Kepware Technologies

Remote OPC DA Quick Start Guide (DCOM)

March, 2013
Ref. 03.10

Table of Contents

1. Overview

This document intends to provide information for quickly setting up a secure DCOM connection between an OPC server and a client running on Microsoft Windows XP Service Pack 2 or later.

1.1 What is DCOM?

Distributed Component Object Model (DCOM) is an extension of Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network, which in turn allows COM to communicate beyond the boundaries of the local machine.

Because DCOM poses a security threat, care should be taken to not expose more than what is required for the application. Although multiple security layers exist, it is still possible that some part of the system will be compromised.

1.2 What is OPCEnum?

The OPC server stores OPC specific information in the registry. Since OPC clients need to be able to discover servers running on both the same machine and remote machines, there needs to be a standard method for accessing this registry information (which is not available for remote access). To do so, a component called OPCEnum is provided by the OPC Foundation. OPCEnum is an executable that is typically installed on a computer along with the OPC server. It runs as a System service and provides a means to browse the local machine for OPC servers and then expose the list to the OPC client.

2. Users and Groups

To ensure that an OPC connection is secure, create users and groups that are exclusively for this use. These can be manually added by any user who has the proper credentials to do so.

2.1 Domains and Workgroups

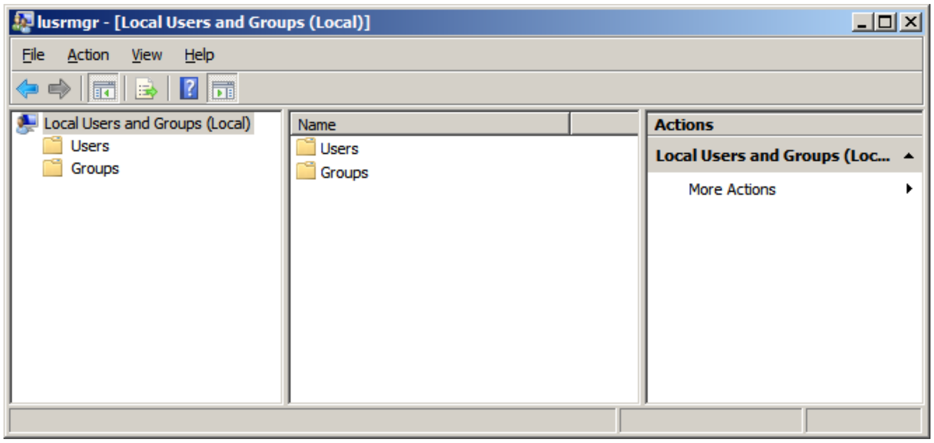
When working within a workgroup, each user will need to be created locally on each computer involved in the connection. Furthermore, each user account must have the same password in order for authentication to occur. A blank password is not valid in most cases. Because changes may need to be made to the local security policy on each computer, remote connectivity within a workgroup has the potential to be the least secure connection. For more information, refer to Local Security Policies.

When working within a domain, local users and groups are not required to be added to each computer. A domain uses a central database that contains the user accounts and security information. If working within a domain is preferred, a network administrator may have to implement the changes.

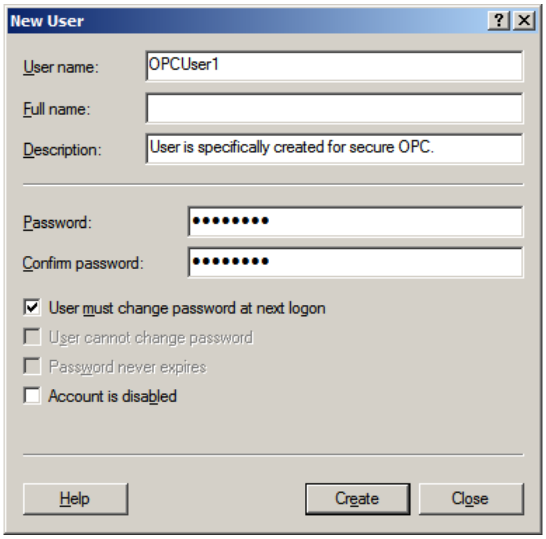
Mixing domains and workgroups will require both computers to authenticate with the lesser of the two options. This means that the domain computer will require the same configuration as it would if it were on a workgroup. Local user accounts must be added to the domain computer.

2.2 Adding a Local User

1. Launch the **Local User and Groups** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "lusrmgr.msc".


lusrmgr - [Local Users and Groups (Local)]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Users
Groups
Actions
Local Users and Groups (Loc...
More Actions

2. Next, click **Users**. Then, select **Action | New User.**



User name: OPCUser1

Full name:

Description: User is specifically created for secure OPC.

Password: •••••••••

Confirm password: •••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

3. Type the appropriate information in the dialog box.

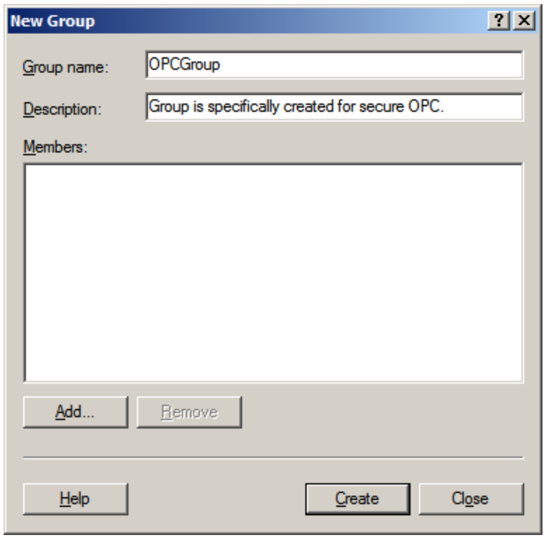
4. Change the following options as required:
   - User must change password at next logon
   - User cannot change password
   - Password never expires
   - Account is disabled

5. Click **Create**. Then, click **Close.**

2.3 Adding a Local Group

1. Launch the **Local User and Groups** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "lusrmgr.msc".

2. Click **Groups** and then select **Action | New Group**.



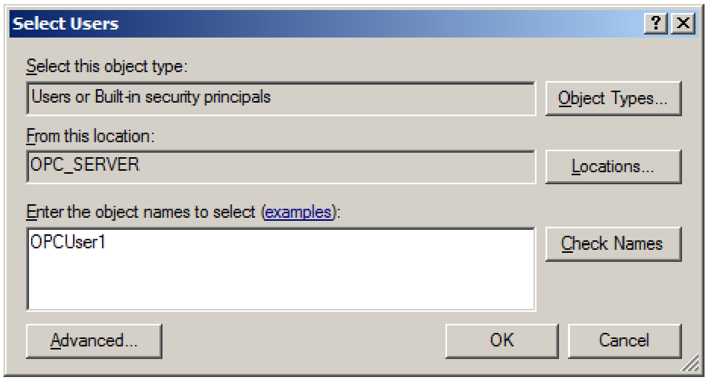
Group name: OPCGroup

Description: Group is specifically created for secure OPC.

3. In **Group name**, type a name for the new group.
4. In **Description**, type a description of the new group.
5. Click **Create** and then click **Close**.

2.4 Adding Users to a Group

1. Launch the **Local User and Groups** snap-in.
2. Next, select **Groups**. Then, right-click on the group in which a member will be added and point to **All Tasks**. Click **Add to Group | Add**.



Select this object type: Users or Built-in security principals

From this location: OPC_SERVER

Enter the object names to select (examples): OPCUser1

3. In **Object Types**, select the types of objects to find.
4. In **Locations**, click the domain or the computer that contains the users to add. Then, click **OK**.
5. Type the name of the user or group that will be added to the group and then click **OK.** To validate the user or group names being added, click **Check Names.**

3. Server Runtime

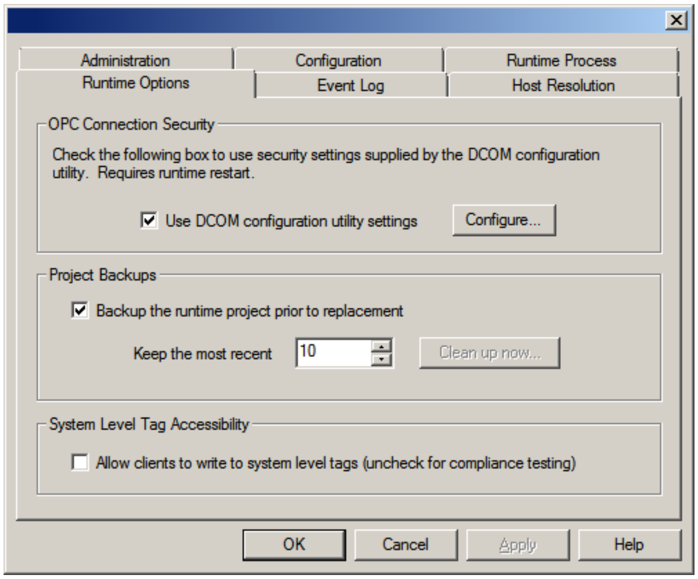
Before DCOM is configured on the server computer, both the level of security and the Runtime's process mode should be considered. To provide the highest level of security, users must enable the appropriate settings. The process mode should be chosen since the DCOM configuration is reset when the process mode is changed.

For more information on which process mode is appropriate for the specific application, refer to the server's help file.

3.1 OPC Connection Security

To provide the highest level of security, DCOM must be enabled in the Runtime. This option, which is enabled by default, ensures that DCOM settings are obeyed and user authentication is performed. Disabling the option is not recommended since the server will impersonate the security of the client when performing any actions on behalf of the client application.

1. Right-click on the server **Administration** icon in the system tray and then select **Settings**. If the Administration icon is not present, it can be accessed from the **Start** menu.
2. Select the **Runtime Options** tab.
3. Check **Use DCOM configuration utility settings** (if it is not already enabled).



Check the following box to use security settings supplied by the DCOM configuration utility. Requires runtime restart.

☑ Use DCOM configuration utility settings

☑ Backup the runtime project prior to replacement

Keep the most recent 10

□ Allow clients to write to system level tags (uncheck for compliance testing)

4. Select **Apply** or **OK**.

   Note: If prompted to restart the Runtime, choose **Yes**.

3.2 Process Mode

The server Runtime has the ability to run as a service or to run interactively under a user account. By default, the Runtime is installed as a service. In a few cases, however, it may be necessary to change the process mode to allow interactive functionality. For more information on how to switch the process mode, refer to the server's help file.

Caution: Application DCOM settings are reset when the server's process mode is changed.

When remote OPC connections are required, selecting System Service Mode will produce the most predictable results. The Runtime will be started when the system starts and will not require user intervention. A specific user is not required to be logged on.

Using the Runtime in Interactive Mode may require additional DCOM configuration. The simplest way to authenticate the connection and prevent this additional configuration is to have a DCOM privileged user account logged on to the Windows operating system on both the server and client side. This user account must have the appropriate permissions set in the DCOM settings as described in DCOM Configuration.

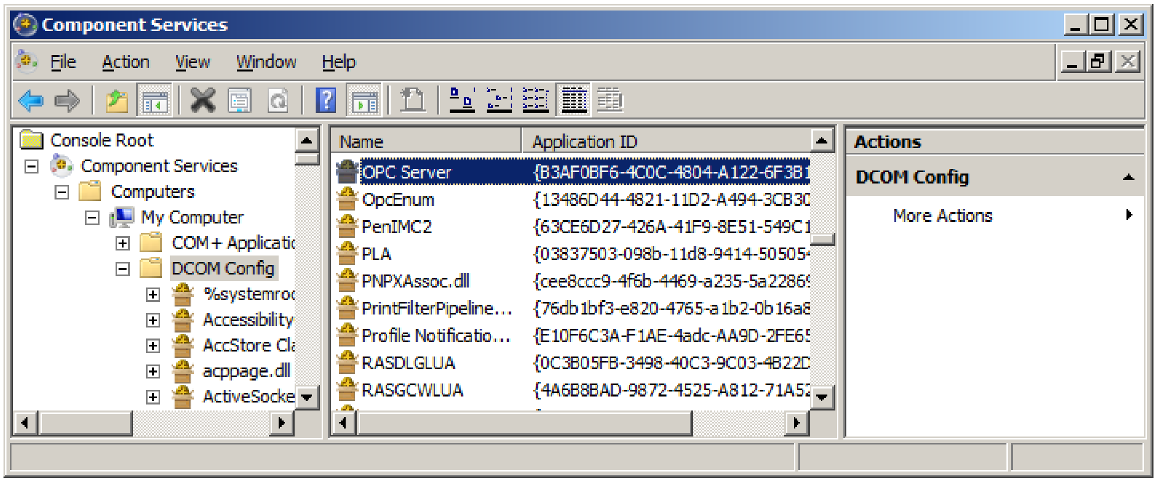
Note: For some situations, extra DCOM configuration is required. For more information, refer to Configuring the Application Identity (Optional).

4. DCOM Configuration

The computer running the OPC server must make changes to the application and system levels in order to setup DCOM correctly.

4.1 Configuring the Application

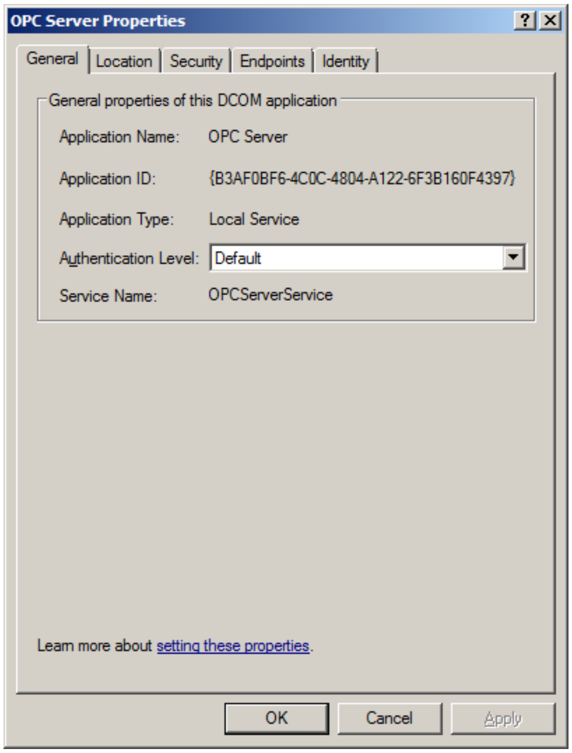
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "dcomcnfg".
2. Under **Console Root**, expand **Component Services**, **Computers**, **My Computer** and **DCOM Config**.



Name	Application ID
OPC Server	{B3AF0BF6-4C0C-4804-A122-6F3B1
OpcEnum	{13486D44-4821-11D2-A494-3CB30
PenIMC2	{63CE6D27-426A-41F9-8E51-549C1
PLA	{03837503-098b-11d8-9414-50505
PNPXAssoc.dll	{cee8ccc9-4f6b-4469-a235-5a2286
PrintFilterPipeline…	{76db1bf3-e820-4765-a1b2-0b16a8
Profile Notificatio…	{E10F6C3A-F1AE-4adc-AA9D-2FE65
RASDLGLUA	{0C3B05FB-3498-40C3-9C03-4B22D
RASGCWLUA	{4A6B8BAD-9872-4525-A812-71A52

3. Browse the DCOM enabled objects until the OPC server application is located. In this example, “OPC Server” is displayed where the actual application name will appear.
4. Right-click on the server application and select **Properties**.

5. Open the **General** tab. Then, verify that the **Authentication Level** is set to **Default.**



OPC Server Properties

General | Location | Security | Endpoints | Identity

General properties of this DCOM application

Application Name: OPC Server

Application ID: {B3AF0BF6-4C0C-4804-A122-6F3B160F4397}

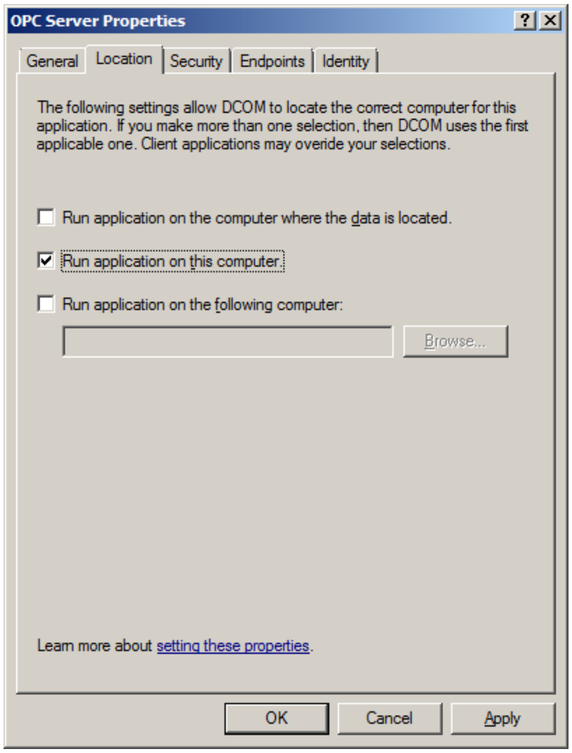
Application Type: Local Service

Authentication Level: Default

Service Name: OPCServerService

Learn more about setting these properties.

6. Open the **Location** tab. Then, verify that only the **Run application on this computer** option is enabled.



OPC Server Properties

General | Location | Security | Endpoints | Identity

The following settings allow DCOM to locate the correct computer for this application. If you make more than one selection, then DCOM uses the first applicable one. Client applications may overide your selections.

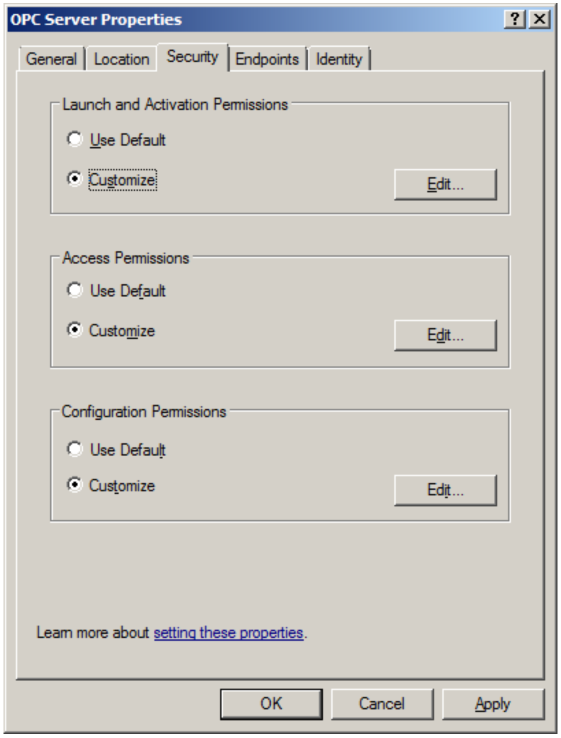
☐ Run application on the computer where the data is located.

☑ Run application on this computer.

☐ Run application on the following computer:

Learn more about setting these properties.

7. Open the **Security** tab.



Launch and Activation Permissions
○ Use Default
● Customize

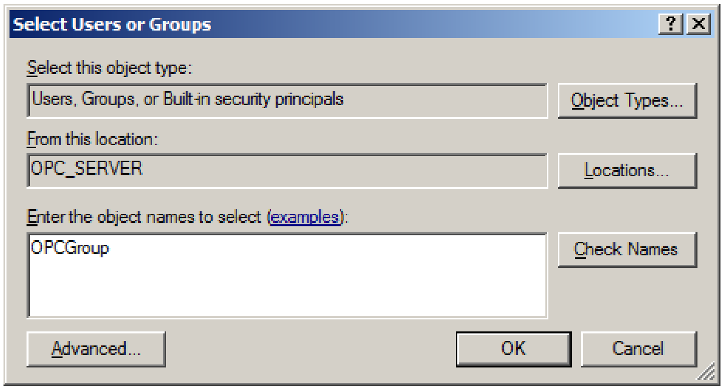
Access Permissions
○ Use Default
● Customize

Configuration Permissions
○ Use Default
● Customize

8. In **Launch and Activation Permissions**, select **Customize**. Here, users and groups can be granted permission to start the OPC server if it is not already running.

9. Click **Edit.**

10. In **Launch and Activation Permissions**, select **Add**.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
OPC_SERVER

Enter the object names to select (examples):
OPCGroup

11. In **Object Types**, select the desired object type.

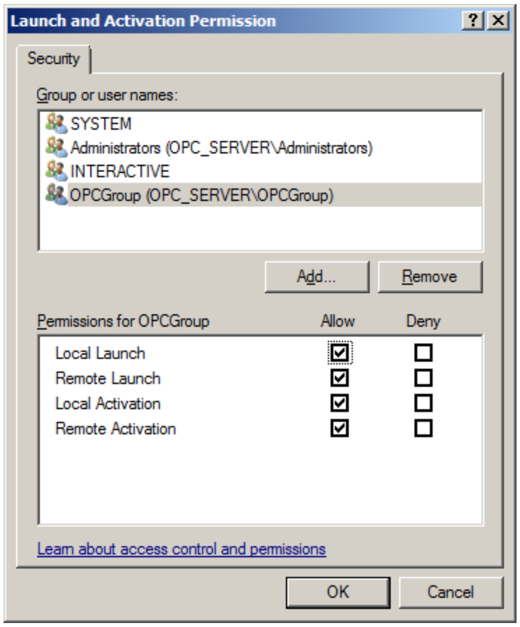
12. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.

13. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.

14. After the account has been validated, click **OK**.

15. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.

16. Next, select the new user or group.



Launch and Activation Permission

Security

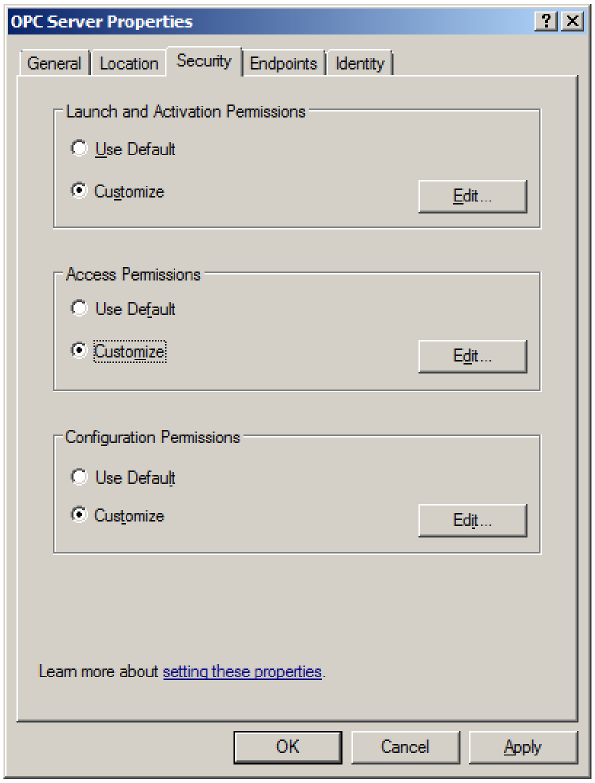
Group or user names:

- SYSTEM
- Administrators (OPC_SERVER\Administrators)
- INTERACTIVE
- OPCGroup (OPC_SERVER\OPCGroup)

Permissions for OPCGroup	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

17. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

18. Repeat the process for all accounts that have been added. Then, click **OK**.



OPC Server Properties

General | Location | Security | Endpoints | Identity

Launch and Activation Permissions
○ Use Default
● Customize

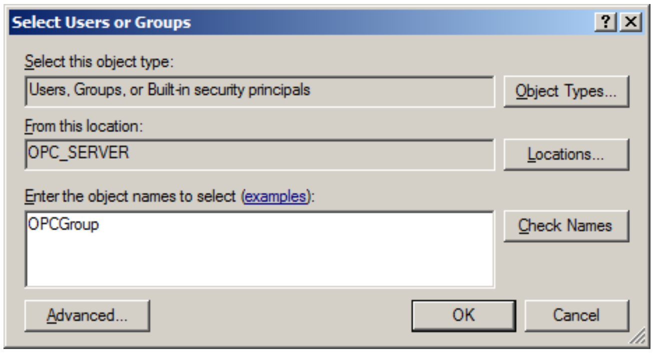
Access Permissions
○ Use Default
● Customize

Configuration Permissions
○ Use Default
● Customize

19. Select **Customize** in the **Access Permissions** group. Here, users and groups can be granted permissions to make calls to the OPC server. These calls include browsing for items, adding groups and items, or any other standard OPC call.

20. Click **Edit**.

21. In **Access Permissions**, select **Add**.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
OPC_SERVER

Enter the object names to select (examples):
OPCGroup

22. In **Object Types**, select the desired object type.

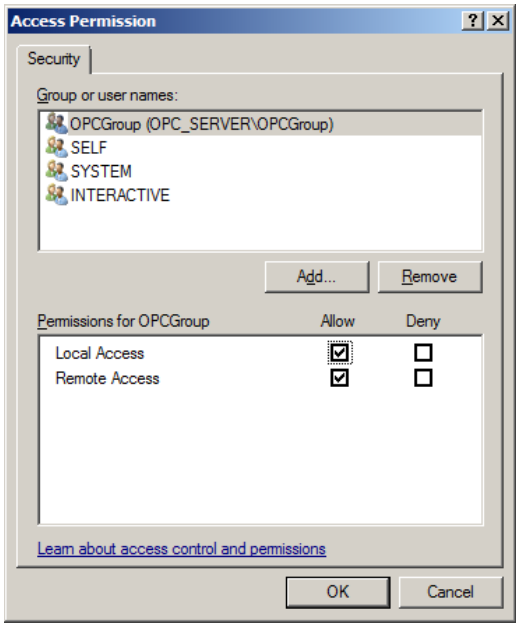
23. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.

24. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.

25. After the account has been validated, click **OK**.

26. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.

27. Select the new user or group.



Group or user names:
- OPCGroup (OPC_SERVER\OPCGroup)
- SELF
- SYSTEM
- INTERACTIVE

Permissions for OPCGroup	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

28. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

29. Repeat the process for all accounts that have been added. Then, click **OK**.

30. Click **OK** to close the **Application Properties** window.

4.2 Configuring the Application Identity (Optional)

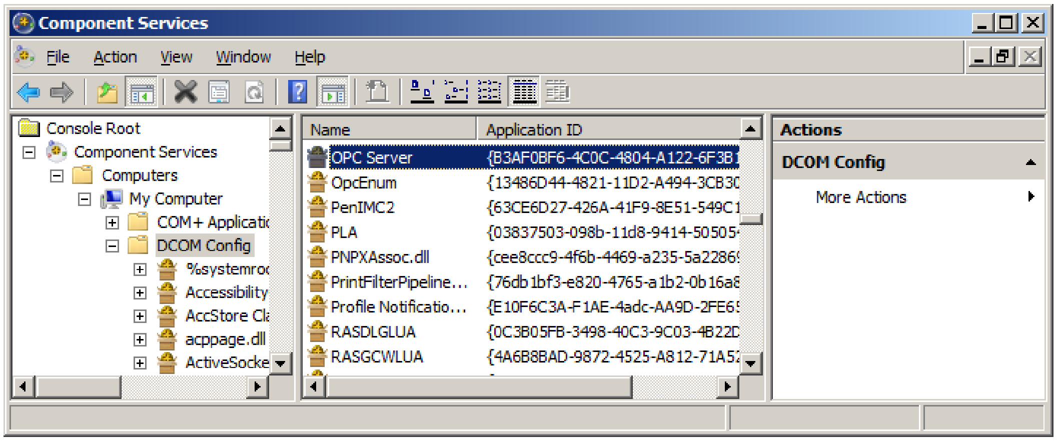
The **Identity** needs to be set when the process mode is set to Interactive and one of the following conditions is present:

- The computer that is being used as the server is required to run with multiple user accounts.
- Users that have not been granted DCOM permissions will be using the computer.

Setting the Identity to **This user** allows a specific user account to be selected to run the application. Clients are then directed to the account allowing a connection to be made to the server. The specified user is not required to be logged on to the Windows operating system in order for this to happen.

Note: In this case, the specified user must be part of the Administrators group. If not, the server will not start.

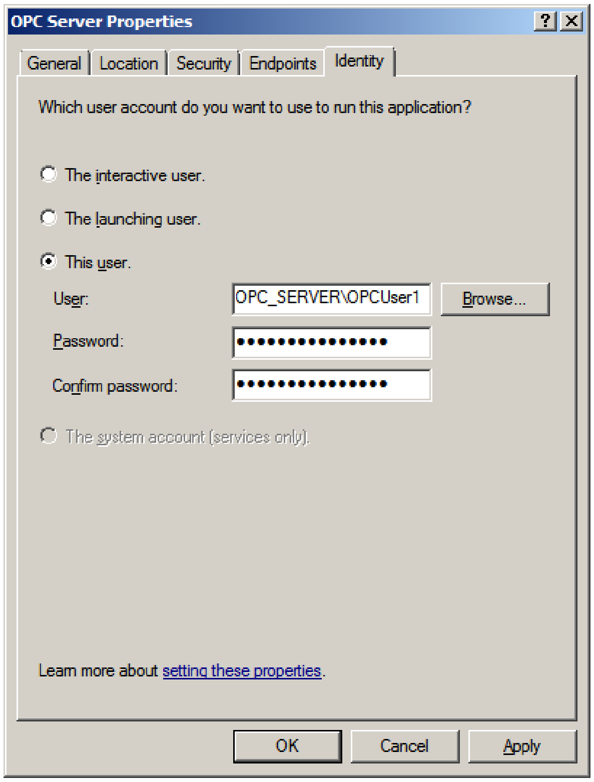
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "dcomcnfg".
2. Under **Console Root**, expand **Component Services**, **Computers**, **My Computer** and **DCOM Config**.



Name	Application ID
OPC Server	{B3AF0BF6-4C0C-4804-A122-6F3B1
OpcEnum	{13486D44-4821-11D2-A494-3CB30
PenIMC2	{63CE6D27-426A-41F9-8E51-549C1
PLA	{03837503-098b-11d8-9414-50505
PNPXAssoc.dll	{cee8ccc9-4f6b-4469-a235-5a2286
PrintFilterPipeline...	{76db1bf3-e820-4765-a1b2-0b16a8
Profile Notificatio...	{E10F6C3A-F1AE-4adc-AA9D-2FE65
RASDLGLUA	{0C3B05FB-3498-40C3-9C03-4B22D
RASGCWLUA	{4A6B8BAD-9872-4525-A812-71A52

3. Browse the DCOM enabled objects until the OPC server application is located. In this example, “OPC Server” is displayed where the actual application name will appear.
4. Right-click on the server application and then select **Properties**.

5. Next, select the **Identity** tab.



Which user account do you want to use to run this application?

○ The interactive user.

○ The launching user.

● This user.

User: OPC_SERVER\OPCUser1

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

○ The system account (services only).

Learn more about setting these properties.

6. Enter the user name or click **Browse** to launch the **Select User** dialog to assist in selecting a valid user name.

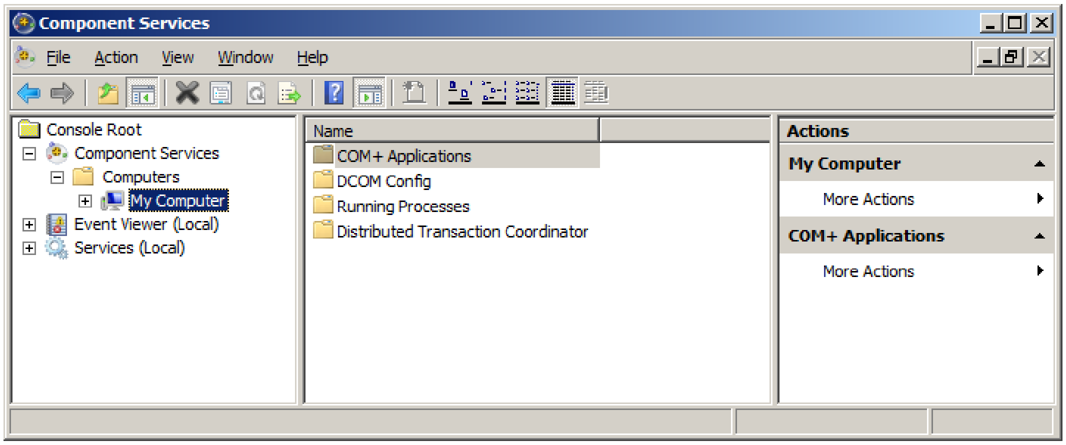
7. Enter and confirm the password of the user that has been chosen to run the server application.

8. Select **OK** to close the **Server Properties**.

4.3 Configuring the System

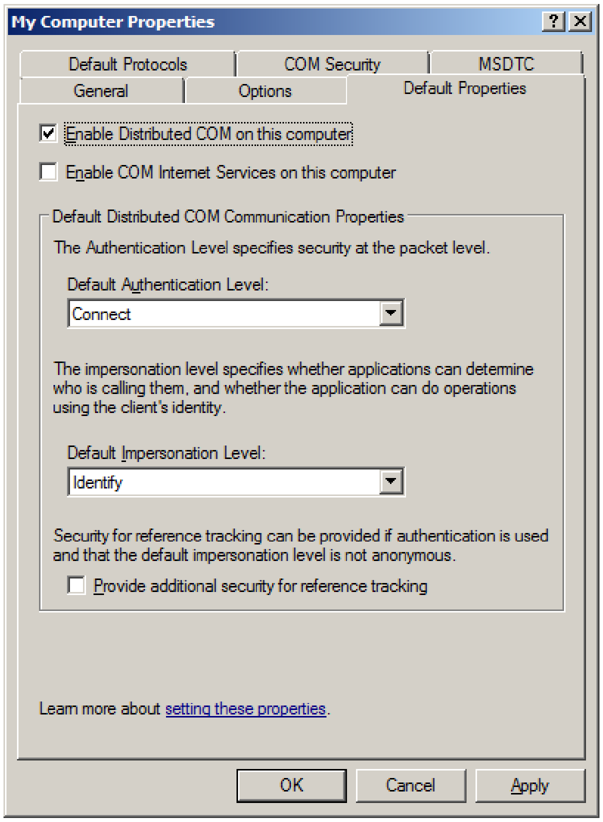
1. Launch the **Component Services** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "dcomcnfg".

2. Under **Console Root**, expand **Component Services** and **Computers**.



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

4. Next, select the **Default Properties** tab.



☑ Enable Distributed COM on this computer

□ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level:

Connect

The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level:

Identify

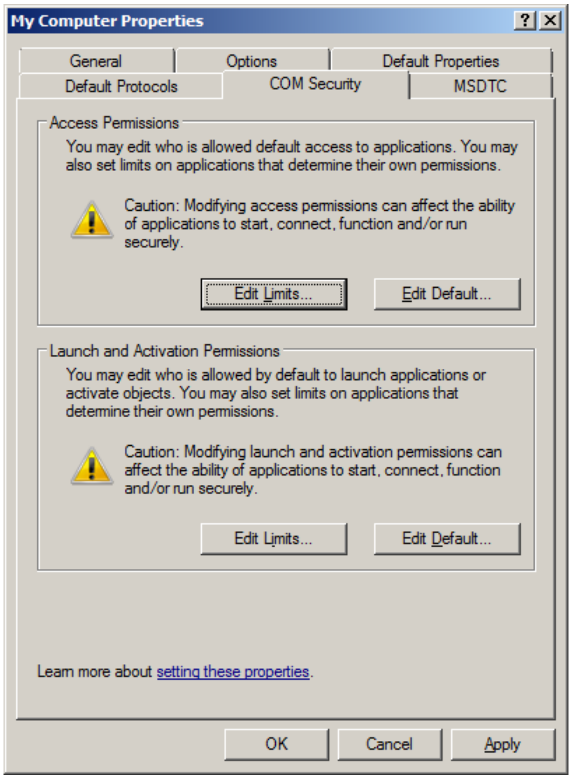
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

□ Provide additional security for reference tracking

Learn more about setting these properties.

5. Verify that the **Enable Distributed COM on this computer** option is enabled.
6. Select **Connect** for the **Default Authentication Level**.
7. Select **Identify** for the **Default Impersonation Level**.

8. Next, select the **COM Security** tab.



Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

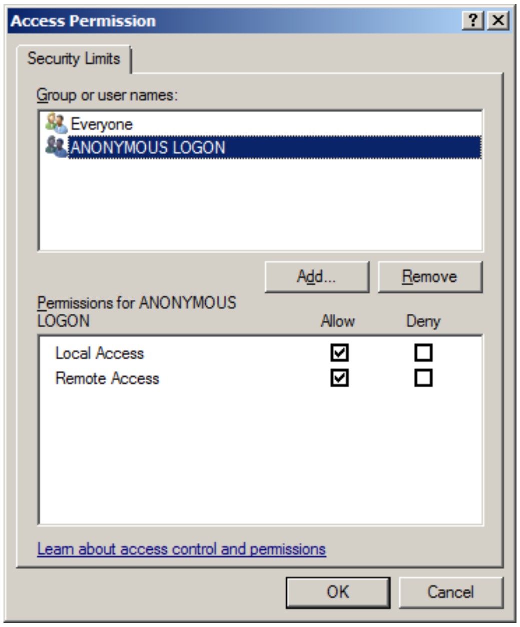
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

9. Select **Edit Limits** in the **Access Permissions** group.

10. Select the **ANONYMOUS LOGON** group account in the **Group or user names** list.



Group or user names:

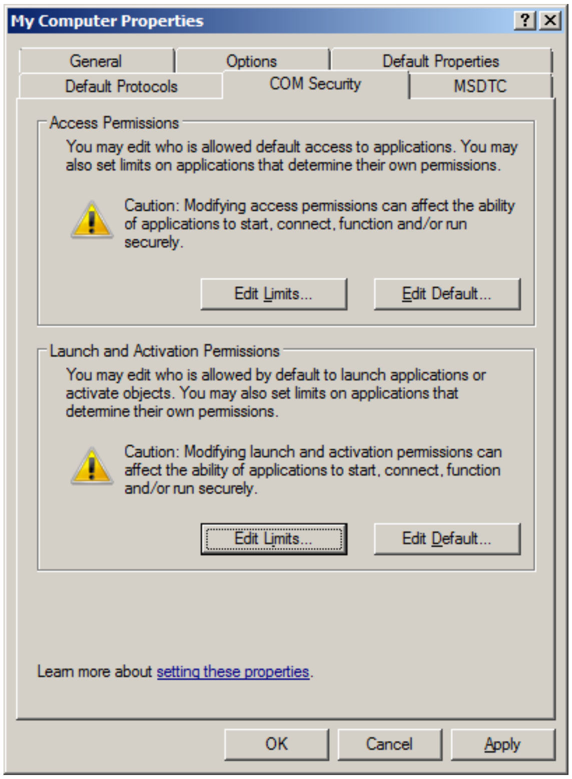
- Everyone
- ANONYMOUS LOGON

Permissions for ANONYMOUS LOGON	Allow	Deny
Local Access	☑	☐
Remote Access	☑	☐

Learn about access control and permissions

11. Enable the local and remote permissions for this group. OPCEnum overrides DCOM settings and opens accessibility to everyone. In Windows XP Service Pack 2 and above, this step is required because applications are not permitted to perform this action without user interaction.

12. Click **OK** to return to the **COM Security** tab.



You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

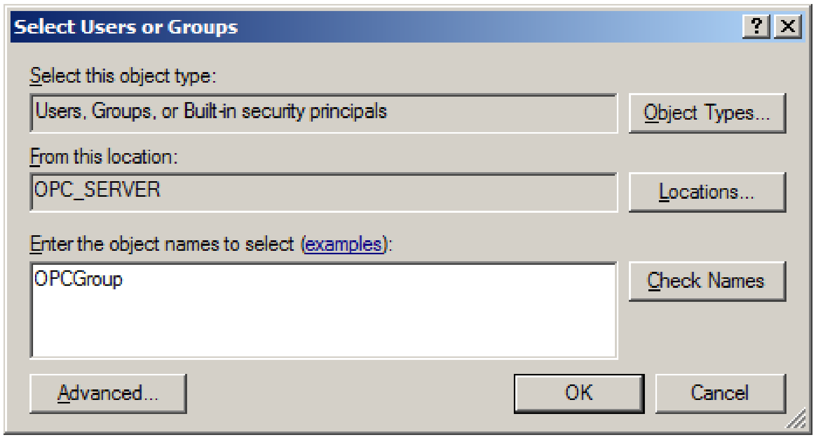
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

13. In the **Launch and Activation Permissions** group, select **Edit Limits**.

14. In **Launch and Activation Permissions**, select **Add**.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
OPC_SERVER

Enter the object names to select (examples):
OPCGroup

15. In **Object Types**, select the desired object type.

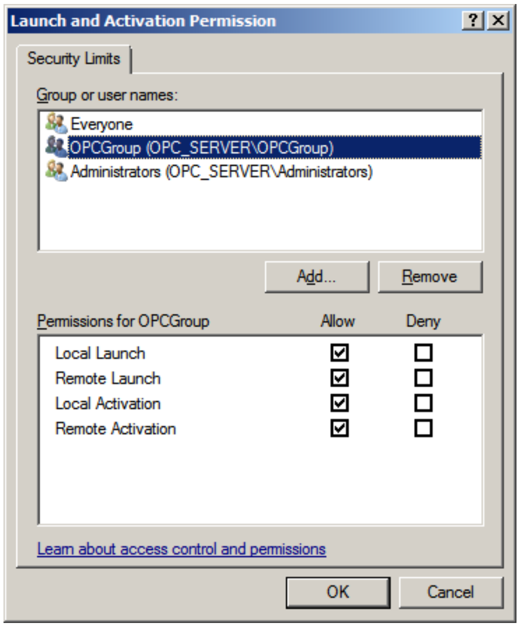
16. In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.

17. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.

18. After the account has been validated, click **OK**.

19. Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the **Group or user names** list.

20. Next, select the new user or group.



Launch and Activation Permission
Security Limits
Group or user names:
Everyone
OPCGroup (OPC_SERVER\OPCGroup)
Administrators (OPC_SERVER\Administrators)
Add...
Remove
Learn about access control and permissions
OK
Cancel

Permissions for OPCGroup	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

21. To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

22. Repeat the process for all accounts that have been added. Then, click **OK**.

23. Click **OK** to close the **My Computer** properties window.

4.4 Applying Changes

After the DCOM settings have been modified, the changes made may not be applied immediately. While some operating systems require a reboot for DCOM changes to take effect, others will only require restarting the Runtime. To do so, right-click on the **Administration** icon in the **System Tray** and then select **Stop Runtime**. Once the Runtime has stopped, the **Start Runtime** menu item will be enabled and ready for selection.

5. Firewalls

In some cases, it is easier to turn off any firewalls that may be running on both the client and server machine before DCOM is setup. Once a connection has been successfully created, it is recommended that the firewall security is restored and the correct exceptions are added.

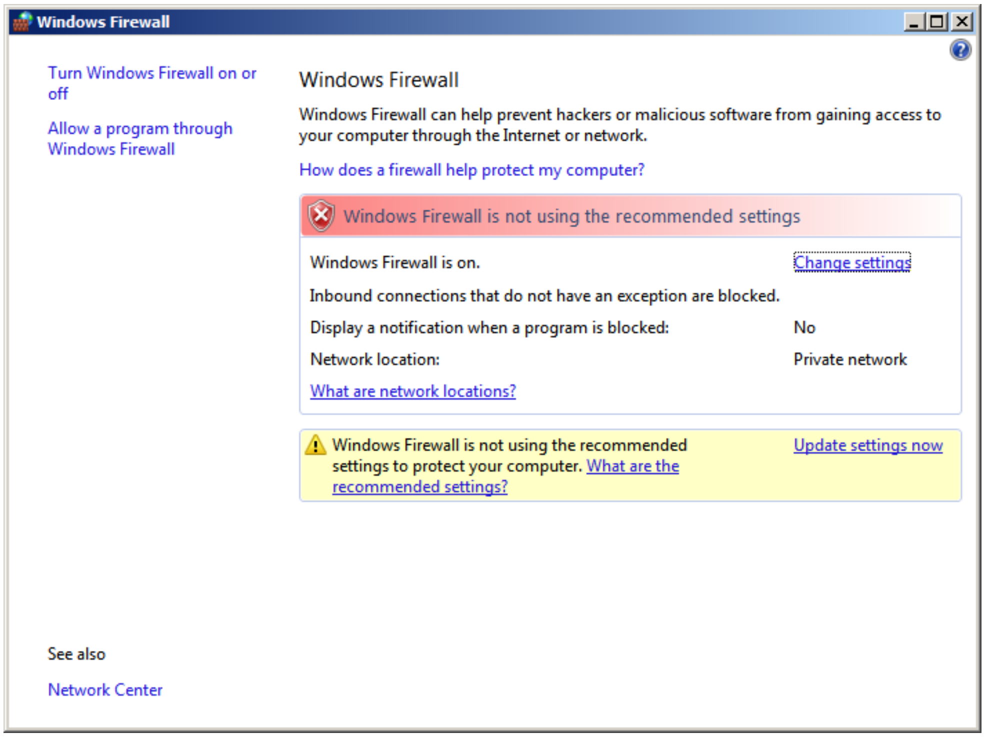
5.1 What is the Windows Firewall?

The Windows Firewall is the firewall service included with desktop and server releases of Microsoft Windows. Prior to Windows XP Service Pack 2, it was named “Internet Connection Firewall.” Its purpose is to drop incoming traffic that is not expected (unsolicited traffic) or traffic that does not correspond to the exceptions (excepted traffic) that are set within the firewall.

Note: Aside from the server computer, the firewall must also be set on client computer so that callbacks can be received.

5.2 Server Side Exceptions

1. Launch the **Windows Firewall** by selecting **Start** | **Run** and then typing "firewall.cpl".



Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

Windows Firewall is not using the recommended settings

Windows Firewall is on.

Inbound connections that do not have an exception are blocked.

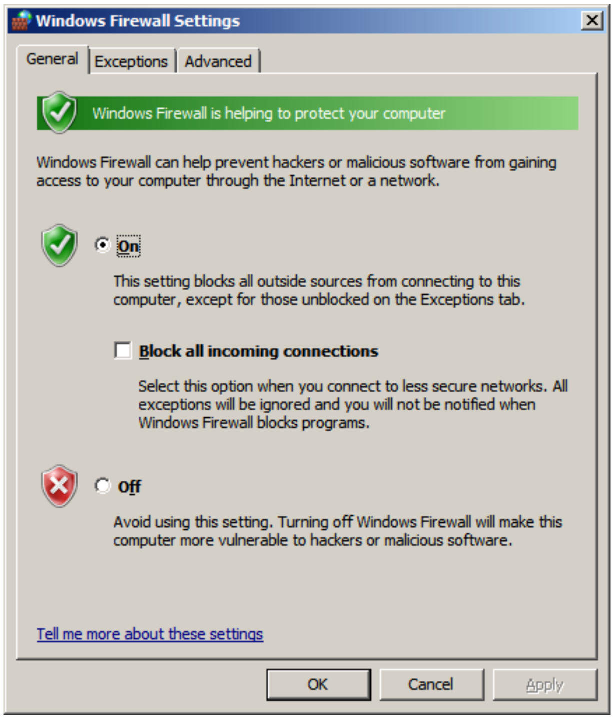
Display a notification when a program is blocked: No

Network location: Private network

Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings?

Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
How does a firewall help protect my computer?
Change settings
What are network locations?
Update settings now
See also
Network Center

2. Windows Vista or Windows Server 2008 will not directly display the settings dialog. To view the dialog, select **Change Settings**.
3. Next, select the **General** tab.



Windows Firewall Settings

Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

□ Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

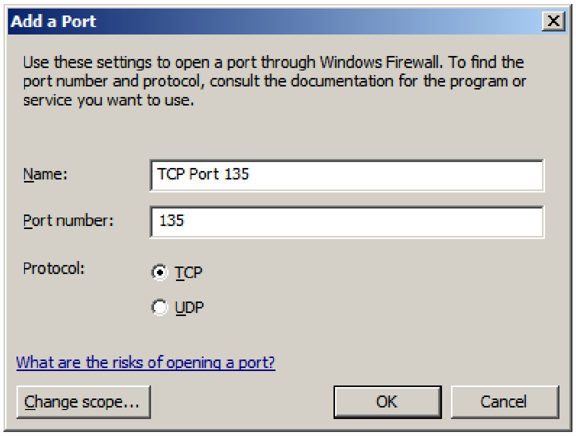
○ Off

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

4. Verify that the firewall is enabled by choosing **On**.
5. Next, select the **Exceptions** tab.

6. Click **Add program**.
7. Click **Browse** and then locate **OPCEnum.exe**. This is located in *C:\Windows\System32\*.
8. Click **OK**.
9. Click **Add program**.
10. Next, select **Browse** and then locate the OPC server application's executable file. This is usually located in *C:\Program Files\<company name>\<product name>* or in *C:\Program Files\product name>*.

    Note: In this example, a generic server name of “OPC_Server.exe” is used in order to apply to any OPC server's configuration.
11. Click **OK**.
12. Click **Add port**.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: TCP Port 135

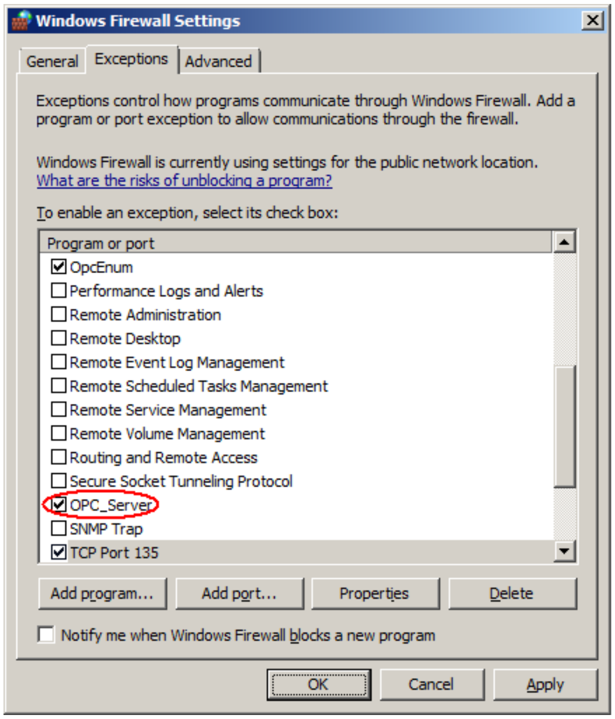
Port number: 135

Protocol: ● TCP ○ UDP

What are the risks of opening a port?

13. In **Name**, enter **TCP Port 135**. This port is commonly used for allowing clients to discover and utilize a DCOM service.
14. In **Port number**, enter **135**.
15. Verify that the correct **Protocol** is selected. The default setting is **TCP**.

16. Click **OK**.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

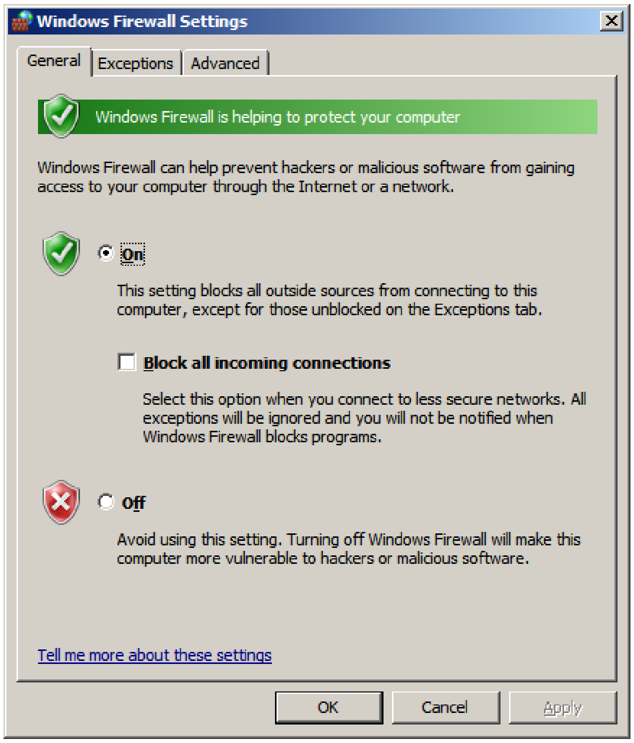
Program or port
☑ OpcEnum
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Desktop
☐ Remote Event Log Management
☐ Remote Scheduled Tasks Management
☐ Remote Service Management
☐ Remote Volume Management
☐ Routing and Remote Access
☐ Secure Socket Tunneling Protocol
☑ OPC_Server
☐ SNMP Trap
☑ TCP Port 135

☐ Notify me when Windows Firewall blocks a new program

17. Click **OK** to close the settings dialog.

5.3 Client Side Exceptions

1. Windows Vista or Windows Server 2008 will not directly display the settings dialog. To view the dialog, select **Change Settings**.
2. Next, select the **General** tab.



Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

☐ Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

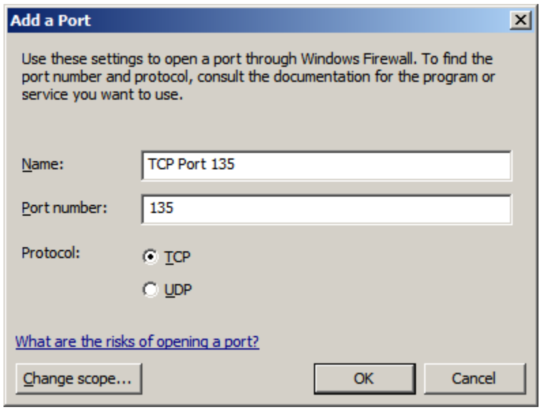
○ Off

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings

3. Verify that the firewall is enabled by choosing **On**.

4. Next, select the **Exceptions** tab.
5. Click **Add program**.
6. Next, click **Browse** and locate the server application's executable file. In this example, the OPC Quick Client is used and is usually located in *C:\Program Files\<company name>\<product name>*.
7. Click **OK**.
8. Next, click **Add port**.



Add a Port

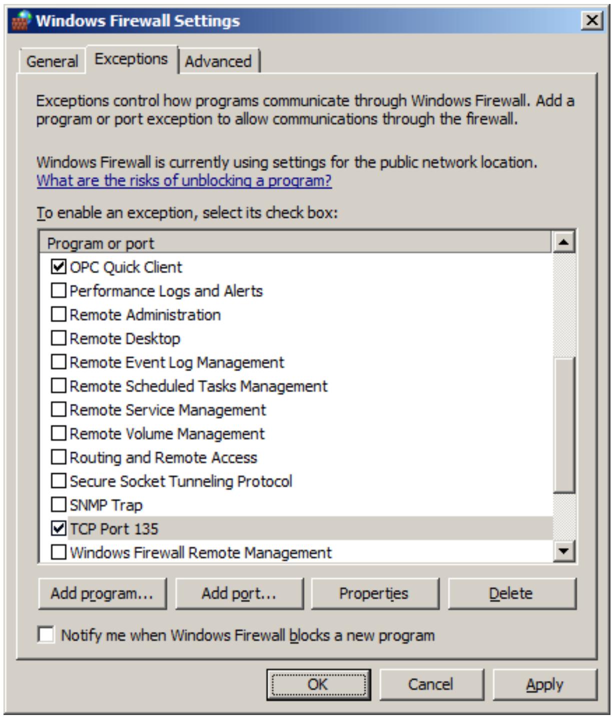
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: TCP Port 135

Port number: 135

Protocol: ● TCP ○ UDP

9. In **Name**, enter **TCP Port 135**.
10. In **Port number**, enter **135**.
11. Verify that the correct **Protocol** is selected. The default setting is **TCP**.
12. Click **OK**.



Windows Firewall Settings

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☑ OPC Quick Client
□ Performance Logs and Alerts
□ Remote Administration
□ Remote Desktop
□ Remote Event Log Management
□ Remote Scheduled Tasks Management
□ Remote Service Management
□ Remote Volume Management
□ Routing and Remote Access
□ Secure Socket Tunneling Protocol
□ SNMP Trap
☑ TCP Port 135
□ Windows Firewall Remote Management

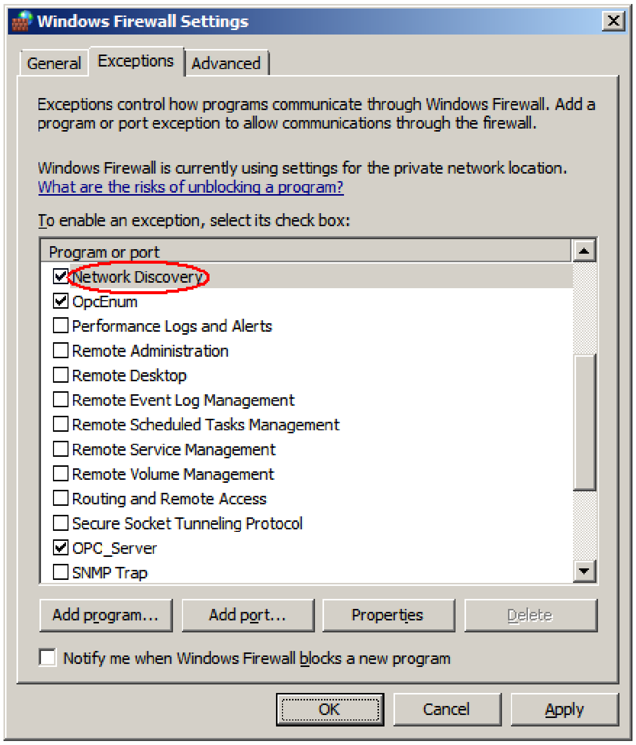
□ Notify me when Windows Firewall blocks a new program

13. Click **OK** to close the settings dialog.

6. Network Discovery

The **Network Discovery** setting was first introduced in Vista and allows or prevents the computer to see or be seen by other computers on the network. If the setting is off (or if it is not set as an exception in the firewall) OPC clients might not be able to browse for the server.

1. Click **Start** | **Control Panel** | **Network and Sharing Center**.
2. Under the **Sharing and Discovery** section, click the **Down Arrow** in the **Network Discovery** row.
3. Click the **Turn on network discovery** radio button, and then click **Apply**.
4. If the state of **Network Discovery** displays **Custom**, it is because the firewall is not allowing for network discovery or because a required service (**dnscache**, **fdrespub**, **ssdpsrv**, and **upnphost**) is not running. While not all services are necessary, the firewall must be set correctly.
5. Launch the **Windows Firewall** and view the settings dialog.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the private network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port

☑ Network Discovery
☑ OpcEnum
□ Performance Logs and Alerts
□ Remote Administration
□ Remote Desktop
□ Remote Event Log Management
□ Remote Scheduled Tasks Management
□ Remote Service Management
□ Remote Volume Management
□ Routing and Remote Access
□ Secure Socket Tunneling Protocol
☑ OPC_Server
□ SNMP Trap

□ Notify me when Windows Firewall blocks a new program

6. Search for **Network Discovery** in the list and then verify that the exception is enabled.
7. Click **OK** to close the **Settings** dialog.

7. Local Security Policies

When the computers that are involved in the remote connection are part of a workgroup, it may be necessary to edit the **Local Security Policy**. This can pose as a security risk and should only be done if it is absolutely necessary. In most cases, the server computer may require changes to the authentication model whereas the client computer needs to have access to browse for servers.

7.1 Sharing and Security Model for Local Accounts

This setting determines how local users will be authenticated. When the setting is set to **Classic**, remote logons will use the same level of access that is set for the local account given that it has the same username and password. If set to **Guest only**, network logons will use the same level of access that is set for the **Guest** account.

The **Sharing and Security Model** may need to be set to **Classic** on the server computer only. An error code (HR=80070005) will be returned to the client when attempting to add items if this is required.

1. Launch the **Local Security Policy** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "secpol.msc".
2. Under **Security Settings**, expand **Local Policies**.
3. Next, select **Security Options**.
4. In the list, right-click on **Network access: Sharing and security model for local accounts** and then select **Properties**.
5. Choose **Classic – local users authenticate as themselves** and then click **OK**.

7.2 Let Everyone Permissions Apply to Anonymous Users

This setting determines the additional permissions that are granted for anonymous logons. When the option is disabled, the permissions granted to the Everyone security identifier do not apply to anonymous users. If the option is enabled, anonymous users are given the same permissions as the Everyone group.

The **Everyone Permissions** setting needs to be enabled on the client computer only. If clients cannot browse for the remote server even after DCOM has been set up, this setting is required.

1. Launch the **Local Security Policy** snap-in, which is part of the **Microsoft Management Console**. It can be viewed directly by selecting **Start | Run** and then typing "secpol.msc".
2. Under **Security Settings**, expand **Local Policies**.
3. Select **Security Options**.
4. In the list, right-click on **Network access: Let Everyone permissions apply to anonymous users** and then select **Properties**.
5. Choose **Enable** and then select **OK**.

8. Summary

Because OPC uses DCOM to allow remote communications, it is imperative that it is correctly configured. Users can create a secure connection by following the instructions in this document. For more information, refer to the OPC Foundation's support documentation at http://www.opcfoundation.org/.