Microsoft®
Exchange 2000
Server

Exchange 2000 Recipient Management

White Paper

Published: October 2001

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

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

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

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

Exchange 2000 Recipient Management

Abstract

Managing recipients in Microsoft® Exchange 2000 Server is significantly different from managing recipients in previous versions of Exchange. This release introduces new features, and integration with Microsoft Windows® Active Directory™ service means considerable changes. Windows user accounts and Exchange recipients are merged conceptually and managed through the same interface. The establishment of recipient policies and improvements in address lists provide further administrative flexibility. However, as with other components in Exchange, functionality is restricted in recipient management in mixed environments where previous versions of Exchange Server are present. This document helps you perform familiar tasks, leverage new features, and successfully maintain coexistence of Exchange 2000 Server and Exchange Server version 5.5.

For more information, see http://www.microsoft.com/exchange/.

Contents

Exchange 2000 Recipient Management

Introduction

The recommendations made in this documentation are based on the assumption that you use the Microsoft Windows 2000 Active Directory Users and Computers snap-in to manage your recipients, and the System Manager snap-in in Microsoft Exchange 2000 to manage your Exchange servers. We discuss both native and mixed environments because many customers support Exchange Server version 5.5 in their organizations. However, we do not refer to versions older than 5.5.

Definition of Exchange Recipients

Exchange recipients are objects that have e-mail capabilities. This section explains the four types of Exchange 2000 recipients: users, contacts, groups, and public folders.

Users

Active Directory user accounts enable users to log on to computers and domains with identities that can be authenticated and authorized for access to domain resources. Users who log on to the network must have their own unique user accounts and passwords. User accounts also can be used as service accounts for some applications. Users can be added to groups and appear in the global address list (GAL).

Note the difference between *mail*-enabled and *mailbox*-enabled users. A mailbox-enabled user is equivalent to an Exchange 5.5 user, while a mail-enabled user is equivalent to a custom recipient. If a user account is mail-enabled but not mailbox-enabled, the user can receive e-mail at an external e-mail address but cannot store messages on your Exchange server. Only recipients with Active Directory accounts can be mailbox-enabled to send and receive e-mail. You must install Exchange to mailbox-enable a user. You then can specify the location of the user's mailbox on the Exchange store. However, the Windows 2000 operating system has native Simple Mail Transfer Protocol (SMTP) service capabilities that enable you to specify external e-mail addresses for users even before Exchange is installed.

Contacts

A contact is an Active Directory object that does not have permissions to access domain resources. A contact usually represents someone outside your Exchange organization, such as a partner or a customer. Contacts cannot be given mailboxes on your Exchange server. However, you can specify external e-mail addresses for contacts and add them to groups and GAL.

A contact is equivalent to a custom recipient in Exchange 5.5.

Groups

A group is an Active Directory object that can contain users, contacts, public folders, and other groups. There are two main types of groups: security groups and distribution groups. Security groups are used to collect objects into a manageable unit for controlling access to resources; they can be mail-enabled. Distribution groups are used only as e-mail distribution lists.

You can break down groups further into domain local, global, and universal groups. Each group represents a different scope for membership criteria and access permissions. When the forest is in native Windows 2000 mode, you can freely convert between security and distribution group types, and change the scope of the groups. When the forest is in mixed mode, however, conversion is not allowed and only distribution groups can have universal scope. It is not necessary to have a detailed understanding of all the group types. However, it is recommended that you read the Windows 2000 documentation to become familiar with all the different varieties.

Note: Only the membership of a universal group is replicated across domains. This design minimizes replication traffic, but it means you must configure your distribution lists as mail-enabled groups of universal scope. Otherwise, if you use a domain local or global group, you must specify an expansion server in the same domain as this group. This ensures proper membership expansion for delivery of e-mail sent to the group. When Exchange 5.5 distribution lists are replicated to Active Directory, they are converted to universal security groups.

Public Folders

A public folder is an Exchange-specific object that stores messages or information that can be shared among users in your organization. Unlike users and contacts, which are native Windows objects, public folders only appear in Active Directory if you mail-enable them.

In a mixed environment, all the Messaging Application Programming Interface (MAPI) folders are mail-enabled by default. This is to make them compatible with Exchange 5.5, in which all the public folders had an associated directory object. However, Exchange 2000 provides the capability for unlimited creation of general-purpose public folder trees. Folders under these trees are not mail-enabled by default. In addition, in a native environment, no public folders are mail-enabled by default.

Mail-enabled public folders can be displayed in GAL and can be added to groups. For example, you may want to include a public folder in a group to archive all the messages sent to that group.

Key Concepts

- Mailboxes are equivalent to Exchange 5.5 users.
- Mail-enabled users and contacts are equivalent to Exchange 5.5 custom recipients.
- MAPI public folders are mail-enabled by default in a mixed environment; general-purpose folders are not.
- In a pure Exchange 2000 environment, public folders are not mail-enabled by default, thus there are no directory objects for them.
- Only universal group membership will be replicated across domains.

Managing Recipients

When Exchange 2000 Server is installed, it extends the Active Directory Users and Computers snap-in with additional tabs on the Properties page and with right-click menu items. Although you can manage recipients from previous versions of Exchange, it is highly recommended that you only use Active Directory Users and Computers for consistency and simplicity. Using Active Directory Users and Computers enables you to combine the administration of Windows user accounts with that of Exchange recipients. However, note that system administration tasks are performed by using a completely separate interface.

This section identifies some Active Directory concepts that are essential to organizing and managing Exchange recipients. This documentation reviews the process of mail-enabling and mailbox-enabling users, and discusses administrative roles and boundaries.

Domains

A domain is a grouping of network objects such as users, groups, and computers. All objects in a domain are stored in Active Directory. Domains can be nested in a hierarchical structure called a domain tree. Multiple domain trees form a forest.

Each domain is a security boundary in that security policies and settings—such as administrative rights, security policies, and access control lists (ACLs)—do not cross from one domain to another. The administrator of a particular domain has rights to set policies in that domain only. Different administrators can create and manage different domains in an organization.

Each domain may have one or more domain controllers, and changes made to directory objects are written to a domain controller. Your organization may have multiple domains that make up a forest. Active Directory replicates across domains in order to keep all the information synchronized. A special type of domain controller hosts the Global Catalog, which contains a full replica of all objects in the directory for its own domain and a partial replica of all objects contained in the directory of every other domain in the forest. For more information about domains, forests, domain controllers, and global catalog servers, refer to the Windows documentation.

Organizational Units

Organizational units are Active Directory containers in which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains.

An organizational unit is the smallest scope or unit to which you can delegate administrative authority. Organizational units can be used to create hierarchies in a domain that follow the structure of your organization, providing a logical and intuitive administrative model.

A user can be granted administrative authority for all organizational units in a domain or for a single organizational unit. An administrator of an organizational unit does not need to have administrative authority for any other organizational units in the domain.

Administrative Roles

Now that you have learned about the basic containers for organizing recipients, it is time to consider the role of recipient manager. There are many permissions (access to objects) and rights (granted to users) that can be configured to implement a security model. Fortunately, the management of Exchange recipients only deals with a relatively small subset of these permissions and rights.

Depending on the size and structure of your organization, the person who manages user accounts may or may not be the same person who manages your Exchange servers. In case of the latter, the user manager needs to have appropriate permissions to Exchange as well. This ensures that recipients can be associated with an Exchange server and mailbox store for proper mail delivery. At a minimum, the recipient manager is required to have view-only permission on the administrative group container in order to create e-mail addresses or mailboxes. For more information about the Exchange permission model, see the Exchange 2000 Server documentation.

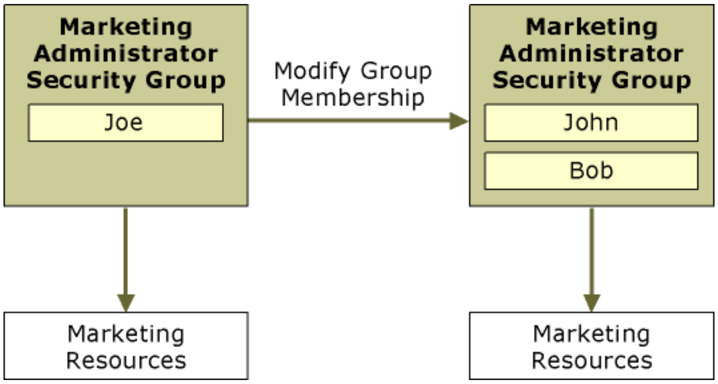
Assigning Permissions

You must put administrators into security groups and assign proper permissions to each group. As mentioned previously, security groups are used to collect users and other groups into manageable units. Each account added to a group receives the rights and permissions defined for that group. The permissions are assigned once to the group, instead of several times to each individual user.

For example, suppose that the recipients are organized into organizational units that correspond to the various departments in your organization: Marketing, Sales, and Development. You would like Joe to manage the Marketing and Sales departments. The Development team is larger, so both Mary and Alice manage it.

You can create three security groups, Marketing Admin, Sales Admin, and Dev Admin. You should include Joe in the membership of the first two, Mary and Alice on the last one. Use the delegation tool in Active Directory Users and Computers to give each of these groups rights on the appropriate organizational unit.

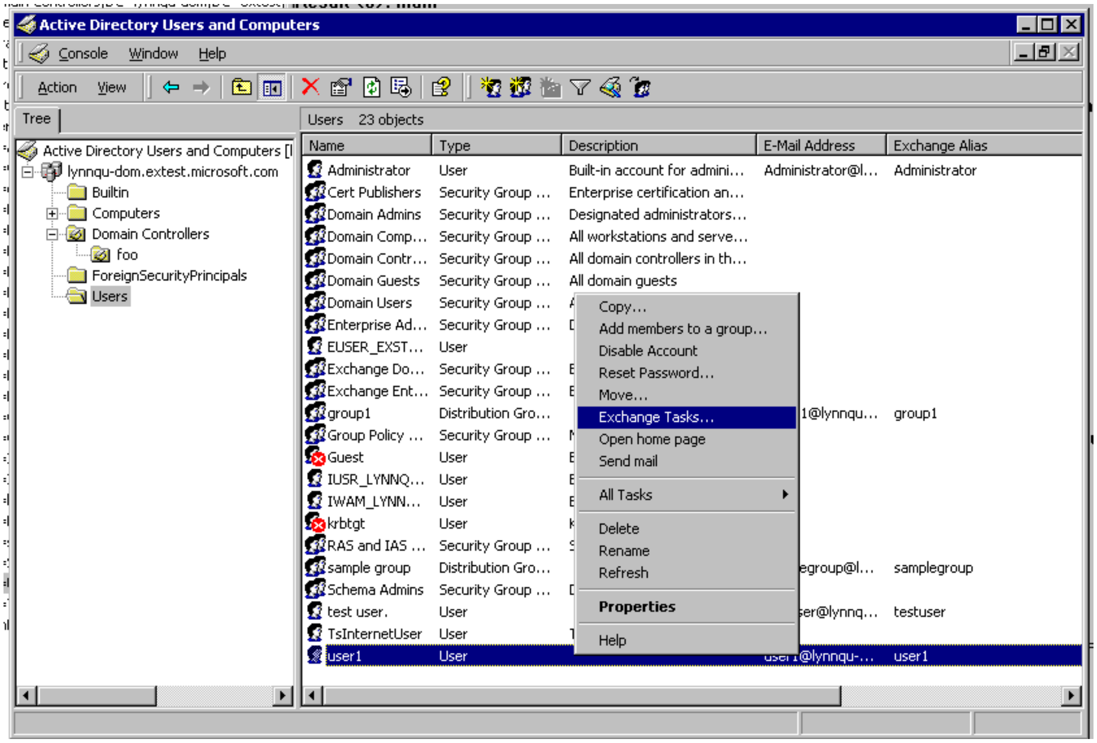
Next suppose that the Sales team suddenly triples in size and you decide to hire Bob and John to manage the new larger Sales staff, and let Joe concentrate on managing the Marketing team. Instead of modifying permissions on John, Bob, and Joe to accommodate their new roles, simply add John and Bob to the Sales Admin group and remove Joe from it.


Marketing Administrator Security Group
Joe
Modify Group Membership
Marketing Administrator Security Group
John
Bob
Marketing Resources
Marketing Resources

Group permissions

Creating Mailboxes

One of the most common and basic tasks you will perform is the creation of mailboxes. In the righthand pane of the Active Directory Users and Computers snap-in, right-click the recipient and then click Exchange Tasks. This launches a simple wizard that enables you to perform almost all of the Exchange-related tasks applicable to that recipient. Choose Create Mailbox and proceed until completion.



Name	Type	Description	E-Mail Address	Exchange Alias
Administrator	User	Built-in account for admini...	Administrator@l...	Administrator
Cert Publishers	Security Group ...	Enterprise certification an...		
Domain Admins	Security Group ...	Designated administrators...		
Domain Comp...	Security Group ...	All workstations and serve...		
Domain Contr...	Security Group ...	All domain controllers in th...		
Domain Guests	Security Group ...	All domain guests		
Domain Users	Security Group ...	A		
Enterprise Ad...	Security Group ...	D		
EUSER_EXST...	User			
Exchange Do...	Security Group ...	E		
Exchange Ent...	Security Group ...	E		
group1	Distribution Gro...		1@lynnqu...	group1
Group Policy ...	Security Group ...	M		
Guest	User	B		
IUSR_LYNNQ...	User	B		
IWAM_LYNN...	User	B		
krbtgt	User	K		
RAS and IAS ...	Security Group ...	S		
sample group	Distribution Gro...		egroup@l...	samplegroup
Schema Admins	Security Group ...	D		
test user.	User		er@lynnq...	testuser
TsInternetUser	User	T		
user1	User		user1@lynnqu-...	user1

Exchange Tasks

Creating a mailbox automatically establishes e-mail proxies for the recipient. However, you will not see the proxies in the results pane right away. This is because proxies are generated by the Recipient Update Service (RUS), which runs at customized intervals. Even if the service is set to Always Run, there is still a short latency, usually less than a minute, before proxy generation.

The actual mailbox is not created on the Exchange store database until the user logs on for the first time. Note that a user cannot log on without e-mail addresses (that is, SMTP, X.400, and so forth).

Therefore, even after being mailbox-enabled, a user must wait until RUS has processed the account before trying to log on.

In addition, after Exchange is installed, any new user is created with a mailbox by default. You can clear the Create An Exchange Mailbox check box in the wizard if you do not want a user to have a mailbox.

Deleting Mailboxes

You can use Exchange Task Wizard to delete a mailbox. Deleting a mailbox will permanently remove all the messages contained in that mailbox. Note that when you delete a user account without explicitly deleting the mailbox first, the mailbox will be marked for deletion. It will be deleted when the mailbox cleanup procedure is performed, either manually or when the deletion setting limit has been reached for that database. Until then, the mailbox remains on the Exchange store and can be recovered if needed.

Moving Mailboxes

You may need to move a user's mailbox from one server or mailbox store to another on occasion. For example, if you replace hardware, you must move all users' mailboxes from the old server to the new server. To do this, make sure that the proper mailbox stores have been created on the new server and that you have permissions to access these stores. You then can use Exchange Task Wizard to move mailboxes.

Creating E-Mail Addresses

You can use Exchange Task Wizard to assign external e-mail addresses to users, groups, and contacts. This allows the recipients to be seen in GAL, from which their properties are easily viewable and they can be easily contacted. As mentioned in previous sections, users, contacts, and groups that have only e-mail addresses cannot store their e-mail messages on one of your Exchange servers.

Key Concepts

- To create mailbox-enabled or mail-enabled users, contacts, or groups, you must have at least view-only permissions on administrative groups.
- If you use groups to assign permissions to an object, controlling access is as simple as maintaining group membership.
- A newly created user does not have a proxy until the Recipient Update Service has processed it; therefore, the user cannot log on right away.
- The physical mailbox for the user is only created after he or she logs on for the first time.

Recipient Settings

You can edit various Exchange-related settings on the recipient's Properties page. The Exchange General, Exchange Features, and E-mail Addresses tabs are shown by default. In Advanced mode, you also can view and modify the Exchange Advanced tab.

In addition, many of these settings can be configured on a larger scale by using System Manager. You can configure recipient properties individually but will probably only occasionally need to do so.

Recipient Properties

The following list describes some of the Exchange recipient settings you may want to configure:

- **E-mail addresses.** These are the various proxy addresses at which a recipient can receive e-mail. The primary e-mail address, which is displayed in bold, is the one that appears in the From field of outgoing messages. If there is more than one proxy of the same type, you should specify which one is used as the primary e-mail address. You cannot delete a primary e-mail address. By default, you must have at least one SMTP address and one X.400 address. Typically, e-mail addresses are defined through recipient policies, but you also can modify them on an individual basis.

- **Message format.** This is the format of SMTP e-mail messages sent by users. This is set at an organization-wide level in Internet Message Formats under the Global Settings node in System Manager. You may want to configure specific formats for certain domains if, for example, some of your company's partners use older messaging clients that do not support Multipurpose Internet Mail Extensions (MIME). From the same location, you can control which automatic replies can be sent to that SMTP domain. For example, you may not want out-of-office replies to be sent outside your organization, because you may not want external parties to know that a user is out of town.
- **Delivery restrictions.** These restrictions define outgoing and incoming message size limit, in addition to which users in your organization can send e-mail to a particular user. You can set delivery restrictions at an organization-wide level in Message Delivery under the Global Settings node in System Manager, where you can also block inbound messages from external sources.
- **Delivery options.** These options allow others to send e-mail on behalf of the user and to automatically forward the e-mail messages to another recipient's account.
- **Storage limits.** These are the limits at which users receive warnings or become unable to compose or receive new messages. You can set these at a higher level as properties of the mailbox store. The recipient settings will default to that of the database on which the user's mailbox is located. You may want to change the default for a special-case user.
- **Protocol settings.** These settings enable various protocols for the recipient (HTTP, IMAP4, and POP3). For protocols such as IMAP4 and POP3, you can also specify message formats.
- **Hide from Address Lists.** This option hides the recipient from GAL so that other users in the organization cannot see the recipient or the recipient's properties. Note that Exchange Administrator accounts and Exchange Server accounts can access the hidden properties.
- **Hidden Group Membership.** This option hides the membership of a mail-enabled group so that e-mail can be sent to the group but users cannot view the membership. You also can configure this property in Exchange Task Wizard. Again, Exchange Administrators and Exchange Server accounts can access the hidden membership.

Display Formats

- **Display Name Format.** This is the format in which the user's name is displayed in GAL. By default, Windows has set the form of <first name> <last name>. It is possible to change this default by using Active Directory Services Interface (ADSI) edit.
- **E-mail Address Format.** This is the format of the user's e-mail address. By default, the SMTP address is *alias@yourcompany.com*. If you want to arrange the format differently, you can create a company-wide recipient policy and use a combination of %g(first name), %s(last name), %i(middle initial), and so on, to specify the e-mail address format.

Key Concepts

- Recipient settings should be configured at a high level—under Global Settings in System Manager, or through recipient or system policies.
- Exchange Server and Administrator accounts have access to objects hidden from address lists and hidden memberships.

Recipient Policies

A recipient policy is a collection of settings that can be applied to a select set of Exchange recipients. With Exchange 2000, you can use recipient policies to set up e-mail addresses and allow your Exchange system to accept inbound messages targeted to all these addresses. In particular, SMTP addresses on recipient policies are used to specify the set of SMTP domains (for example, *company1.com, company2.com*) for which your Exchange organization will accept e-mail. The Exchange 2000 routing engine uses these SMTP addresses to define the local domains.

This is a useful feature if your organization needs more than just one default e-mail domain—for example, if you want to distinguish multiple divisions or branch offices in different geographical regions. RUS processes each policy and recipient, and automatically generates e-mail addresses for recipients defined in each policy. However, recipients in a mixed site that also has Exchange 5.5 servers cannot take advantage of this feature because this legacy version of Exchange cannot handle multiple e-mail addresses.

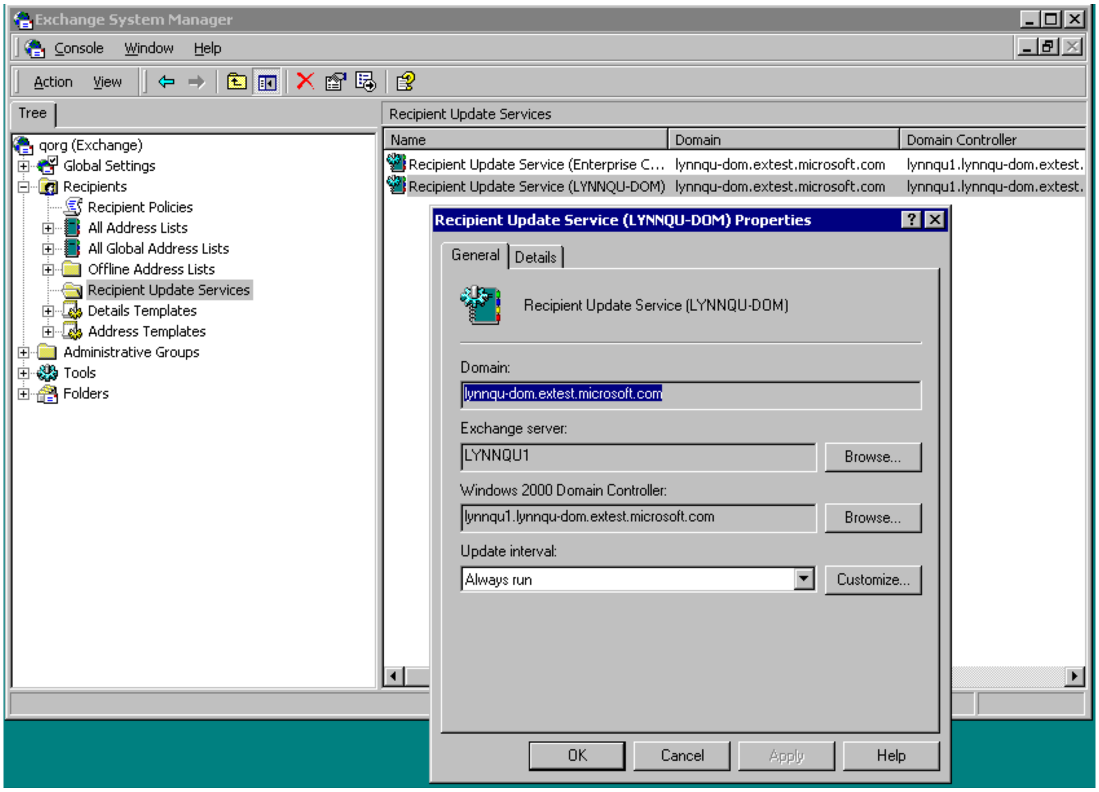
Recipient Update Service

There are two types of Recipient Management Services. One is responsible for processing Exchange system objects in the Configuration container, and the other is responsible for processing recipients in each domain. There is only one of the first type in the entire Windows forest because there is only one Configuration container. The second type of RUS can have multiple instances, even in the same domain. This section focuses on the second type of RUS, which is responsible for processing recipients in each domain, because it applies recipient policies.

You must have at least one RUS for each domain in your organization, and it must be run from an Exchange 2000 server. For domains that do not contain any Exchange 2000 servers, the RUS you create needs to be run from an Exchange 2000 server outside the domain. Each RUS must read from and write to a unique domain controller. If there are multiple domain controllers in a domain, then there can be multiple RUSs running in the same domain.

Setting up multiple RUSs is desirable in order to overcome network latency issues when the domain spans several sites and connection between sites is slow. For example, if you have a site in Seattle and another site in Beijing, there may be a long delay before a mailbox created in Beijing is processed by the RUS in Seattle. As a result, e-mail address generation will be slow and the user must wait a long time before being able to log on to the mailbox (recall that a user cannot log on without a proxy). Ideally, you set up a RUS in Beijing that can use the domain controller in the local site.

You can schedule appropriate intervals to run this service. Make sure that the interval is long enough to allow the update task to complete before the next update begins. You may need to run a few tests to find out how long the update service takes to complete its task. True to the term “update,” RUS processes only changes made since the last time it was run, which makes it efficient. The changes could have come from policies or recipients.



Recipient Update Services

Name	Domain	Domain Controller
Recipient Update Service (Enterprise C...	lynnqu-dom.extest.microsoft.com	lynnqu1.lynnqu-dom.extest.
Recipient Update Service (LYNNQU-DOM)	lynnqu-dom.extest.microsoft.com	lynnqu1.lynnqu-dom.extest.

Recipient Update Service (LYNNQU-DOM)

Domain: lynnqu-dom.extest.microsoft.com

Exchange server: LYNNQU1

Windows 2000 Domain Controller: lynnqu1.lynnqu-dom.extest.microsoft.com

Update interval: Always run

RUS update interval

You can manually force a RUS to run by choosing Update Now or Rebuild from the right-click options. Update Now shortens the interval before the next update, and RUS still updates only the changes. Rebuild forces a complete processing through all the recipient policies and recipients, even those that have not changed. For this reason, rebuilding usually takes significantly longer than updating and should not be used often.

Default Recipient Policy

Default policies cannot be modified or deleted. When you are in a mixed-mode environment, there is one default policy for each Exchange 5.5 site. These default policies are compatible with Exchange 5.5 site addressing and are the only policies that apply to recipients whose mailboxes are on servers in a mixed site. These recipients cannot receive e-mail at multiple e-mail addresses.

In a pure Exchange 2000 organization, a single default recipient policy automatically generates e-mail addresses for all the recipients in the organization. The default SMTP domain name is the Microsoft Windows NT® domain in which your Exchange organization resides. Although it cannot be modified or deleted, you can easily create new policies to override this default.

Creating New Recipient Policies

To create a new recipient policy, you must first define to whom the policy will be applied. Exchange 2000 provides a Find command that allows you to select the desired set of recipients. This interface is based on a Lightweight Directory Access Protocol (LDAP) query, per RFC2254, that allows you to filter by any Active Directory attribute.

For example, suppose that you want to give all your support engineers a more specific e-mail address. First, use the filter to specify that you want all users with a Department attribute equal to “Support.” Exchange maps the requirements to an LDAP query, which is displayed in raw form on the General tab of a policy. You also can bypass the Find command and use the Custom Search option on the

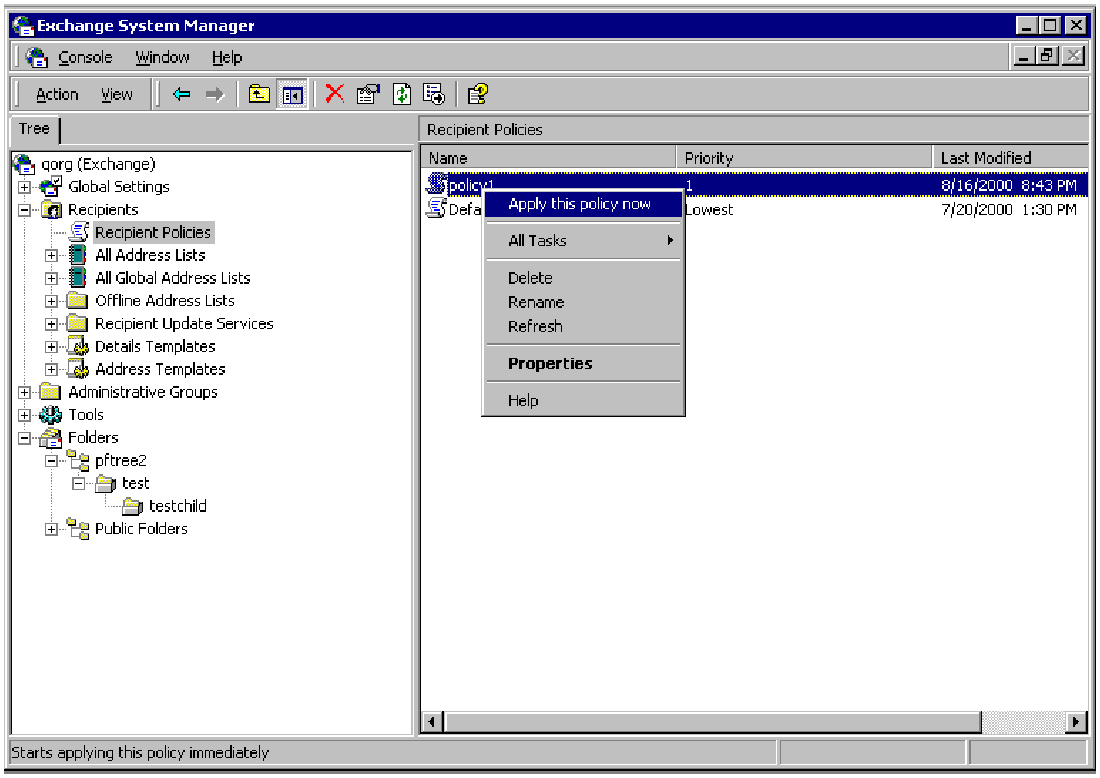
Advanced tab to type the query directly. Alternately, you can copy and paste an existing LDAP query and modify it.

After the filter is created, you can define one or more e-mail addresses that apply to the recipients under the policy. In this example, your policy may include two SMTP e-mail addresses: *alias@support.yourcompany.com* and *alias@yourcompany.com.* This means your Exchange system will accept e-mail for these recipients at both addresses.

In addition, as mentioned earlier, you can change the format of the left portion of the address. For example, %s.%g@yourcompany.com will result in the format of *<last name>.<first name>@yourcompany.com*.

Applying a Policy

If a recipient falls under more than one policy, the highest priority policy takes effect. You can change the priority of the policies, except for the default policies. In addition, you can manually apply a policy instead of waiting for RUS to run at its scheduled interval. This would be useful if you change the policy and want the change to take effect as soon as possible.



Name	Priority	Last Modified
policy1	1	8/16/2000 8:43 PM
Defa	Lowest	7/20/2000 1:30 PM

Starts applying this policy immediately

Applying a policy

Note: If you want to apply a policy to all recipients—both existing recipients and any new recipients that are created—you must manually apply the policy and select the option of applying it to existing users. Otherwise, this policy will affect only newly created users.

Removing a Policy or Proxy

You can remove proxy addresses so that they no longer are assigned to recipients in one of three ways. However, none of these will remove proxy addresses from recipients that already have them.

- **Disable the Proxy.** If you clear the check box on a proxy you have previously defined, new recipients under the associated policy no longer will receive this proxy address. However, existing recipients will continue to receive e-mail at this address.

- **Remove the Proxy.** If you delete the proxy, existing users will still have this proxy address, but newly created users will not. Note that you cannot delete any primary proxy addresses.
- **Remove the Policy.** If you delete the policy object, the proxies that were previously assigned by this policy will not be removed from existing recipients. As mentioned previously, if you create a new policy that applies to this set of orphaned recipients, you need to apply the new policy manually.

Recipient Policy and Web Access

If you have configured multiple recipient policies, you will need to perform one of the following steps to accommodate access using the Web client:

- Create a corresponding HTTP virtual directory for each additional SMTP e-mail domain and point the directory at mailboxes for that domain. This allows Exchange to correctly map out the SMTP address for the user and find his or her mailbox.
- Add the common SMTP domain as a secondary SMTP address for all recipients. This allows the original "flat" namespace (the default SMTP domain) to still work for the client, and Exchange will be able to find the mailbox.

Key Concepts

- Exchange 2000 recipient policy allows you to select a set of users based on an LDAP query and to configure multiple e-mail addresses for them. However, you cannot do this for sites that have Exchange 5.5 servers.
- You must have at least one RUS per domain, and it must run on an Exchange 2000 server. Each RUS must connect to a unique domain controller.
- RUS processes changes each time it runs. If you force a rebuild, RUS will process all objects, which can take a long time.
- Deleting a recipient policy or deleting or disabling a particular proxy does not remove the associated proxy from existing users.
- New policies are not, by default, applied to users previously under another policy.
- You may need to create an additional virtual directory for each unique SMTP domain defined by a recipient policy.

Address Lists

Address lists help you organize the presentation of Exchange recipients to clients such as Microsoft Outlook®. Address lists can be used to address e-mail messages, choose meeting attendees, and look up locations and phone numbers of others in your organization. Exchange 2000 allows you to create address lists based on any attribute in Active Directory. The membership of each address list is maintained by RUS.

Users can access GAL for a complete set of Exchange recipients or relevant subsets of it. In addition, offline address lists can be downloaded as a data resource when you do not have access to the corporate network. Exchange 2000 provides much more flexibility in customization of both the global and offline address lists.

Default Address Lists

Exchange 2000 installs a collection of address lists during setup: All Contacts, All Groups, All Users, All Conferencing Resources, Public Folders, and Global Address List. These are available to every user in your organization by default. Note that, although the criteria of default address lists cannot be modified, they can be renamed or deleted.

Creating Custom Address Lists

You can create customized address lists to meet your users' needs. These custom address lists can be created according to location, department, teams, or any other Active Directory attribute. As with recipient policies, the LDAP query-based filter is used to select the appropriate set of recipients that should be included in the address list. Once created, you can preview the membership of an address list.

It may be a good idea to name the address list so that the name reflects its filter criteria—for example, North American Employees. You also can create empty address lists as a container for organizing address lists underneath it. For example, you might have an empty address list named Full-Time Employees, with address lists such as Engineers, Marketing Staff, Human Resource Staff, and so forth placed under it.

RUS and Address Lists

When RUS runs, it processes changes made in address lists as well as changes in the directory. This is how the membership of the address list is kept current. In particular, when a new recipient is created, RUS sets the showInAddressBook attribute when it processes the recipient. This attribute points to all the address lists in which the recipient is included. Thus, RUS must finish updating before a new recipient will appear in address lists.

In addition, when you hide a recipient from address lists, the ms-Exchange-Hide-From-Address-Lists flag is set on the recipient object. RUS will clear the showInAddressBook attribute, thus preventing the recipient from being viewed in address lists. When you unhide it, RUS reevaluates the attribute based on the filters of the current address lists.

Address List Access Control

You may need to create multiple address lists if your organization has numerous locations, departments, product teams, and so forth. Exchange 2000 allows you to control which users can access these lists by exposing the access control editor on each address list object. On the Security tab of the address list, you can explicitly deny the Open Address List right to anyone who should not be able to access this particular address list.

Exchange 2000 also provides the capability of configuring more than one GAL. However, the user only sees one GAL. The GAL that the client sees is determined by ordered evaluation:

- User has rights to open the GAL
- User is a member of the GAL
- Largest GAL out of those that remain

Offline Address Lists

Exchange 2000 allows you to create multiple offline address lists, which are composed of any combination of existing address lists. Each mailbox store is associated with an offline address list. When users whose mailboxes are on that store connect to the Exchange server remotely, they can download offline address lists. They also can choose to download only updates that were made since the last download.

Offline address lists are generated and stored on a specified server. Only Exchange 2000 servers can generate Exchange 2000 address lists, which means that users connected to servers running Exchange 5.5 must use the legacy version of the offline address book.

You can schedule when offline address lists are updated. Therefore, if there are frequent changes, you can schedule updates to be made more often to keep the data current. You also can manually update the address list if, for example, you just made a change but your next scheduled update is not for some time.

Key Concepts

- Exchange 2000 allows you to create address lists based on an LDAP query, and to build customized global and offline address lists. However, only Exchange 2000 servers can generate these new address lists.

- The showInAddressBook attribute on a recipient contains links to address lists to which the recipient belongs. You set and maintain this attribute through RUS.
- Control access to the address list by setting the Open Address List right on the Security tab.