An Administrators Viewpoint: Configuring DCOM for MFCOM

Nick Holmquist

http://nickholmquist.com

Overview

The purpose of this document is to be a basic guide to configuring DCOM permissions for use with MFCOM. While many of the steps in this document are basic in nature I decided to illustrate each step in case there are those who are unfamiliar with certain aspects of the various pieces involved.

Using this document will help to configure MFCOM for use with not only Farm/Server administrators but it also gives a lot of flexibility for allowing certain users access to the power of MFCOM. With proper permissions you could allow basic users access to run MFCOM scripts to get information for their own sessions, etc.

The possibilities are endless!

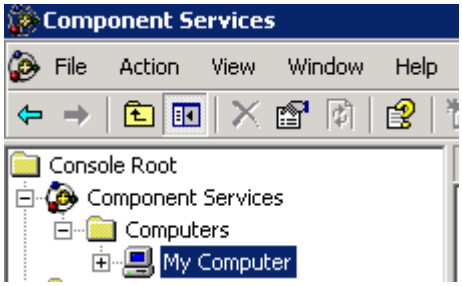
Windows 2003 XenApp Server - DCOM Configuration

The XenApp Servers (Presentation, Metaframe, whatever you want to call it) in your farm must be configured to allow users certain permissions to be able to connect to the COM server both locally and remotely. By default, Administrators have enough permissions to do typically everything they need to do. But what if you wanted to grant non-server administrators access to run certain MFCOM scripts? Well with the configuration we will create you can do just that and make it dynamic enough that you do not have to modify DCOM permissions on each server in the future.

The problem with DCOM permissions across multiple servers is that there is not really a good way to mass modify them all at once. There are ways to accomplish it, it just takes a bit of work. For now we will focus on a single server so you can see what the basic configuration looks like.

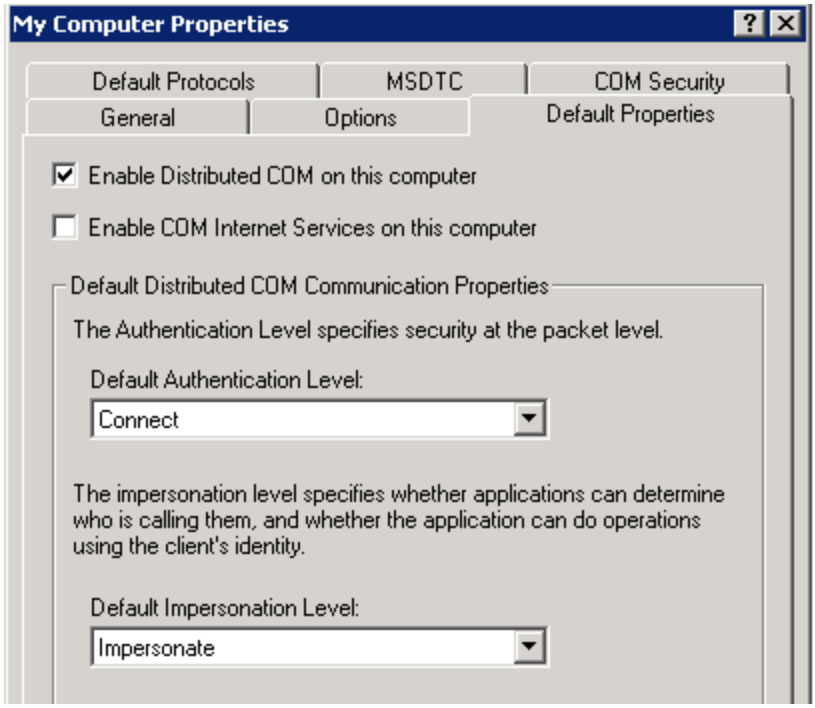
We really have two options in terms of how broad we can configure DCOM on the servers. You can configure the default permissions globally so that it affects most of the DCOM Applications or we can define permissions specifically on the MFCOM DCOM Application. Since it is best to keep a higher level of security whenever possible we will do the latter.

- Log into a XenApp server as an **Administrator**.
- Run **DCOMCNFG.EXE**
- Select **Component Services**
- Expand **Component Services** >> **Computers**

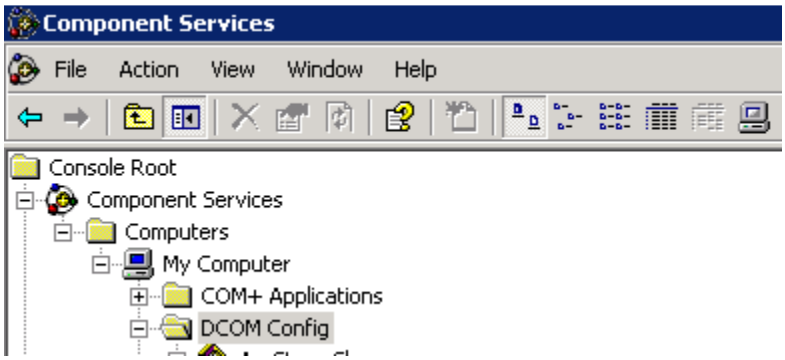


- Right click on **My Computer** and select **Properties**.
- Click the **Default Properties** tab.
- Ensure that the **Enable Distributed COM on this computer** option is checked.
- Under the **Default Impersonation Level** select **Impersonate.**

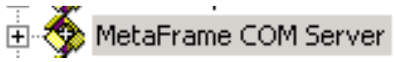
*This is extremely important because DCOM will 'Impersonate' the user whom is making the call to the MFCOM DCOM Application.



- Click **OK** to save the changes.
- Expand **My Computer**
- Expand **DCOM Config**



- This will show a list of DCOM Applications that run on this server. We need to find an item listed as **MetaFrame COM Server**

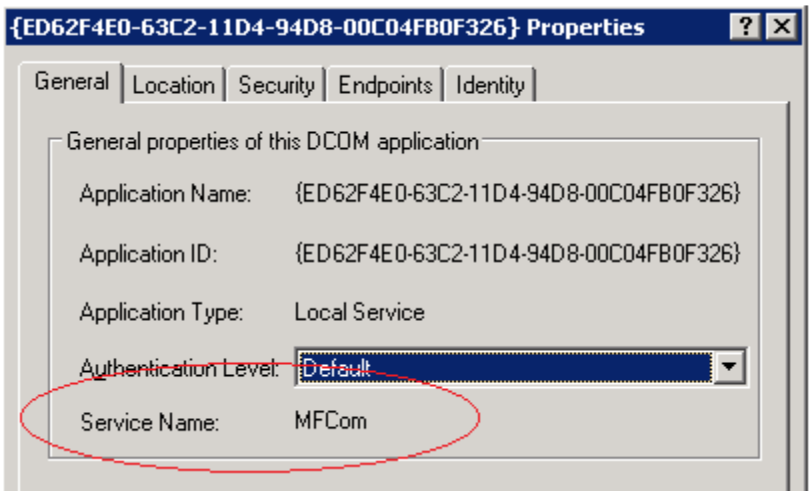


Don't panic if you don't see this item as on some servers it does not seem to register the name properly. Scroll down through the list (typically at the very bottom) until you find an item that begins with **ED62.** (*Remember this as you will may be looking at this quite often).

It does not matter if you found **MetaFrame COM Server** or if your server shows it as an **App ID**.

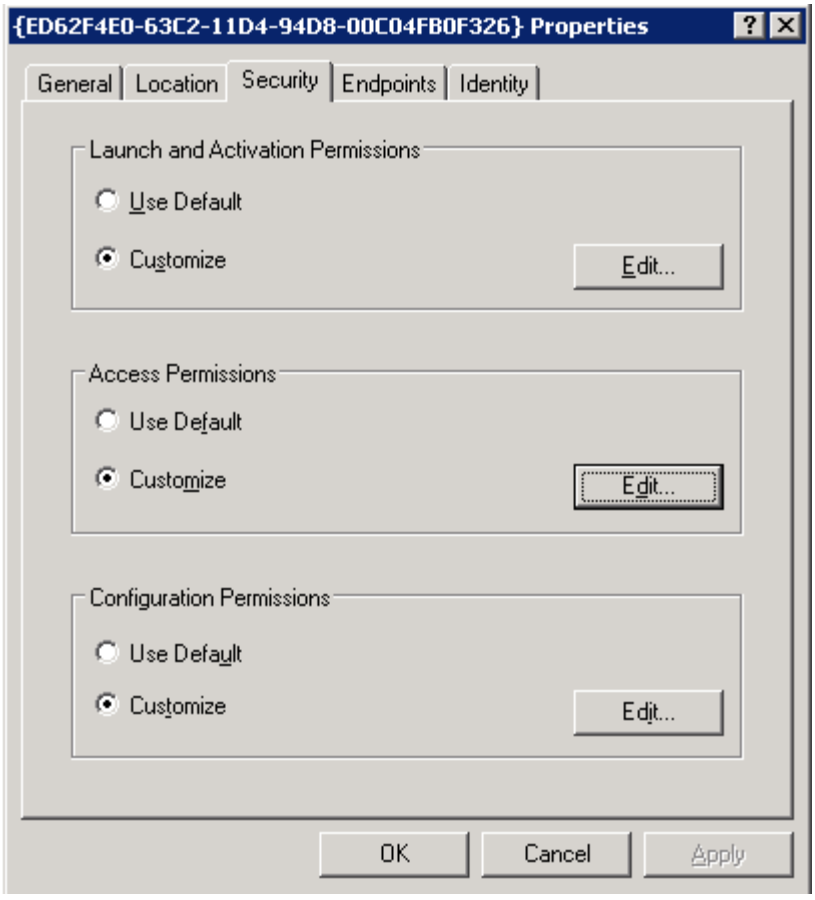
Right click on the item and select **Properties**.

- On the **General** tab you should see MFCOM listed as the service name:



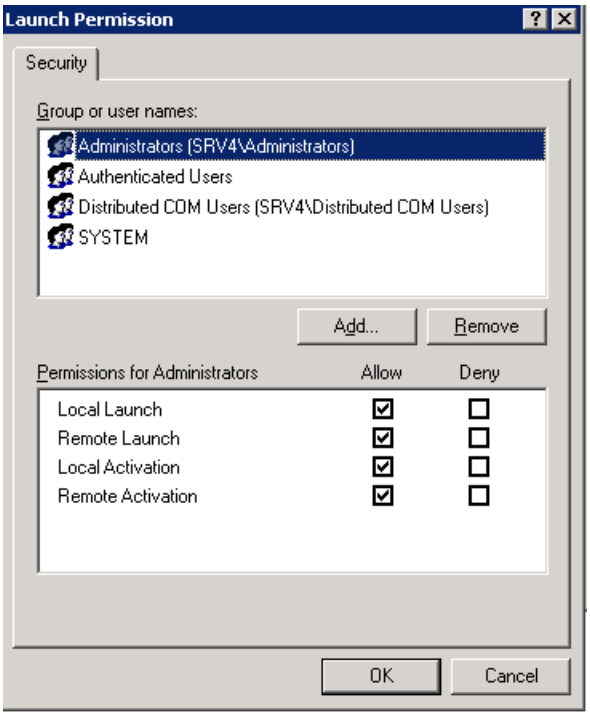
*If not then you are probably not looking at the properties for the MFCOM DCOM Application.

- Click the **Security** tab.



- Under **Launch and Activiation Permissions** section click the Customize Radio button.
- Click **Edit**

*The permissions my/may not be correct. To be sure, configure it as the following:



User	Local Launch	Remote Launch	Local Activation	Remote Activation
Administrator	•	•	•	•
Authenticated Users	•		•	
Distributed COM Users	•	•	•	•
SYSTEM	•	•	•	•

- If any of the accounts are not present simply click **Add**
  1. Select **Advanced**
  2. Click **Location**
  3. Scroll to the top and select the **local server name**
  4. Click **OK**
  5. Click **Find Now**
  6. This will show a list of local accounts.
  7. Add any account that was missing and set the proper permissions.
- Once the permissions are set click **OK** and you will be back at the **Security** tab for the MFCOM DCOM Application properties.
- Under the **Access Permissions** click **Customize**
- Click **Edit**

- Add the same local accounts as you did for the Launch permissions. This time, give them the following permissions:

User	Local Access	Remote Access
Administrator	●	●
Authenticated Users	●	●
Distributed COM Users	●	●
SYSTEM	●	●

- Click **OK**
- Click **OK** again to close the Properties for the MFCOM DCOM Application.

The configuration of this server is complete.

Mass configuring DCOM Permissions for MFCOM

The previous step is quick to perform on a single server but what if you have hundreds that need to receive this configuration? There are local policies that allow you to configure the default permissions but this is not easy to mass modify and typically you want to stay away from local policies whenever possible. Not only that we are configuring permissions only on the MFCOM DCOM Application.

There is a registry key where this information is stored ina Binary format. Unfortunately Group Policy does not support custom ADM templates and binary values (There are 3rd party plugins that do). What we are going to do is export the registry key from the server we just configured and apply it to all of the servers in the farm.

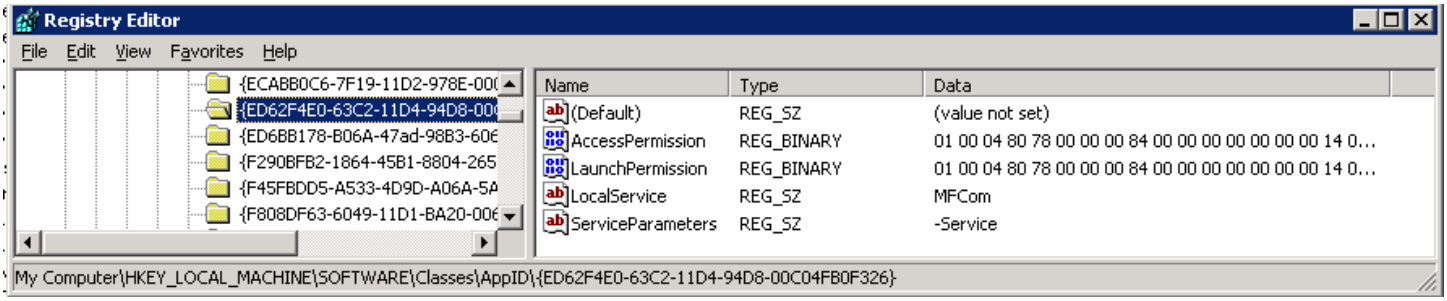
On the server we just configured:

- Oopen **regedit.exe**
- Navigate to the following key:

  X86: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{ED62F4E0-63C2-11D4-94D8-00C04FB0F326}

  X64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Classes\AppID\{ED62F4E0-63C2-11D4-94D8-00C04FB0F326}

  *The key for the x86 version will work as well on x64.



- Right click on the **{ED62F4E0-63C2-11D4-94D8-00C04FB0F326}** key and click **Export**
- Give it a file name and click **Save**
- Edit the .reg file that was just exported (Notepad works)
- Remove the following two lines:

  "LocalService"="MFCom"
  "ServiceParameters"="-Service"

- Save the file.
- We now have a registry file that should work across the board for our servers.

Note: Since the accounts we are granting permission to were OS created accounts, the SID's should not be different across servers. This essentially means the binary values should match. If you wish to confirm this, configure this locally on another server and then compare the exported registry files

Now that you have your registry file you can use whatever utility you wish to roll the change out to the remaining servers. Please keep in mind that since this is not a Group Policy setting you will need to ensure this change gets made on each new XenApp server that is placed into your environment.

Configuring MFCOM use for Non-Server Administrators

Domain Group Creation

Since we may want to create a few scripts/applications that might be ran by non-administrators we need to continue the configuration.

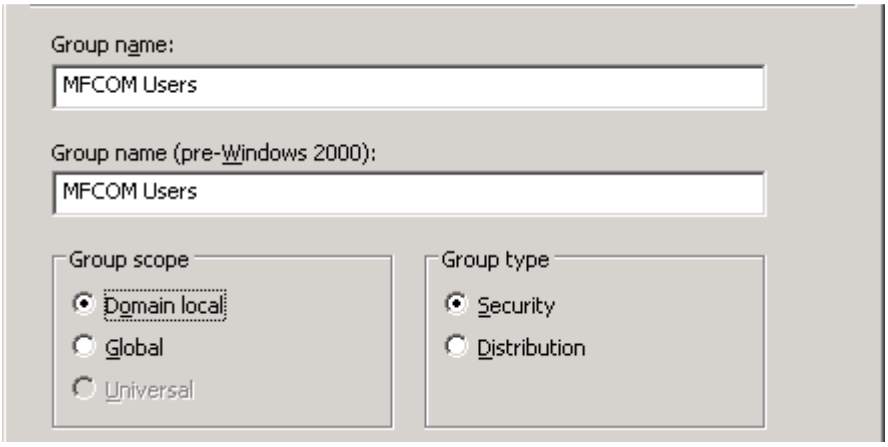
In the previous sections we added the local Distributed COM Users group to the DCOM permissions. This local group is created by Windows 2003 SP1/SP2 when the OS is installed. Windows 2003 SP1 is when Microsoft began changing the default DCOM permissions to tighten security. This would have basically broke a number of legacy applications so Microsoft added the Distributed COM Users group to help alleviate the problem.

We are going to use Group Policy to add additional groups/Users to the local Distributed COM Users group. If you do not use Group Policy you can always add the accounts manually or utilize a script to do so. GPO is simply the easiest way to ensure all servers have the same configuration.

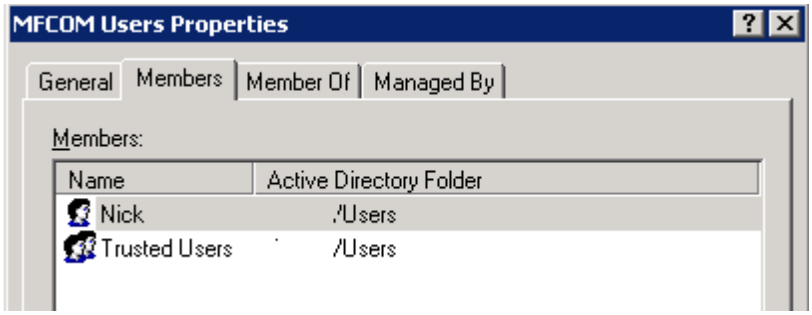
I highly recommend installing Group Policy Management Console. It makes managing/editing group policy objects so much easier.

Download GPMC at: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

- Open **Active Directory Users and Comupters**
- Connect to your domain (If you are not a domain admin you will obviously have to have the following steps performed for you)
- Create a new group. You can name it whatever you wish.



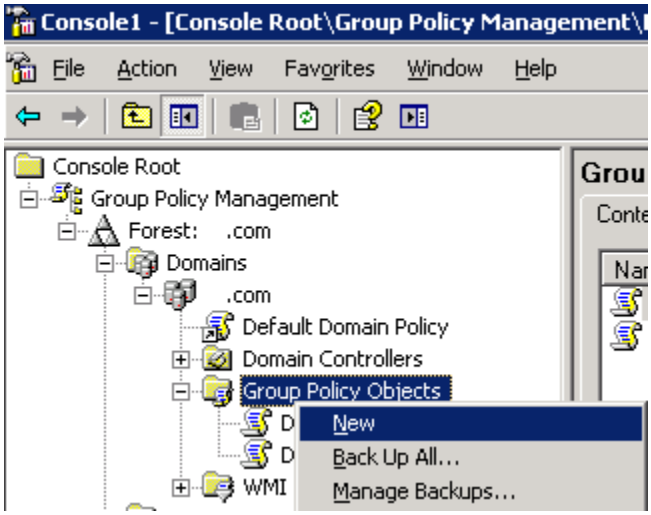
- Once the group is created you can then add the users or nest other groups within it. The purpose here is to have any user that will need MFCOM access as part of this group.



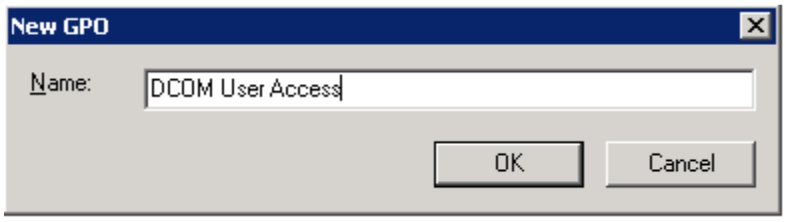
- Once we have our groups the way we need them we can proceed to creating a group policy object to roll out these permissions on all servers.

Creating Group Policy Object

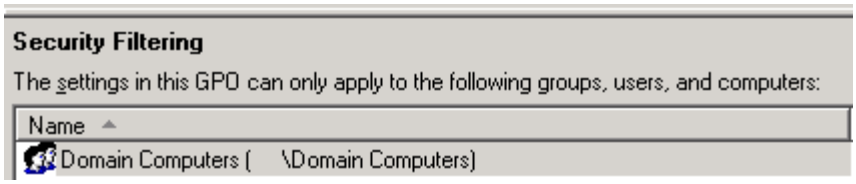
- Open the **Group Policy Management Console** (**GPMC)**
- Expand out the tree until you see the **Group Policy Objects** node
- Right click, select **New**



- Name the policy anything you wish and click **OK**

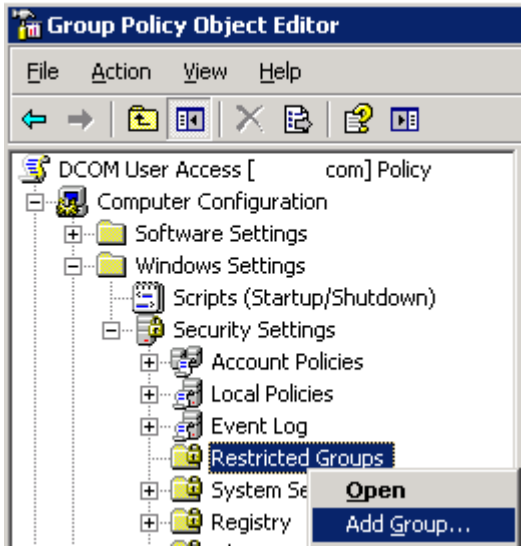


- The GPO will be created.
- Click the newly created object and the **Scope** window will open to the right.
- Under the **Security Filtering** section we want to make sure the policy applies to all computers.
- Click **Authenticated Users** and click **Remove**.
- Click **Add** and search your domain for the **Domain Computers** object and add it.



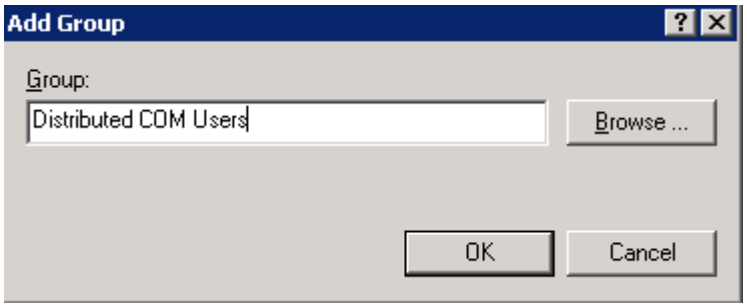
- Right click on the GPO to the left and click Edit
- Expand out the tree until you get to **Restricted Groups**.

Computer Configuration >> Windows Settings >> Security Settings >> Restricted Groups

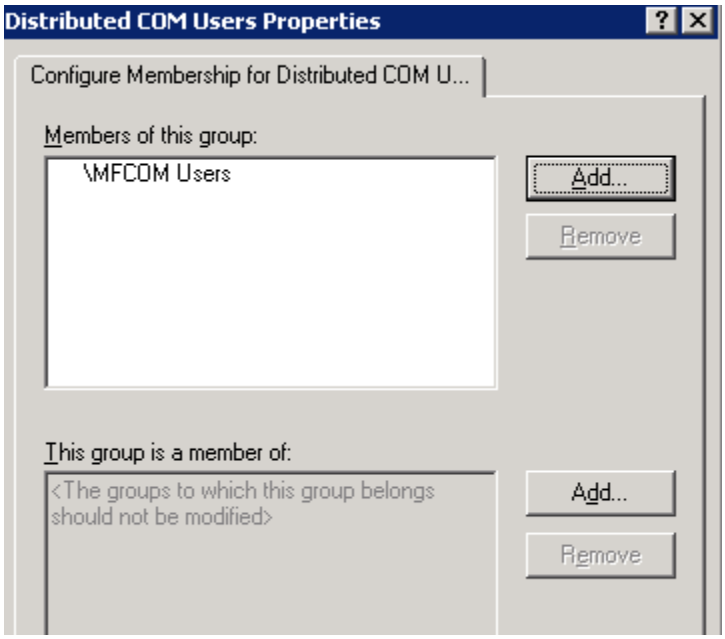


- Right click on **Restricted Groups** and click **Add Group**
- Enter **Distributed COM Users**

**Alternatively you can navigate to the machine you are on and select the group*



- Click **OK**.
- Under **Members of this group** click **Add**



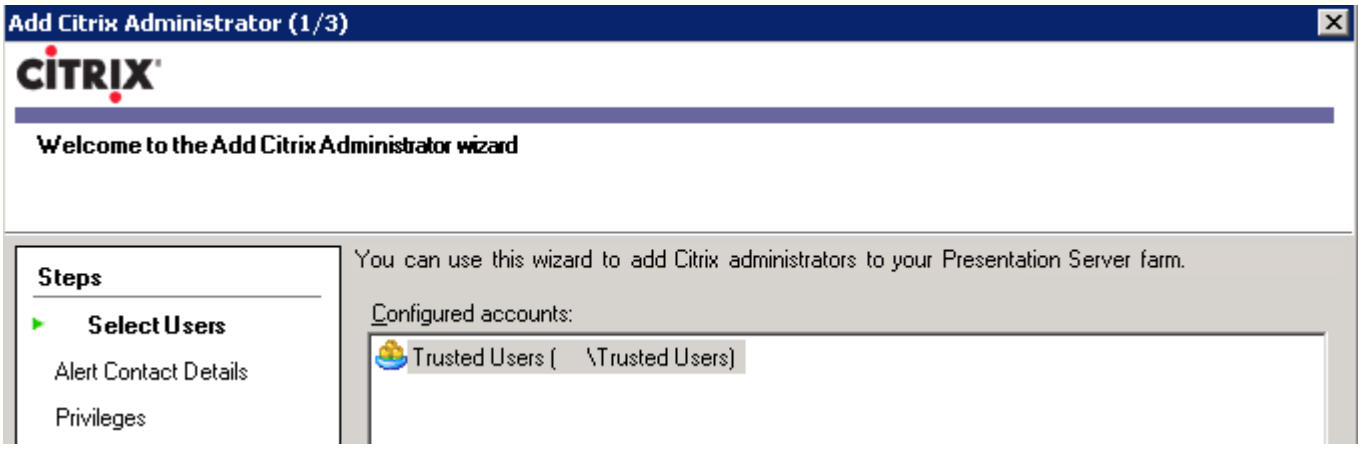
- Navigate through the domain and add the group that was created previously.
- Click **OK**
- Close the **Group Policy Object Editor**.

Group Policy configuration is complete unless you need to link the GPO to a different OU for specific servers, etc.

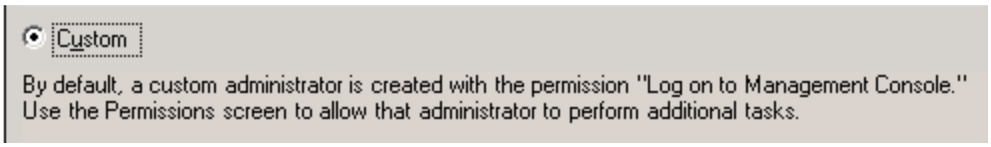
Farm Permissions

We will now configure our XenApp farm permissions to use our newly created group so that non-admin users can run scripts/applications utilizing MFCOM.

- Open the **Access Management Console** or **Citrix Management Console**
- Add an administrator using the group or user you added to the **MFCOM Users** group earlier.



- Assign what type of permissions you want to grant these users. Typically for those who are not full-fledged administrators you want to grant View only or **Custom** permissions.



*The permissions you will need to grant depend on the type of methods you will be using in your script or application. This is where you will have to experiment to give just enough access to what the user would need to do.

Client Configuration

Installing up the SDK

The SDK download and install is NOT needed if all you plan to do is run a script or two from XenApp servers. XenApp servers already have everything necessary to handle MFCOM scripts. As a matter of fact it is generally not a good idea to install the SDK on a XenApp server. If you are not interested in modifying the scripts to a great extent you can feel free to skip this section. For those who do, please read on.

- **Download the SDK**: Navigate to the Citrix CDN website to download the latest XenApp SDK.

  http://community.citrix.com/display/cdn/XenApp+SDK

- **Install the SDK**: Once you have the installer downloaded you can proceed to actually installing it on your client machine. Accept all defaults and the installation should finish quickly.

  **Again I must stress that it is best to install the SDK on a non XenApp server where you will perform your scripting/development so you don't run the risk of affecting a XenApp server.

Once the SDK is installed we need to register it to a XenApp server so that any calls to MFCOM via a script or application can be completed successfully.

- Open a command prompt and naviagte to: **C:\Program Files\Citrix\MPSSDK\utils**
- Run the following command: **mfreg** <*ServerName*>

  *<ServerName> to be replaced by a valid XenApp server

  *Run mfreg.exe by itself to get alist of switches if you are curious

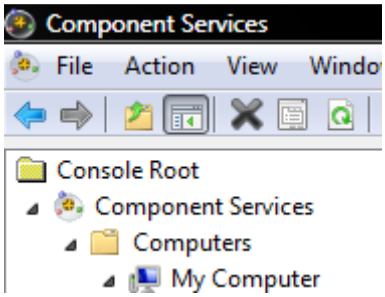
SDK Installation/Configuration is complete

DCOM Configuration

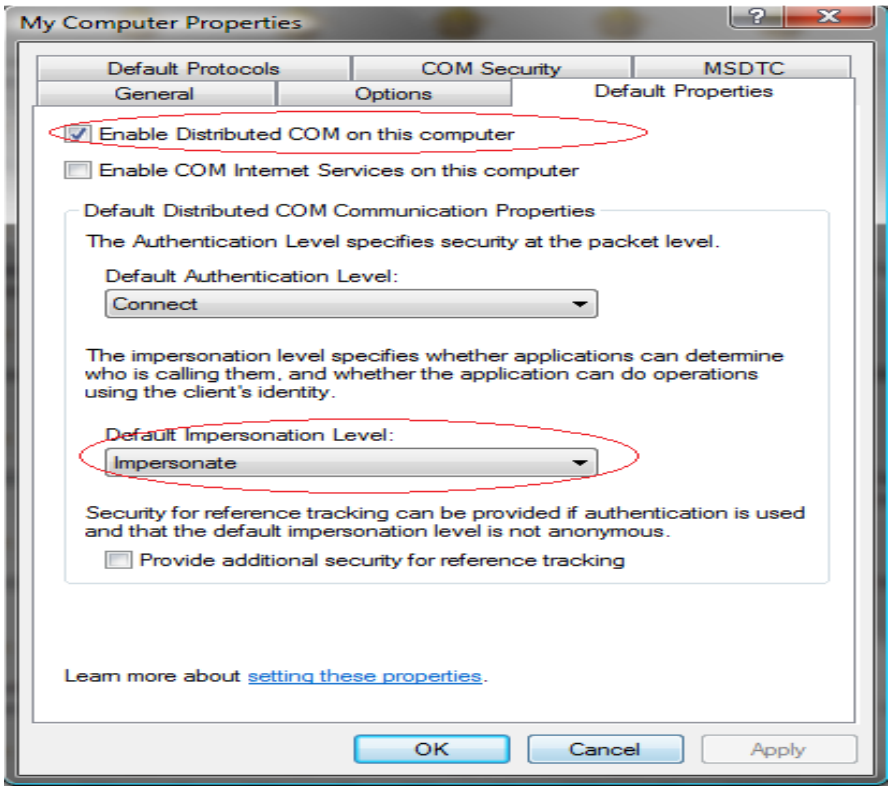
You are probably going to use Windows XP or Windows Vista as the client of choice to create your scripts or applications. The two are identical in their configuration of the SDK and DCOM. Keep in mind with Vista, User Access Control (UAC) may prompt when attempting to perform certain actions.

The process of configuring the client is the same as on the server except we will configure the permissions on My Computer instead of on the specific MFCOM DCOM Application. This is just easier since most of the time the client machine may need to connect to other DCOM Applications as well.

- Run **DCOMCNFG.EXE** on your client machine.
- Expand out the tree until you get to **My Computer**.

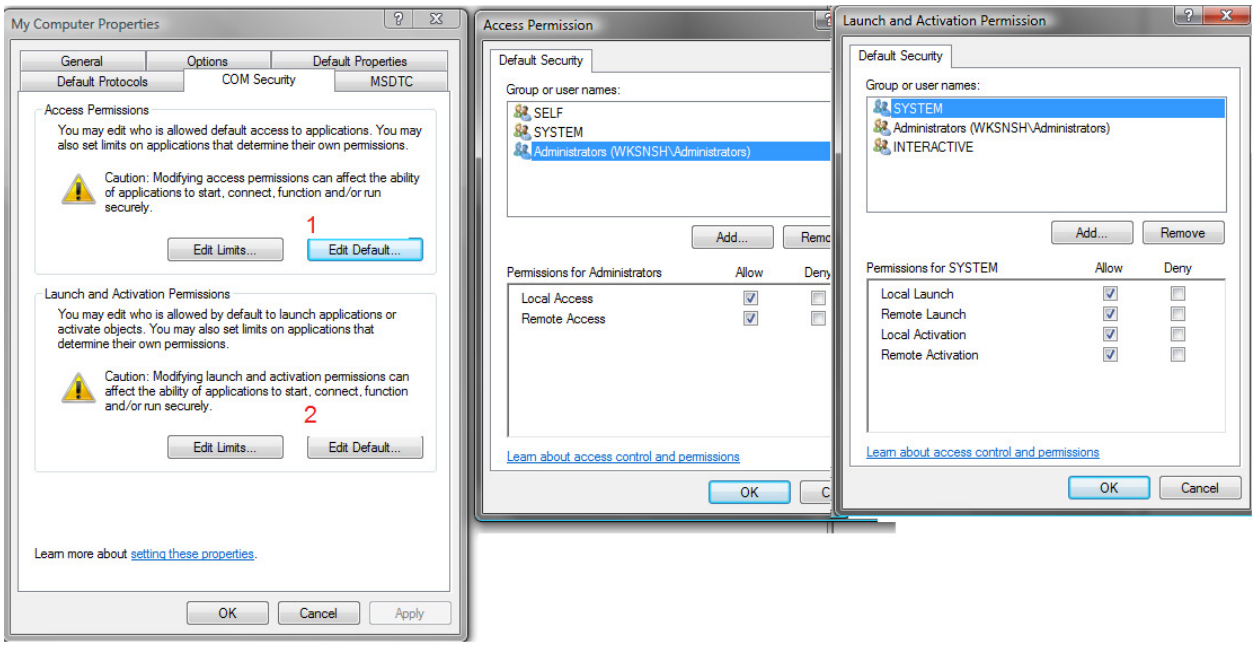


- Right click on **My Computer** and select **Properties**.



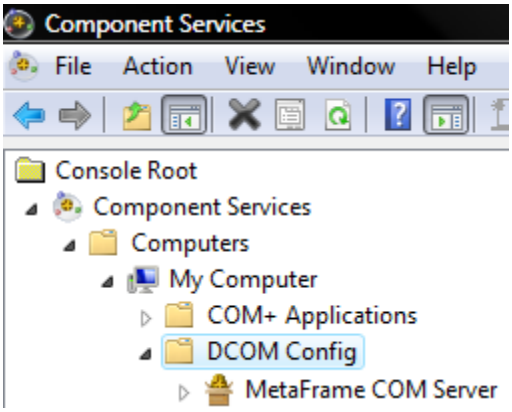
- Click the **Default Properties** tab. Make sure that the **Enable Distributed COM on this computer** option is checked.
- Under the **Default Impersonation Level** select **Impersonate**.

- Once you have the above set click on the **COM Security** tab.

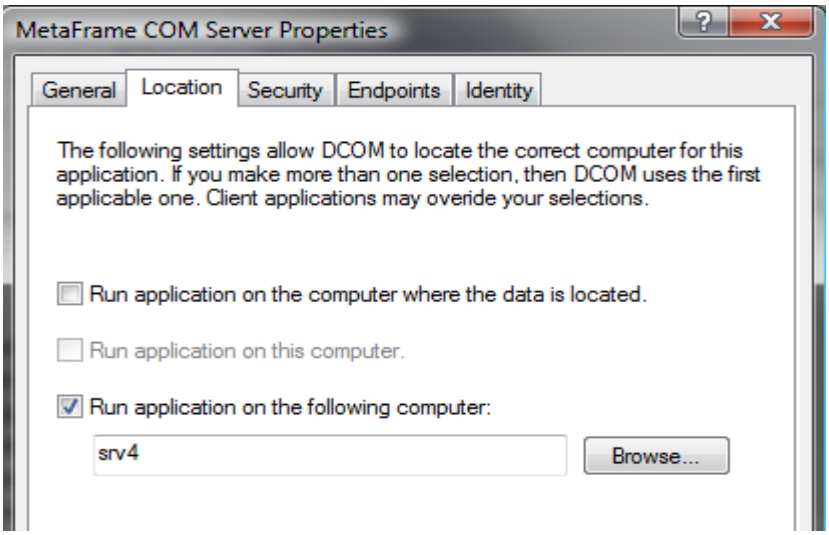


For most installations of XP or Vista your settings should be configured properly for utilizing DCOM. If not ,the above image gives a good guide as to how to configure it. If you are NOT an administrator on your client machine you will need to grant your user/group proper permissions. The best thing to do is grant the user running the script Allow across the board.

- When you have the permissions correct you can click OK all the way out of the My Computer properties.
- Expand the tree down until you get to **DCOM Config**.



- Once expanded you will see a large list of COM Servers. Scroll down until you see **MetaFrame COM Server**.
- Right click on this item and click **Properties**.
- Click the **Location** tab

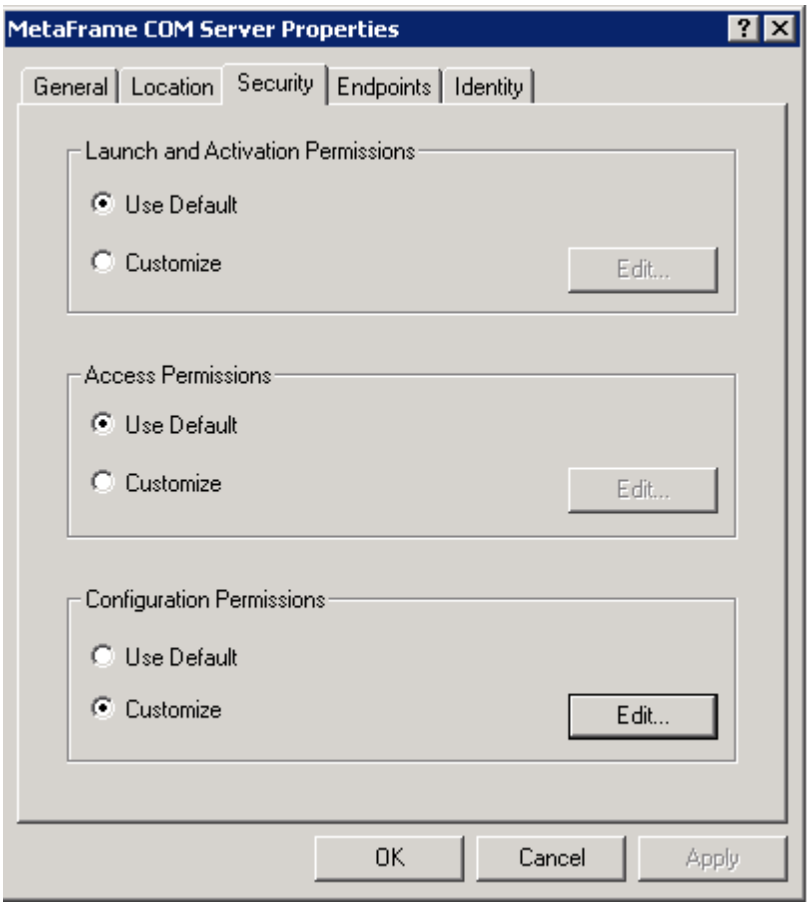


The server we used during the **mfreg** process in the previous section should appear here.

- Click the **Security** tab

You have two options, you can use the **Default settings** from **My Computer** (Those that we just set) or you can define your own specific permissions for this COM Server if you wanted to keep security a bit tighter.

For simplicity we will use the settings as shown below:



- Click **OK**.

The client permission configuration is done

Conclusion

Again I want to stress that this document is not meant to be all encompassing for DCOM or MFCOM. It is aimed at helping to get a handle on DCOM and MFCOM since that can be a pain point for a number of Administrators.

This document is clearly a work in progress and I welcome any feedback to enhance it's content.