DCOM Security and Configuration Guide

OSIsoft, LLC
777 Davis St., Suite 250
San Leandro, CA 94577 USA
Tel: (01) 510-297-5800
Fax: (01) 510-357-8136
Web: http://www.osisoft.com

OSIsoft Australia • Perth, Australia
OSIsoft Europe GmbH • Frankfurt, Germany
OSIsoft Asia Pte Ltd. • Singapore
OSIsoft Canada ULC • Montreal & Calgary, Canada
OSIsoft, LLC Representative Office • Shanghai, People's Republic of China
OSIsoft Japan KK • Tokyo, Japan
OSIsoft Mexico S. De R.L. De C.V. • Mexico City, Mexico
OSIsoft do Brasil Sistemas Ltda. • Sao Paulo, Brazil

Published: 12/3/2012

Table of Contents

Chapter 1. Introduction

This guide tells you how to configure Microsoft Distributed Component Object Model (DCOM) settings for OSIsoft PI OPC products, with special consideration given to security. Although you can use firewalls to help protect your OPC server, this guide does not cover firewall strategies. Firewall configuration is complicated by the dynamic port allocation behavior of DCOM and is beyond the scope of this document. When configuring DCOM for non-OSIsoft OPC products, follow all recommendations and guidelines from your vendor.

PI OPC products include the following:

- PI OPC DA/HDA Server
- PI OPC DA Interface
- PI OPC HDA Interface
- PI OPC A&E Interface
- PI OPC Client

Consider the recommendations in this guide as part of an overall "defense-in-depth" strategy for securing your control system from cyber-intrusion. Industrial control systems are often part of a critical infrastructure (such as electricity, gas, and water) and therefore of interest to parties with malicious intent. Cyber-intrusion can also come internally from personnel with good intentions but inappropriate training or access permissions. Reducing the attack surface and attack vectors of your control system is prudent, regardless of whether the control system is part of critical infrastructure. To protect your business from downtime and data loss, employ a comprehensive cyber-security strategy that includes installing anti-virus software, staying up to date with patches and updates, training your users, and following the security recommendations from this guide and those from other vendors. Other resources are available from organizations such as the United States Computer Emergency Readiness Team (US-CERT), at the following website:

http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

Classic OPC server and client applications are based on Microsoft's COM/DCOM communication model. COM (Component Object Model) provides a set of interfaces that enable software components to communicate on a single computer. DCOM (Distributed Component Object Model) lets software components communicate between networked nodes: a process on one computer can execute code on another. This technology has significant security implications. Permissions must be granted carefully, so that the client and server can communicate without compromising the security of the host computers.

The exact settings required to configure DCOM for OPC depend on operating system, domain or workgroup configuration, firewall configuration, network architecture, and your preferred user-account structure. This guide provides recommendations for the most common configurations.

Note: OSIsoft discourages the use of the Windows 2000 or Windows NT operating systems in any OPC configuration. Microsoft has announced the end of support for both Windows NT and 2000, as follows: “Unsupported products or service packs pose a significant risk to your computer's security. Therefore, Microsoft advises customers to migrate to the latest supported service pack and/or product prior to the end of support.”

Chapter 2. Configuring DCOM for OPC

Prerequisites

To configure DCOM, you must log into the computer with an account that has local administrator privileges. DCOM configuration depends on the deployment of the OPC server and OPC client:

- **Same computer** (recommended): Configure DCOM, though OPC client and server programs running on the same computer do not use DCOM to communicate. Disable the ability of users to configure DCOM.
- **Different computers, same Windows domain:** Grant DCOM permissions to domain accounts.
- **Different computers, no common Windows domain:** Grant DCOM permissions to identical local accounts on both the server and client computers**.**

Before configuring DCOM for your OPC server and client, verify computer connectivity and create user accounts.

Note: In this guide, computers that run a PI OPC interface (DA, HDA, A&E) or a client program that connects to a PI OPC DA/HDA server are referred to as "OPC clients." Computers that run a PI OPC DA/HDA server or third-party OPC servers are referred to as "OPC servers."

Verify Connectivity

If the OPC server and OPC client reside on different computers, check connectivity before configuring your OPC server and OPC client computers for DCOM:

- Verify that the server and client can connect to each other on the network and that port 135 is open (use `telnet`).
- If port 135 is not open, check for issues related to a firewall or other network restrictions. For more information, see the OSIsoft Knowledge Base topic titled "Configuring ports for DCOM for use with the OPC Interface. NAT and Firewall considerations."

Select or Create User Accounts

To configure DCOM, you need to create the appropriate accounts for your configuration. Your OPC server and OPC client deployment determines the required accounts, as follows:

- If the OPC server and client run on the same computer, any account can be used, including a local system account.
- If the OPC server and client run on separate computers in the same Windows domain, use domain accounts.
- If the OPC server and client run on separate computers in different, untrusted Windows domains (or are not members of a domain), you must create identical local accounts (same user name and password) on both computers. These service accounts must have password expiration disabled. This approach is not recommended, because it requires you to maintain multiple identical local accounts.

A recommended approach is to create highly privileged OPC administrator accounts and less privileged user accounts, as follows:

- OPC administrator account

  On the domain controller, configure a privileged OPC administrator account. Assign this account to the user who configures and controls access to OPC software and data. The administrator account must be a member of the **Administrators** group. As a member of this group, the administrator account has full and unrestricted access to the local computer.

- OPC user accounts

  For users who need access to OPC data but who do not configure the software or system, create accounts with the minimum level of permissions required. These users can run the OPC client application and connect to the OPC server. If the server and client computers do not share a common domain, create identical local accounts on both computers.

Set Permissions for Directories containing OPC Executables

If the local users are not part of the **Users** group, grant file-system access to OPC applications and services:

1. Right-click the OPC application's executable folder (not the application executable itself) and then click **Properties**.
2. In the Properties window, click the **Security** tab and then click **Edit.**
3. In the Permissions window, click **Add** to add your OPC users to the list of authorized users authorized to launch and access the application.
4. Set the following permissions to **Allow**:
   - **Read & Execute**
   - **List Folder Contents**
   - **Read**

Note: If your OPC server vendor recommends or requires other permissions, be sure to set them.

Configuring Operating System Settings

Each version of Windows has its own defaults for DCOM settings, which can change when you upgrade your operating system. Be sure to verify that the settings on your OPC server and client computers are configured properly, as described in this guide and by your OPC server vendor. When setting access permissions, do not remove any of the Windows default users or groups (such as Administrator), because they are necessary for proper functioning of DCOM.

To configure the OPC client node (and the OPC server node if so advised by your OPC server vendor), perform the following procedures.

Configure Local Security Settings

You must configure the local security settings that affect DCOM authentication. After making these changes, your Windows platform might require you to reboot to put changes to group membership into effect.

1. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Under **Security Settings**, click **Local Policies > Security Options** and configure settings as follows:
   - **Network access:** Right-click **Sharing and security model for local access** and choose **Classic – local users authenticate as themselves** (which is the same as simple file sharing). Click **OK**.

- **System objects** (Windows XP and Server 2003 only)**:** Default owner for objects created by members of the **Administrators** group . Right-click and select **Administrators** group.

3. Save your settings and exit.

Note: Rather than set the "sharing and security model for local access" security setting as described above, you can disable simple file sharing using the Windows Explorer options. However, be advised that the local guest account remains enabled, and DCOM connections are not authenticated.

Configure Windows Firewall Settings

If Windows Firewall is enabled on your OPC computers, you must allow certain programs through the firewall.

1. Click **Start > Control Panel > Windows Firewall**.
2. On the **Exceptions** tab, enable exceptions for the following:
   - TCP Port 135
   - `opcenum.exe`
   - Your OPC server executable
3. To restrict the source of the incoming TCP connections to the OPC client node exclusively, click **Add Program** or **Add Port and Change scope**. Select the **Custom** list option, enter the OPC client node's IP address and click **OK**.

Configure OPC Client Node DCOM Settings

On client computers that access OPC servers, you must enable DCOM and grant appropriate account access. (Individual OPC server implementations might require different settings. Consult your OPC server vendor to identify the required settings.)

To configure the required settings, perform the following steps:

1. In a command window, issue the `dcomcnfg` command. The **Component Services** window is displayed.
2. Expand **Console Root > Component Services > Computers**, right-click **My Computer** and then click **Properties**.
3. In the **My Computer Properties** window, click the **Default Properties** tab and set the appropriate settings:
   a. Select the **Enable Distributed COM on this computer** check box if the OPC client must connect to an OPC server running on a different computer. DCOM can be disabled if the client and server run on the same computer. Disabling DCOM is secure but doing so disables many remote management functions.
   b. Set **Default Authentication Level** to **Connect**.
   c. Set **Default Impersonation Level** to **Identify**.

d. If the OPC user account is a local user account, click the **COM Security** tab, and add the account to the appropriate access control lists (ACLs) as follows: Under **Access Permissions**, add the user (and the OPC administrator) to both the **Limits** and **Defaults** ACLs. Set **Access Permissions** for the default users and groups as follows:

Permissions	User	Setting	Access Type(s)
Limits	Everyone	Allow	Local Access and Remote Access
	ANONYMOUS LOGIN	Allow	Local Access
Default	SELF	Allow	Local Access and Remote Access
	SYSTEM	Allow	Local Access

4. Under **Launch and Activation Permissions**, add the user to both the Limits and Defaults ACLs. Set the **Launch and Activation Permissions** for the default users and groups as follows:

Permissions	User	Setting	Access Type(s)
Limits	User under which OPC Server runs, or Administrators	Allow	Local Launch Remote Launch Local Activation Remote Activation
	Everyone	Allow	Local Launch and Local Activation
Default	User under which OPC Server runs, or Administrators	Allow	Local Access and Remote Access (or Launch and Activation, depending on your Windows operating system)
	INTERACTIVE	Allow	Local Access and Remote Access (or Launch and Activation, depending on your Windows operating system)
	SYSTEM	Allow	Local Access and Remote Access (or Launch and Activation, depending on your Windows operating system)

Configure OPC Server Node DCOM Settings

If your OPC server vendor recommends specific DCOM settings, be sure to follow those recommendations. If you are running an OSIsoft OPC server, or no specific recommendations are available from the vendor, configure DCOM settings for the user that runs the OPC server as follows:

1. Launch the `dcomcnfg` program and browse to **Console Root** > **Component Services** > **Computers** > **My Computer** > **DCOM Config**.
2. In the list of applications in the right pane, right-click your OPC server and choose **Properties**.

Note: By default, the `dcomcnfg` program does not display an entry for **PI OSI DA Server** or **PI OSI HDA Server** on the 64-bit version of Microsoft Windows 7 and Microsoft Windows Server 2008 R2. To ensure these servers are listed, issue the following command, which launches the 32-bit version of `dcomcnfg`:

```
MMC /32 %windir%\syswow64\comexp.msc
```

3. On the **General** tab, set **Authentication Level** to **Default**.
4. On the **Location** tab, check **Run application on this computer**.
5. On the **Security** tab, set permissions as follows:

   OPC users:

   - Launch and Activation Permissions: Use System Defaults
   - Access Permissions: Use System
   - Configuration Permissions: Allow Read

   OPC administrators:

   - Launch and Activation Permissions: Use System Defaults
   - Access Permissions: Use System Defaults
   - Configuration Permissions: Full Control

5. On the **Endpoints** tab, add **Connection-oriented TCP/IP** to the protocol list**.**
6. On the **Identity** tab, choose the **This user** option and enter the user name and password for the OPC user you created.
7. Click **OK** to save your settings.

Authentication

Authentication confirms the identity of a user (as opposed to *authorization*, which controls what the user is permitted to do). For authentication, the DCOM security model uses the Microsoft Windows extensible security provider. For Microsoft Windows NT-based operating systems operating in a workgroup, DCOM uses NTLMSSP (NT LAN Manager Security Support Provider). When OPC nodes are members of a domain, Active Directory for Windows Server 2003/2008 uses Kerberos authentication protocol as the security provider.

Never enable unauthenticated communication (authentication level set to **None**), which permits any user in the network to connect to the OPC server node without any type of authentication and auditing.

DCOM supports the following levels of authentication and privacy, listed from least to most secure:

- **None** (NOT recommended)**:** No authentication occurs.
- **Connect:** Authenticates credentials only when the connection is made.
- **Call:** Authenticates credentials at the beginning of every RPC call.

- **Packet:** Authenticates credentials and verifies that all data is received.
- **Packet Integrity:** (Recommended) Authenticates credentials and verifies that no data has been modified in transit. Verify that this level of authentication does not affect the performance of your scan classes.
- **Packet Privacy:** Authenticates credentials and encrypts the packet, including the data and the sender's identity and signature.

Authentication levels configured using the `dcomcnfg` program override the authentication level set in the system-wide settings. For communication between OPC client and OPC server, the effective authentication level is the highest minimum. For example, if the OPC server is configured for **Packet Integrity** and the OPC client is set to **None**, then **Packet Integrity** is applied.

Configuring the Effective User

When configuring the account used to run the OPC server, include the account in the ACLs and in the `dcomcnfg` **Identity** tab. If the OPC server runs as a Windows service, the account specified in the **Identity** tab must be the same as the account specified in the **Log On** tab on the **Service Properties** window.

To view the account that is running an OPC process, check the **Processes** tab of **Windows Task Manager**.

Interactively-Run Programs

Programs that are run interactively, such as PI OPC Client and the PI OPC interface when started from the command line, are associated with the user logged into the computer (unless the Windows **Run As** command is used). If the account is a local user account, then, by default, it lacks the privileges required to run applications that were installed by an administrator. To enable this user to run applications that were installed by an administrator, add the local user account to the security properties of the folder that contains the application's executable and assign **Read** and **Execute** permissions.

Windows Services

For programs that run as a Windows service, specify the user account in the **Log On** tab of the service. The user account specified here must be the same as the account specified for the application in the **Identity** tab of `dcomcnfg`.

To verify or change this account:

1. Click **Start > Run** and enter `services.msc`.
2. Right-click the service and then click **Properties**.
3. Click the **Log On** tab and specify the user account in the **This account** section.

Impersonation

Impersonation is a mechanism that enables a DCOM server to access secured objects using the credentials associated with the client rather than those of the server itself. Impersonation is usually not supported by OPC servers except for those that support the OPC Security specification. If your OPC server supports this specification, consult the vendor documentation for the required impersonation settings for both the client and server computers.

DCOM authorization is supported by the following levels of impersonation:

- **Anonymous:** The server can impersonate the client, but the identity of the user associated with the OPC client is hidden from the OPC server.
- **Identify**: (Recommended) The OPC server can identify the user associated with the OPC client, and can perform actions as that user.
- **Impersonate**: The OPC server can perform actions as the user associated with the OPC client, but is not allowed to access other computers as that user.
- **Delegate**: The user that runs the OPC server can act as the user associated with the OPC client, including access to other computers as that user.

Chapter 3. Checklist for Hardening OPC Security

For a comprehensive discussion of OPC security hardening, see:

OPC Security Whitepaper #3 - Hardening Guidelines for OPC Hosts

Following are general guidelines for maximizing OPC security.

- Disable all unnecessary services, including OPCEnum, which is not required for normal OPC interface operation.
- Disable file and printer sharing
- If the OPC interface and server run on the same computer, disable DCOM and remote registry access.
- User accounts:
  - Define a low-privilege OPC users group and add *only* users who need OPC access
  - Define a high- privilege OPC administrators group limited to specific computers
  - Disable **Guest** access
  - Require robust passwords
  - Configure firewall to limit traffic to trusted computers and create a policy based on this configuration
  - Protect the Windows registry (no administrative rights for regular users, disable remote registry editing)
- DCOM configuration:
  - Set the minimum authentication level to **Packet integrity** (verify that the overhead incurred does not interfere with the performance of the interface)
  - Security:
    - Launch: OPC administrator account only if the OPC server runs as a Windows service.
    - Access: OPC administrator and OPC user accounts
    - Configuration: OPC administrator: full control. OPC Users: read-only,
  - Identity: Member of opcuser group
  - DCOM transport protocols: restrict to TCP

Chapter 4. Troubleshooting

The following sections list and discuss logs useful for troubleshooting, common DCOM security errors, and errors by numeric code and category.

Logging of DCOM Errors

PI Log Errors

OSIsoft products log DCOM security errors in the OPC client node's local PI message log file. Errors might also appear in the Windows System log. You can use these errors to troubleshoot common DCOM errors. Connection errors (CoCreateInstanceEx) indicate problems instantiating the OPC server, usually because the OPC server cannot authenticate the account used by the client or because that account does not have permission to use the server. Advise errors indicate the reverse: the OPC client cannot authenticate the account that is associated with the OPC server, or the account does not have the permissions required to use the interface node.

DCOM Failure Logging

To configure Windows logging of DCOM failures, use REGEDIT to define the following registry values in the `HKEY_LOCAL_COMPUTER\SOFTWARE\Microsoft\Ole` entry and set them to 1:

Registry Key	Description
`ActivationFailureLoggingLevel`	Log failed requests for component launch and activation.
`CallFailureLoggingLevel`	Log failed calls to components after the component has been activated.
`InvalidSecurityDescriptorLoggingLevel`	Log invalid security descriptors for component launch and access permissions.

You must restart OPC servers and client instances before these settings take effect. After you enable logging, DCOM security errors appear in the Windows System event log.

Windows Security Auditing

Security audits can help you diagnose DCOM permission problems. You must enable Windows security auditing on the OPC server and client nodes. To enable Windows security auditing:

1. Launch the **Local Security Policy** control panel.
2. Browse to **Local Policies > Audit Policy**.
3. Set the following policies to audit failures:
   - **Audit account logon events**
   - **Audit logon events**
   - **Audit object access**

You can find security audit logs in the Security log in the Windows Event Viewer.

Common DCOM Security Errors

Unknown User or Bad Password

The following event indicates a failed logon due to an unknown user name. A failed logon due to a bad password is identical except that the error code is 0xC000006A.

```
Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID:     680
Date:         10/16/2012
Time:         5:20:48 PM
User:         NT AUTHORITY\SYSTEM
Computer:     OPCLANDDescription:
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon account:  opcaccount
Source Workstation: ONELOVE
Error Code: 0xC0000064
```

Anonymous Logon

The following event shows a failure on a Windows XP SP2 computer when the user is not in the computer-wide limit access control list. In this case, a logon failure causes the user to appear as "Anonymous logon."

```
Event Type:   Error
Event Source: DCOM
Event Category:None
Event ID:     10014
Date:         10/16/2012
Time:         3:48:09 PM
User:         NT AUTHORITY\ANONYMOUS LOGON
Computer:     OPCLAND
Description:
The computer wide limit settings do not grant Remote
Activation permission for COM Server applications to the user
NT AUTHORITY\ANONYMOUS LOGON SID (S-1-5-7).  This security
permission can be modified using the Component Services
administrative tool.
```

Failed OPC Server Activation

This event shows a failure to activate the OPC server. The server name is not included in the log but can be determined by searching the registry for the CLSID.

```
Event Type:   Error
Event Source: DCOM
Event Category:    None
Event ID:     10016
Date:         10/16/2012
Time:         4:05:13 PM
User:         NT AUTHORITY\ANONYMOUS LOGON
Computer:     OPCLAND
Description:
The application-specific permission settings do not grant
Remote Activation permission for the COM Server application
with CLSID
{13486D51-4821-11D2-A494-3CB306C10000}
to the user NT AUTHORITY\ANONYMOUS LOGON SID (S-1-5-7).  This
security permission can be modified using the Component
Services administrative tool.
```

DCOM Errors by Numeric Code

Error	Description
0x80004002	`No such interface supported.` This error occurs when the client connects to the server. It indicates that the client has connected to the server but cannot obtain a pointer to a COM interface. The OPC standards include facilities that are optional; This error is returned if an optional COM interface is not supported. However, this error is more commonly seen with servers that implement their own security, for the following reasons: • Some OPC servers do not accept connections from third-party OPC clients and return this error if such clients attempt to use the server. • The account used to run the client is not authorized by the server's own security. • The license for the OPC server is not installed correctly. • The default authentication level for the client computer is set to none, or simple file sharing is enabled, which results in an anonymous logon.
0x8000401a	`The server process could not be started because the configured identity is incorrect.` This connection error indicates a problem with the OPC server identity settings: • The account specified for the server identity does not exist. • The password for the account specified for the server identity is incorrect or expired. • The server has been configured with an identity of "Interactive user," but no user is logged on to the console of the server computer. Check the identity specified in the DCOM configuration for the server. Verify that the account exists, and verify the password. Use of "interactive user" as the server identity is discouraged because it requires that a user be logged on to the computer before the client attempts connection.
0x80040111	`ClassFactory cannot supply requested class.` This connection error indicates that either the OPC is not registered correctly or the server does not accept the type of connection requested by the client. Most OPC servers accept both local and remote connections, but some may only accept one type. OSIsoft OPC clients use a local connection if the server node name is omitted or if "localhost" is used as the node name. If a server accepts only remote connections, the client can be run on the OPC server node by including the server node name in the /server parameter (for example, "/server=myopcserver::some.opcserver.1").
0x80040112	`Class is not licensed for use.` . Not a DCOM security problem. Verify that the license for the OPC server is installed.
0x80040154	`Class not registered.` This connection error can occur if the interface cannot obtain the OPC server information from the registry. In some cases, the problem is identical to that described for error 80040111 (ClassFactory cannot supply requested class).

0x80040202	`Connection attempt failed.`
	`Unable to open the access token of the current thread. (incorrect error string)`
	This error occurs when the client attempts to advise a group if the OPC server cannot establish a new connection to the interface. This error might be caused by DCOM security problems or by general network issues, as follows:
	Security
	• The client Limits ACL does not allow a connection from the account used as the server's identity.
	• The server's authentication level is set to NONE and the client computer Limits ACL does not allow a connection from ANONYMOUS LOGON.
	• Simple file sharing is enabled on the server computer.
	Network
	• A firewall prevents the server from initiating a connection to the client computer.
	• A firewall between the server and client uses network address translation (NAT).
	• The DNS server for the network is returning an incorrect IP address for the client computer.

0x80070005	`General access denied error.` The most common DCOM security error. Either the user account associated with the OPC interface does not have permission to perform the requested action, or the account cannot be authenticated by the server. "Access denied" errors can occur when the client attempts to connect to the server (CoCreateInstanceEx errors) if the account running the client does not have permission to access the server, or when the client attempts to advise groups if the account associated with the server does not have permission on the client computer. **Connect** • The account running the client does not have required permissions to activate or launch the OPC server. • The client account does not have remote access permission in the system-wide **Limits** access control list. • The account running the client cannot be authenticated by the server computer. • The default authentication levels for both server and client computer is set to NONE or simple file sharing is enabled, which results in an anonymous logon. To troubleshoot "access denied" errors on connection, you must determine if the account that is being used for the connection is the one you intend, and that the account has the required permissions. First, check the Windows security log on the server computer (security auditing must be enabled). Logon failure audits indicate problems with the client account, due to either an unknown user or bad password. If no logon failures are recorded, check success audits to identify logons from the client computer and note the account. If the account is ANONYMOUS LOGON, the effective authentication level might be NONE, or simple file sharing might be enabled on the server computer. Next, check the Windows System log for DCOM errors. If the client account is not in the default of server-specific DCOM ACLs, an error is logged. **Advise** • The account used as the server identity does not have required permissions in the system default DCOM ACL. • The account used as the server identity does not have remote access permission in the system-wide **Limits** ACL. • The account used as the server identity cannot be authenticated by the server computer. • The default authentication levels for both server and client computer is set to NONE, or simple file sharing is enabled, which results in an anonymous logon. Troubleshooting advise access failures follows the same steps as those for connection failures, except that you will be looking at the client computer's logs and that there are no DCOM ACLs specific to the client process, only the system default ACLs.

0x8007007e	`The specified module could not be found.` This connection error indicates a problem with the installation of the OPC server. The executable file for the OPC server cannot be loaded.
0x800706ba	`The RPC server is unavailable.` This error might be generated either on connection or advise. It indicates that a connection to the Windows Remote Procedure service (RPCSS) cannot be made, either because the service itself is not running or impaired or because a firewall prevented the connection. **Connect** Using the Windows **Services** control panel, verify that the Windows Remote Procedure service is running on the server computer (the task list cannot be used in recent Windows versions because it actually runs under the svchost.exe process). To determine whether the computer is listening on port 135, issue the `netstat –a` command. If RPCSS is not running, verify that DCOM is enabled on the computer and, if necessary, restart the service. If there are no obvious problems with the RPCSS service, it is likely that access to port 135 is blocked. If the server is using Windows Firewall, add TCP port 135 to the firewall exception list. **Advise** Steps for troubleshooting RPC server failures on advise calls are the same as those above, except that they will be done on the client computer rather than the server.

0x80080005	`Server execution failed.`
	Generic failure code that occurs on connection, if the OPC server does not register with DCOM before timing out. The error is non-specific, but can be caused if the account configured as the identity for the OPC server does not have file system access to the server executable. Check the Event Viewer for the following error:
	`(EventID =10010, Type=Error):`
	`"Server [X] did not register with DCOM within the required timeout"`
	Edit the permissions for the directory containing the executable to include the account used as the server identity with full permissions, as described previously. Consult your OPC server vendor or documentation for proper settings.

Technical Support and Resources

For technical assistance, contact OSIsoft Technical Support at +1 510-297-5828 or techsupport@osisoft.com. The OSIsoft Technical Support website offers additional contact options for customers outside of the United States.

When you contact OSIsoft Technical Support, be prepared to provide this information:

- Product name, version, and build numbers
- Computer platform (CPU type, operating system, and version number)
- Time that the difficulty started
- Log files at that time
- Details of any environment changes prior to the start of the issue
- Summary of the issue, including any relevant log files during the time the issue occurred

The OSIsoft Virtual Campus (vCampus) website has subscription-based resources to help you with the programming and integration of OSIsoft products.