3.2.0.3

**Measuresoft Development Ltd.**

**RTE OPC Server Manual**

**Version:4.7.6.13**

**measuresoft development limited**

**partnership court**

**the ramparts**

**dundalk**

**co. louth**

**ireland**

**tel + 353 42 933 2399**

**fax + 353 42 932 7187**

This document is the copyright of Measuresoft, and may not be modified, copied, or distributed in any form whatsoever without the prior permission of Measuresoft

**prepared for measuresoft by**

**Tuesday, October 08, 2013**

**© measuresoft development**

Table of Contents

This section is mandatory.

1. Introduction 3

2. Getting Started 3

2.1. The Registry Browser Options 3

2.2. The Registry Display Options 3

2.3. Server Machine DCOM Configuration 3

Application Configuration 3

Default Properties 3

Default Security 3

2.4. Configuring a Restricted DCOM Port Range DCOM 3

2.5. Register OPC Proxy 3

3. Advanced Configuration of DCOM (Distributed COM) to Connect an OPC client to an OPC Server on another Machine 3

DCOM Tutorial - Preface and Best Practices 3

3.1. DCOM Tutorial - Intro to the DCOMCNFG.EXE Utility 3

What is DCOM Config (aka "DCOMCnfg")? 3

So where is the DCOM Config Utility on my computer? 3

What does the DCOM Config Utility Look like? 3

Major parts of DCOM Config 3

How should I use DCOM Config? 3

Things to remember when using DCOM Config 3

3.2. OPC Client Computer Recommended Settings 3

Client Side DCOM Configuration Properties: Default Properties Tab 3

Client Side DCOM Configuration Properties: Default Security Tab 3

Client Side DCOM Configuration Properties: Default Security Tab - Default Access Permissions Dialog 3

Client Side DCOM Configuration Properties: Default Security Tab - Default Launch Permissions Dialog 3

Client Side DCOM Configuration Properties: Default Security Tab - Default Configuration Permissions Dialog 3

Client Side DCOM Configuration Properties: Default Protocols Tab 3

3.3. OPC Server Computer Recommended Settings 3

3.4. OPC Server Computer Recommended Settings - Step 1 3

DCOM Configuration Properties: Default Properties Tab 3

DCOM Configuration Properties: Default Security Tab 3

DCOM Configuration Properties: Default Security Tab - Default Access Permissions Dialog 3

DCOM Configuration Properties: Default Security Tab - Default Launch Permissions Dialog 3

DCOM Configuration Properties: Default Security Tab - Default Configuration Permissions Dialog 3

DCOM Configuration Properties: Default Protocols Tab 3

3.5. OPC Server Computer Recommended Settings - Step 2 3

Server Specific Properties: General Tab 3

Server Specific Properties: Location Tab 3

Server Specific Properties: Security Tab 3

Server Specific Properties: Identity Tab 3

Server Specific Properties: Endpoints Tab 3

3.6. OPC Server Computer Recommended Settings - Step 3 3

OPCEnum Properties: General Tab 3

OPCEnum Properties: Location Tab 3

OPCEnum Properties: Security Tab 3

OPCEnum Properties: Identity Tab 3

3.7. User Permissions Considerations when setting up a DCOM Connection between An OPC Client and OPC Server 3

Types of Permissions: 3

Users and Groups: 3

What's a Domain ? 3

Get in the Domain - if you can 3

No Domain - What do you do? 3

3.8. Configuring DCOM (Distributed COM) to Connect an OPC client to an OPC Server on another Machine NT/2000 Domain Trust Relationship Considerations 3

4. Configuration of DCOM (Distributed COM) to Connect an OPC client in a Workgroup to an OPC Server in another Domain 3

4.1. OPC Server Configuration 3

 Click ApplyDefault Security 3

 Default Security 3

4.2. OPC Client Configuration 3

Default COM Settings 3

Application Configuration 3

5. Windows XP Service Pack 2 Firewall Exceptions 3

# Introduction

OPC (Object Linking and Embedding for Process Control) is the new "plug and play" open automation industry standard. Based on Microsoft's Component Object Model (COM) and Distributed Component Object Model (DCOM), OPC provides the technical basis for the connectivity of automation software with control hardware and field devices. It also provides seamless integration with Enterprise Wide MRP/ERP, SCADA and MES systems.

The RTE OPC server utilises the OPC standard interface to allow OPC clients to communicate with the Measuresoft SCADA Run Time Engine (RTE) channel data.

OPC I/F

FactorySoft

Control

Devices

ProcessX

Viewer

RTE I/F

RTE

System

OPC I/F

RTE OLE

Server

Processors

OPC I/F

FactorySoft

Client

The above diagram illustrates that the RTE system maintains its existing proprietary interface to devices and processors and that in conjunction with the OPC interface a client can communicate with any device or processor through the RTE OPC Server.

**NOTE: The RTE OPC Server is not supported under Terminal Server.**

**DCOM facilities for this product are not supported on Windows 95.**

# Getting Started

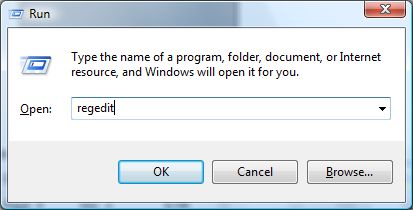
The RTE OPC server presents its browser interface in a variety of forms dependent upon registry settings. So before using the RTE OPC server there are a number of simple steps to be taken to set the registry.

## The Registry Browser Options

The browser interface can be presented either Flat or Hierarchical formats. These options are configured using the system Registry. These options are stored in

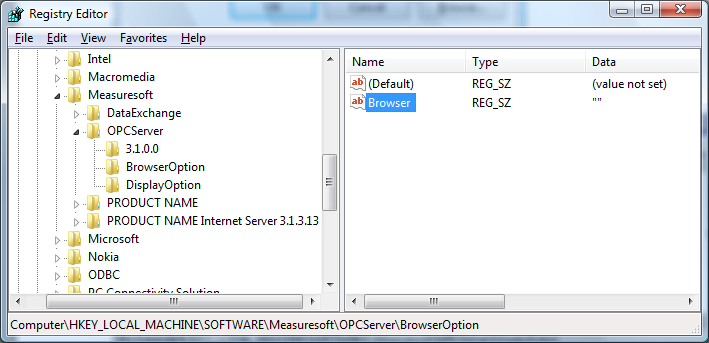
**KEY\_LOCAL\_MACHINE\Software\Measuresoft\OPCServer\BrowserOption** and can be set to Flat or Group. The default browser interface is Group.

From the “Start/Run…” menu type **regedit**, and select “OK” to open the **Registry Editor**.



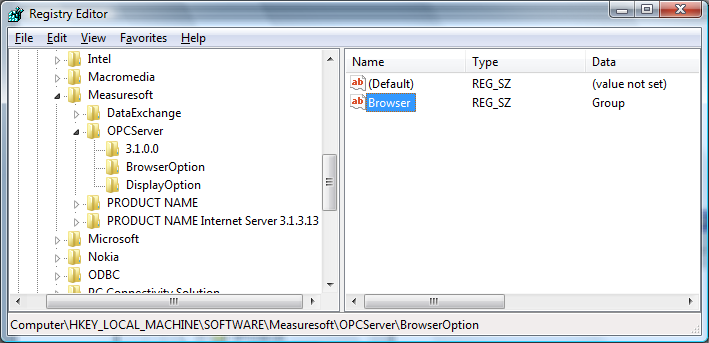
Locate the registry key **HKEY\_LOCAL\_MACHINE\Software\Measuresoft\OPCServer\**

**BrowserOption**.If it does not exist then create it.



Create a string value under this key and call it “Browser”. Set the value of this key to either of the options below.

1. GROUP specifies the Hierarchical namespace
2. FLAT specifies the Flat namespace



## The Registry Display Options

In addition to specifying the browser options the RTE OPC Server can also display the data item in a number of formats. The item can be displayed with the following format:

**Format 1: Channel+Prefix+[Tag]+[Description]**

**Format 2: Tag**

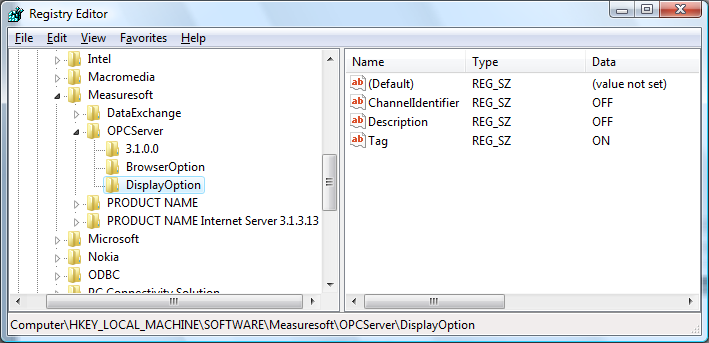
The [] indicates that these descriptors are optional.

These optional descriptors can be set under the following key **HKEY\_LOCAL\_MACHINE\Software\**

**Measuresoft\OPCServer\DisplayOption.** If this key does not exist then create it.

Create three string values under this key and call them “Channel Identifier”, “Tag” and “Description”. Set these values to either of the options below.

1. ON specifies the descriptor will be displayed as part of the item
2. OFF specifies the descriptor will not be displayed as part of the item

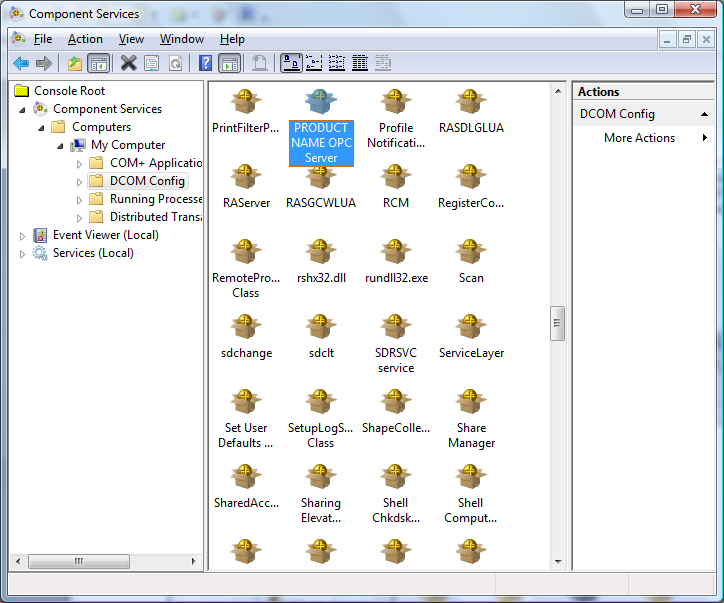
Note if “Channel Identifier” is set to “OFF”, only the channel TAG will be visible. 

## Server Machine DCOM Configuration

The server machine is assumed to already have the RTE OPC Server registered / installed. After this the main changes required are to configure the system and security to allow remote users to connect. The method described in the following pages does this by allowing all COM servers to be used by the specified remote users. If it is necessary to have tighter control of COM / DCOM security permissions, contact your security administrator, for alternative configuration options.

### Application Configuration

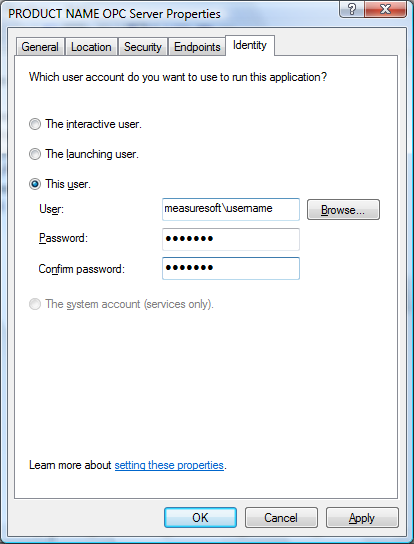
From the Start bar choose Run. Enter ***DCOMCNFG*** into the edit field and Click OK.



However it will cause a separate copy of the OPC server process, to be launched for each user connected. If it is desired to use the same OPC server process for all users, the OPC server process should be configured to “Run As” a particular user. This user must have sufficient security permissions to access the Orchestrator service.

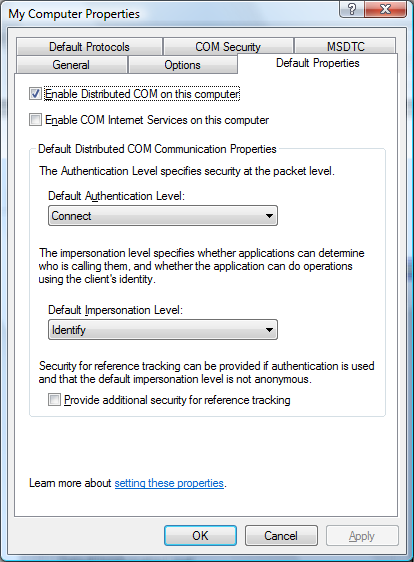
To configure the OPC Server to “Run As” a particular user, follow the steps below:

Expand Component Services, Computers, My Computer and DCOM Config. Find the RTE OPC Server., select the RTE OPC Server and click the “Properties” button.



* Select the “Identity” tab
* Select the “This user” radio button.
* Enter the user name and password of the account in which the OPC server process should run.
* Click the “Apply” button.
* Click the “OK” button.

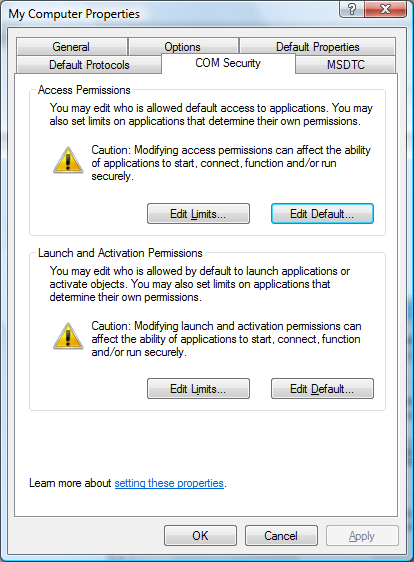
### Default Properties



* Select the “Default Properties” tab:
* Set the “Enable Distributed COM (DCOM) on this machine” check box.
* Set “Default Authentication Level”
* If the opc server is being run within a domain this field can be set to “connect”
* If the opc server is NOT being run within a domain this filed must be set to “none”
* Set “Default Impersonation Level” to “Identify”.
* Clear the “Provide additional security for reference tracking” check box.
* Click the “Apply” button.

### Default Security

* Select the “Default Security” tab.



* Edit the “Default Access Permission”. Add both the SYSTEM account and the required users / groups to the list of users / groups who are “Allowed Access”.
* Edit the “Default Launch Permission”. Add both the SYSTEM account and the required users / groups to the list of users / groups who are “Allowed Launch”.
* Default Configuration Permissions are not important at run time.

**N.B.**

If after doing this you are still unable to retrieve data from the system you may have an issue with the users you have selected to run the OPC server. In this case add “everyone” to the “Default Access Permission” and “Default Launch Permission”. If this works correctly you should contact your system administrator with regards to the accounts you are using.

## Configuring a Restricted DCOM Port Range DCOM

To make the RTE OPC Server run through a firewall it is necessary to configure DCOM using the following procedure in order to workaround some bugs in Mircosoft documentation.

**Windows NT 4.0 Service Pack 6**

1. Run the ***dcomcnfg.exe*** utility, open the *Default Protocols* tab.
2. Move *Connection-Oriented TCP/IP* protocol to the top of the list.
3. Select *Connection-Oriented TCP/IP* protocol and click *Propertie*s button
4. Remove any port ranges in list, Add new port range *5000-5200*
5. Select *Internet range* in both radio buttons, click *OK* to close dialog box.
6. Click *OK* to close dcomcnfg.
7. Open ***regedt32.exe*** utility (Do **NOT** use the usual regedit utility)
8. Select **HKEY\_LOCAL\_MACHINE\Software\Microsoft\RPC\Internet** key
9. Select *Ports* value entry in right panel
10. Edit the Ports entry (spaces are not allowed, there should only be one line, check for spaces on either side of the "-") the entry should look like:   
    5000-5200
11. *Restart* the computer
12. Repeat the same process all another servers, establish communications, and check

port range used with netstat utility

To configuring a firewall to allow DCOM calls – refer to the paper at <http://www.microsoft.com/com/wpaper/dcomfw.asp>

You must open ports **135** and **5000-5200 i**n the appropriate way.

Troubleshooting:

1. If you restart the computer and get the message that "*At least one service was not started*" and in event list you find the message “*Not enough resources available” messages from FTP or WWW service …"*Check the

* **KEY\_LOCAL\_MACHINE\Software\Microsoft\RPC\Internet\Ports**. Make sure it is configured as above.

1. You get an *"RPC server is unavailable"*message when trying to connect remote OPC server.  
   Check that:
   * Port 135 is opened on the firewall
   * Ports 5000-5200 are opened on the firewall

* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\RPC\Internet\Ports.** Make sure it is configures as above.

## Register OPC Proxy

The OPC Proxy DLL (“OPCProxy.dll”) must be registered on the client machine. This DLL contains the information needed to send data between any OPC client and server. The proxy is registered using the RegSvr32.exe” utility. Copy the OPC Proxy DLL to the <Windows>\system32 directory and from the command prompt in that directory, run “RegSvr32 OPCProxy.dll”.

# Advanced Configuration of DCOM (Distributed COM) to Connect an OPC client to an OPC Server on another Machine

The ability of applications (i.e. HMI/SCADA clients and I/O servers) using the OLE for Process Control (OPC) standard to connect from one machine to another - i.e have the OPC client application one computer and the OPC server on another -- is quite powerful and enables many interesting applications. However, it is probably one of the least understood aspects of using OPC by the general user population and like it or not, there are some important details one must be concerned with when setting up a system for DCOM. This article is provided to aid our clients and prospective clients by sharing our techincal expertise based on our extensive experience with DCOM and testing with our OPC Data ActiveX with both our OPC servers as well as many other OPC servers from other vendors at multiple OPC interoperability workshops.

### See section on Windows XP/Vista Firewall Exceptions if necessary.DCOM Tutorial - Preface and Best Practices

We recommend you read these best practices, and although you may not understand all of them now, you will as you go through the setups see why they are important.

If using DCOM, please try and use Windows NT/2000/XP if at all possible - although you can get DCOM for Windows 95 and it came with Windows 98, the versions of DCOM in those operating systems is far from perfect and since Microsoft has officially obsoleted those operating systems, don't count on any upgrades to them for the known bugs in the OS.

If you aren't logged in as the Administrator or an account with Administrator rights on the NT machines you are setting up DCOM on, you won't find much success with the information presented here. You do not have to run your applications as an Administrator in order to use DCOM, but you'll need Admin rights to set it up.

If you make a change to any DCOM config or security related setting on the CLIENT side, you must restart the client application for the changes to take effect. Likewise, if you make such changes on the SERVER side, you must restart the server application for the changes to take effect. You typically only need to reboot either or both machines in special instances where you are changing settings that globally affect all DCOM applications on the machine. For example, if you change the DCOM Default Authentication Level or Default Impersonation level, it's a good idea to reboot the machine after this change as this is a very broad change in what it covers relative to your machine's use of DCOM.

Security matters - if the 2 machines you're trying to connect over DCOM do not have security rights for the user names to be used to access the machines, then you'll never get DCOM to work.If you are not familiar with this topic we STRONGLY recommend you read our note on NT/2000 User Permissions as they relate to OPC client/server connections over DCOM. However, do not confuse access rights to get at shared folders and printers with properly setup DCOM rights. Although it helps if you know that you can access shared folders because that means that the machines are at least allowing logon rights, there are still things that must be setup that specifically allow you to connect to COM servers (i.e. OPC servers) and receive data back from them on a client machine (i.e. one running your HMI/SCADA application).

Try and have the OPC client computer and OPC server computer in the same Domain if you can - and use Domain User accounts and Domain Groups for granting permissions if you can.

This document is not intended as the "be all and end all" of DCOM - but it will help you in setting up your DCOM applications. If you really want to get into the technical nuts and bolts, we recommend reading the following Microsoft Articles: DCOM Architecture and DCOM Technical Overview. You in NO WAY need to read these to setup DCOM properly. We provide these links for our readers who really want to get into the "nuts and bolts" details. These articles assume you know the NT/2000 security model, related terminology, and in some cases, some C++ programming.

If you plan to run DCOM to connect between computers in DIFFERENT NT Domains there are additional concerns and considerations that you must take into account when setting up DCOM regarding NT Domain Trusts relationships.

## DCOM Tutorial - Intro to the DCOMCNFG.EXE Utility

### What is DCOM Config (aka "DCOMCnfg")?

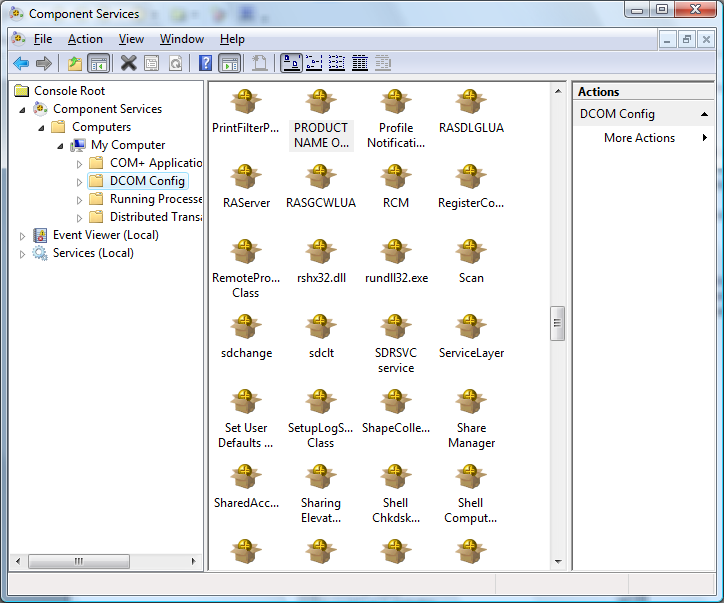
To get DCOM to work right, you've probably heard there are a lot of registry settings.  Although this sounds intimidating, the DCOM Config utility makes things a lot easier because it lets you use a point-and-click interface to get at the various types of settings and it takes care of the "dirty work" for you.  We've spent time learning what entries it makes where and learning the "nuts and bolts" so you don't have too.

### So where is the DCOM Config Utility on my computer?

As with many of Microsoft's most useful utilities, no icon or menu item is provided to indicate the existence of the DCOM Config utility, but it's there.  It should be installed in your \Winnt\System32 directory on either NT or 2000 and the file is named DCOMCNFG.EXE.  The easiest way to launch it is to choose the Run option from the Windows Start menu, and type (or browse for) DCOMCNFG.EXE, then click OK to run it.  You should not have to type the whole path - we don't on our machines which have a standard NT/2000 load.

### What does the DCOM Config Utility Look like?

When you first launch the utility, it will look like the screen below.  Don't be surprised if launching it takes 5 to 10 seconds.  When DCOM Config launches, it goes out and finds all the COM servers on your computer, not just OPC servers but any object that is setup to function as a COM object and provide services to other applications.



### Major parts of DCOM Config

There are 4 main tabs in the DCOM Config utility.  Get to know them by name as we will be very specific in our terminology in the client setups and server setups.

**Applications Tab** - shown here, this tab is used to make settings for a *specific**COM server,* including a specific OPC server.  Settings you make here may *override* settings you make on the "Default" tabs below.  There are also a couple of important settings not covered by the "Default" tabs that you will make for your OPC server here when we do the server side setups.  You pick the server you want to set from the list and click on the "properties" button to bring up server specific settings.  If you wonder why you see some big long alphanumeric strings for some servers -- that's because the server vendor did not include a "Friendly name" for their COM server when they installed it on the machine.  This might be because they do not want people changing the settings unless they know what they are doing, or because they just didn't cover all the details.  Most OPC servers we have seen have a "friendly" name, including OPC servers sold by Measuresoft.

**Default Properties** - on this tab you setup whether DCOM is even enabled and you tell the operating system *how* you want it to authenticate who (i.e. what users and groups of users) you will let connect.  This tab doesn't name specific users, it just specifies the *method* of determining who has access.

**Default Security** - on this tab is where you say *who has access* if nothing else is specified on the Applications tab.  We recommend that you get these settings right and only use server specific settings on the Applications tab if you must.  It makes life much easier if you have multiple OPC servers and clients if you get this right.

**Default Protocols** - on this tab you tell DCOM which of the installed network protocols to use and in what order.  How you have this set can drastically affect timeouts.  DCOM will try all available protocols in the order set on the Default Protocols tab before it finally times out.  Trust us, too many protocols and you'll have a long wait.  Our normal recommendation is that you have "Connection Oriented TCP-IP" on the top of the list on this tab and remove the other protocols unless you have a good reason to use them.

### How should I use DCOM Config?

There are 3 major things that you may need to set with DCOM Config:

Your OPC client machine's settings to allow the OPC server to have Access Permissions to send data back upon subscription/exception

Your OPC server machine's settings to allow desired OPC clients to have Access and Launch Permissions on that machine and to the desired OPC servers so that they can connect to the OPC server(s) on your machine and get data from them, and if necessary, launch them if they are not already running.

On your OPC server machine, setup the COM server OPCEnum so that remote clients can connect and browse (get a list) for available of OPC servers on the OPC server computer.

### Things to remember when using DCOM Config

If you change Access or Launch Permissions on the client side, you will need to restart your client side application.  If you are using a VB program and are in VB development mode - you will need to restart VB - just stopping and restarting your VB application from debug to run mode will not cause security on the application be reinitialized with the new settings.

Likewise, if you change Access or Launch Permissons on the OPC server side either through the Default Security tab or from the Applications tab, you will need to restart the server side application for the changes to take effect.

If you change anything on the Default Properties or Default Protocols tab, we recommend you reboot the computer before assessing if the changes took effect.

Once you get your DCOM Config settings right, you should not have to change them again.

Document your settings carefully - make screenshots if you want and paste them into a Word document.  Proper and organized documentation of how you have your machine setup can be a lifesaver if you have to reload a machine in an emergency (i.e. drive failure, hardware failure, etc).

## OPC Client Computer Recommended Settings

This section is intended to provide general guidance on proper DCOM Config utility settings for the computer on which your OPC Client application is running.  Please note that depending on whose OPC client you are running and how you intend to run your system (user logged in or not, OPC server as a service or not, etc), these settings may vary.  Measuresoft is able to provide extensive assistance with settings for OPC servers that are purchased from us and limited assistance with OPC servers that are not bought from us, provided that you are using one of our client applications such as the Data Exchange Processor.

This part of the tutorial is primarily oriented around the use of our Data Exchange Processor as an OPC client, thought the concepts and principles used here can apply to other OPC clients.  We expect that you have already done the **OPC server computer settings** before doing this part.

If you are not already familiar with the DCOM Config utility and how to launch it, please review the DCOM Config Utility Introduction.  If you are familiar, please launch the DCOM Config utility on the computer where your target **OPC Client Application** is running if you intend to setup your machine with these instructions.

|  |  |  |
| --- | --- | --- |
| Client Side DCOM Configuration Properties: Default Properties Tab 1. First, the Enable Distributed COM on this computer MUST be checked.  2. The Default Authentication Level should be set to Connect.  3. The Default Impersonation Level should be set to Identity  **Note:** There are other settings that can work, but there are also combinations that should have been left out of this Microsoft utility.  For example, if you set Authentication to connect and Impersonation to Anonymous, you will not be able to access local OPC servers, much less remote ones!  The only other combination of these two settings we usually see as acceptable is Authentication="None" and Impersonation ="Anonymous" or "Identify" which basically means to "let anyone have access - don't authenticate any DCOM connections". | |  | | --- | |  | |

|  |
| --- |
| Client Side DCOM Configuration Properties: Default Security Tab It is on this tab that you tell the operating system *who* you will allow to access the OPC client application from remote OPC servers (Default Access Permissions).  Unlike in the OPC server side configuration, the only setting we are concerned with on the client side is the Default Access Permissions on this tab.  It is important that you understand the concept of NT/2000 users and groups (read tutorial if you do not) to make this part go smoothly.  Before you start configuring, you will need to know the following:  What user name and/or groups that OPC Servers will be running under on the machine(s) where OPC servers you wish to connect to are located.  Whether this machine is a member of a domain or not and if so, the name of the domain and associated domain users/groups you will grant access to.  Whether or not you will be running the OPC server as an unattended NT/2000 service or not. If running as a service, what user name (system account) or named user, you will be running the service as.  Note - the OPC clients on remote machines do NOT need to be Administrators on either machine unless you want that - they can be regular user accounts, so long as you grant them access in DCOM Config on the OPC server machine to Access and Launch the OPC server, either explicitly through their user name or through a group containing them (i.e. Domain users) |

|  |  |
| --- | --- |
| Client Side DCOM Configuration Properties: Default Security Tab - Default Access Permissions Dialog It is on this dialog that you will set *who* (i.e. users that remote OPC servers are running under) will have access to make callbacks to this machine when subscription/exception based reads are being done.  **Important:**  Wrong settings here are the most common reason why we see users able to do one time reads of remote OPC servers but NOT get data back when they are subscribed to the OPC server and expecting the OPC server to send back data only when it changes.  The **key** is that the User Name or a Group containing the User Name that the **remote OPC server** is running under be granted access here.  Failure to grant access to the proper user or group will prevent the OPC client from receiving the callbacks on subscription/exception reads from the remote OPC server.  To access this dialog, click on the Edit Default under the subheading Default Access Permissions on the Dcom Config Default security tab.  In the dialog on the right, when you click "Add" you will be presented with a dialog that lets you browse the local machine and domain (if applicable and logged into a domain) for users and groups to grant permission to.  It is up to *you* to know what users and groups you wish to grant permissions to.  If you want to be very broad in your access you could add the Domain Group named "Everyone".   A bit more specific but still fairly "open" is to add the group "Domain Users". | |
| Client Side DCOM Configuration Properties: Default Security Tab - Default Launch Permissions Dialog No changes normally required here. | |
| Client Side DCOM Configuration Properties: Default Security Tab - Default Configuration Permissions Dialog No changes normally required here. | |
| Client Side DCOM Configuration Properties: Default Protocols Tab On this tab you set which of the installed network protocols on your computer to use for DCOM.  We recommend that you use Connection Oriented TCP-IP.  You should have the preferred protocol at the TOP of the list in this tab.  If you don't want to use any of the other protocols, remove them from the list.  Note this does NOT remove the protocols from your computer, but rather just says "do not use them for DCOM".  The fewer the protocols in the list, the shorter your timeouts will be in DCOM waiting for a call or connect to fail. |  |

## OPC Server Computer Recommended Settings

This section is intended to provide general guidance on proper DCOM Config utility settings for the computer on which your OPC server(s) are running.  Please note that depending on whose OPC server you are running and how you intend to run your system (user logged in or not, OPC server as a service or not, etc), these settings may vary.  Measuresoft is able to provide extensive assistance with settings for OPC servers that are purchased from us and limited assistance with OPC servers that are not bought from us, provided that you are using one of our client applications such as the Data Exchange Processor.

By far, the settings on the OPC server computer are many more than on the OPC client computer.  This document is probably the longest one in the tutorial on how to properly setup DCOM.

If you are not already familiar with the DCOM Config utility and how to launch it, please review the DCOM Config Utility Introduction.  If you are familiar, please launch the DCOM Config utility on the computer where your target **OPC Server** is running if you intend to setup your machine with these instructions.

There are 3 areas you will need to setup - please do them all before moving to the OPC client setup.

**Step 1:** Default DCOM Configuration for the OPC server computer

**Step 2:** OPC Server specific settings for your OPC server

**Step 3:** Settings for OPCEnum, the tool that lets remote clients browse for available OPC servers on the machine where your OPC servers are installed.  If you will NOT be letting remote OPC clients browse for available servers, then you can skip this step.

## OPC Server Computer Recommended Settings - Step 1

This section covers the default DCOM settings for the OPC server computer.

If you are not already familiar with the DCOM Config utility and how to launch it, please review the [DCOM Config Utility Introduction](http://www.opcactivex.com/Support/DCOM_Config/DCOMConfigUtility/dcomconfigutility.html).  If you are familiar, please launch the DCOM Config utility on the computer where your target **OPC Server** is running if you intend to setup your machine with these instructions.

|  |  |  |
| --- | --- | --- |
| DCOM Configuration Properties: Default Properties Tab 1. First, the Enable Distributed COM on this computer MUST be checked.  2. The Default Authentication Level should be set to Connect.  3. The Default Impersonation Level should be set to Identity    **Note:** There are other settings that can work, but there are also combinations that should have been left out of this Microsoft utility.  For example, if you set Authentication to connect and Impersonation to Anonymous, you will not be able to access local OPC servers, much less remote ones!  The only other combination of these two settings we usually see as acceptable is Authentication="None" and Impersonation ="Anonymous" or "Identify" which basically means to "let anyone have access - don't authenticate any DCOM connections". | |  | | --- | |  | |

|  |
| --- |
| DCOM Configuration Properties: Default Security Tab     This tab has the most settings to make.  It is on this tab that you tell the operating system *who* you will allow to access OPC servers on this machine (Default Access Permissions), *who* you will allow to launch OPC servers on this machine (Default Launch permissions), and *who* you will allow to configure OPC servers on this machine (Default Configuration Permissions.  It is important that you understand the concept of NT/2000 users and groups (read [tutorial](http://www.opcactivex.com/Support/DCOM_Config/NT_UserPermissions/nt_userpermissions.html#UsersAndGroups) if you do not) to make this part go smoothly.  Before you start configuring, you will need to know the following:  What user name and/or groups that OPC clients will be running under on the remote client machines  What user name and/or groups that any *local (same machine as the OPC server)* OPC clients will be running under.  Whether this machine is a member of a domain or not and if so, the name of the domain and associated domain users/groups you will grant access to.  Whether or not you will be running the OPC server as an unattended NT/2000 service or not. If running as a service, what user name (system account) or named user, you will be running the service as.  Note - the OPC clients on remote machines do NOT need to be Administrators on either machine unless you want that - they can be regular user accounts, so long as you grant them access in DCOM Config either explicitly through their user name or through a group containing them (i.e. Domain users) |

|  |
| --- |
| DCOM Configuration Properties: Default Security Tab - Default Access Permissions Dialog   It is on this dialog that you will set *who* will have access to OPC servers on this machine, unless you override the settings for a specific OPC server on the Applications tab in DCOM Config.  To access this dialog, click on the Edit Default under the subheading Default Access Permissions on the Dcom Config Default security tab.  In the dialog on the right, when you click "Add" you will be presented with a dialog that lets you browse the local machine and domain (if applicable and logged into a domain) for users and groups to grant permission to.  It is up to *you* to know what users and groups you wish to grant permissions to.  If you want to be very broad in your access you could add the Domain Group named "Everyone".   A bit more specific but still fairly "open" is to add the group "Domain Users". |

|  |  |
| --- | --- |
| DCOM Configuration Properties: Default Security Tab - Default Launch Permissions Dialog   It is here that you define *who* can actually start your OPC server on this computer. To access this dialog, click on the Edit Default under the subheading Default Launch Permissions on the Dcom Config Default security tab. Adding of users/groups is done the same way as was done for Access Permissions.  If you plan to have a local client running on this computer and thus launching the OPC server or have the OPC server running as a service, you will need to make sure that the username or group containing the user that you intend to have launch the OPC server is included here.  Also, if you plan to NOT have the OPC server running until a remote client requests a connection, at which time under COM rules, the OPC client will detect this and tell the server to activate, that you MUST have the username OR a group containing the username that your remote OPC client is running under included here.  If you do NOT have this set right, and a remote client attempts to connect, and the OPC server is not running ,it will not launch because that remote user does not have "Launch Permissions".  Again, the rule of "know thy own users and groups applies."  As a general statement, you can include Adminstrators (local or domain) if you want be very broad.  At a minimum you should include the group INTERACTIVE so that local logged in users can launch the server and if you are running the OPC server as a service you may need the SYSTEM account included as well. | |
| DCOM Configuration Properties: Default Security Tab - Default Configuration Permissions Dialog To access this dialog, click on the Edit Default under the subheading Default Configuration Permissions on the Dcom Config Default security tab  This dialog sets what users can change the DCOM configuration of the OPC servers on the machine.  Nearly all systems we see have this properly setup by default, therefore, we recommend that if you are setting up DCOM the first time that you not change these settings.  If you have changed them before, we assume you know what you are doing by changing these settings. | |
| DCOM Configuration Properties: Default Protocols Tab On this tab you set which of the installed network protocols on your computer to use for DCOM.  We recommend that you use Connection Oriented TCP-IP.  You should have the preferred protocol at the TOP of the list in this tab.  If you don't want to use any of the other protocols, remove them from the list.  Note this does NOT remove the protocols from your computer, but rather just says "do not use them for DCOM".  The fewer the protocols in the list, the shorter your timeouts will be in DCOM waiting for a call or connect to fail. | |  | | --- | |  | |

## OPC Server Computer Recommended Settings - Step 2

|  |  |
| --- | --- |
| This section covers the DCOM settings for the OPC server computer that are specific to your OPC server.  You should already have the DCOM Config Utility running and go to the Applications tab.  The settings shown here are OPC server specific and are done on the Applications Tab of the DCOM configuration utility.   We will make general statements here and specific recommendations about OPC server products from Measuresoft.  The rule "know thy own OPC server" applies to these settings - consult the documentation for your OPC server for any DCOM settings recommended by your server vendor.  To set the OPC server specific settings, go to the Applications tab in DCOM Config and browse until you find the OPC server of your choice.  Highlight it and either double click on it or click the Properties button to enter the server specific settings. | |
| Server Specific Properties: General Tab On the General Tab, we recommend that you leave the Authentication level to Default.  This will mean that this server will use the *method* of determining who will be allowed access that was setup on the Default Properties tab in the DCOM Config utility.  We do NOT recommend that you change this setting unless you know what you are doing or are directed to by one of our support engineers. | |  | | --- | |  | |
| Server Specific Properties: Location Tab Make sure that the **Run application on this computer** is the ONLY check box checked.  The Run application on the computer where the data is located check box should NOT be checked, and the Run application on the following computer should NOT be checked.  This is the only valid configuration for OPC servers that we have worked with before. | |  | | --- | |  | |
| Server Specific Properties: Security Tab 1. We suggest you select "Use Default Access Permissions", which will mean users/groups shown under Default Access Permissions on the Default Security tab in the DCOM Config utility will have access to connect to this *specific* OPC server.  Understand that if you select "custom" and put no groups/users into the list, then no client, local or remote, will be able to connect.  So if you choose to use the custom permissions to override the defaults, know which users/groups you wish to grant permission to.  2. We also suggest that you use the Default Launch Permissions, which will mean users/groups shown under Default Launch Permissions on the Default Security tab in the DCOM Config utility will have access to launch this *specific* OPC server.  The same rules apply about using custom launch permissions here as they do for custom access permissions - use with care and know what you are setting.  If you use custom and set nothing, no users will be able to launch your OPC server.  3.  Nearly every OPC server we have every seen sets up Custom Configuration Permissions by default - it is our recommendation that you do not modify these unless instructed by the OPC server documentation or the OPC server vendor's support staff.  If instructed to change these, seek to understand "why", as these permissions do not normally affect simple OPC client/server connections. | |

|  |
| --- |
| Server Specific Properties: Identity Tab On the **Identity** tab, you specify under what user account you want the OPC server to run under.  This is probably one of the MOST important settings for the OPC server in some cases.  The answer is very dependent on HOW you will be using your system.  If you will NOT have anyone logged onto the machine where the OPC server is running, then do NOT use the Interactive user.  The reason is that if you did, and a remote client tried to launch the server, and on one was logged in on the OPC server computer, there would be no "interactive user" logged in to start the OPC server process under, thus it would fail to start.  In this case we recommend that you try and run the OPC server as a service under the System account if that is an option with the OPC server you are using, otherwise use a named user.  If a user will always be logged in on the machine where the OPC server is running, then you may use the Interactive User because that means there will be an "interactive user" under which to run the OPC server process.  We do NOT recommend using the Launching user as this will result in multiple copies of the same OPC server being started when multiple OPC clients connect. Server Specific Properties: Endpoints Tab No changes required on this tab. |

## OPC Server Computer Recommended Settings - Step 3

|  |  |
| --- | --- |
| This section covers the DCOM settings for the OPC server computer that are specific to the application OPCEnum that every OPC server should install.  You may skip this step depending on how your application works.  If your OPC client allows your users to browse for OPC servers that are on the machine where your OPC servers are installed and then pick from a list, then you will need to complete this step.  Also, if you will be running the Data Exchange Processor that allows for server browsing, then you will need to complete this step.  You should already have the DCOM Config Utility running and go to the Applications tab.  Go to the Applications tab in DCOM Config and browse until you find the listing OPCEnum and highlight it and either double click on it or click the Properties button to enter the server specific settings.  Note - the settings we are about to make are the same as the recommended settings for most OPC servers - we have found that if you change one of these, you need to change the other *if* you allow clients to browse for available servers in your client application. | |
| OPCEnum Properties: General Tab On the General Tab, we recommend that you leave the Authentication level to Default.  This will mean that this server will use the *method* of determining who will be allowed access that was setup on the Default Properties tab in the DCOM Config utility.  We do NOT recommend that you change this setting unless you know what you are doing or are directed to by one of our support engineers. | |  | | --- | |  | |
| OPCEnum Properties: Location Tab Make sure that the **Run application on this computer** is the ONLY check box checked.  The Run application on the computer where the data is located check box should NOT be checked, and the Run application on the following computer should NOT be checked. | |  | | --- | |  | |
| OPCEnum Properties: Security Tab 1. We suggest you select "Use Default Access Permissions", which will mean users/groups shown under Default Access Permissions on the Default Security tab in the DCOM Config utility will have access to connect to OPCEnum and browse for available servers.  Understand that if you select "custom" and put no groups/users into the list, then no client, local or remote, will be able to connect.  So if you choose to use the custom permissions to override the defaults, know which users/groups you wish to grant permission to.  2. We also suggest that you use the Default Launch Permissions, which will mean users/groups shown under Default Launch Permissions on the Default Security tab in the DCOM Config utility will have access to launch OPCEnum and browse for available servers.  The same rules apply about using custom launch permissions here as they do for custom access permissions - use with care and know what you are setting.  If you use custom and set nothing, no users will be able to launch your OPC server.  3.  When properly installed by an OPC server install set OPCEnum sets up Custom Configuration Permissions by default - it is our recommendation that you do not modify these unless instructed by the OPC server documentation or the OPC server vendor's support staff. | |
| OPCEnum Properties: Identity Tab On the **Identity** tab, you specify under what user account you want the OPCEnum to run under.  This is probably one of the MOST important settings for OPCEnum in some cases.  The answer is very dependent on HOW you will be using your system.  1. If you will NOT have anyone logged onto the machine where the OPC server and OPCEnum are running, then do NOT use the Interactive user.  The reason is that if you did, and a remote client tried to launch the server, and on one was logged in on the OPC server computer, there would be no "interactive user" logged in to start the OPCEnum process under, thus you would not be able to get a list of available servers on this machine.  In this case we recommend that run OPCEnum as a named user.    2.  If a user will always be logged in on the machine where the OPC server is running, then you may use the Interactive User because that means there will be an "interactive user" under which to run the OPCEnum process.  3.  We do NOT recommend using the Launching user as this will result in multiple copies of OPCEnum being started when multiple OPC clients connect.  This does not cause the same harm as letting multiple copies of an OPC server launch though.  OPCEnum Properties: Endpoints Tab - No changes required on this tab. | |

## User Permissions Considerations when setting up a DCOM Connection between An OPC Client and OPC Server

A key foundation for setting up a DCOM connection between two computers is to have the machines setup so that they have permission to access each other. This is a two way street. The client must have permissions to access the machine with the OPC server and vice versa. If you don't have permissions set both ways, then you will not have success. This article is not intended to be a substitute for good knowledge of the Microsoft Windows NT and Windows 2000 user accounts and security model. There are plenty of good books on the subject available at any local bookstore. This article is intended to point out some key things you need to have setup before you even try to configure a DCOM connection between an OPC client and an OPC server.

### Types of Permissions:

There are some common types of permissions we discuss in our DCOM tutorial

* **Access** -- these permissions allow a client machine to connect to a server computer, retrieve a list of OPC servers and connect to a server.  They also allow the OPC server to make what is known as a "callback" to your client.  A callback occurs when you ask the OPC server to notify your client only when data changes.  If you use these types of reads, sometimes called "subscription" or "exception" reads, then it is important that Access permissions be set right on the client machine.

* **Launch** - these permissions are what allows an OPC client application to start or "launch" an EXE running on the machine where the OPC server is located.  There are 2 common EXEs that get launched: (1) OPCEnum.exe, a standard OPC common component that lists the available OPC servers on a machine and returns that list to a client and (2) the actual EXE that corresponds to the OPC server.  For example, our RTE OPC server EXE is "ms\_opcsvr.exe"

* **Configuration** - these permissions allow a remote client to change the configuration of the OPC servers setup in the registry - you should rarely have to touch these permissions and in fact should not unless you know what you are doing.

So, the most common permissions you will see us discuss are **Access** and **Launch** permissions.

### Users and Groups:

This document is not meant to replace common books on NT/2000 security, but there are some key concepts we want to emphasize.

* ***Users:***  A user is a particular login name+password combination used to gain access to a machine running Windows NT/2000.
* ***Groups:***A group contains one to many *users.* Groups are a useful way to combine a set of user accounts and grant them certain rights for access and launch.  If the actual user names that you wish to have access to your OPC servers will change with any frequency, we recommend you use Groups when granting all rights.  Then all you have to do is add/remove users from the Groups in the NT/2000 user manager and their rights to access OPC servers will carry along.  Proper use of Groups, whether they be ones you create on your own or any of the NT/2000 default groups, is a great way to reduce your long term maintenance cost of the system
* ***Local Users/Groups:***A Local user is an account that is known ONLY to the machine on which the account was setup.  Likewise for a Local Group.  If you need an account to have access to another machine, and the account is a Local User, you will need to create a Local user with the identical username+password on the remote machine.   For this reason, we recommend running OPC Client - Server setups in a Domain if you can - the maintenance and setup is easier.
* ***Domain Users/Groups:***A Domain User account is one that can be used anywhere within an NT/2000 domain so long as the computer is a member of the domain.  Authentication of the user is handled by a primary domain controller machine, thus allowing you to centralize your security management on the user/group level.  A Domain Group is a group that is available to any computer that is a member of the domain.  We recommend using Domain user accounts and Groups to setup your DCOM Config permissions when setting up OPC client/server connections-- the risk of problems is lower and the long term maintenance is much easier.

### What's a Domain ?

In Windows NT there is the concept of a Domain (in in Win 2000 domains still applies, though the concept has been evolved to talk about Forests/Trees, something beyond the scope of this article). A domain is a group of machines that have reasons to need to be able to work together. For example, you might have the paint shop domain, the body shop domain, the accounting domain, the marketing domain, and sales domain in a large company. For the majority of their day to day work, the users in each domain need only to access the machines in their group but not others. The Windows NT concept of a Domain allows you to setup a Domain Server in the group and setup security in the Domain so that the users within the domain have common access to the Domain server and to some degree, to each other's machines. So for example, in the Paint Shop, you might have a Domain Server (also called a Primary Domain Controller or PDC in Microsoft-speak) and 10 Windows NT machines. When users login to their boxes, they log in to the Paint\_Shop domain, which then gives them access to any shared resources (drives, printers, etc) in the Paint\_Shop domain. Their user name and passwords are authenticated (validated, checked - pick your term) against a database of users stored on the Domain Server. Unless a special relationship called a "Domain Trust Relationship" has been setup, users in the Marketing domain would not have access to shared resources in the Paint\_Shop domain. In a Domain Trust Relationship, the PDC (Primary Domain Controller) for the Paint\_Shop domain agrees to trust the Marketing domain's users as if they were their own. Domain Trust relationships and their setup and maintenance is an advanced topic beyond this discussion - just be aware that if you have multiple domains, you have to be more careful with your access rights setup.

In Windows 2000, machines can still be a member of a Domain, but you can optionally also setup Windows 2000 machines to support the new Active Directory security model, a subject which is beyond the scope of this particular document.

### Get in the Domain - if you can

Now that you have the idea of a domain, why does it matter to OPC? The primary benefit of both the OPC client computer and the OPC server computer being a member of a domain is that security is centralized. Both machines will trust accounts that are members of the domain, meaning their username/password combinations are found in the security database of the PDC machine. The downside is that if the PDC goes down, you might not be able to validate security after reboot of a machine in the domain until the PDC comes back. Fortunately you can have BDCs or "Backup Domain Controllers" in a Domain to decrease this risk.

When you run an OPC client application on an NT/2000 machine, that application, even if it is running as a service, has to run under some user name -- you'll hear this sometimes called "running in the context of user name JoeSmith" -- it means you are running the application as if it were launched after a user JoeSmith logged into that machine. The same applies to an OPC server -- it too runs under some user name or "context".

So if we have OPC client on machine A, running under username JoeSmith, and it wants to talk to an OPC server on machine B, that is running under the name BillJones, then DCOM security defaults require that JoeSmith have access to Machine B, and BillJones have access to MachineA. Without BOTH of those requirements met, you'll never get your DCOM connection to work, at least not without some major trickery that just isn't worth the hassle.

OK - so what -- how does a Domain help this situation ? Simple -- if Machine A and B are members of the Paint\_Shop domain, and users JoeSmith and BillJones are both accounts in the domain Paint\_Shop, then unless you have done something to abnormally restrict those user's rights (i.e. taken them out of the Domain Users group or other manual editing of rights), the permissions are already setup, you're done. This is because Machine A trusts the PDC of the Paint\_Shop domain to advise it that BillJones has access, and Machine B trusts the PDC of the Paint\_Shop domain to advise it that JoeSmith has access.

Because of these relationships, getting an OPC client and OPC server on machines in the same domain is probably the easiest scenario.

### No Domain - What do you do?

If you don't have a domain, it's OK. The risk of the PDC or having to have a BDC to decrease that risk may be something your network design said doesn't work for you. If your NT/2000 machines are not members of a domain, then they are running as standalone machines. Every NT/2000 machine (even those in a domain) has it's own "local" database of trusted users. When a machine is not a member of the domain, the ONLY user accounts it will trust are those it finds in it's own "local" security database.

Here is how this can get you into trouble on setting up and OPC client to server connection. If machine A has an account JoeSmith and Machine B has an account BillJones, and that is all, then how can an OPC client running as JoeSmith on Machine A, gain access to an OPC server running as BIllJones on Machine B? It can't -- when Machine B receives a request from the OPC client, embedded inside that request is the notation "this is from user JoeSmith on Machine A". Machine B says "I don't know any JoeSmith" and refuses the connection. The typical error message thrown is "Access Denied". A sure sign you have this issue is when you try to connect to a remote machine with an OPC client to browse available servers and you can't even connect to the machine through the browse dialog without getting and "Access Denied" error. That's a sure sign you have a permissions issue between your two boxes.

So what is the solution? Well fortunately you can trick the boxes. All you need to do is create the EXACT SAME user account names AND passwords on BOTH BOXES. So on Machine A, you need to have an account JoeSmith AND BIllJones. On Machine B, you also need an account JoeSmith and BIllJones. The passwords for BOTH JoeSmith accounts MUST match. The passwords for the BillJones accounts must match on both boxes. JoeSmith and BillJones CAN have different passwords between the two account names, and should for good security measure. You should also make sure those accounts have identical access rights if you can.

Once you have that setup, when Machine A comes calling on Machine B with an OPC request and identifies himself as JoeSmith with some password (it's encrypted), Machine B will look in it's database, see the same accountname, the same password, and same "come on in request from Machine A". When Machine B goes to return it's data from the OPC server to the OPC client on machine B, the OPC server will go call Machine A as BillJones with a password -- Machine A will look in it's database, see that it has that account, and accept the call.

A good way to see if you have these permissions set right is to go to Network Neighborhood, browse from Machine A to Machine B and try to connect to Machine B. You may not have any shared folders or printers, but so what - if you can connect to the machine without error, even if no shared resources are available, you likely have solved the first phase of the Access permissions challenge, gaining access to the machine.   Your next step would be to make sure that the users you've setup are granted the proper rights in the DCOM Config utility on the client side and server side.

We know this may sound like a lot but if you read over this a few times, think about the simple concept of Machine's A and B allowing people access to the machines, you can see why this permissions issue is so crucial to proper DCOM configurations and setup.

If you have your basic access permissions working (i.e. you can at least see the machine and see shared folders/shared printers), you can go on to DCOM Client setups or DCOM Server setups.

## Configuring DCOM (Distributed COM) to Connect an OPC client to an OPC Server on another Machine NT/2000 Domain Trust Relationship Considerations

When you're going from one domain to another in NT and browsing OPC servers, probably the biggest issue to be concerned with is domain trust relationships.  When you have multiple NT domains, there are setups in BOTH domains that must be made so that Domain A trusts users from Domain B and vice versa.   For DCOM to work properly you'd have to have the trust going both ways because there are DCOM calls going both ways and the NT security model will try and validate the security credentials of the user going both ways.  It is beyond the scope of our free support to show users how to setup NT Domain Trusts, but the good news is any decent NT administration book will address the issue.

Having said that, with Domain trusts setup properly, then you still have to have the DCOM permissions setup properly as we discuss in our DCOM Configuration appnote.

# Configuration of DCOM (Distributed COM) to Connect an OPC client in a Workgroup to an OPC Server in another Domain

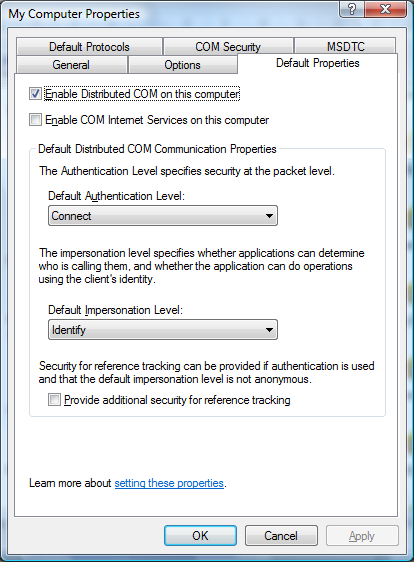
## OPC Server Configuration

In order to get Remote OPC communication operational the follow settings must be changed on the OPC Server machine.

**See section on Windows XP Service Pack 2 Firewall Exceptions if necessary.**

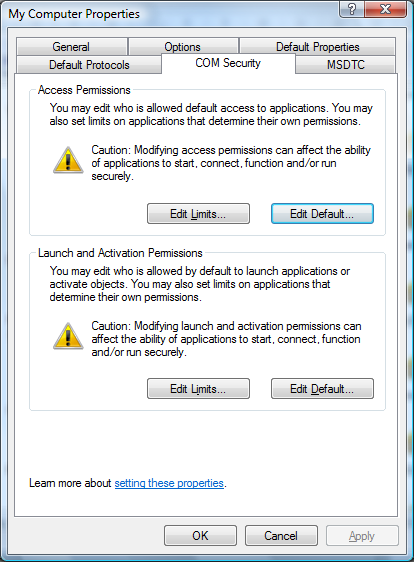
**System DCOM Settings**

* From the Start bar choose Run. Enter DCOMCNFG into the edit field and Click OK.
* Expand Component Services, Computers and My Computer.
* Right click on My Computer and select properties.
* Click the Default Properties tab. Select the settings shown below:



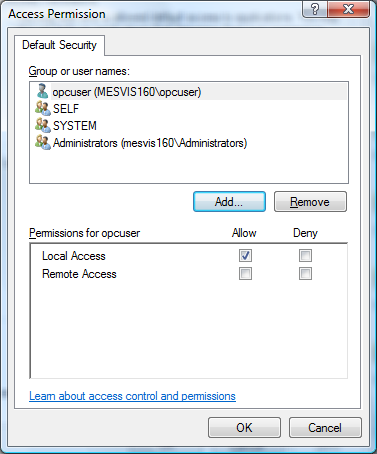
### Click ApplyDefault Security

* Select the “COM Security” tab.

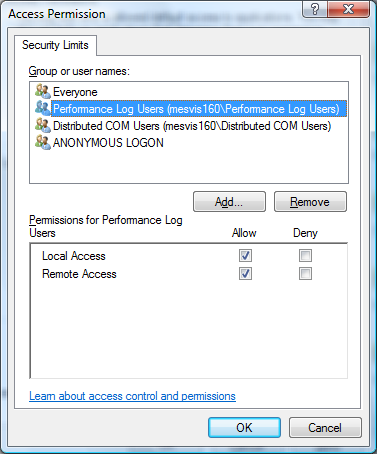


**Access Permissions**

* Edit the “Default Access Permission”. Add the SYSTEM account and the required users / groups to the list of users / groups who are “Allowed Access”. Also Add ANONYMOUS LOGON as shown in the image below.

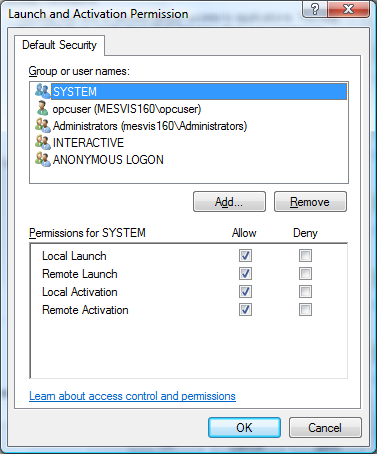


* Click “Edit Limits”. By Default the Everyone group has already been added. Also Add ANONYMOUS LOGON as shown in the image below. Ensure Remote Access is checked.

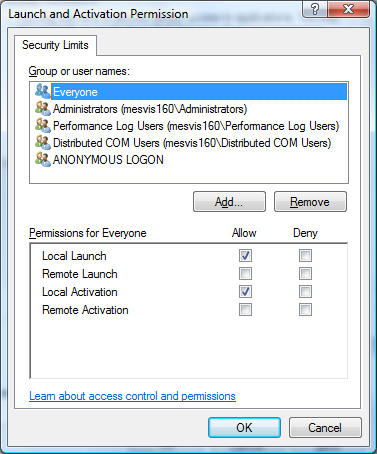


**Launch and Activation Permissions**

* Edit the “Default Launch Permission”. Add SYSTEM, INTERACTIVE and the required users / groups to the list of users / groups who are “Allowed Launch”. Also Add ANONYMOUS LOGON as shown in the image below.

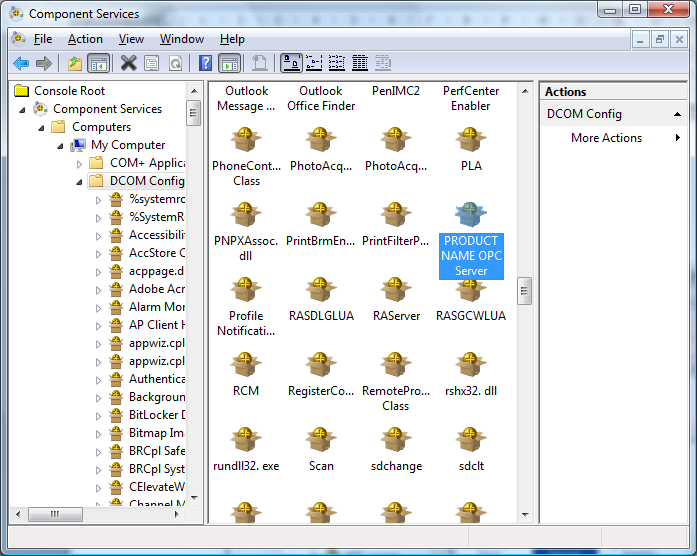


* Click the Edit Level button. Add ANONYMOUS LOGON and ensure that Remote Launch, Local Activation and Remote Activation options are checked. As shown in the image below.

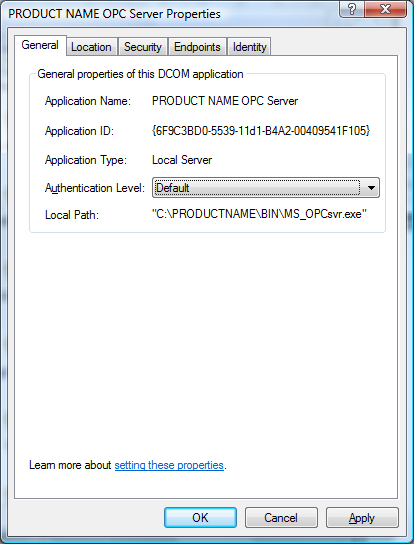


**OPC Server DCOM Settings**

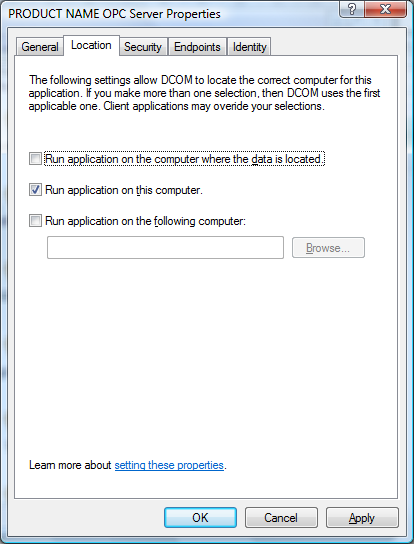
* Expand the DCOM Config Group and find the *ProductName* OPC Server



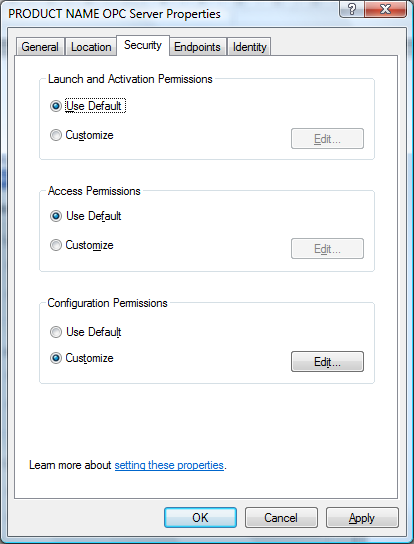
* Right click on EXTRAK OPC Server and select properties.
* On the General Tab make sure the Authentication Level is set to default as shown below:



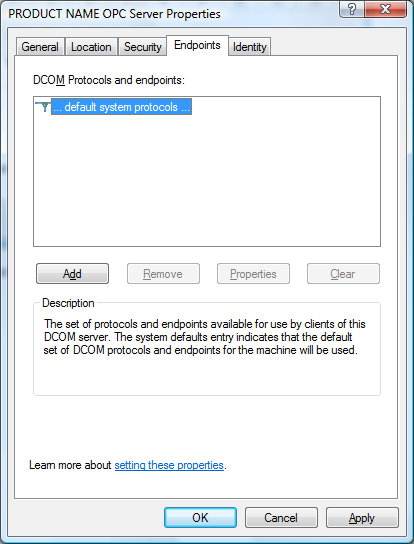
* Click the Location Tab



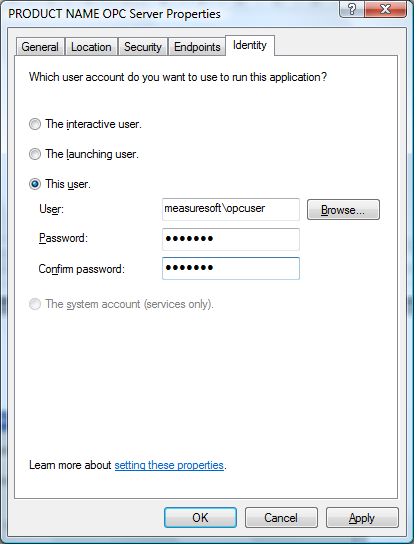
* Click the Security Tab



* Click the Endpoints Tab



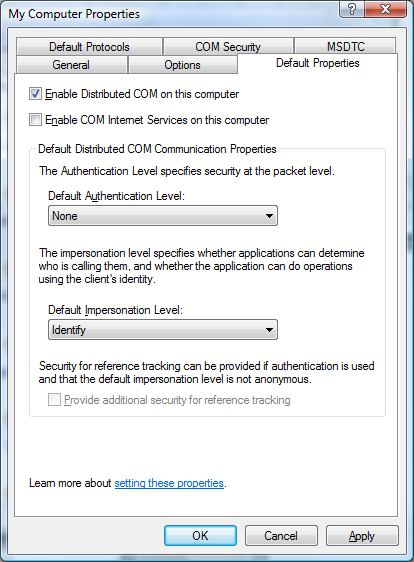
* Click the Identity Tab, specify a user name and password.



## OPC Client Configuration

### Default COM Settings

From the Start bar choose Run. Enter DCOMCNFG into the edit field and Click OK. Expand Component Services and Computers. Right Click on My Computer and select Properties.

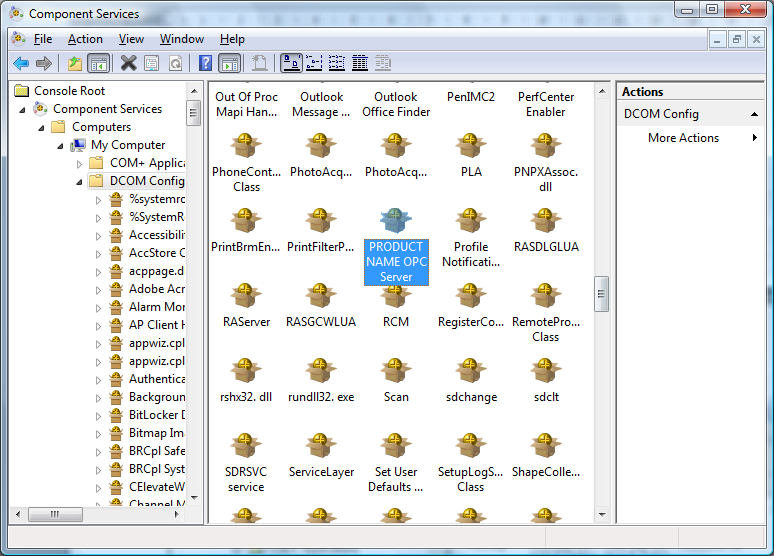


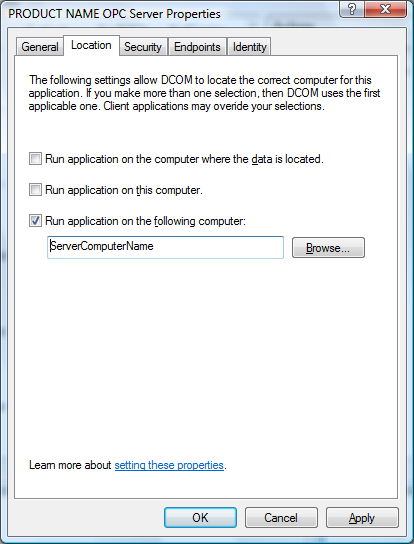
From the Default Properties Tab set the Default Authentication Level to “None”. Set the Default Impersonation Level to “Identify”.

### 

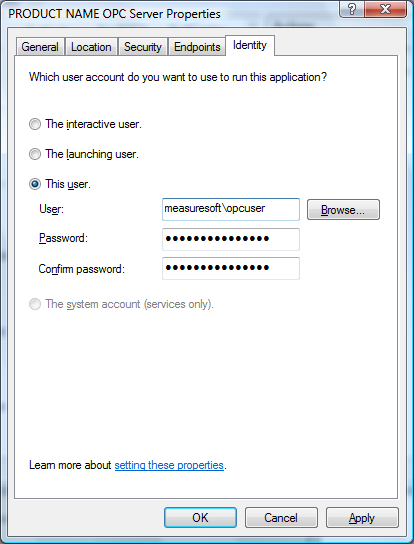
### Application Configuration

Expand the DCOM Config group and find the *ProductName* OPC Server applet. Right click on the applet and select properties. From the General Tab ensure that the Default Authentication Level is set to Default.

 Click the “Location” tab.



* If checked, clear the “Run application on this computer” check box.
* Set the “Run application on the following computer” check box.
* Enter the name of the server machine in the following edit box.
* Click the “Apply” button.
* Click the “OK” button.



* Select the “Identity” tab
* Select the “This user” radio button.
* Enter the user name and password of the account in which the OPC server process should run.
* Click the “Apply” button.
* Click the “OK” button.

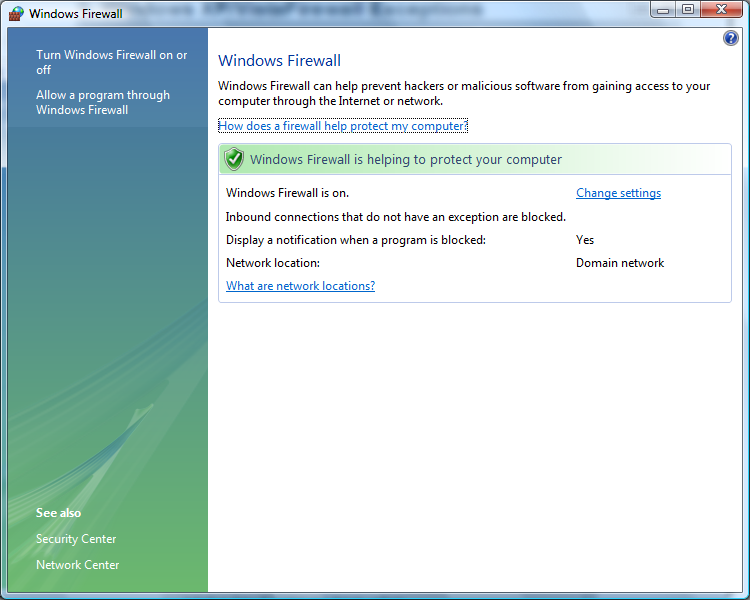
**Note: The Orchestrator Service must be configured to run as a user on the client system.**

To configure the Orchestrator Service to start as a user click Start, Control Panel, Administrative Tools and open the Services applet. From the list of Services find and double click on the Orchestrator service. Click the Log On tab and click “This Account”. Specify a user account that has sufficient rights to access the OPC Server PC.

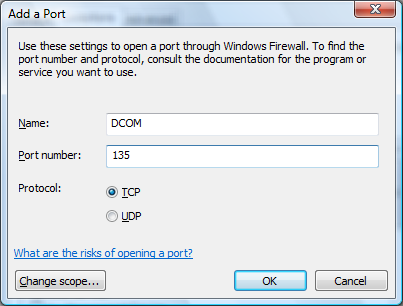
# Windows XP/VistaFirewall Exceptions

When XP Service Pack 2 is installed the Firewall is turned on by default, this setting recommended to give the machine the highest possible protection. It may be appropriate to turn of the Firewall completely if the machine is sufficiently protected behind a corporate Firewall. The steps below describe configuration changes required to allow Remote OPC Communication when the Firewall is turned on.

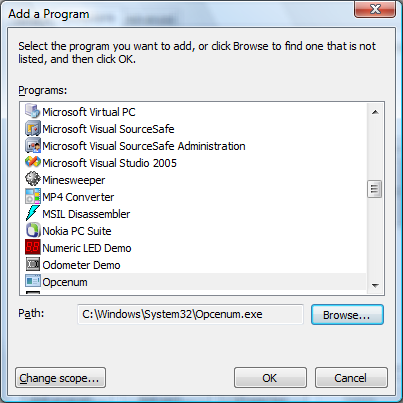
* From the Start Menu open the Control Panel
* Double Click on Windows Firewall



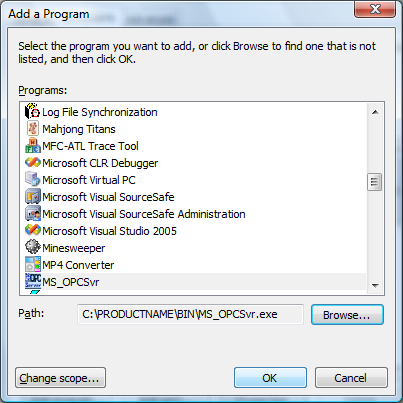
* Click Change Settings
* Click the Exceptions Tab
* Click the Add Port button.



* Select File & Printer Sharing and select Edit
* TCP Port 445 is required to allow a ping to function. This is useful for diagnostics
* Click Add a Program. Browse to c:\windows\system32 and select OPCEnum.exe



* Click Ok
* Click Add Program again and browse to c:\Product\_Name\Bin\ and select MS\_OPCSvr.exe



* When finished you should have the following items listed in your Firewall Exceptions
  + DCOM
  + MS\_OPCSvr
  + OPCenum

# Code Error 80070005 - Access Denied Article

http://www.computerperformance.co.uk/Logon/code/code\_80070005.htm

**Local Security Policies**

1. Start -> Control Panel -> Administrative Tools -> Local Security Policy  
2. Navigate to Security\Local Policies\Security Options  
a. Network Access: Let everyone permissions apply to anonymous users - **Set to Enabled**  
c. DCOM: Machine Access Restrictions - **Add Anonymous, Everyone, Interactive, Network, System with full rights options set.**  
d. Network Access: Let everyone permissions apply to anonymous users - **Set to Enabled**  
e. Network Access: Sharing security model for local accounts - **Set to Classic**

The "Sharing Security model" is the real offending item I believe, and setting the above should fix the problem. If not then I went as far as setting the following in DCOMCNFG.

**DCOM Configuration**

1. Click Start -> Run  
2. Enter DCOMCNFG and press OK. This will open the DCOMCNFG window.  
3. Browse down the tree to Console Root -> Component Services -> Computers -> My Computer  
4. Right click on "My Computer" and select properties  
5. Select the "Default Properties" tab  
  a. Enable Distributed COM on this computer - Option is checked  
b. Default Authentication Level - Set to Connect  
c. Default Impersonation Level - Set to Identify  
6. Select the "COM Security" tab  
7. Click on Access Permissions ' Edit Default  
a. Add "Anonymous", "Everyone", "Interactive", "Network", "System" with Local and Remote access permissions set.  
8. Click on Launch and Activation Permissions ' Edit Default  
a. Add "Anonymous", "Everyone", "Interactive", "Network", "System" with Local and Remote access permissions set.  
9. Click on OK  
10. Close the DCOMCNFG window

Setup firewalls to allow port 135, opeenum and ms\_opcsvr