OPC & DCOM Troubleshooting: Quick Start Guide

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

January 2008

OPC & DCOM Troubleshooting: Quick Start Guide

OPC technology provides an interoperable, reliable and secure communication platform. However, OPC relies on a well-configured DCOM infrastructure. This includes setting Windows security and firewalls, access control lists, server identities, etc. Consequently, OPC may not always work as expected and the initial troubleshooting can be difficult because each problem masks itself with a variety of symptoms. This whitepaper discusses the 5 most common problems, their causes, and how to resolve them.

A well structured approach can quickly solve the following 5 common problems:

1. Can't browse OPC servers on remote PC
2. Can't connect to OPC Server on remote PC
3. All items show Bad Quality
4. OPC Client doesn't receive data updates
5. PC with OPC Server has high CPU Usage

After identifying the specific problem you are having, this whitepaper describes their typical causes, and the required steps to solve them.

1. Can't browse OPC servers on remote PC

The first challenge Users encounter with OPC is Browsing for available OPC Servers on a remote PC. Browsing is the process whereby the OPC Client application is able to view the OPC Servers that are installed on the remote PC. When the OPC Client performs a Browse, it actually connects to a copy of OpcEnum, which resides on the remote PC, and retrieves the list of available OPC Servers. This list includes the ProgID (human friendly name) and the GUID (the numerical identification) of each OPC Server. At this point, the OPC Client does not actually connect to the OPC Servers directly. Consequently, the retrieval of the list is independent of the state of each OPC Server and whether it is operational or not.

A failure to browse for OPC Servers is a direct result from the inability to properly establish communication with the copy of OpcEnum on the remote PC. There are several possible factors for this, and they are listed below.

1.1 OpcEnum is not installed

The OPC Foundation is responsible for the creation and maintenance of OpcEnum. OPC Foundation members can obtain OpcEnum for free directly from the OPC Foundation. OpcEnum is typically installed when you install an OPC Client or OPC Server; however, this is not always the case. Thus, it is possible that a computer does not have a local copy of OpcEnum installed.

OpcEnum is only able to browse for OPC Servers on the machine on which it is running. Therefore, OpcEnum cannot perform a Browse on remote PC. Thus, even if a copy of OpcEnum is present on your own PC, you will not be able to browse the remote PC.

Use Windows Explorer to find out if OpcEnum is installed on the PC you wish to browse. The file is called OpcEnum.exe. If OpcEnum isn't installed, you will need to install it.

1.2 OpcEnum is disabled

Even if OpcEnum is installed on the remote PC, it must be able to execute, otherwise, communication will fail. If the "Startup Type" for OpcEnum is set to "Disabled" then Windows will be unable to start OpcEnum. Thus, you will have to enable OpcEnum.

To check the Startup Type for OpcEnum follow the steps below:

- Click Start, and then click Control Panel. Click Performance and Maintenance, click Administrative Tools, and then double-click Computer Management. The Computer Management window for the local computer is displayed. "Computer Management (Local)" is displayed at the root of the console tree.
- In the console tree, expand Services and Applications, and click on the Services container.
- Look for OpcEnum in the right-hand window pane. If the Startup Type is set to "Disabled", then OpcEnum is indeed disabled and you will have to enable it (below). If OpcEnum is not on the list, then it has likely not been installed, so you should go back to step "1.1 OpcEnum is not installed". If the Startup Type for OpcEnum is already set to either Manual or Automatic, then skip to step "1.3 Anonymous Logon access not given".

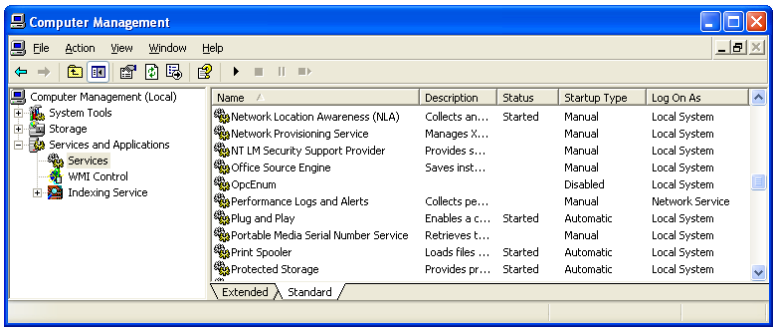

Image 1: The Services panel indicates that the OpcEnum services is Disabled.

- To enable OpcEnum, right click on OpcEnum, and select the Properties option. In the Startup Type Combo Box, select Manual. While it is also possible to select the Automatic setting, I recommend that you select Manual so that OpcEnum will only execute when required.

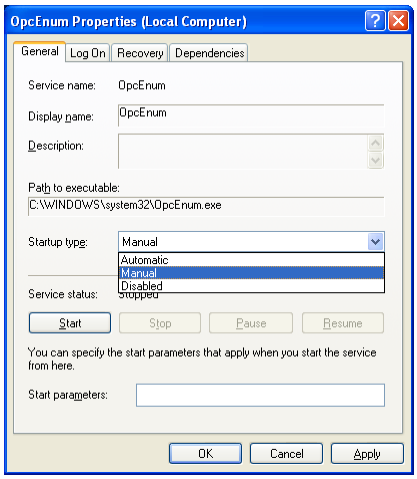

Image 2: Set the Startup Type for OpcEnum to Manual.

Now that the Startup Type for OpcEnum is properly set, try to browse the remote computer again. If it still doesn't work, move to the next step.

1.3 Anonymous Logon access not given

OpcEnum requires Anonymous Logon access to work properly. If you do not provide this access, no one will be able to connect to OpcEnum and browse the PC. It is possible that this access was overlooked during the setup. Thus, you will have to add Anonymous Logon access to the default Windows COM Security. I described this in detail in my whitepaper titled "OPC and DCOM: 5 things you need to know" (visit www.opcti.com for a copy). Specifically, look for section "3.3 COM Security".

2. Can't connect to OPC Server on remote PC

The act of connecting to a remote OPC Server is actually independent of the ability to browse for OPC Servers on the remote PC. For example, it is possible to connect to a remote OPC Server even though the remote copy of OpcEnum is not even installed. In any case, if you know the identity of the remote OPC Server (either through a remote browse or by simply "knowing" the right GUID), but are still unable to establish the OPC connection, there can be several factors that could cause a failure.

2.1 OPC Server is disabled

If the OPC Server is set to run as a Windows Service, it is possible that it was disabled. To check if this is the case, follow the same steps I covered in section "1.2 OpcEnum is disabled". Set the Startup Type to the setting that the OPC Server vendor recommends.

2.2 User Authentication Issues

It is possible that you are not authenticated on the remote PC. Authentication is the process of verifying that you are the user that you claim to be. Windows compare the User Name with the stored password. If Windows does not recognize your User Account, it will reject your entry immediately without attempting to make a connection to the OPC Server. This can happen under at least a couple of circumstances.

a) ***The User Account does not exist on remote PC:*** If you are attempting entry from one Windows Domain to another, then you will either have to establish a Domain Trust, or add your User Account to both Windows Domains. If you are using a Workgroup, then you will have to add the User Account to the remote PC. Ensure that you use the same spelling for the user name (but capitalization does not matter). As well, ensure you use the same spelling and capitalization for the password. Note that if you are using a single Windows Domain, this problem will not happen.

b) ***Simple File Sharing is turned on:*** Simple File Sharing strips the username and password from requests coming in from remote computers. Thus, users will not be able to authenticate properly. To learn more about how this feature affects OPC, and how to turn this feature off, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "2.2 Local Users Authenticate as Themselves".

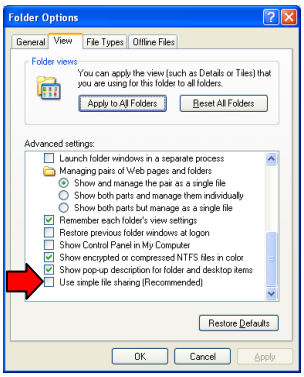

Image 3: Turn off "Simple File Sharing" to enable Windows to Authenticate User Accounts properly.

2.3 Access Control List issues

After authenticating an incoming User Account, the Operating System then checks whether or not the User Account is allowed to Launch and/or Access the OPC Server. This is done with the use of an Access Control List (ACL). The ACL for each application includes information on the User Accounts that are permitted or denied from taking specific actions. Thus, it is possible that the Operating System will deny access either because the ACL does not include the necessary permissions for a User Account, or because that User Account is explicitly denied from receiving launch/access rights. If either of these is the case, you must change the ACL for the OPC Server. To learn more about how the ACL affects OPC Servers and how to set it properly, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "3.3 COM Security".

2.4 OPC Server Identity issues

Access to OPC Servers is governed by the ACL. However, you must also match the OPC Server Identity with the business situation at hand. To learn more about the OPC Server Identity, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "4. Configure Server Specific DCOM settings". When you understand the OPC Server Identity settings, refer to the bullets below to diagnose the connection problem you are having.

- ***Interactive User:*** The OPC Server Identity is set to Interactive User but there is no Interactive User. In this case, the Operating System will be unable to launch the OPC Server because no one is logged in the computer. If this setting is actually correct, you must ensure that someone is logged in to Windows.
- ***Launching User:*** The OPC Server Identity is set to "Launching user" and someone is already connected to the OPC Server. If your server only supports a single instance at a time, and someone is already connected to the OPC Server, then the second person will be unable to establish a connection. Once the first person disconnects, the second person will be able to connect. If this setting is actually correct, you must ensure that no one is connected to the OPC Server.
- ***This User:*** The OPC Server Identity is set to "This user" and the specific User Account was deleted after setup. In this case, the OPC Server will fail to launch because the User Account under which it must execute is no longer valid. If this setting is desirable, then you must ensure that the OPC Server uses a valid User Account.

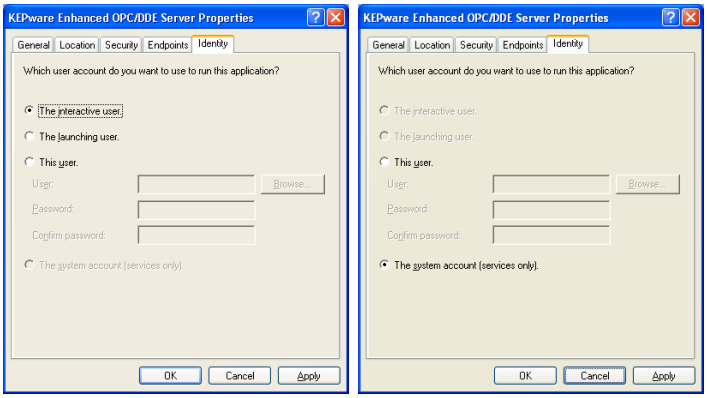

Image 4: Use the Identity Tab to set the OPC Server's identity. Typically, OPC Server Identity should be set to "The system account (services only)".

In general, I do not recommend any of the settings above due to the problems that they cause. Instead, I recommend that you use "The system account (services only)" setting, unless your OPC vendor specifies otherwise.

3. All items show Bad Quality

When you establish a connection with an OPC Server, you know that the remote PC recognizes your User Account and that you have the proper permissions to access the OPC Server. This also means that you have established synchronous communication with the OPC Server and can poll the OPC Server for data.

If all the items in the OPC Server indicate that they have a bad quality, it could be due to a couple of factors as listed below. Ensure you investigate them in order.

a) The data in the OPC Server is actually bad. In other words, the OPC Server is truly failing to receive data from its data source. There are various reasons for this, but in general, it could be as simple as the OPC Server is not connected to the PLC. To find out if this is the case, simply issue a synchronous Device Read. This type of read will force the OPC Server to retrieve the latest value from its data source. If the OPC Server still returns a bad value, then you should investigate the communication between the OPC Server and its data source.

b) The OPC Client is subscribed to updates, but callbacks are failing. If this is the case, proceed to section "4. OPC Client doesn't receive data updates".

By following the steps above you will ensure that the OPC Server is receiving data properly. If this isn't the case, no amount of Windows security configuration will help you get values as there is simply no data to retrieve.

4. OPC Client doesn't receive data updates

OPC Client applications often fail to receive updates due to a security configuration issues. However, before you conclude that data updates are the cause of the failure, refer to section "3. All items show Bad Quality" to ensure that the OPC Server is actually receiving data properly. Once you confirm that the OPC Server is indeed receiving data, you should begin to suspect that unsolicited data updates from the OPC Server are failing.

OPC supports a report-by-exception mechanism whereby the OPC Server sends data updates to the OPC Client whenever the data changes. OPC terminology refers to this mechanism as "subscription." OPC Servers are able to achieve subscription updates through the use of asynchronous callbacks. In other words, when the OPC Server detects a change in the data, it immediately "calls" the client back with the data update. This is an asynchronous mechanism because the OPC Client does not know when the OPC Server will send the data. However, if you don't set the security settings properly, these data updates will fail. OPC Client applications typically indicate this failure by setting the Quality value of an item to "Bad."

To find out if data updates from the OPC Server are failing, try to make a synchronous read from the OPC Server. If a proper data value suddenly appears, then you can be sure that asynchronous callbacks are failing, which can be due to any of the causes below.

4.1 Firewall

If the OPC Client PC is behind a (hardware or software) firewall, callbacks may fail to arrive at their destination. While the OPC Client will be able to make outgoing OPC calls, callbacks from the OPC Server may be blocked by the firewall. To learn more about the Windows Firewall and how to disable it, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "1. Remove Windows Security".

Image 5: Temporarily turn off the Windows Firewall to allow remote access to the OPC Server computer.

4.2 Authentication failure

Once a callback reaches the OPC Client PC, the Operating System will attempt to authenticate the arriving User Name and Password combination with its existing list. Windows will reject this combination for various reasons as below.

4.2.1 User Name and Password combination

It is imperative that both the User Name and Password are recognized on both the OPC Client and Server PCs. In the case of callbacks, it is possible that the User Name and Passwords on one PC do not match the other PC. You must carefully ensure that all combinations match on both PCs.

4.2.2 Guest Only

The default setting in Windows XP and later when using Workgroups is to force local users to authenticate as Guest. This is also known as Simple File Sharing. This default setting will not enable you to get the necessary authentication level working. Thus, you will have to turn this option off. To learn more about modifying network access, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "2.2 Local Users Authenticate as Themselves".

4.2.3 OPC Server Identity issues

Callbacks take the identity of the OPC Server. This identity is governed by the OPC Server Identity setting. To learn more about the OPC Server Identity, refer to my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "4. Configure Server Specific DCOM settings". When you understand the OPC Server Identity settings, refer to the bullets below to diagnose the connection problem you are having.

- ***Interactive User:*** The OPC Server Identity is set to Interactive User but the Interactive User is not known to the OPC Client PC. In case, the OPC Client PC does not recognize the User Account of the person who is currently logged on the OPC Server PC. Consequently, the OPC Client PC rejects the callback because authentication fails. If this setting is necessary, you will have to add the User Account of this person to the OPC Client PC. It is also possible that this User Account does not have access rights to the OPC Client PC, or that their User Account is explicitly denied access in the ACL of the system-wide DCOM settings.
- ***This User:*** The OPC Server Identity is set to "This user" and the OPC Client PC does not recognize this specific User Account. To deal with this issue, refer to the "Interactive User" setting above.
- ***The system account (services only)***: The OPC Server Identity is set to the System account, but System is denied remote access. In this case, simply follow the guidelines I indicated in my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "3. Configure System-Wide DCOM settings".

In general, I recommend that you use "The system account (services only)" setting, unless your OPC vendor specifies otherwise.

4.3 Access Control List issues

Once Windows authenticates the User Account that initiated the callback, it will check the access rights of the User Account in the OPC Client's Access Control List (ACL). However, you will recall that an OPC Client application does not have its own ACL; consequently, it refers back to the System-Wide DCOM settings. In this case, simply follow the guidelines I indicated in my whitepaper titled "OPC and DCOM: 5 things you need to know." Specifically, look for section "3. Configure System-Wide DCOM settings".

5. PC with OPC Server has high CPU Usage

Sometimes you may notice that the CPU of the OPC Server PC is much busier than you believe to be necessary. I did not write specific percent usage values because they are rather situational. In other words, only you can decide whether the CPU load is high or not. Nevertheless, if you believe that a load is too high, it is worth an investigation.

If the OPC Client application seems to be receiving data updates properly, have a closer look at how the OPC Client is receiving data updates:

- OPC Client issues synchronous reads only: In this case, the OPC Client is negating any optimization that the OPC Server might have, which will likely cause the OPC Server to demand more CPU cycles from the PC than would be required otherwise. Find out how to change these calls to asynchronous subscriptions instead. This change could significantly reduce the load on your OPC Server PC because you will enable the OPC Server to properly optimize its operation. Note that integrators often select synchronous reading methods simply because they are unable to get asynchronous subscriptions to work. This is often due to Windows security configuration. If this is indeed the case, follow the steps I outlined in section "4. OPC Client doesn't receive data updates".

- OPC Client issues device reads: In this case, the OPC Client is constantly asking the OPC Server to bypass its own built-in data exchange optimization and retrieve values directly from the device/PLC. This can slow the OPC Server down significantly. If this is the case, check into changing all reading calls to Cache instead of Device reads.
- OPC Client issues asynchronous reads: In this case, you should suspect that the OPC Server is not properly optimized and the cause likely has nothing to do with OPC communication. Instead, you should suspect the communication between the OPC Server and its data source. This deserves a call to the OPC Server vendor. Let them know about your concern, and ask them for help in optimizing your communication.

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