OPC and DCOM: 5 things you need to know

Author: Randy Kondor, B.Sc. in Computer Engineering

December 2007

OPC™
TRAINING INSTITUTE

OPC and DCOM: 5 things you need to know

Author: Randy Kondor, B.Sc. in Computer Engineering

OPC technology relies on Microsoft's COM and DCOM to exchange data between automation hardware and software; however it can be frustrating for new users to configure DCOM properly. If you have ever been unable to establish an OPC connection or transfer OPC data successfully, the underlying issue is likely DCOM-related. This whitepaper discusses the steps necessary to get DCOM working properly and securely.

A simple and effective strategy to establish reliable DCOM communication involves the following steps:

1. Remove Windows Security
2. Setup mutual User Account recognition
3. Configure System-Wide DCOM settings
4. Configure Server Specific DCOM settings
5. Restore Windows Security

In addition, the whitepaper covers troubleshooting tips to identify common OPC and DCOM problems, their symptoms, causes, and how to solve them. This will help integrators set up reliable and secure OPC connections.

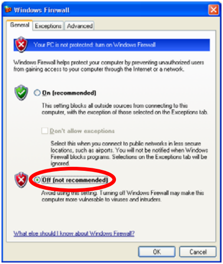
1. Remove Windows Security

The first step to establish DCOM communication is to disable the Windows Firewall, which is turned on by default in Windows XP Service Pack 2 and later. The Firewall helps protect computers from unauthorized access (usually from viruses, worms, and people with malicious or negligent intents). If the computer resides on a safe network, there is usually little potential for damage as long as the Firewall is turned off for a short period of time. Check with the Network Administrator to ensure it is safe to turn off the Firewall temporarily. You will turn the Firewall back on in section 5, titled “Restore Windows Security,” on page 7.

To turn off the Windows Firewall, follow the steps below:

a. Click on the Windows Start button, select the Control Panel, and finally click on Windows Firewall.

b. In the General tab, select the “Off (not recommended)” radio button (refer to Image 1).



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Image 1: Temporarily turn off the Windows Firewall to allow remote access to the OPC Server computer.

2. Setup mutual User Account recognition

To enable both computers to properly recognize User Accounts, it is necessary to ensure that User Accounts are recognized on both the OPC Client and Server computers. This includes all the User Accounts that will require OPC access.

2.1 Adding User Accounts

Ensure that both computers have access to the same User Name and Password combinations. User Names and Passwords must match on all computers that require OPC access. Note:

- A User Account must have a User Name and Password. It is not possible to establish communication if a User Account does not have a Password.
- When using Windows Workgroups, each computer must have a complete list of all User Accounts and Passwords.
- When using a single Windows Domain, User Accounts are properly synchronized by the Domain controller.
- When using multiple Windows Domains, you will either have to establish a Trust between the Domains, or add a Local User Account to the affected computers. (Refer to http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/deploy/dgbe_sec_ztsn.mspx?mfr=true about establishing a Domain Trust.)

2.2 Local Users Authenticate as Themselves

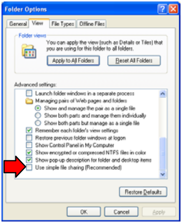
In Windows XP and Windows Vista, there is another setting that you should modify. This is not necessary in Windows 2000 or earlier. Simple File Sharing is always turned on in Windows XP Home Edition-based computers. By default, the Simple File Sharing user interface is turned on in Windows XP Professional-based computers that are joined to a workgroup. Windows XP Professional-based computers that are joined to a domain use only the classic file sharing and security interface. Simple File Sharing forces every remote user to Authenticate as the Guest User Account. This will not enable you to establish proper security. There are two ways to turn this option off. Either way will work. I personally prefer the second method because there are more security options that Windows exposes to me.

Method 1: Turning off Simple File Sharing

a. Double-click "My Computer" on the desktop.

b. On the Tools menu, click Folder Options.

c. Click the View tab, and then clear the "Use Simple File Sharing (Recommended)" check box to turn off Simple File Sharing (refer to Image 2).



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

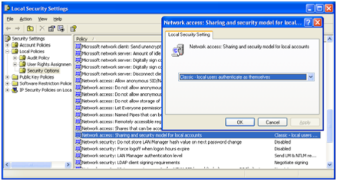
□ Launch folder windows in a separate process
Managing pairs of Web pages and folders
● Show and manage the pair as a single file
○ Show both parts and manage them individually
○ Show both parts but manage as a single file
☑ Remember each folder's view settings
□ Restore previous folder windows at logon
□ Show Control Panel in My Computer
☑ Show encrypted or compressed NTFS files in color
☑ Show pop-up description for folder and desktop items
□ Use simple file sharing (Recommended)

Image 2: Turn off "Simple File Sharing" to enable Windows to Authenticate User Accounts properly.

Method 2: Set Local Security Policies

- Click on the Windows Start button, and then select Control Panel, Administrative Tools, and Local Security Policy. If you can't see Administrative Tools in the Control Panel, simply select Classic View in the Control Panel. As an alternative to all of this, click on the Windows Start button; select the Run menu option, and type "secpol.msc".

- In the tree control, navigate to Security Settings, Local Policies, and finally select the Security Options folder (refer to Image 3).
- Find the “Network access: Sharing and security model for local accounts” option and set it to “Classic – local users authenticate as themselves”.



Network access: Sharing and security model for local...

Local Security Setting

Network access: Sharing and security model for local accounts

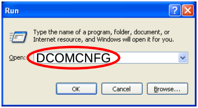
Classic - local users authenticate as themselves

Image 3: Appropriate OPC security for requires Windows to enable local users to authenticate as themselves rather than as Guest.

3. Configure System-Wide DCOM settings

OPC specifications that precede OPC Unified Architecture (OPC UA) depend on Microsoft’s DCOM for the data transportation. Consequently, you must configure DCOM settings properly. It is possible to configure the default system-wide DCOM settings, as well for a specific OPC server.

The system-wide changes affect all Windows applications that use DCOM, including OPC application. In addition, since OPC Client applications do not have their own DCOM settings, they are affected by changes to the default DCOM configuration. To make the necessary changes, follow the steps below:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: DCOMCNFG

Image 4: Use DCOMCNFG to

a. Click on the Windows Start button, and select the Run menu option (refer to Image 4).

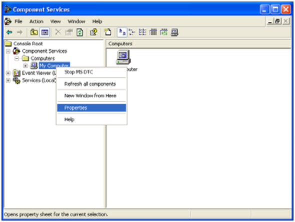
b. In the Run dialog box, type "DCOMCNFG" to initiate the DCOM configuration process, and click the OK button. The Component Services window will appear (refer to Image 5).

modify DCOM settings on the computer.

c. Once in the Component Services window (which is initiated by DCOMCNFG as above), navigate inside the Console Root folder to the Component Services folder, then to the Computers folder. Finally, you will see the My Computer tree control inside the Computers folder.

d. Right-click on My Computer. Note that this is not the “My Computer” icon on your desktop; rather it is the “My Computer” tree control in the Console Services application.

e. Select the Properties option.



Opens property sheet for the current selection.

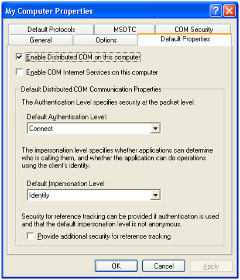
Image 5: Right-click on the My Computer tree control to access the computer's default DCOM settings

3.1 Default Properties

In the Default Properties tab, ensure that three specific options are set as follows (refer to Image 6):

a. Check the “Enable Distributed COM on this computer” menu option. Note that you will have to reboot the computer if you make changes to this checkbox.

b. Set the “Default Authentication Level” to Connect. It is possible to use other settings in the list, but the “Connect” option is the minimum level of security that you should consider.


My Computer Properties

☑ 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.

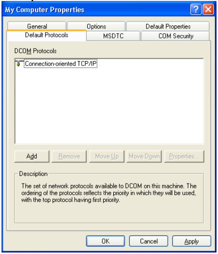
Default Impersonation Level: Identify

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

Image 6: The Default Properties tab enables users to turn DCOM on or off, as well as set the Authentication and Impersonation configuration.

c. Set the “Default Impersonation Level” to Identify.Default Protocols


My Computer Properties

DCOM Protocols

Connection-oriented TCP/IP

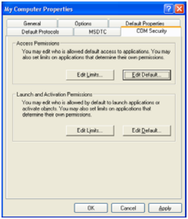
Description

The set of network protocols available to DCOM on this machine. The ordering of the protocols reflects the priority in which they will be used, with the top protocol having first priority.

Image 7: In the Default Protocols tab, set the DCOM Protocols to "Connection-Oriented TCP/IP".

In the Default Protocols tab (refer to Image 7), set the DCOM protocols to “Connection-Oriented TCP/IP”. OPC communication only requires “Connection-Oriented TCP/IP”, so it is possible to delete the rest of DCOM protocols. However, if these protocols are indeed required for non-OPC applications, you can leave them there. The only consequence is that timeouts may take a little longer to reach.

3.2 COM Security



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

Image 8: Use the COM Security tab to set the default Access Control Lists (ACLs).

Windows uses the COM Security tab (refer to Image 8) to set the system-wide Access Control List (ACL) for all objects. The ACLs are included for Launch/Activation (ability to start an application), and Access (ability to exchange data with an application). Note that on some systems, the “Edit Limits” buttons are not available.

To add the right permissions, follow the steps below:

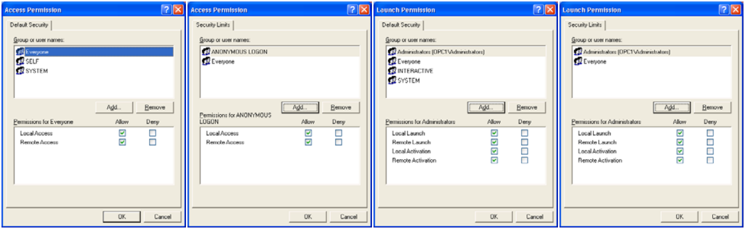
a. In the Access Permissions group, click the “Edit Default...” button (refer to Image 9). Add “Everyone” to the list of “Group or user names”. Click the OK button.

b. In the Access Permissions group, click the “Edit Limits...” button (refer to Image 9). Add “Anonymous Logon” (required for OPCEnum) and “Everyone” to the list of “Group or user names”. Click the OK button.

c. In the Launch and Activation Permissions group, click the “Edit Default...” button (refer to Image 9). Add “Everyone” to the list of “Group or user names”. Click the OK button.

d. In the Launch and Activation Permissions group, click the “Edit Limits...” button (refer to

Image 9). Add “Everyone” to the list of “Group or user names”. Click the OK button.



Access Permission — Default Security

Group or user names:
- Everyone
- SELF
- SYSTEM

Permissions for Everyone

	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Access Permission — Security Limits

Group or user names:
- ANONYMOUS LOGON
- Everyone

Permissions for ANONYMOUS LOGON

	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Launch Permission — Default Security

Group or user names:
- Administrators (OPC1\Administrators)
- Everyone
- INTERACTIVE
- SYSTEM

Permissions for Administrators

	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Launch Permission — Security Limits

Group or user names:
- Administrators (OPC1\Administrators)
- Everyone

Permissions for Administrators

	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Image 9: Add Everyone and Anonymous Logon to the Launch and Access Permissions. Once communication is working properly, remember to return to this setup to ensure you comply with corporate security policies.

4. Configure Server Specific DCOM settings

Once the system-wide DCOM settings are properly configured, turn attention to the server-specific DCOM settings. These settings will eventually be different for every OPC Server. To change these settings, begin by:

a. Click on the Windows Start button, and select the Run menu option (refer to Image 4).

b. In the Run dialog box, type "DCOMCNFG" to initiate the DCOM configuration process, and click the OK button. The Component Services window will appear (refer to Image 10).

c. Once in the Component Services window (which is initiated by DCOMCNFG as above), navigate inside the Console Root folder to the Component Services folder, then to the Computers folder, expand My Computer, finally click on the DCOM Config folder.

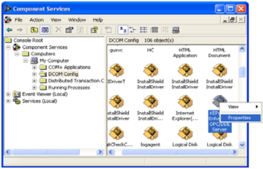
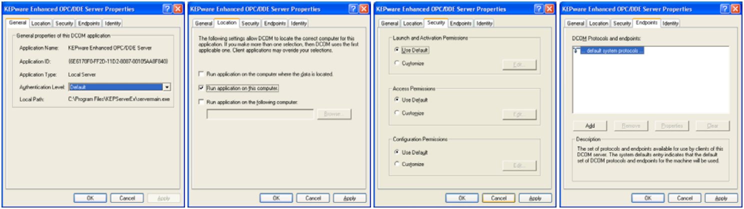


Image 10: Server-specific DCOM settings are located in the DCOM Config folder.

d. In the list of objects in the right window pane, find the OPC Server to configure and right-click on it. Select the Properties option.

In the OPC-Server specific settings, only the Identity tab needs to change from the default settings. The rest of the tabs (refer to Image 11) can refer to the default configuration that was set in section 3 (Configure System-Wide DCOM settings) on page 3.



General properties of this DCOM application

Application Name: KEPware Enhanced OPC/DDE Server

Application ID: {6E6170F0-FF2D-11D2-8087-00105AA8F840}

Application Type: Local Server

Authentication Level: Default

Local Path: C:\Program Files\KEPServerEx\servermain.exe

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:

Launch and Activation Permissions

● Use Default

○ Customize

Access Permissions

● Use Default

○ Customize

Configuration Permissions

● Use Default

○ Customize

DCOM Protocols and endpoints:

... default system protocols ...

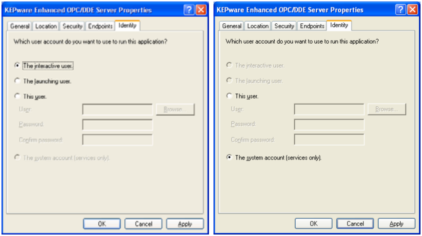
Description

The set of protocols and endpoints available for use by clients of this DCOM server. The system defaults entry indicates that the default set of DCOM protocols and endpoints for the machine will be used.

Image 11: The settings in the first four tabs (General, Location, Security, and Endpoints) should remain at their default settings as shown above.

You must pay special attention to the Identity tab. The Identity tab will look like one of the two screen captions in Image 12 below.

The 4 (four) Identity options are:



KEPware Enhanced OPC/DDE Server Properties

General | Location | Security | Endpoints | Identity

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

● The interactive user.
○ The launching user.
○ This user.
User: Browse...
Password:
Confirm password:
○ The system account (services only).

OK | Cancel | Apply

KEPware Enhanced OPC/DDE Server Properties

General | Location | Security | Endpoints | Identity

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

○ The interactive user.
○ The launching user.
○ This user.
User: Browse...
Password:
Confirm password:
● The system account (services only).

OK | Cancel | Apply

Image 12: Use the Identity Tab to set the OPC Server's identity. Typically, OPC Server Identity should be set to "The system account (services only)".

- ***The interactive user***: The OPC Server will assume the identity of the Interactive User. This is the person who is currently logged on and using the computer on which the OPC Server resides. Note that someone must be logged on. If no one is logged on to the computer, the OPC Server will fail to launch. In addition, if someone is currently logged on, the OPC Server will shutdown as soon as the person logs off. Last, in the case of a reboot, the OPC Server will not launch until someone logs on. Consequently, this is typically a poor setting for OPC Servers. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly.

- ***The launching user***: The OPC Server will take the identity of the User Account that launched it. With this setting, the Operating System will attempt to initiate a new instance for every Launching User. There are three general problems with this setting. The first problem is that some OPC Servers will only allow a single instance to execute. Consequently, the second Launching User will be unable to make the connection because an instance of the OPC Server is already running on the computer. The second problem occurs when the OPC Server vendor allows more than one instance of the OPC Server to execute concurrently. In this case, the computer on which the OPC Server resides will have multiple copies of the OPC Server executing concurrently, which will consume a significant portion of the computer resources and might have an adverse affect on the computer's performance. In addition, some system resources might be unavailable to any instances of the OPC Server that follow the first. For example, the first Launching User will be able to connect to a serial port, while every other Launching User will simply receive Bad Quality data. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly. Last, the Launching User must have Administrative rights on the OPC Server computer. They can not be configured as a “Limited” user.

- ***This user***: The OPC Server will take the identity of a specific User Account. This setting might be required when the OPC Server is tightly coupled with the underlying data source. In this case, the OPC Server must assume a specific Identity to exchange data with the data source. However, since the OPC Server uses a specific User Account, it is possible that the computer running the OPC Client does not recognize the OPC Server’s User Account. In this case, all callbacks will fail and all OPC data Subscriptions (asynchronous data updates) will fail. If this is indeed the case, you will have to add the OPC Server account on the computer running the OPC Client application. Various DCS vendors require this setting for their OPC Server. OPCTI does not recommend that you use this setting unless the OPC Server vendor specifies this setting explicitly.

- ***The system account (services only)***: The OPC Server will take the identity of the Operating System (or System for short). This is typically the desired setting for the OPC Server as the System Account is recognized by all computers on the Workgroup or Domain. In addition, no one needs to be logged on the computer, so the OPC Server can execute in an unattended environment. OPCTI recommends configuring the Identity of the OPC Server with this setting, unless the OPC Server vendor specifies a different setting explicitly. Note that Windows disables this option if the OPC Server is not setup to execute as a Windows Service. If this is the case, simply configure the OPC Server to execute as a service before configuring this setting.

5. Restore Windows Security

Once you establish the OPC Client/Server communication, it is important to secure the computers again. This includes (but is not limited to):

a. Turn on the Windows Firewall again. This will block all unauthorized network traffic. You will also need to provide exceptions on two main levels:

- Application level: specify which applications are able to respond to unsolicited requests.
- Port-and-protocol level: specify that the firewall should allow or deny traffic on a specific port for either TCP or UDP traffic.

b. Modify the Access Control Lists (ACLs) to allow and deny the required User Accounts. This can be accomplished either through the system-wide settings of DCOMCNFG, or in the server-specific settings. Remember that OPCEnum requires the “Anonymous Logon” access. You may wish to remove this access. The consequence of this action will simply be that OPC Users will be unable to browse for OPC Servers on the specific computer where Anonymous Logon access is not available. However, users will indeed be able to properly connect to and exchange data with the OPC Server.

We encourage you to complete your DCOM setup with this step. Integrators frequently establish OPC communication and don’t spend the necessary time to secure the computers again. This can lead to catastrophic results if network security is compromised due to a virus, worm, malicious intent, or simply unauthorized “experimentation” by well-meaning coworkers. Specific settings are discussed in a separate whitepaper.

6. Conclusion

OPC is powerful industrial communication standard. However, OPC relies on having DCOM work properly. Luckily, DCOM problems can usually be overcome with relatively simple configuration changes as documented in this whitepaper. To get a deeper understanding of OPC, DCOM, and the diagnosis of all common problems OPCTI highly recommends that you take time to get formal OPC training. This will enable you to structure your OPC knowledge to help you reduce your short and long-term project costs.

OPCTI also encourages you to provide us with feedback. Let us know about new problems and solutions that you found. We will pass these on to the rest of the OPC community, to help everyone get connected.

About the author: Randy Kondor is a Computer Engineer, and is the President of the OPC Training Institute, the world's largest OPC Training company. Since 1996, Randy has been vastly involved within the OPC industry and a strong supporter of the OPC Foundation. He continues to dedicate himself to spreading the OPC Foundation's message about system interoperability and inter-vendor cooperation.

Contact information:
Email: randy.kondor@opcti.com
Phone: +1-780-784-4444
Fax: +1-780-784-4445

OPC Training Institute

16420 – 89 Avenue

Edmonton, Alberta

Canada T5R 4R9

T 1-780-784-4444

F 1-780-784-4445

info@opcti.com

www.opcti.com