0x80070005 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

DCOM Error 0x80070005 appears in the OPC Client application when it succeeds in launching an OPC Server or OpcEnum, but fails to receive a reply from either of the applications. This error could be caused under several conditions:

On the OPC Server PC, the OPC Client User Account does not have the right Access Control List (ACL) permissions in the System-Wide DCOM settings, Access Permissions, Edit Default.

On the OPC Client PC, the OPC Server User Account does not have the right Access Control List (ACL) permissions in the System-Wide DCOM settings, Access Permissions, Edit Limits.

On the OPC Client PC, the DCOM Default Impersonation Level is set to "Anonymous" instead of "Identify", and the "ANONYMOUS LOGON" Access Control Entry (ACE) does not exist in the OPC Client PC, Access Control List (ACL) permissions in the System-Wide DCOM settings, Access Permissions, Edit Limits.

Background

There are cases where an OPC client application can launch a remote OPC Server, but is unable to receive further responses. Thus, DCOM will inform the OPC Client that the launch of the remote server was successful, but the OPC Client will be unable to continue communicating with the OPC Server application. In this case, the OPC Client application will display DCOM Error 0x80070005. In essence, this error occurs when DCOM communication is stopped by the Access Control List (ACL) of either the OPC Client PC or OPC Server PC.

Test

If you receive DCOM Error 0x80070005, check if the OPC Server application is actually running on the OPC Server PC. If you received this error when you tried to browse for OPC Servers on the OPC Server PC, check if OpcEnum is running. If either is running, end both processes on the OPC Server PC. Then try to establish communication again. If you still receive the same DCOM Error 0x80070005, then the cause is as listed above, and you will simply need to follow the repair procedure below. If you receive a different DCOM error, then you will need to search for that specific error instead.

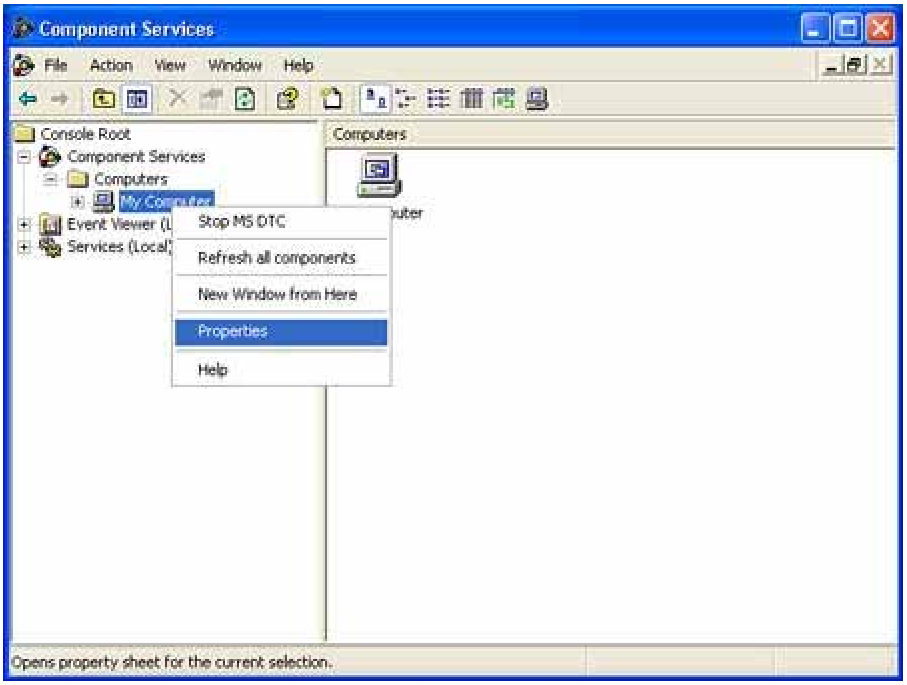
Repair Procedure

DCOM Error 0x80070005 is generated when a PC’s Access Control List (ACL) blocks DCOM communication. To fix this error, follow the procedure below.

OPC Server PC Access Control List (ACL)

You will need to make this change on the OPC Server PC.

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:



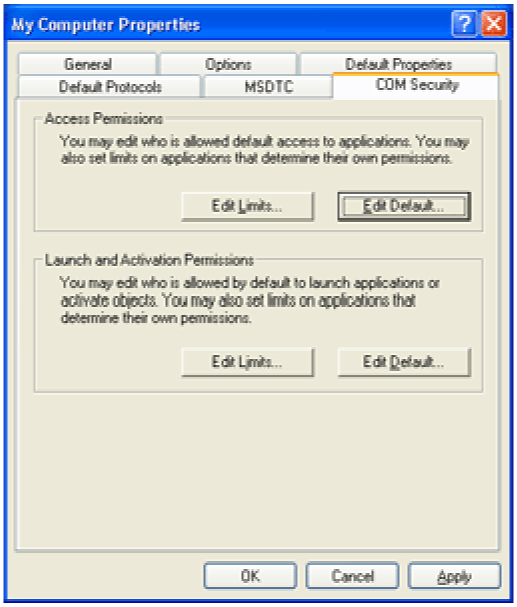
Opens property sheet for the current selection.

Image 1: Right-click on the My Computer tree control to access the computer's default DCOM settings.

1. Click on the Windows Start button, and select the Run menu option.
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 1).
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.

Windows uses the COM Security tab (refer to Image 2) 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.

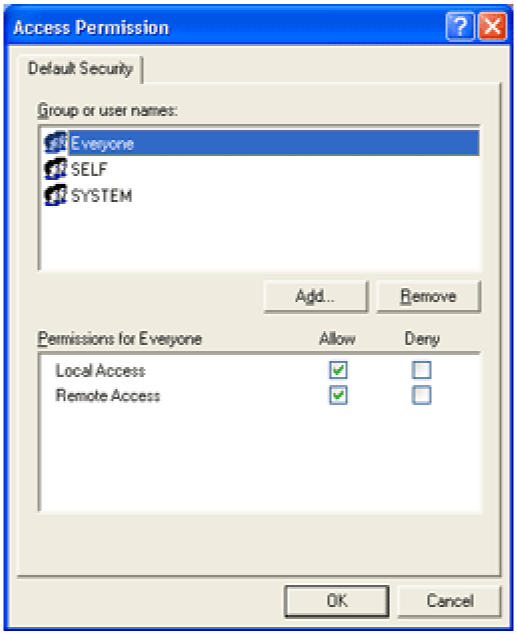


You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

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 2: the COM Security tab to set the default Access Control Lists (ACLs).

In the Access Permissions group, click the "Edit Default..." button (refer to Image 3). Add "Everyone" to the list of "Group or user names". Click the OK button.



Group or user names:

- Everyone
- SELF
- SYSTEM

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

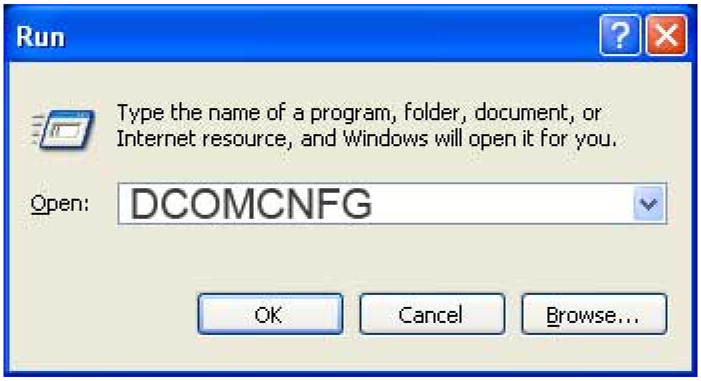
Image 3: Add the "Everyone" Access Control Entry (ACE) to Default Security. Once communication is working properly, remember to return to this setup to ensure you comply with corporate security policies.

OPC Client PC Access Control List (ACL)

You will need to make this change on the OPC Client PC.

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.
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 4).

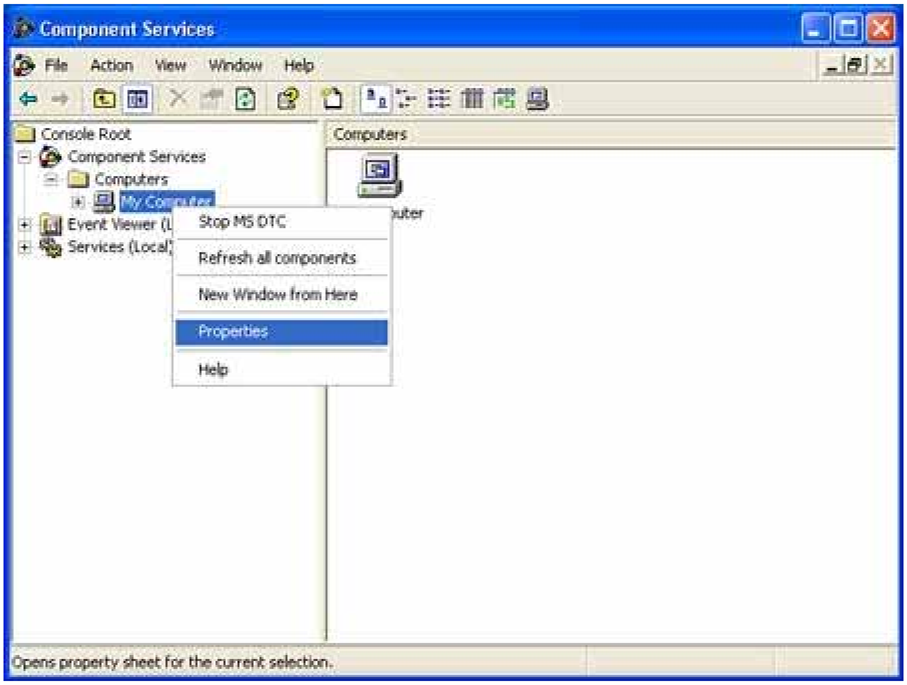


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: DCOMCNFG

Image 4: Use DCOMCNFG to modify DCOM settings on the computer.

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 (refer to image 5).
5. Select the Properties option.

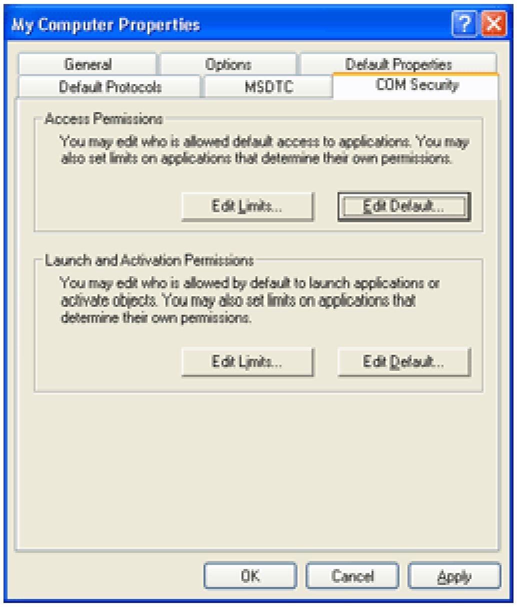


Opens property sheet for the current selection.

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

COM Security

Windows uses the COM Security tab (refer to Image 6) 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.

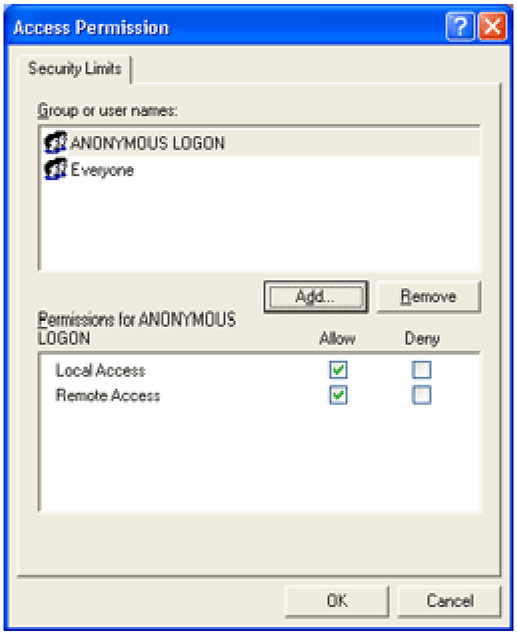


You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

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

In the Access Permissions group, click the "Edit Default..." button (refer to Image 7). Add "Everyone" to the list of "Group or user names". Click the OK button.



Group or user names:

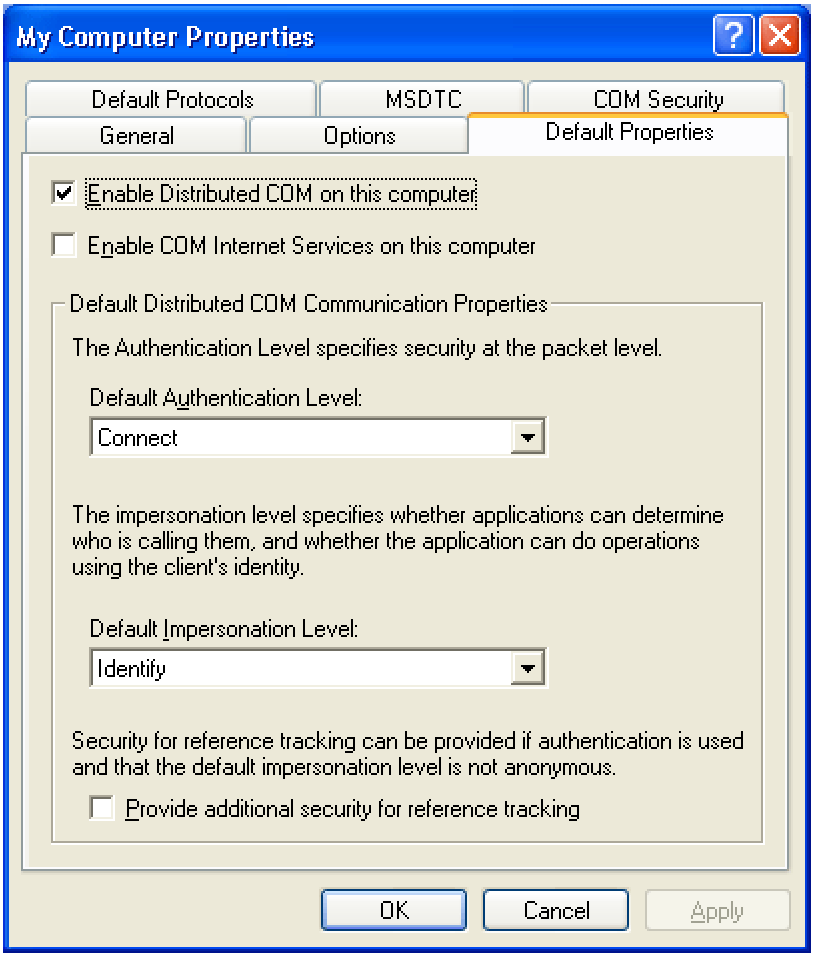
ANONYMOUS LOGON
Everyone

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

Image 7: Add the "Everyone" and "ANONYMOUS LOGON" Access Control Entries (ACEs) 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.

Default Properties

In the Default Properties tab, set the "Default Impersonation Level" to Identify (refer to Image 8).



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