OPC and DCOM: 5 things you need to know (Windows 10)

Randy Kondor P.Eng.

January 2016

OPC™
TRAINING INSTITUTE

OPC and DCOM: 5 things you need to know (Windows 10)

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 ensure DCOM functions 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

OPC communication often uses 2 computers. One computer runs an OPC server (which connects directly to automation hardware such as a PLC, DCS, or RTU). A second computer runs an OPC client application (such as an HMI, Historian, etc.). To ensure successful communication, configure both computers as per this whitepaper. While tweaking these settings can further optimize and secure communication, beginners find it easier to first establish some communication and conduct optimization steps afterwards.

This whitepaper focuses on these operating systems:

- *Windows 8*
- *Windows 8.1*
- *Windows 10*
- *Windows 2012*
- *Windows 2012R2*
- *Windows Server 2016*

Steps for other Windows versions are almost identical, but options are often in different locations. Refer to the proper whitepaper for your version of Windows.

OPCTI has separate whitepapers for Windows XP and Windows 7-based systems.

1. Remove Windows Security

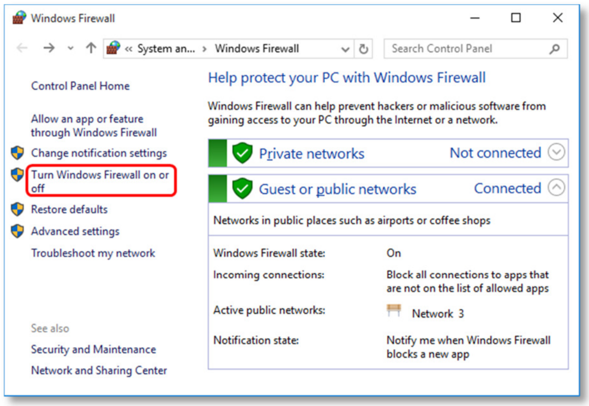
The first step to establish DCOM communication is to disable Windows Firewall, which Windows activates by default. Firewalls help protect computers from unauthorized access (usually from viruses, worms, and people with malicious or negligent intents). Check with the Network Administrator to ensure it is safe to turn off the Firewall temporarily. You will turn the Firewall back on in section 5, titled "Restore Windows Security," on page 8.

To deactivate Windows Firewall, follow the steps below:

a. In Search, type "firewall", and select "Windows Firewall".

b. Select "Turn Windows Firewall on or off". Note: Network policy settings might prevent you from making changes. In this case, refer to group or domain policies.

c. In "Customize Settings" select both radio buttons labeled "Turn off Windows Firewall", and click OK. Note: Microsoft does not recommend deactivating Windows Firewall, however, this step is only temporary and we will activate Windows Firewall later on.


Windows Firewall
« System an... › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

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

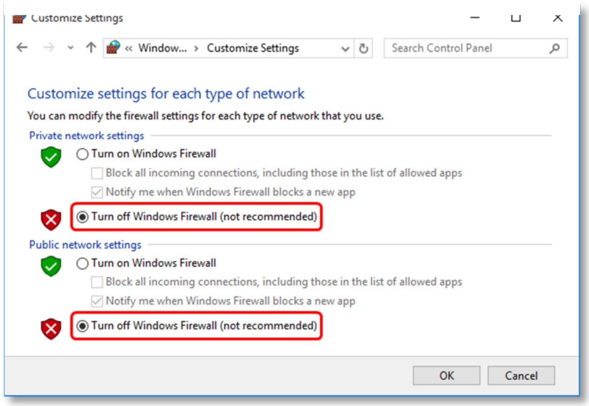
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network 3
Notification state:	Notify me when Windows Firewall blocks a new app

Image 1: Find Windows Firewall settings using Windows search



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Firewall blocks a new app
● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Firewall blocks a new app
● Turn off Windows Firewall (not recommended)

Image 2: Temporarily turn off Windows Firewall to allow remote access to this computer.

2. Setup mutual User account recognition

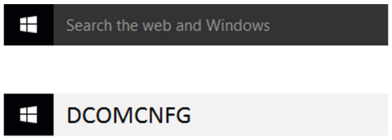
To enable both computers to properly recognize User accounts, it is necessary to ensure all affected computers recognize all user accounts requiring OPC access.

Ensure both computers have access to the same user name and password combinations. User names and passwords must match on all computers requiring OPC access. Notes:

- Each user account must have a password. Default settings do not allow establishing 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 each computer. Refer to Microsoft's documentation about establishing a Domain Trust for more information.

3. Configure System-Wide DCOM settings

OPC Classic specifications, which precede OPC Unified Architecture (OPC UA), depend on Microsoft's DCOM for data transportation. Consequently, you must configure DCOM settings properly. This whitepaper first configures default system-wide DCOM settings (i.e. for the entire computer), and subsequently directs you to modify each OPC server specifically.



DCOMCNFG

Image 3: Use Windows Search to execute DCOMCNFG.

System-wide DCOM changes affect all Windows applications using DCOM, including OPC applications. 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 changes, follow the steps below:

a. In Search, type "DCOMCNFG" (refer to Image 3). The Component Services window will appear (refer to Image 4).

b. In the Component Services window (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.

c. Right-click "My Computer". Note: this is not the "My Computer" icon on your desktop; rather it is the "My Computer" tree control in the Console Services application.

d. Select the Properties option (refer to Image 4).

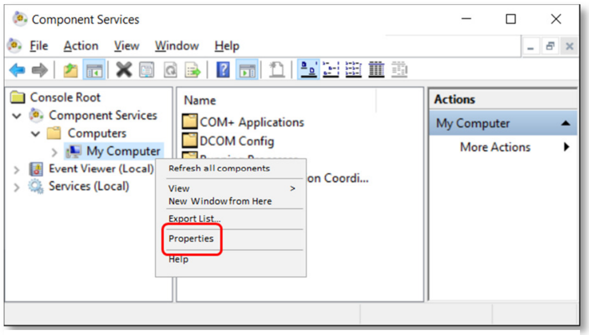


Image 4: Right-click "My Computer" to access the computer's default DCOM settings.

3.1 *Default Properties*

In the Default Properties tab, ensure to set the options below (refer to Image 5):

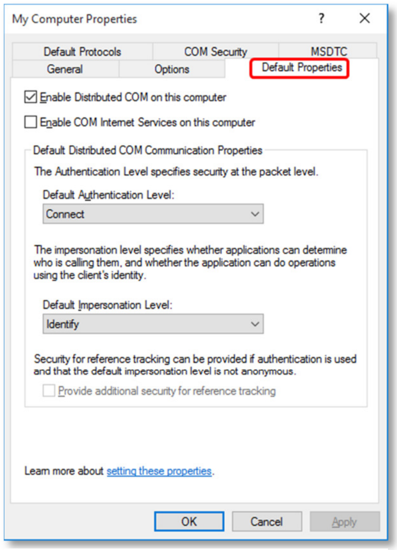
a. Check the "Enable Distributed COM on this computer" checkbox.

b. Uncheck "Enable COM Internet Services on this computer".

c. 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. Do not use "None".

d. Set the "Default Impersonation Level" to Identify. Setting this level to "Impersonate" or "Delegate" is also acceptable, but do not use "Anonymous".

OPC Training Institute's courses provide further in-depth explanations of all these settings and their effects on your connectivity and security. Nevertheless, following these instruction will ensure you will be able to establish connectivity.



☑ 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

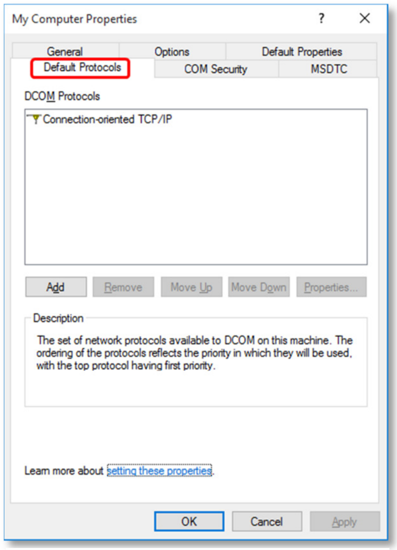
Learn more about setting these properties.

Image 5: The Default Properties tab enables users to turn DCOM on or off, as well as set the Authentication and Impersonation configuration.

3.2 Default Protocols

In the Default Protocols tab (refer to Image 6), 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.

As you work through this whitepaper, you may question the reason for each setting. OPC Training Institute's hands-on OPC workshops explain each step in detail. Consider attending these workshops either in-person or remote (online).



Connection-oriented TCP/IP

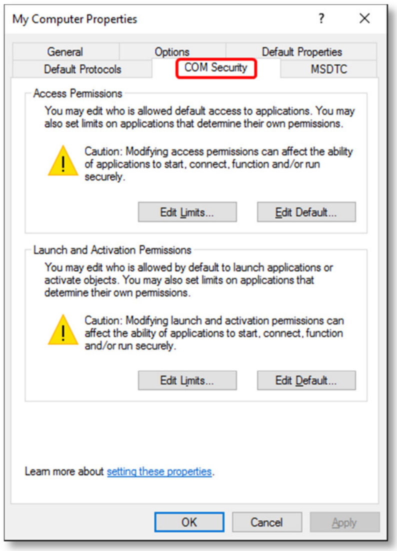
The set of network protocols available to DCOM on this machine. The ordering of the protocols reflects the priority in which they will be used, with the top protocol having first priority.

Learn more about setting these properties.

Image 6: In the Default Protocols tab, set the DCOM Protocols to "Connection-Oriented TCP/IP".

3.3 COM Security

Windows uses the COM Security tab (refer to Image 7) to set system-wide Access Control Lists (ACLs). ACLs are included for Launch/Activation (ability to start an application), and Access (ability to exchange data with an application). Administrators can also disable the "Edit Limits" buttons, so if this is the case, please contact OPC Training Institute.



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.

Image 7: Use the COM Security tab to set the default Access Control Lists (ACLs).

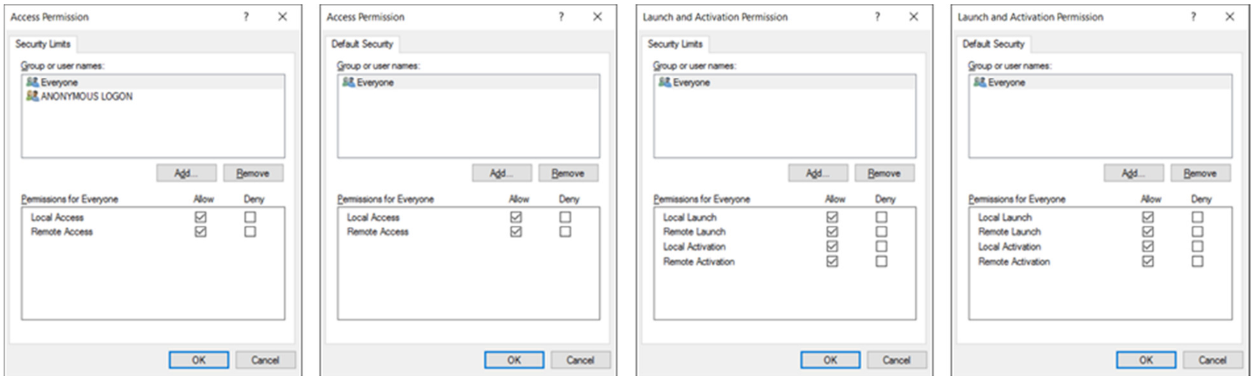
To add the right permissions, follow the steps below:

a. In the Access Permissions group, click the "Edit Limits…" button (refer to Image 8). Add "Everyone" and "Anonymous Logon" to the list of "Group or user names". Check all "Allow" permissions and click OK.

b. In the Access Permissions group, click the "Edit Default…" button (refer to Image 8). Add "Everyone" to the list of "Group or user names". Check all "Allow" permissions and click OK.

c. In the Launch and Activation Permissions group, click the "Edit Default…" button (refer to Image 8). Add "Everyone" to the list of "Group or user names". Check all "Allow" permissions and click OK.

d. In the Launch and Activation Permissions group, click the "Edit Limits…" button (refer to Image 8). Add "Everyone" to the list of "Group or user names". Check all "Allow" permissions and click OK.



Access Permission — Security Limits

Group or user names: Everyone; ANONYMOUS LOGON

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

Access Permission — Default Security

Group or user names: Everyone

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

Launch and Activation Permission — Security Limits

Group or user names: Everyone

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

Launch and Activation Permission — Default Security

Group or user names: Everyone

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

Image 8: Add Everyone to the Access Permissions. Add Everyone and Anonymous Logon to the Security Limits (Edit Limits) of 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

After configuring system-wide DCOM settings, turn attention to server-specific DCOM settings. Although these settings will eventually be different for every OPC server, use the guidelines below for initial configuration:

a. In the Component Services window, navigate inside the Console Root folder to the Component Services folder, then to the Computers folder, expand My Computer, and finally click on the "DCOM Config" folder.

b. In the list of objects in the right window pane, find the OPC Server to configure, right click it, and select Properties from the menu (refer to Image 9).

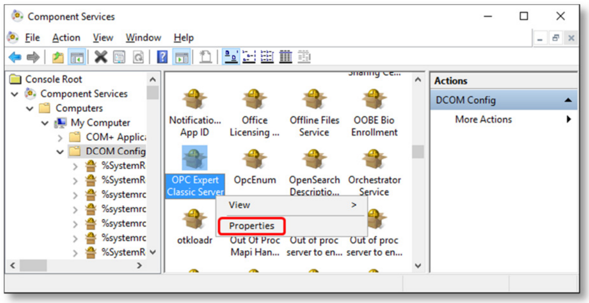
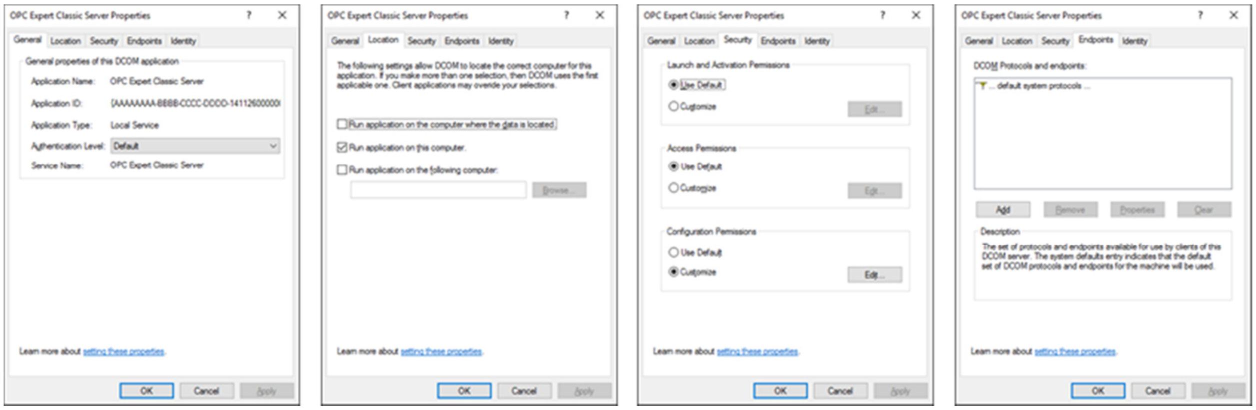


Image 9: Server-specific DCOM settings are located in the DCOM Config folder.

In the OPC-Server specific settings, only the Identity tab should potentially change from default settings. The rest of the tabs (refer to Image 10) can refer to the default configuration set in section 3 (Configure System-Wide DCOM settings).



OPC Expert Classic Server Properties — General

General properties of this DCOM application

Application Name: OPC Expert Classic Server
Application ID: {AAAAAAAA-BBBB-CCCC-DDDD-14112600000
Application Type: Local Service
Authentication Level: Default
Service Name: OPC Expert Classic Server

OPC Expert Classic Server Properties — Location

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 override your selections.

□ Run application on the computer where the data is located.
☑ Run application on this computer.
□ Run application on the following computer:

OPC Expert Classic Server Properties — Security

Launch and Activation Permissions: ● Use Default ○ Customize
Access Permissions: ● Use Default ○ Customize
Configuration Permissions: ○ Use Default ● Customize

OPC Expert Classic Server Properties — Endpoints

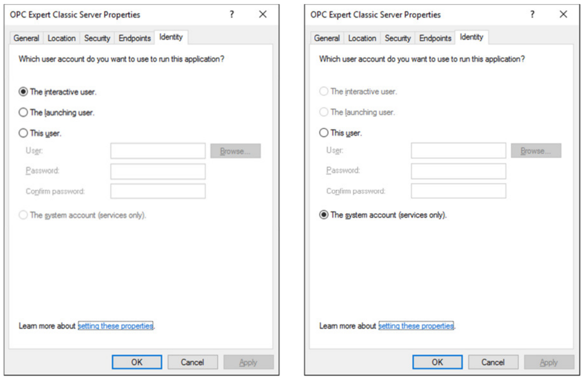
DCOM Protocols and endpoints: ... default system protocols ...

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.

Learn more about setting these properties.

Image 10: 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 below (refer to Image 11).



OPC Expert Classic 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:
Password:
Confirm password:
○ The system account (services only).

Learn more about setting these properties.

OPC Expert Classic 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:
Password:
Confirm password:
● The system account (services only).

Learn more about setting these properties.

Image 11: 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 four identity options are:

- ***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: *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 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 (i.e. started) it. With this setting, Windows 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. Last, the Launching User must have Administrative rights on the OPC Server computer; they can not be configured as a "Limited" user. OPCTI does not recommend this setting unless the OPC Server vendor specifies this setting explicitly.
- ***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 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 (i.e. "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, 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 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.

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. We discuss and configure specific settings in the hands-on classes (which you can find on www.OPCTI.com.

6. Additional Ideas

Configuring DCOM for OPC communication can be a daunting task, but the steps above will help you get your communication working efficiently. This section covers related concepts that are necessary for communication. For automated (and free) troubleshooting, download OPC Expert (www.OpcExpert.com).

6.1 Network Configuration

DCOM depends on a solid network infrastructure. To assure the success of your project, you must also ensure that basic networking is functioning properly, including the following:

- "Valid" IP address (an address such as 169.254.x.y is a typical sign of trouble)
- Connection to the right Windows Workgroup/Domain
- Unique computer name (ensure no other computer in the Workgroup/Domain has the same name)
- Connection between the OPC Client and Server computers (usually verified with Ping)

While the above bullets highlight basic network information, a proper network infrastructure also includes hardware such as routers, switches, firewalls, etc. However, these are outside the scope of this whitepaper, and the bullets above only highlight the most important aspects of network connectivity as it applies to DCOM.

6.2 OPC Tunneling

If you are unable to get DCOM working at your facility, you should consider the use of an OPC Tunneling product. As a group, these products enable OPC communication to occur without the use of DCOM. In effect, these products bypass DCOM (and DCOM configuration) altogether. These products are useful for two main reasons:

a. ***Troubleshooting***: OPC Tunneling products enable you to troubleshoot communication problems. If your communication fails with both DCOM and the OPC Tunnel, you should first investigate the network connection itself. It could be that you have a problem with the IP addresses, or that a firewall might be blocking the data transfer, etc. In all these cases, basic network issues will stop all communication. In other cases, the OPC Tunnel might work, while the DCOM communication still fails. For instance, you may not have properly synchronized the User Names and Passwords in User accounts, you might be using different Windows Domains, or Access Control List (ACL) permissions might be configured incorrectly. In these cases, you should immediately investigate the DCOM settings as you have now verified that the underlying network infrastructure is relatively sound.

b. ***Overcoming DCOM***: There are some rare cases where DCOM is simply not appropriate. For instance, you may require communication over low bandwidth networks, using unreliable connections, or through firewalls that only provide a single open port. In these cases, DCOM may not be an appropriate choice for OPC communication and the OPC Tunnel could enable OPC communication to take place easily.

Use OPC Expert (www.OpcExpert.com) to establish such a tunnel. You can do this for free and there are several helpful videos on the OPC Expert website.

7. 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.

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 in OPC technology 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. Find Randy on LinkedIn.com and OPCTI.com.

OPC Training Institute
T 1-780-784-4444
F 1-780-784-4445
www.opcti.com