# Hosting Multiple Virtual Organizations with Microsoft Windows 2000 and Microsoft Exchange 2000 Server

Implementing virtual organizations for Windows 2000 and Exchange 2000 is going to require several basic steps, each of which will be illustrated in more details below:

1. Add a **domain suffix** for each virtual organization, that suffix will be used in defining the user's User Principle Name (UPN) and e-mail address.
2. Set up a **mail Exchanger (MX) record** in the Domain Name System (DNS) for each virtual organization to point to the hosting organization.
3. Create new **storage groups and databases** for each virtual organization ***(optional)***.
4. Create **OUs** for each virtual organization.
5. Create **global groups** for each virtual organization; all members for each OU will go in these groups.
6. Set the appropriate **rights** on the default Windows 2000 containers, and assign special rights to the OUs that are created.
7. Add the **domain names** to the list of domains for which Exchange will accept and route mail as inbound.
8. Create a **public folder** psuedo root for each virtual organization, and set rights on it so that it is only visible and accessible by members of that virtual organization ***(optional)***.
9. Once it's working, **delegate the appropriate permissions** and deliver custom Microsoft Management Console (MMC) workspaces with which delegated administrators can perform their tasks ***(optional)***.

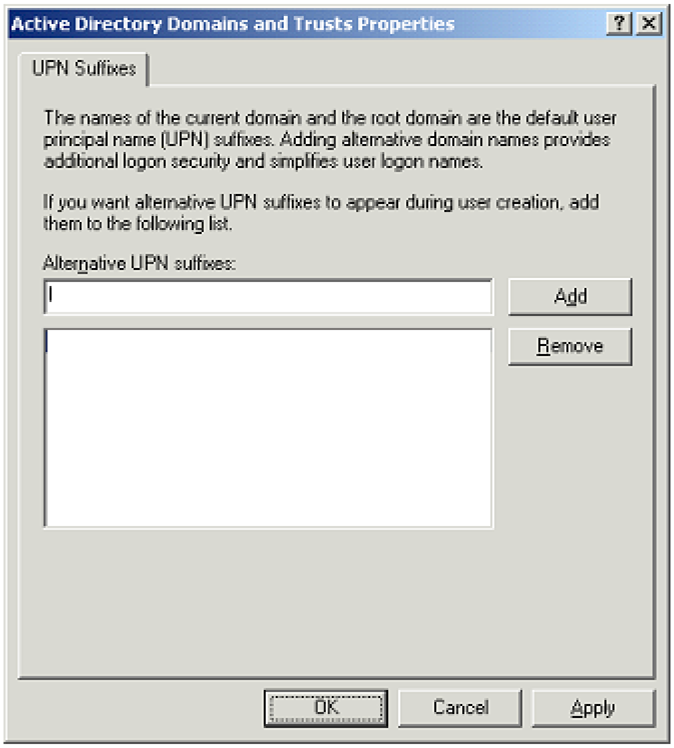
To help illustrate each of these points, this paper will walk through the scenario of the fictitious organization, Wide World Importing, an organization that is running Windows 2000 and Exchange 2000 and has decided to offer mail hosting services. They have already installed Windows 2000 and Active Directory with a namespace of Wide-World-Importers.Microsoft.com. They have also installed Exchange 2000 and are able to send and receive e-mail for Contoso.Microsoft.com users.

Three companies have signed up for the hosting services – Contoso.Microsoft.com, ContosoCable.Microsoft.com, and ContosoTelecom.Microsoft.com. Here is the process to go through to create the infrastructure to support each of those virtual organizations.

## *1.Adding a New Domain Suffix*

The first thing that needs to be done is to add a domain suffix for each of the three companies that are being hosted. This allows users within an OU to have a UPN and e-mail address that corresponds to their company name, instead of Wide-World-Importers.com. To add a new suffix, do the following:

1. Open the **Active Directory Domains and Trusts** snap-in.
2. Right-click on the top-most node in the tree that is titled **Active Directory Domains and Trusts**, ***NOT*** the actual domain that is shown in the MMC.
3. Click **Properties** from the menu, and a dialog box with one tab titled **UPN Suffixes** appears.



Active Directory Domains and Trusts Properties

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

4. Type in the name of each virtual organization and click **Add**. Once all the suffixes have been added to the list click **OK**. Those suffixes will now appear in the list of domains drop down that is used for logon domain during user account creation.

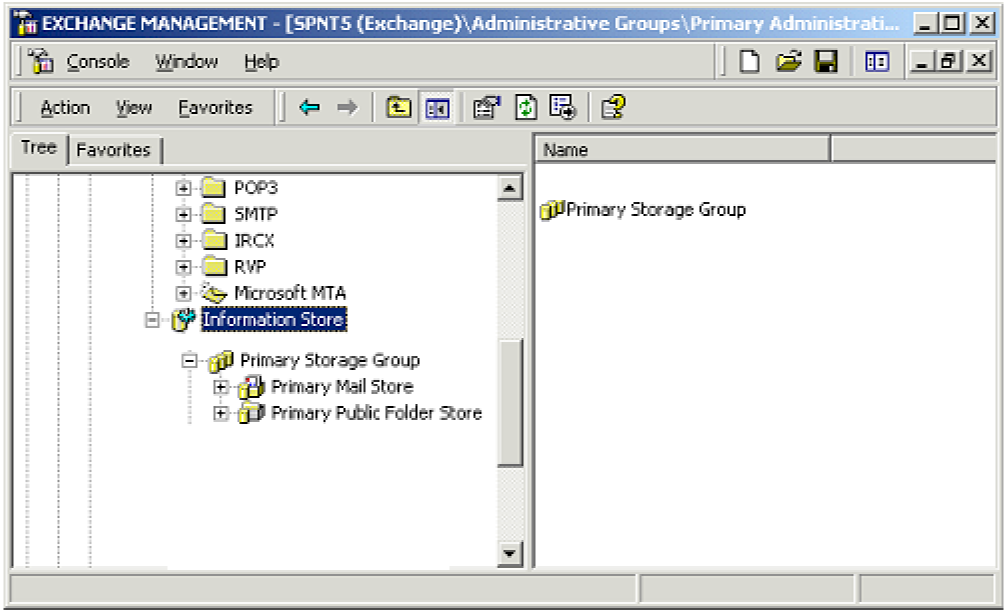
## *2.DNS Setup*

DNS needs to contain a Mail Exchanger (MX) record for each virtual organization that is being hosted. In order for routing to properly occur, the MX record should point to the IP address(es) of the Exchange machines that are already configured to send and receive SMTP messages to and from the Internet. The Exchange servers act as the routing backbone for the various virtual organizations, sending each message to its appropriate server based upon recipient.

## *3.Creating Storage Groups and Databases*

This step is **optional**, and its necessity should only be driven by business requirements. It may be required or preferred to create separate storage groups and databases for each virtual org. The advantages in doing this are that it allows for more flexibility and granularity in configuring the organization. In addition, if there are problems with the database for one virtual organization, the other organizations are not affected by it.

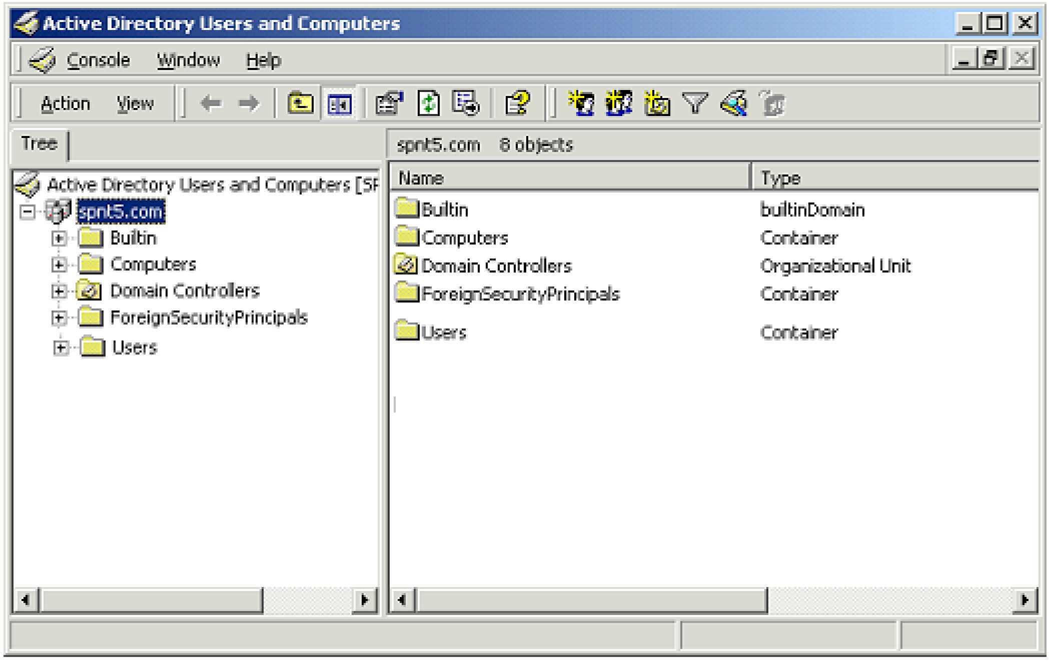
In this scenario where there are multiple virtual organizations being hosted on one box, we are creating separate storage groups for each org. Each storage group also has its own private mailbox store database. Once those have been created, the storage structure of the server looks like this:



It includes storage groups and databases for each of the virtual organizations that are going to be created, in addition to the default storage group, mail store and public folder store. It's important to note that there are limitations when running multiple private mail stores on one server, such that they can all only be linked to one default public folder store. So, in this scenario the private mail stores are all associated with the Primary Public Folder Store for their default public store data.

## *4. Creating Organizational Units*

The next step is to create Organizational Units (OUs) in Active Directory for each virtual organization being hosted. To do this, start the **Active Directory Users and Computers** snap-in. Right-click on the domain and select **New…Organizational Unit** from the menu. A dialog box appears where you can type the name of the OU to add. Repeat this step for each virtual organization being hosted.


Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Active Directory Users and Computers [SF
spnt5.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
spnt5.com 8 objects

| Name | Type |
|---|---|
| Builtin | builtinDomain |
| Computers | Container |
| Domain Controllers | Organizational Unit |
| ForeignSecurityPrincipals | Container |
| Users | Container |

## 5.Creating Groups and Add Users

After the OU has been created, a global group needs to be created in every OU. That group name should reflect the fact that it contains all users in that OU. To do this:

1. Right-click the OU name in the left pane of the **Active Directory Users and Computers** snap-in.
2. Select **New…Group** from the menu. A wizard dialog box appears.
3. Type in the group name, and select the options to make it **Global** in scope and **Security** in type.
4. Click **Next** on the wizard. You now have the option of creating an e-mail address for the group. This is recommended since it gives you an alias by which you can e-mail every member of the virtual organization.
5. Type the name of Exchange alias you want for the group – the **Create an Exchange e-mail address** box is already checked by default – and click **Next** to continue.
6. Click **Finish** to complete the wizard.

After the group has been added, add the users for the virtual organization. Create each user in the corresponding OU for that virtual org.

When creating the user, make sure an Exchange mailbox is created also. If separate databases and/or storage groups were created for each virtual org, make sure the mailbox is created in the appropriate storage location for the organization to which the user belongs.

After all the users have been added to the OU, put them all in the global group for that OU. As new users are added to the organization, they need merely be created in the OU and added to the global group for that OU to inherit all the same permissions as other users in that org.

Finally, one “master” global or universal group should be created that contains the OU’s global group for every virtual organization you are hosting (note that your domain needs to be in Native mode to support Universal groups or nesting global groups within other global groups). When this group is created make sure to create an e-mail alias for it. If new organizations are added in the future, their global group also needs to be added to this master group. The necessity of this is for creating multiple psuedo public folder roots in the Exchange organization (one for each virtual organization).

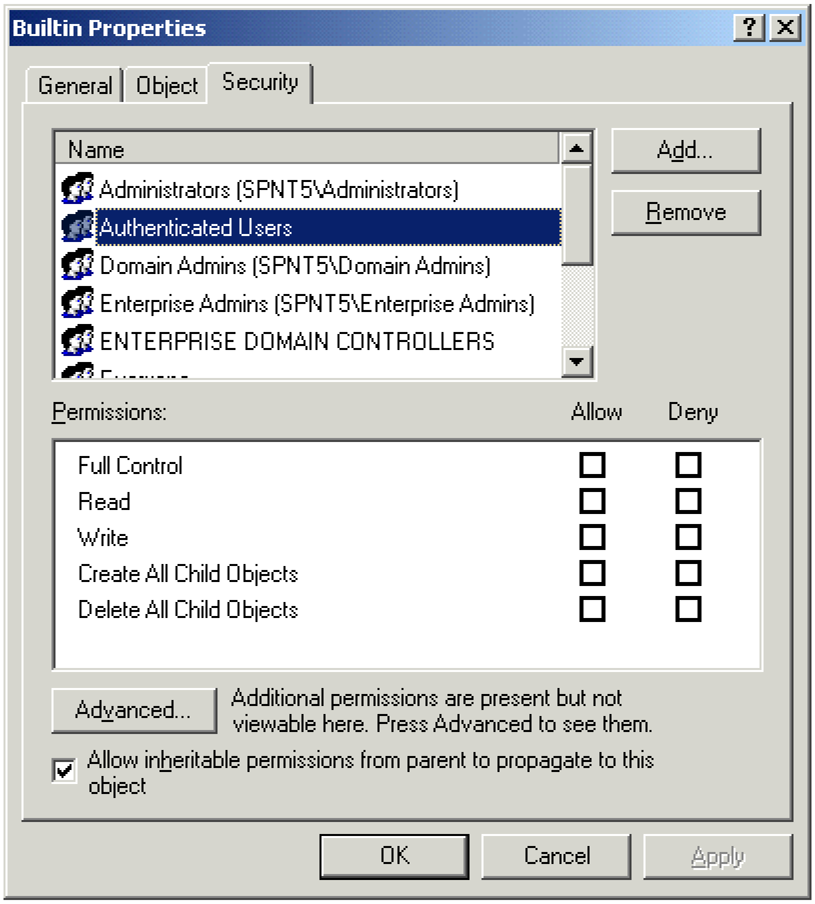
## *6.Setting Rights*

After the groups have been created, rights need to be set on each OU to properly restrict the ability to see other users and organizations. In short, users should be able to see only other users in his or her OU. Domain administrators and related groups should be able to see all users in all organizations so that they can be sufficiently managed and maintained. Once these permissions have been set on the directory then Exchange respects them and limits the amount of data that is returned when using the Address Book, searching for other users, etc. So it serves the dual purpose of also creating your GAL.

> **NOTE:** There is a very important exception to this rule. Users that access e-mail via the Microsoft Outlook® Web Access (OWA) client do not have the per-user rights for Active Directory applied to directory queries. This effectively allows them to see ALL users in the Active Directory directory service irrespective of the ACLs that have been assigned. To control this, there is an attribute that was put in place to control the scope of searches that OWA performs, but it is not exposed in the MMC admin. To close this security hole, you need to set the attribute *msExchQueryBaseDN* to point to the OU for the user's virtual organization (or Address List if you use them) to scope the search. This needs to be set on each user that will be using OWA. A tool like LDP or a custom CDOEXM script can be used to set this attribute.

Setting up the rights is a two-step process. The first step is to remove the rights that exist by default on all existing and new OUs. This can be accomplished by removing all rights for Authenticated Users on each default container (i.e. everything except for the OUs that were created for each virtual organization). Do the following to remove the default rights:

1. Open the **Active Directory Users and Computers** snap-in.
2. Select **View…Advanced Features** from the menu. This is required to see the security settings on each container.
3. For each container, right-click on the container and select **Properties** from the menu. This brings up a properties dialog box with three tabs.
4. Click on the **Security** tab. Listed on it are all the groups that have access rights to the container. Find the entry for **Authenticated Users**.



Name

- Administrators (SPNT5\Administrators)
- Authenticated Users
- Domain Admins (SPNT5\Domain Admins)
- Enterprise Admins (SPNT5\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | □ | □ |
| Write | □ | □ |
| Create All Child Objects | □ | □ |
| Delete All Child Objects | □ | □ |

Additional permissions are present but not viewable here. Press Advanced to see them.

☑ Allow inheritable permissions from parent to propagate to this object

5. Deselect all the rights for the **Authenticated Users** group. DO NOT change the rights for the **Domain Admins, Exchange Admins** or **Enterprise Admins** groups. The **Everyone** group may also be in there; if so, remove all rights for it also.

   **NOTE:** Make sure that you just deselect the rights, and do not choose **Deny** rights. Doing so will prevent all users from gaining access until the **Deny** setting is changed.

6. Click **OK** to save the settings. Repeat for every default container in the domain.

Now that all the default rights have been removed from the built in containers, users in each virtual organization will not be able to see any of the objects that live within them. Domain Admins, Exchange Admins, and Enterprise Admins however, can still see all objects in the directory. The next step is to further refine the rights so that OU members can only see other members of their own OU. Right now, any OU member can see any other OU member. To set the final set of permissions, do the following (these instructions assume that the Users and Computers snap-in is still open; if not follow steps 1 and 2 above):

1. Right-click on each OU that was created and select **Properties** from the menu. A dialog box with five tabs appears.
2. Select the **Security** tab.
3. Deselect all view rights for the **Authenticated Users** group. This is the same process that was done to the built in containers in the previous part of this section.
4. Click **Add** to bring up the list of users and groups in Active Directory. Find the name of the global group created for the OU with which you are working and click **OK** to add it to the list of security principals for the OU.

5. Verify that the group added in step 4 was given **Read** rights; if it wasn't it, add it now.
6. Click **OK** to apply the changes and dismiss the dialog box. Repeat these steps for each virtual organization OU.

Once these steps have been completed, the permissions portion of configuration is complete. If you were to log off and log on as a member of one of the OUs and set ACLs on an object, the list of objects that would show up in the dialog box would only include other objects in that user's home OU.

The remaining steps implement the security that has been created thus far into Exchange.

## *7.Domain Setup*

For Exchange to understand that messages coming in need to be routed as internal recipients even when the e-mail domain name doesn't match the Windows domain name, you need to create recipient policies for each domain name. When adding the recipient policy, you can make the determination about whether the Exchange organization should be authoritative for the domain that is being added. In most cases, that option should be selected. You can do so by simply checking the authoritative box on the recipient policy. Add the policy by doing the following:

1. Open the Exchange **System Manager** tool.
2. Expand the **Recipients** folder and click **Recipient Policies** in the left pane.
3. Right-click on **Recipient Policies** and select **New…Recipient Policy** from the menu.
4. Type in a name for the recipient policy in the *Name* edit box.
5. Click **Modify**. This brings up the **Find Exchange Recipients** dialog box where you can create a filter for users to which the policy will apply.
6. Select the **Advanced** tab.
7. Create a filter criterion for group membership. Click **Field**, select **User** then select **Group Membership**. Set the criteria to be **Is (exactly***)* the name of the OU group for which you are creating the policy and click **Find Now**.

   Entering the correct group name may not be completely intuitive at first. It only works if you use the fully qualified LDAP name. For example,

   *CN=All Contoso Users,OU=Contoso,DC=spnt5,DC=com*

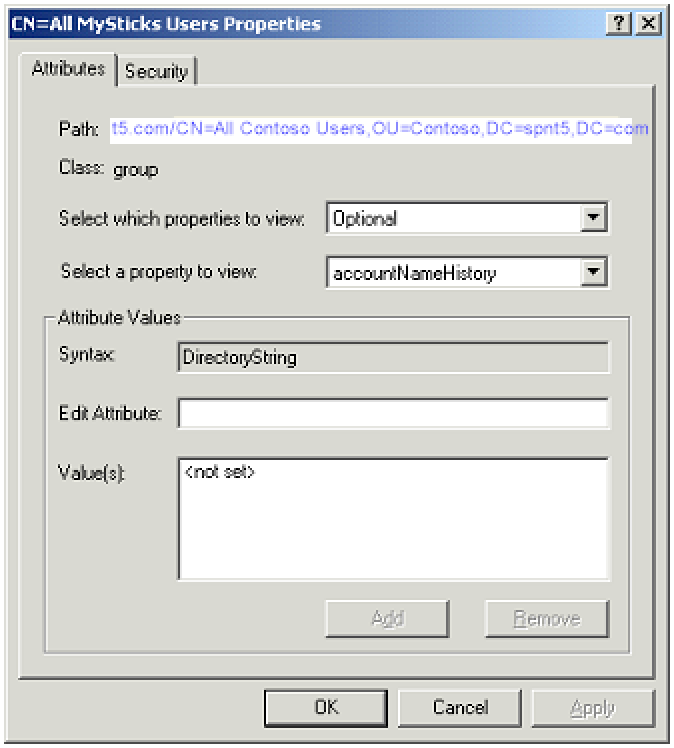
   If you are not sure what the correct name is the easiest way to find it is with ADSI Edit, which you can install with the Windows 2000 Resource Kit. It's included on the Windows 2000 CD ROM in the Support directory.

   To find the fully qualified name, open ADSI Edit and expand the Domain NC (naming context) tree. Under that, expand the tree for your domain. Underneath it you will see a list of all the containers and OU's in the domain. Expand the OU to get a list of all the users and groups within it. Right-click the group name and select **Properties** from the menu to bring up the properties dialog box.

   At the top of the dialog box is a **Path:** field that contains the fully qualified name. You need to capture the entire string ***after*** the server name. For example, in the *All Contoso* sample above, the path in ADSI Edit looks like this:

   LDAP://sp2000.spnt5.com/CN=All Contoso Users,OU=Contoso,DC=spnt5,DC=com

   You just need to click in the field and drag all the way to the right, beginning after *LDAP://sp2000.spnt5.com/*. The remainder is what needs to be input in the **Find** dialog box. Another point to remember is that the criteria of **Is (exactly)** is misleading in this case. A user can belong to multiple groups, and he will have a multivalued value for his **memberOf** property. **Is (exactly)** will still find the match as long as he has one complete group membership string that matches the entry in the **Find** dialog box.



Path: t5.com/CN=All Contoso Users,OU=Contoso,DC=spnt5,DC=com

Class: group

Select which properties to view: Optional

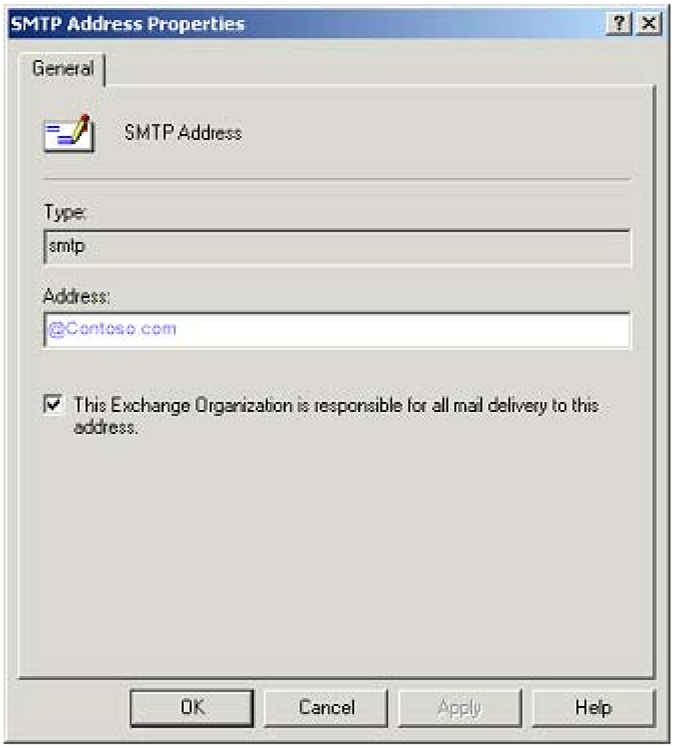
Select a property to view: accountNameHistory

Syntax: DirectoryString

Edit Attribute:

Value(s): <not set>

8. Click **OK** on the search dialog box when it is returning the results you expect. This returns focus to the policy **Properties** dialog box.
9. Click **Apply**. This saves the policy, which is required before you can start adding additional domain addresses to it.
10. Select the **E-Mail Addresses** tab.
11. Click **New**.
12. Click **SMTP Address** in the **E-mail address type:** list box, and click **OK**. This brings up the **SMTP Address Properties** dialog box where you can type in the e-mail domain information for the domains for which Exchange should route messages.
13. Type in the domain name info (i.e. @Contoso.com). Leave the **This Exchange Organization is responsible for all mail delivery to this address** checkbox selected (it is by default).



Type:
smtp

Address:
@Contoso.com

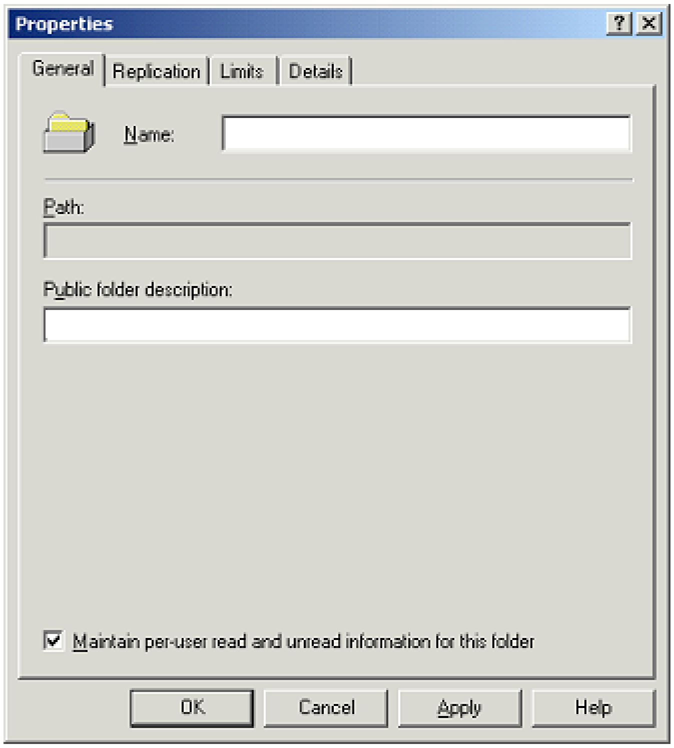
☑ This Exchange Organization is responsible for all mail delivery to this address.

14. Click **OK** to save the new address entry.
15. Click the new entry in the **Generation Rules** list box and check the box next to it.
16. Click **Set As Primary** on the dialog box, then click **OK** to save changes.  A dialog box appears asking if it is okay to update all corresponding e-mail addresses to use the new address.
17. Click **Yes** to accept.  This will assign the new domain e-mail address to all the users in the OU's global group.

## *8.Setting Public Folder Virtual Roots*

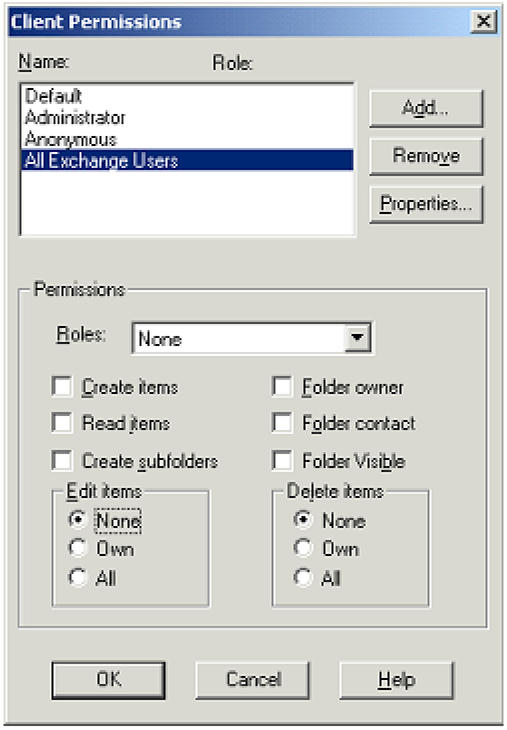
To complete the set of tools available for users, a Public Folder root will likely need to be established for each virtual organization.  The same set of principals that were used in configuring the other elements of Exchange should be used here – each virtual organization should only "see" one public folder root, and within that root they should have exclusive domain to control it as if they were the only organization in Exchange.  To accomplish that, a public folder needs to be created for each virtual organization that is at a peer level to the public folder "root" for every other virtual org.  To configure the psuedo public folder root do the following:

1. Open the Exchange System Administrator.
2. Expand down to the **Public Folders** node.
3. Right-click on the **Public Folders** node and select **New…Public Folder** from the menu.
4. Type in a name in the **Name** edit box that will make the folder easily distinguishable as the root for that virtual organization.



☑ Maintain per-user read and unread information for this folder

5. Click **OK** to create the folder. The dialog box will close and the folder is created. Next, permissions need to be set on the folder to limit its visibility to only members of the virtual organization and the administration teams for Windows 2000 and/or Exchange 2000.
6. Go to the System Administrator on the folder that was just created and select **Properties** from the menu.
7. Select the **Permissions** tab. The first set of rights to be set is client rights.
8. Select **Client Permissions….**
9. Click **Add** and select a) the global group for the OU and b) the master group of all OU global groups that was described in the section on creating groups and users. Click **OK** to close the GAL dialog box and add the groups to the permissions list.
10. Select the OU global group in the permission list. Make sure that at a minimum rights have been given to that group for **Folder Visible** and **Read Items**.
11. Click on the master group in the permission list. Deselect ALL the rights for this group.



**Client Permissions**

Name: Role:

- Default
- Administrator
- Anonymous
- All Exchange Users

Permissions

Roles: None

☐ Create items ☐ Folder owner
☐ Read items ☐ Folder contact
☐ Create subfolders ☐ Folder Visible

Edit items: ● None ○ Own ○ All

Delete items: ● None ○ Own ○ All

By setting the rights in this manner, it will prevent users from all other virtual organizations from seeing this public folder psuedo root, yet still allow users in the OU's global group to see and work with it as if it were the only public folder in the tree. Of course, additional folders can be created beneath this folder to create the "virtual tree" for the virtual org.

12. Click **OK** to save changes to the client permissions and close the dialog box.
13. Click **Directory Rights….** Permissions will be set in here to eliminate the ability for non-Exchange users to see the public folders in the directory, unless they have administrative privileges for Windows or Exchange.
14. Uncheck the **Allow inheritable permissions…** check box. This is necessary to modify the directory-related permissions on the object. When the dialog box appears after deselecting the box, click **Copy**.
15. Click **Authenticated Users** group in the list of security principals for this object.
16. Click **Remove**. This eliminates the default rights of all users to see the object in the directory. Also, by default though, Windows and Exchange administrators do have the right to see the object.
17. Click **OK** to save changes.
18. Click **OK** again for the folder properties dialog box to save the entire permissions configuration that was done.

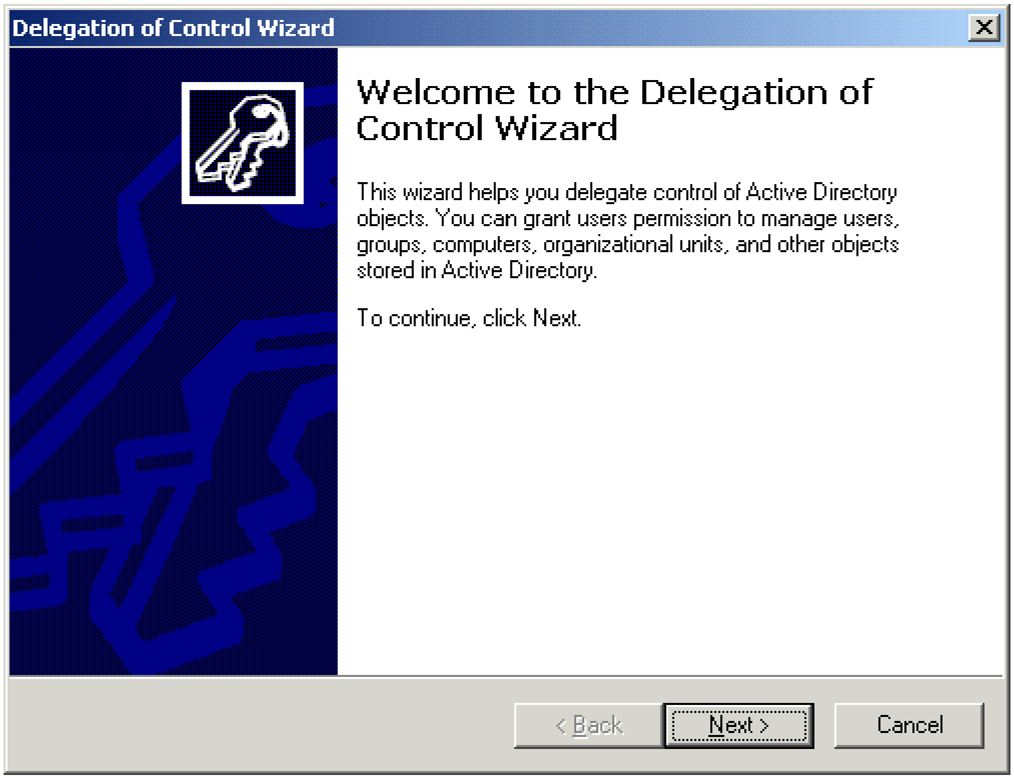
The "rights configured" is now complete. In addition, setting rights below each of these virtual folder roots is now much easier, because the **Everyone** group can be used for rights assignment if desired. The *Everyone* group can be used for folders below the virtual root because users in other OUs can't see the root to begin with, so setting rights for *Everyone* below the virtual root means that they will just be applied to those users that can see the root folder. This means that it's relatively easy to set up a hierarchy of folders for the virtual organization in which some are read-only, some are read/write, and others can be create/read/write.

## 9.Administration Delegation

It should be repeated that this step is also **optional**. By doing the steps in this section, you will grant administrative rights to certain end users in the organization to perform administrative tasks. This should only be permitted if it is a business requirement for one or more members of the virtual organization to be able to administer the other users in his or her virtual org. Following these steps will give the user(s) rights in the directory itself and in Platinum for things such as creating and deleting users, mailboxes, groups, setting rights on a per-mailbox basis, etc. If your business model does not require that level of delegation then you should not perform the steps in this section.

To delegate administrative rights for the virtual organization's **entire** OU to an OU member, do the following:

1. Open the **Active Directory Users and Computers** snap-in.
2. Select the OU for the virtual organization for which you want to set up delegated rights.
3. Select the **Action** menu, then **Delegate Control…** from there. The Active Directory Delegation Wizard appears.



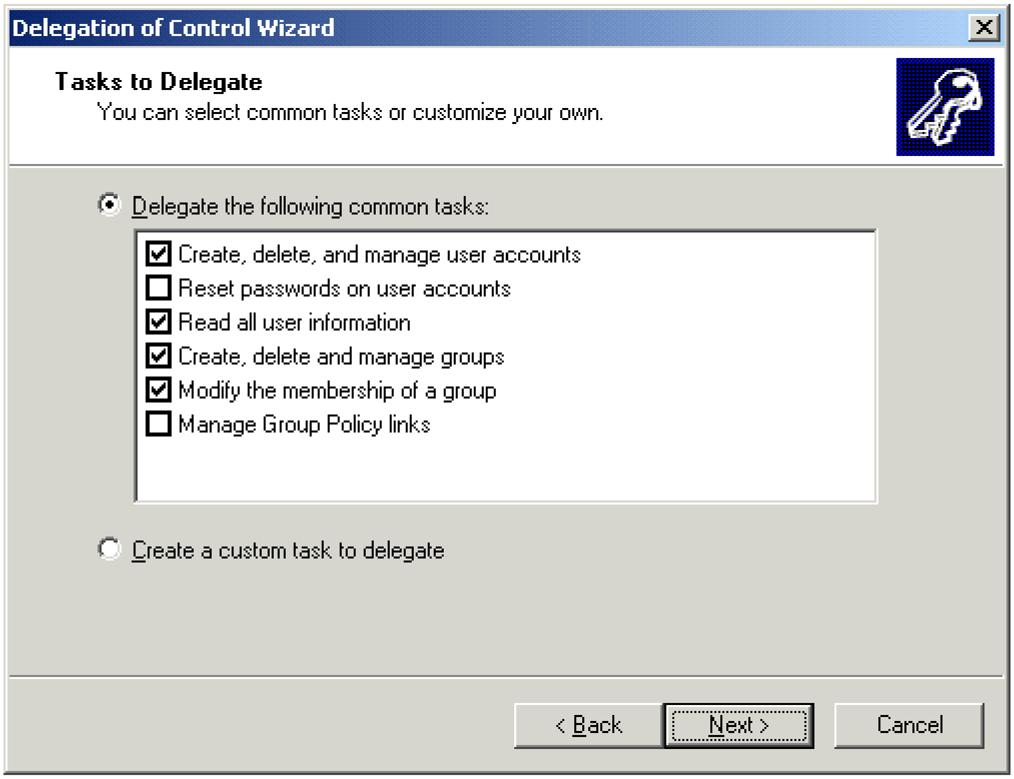
Delegation of Control Wizard

Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory.

To continue, click Next.

4. Using the wizard, select the user(s) or group(s) that you want to have administrative control over the OU, including the ability to add and delete mailboxes, change mailbox settings, etc. Click **Next** to continue. On the **Tasks to Delegate** page, the option to *D***elegate the following common tasks** is selected by default. Use this option to select rights at a reasonably high level. If you want or need to select very granular rights, then select **Create a custom task to delegate** option; following the wizard you can select individual properties to which rights can be assigned.
5. Assuming that the default delegation option was selected (see #4 for a more detailed explanation), select the following rights:
   a. Create, delete, and manage user accounts
   b. Read all user information
   c. Create, delete, and manage groups (such as Distribution Lists)
   d. Modify the membership of a group



**Tasks to Delegate**

You can select common tasks or customize your own.

● Delegate the following common tasks:

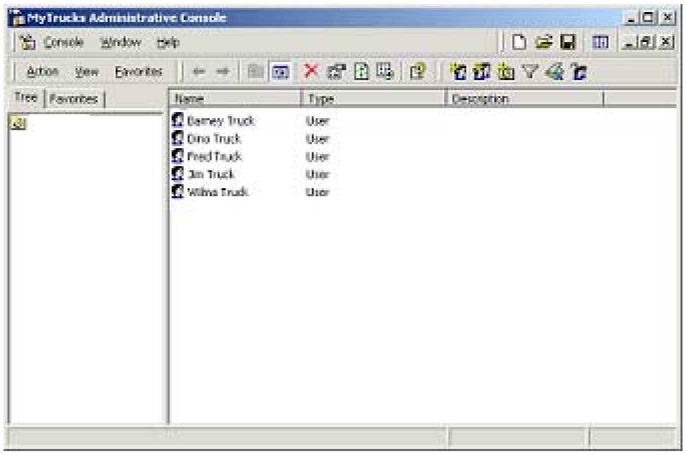
- ☑ Create, delete, and manage user accounts
- ☐ Reset passwords on user accounts
- ☑ Read all user information
- ☑ Create, delete and manage groups
- ☑ Modify the membership of a group
- ☐ Manage Group Policy links

○ Create a custom task to delegate

6. Click **Next** then **Finish** to complete the wizard. The rights for management have now been delegated.

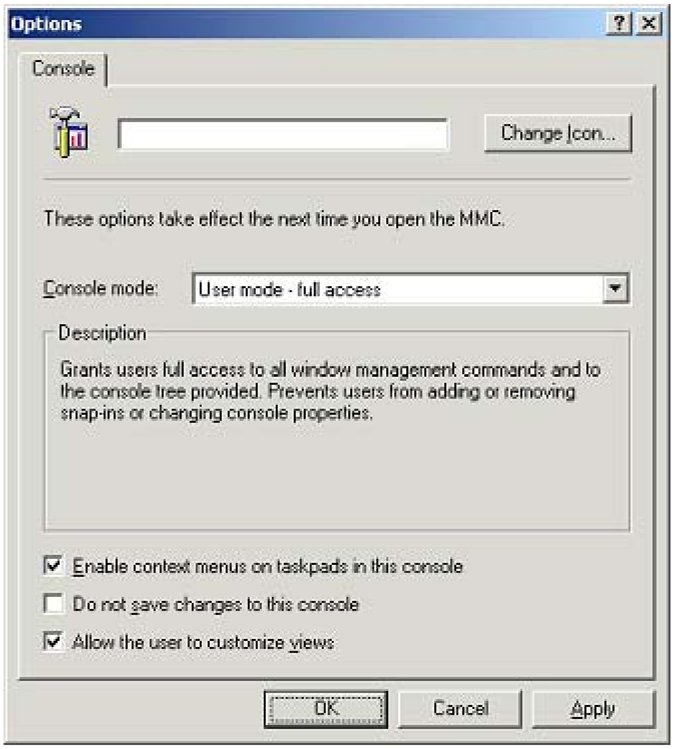
You may also wish to create a custom **Users and Computers** snap-in for the individuals that have delegated administrative control. It provides a view of only the OU to which the rights have been delegated. To create the custom snap-in, do the following:

1. Click **Start**, **Run** and type "**MMC**" in the edit box, and press **Enter**. This starts an empty MMC shell.
2. Click on the **Console** menu, then **Add/Remove Snap-ins** menu. This brings up a dialog box of snap-ins that have been added for this MMC file.
3. Click **Add** to add a new snap-in.
4. Double-click on the **Active Directory Users and Computers** snap-in to add it to this MMC.
5. Click **Close** to dismiss the list of snap-ins dialog box, then click **OK** to close the current snap-in list dialog box and return to the MMC. The Users and Computers snap-in should be displayed in the MMC at this point.
6. Click on the OU for the virtual organization.
7. Select the **Action** menu, then the **New Window From Here** menu. You now have two windows open in the MMC – one with the entire domain and one with only the OU. You need to close the window for the entire domain.
8. Select the **Window** menu then select the first item in the window list – it should start with **Console Root\Active Directory Users and Computers**. That should bring up the first window again with all of the domain information in it.
9. Close the window only, not the entire console. This should leave a console with only one window in it – the view of the OU. Now rights need to be set so that the MMC that has been created can't be seriously modified or damaged.



| Name | Type | Description |
|---|---|---|
| Barney Truck | User | |
| Dino Truck | User | |
| Fred Truck | User | |
| Jim Truck | User | |
| Wilma Truck | User | |

10. Select **Console** then **Options** from the menu. A dialog box appears with options for the console you're creating. The only option that really needs to be set is to change the **Console Mode** to **User Mode – Full Access**. This should allow the user to customize the MMC file without breaking it.



These options take effect the next time you open the MMC.

Console mode: User mode - full access

Description

Grants users full access to all window management commands and to the console tree provided. Prevents users from adding or removing snap-ins or changing console properties.

☑ Enable context menus on taskpads in this console

☐ Do not save changes to this console

☑ Allow the user to customize views

11. Click **OK** to save the console settings.
12. Click **Console** then **Save** from the menu and save the MMC to a file. Once the file has been saved, you can e-mail it to anyone that needs to administer the OU for the virtual organization. They just need to open the MMC file and it will automatically display information for the OU to which they've been delegated rights.

Those are all the steps required to set up rudimentary administrative delegation for the virtual organizations. That also completes the process for setting up hosting of a virtual organization. Ideally you would also be able to delegate rights to administer one information store or database, recipient policies, etc., but the granularity required in Exchange to permit that is not present yet, or at least not documented.

**Note:** Don’t forget to vote this topic in certsbraindumps.com forum.