DCOM 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: 05-Apr-10

Table of Contents

Chapter 1

Introduction

DCOM Configuration Guide explains how to set up Distributed Component Object Model (DCOM) for OPC applications that reside on different nodes in common security environments. The procedures in this guide will help you establish a generic DCOM configuration to secure communication between two OPC nodes.

The recommendations in this guide apply to all PI OPC DA/HDA Servers, PI OPC DA Interface, PI OPC HDA Interface, and the PI OPC A&E Interface.

Factors that vary in the environments under which OPC applications run, such as Operating System, domain or workgroup configuration, firewall configuration, network architecture and user account types, determine how each OPC node will be configured.

This guide illustrates how to apply generic DCOM configuration sets under such varying conditions. These guidelines can be modified if, for example, more vigorous security is required at specific deployment sites.

The procedures described in this guide will generally apply to both Server and Interface nodes. Exceptions are noted.

DCOM configuration procedures for the following Operating Systems are included:

- Microsoft Windows XP SP2, and later
- Microsoft Windows Server 2003 SP1, and later
- Microsoft Windows Vista SP1, and later
- Microsoft Windows Server 2008 SP1, and later.
- Microsoft Windows Server 2008 R2.
- Microsoft Windows 7

Caution: Previous versions of Windows require additional configuration, yet still expose vulnerabilities known to be associated with those platforms. OSIsoft recommends upgrading OPC nodes to any of the patched Operating Systems described in this guide.

Prerequisite Knowledge

Users of this guide should be familiar with Microsoft Windows administration and DCOM technology. For a more detailed overview of DCOM and the most common security aspects related to DCOM, see *Appendix A - Related DCOM Fundamentals* (page 23).

PI OPC Products

For additional information about OPC products offered by OSIsoft, related documents, and training, see the OPC Home Page at the *OSIsoft Technical Support Web site* (http://techsupport.osisoft.com/).

Chapter 2

DCOM Configuration Procedures

This chapter provides procedures to configure DCOM when running the OPC Server or PI OPC Interface on Windows XP SP2, Windows Server 2003 SP1, Windows Vista SP1, Windows Server 2008 SP1 and later, Windows Server 2008 R2 or Windows 7 under these conditions:

- If neither the OPC server nor the client node is a member of a Windows domain, see *Scenario 1* (page 3).
- If one of the OPC nodes, that is, either the OPC server or the client node, is a member of a Windows domain, see *Scenario 2* (page 18).
- If both the OPC server and the client node are members of a Windows domain, see *Scenario 3* (page 19).
- If both nodes do not share a common Windows domain, see *Scenario 4* (page 21).

Note: Computers that run PI OPC DA Interface or PI OPC HDA Interface or PI OPC A&E Interface will be referred to as client nodes in this guide.

Scenario 1: OPC Nodes Are Not Members of a Windows Domain

If the OPC server and client applications run on separate nodes and neither node is member of a Windows domain, independent of Workgroup membership (same or different Workgroups), complete these procedures to configure DCOM:

- *Verify network connectivity* (page 3) between the OPC Server and the Client node.
- *Create identical user accounts* (page 4) (that is, same username and password) on both nodes.
- *Configure the Operating Systems* (page 5) for DCOM security settings on each node.
- Configure *DCOM settings* (page 6) on each node.

Verify Network Connectivity

Multiple tests can be performed to verify network connectivity between the OPC nodes. From the Windows command line on both OPC nodes, you can launch basic network tests such as:

- Ping the remote host, for example:

  ```
  ping <remote opc node>
  ```

The output should show the returned ping response from the remote OPC node.

- Tracert/Pathping the remote host, for example:

  `tracert <remote opc node>` or `pathping <remote opc node>`

  The output should show the path to the destination remote OPC node.

- Telnet remote host on port 135, for example:

  `telnet <remote opc node> 135`

  The output should show a blank console with a blinking cursor. If this not the case, port 135, required for DCOM communication, might not be accepting incoming connections due to firewall, Network Address Translation (NAT), or other network restrictions.

If none of these tests show expected results, further troubleshoot the network before proceeding with the following procedures.

Create New User Accounts

The accounts you create on the OPC Server and Client nodes must both have an identical username and password.

Using the **Local Users and Groups** management console, under **Start > Control Panel > Administrative Tools > Computer Management**, either a new local user account or local administrator account for use with DCOM can be created, depending on company policies. Local administrator accounts require less operating system and DCOM customization than local user accounts. Some considerations regarding each type of account are:

Local Administrator Account

The local administrator account must be part of the built-in Administrators Group account. As a member of this group, the local administrator account has full and unrestricted access to the local computer.

Local User Account

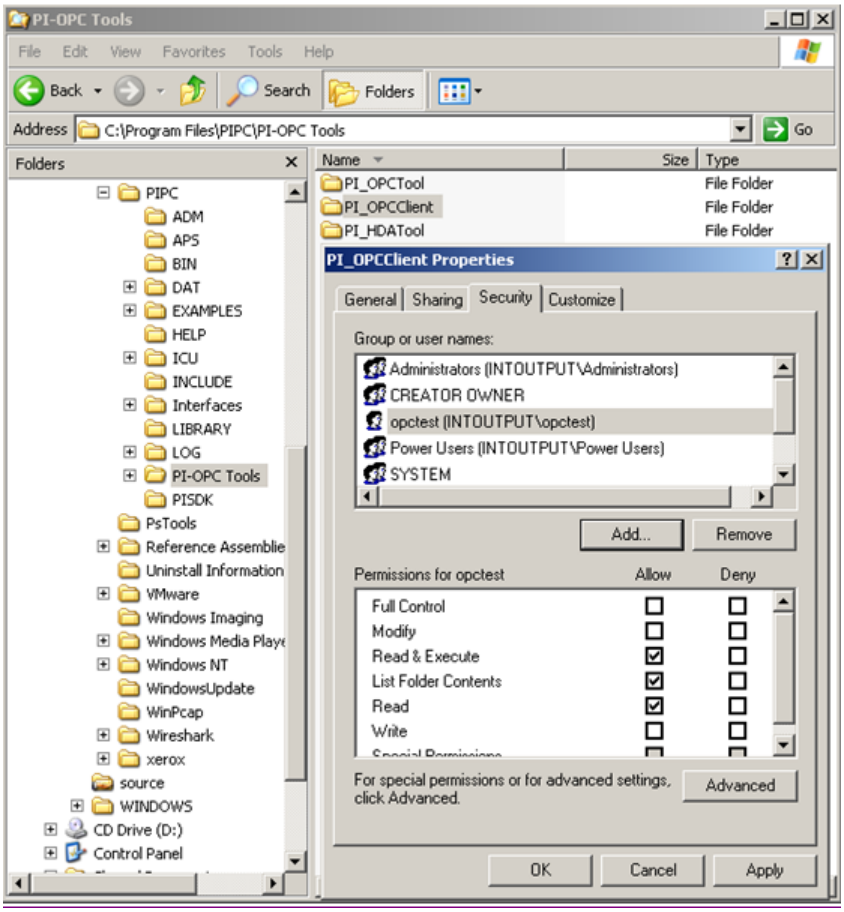
The local user account has very limited privileges on the local computer unless you specifically grant higher privileges, or add the user, to groups that already possess those privileges.

If the local user is not part of the Users group, you can allow this user to run applications and services such as PI OPC Client, PI OPC DA/HDA Interface, ICU, and PI OPC DA/HDA Server, by adding the local user account to the security properties of the folder that contains the application's executable and assigning **Read & Execute**, **List Folder Contents**, and **Read** permissions:

1. Right-click on the application's executable folder and select **Properties**.
2. Click on the **Security** tab and select **Add** to add the OPC user to the list of users who will be allowed to launch and access the application.

3. Select **Read & Execute**, **List Folder Contents**, and **Read** to assign the permissions.

   For example, here the **opctest** user is added to the list of users that will be enabled to launch and access the PI OPC Client, and is assigned **Read & Execute**, **List Folder Contents**, and **Read**.



Configure the Operating Systems for DCOM Security Settings

Use these procedures to configure the Operating Systems on the OPC Server and Client nodes to allow DCOM:

1. Turn off **Simple File Sharing**. Simple file sharing is enabled by default for Windows XP SP2 when the OPC nodes are not members of a domain. In this mode, the **guest** account is enabled, and all remote access is done anonymously. To disable **Simple File Sharing**:

   a. Open **Windows Explorer** and select **Tools > Folder Options**.

   b. Click on the **View** tab and deselect **Use simple file sharing (Recommended)**.

   c. Click **OK**.

Note: Nodes that are members of a domain are not affected. Additional information about Simple File Sharing is available at: http://microsoft.com/technet/security/advisory/906574.mspx.

2. Change the local security settings. New default Windows policies limit secure object access to the creator of the object.

Caution: Do not skip these steps. If these settings are not correct, you will be unable to list OPC Servers from the OPC client node and will receive an `80070005 access denied` error.

To change these policies, go to **Control Panel** > **Administrative Tools** > **Local Security Policy.** Open **Security Settings** > **Local Policies** > **Security Options** and browse to change:

- **Network access:** Sharing and security model for local accounts. Right-click and select **Properties**, and then **Classic – local users authenticate as themselves**. Click **OK**.
- **System Objects:** Default owner for objects created by members of the **Administrators** group. Right-click and select **Administrators** group. Click **OK**.

Configure DCOM Settings

When using local administrator accounts, PI OPC Client applications and most OPC Servers will generally work with the default settings found in the **Windows Component Services** administrative tool. However, OSIsoft recommends that you review the configuration if settings might have changed since the last operating system installation.

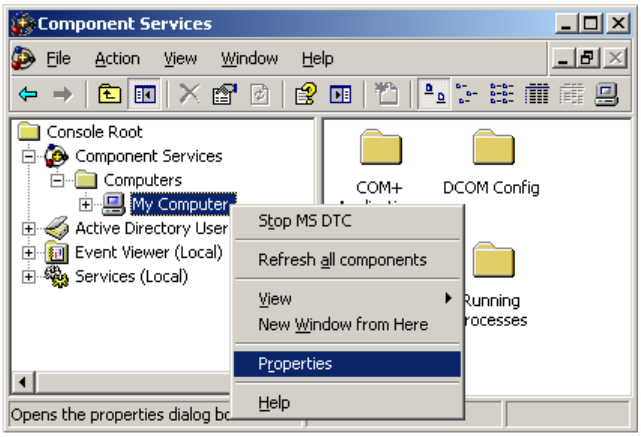
Note: If you are using local user accounts, it is important to complete the procedure described in Step 4.

Perform these procedures on each node – the OPC Server and Client node:

1. Launch the DCOM Configuration utility:

   Go to **Start** > **Run**. Type `dcomcnfg` and click **OK**.

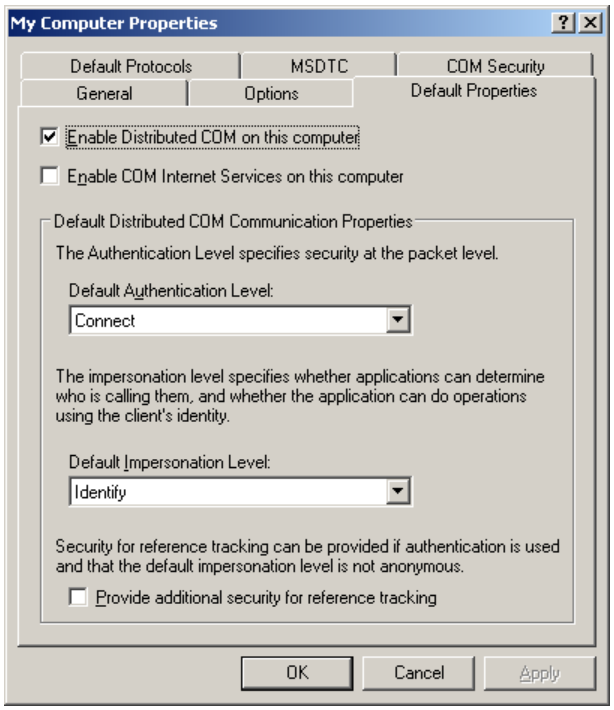
2. Select **Console Root** > **Component Services** > **Computers** > **My Computer** in the **Component Services** dialog. Right-click on **My Computer** and select **Properties**:



3. Go to the **Default Properties** tab in the **My Computer Properties** dialog and verify that:

- **Enable Distributed COM on this computer** is selected.
- **Default Distributed COM Communication Properties** are set to:
  - Connect for Default Authentication Level
  - Identify for and Default Impersonation Level

Note: These **Default Properties** are appropriate for most cases. However, due to individual OPC server implementations, these settings might not work occasionally. If this is the case, identify and use the workable settings.



4. If the OPC User account is a local user account, you must add that account to **Launch and Activation Permissions** Access Control Lists (ACLs):

a. From the **COM Security** tab, click **Edit Limits . . .** under **Launch and Activation Permissions** and add the user to the **Edit Limits** ACL.

b. Next, click **Edit Default** . . . under **Launch and Activation Permissions** and add the user to the **Edit Default** ACL.

5. For both the local administrator or local user:

- Add the OPC User account to the **Access Permissions** ACL. To do this:

a. First, from the **COM Security** tab, click **Edit Limits . . .** under **Access Permissions** to add the user to the **Edit Limits** ACL.

b. Then, click **Edit Default** . . . under **Access Permissions** to add the user to the **Edit Default** ACL.

- Next, set **Access Permissions** for the default users and groups as follows:

Note: Do not remove any of the default users or groups; they are necessary for proper functioning of the Component Services.

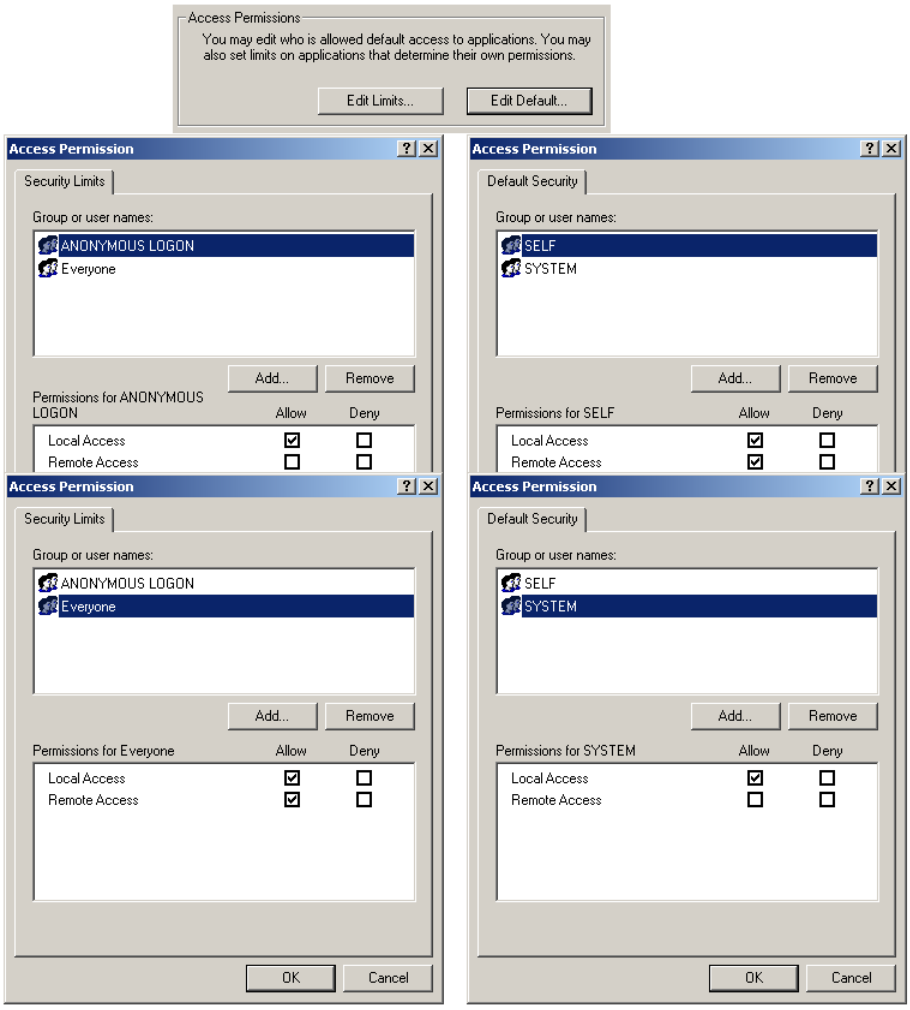
a. Select the **COM Security** tab in the **My Computer Properties** and click **Edit Limits . . .** , then set the **Access Permissions** for the default users and groups:

User	Setting	Access Type(s)
Everyone	Allow	Local Access and Remote Access
ANONYMOUS LOGIN	Allow	Local Access

b. Next, click **Edit Default** . . . , then set these **Access Permissions** for the default users and groups:

User	Setting	Access Type(s)
SELF	Allow	Local Access and Remote Access
SYSTEM	Allow	Local Access

The settings should look like this:



- Next, set the following **Launch and Activation Permissions** for the default users and groups as follows:

Note: Do not remove any of the default users or groups; they are necessary for proper functioning of the Component Services.

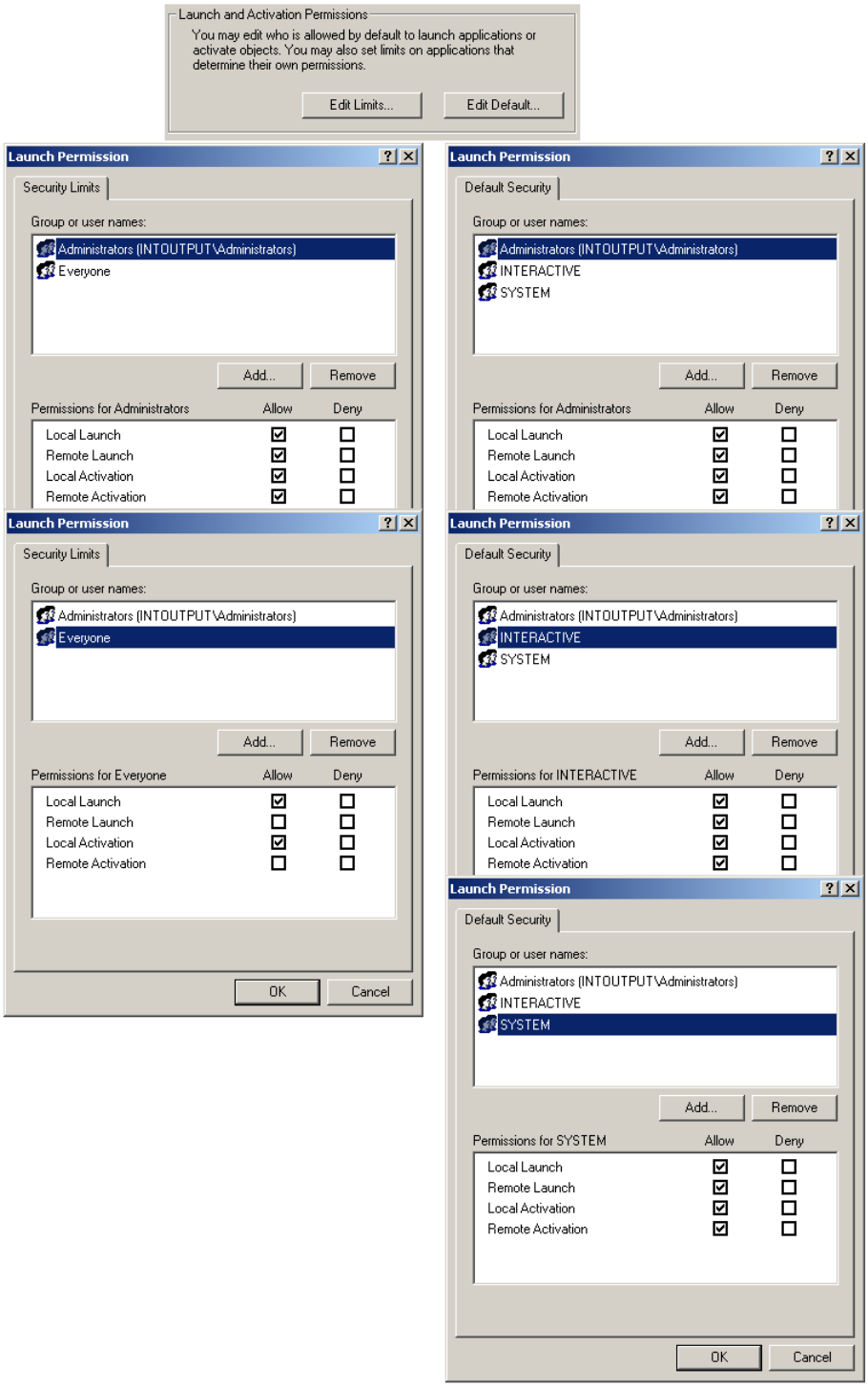
a. Select the **COM Security** tab in the **My Computer Properties**, click **Edit Limits . . .** , then set these **Launch and Activation Permissions** for the default users and groups:

User	Setting	Access Type(s)
User under which OPC Server runs, or Administrators	Allow	Local Launch, Remote Launch, Local Activation, and Remote Activation
Everyone	Allow	Local Launch and Local Activation

b. Next, click **Edit Default . . .** , then set the **Launch and Activation Permissions** for the default users and groups, as follows:

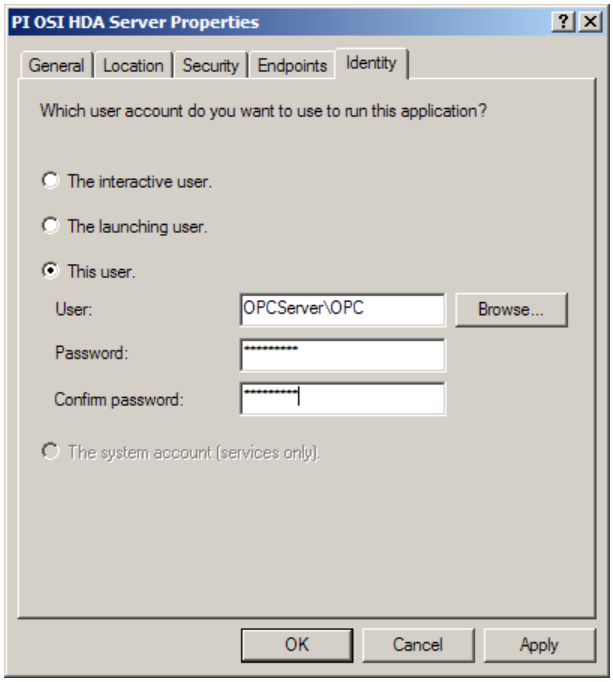
User	Setting	Access Type(s)
User under which OPC Server runs, or Administrators	Allow	Local Access and Remote Access
INTERACTIVE	Allow	Local Access and Remote Access
SYSTEM	Allow	Local Access and Remote Access

The settings for the **Launch and Activation Permissions** should look like this:



Perform these steps on the OPC Server node only. Configure the server-specific settings on the OPC Server to define which user account will run the OPC Server in the Component Services dialog:

1. Go to **Console Root > Component Services > Computers > My Computer > DCOM Config**.
2. Find the OPC Server in the list of applications, right-click and select **Properties**.
3. Select the **Identity** tab in the **OPC Server Properties** dialog. Select **This user** option and enter the OPC username and password for the OPC user you created.
4. Click **OK**.



Caution: The **General** tab must use **Default for the Authentication Level**. In the **Security** tab, select **Use Default** for the first two permissions and use the default settings for the Configuration permissions. The **Location** and **Endpoints** tabs must use the Operating System default configuration as well. For more details, see *Appendix A - Related DCOM Fundamentals* (page 23).

PI OPC DA/HDA Server COM Objects for 64-bit Operating Systems

If you run the **DCOM Configuration** utility, `dcomcnfg`, in the 64-bit version of Microsoft Windows 7 and Microsoft Windows Server 2008 R2, you may not be able to see an entry for **PI OSI DA Server** or **PI OSI HDA Server** in the list of COM objects.

To find these servers, make the **PI OSI DA Server** and **PI OSI HDA Server** entries visible before you run `dcomcnfg`:

1. Run `MMC /32 %windir%\syswow64\comexp.msc` to open the 32-bit version of **DCOM Configuration** utility. This needs to be done just once. Then, these entries will permanently appear when running `dcomcnfg`.
2. Use the **PI OSI DA Server** and **PI OSI HDA Server** entries to configure the OPC server-specific settings on Windows 7 and Microsoft Windows Server 2008 R2 Operating Systems.

Note: This section does not apply for the 64-bit version of Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Vista, and Microsoft Windows Server 2008.

Settings for an Enabled Windows Firewall

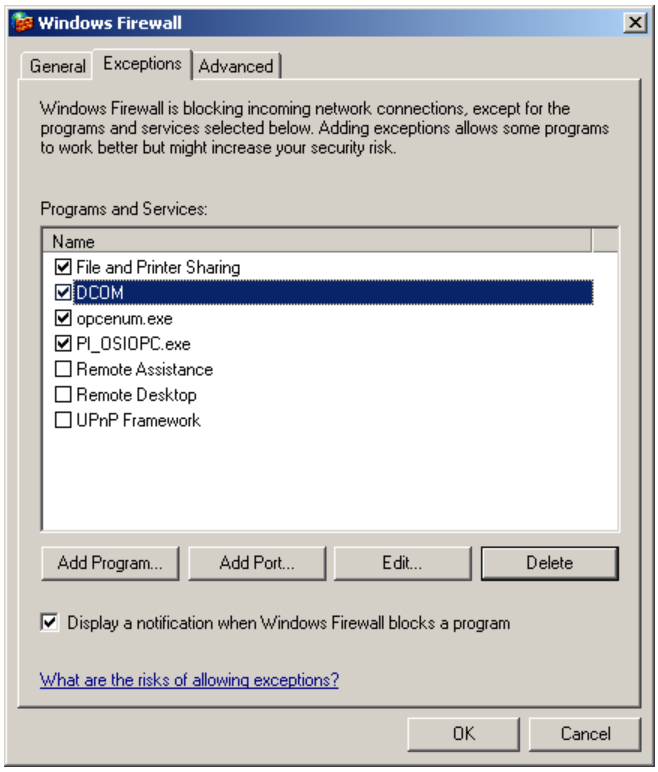
The settings described in this section apply to any scenario where a Windows firewall has been enabled, independently of the Workgroup or domain configuration.

Set OPC Server Node Windows Firewall Exceptions

If Windows Firewall is enabled on the server node, use these steps to set the required **Exceptions** on the OPC Server node firewall:

1. Go to **Start > Control Panel > Windows Firewall**.
2. Select the **General** tab of the **Windows Firewall** dialog, and select **On**.
3. Select the **Exceptions** tab and edit the **Program and Services** list in the **Windows Firewall** dialog to enable these minimal exceptions to allow DCOM and OPC Applications to work:

- TCP Port 135 is required for DCOM.
- Program `opcenum.exe` is required for the PI OPC client in order to browse existing OPC Servers.
- OPC Server application executable, for example `PIOSIOPC.exe`, is required for the interface node to collect data from the OPC Server.
- **File and Printer Sharing** is required only if the OPC Applications use host names instead of IP addresses. This setting will also allow incoming ICMP packets; that is, `ping <remote opc node>`.



4. With the exceptions covered in the previous step, the Windows Firewall is fully configured to allow DCOM communication to all nodes. Optionally, 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 and enter the OPC Client node's IP address and click **OK**.

   For example, to add the program `Opcenum` to the Windows Firewall exception list and restrict the source of the incoming TCP connection to the OPC Client node exclusively:

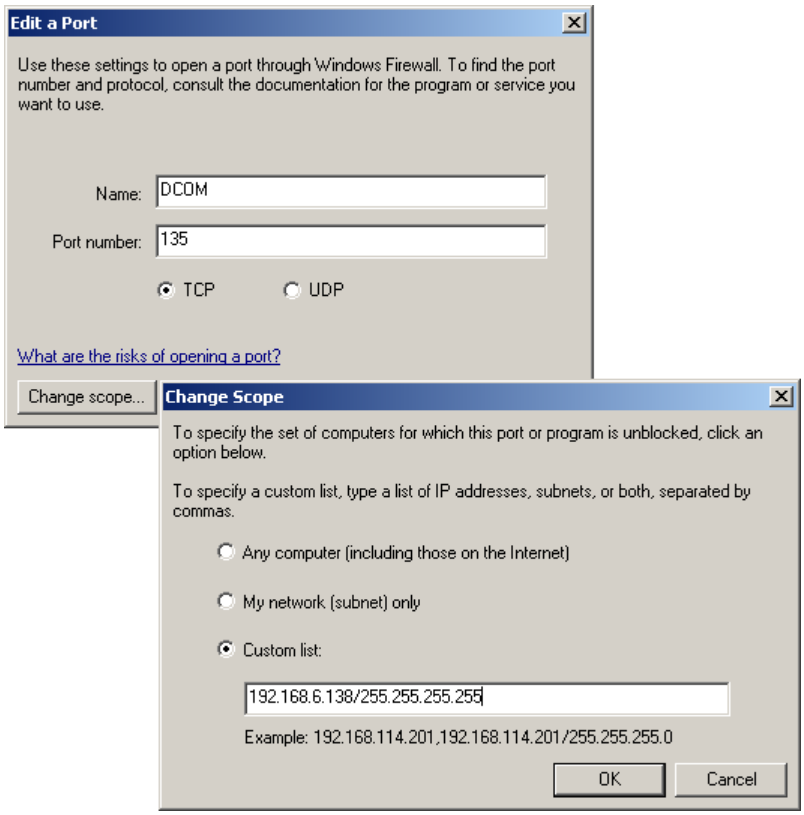
   a. Go to **Start > Control Panel > Windows Firewall**.

   b. Select the **Exceptions** tab on the **Windows Firewall** dialog and click **Add Program…**. Browse to `C:\WINDOWS\system32\opcenum.exe` and click **Open**.

   c. Click **Change scope…** in the **Add a Program** dialog, select the **Custom list** option, enter the IP Address of the OPC Client node and click **OK**.

   d. Click **OK** in the **Add a Program** window.

This next example shows how to restrict the source of the incoming TCP connection to port 135 to the OPC Client node with IP Address 192.168.6.138. Here, the IP Address 192.168.6.138 is added to the set of computers for which the port 135 is allowed:



Note: These same types of restrictions can be made to the different ports and programs considered on the exceptions list.

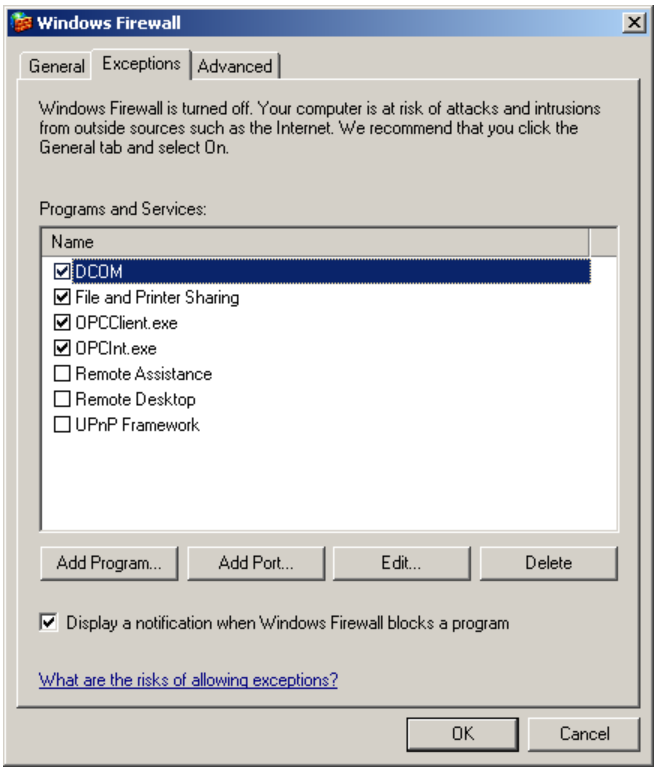
Set OPC Client Node Windows Firewall Exceptions

If Windows Firewall is enabled, on the client node, use these steps to set the required **Exceptions** on the OPC Client node firewall:

1. Go to **Start** > **Control Panel** > **Windows Firewall**.
2. Select the **General** tab of the Windows Firewall dialog, and select **On**.
3. Click on the **Exceptions** tab and edit the **Program and Services** list to enable these minimal exceptions to configure the Windows Firewall to allow DCOM communication to all nodes:

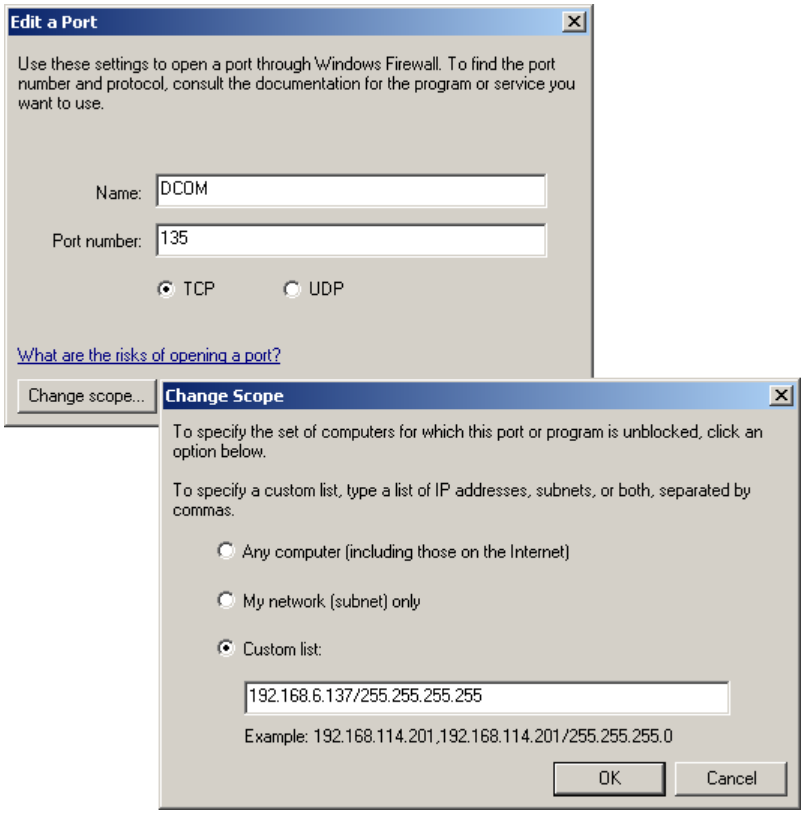
- TCP Port 135 is required for DCOM.
- Program `OPCClient.exe` is required for the PI OPC client in order to connect to the OPC Server.

- Program `OPCInt.exe` is required for the interface in order to collect data from the OPC Server.
- **File and Printer Sharing** is required only if the OPC Applications use host names instead of IP addresses. This setting will also allow incoming ICMP packets; that is, `ping <remote opc host>.`



4. Optionally, to restrict the source of the incoming TCP connections to the OPC Server node exclusively, click **Add Program** or **Add Port and Change scope…**. Select the **Custom** list option and enter the OPC Server node's IP address and click **OK**.

   In this example, to restrict the source of the incoming TCP connection to port 135 to the OPC Server node with IP Address 192.168.6.137, the IP Address 192.168.6.137 is added to the set of computers for which the port 135 is allowed:



Note: These same types of restrictions can be made to the different ports and programs considered on the exceptions list.

Scenario 2: One of Two Nodes is Within a Windows Domain

When one node is member of a domain and the other is not, both the PI OPC Interface/Client and the OPC Server must run under a local user account. This account must have the same username and password on both nodes.

To properly configure DCOM when one node is member of a Windows domain:

- Follow the procedures for *Scenario 1: OPC Nodes Are Not Members of a Windows Domain* (page 3).
- For the user account creation, ensure that you create a local account, not a domain account, on the node that is member of the Windows domain. In this case, the local account on the node that is member of a domain can use the same user name and password as any domain account.

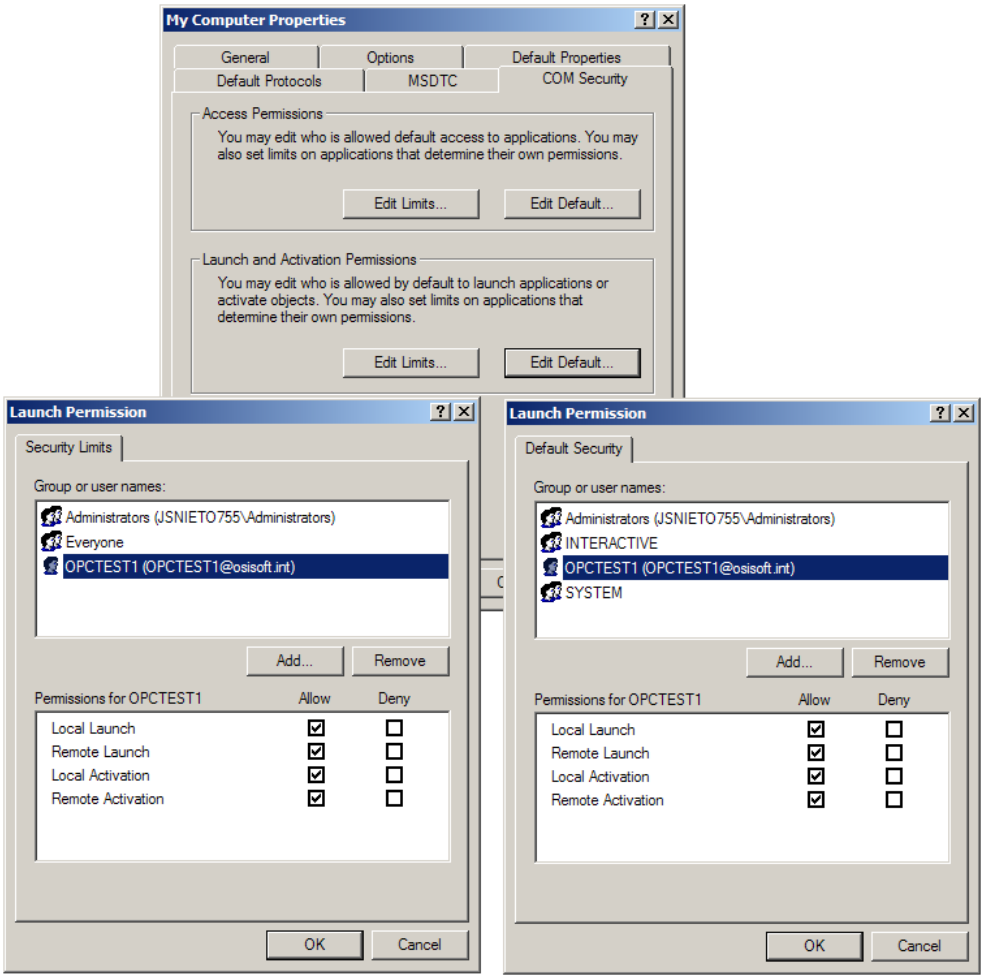
Caution: If these guidelines are not followed, the attempt to connect to the OPC Server node will fail with an Access Denied error.

Scenario 3: Both Nodes Share a Common Domain

If the OPC server and client run on separate nodes, and both nodes are members of a Windows domain, you must use *either* domain *or* local accounts.

To properly configure DCOM when both nodes are members of a Windows domain:

- Follow the procedures for *Scenario 1: OPC Nodes Are Not Members of a Windows Domain* (page 3), except for the *creation of local accounts* (page 4) if domain accounts are used.
- When using domain accounts, grant domain users **Launch and Activation Permissions**.
- To grant these permissions, select the **COM Security** tab in the **My Computer Properties** dialog from the OPC server node. Then, use the **Launch and Activation Permissions** tab to add to the **Edit Limits** and **Edit Defaults** for each account that will access the OPC Server from the remote OPC client node. For details about these settings, see Step 4 in *Configure DCOM Settings* (page 6). As an example, the following figure shows that a domain account, **OPCTEST1**, has been added to the **Launch and Activation Permissions**.



Scenario 4: Both Nodes Do Not Share a Common Domain

If the OPC server and client run on separate nodes, and each node is a member of a separate Windows domain, you must use *either* domain accounts and establish bi-directional trusts between domains *or* local accounts.

Note: Refer to the Microsoft Windows Server administration documentation on how to configure domain trusts.

To properly configure DCOM when both nodes are members of separate Windows domains:

- Follow the procedures for *Scenario 1: OPC Nodes Are Not Members of a Windows Domain* (page 3), except for the *creation of local accounts* (page 4) if domain accounts are used.
- When using domain accounts, grant domain users **Launch and Activation Permissions**.
- To grant these permissions, select the **COM Security** tab in the **My Computer Properties** dialog from the OPC server node. Then, use the **Launch and Activation Permissions** tab to add to the **Edit Limits** and **Edit Defaults** for each account that will access the OPC Server from the remote OPC client node. For details about these settings, see Step 4 in *Configure DCOM Settings* (page 6).

Appendix A

Related DCOM Fundamentals

This guide provides DCOM configuration procedures that OSIsoft recommends when you use OSIsoft software. If, for some reason, these recommended settings cannot be used, the information in this appendix provides an overview of DCOM, its most common security aspects, and common DCOM errors. This appendix also offers generic guidelines for the user account configurations, authentication levels, the `dcomcnfg` administrative tool and event viewer logging.

DCOM Overview

All current OPC server and client applications are based on Microsoft's COM/DCOM communication model. The forthcoming OPC UA (OPC Unified Architecture), which contains inherent security features, will supersede this model when released.

COM (Component Object Model) provides a set of interfaces allowing software components to communicate on a single computer. DCOM (Distributed Component Object Model) is the network communication protocol that extends COM to allow different software components to communicate between networked nodes. Such communication requires a proper DCOM security configuration in OPC Client and Server nodes. Since both nodes make use of callbacks, where OPC Servers also act as DCOM clients, and OPC Clients also act as DCOM Servers, the procedures described in this guide generally apply to both Server and Interface nodes. Exceptions are noted.

Factors such as Operating System version and patching, domain or workgroup configuration, antivirus and firewall configuration, network architecture, and user account types will affect which DCOM settings can be applied to a specific deployment to obtain a secure solution. For current installations, OSIsoft recommends security measures be implemented at each of those levels in addition to the recommendations described in this guide at a DCOM object level.

For new OPC deployments where high security is imperative, OSIsoft encourages you to look into OPC Unified Architecture applications. Security is an integral part of these products.

At all times, especially at the control process network level, OSIsoft recommends security measures be implemented for all OPC nodes and platforms on which OPC applications reside, and that security and its configuration be constantly assessed and monitored.

Using Default DCOM Settings

Default Authentication Level and Default Impersonation Level

The DCOM security model uses the extensible security provider in Microsoft Windows. For Microsoft Windows NT based Operating Systems operating in a Workgroup, NTLMSSP (NT LAN Manager Security Support Provider) is the common security provider used by DCOM. When OPC nodes are members of a domain, Active Directory for Windows Server 2003/2008 include Kerberos authentication protocol as the security provider. Both mechanisms, NTLMSSP and Kerberos, ensure:

- Authentication by verifying the user that is requesting access to the server.
- Authorization by ensuring that the user has permissions to use the server.

Different levels of authentication and privacy are supported by DCOM:

- **None:** No authentication occurs. Unauthenticated users are allowed to connect.
- **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:** Authenticates credentials and verifies that no data has been modified in transit.
- **Packet Privacy:** Authenticates credentials and encrypts the packet, including the data and the sender's identity and signature.

DCOM authorization is supported by different levels of impersonation:

- **Anonymous:** The client is anonymous to the server. Even though the server can impersonate the client, the identity of the user associated with the PI OPC Interface is hidden from the OPC server.
- **Identify:** The OPC Server can identify the user associated with the PI OPC Interface, and can perform actions as that user.
- **Impersonate:** The OPC Server can perform actions as the user associated with the PI OPC Interface, 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 PI OPC Client, including access to other computers as that user (only supported in Windows 2000 and later.)

The default settings of **Connect** and **Identify** are appropriate for most cases. However, due to individual OPC server implementations, these settings might not work occasionally. If this is the case, identify and use the workable settings.

Predominant Authentication level

When configuring DCOM, it is important to consider that on the PI OPC Interface node, any Authentication Level set on the PI OPC Client application or the PI OPC Interface will override the authentication level set in the system-wide settings configured using the **Component Services** administrative tool.

The same principle applies for the OPC Server node. Any Authentication Level set specifically on the OPC server-specific settings using the **Component Services** administrative tool will override the Authentication Level set under the system-wide settings.

Now, having this in mind, and knowing which Authentication Level prevails on each node, it is important to understand what Authentication Level will be used during the execution of the different RPC's between both nodes. The final Authentication Level used by each RPC will be set by the computer that has the highest minimum level of Authentication. This means, for example, that if the OPC server dictates that the Authentication Level is **Packet Integrity**, even though the Authentication Level for the OPC Client is set to **None**, the RPC's will use **Packet Integrity**, regardless of which node executes the RPC.

DCOM Settings Configuration with Dcomcnfg.exe

The DCOM settings configuration will determine which users can activate objects, launch and access applications, and the user ID under which applications will run.

Theses settings can be configured in one of two ways:

- Programmatically, when an application starts up, it can declare its settings when it initializes COM.
- Manually, before the application starts up, the settings can be configured in the registry by using the Component Services administrative tool, that is, `dcomcnfg.exe`.

The **Windows Component Services** administrative tool allows you to configure the system-wide settings that will apply to all COM applications running on the computer. Also, the tool provides access to the server-specific settings.

System-wide settings

The system-wide settings will be used by COM applications when their specific settings indicate to use the default settings. The tabs that require configuration for OPC communication are:

Default properties which enables DCOM and sets the default DCOM communications properties:

- **Default Authentication Level** indicates what minimum degree of authentication is required for communication with an application.
  - Since **None** allows unauthenticated users to connect, this setting is not recommended. For further details, see *Authentication Level None: (ANONYMOUS LOGON)* (page 32).
  - A minimum authentication level of **Connect** is recommended.
  - Further hardening could be pursued with more restrictive authentication levels such as **Packet** and higher.
  - If these settings affect the OPC nodes operations performance, a minimum level of **Connect** is recommended and lower level solutions, such as VPN, are recommended.
- **Default Impersonation Level** is the process by which a server makes a call on behalf of a client and presents the client's identity and credentials in place of its own when making the call. **Anonymous Logon** is not recommended and should be restricted by OPC Server implementations. For further details, see *Authentication Level None: (ANONYMOUS LOGON)* (page 32).

COM Security which allows you to set the default Access Control List (ACL) for all objects with the following permissions:

- **Access Permissions** provide permissions to exchange data with an application.
  - The **Edit Default…** button updates the (Access Control List) ACL that determines which users have default Access Permissions.
  - The **Edit Limits…** button updates the ACL that sets the limits for applications that programmatically configure their own DCOM permissions.

- **Launch and Activation Permissions** that will provide the permissions to start an application.
  - The **Edit Default…** button updates the ACL that determines which users have default **Launch and Activation Permissions**.
  - The **Edit Limits…** button updates the ACL that sets the limits for applications that programmatically configure their own DCOM permissions.

Default protocols set TCP/IP as the network protocol available to DCOM. If **Connection-oriented TCP/IP** is not present by default, add it to the protocol list and move it to the top of the list. In fact, other protocols are not required between OPC nodes, thus OSIsoft recommends TCP/IP as the only network protocol available at the Operating System level. Set this by using the Windows Registry, with the permission of your OPC node administrator.

Server-specific settings

The server-specific settings configure the application's specific settings to the default, the system-wide settings, or to a custom DCOM configuration unique to the application itself. The tabs that require configuration for OPC communication are:

General:

Sets the Authentication Level that indicates the minimum degree of authentication the server will accept. The level chosen here *overrides* the authentication level chosen on the system-wide settings. If however the default settings are chosen, then the system-wide Authentication Level settings apply.

Location:

Enables DCOM to locate the computer where the application runs. **Run application on this computer** is selected by default. If that is not the case, then change the setting to **Run application on this computer**.

Security:

Updates the ACL for the specific object, according to the settings in the **Launch and Activation Permissions**, and the **Access Permissions** dialogs.

- If the **Use Default** option is selected, then the specific application uses the system-wide settings.
- If the **Customize** option is selected, then the specific application uses its own ACL.

Endpoints

Defines the set of protocols and endpoints available for use by clients of the specific DCOM server. If …default system protocols… are set, then **Connection-oriented TCP/IP protocol configured in the system-wide settings will be used. If** …default system protocols… are not present by default, then add **Connection-oriented TCP/IP to the protocol list.** When supported, OPC Servers can restrict the use to a specific port or a range of ports to further restrict the security of the OPC node.

Identity

Defines which user account is used to run the application. OSIsoft recommends that you specify an account created for use with OPC clients and servers. Using **The interactive user** and **The launching user** settings can lead to several problems that can be easily avoided by using the option **This user**.

User accounts

The DCOM Authentication process verifies the user account that is requesting access to the server. The user has to be specified on the appropriate ACL in the system-wide settings or server-specific settings. This process will be handled by the security provider, either NTLMSSP or Kerberos, depending on the network that the computers are in, the Operating Systems, and whether a Windows domain or a workgroup is used. The most common scenarios and guidelines for setting up user accounts are as follows:

- If the OPC server and client will run on the same computer, then any account can be used, including the local system account.
- If the OPC server and client will run on separate nodes, and one node is member of a Windows domain, but the other node is not, then identical local accounts must exist on both nodes.
- If the OPC server and client will run on separate nodes, and both nodes are members of a Windows domain, then either domain or local accounts can be used.
- If the OPC server and client will run on separate nodes that do not share a Windows domain, then identical local accounts (same user name and password) must exist on both nodes. Local system accounts cannot be used.

You can set the user account associated with a process in several ways for *interactive programs* (page 29) and for programs that run as a *Windows service* (page 30).

Interactive programs

For interactive programs such as the PI OPC Client, the user account will be the same as that of the user running the program. Generally, the user that logged into Windows will be the owner of the interactive program process, unless a different account is used through the **Run As** command.

If this specific account is a local user account, by default, it will not be assigned sufficient privileges to run applications installed by an administrator.

To allow this user to run applications and services such as PI OPC Client and PI OPC Interface, add the local user account to the security properties of the folder that contains the application's executable and assign **Full Control** permissions.

If you use Windows Vista, Windows Server 2008, or Windows 7, the **Run As** option is no longer available in the right-click menu. In this case, to run an application with a different user account than the one that is currently logged in, open the command line console and execute the following commands:

- In a workgroup environment:

  ```
  Runas /u:username Executable
  ```

- In a domain environment:

  ```
  Runas /u:domain\username Executable
  ```

Programs that run as a Windows service

For programs that run as a Windows service, specify the user account in the **Log On** tab of the service. The user account used here must be the same as the one specified in the Identity tab of the *DCOM Server-specific settings* (page **Error! Bookmark not defined.**). To use the **Services** snap-in to verify or change this user:

1. Select **Run…** from the **Start** menu and enter `services.msc`.
2. Right-click on the specific service and select **Properties**.
3. Select the **Log On** tab and specify the user account in the **This account** section.

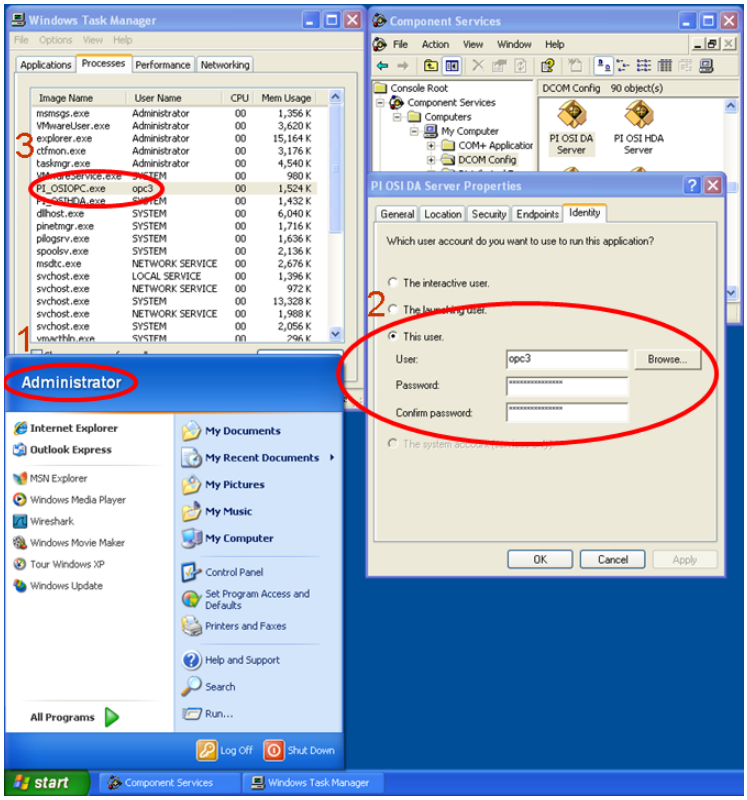
Further recommendations

To ensure the correct process is run by the appropriate user, OSIsoft recommends the **Processes** tab of the **Windows Task Manager** be monitored. To launch the **Windows Task Manager**, right-click on the Taskbar and select **Task Manager**.

The user account that will be used to run the OPC server should be included in the ACLs and configured as described in *Configure DCOM Settings* (page 6). It should also be included in the **Identity** tab of the server-specific settings in the **Component Services** administrative tool. If the OPC server runs as a Windows service, the account specified in the **Identity** tab must be the same as the one specified in the **Log On** tab under the **Service Properties** dialog.

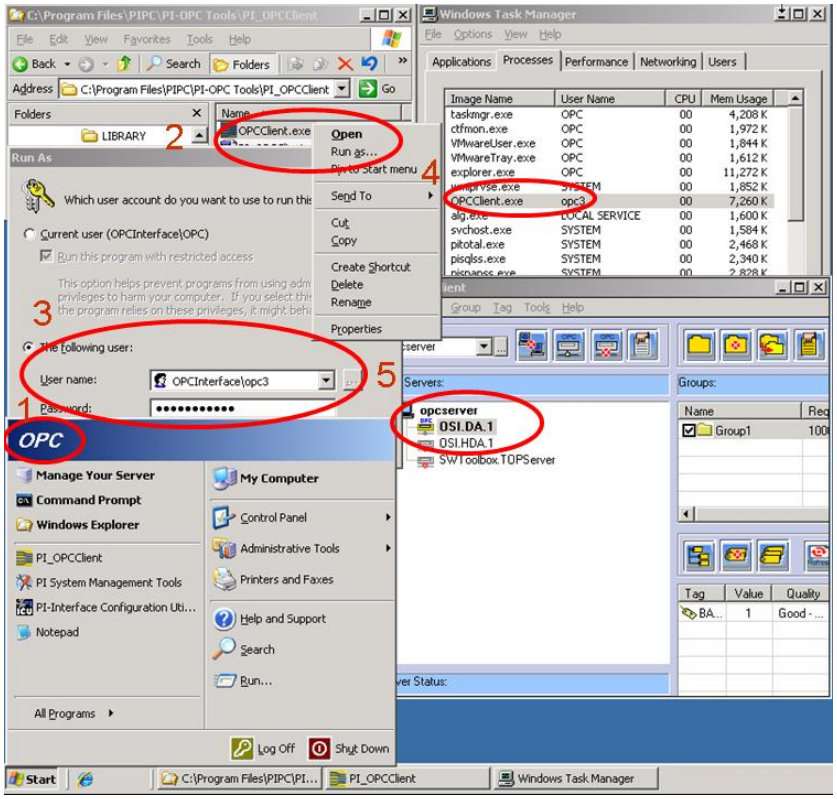
The following example summarizes a common scenario where multiple accounts are used. The node that runs the OPC Server is shown as containing:

1. A user **Administrator** with administrator privileges is logged in to the computer.
2. A user **opc3** is a limited user account configured on the OPC Server specific-settings to run the server application.
3. The server process that is run by the **opc3** user. It appears on the **Windows Task Manager** as soon as the client establishes the connection with the server, as shown in the second illustration.



Continuing with the example, the next illustration shows that the PI OPC Client is run by the **opc3** user since, as described above, this is the only user that can run the server application.

1. The user **OPC** with administrator privileges is logged in to the computer.
2. The **OPC** user, even though it has administrator privileges on the PI OPC Interface computer, is not allowed to run the server. To resolve this, right-click over the PI OPC Client application and select **Run as…**
3. In the **Run As** dialog, enter the **opc3** user to run the server application. This is the only user configured on the server side to run the server application.
4. The PI OPC Client process run by the **opc3** user then appears on the **Windows Task Manager**.
5. The PI OPC Client successfully connects to the specific OPC server.



Authentication Level None: (ANONYMOUS LOGON)

With the configuration guidelines described through the guide, the OPC DA/HDA server, among others, will accept any Default Authentication level specified by the Client, except when the Authentication level on the OPC Server node is set to **None**.

OSIsoft does not recommend that you use the unauthenticated communication that occurs with the authentication level set to **None**. This would allow any user in the network to connect to the OPC Server node without any type of authentication and auditing. For recommended settings, see *Configure DCOM Settings* (page 6).

Refer to this section only if you need information about the security implications of using unauthenticated DCOM communication through **Anonymous Logon**.

Authentication level: Server (None) – Client (None) (NOT RECOMMENDED)

If you use unauthenticated DCOM communication and your settings are:

On the computer that runs the OPC Server:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCEnum specific	None	
OPCServer specific	None	

On the computer that runs the OPC Client:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCClient specific	None	

The **Anonymous Logon** in the **Access Permissions Edit Limits** ACLs on both Client and Server nodes must be added. This allows unauthenticated communication, that is, any user in the network can connect to the OPC Server node without any type of authentication and auditing.

If remote **Anonymous Logon** is not allowed on the OPC Server node, the OPC Servers will not be visible to the PI OPC Client since the access to the COM application OPCEnum will fail, and the node running the OPC server will deny access to the PI OPC Client and the PI OPC Interface. PI OPC Client will not report any error code; it will simply not list any OPC Servers. PI OPC Interface will report an error on the PIPC.log that looks like this:

```
OPCpi> 1> /f=00:00:02
OPCpi> 1> Unable to find any such OPC Server on that node
OPCpi> 1> CoCreateInstanceEx: : No such interface supported
(80004002)
OPCpi> 1> Can't connect to OPC server, going into slow cycle
wait
```

If remote **Anonymous Logon** is not allowed on the OPC Client node and allowed on the OPC Server node, the PI OPC Client is able to connect to the OPC Server, but it obtains the error `Unable to advise for shutdown notification` while establishing the unauthenticated connection. When connected, a group can be created on the PI OPC Client to read data from an OPC Server Item.

Click **OK** on this Error window and create a group on the PI OPC Client to read data from an OPC Server Item. Be advised that when the item from which the data is to be read is added to the group, the message `Advise returns error 80040202`, will be returned when trying to poll data from the PI OPC Client.

The two errors described here indicate that the OPC Client node is not allowing OPC Server callbacks to the **Anonymous Logon** user.

The unauthenticated communication for each RPC can be seen through the use of Wireshark to capture network traffic information: Select any DCOM package and observe that the **Auth Length** is set to **0**. Any other authentication level forces this field to have a value higher than **0** and for some NTLMSSP or Kerberos authentication field to be included on the DCE RPC layer.

Authentication level: Server (None) – Client (Connect)

If the Authentication Level is set to **None** on the OPC Server node, but is set to **Connect** on the OPC Interface node as shown here:

On the computer that runs the OPC Server:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCEnum specific	None	
OPCServer specific	None	

On the computer that runs the PI OPC Client:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCClient specific	Connect	Identify

These results are expected:

- The connection gets established.
- All DCOM request calls set the Authentication Level to **Connect**, regardless of whether the calls are initiated on the OPC Server or PI OPC Interface node.
- All DCOM response calls set the Authentication Level to **None**, regardless of whether they are initiated on the OPC Server or PI OPC Interface node.
- On Wireshark, as mentioned earlier, the **Auth Length field** will have a value higher than **0**. There will also be different Authentication parameters associated with each Authentication Level that will vary depending on the Authentication Level selected. In this case, on the DCE RPC layer the **Auth Level** field will reflect a setting of **Connect**.

Authentication level: Server (None) – Client (Packet)

If the Authentication Level is set to **None** on the OPC Server node, but is set to Packet on the OPC Interface node as shown here:

On the computer that runs the OPC Server:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCEnum specific	None	
OPCServer specific	None	

On the computer that runs the OPC Client:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCClient specific	Packet	Identify

These results are expected:

- The connection gets established.
- All DCOM request and response calls set the Authentication Level to **Packet**, regardless of whether they are initiated on the OPC Server or PI OPC Interface node.
- On Wireshark, as mentioned earlier, the **Auth Length** field will have a value higher than **0**. There will also be different Authentication parameters associated with each Authentication Level that will vary depending on the Authentication Level selected. In this case, on the DCE RPC layer the **Auth Level** field will reflect a setting of **Packet**.

Authentication level: Server (None) – Client (Packet Privacy)

If the Authentication Level is set to **None** on the OPC Server node, but is set to **Packet Privacy** on the OPC Interface node as shown here:

On the computer that runs the OPC Server:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCEnum specific	None	
OPCServer specific	None	

On the computer that runs the OPC Client:

	Default Authentication	Default Impersonation
System wide	None	Identify
OPCClient specific	Packet Privacy	Identify

These results are expected:

- The connection gets established.
- All DCOM request and response calls set the Authentication Level to **Packet Privacy**, regardless of whether they are initiated on the OPC Server or PI OPC Interface node.
- On Wireshark, as mentioned earlier, the **Auth Length** field will have a value higher than **0**. There will also be different Authentication parameters associated with each Authentication Level that will vary depending on the Authentication Level selected. In this case, on the DCE RPC layer the **Auth Level** field will reflect a setting of **Packet Privacy**.

Monitoring and Troubleshooting DCOM Settings

Auditing Policies and Registry Settings

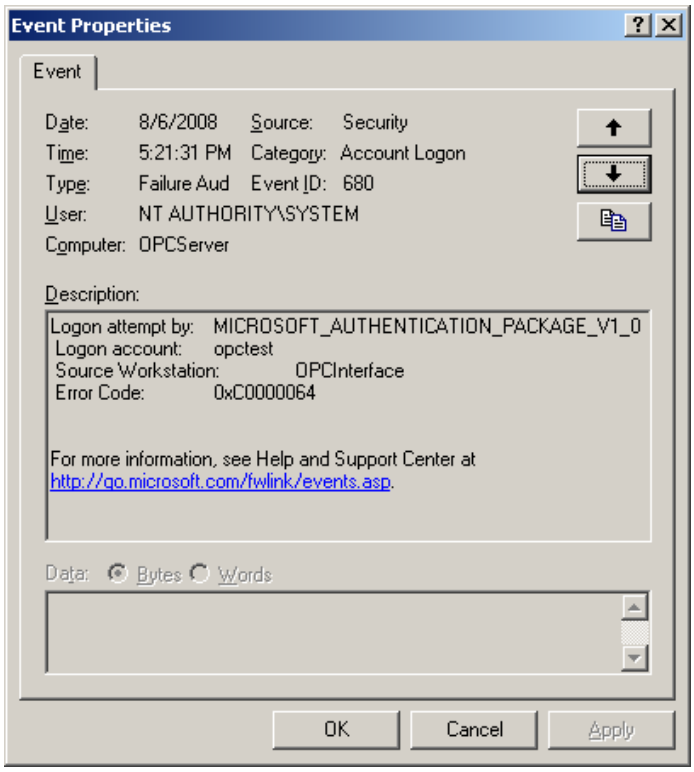
There are several audit policies and registry settings that can be configured to increase the amount of information that Windows provides to solve DCOM configuration problems, and track potential security vulnerabilities. To see this information in the **Windows Event Viewer**, go to **Start > Control Panel > Administrative Tools > Event Viewer** or go to **Start > Run…** and enter `eventvwr`.

Audit Policy

As a first step toward diagnosing DCOM communication problems, OSIsoft recommends these settings:

- Log Failures on both the OPC server and client nodes. To do so, enable **Audit account logon events**, **Audit logon events**, and **Audit object access**.
- Run the Local Security Policy snap-in: **Start > Control Panel > Administrative Tools > Local Security Policy**.
- Select **Security Settings > Local Policies > Audit Policy** and enable **Audit account logon events**, **Audit logon events**, and **Audit object access** to audit Success and Failure attempts. To avoid flooding the log, set **Audit object access** to log only failures.

  Monitor failure messages on the **Security** plug-in of the **Windows Event Viewer**. For example, if a PI OPC Client tool on one node attempts to establish a connection to a second node within the same Workgroup through a user account that does not exist on the server node, error code `0xC0000064` will appear. This indicates a failed logon due to an unknown user name on the server node. A failed logon due to a bad password will be identical, except that the error code will be `0xC000006A`.



Registry Settings for DCOM Failure Logging

To enable additional logging for DCOM failures, create the following three entries as a DWORD Value in the registry under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole` and set their values to **1**:

- `DWORD ActivationFailureLoggingLevel`

  This key sets the verbosity of event log entries about failed requests for component launch and activation.

- `DWORD CallFailureLoggingLevel`

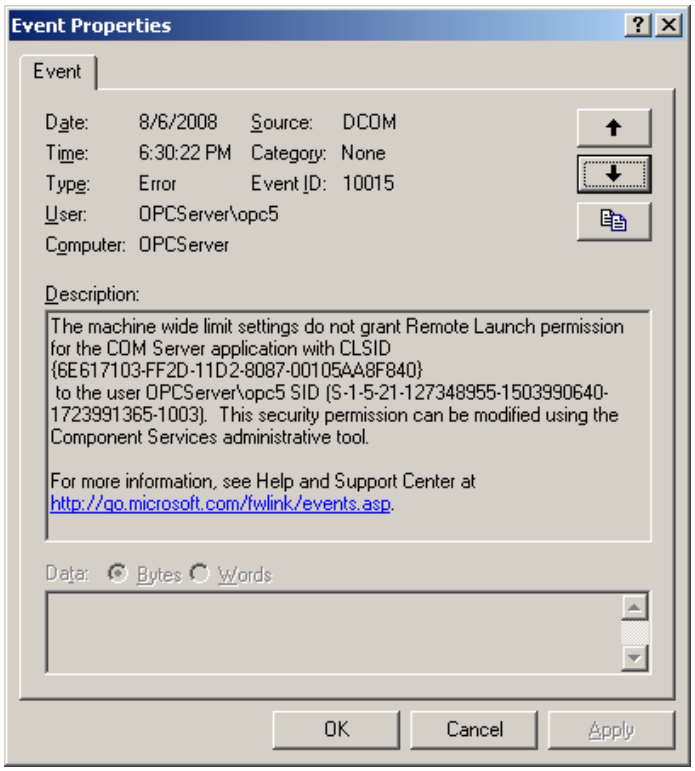
  This key sets the verbosity of event log entries about failed calls to components once the component has been activated.

- `DWORD InvalidSecurityDescriptorLoggingLevel`

  This key sets the verbosity of event log entries about invalid security descriptors for component launch and access permissions.

Restart any running DCOM servers for setting changes to take effect. You can view DCOM security errors in the **Windows Event Viewer**. Because only errors get logged, you can leave this additional logging enabled.

For example, a system log event that occurs when the OPC Server system-wide limit settings do not grant remote launch permission. This figure shows a failure on a Windows 2003 SP2 node when a user with no remote launch permissions in the system-wide limits ACL tries to launch the OPC Server:



Common DCOM Errors

Error code 80070005

This is the most common DCOM General Access Denied error. The access can be denied by any of the multiple existent Access Control Lists (ACLs) configured on a Windows Operating System. Here are some potential sources to this common error:

If the OPC user is not contemplated on the **Edit Limits** ACL under **Launch and Activation Permissions**, the PI OPC Interface node will obtain the following errors:

- In PI OPC Client:

  ```
  Unable to find any OPCEnum server on opcserver; search for CLSID
  returns 80070005
  ```

- In Opcint1 (OPCInterface):

  ```
  No such OPC Server;  CLSID_OPCServerList returns :
  80070005(Access is denied.)
  OPCpi> 1> Can't get GUID for CLSID: 80070005(Access is denied.)
  ```

To solve this access denied error, add the OPC User account to the **Edit Limits** ACL under **Launch and Activation Permissions** in COM Security, and assign to it local and remote permissions.

A very similar error message with the same error code will occur if the OPC user is not contemplated on the **Edit Default** ACL under **Launch and Activation Permissions**:

- In PI OPC Client:
  ```
  -Unable to Connect to'opcserver::SWToolbox.TOPServer';
  CoCreateInstanceEx returns 80070005
  ```
- In Opcint1 (OPCInterface)
  ```
  CoCreateInstanceEx: : 80070005(Access is denied.)
  OPCpi> 1> Can't connect to OPC server, going into slow cycle wait
  ```

  To solve the Access Denied error, add the OPC User account to the **Edit Default** ACL under **Launch and Activation Permissions** in **COM Security**, and assign to it local and remote permissions.

  Both of these errors can be detected on Wireshark as a DCOM error. The `HResult: E_ACCESSDENIED (0x80070005)` indicates the type of error. Also, if the proper registry keys have been enabled, the error message is visible in the **Event Viewer**. See *Registry Settings for DCOM Failure Logging* (page 38) to learn how to enable a higher DCOM logging level.

The same error occurs while trying to connect with an account that does not exist on the OPC Server node.

The same behavior occurs when the **Everyone** user does not have remote access permission, as described in *Configure DCOM Settings* (page 6) on the **Access Permissions Edit Limits** ACL.

- The same error occurs if **Use simple file sharing** is enabled. Further information about Simple File sharing is available here:
  ```
  http://www.microsoft.com/technet/security/advisory/906574.mspx
  ```

Error code 800706BA

On the OPC Server node:

If the OPC Server program is not contemplated on the firewall exception list, the PI OPC Client will return the following error:

```
-Unable to Connect to 'opcserver::OSI.HDA.1';
CoCreateInstanceEx returns 800706BA
```

On Wireshark, the `HResult: 800706BA` shows how the exception originated in the server side.

To resolve this error, add the OPC server executable to the firewall exception list on the OPC Server node. For details, see *Set OPC Server Node Windows Firewall Exceptions* (page 14).

Similarly, if TCP port 135 is not considered on the firewall exception list, the PI OPC Client will prompt with the following error:

`Unable to find any OPCEnum server on opcserver; search for CLSID returns 800706BA`

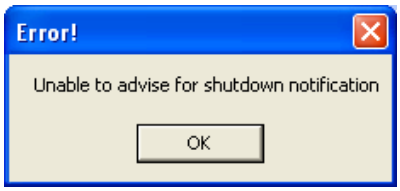
The fix for this would be to add the TCP port 135 to the firewall exception list on the OPC Server node.

On the PI OPC Interface node:

To connect to the OPC Server from the PI OPC Client and the PI OPC Interface, be aware that if TCP port 135 is not on the firewall exception list, any callback generated on the OPC Server node will not be granted remote access to the PI OPC interface node. As a result, the callback will be seen on the PI OPC Interface node as an incoming TCP request. Since most firewalls drop any incoming connection, then the OPC Server will be restricted exclusively to established TCP connections.

For this reason, the PI OPC Client shows which OPC servers are installed on the remote OPC Server node. In this case, the client is performing an outgoing TCP request, and the server uses the same established TCP connection to respond back to the client with the list of installed OPC Servers.

The problem arises when attempting to connect to a specific OPC Server from the returned list. In this case, the OPC Server performs a new outgoing TCP request but the client node's firewall interprets this as an incoming TCP request. Consequently, the firewall will drop that incoming request and the PI OPC Client will show this error:



Note: In addition to allowing TCP port 135 to accept incoming connections, the PI OPC Client executable and the PI OPC Interface executable must be added to the firewall exception list to grant remote access to any incoming OPC Server request.

Click **OK** on this Error window and create a group on the PI OPC Client to read data from an OPC Server Item. Be advised that when the item from data that is to be read is added to the group, the message `Advise returns error 800706BA` will be received when trying to poll data from the PI OPC Client. Again, this is the result of the firewall rejecting any new incoming TCP connection request.

To avoid this error, add the TCP port 135, the PI OPC Client executable, and the PI OPC Interface executable to the firewall exception list.

This error also appears if the specified OPC Server name on the PI OPC Interface node is misspelled or it does not exist.

Error code 8000401A

The server process cannot be started because the configured identity is incorrect. Check the username and password. This indicates a problem with the OPC server's identity specific settings. Make sure that the specified account exists on the OPC Server node.

Also, if the identity specific setting is set to interactive and no user has logged on to the server, then the interface will not be able to connect:

```
-OPCpi> 1> CoCreateInstanceEx: : 8000401a(The server process
could not be started because the configured identity is
incorrect.  Check the username and password.)

OPCpi> 1> Can't connect to OPC server, going into slow cycle wait
```

Error code 0xC0000064

The specified user does not exist. This error will be seen on the **Windows Event Viewer** under **Security** when the PI OPC Client or PI OPC Interface attempts to obtain a list of OPC Servers from OPCenum with a user that doesn't exist on the OPC Server node.

Error code 80080005

Server execution failed. This is a generic failure error. The OPC server did not register with DCOM within the required timeout. Usually this means that the user account has limited privileges and restricted access to the OPC server executable. To grant execution permissions to the limited user account, modify the security properties of the folder where the server software resides. To do this, right click on the folder, and select **Properties**. Select the **Security** tab in On the **Properties** dialogue, and click on the **Add** button to add the limited user account. Then, assign the user **Full Control** permissions.

Error code 80004002

If the Authentication Level is set to None in both computers, the **Anonymous Logon** user needs to be added to the Edit Limits ACL under Access permissions. If you configure **Anonymous logon** only on the OPC Server node, then the message: `Unable to advise for shutdown notification` appears when you try to connect from the PI OPC Client. You can see this in Wireshark as an `E_NOINTERFACE (0x80004002)` error.

- Click **OK** on this Error window and create a group on the PI OPC Client to read data from an OPC Server Item. Be advised that when the item from which the data to be read is added to the group, you will receive the message `Advise returns error 80040202`, when trying to poll data from the PI OPC Client.

Error code 80004002 is received when trying to establish a connection to a COM Server might not indicate a DCOM security error. Some OPC servers will not accept connections from third-party OPC clients and will return this error if such clients attempt a connection. The error message will look similar to:

```
- Unable to get [OPC Server Name] pointer; CoCreateInstance
returns 80004002
- CoCreateInstance: No such interface supported (80004002)
```

Error code 8007002

The OpcEnum service failed to start because the system cannot find the file `opcenum.exe`.

In PI OPC Interface log, PIPC.log:

```
OPCpi> 1> No such OPC Server;  CLSID_OPCServerList returns :
80070002(The system cannot find the file specified.)

OPCpi> 1> Can't get GUID for CLSID: 80070002(The system cannot
find the file specified.)
```

There are multiple ways to recover from this error:

- The quickest method is to copy the `opcenum.exe` from `C:\Windows\system32\` in the Interface node to `C:\Windows\system32\` in the OPC Server node.
- If you cannot get a copy of `opcenum.exe`, you can import to the PI OPC Interface node, the OPC Server registry keys located from this directory on the OPC Server node: `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\[OPCServer]`

Error code 80070776

This error indicates some type of network conflict. Check that the nodes' IP addresses and network names are unique.

Appendix B

Technical Support and Resources

You can read complete information about technical support options, and access all of the following resources at the OSIsoft Technical Support Web site:

http://techsupport.osisoft.com

Before You Call or Write for Help

When you contact OSIsoft Technical Support, please provide:

- Product name, version, and/or build numbers
- Computer platform (CPU type, operating system, and version number)
- The time that the difficulty started
- The log files at that time

Help Desk and Telephone Support

You can contact OSIsoft Technical Support 24 hours a day. Use the numbers in the table below to find the most appropriate number for your area. Dialing any of these numbers will route your call into our global support queue to be answered by engineers stationed around the world.

Office Location	Access Number	Local Language Options
San Leandro, CA, USA	1 510 297 5828	English
Philadelphia, PA, USA	1 215 606 0705	English
Johnson City, TN, USA	1 423 610 3800	English
Montreal, QC, Canada	1 514 493 0663	English, French
Sao Paulo, Brazil	55 11 3053 5040	English, Portuguese
Frankfurt, Germany	49 6047 989 333	English, German
Manama, Bahrain	973 1758 4429	English, Arabic
Singapore	65 6391 1811 86 021 2327 8686	English, Mandarin Mandarin
Perth, WA, Australia	61 8 9282 9220	English

Support may be provided in languages other than English in certain centers (listed above) based on availability of attendants. If you select a local language option, we will make best efforts to connect you with an available Technical Support Engineer (TSE) with that language skill. If no local language TSE is available to assist you, you will be routed to the first available attendant.

If all available TSEs are busy assisting other customers when you call, you will be prompted to remain on the line to wait for the next available TSE or else leave a voicemail message. If you choose to leave a message, you will not lose your place in the queue. Your voicemail will be treated as a regular phone call and will be directed to the first TSE who becomes available.

If you are calling about an ongoing case, be sure to reference your case number when you call so we can connect you to the engineer currently assigned to your case. If that engineer is not available, another engineer will attempt to assist you.

Search Support

From the OSIsoft Technical Support Web site, click **Search Support**.

Quickly and easily search the OSIsoft Technical Support Web site's support solutions, documentation, and support bulletins using the advanced MS SharePoint search engine.

E-Mail–Based Technical Support

techsupport@osisoft.com

When contacting OSIsoft Technical Support by e-mail, it is helpful to send the following information:

- Description of issue: Short description of issue, symptoms, informational or error messages, history of issue
- Log files: See the product documentation for information on obtaining logs pertinent to the situation.

Online Technical Support

From the OSIsoft Technical Support Web site, click **Contact Us > My Support > My Calls**.

Using OSIsoft's Online Technical Support, you can:

- Enter a new call directly into OSIsoft's database (monitored 24 hours a day)
- View or edit existing OSIsoft calls that you entered
- View any of the calls entered by your organization or site, if enabled
- See your licensed software and dates of your Service Reliance Program agreements

Remote Access

From the OSIsoft Technical Support Web site, click **Contact Us > Remote Support**.

OSIsoft Support Engineers may remotely access your server in order to provide hands-on troubleshooting and assistance. See the Remote Access page for details on the various methods you can use.

On-Site Service

From the OSIsoft Technical Support Web site, click **Contact Us > On-site Field Service Visit**.

OSIsoft provides on-site service for a fee. Visit our On-site Field Service Visit page for more information.

Knowledge Center

From the OSIsoft Technical Support Web site, click **Knowledge Center**.

The Knowledge Center provides a searchable library of documentation and technical data, as well as a special collection of resources for system managers. For these options, click **Knowledge Center** on the Technical Support Web site.

- The Search feature allows you to search Support Solutions, Bulletins, Support Pages, Known Issues, Enhancements, and Documentation (including user manuals, release notes, and white papers).
- System Manager Resources include tools and instructions that help you manage archive sizing, backup scripts, daily health checks, daylight saving time configuration, PI Server security, PI System sizing and configuration, PI trusts for interface nodes, and more.

Upgrades

From the OSIsoft Technical Support Web site, click **Contact Us > Obtaining Upgrades**.

You are eligible to download or order any available version of a product for which you have an active Service Reliance Program (SRP), formerly known as Tech Support Agreement (TSA). To verify or change your SRP status, contact your Sales Representative or *Technical Support* (http://techsupport.osisoft.com/) for assistance.

Index