0x800706BA DCOM Error

OPC Training Institute

OPC Training Institute
Tel: 1-780-784-4444 | Fax: 1-780-784-4445
Web: www.opcti.com | Email: info@opcti.com

Cause

The 0x800706BA DCOM error appears in the OPC Client application when the OPC Client "believes" that it has a live connection to the OPC Server, but truly does not. This can happen under several conditions including:

- The OPC Client application launched the OPC Server successfully, but due to lack of permissions (DCOM or otherwise), the OPC Client can't access the OPC Server for data. In this case, the OPC Server might actually be running, but not accessible to the OPC Client.
- The OPC Server was initially running, but access has since been terminated. For example, the server was shutdown.
- The OPC Client PC is trying to create a group, but the OPC Client PC's Firewall is on.

DCOM Error 0x800706BA is only slightly different from DCOM Error 0x80040202 in that the OPC Client is typically unable to establish ANY communication with the OPC Server (even though it successfully launched it initially). In DCOM Error 0x80040202, the OPC Client is indeed able to establish Synchronous communication with the OPC Server.

Symptoms

When an OPC Client application is unable to receive callbacks from an OPC Server, users will notice at least three symptoms:

1. The OPC Client application will fail to create an OPC Group altogether.
2. The OPC Client application will not be able to show data updates. Instead, data values will remain unchanged.
3. The OPC Server will show as running on the OPC Server PC, but the OPC Client application will be unable to connect to the OPC Server.

Background

In DCOM Error 0x800706BA, the OPC Server suddenly becomes unavailable to the OPC Client (or simply disconnected from the OPC Client application). This can happen due to any of the following factors:

- OPC Server has shutdown without informing the OPC Client application. This shutdown could be due to a user that ends the OPC Server's Windows process (using Task Manager) or a "bug" in the OPC Server software that caused it to "crash".

- OPC Server becomes physically disconnected from the OPC Client application. For instance, someone disconnects a network cable, or a network device (such as a hub, switch, router, etc) fails.
- The OPC Client application is suddenly unable to receive callbacks from the OPC Server due to a change in its own Windows configuration. For example, someone might turn on the Windows Firewall, enables Simple File Sharing, changes the Security Limits of the DCOM Access Permissions.

OPC supports a report-by-exception (RBX) mechanism whereby the OPC Server sends data updates to the OPC Client (such as an HMI, Historian, APC, ERP, etc.) whenever the data changes (also known as "on data change"). 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".

Callbacks force an OPC Server to actively establish a connection with an OPC Client. In a sense, the OPC Server becomes a Client and the Client becomes a Server.

Test

One simple test to determine whether or not a callback is failing is to force the OPC Client to issue a "Synchronous Cache Read" or a "Synchronous Device Read." If either one of these return values with "Good" quality, then the lack of data updates is likely due to the OPC Server being unable to send callbacks to the OPC Client application.

However, if you determine that the OPC Client application is indeed able to launch the OPC Server, but is unable to read values from it (even Synchronous), then it is likely that the User Account that is running the OPC Client application does not have sufficient permissions to access the OPC Server. In this case, you should inspect DCOM Access Permissions on the OPC Server PC.

Repair Procedure

In the case of DCOM Error 0x800706BA, you first need to check if the OPC Server is still running. If the OPC Server has shutdown, you will need to restart it. Then you should trace the cause of the unexpected shutdown. Specifically, find out if a User terminated the OPC Server manually, or if a software bug caused the OPC Server to

shutdown/crash. Once the OPC Server is available again, reconnect the OPC Client to the Server.

Once the OPC Server is available, ensure that the OPC Client application is able to retrieve data using a synchronous method. Specifically, you should attempt to issue a Synchronous Cache Read, or a Synchronous Device Read. Each OPC Client application will do this in a different way, so check with you OPC Client application vendor to find out how do conduct this type of read.

If the Synchronous Read operation fails, you will need to modify the DCOM permissions on the OPC Server as in section 5.1 Access Permissions on the OPC Server PC. However, if the Synchronous Read returns results successfully but you still receive the same DCOM Error 0x800706BA, follow the steps starting at section 5.2 Firewall below.

1. Access Permissions on the OPC Server PC

Windows uses the COM Security tab (refer to Image 1) 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.

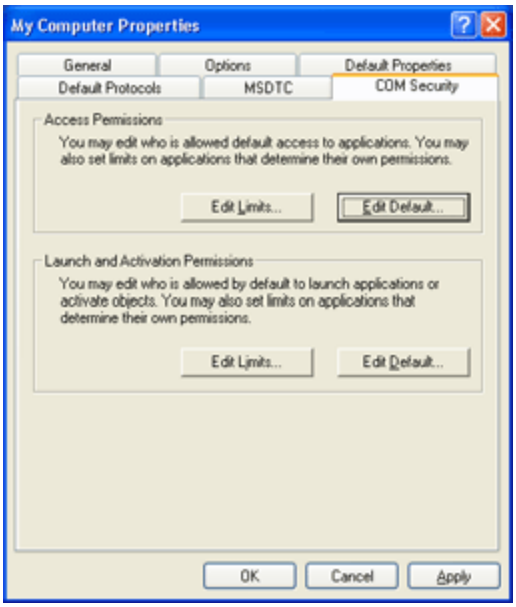

Image 1: Use the COM Security tab to set the default Access Control Lists (ACLs).

To add the right permissions, follow the steps below:

1. 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.
2. 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.
3. 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.

4. 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.

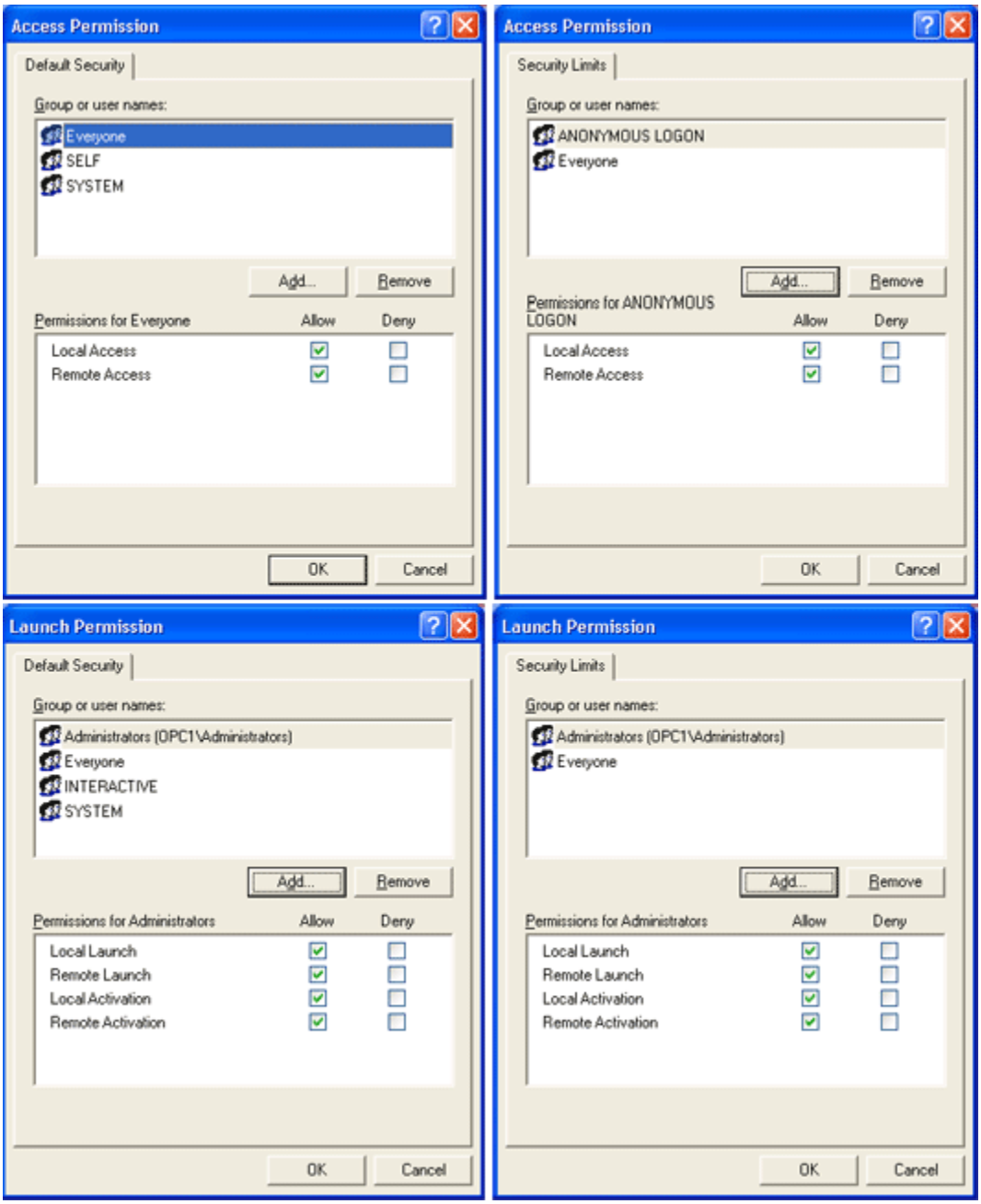

Image 2: Add Everyone to the Launch and Access Permissions. Add Everyone and Anonymous Logon to the Security Limits (Edit Limits). Once communication is working properly, remember to return to this setup to ensure you comply with corporate security policies.

2. 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.

Microsoft turned on the Windows Firewall 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.

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

1. Click on the Windows Start button, select the Control Panel, and finally click on Windows Firewall.
2. In the General tab, select the "Off (not recommended)" radio button (refer to Image 3).

Once you have communication working, ensure that you turn the Firewall back on to comply with your company's IT policies, Industry practices, and Government regulations.

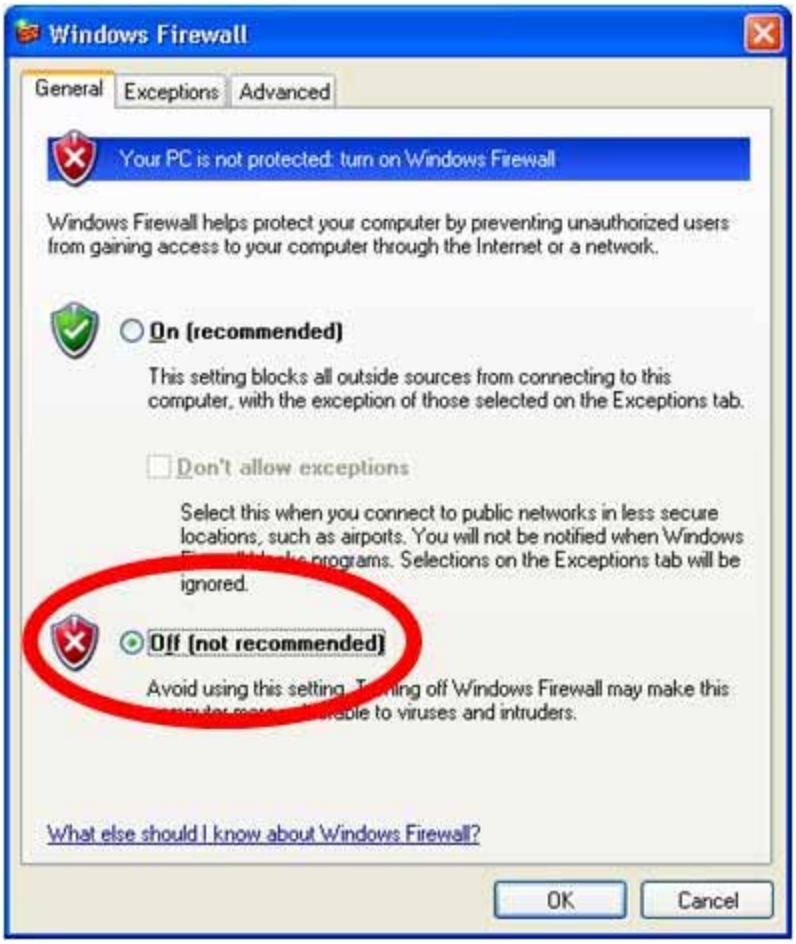

Image 3: Temporarily turn off the Windows Firewall to allow remote access to the OPC Server computer.

3. 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.

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.

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.

Local Users Authenticate as Themselves

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. (This is not necessary in Windows 2000 or earlier.)

Method 1: Turning off Simple File Sharing

1. Double-click "My Computer" on the desktop.
2. On the Tools menu, click Folder Options.
3. Click the View tab, and then clear the "Use Simple File Sharing (Recommended)" check box to turn off Simple File Sharing (refer to Image 4).

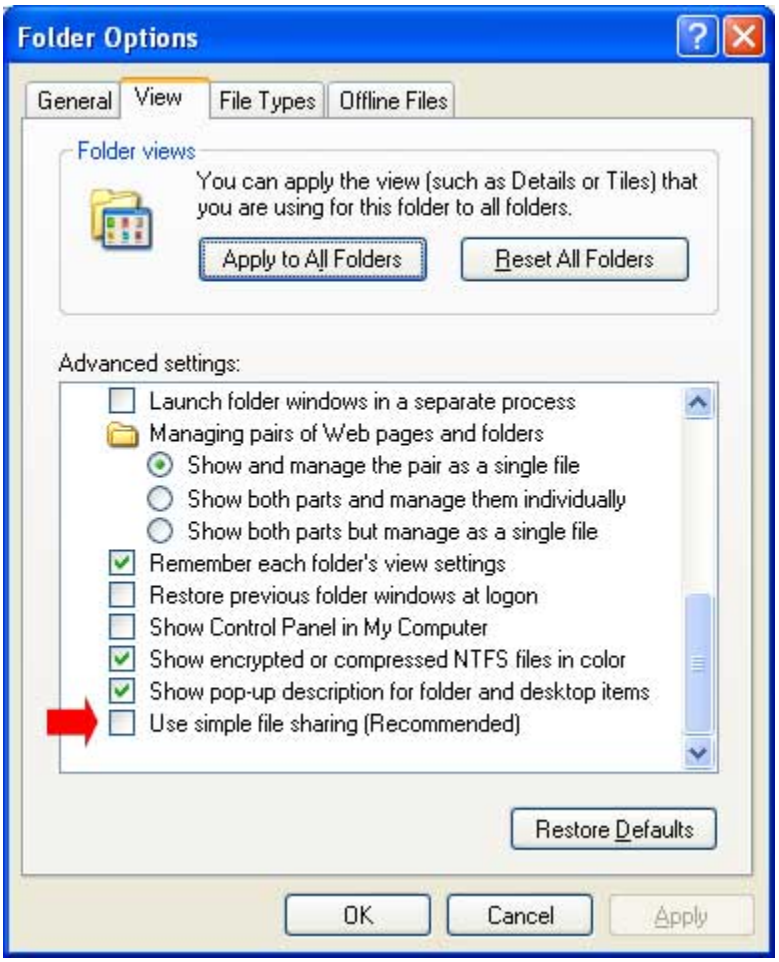

Image 4: Turn off "Simple File Sharing" to enable Windows to Authenticate User Accounts properly.

Method 2: Set Local Security Policies

1. 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".
2. In the tree control, navigate to Security Settings, Local Policies, and finally select the Security Options folder (refer to Image 5).
3. Find the "Network access: Sharing and security model for local accounts" option and set it to "Classic - local users authenticate as themselves".

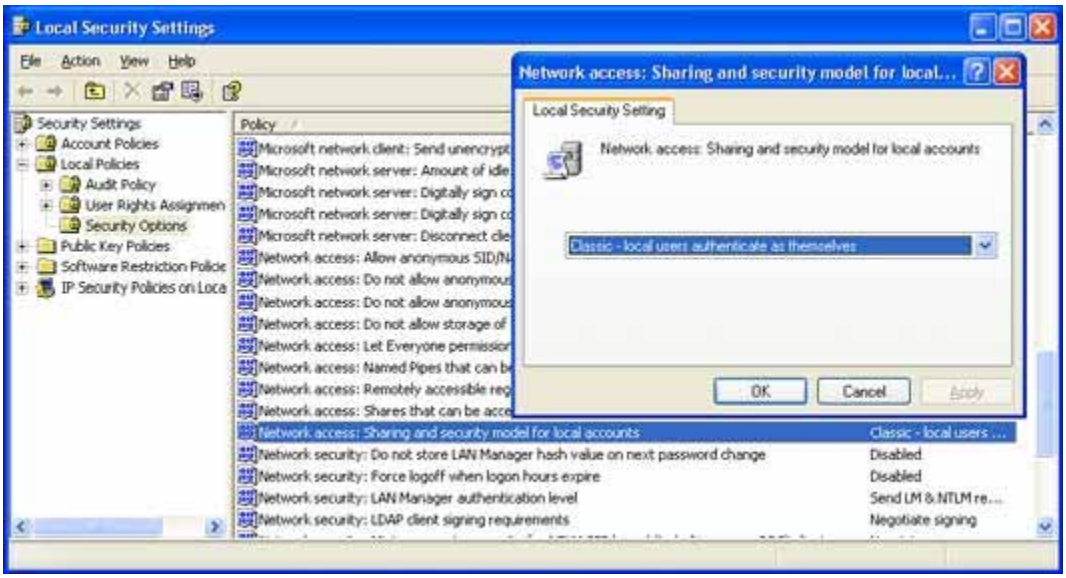

Image 5: Appropriate OPC security for requires Windows to enable local users to authenticate as themselves rather than as Guest.

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 the OPC Training Institute's 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.

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). In this case, since we are working with a callback, Windows refers to the "Security Limits" settings for the DCOM Access Permissions.

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:

1. Click on the Windows Start button, and select the Run menu option (refer to Image 6).

Image 6: Use DCOMCNFG to modify DCOM settings on the computer.

2. 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 7).

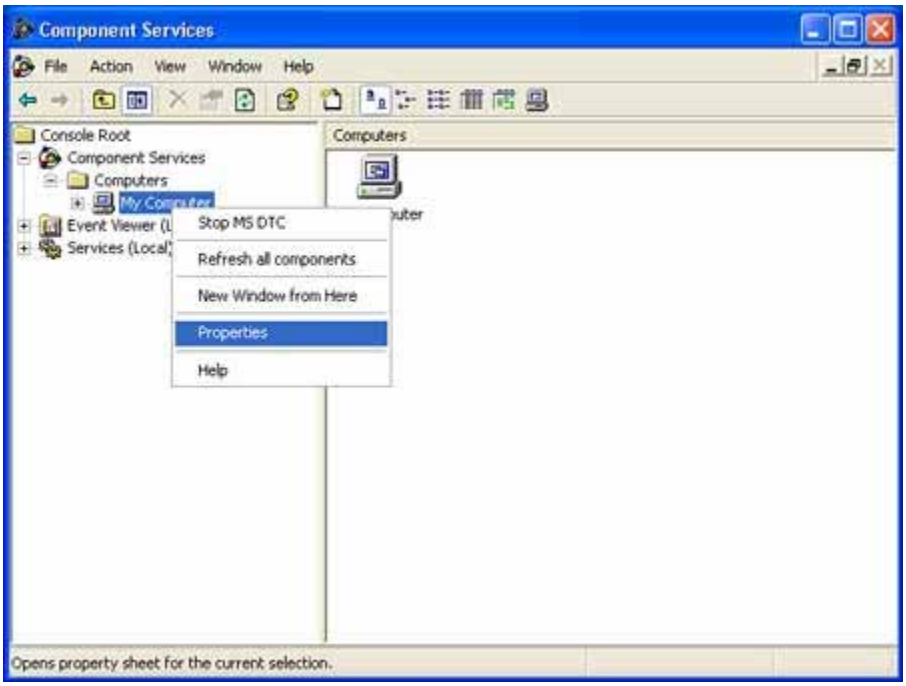

Image 7: Right-click on the My Computer tree control to access the computer's default DCOM settings.

3. 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.
4. 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.
5. Select the Properties option.

4. COM Security

This step should be done on both the OPC Client PC and OPC Server PC. 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 Microsoft only added the "Edit Limits" buttons in Windows XP Service Pack 2, and Windows 2003 Service Pack 1. Thus, if you have an earlier system, these buttons will not be available.

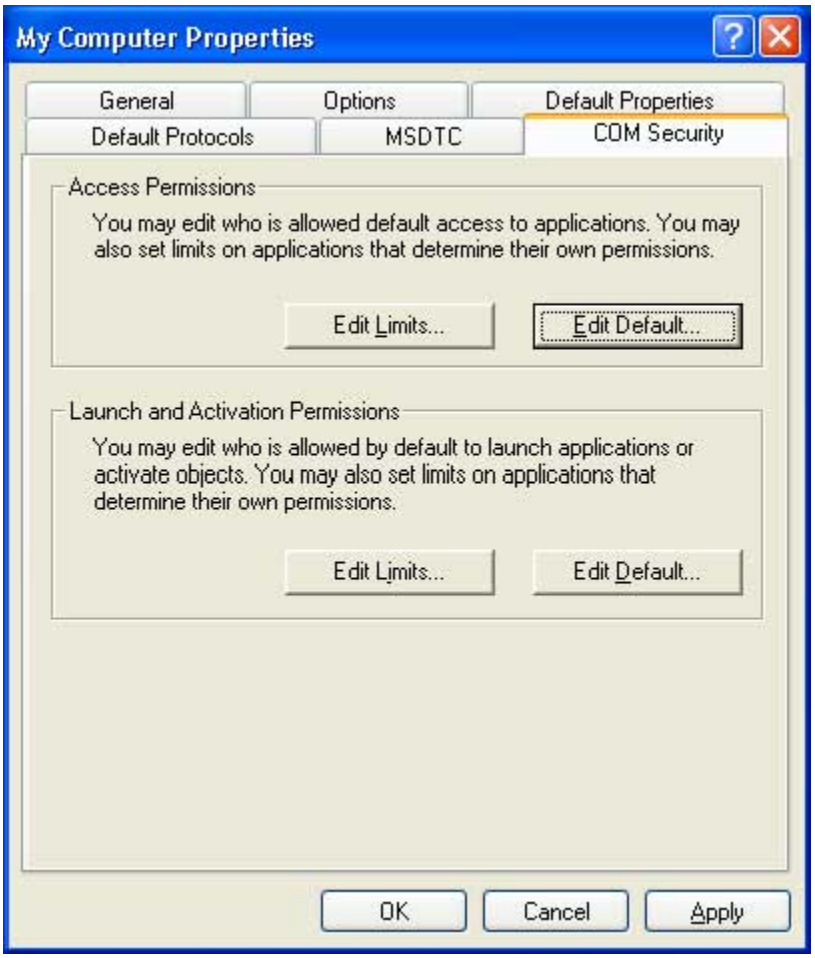

Image 8: Use the COM Security tab to set the default Access Control Lists (ACLs).

To add the right permissions for the Security Limits, follow the steps below:

1. In the Access Permissions group, click the "Edit Limits..." button (refer to Image 9).

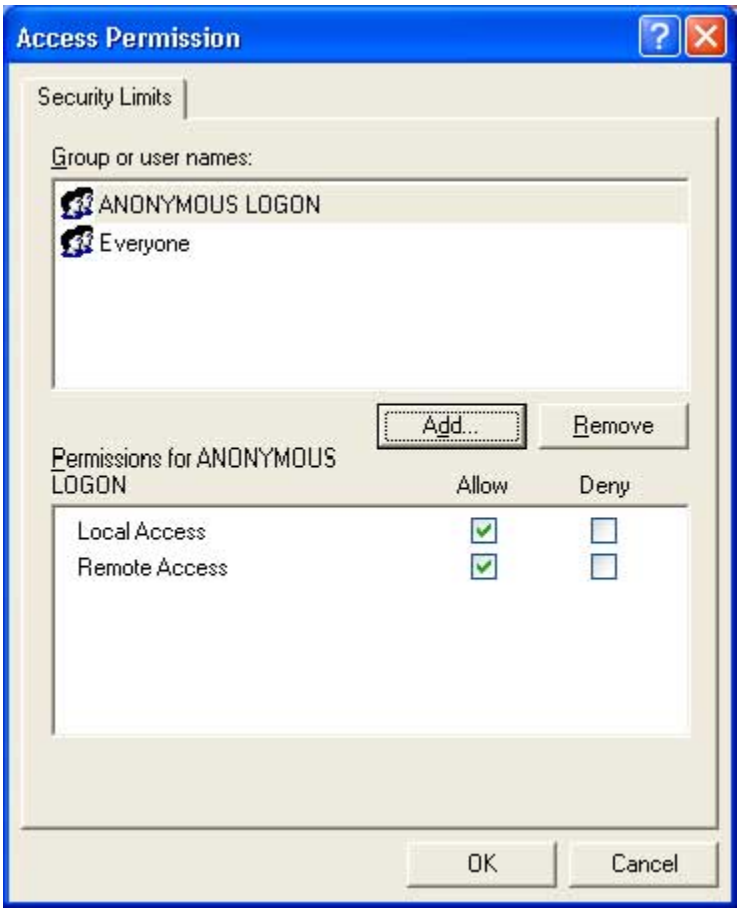

Image 9: Security Limits are the ACL used for callbacks. Once communication is working properly, remember to return to this setup to ensure you comply with corporate security policies.

2. Add "Anonymous Logon" (required for OPC Servers that run as System).
3. Add "Everyone" to the list of "Group or user names".
4. Click the OK button.