to carefully configure your SMTP service to avoid being a mail-relay for others.

Unlike earlier versions of Exchange, the default behavior of E2K doesn't relay. If you need to provide relay capabilities for specific requirements, you need to change the behavior of E2K. For details, see the Microsoft article Q268838 "XGEN: Configuring

Exchange 2000 to Receive Mail from Multiple Domains,” available at <http://support.microsoft.com/support/kb/articles/Q268/8/38.ASP>.


 You can find information on how to ensure that your Exchange server isn't used as a relay for spam in the Microsoft article Q193922 “XFOR: Preventing the Internet Mail Service From Relaying Unsolicited Commercial Email Messages,” available at <http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q193922>.

Using the Mailbox Manager

Included with E2K SP1 is the Mailbox Manager, which was originally included as part of the Microsoft BackOffice Resource Kit shipped to support earlier versions of Exchange. When you install SP1, the service runs as part of E2K System Attendant.


The Mailbox Manager allows you to enforce corporate email retention policies by regularly deleting messages that match the rules you specify. It also offers:

- Prescheduled automated operations.
- Individual folders (Inbox, Contacts, and so on) that have their own retention times.
- Administrator reports at the end of each run.
- Deletion of messages of a specific age and/or size. For example, you can specify that Inbox messages should be automatically deleted, or moved to a deletion area, when they're more than xx days old and/or over XXXX kilobytes (KB) in size.

 You can find more information about the Mailbox Manager in the Microsoft article “XADM: Exchange 2000 Server SP1 Mailbox Manager,” available at <http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q278024>.

Applying the Latest Patches

One of the final things you need to monitor as you apply security to your E2K environment is the patch (or hotfix) level of your installations. Microsoft has had a number of problems with patches and SPs—for example, SP1 for E2K was “released” three times before it was considered stable. You obviously need to test all possible software installations in a test environment, and you need to test all the related functionality you use, even if the release comes from Microsoft.

 You can obtain information about the latest service packs for E2K in the Microsoft article Q301378, “XGEN: How to Obtain the Latest Exchange 2000 Server Service Pack.” It's available at <http://support.microsoft.com/support/kb/articles/Q301/3/78.ASP>.

Summary

That's it for this journey through Windows and Exchange migration. There are many other avenues you could have taken as you planned your migration, and I thank you for taking the journey with me. At the beginning of this book, I said that it would be a concise and practical guide to Win2K and E2K migration. I hope you found this to be the case, and I welcome any comments you care to make. I tried to present topics that were useful and applicable to all

readers, but the amount of information provided in areas such as management and tools is only functional and not necessarily comprehensive.

I recommend that you check out the resources in Appendix A. They include not only a consolidated list of the tools that have been discussed throughout this book but also Web sites that you'll find useful for keeping current on the topic of migration.

[Editor's Note: This content was excerpted from the free eBook *The Definitive Guide to Windows 2000 and Exchange 2000 Migration* (Realtimepublishers.com) written by Archie Reed and available at <http://cc.realtimepublishers.com/publicationhome.asp?pid=23>.]