Cyberlogic Knowledge Base

KB2010-11: USING THE CYBERLOGIC OPC SERVER VIA DCOM

INTRODUCTION

The OPC client/server architecture is based on the Microsoft COM (Component Object Model) technology. The distributed version of this technology is called DCOM, and it allows OPC clients to interface to remote OPC servers over a network connection.

In a networked environment, a key concern of Windows operating systems is security, including the protection of the system against malicious attacks. As part of this security, DCOM function calls between OPC client and server systems are checked for correct security permissions by the operating system. If the security settings are incorrect, DCOM communication will not work. In particular, this is a problem for systems running under Windows XP Service Pack 2, because the default SP2 settings disable DCOM, preventing remote OPC communications.

Note
This document is primarily concerned with OPC communications using DCOM. This is an issue when the OPC server and OPC client reside on different systems. However, even if both applications are on the same system, users without Administrator privileges may run into similar issues and therefore should follow the recommendations in this document.

Caution!
The procedures in this document will affect the security settings of the systems and networks involved. They include changes to the Windows firewall, permissions, user accounts and other security-related features. Before you implement any of these recommendations, be sure that you understand how they will affect your system and network security, including increased risk of malicious attacks. In addition, be sure to discuss any proposed changes with your System Administrator or IT department.

BECAUSE EVERY NETWORK SITUATION IS UNIQUE, ONLY YOUR IT PROFESSIONALS CAN DETERMINE WHAT SECURITY MEASURES ARE APPROPRIATE FOR YOUR SYSTEMS. CYBERLOGIC TECHNOLOGIES INC. MAKES NO REPRESENTATION THAT THE INFORMATION OR RECOMMENDATIONS IN THIS PAPER ARE SUITABLE FOR A PARTICULAR INSTALLATION AND CANNOT ACCEPT RESPONSIBILITY FOR ANY PROBLEMS, DAMAGES OR LOSS OF SERVICE, WHICH MAY BE INCURRED.

It is important to understand that the OPC callback mechanism causes the OPC client to function as a DCOM server and the OPC server to function as a DCOM client. Because of this, the configuration issues in this document affect both the client and server systems.

Note
You must have Administrator privileges to perform the configuration changes described in this document.

The issues covered are divided into four areas of concern:

- Network Configuration Issues
- Operating System Specific Issues
- System-Wide DCOM Configuration Issues
- Server-Specific DCOM Configuration Issues

NETWORK CONFIGURATION ISSUES

In any network configuration, the identification of the Users on each machine is handled by the operating system. How this is done depends on the specific operating system and whether the computers are members of a Workgroup or a Domain. Ideally, the client and server machines should both be members of the same Workgroup or Domain. It is possible, however, to use a Mixed Configuration, in which one is in a Workgroup and the other in a Domain.

Domain

Domains have a Domain controller that authenticates Users across the Domain. Having a central point for authentication greatly simplifies Users and User Groups identification. Therefore, this is the preferred network architecture.

Some considerations:

- Ideally, the client and server systems should be members of the same Domain. If they are in different Domains, the Domains must be configured to trust each other.

- Authentication of Users and User Groups is handled by the Domain controller. These Users and Groups can then be used in the DCOM settings of the client and server.

- It is preferable that all systems have the same operating system.

Workgroup

Workgroups have no central point for user authentication. This means that each machine in the Workgroup must have all the information on all of the Users that will access the node remotely. This, of course, can dramatically increase the administrative effort when adding new Users.

Some considerations:

- It is preferable to have the client and server systems as members of the same Workgroup.

- Each User account that will be used with DCOM must exist on both the client and server systems and use identical usernames and passwords on both systems. Refer to the section Using Run *As...* for help in testing this requirement.

- It is preferable that all systems have the same operating system.

Mixed Configuration

If one system is a member of a Workgroup and the other is a member of a Domain, you must use double identification. This means that you must add User accounts to the Workgroup machine that are identical (username and password) to the User accounts in

the Domain. This will allow function calls to the Workgroup machine to be identified and granted locally, without asking the Domain controller.

In some situations, it may be inconvenient to login as a new User. For those cases, the next section, Using Run As..., provides a useful workaround for testing purposes.

Using *Run As...*

It may be difficult or inconvenient to login under a new User account that you have created, especially on a server system that is running in a production environment. In many cases, you can use the Windows Run As... feature as a temporary troubleshooting measure.

In addition, you may want to allow the software to be run by Guests or other users that do not have the necessary security settings. A convenient way to do this is to set up a shortcut that uses Run As... to make this possible.

Context Menu Method

This method does not require you to create a shortcut, but will require you to enter the username and password each time you run the application.

1. Right-click on the application you want to run, and then select **Run As...** from the context menu.
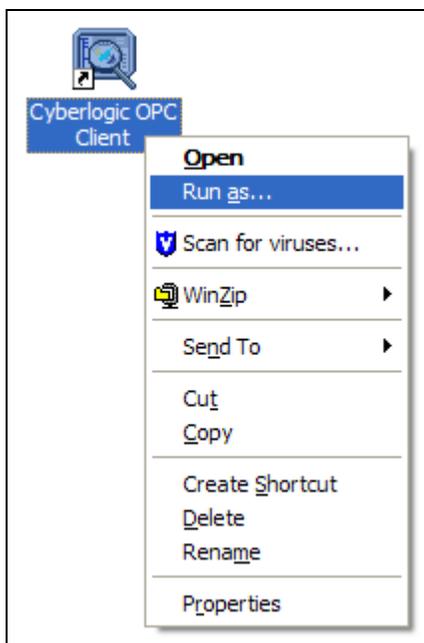
2. From the Run As dialog box, select **The following user:** option.

3. Enter the User name and password for the account you want to run as, and then click **OK**.
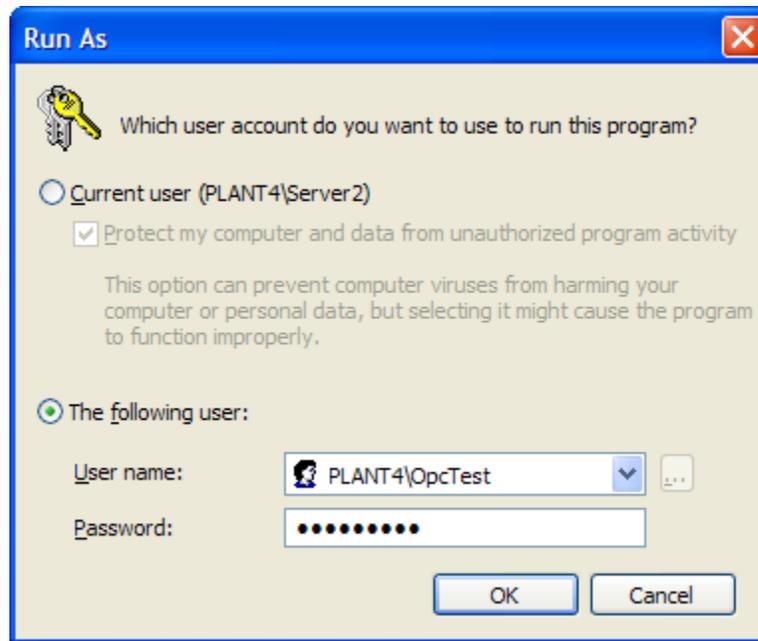
Shortcut Method

This method will require the user to enter only a password each time the application is run.

1. Create a new shortcut for the desired application or make a copy of an existing shortcut.

2. Right-click on the shortcut and select **Properties**.
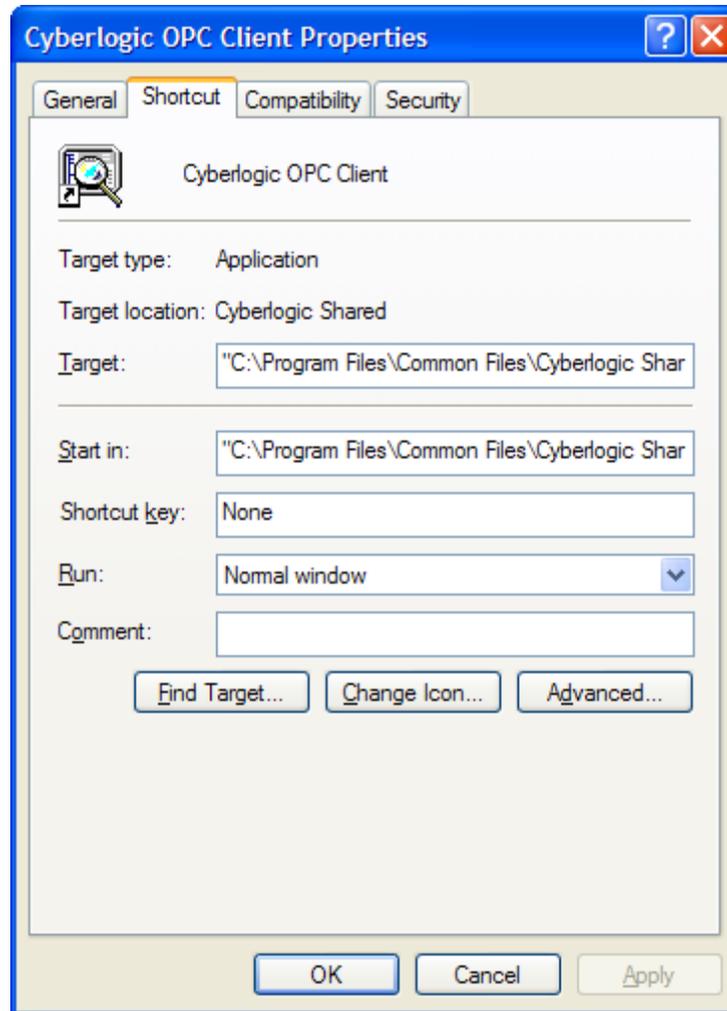
3. Edit the **Target** field to add the following ahead of the existing path and program name:

    runas.exe /user:OPCUSER

    In place of **OPCUSER** in the above string, enter the username of the account you wish to run as. Be sure to include a space before the / and after the username. The result will look like the string below, but it will use the path and file name for the application you want to run.

    runas.exe /user:OPCUSER "C:\Program Files\Common Files\Cyberlogic Shared\CyberlogicOpcClient.exe"

    The shortcut properties will look like the following figure. Click **OK** to save the changes.
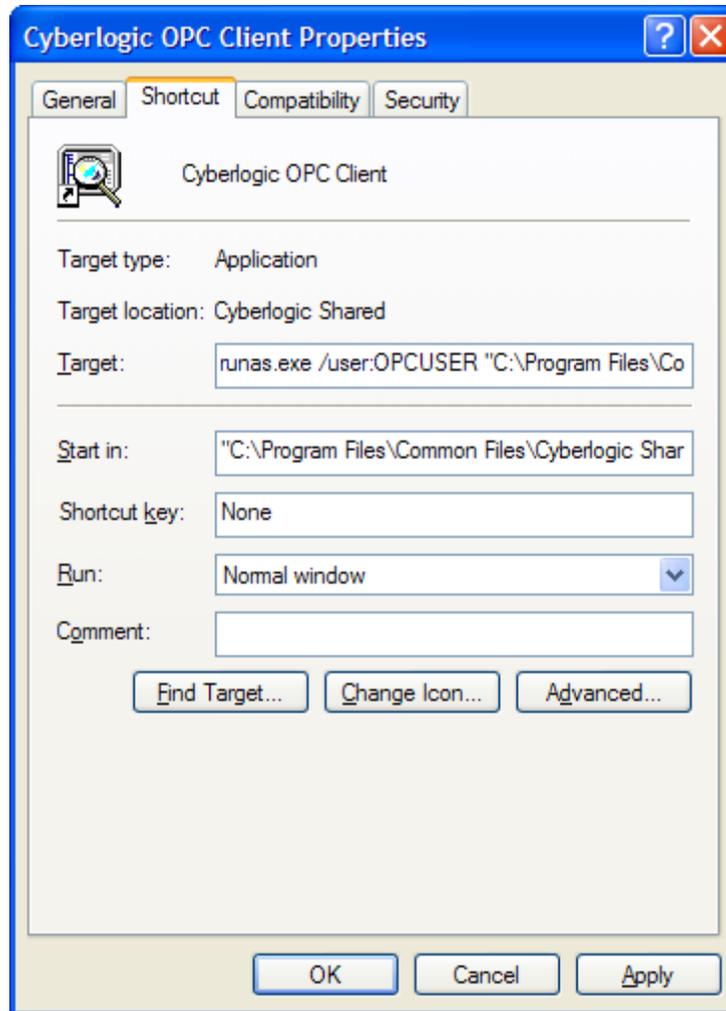
4. Any user may now run the application by double-clicking the shortcut. Windows will request the password associated with the username.

OPERATING SYSTEM SPECIFIC ISSUES

Certain configuration issues apply only to the Windows 2000 or Windows XP operating systems. They are described in the following sections.

Note	For Windows NT and Windows 2000 systems with firewalls, read the Windows Firewall section for Windows XP. The issues described there apply to all firewalls and similar procedures should be followed.

Windows 2000

There is a known bug that affects systems running Windows 2000 with Service Pack 1. DCOM servers on these machines may stop sending callbacks after a few days or weeks, preventing function calls such as OnDataChange from completing. In these cases, the DCOM server will return the error code 0x80010108 RPC_E_DISCONNECTED. All other types of calls from the client to the server will continue to work.

There are three ways to deal with this problem:

- Recommended: Install Windows 2000 Service Pack 3 or higher.
- Install COM + Rollup Package 18.1 (Post Service Pack 2).
- As a workaround, stop and restart the client application.

Windows XP

There are two concerns in Windows XP systems: the network access setting and the Windows firewall configuration.

Network Access

By default, Windows XP forces remote users to authenticate as Guest. This setting simplifies the setup of home and small business networks that are not configured as Domains. However, this can create problems for OPC servers and clients.

When an OPC server is running on an XP machine with its default network access security setting, the Guest account must be enabled and have enough rights to launch the server, or the clients will not be allowed to connect. In addition, if an OPC server sends a callback to a remote client installed on an XP machine, the server will authenticate as Guest and the callback may not get through to the client. Finally, the Guest-authentication default restricts the tools that are available for administering permissions for various users.

Due to the above complications, we do not recommend using the default network access security setting on XP machines. Instead, we recommend changing the Network Access setting from **Guest Only** to **Classic**. The **Classic** setting forces Windows XP to behave

like Windows 2000, forcing remote users to authenticate as themselves rather than as Guests.

To change this setting:

1. Open the **Start** menu, then select **Control Panel**, **Administrative Tools** and then **Local Security Policy**.

2. From the tree, select **Local Policies** and then **Security Options**.

3. Locate the entry called **Network access: Sharing and security model for local accounts**.

4. Double-click on it and change the setting to **Classic – users authenticate as themselves**.
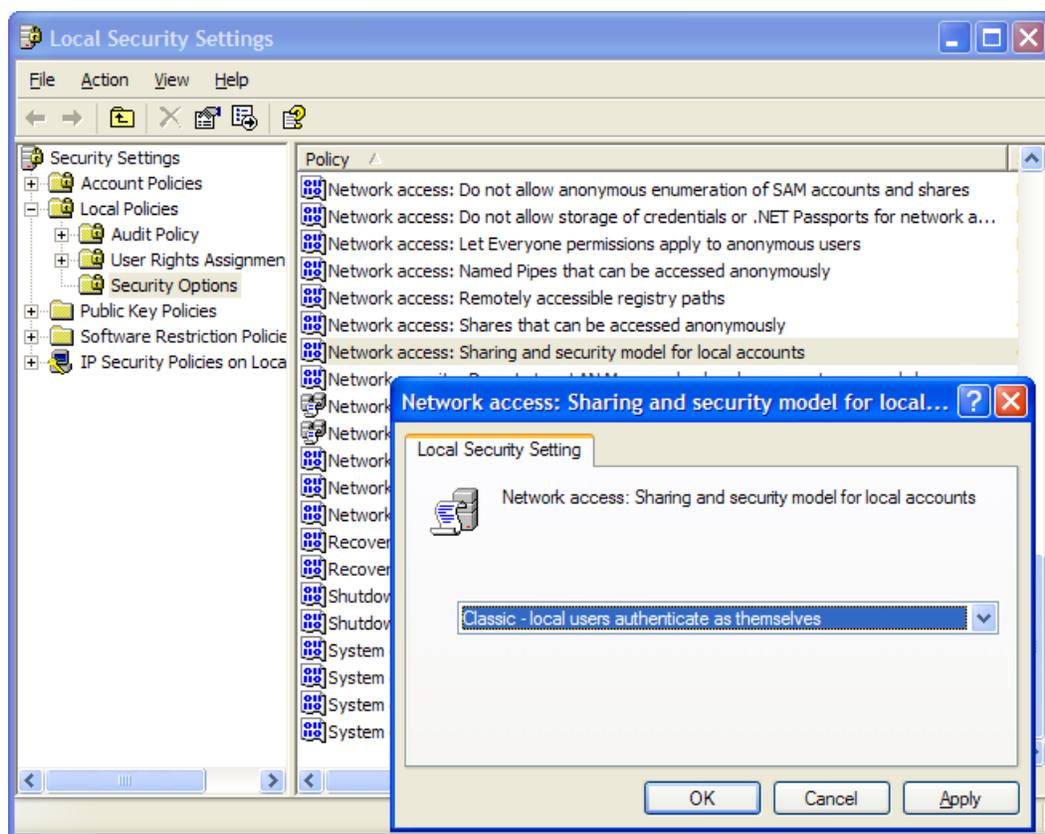
Windows Firewall

By default, the Windows Firewall allows traffic across the network when the traffic is initiated locally, but stops most incoming unsolicited traffic. However, administrators can specify exceptions to this rule, allowing responses to unsolicited requests.

Firewall exceptions can be specified at two main levels: the application level, and the port-and-protocol level. At the application level, you specify which applications are able to respond to unsolicited requests. At the port-and-protocol level, you specify that the

firewall should allow or disallow traffic on a specific port for either TCP or UDP traffic. To make any OPC client/server application work via DCOM, changes must be made on both levels. The Cyberlogic OPC Server (CybOpcRuntimeService.exe), the Microsoft Management Console (mmc.exe), and the OPC utility (OPCEnum.exe) must be added to the exceptions list at the application level, and the DCOM port 135 must be enabled at the port-and-protocol level.

The following procedure will guide you through the process of making these changes.

1. To edit the firewall settings, open the **Start** menu, select **Control Panel**, then **Security Center** and finally **Windows Firewall**.
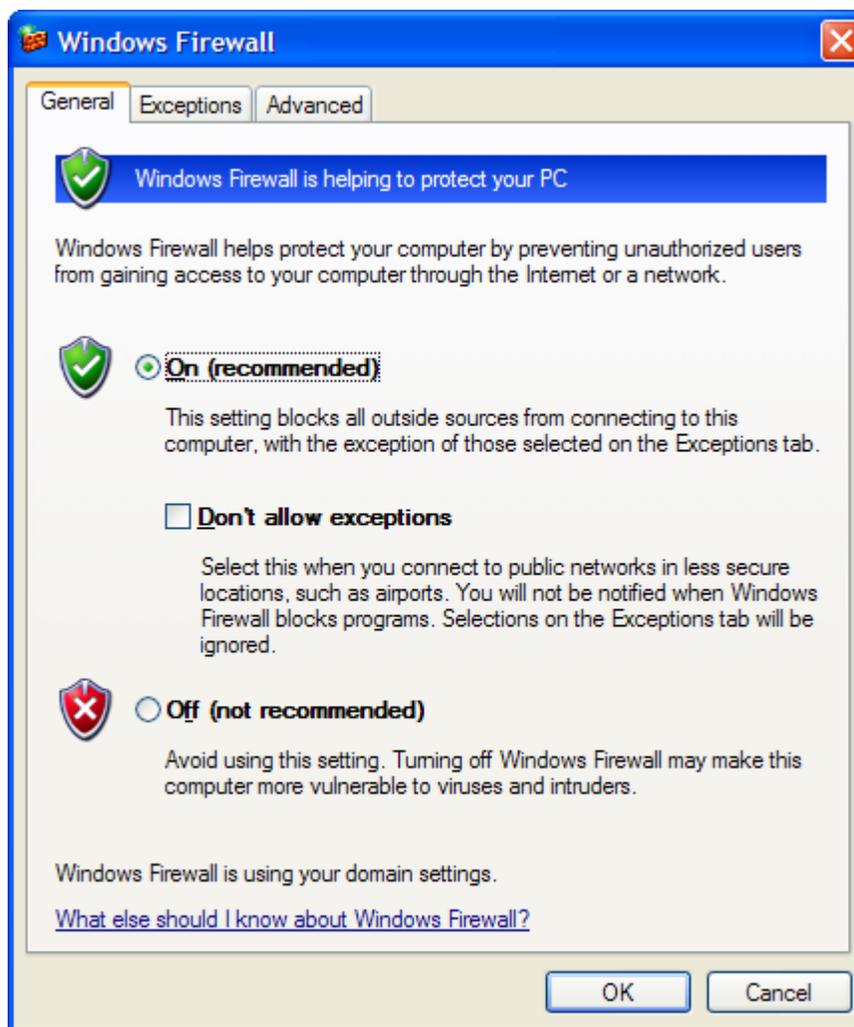
2. Select **On** to enable the firewall.

    This is the default setting and is recommended to protect your machine from outside security threats. For troubleshooting purposes, you may want to set the firewall to **Off** temporarily. This will help you to determine if the firewall configuration is the cause of the communication problems you are experiencing. After the tests, be sure to turn the firewall back on.

Note	If the computer is protected by a corporate firewall or the network is otherwise secured, it may be safe to turn the firewall off permanently. In that case, the rest of the firewall settings in this section are not necessary.

3. Select the *Exceptions* tab and add all OPC clients and servers to the exception list.
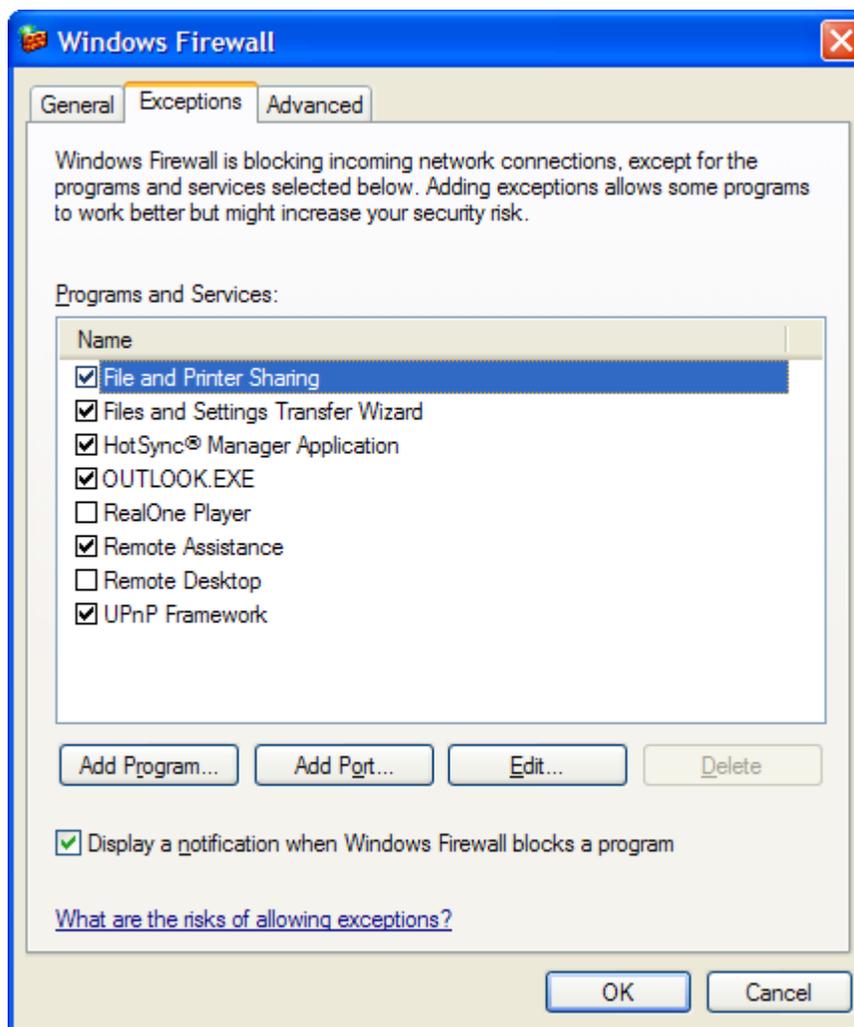
4. To add a program, click *Add Program...* and select the desired program from the list.
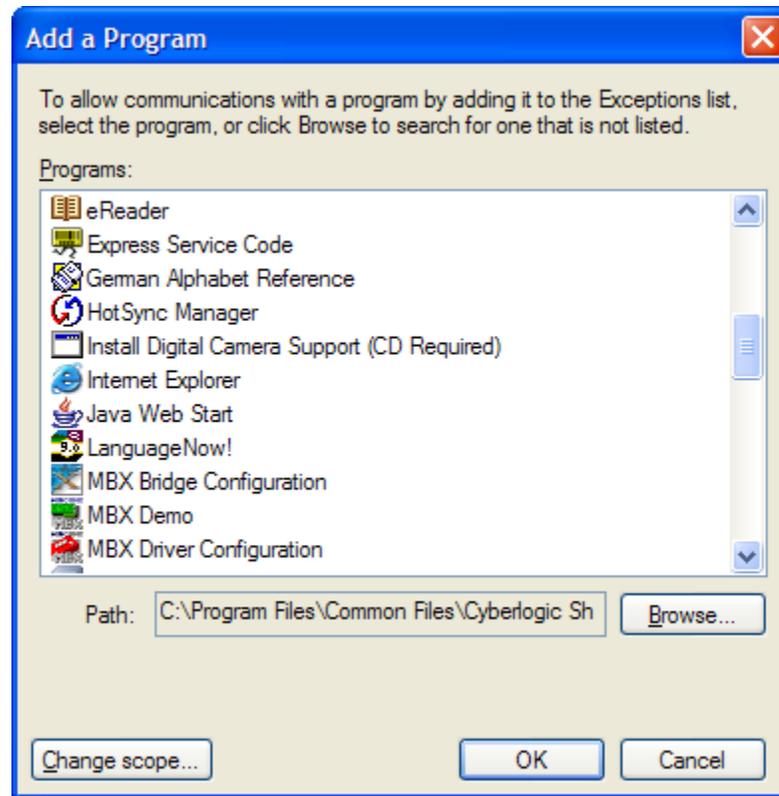
5. If Cyberlogic's OPC Server is not on the list, click **Browse...** and navigate to **C:\Program Files\Common Files\Cyberlogic Shared\OPC**. There you will find **CybOpcRuntimeService.exe**, the program you must add to the exception list.
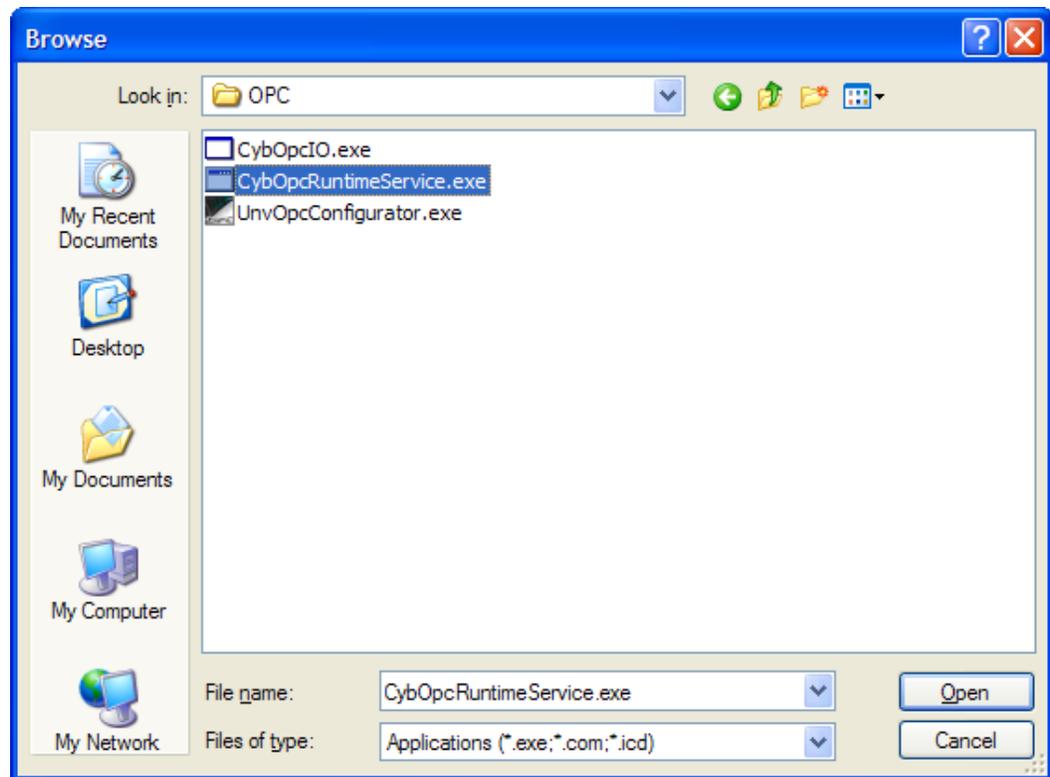
6. You must also add the Microsoft Management Console (*mmc.exe*) and the OPC utility *OPCEnum.exe*, both of which are found in the *Windows\System32* directory.

   The mmc.exe application is needed to run the DCOM configuration editor. OPC client applications use OPCEnum.exe to obtain a list of available servers on the local or remote machines.

7. Click *Add Port…* and enter the information shown in the figure below to add TCP port 135 to the exceptions list. This port is needed to permit DCOM communications.
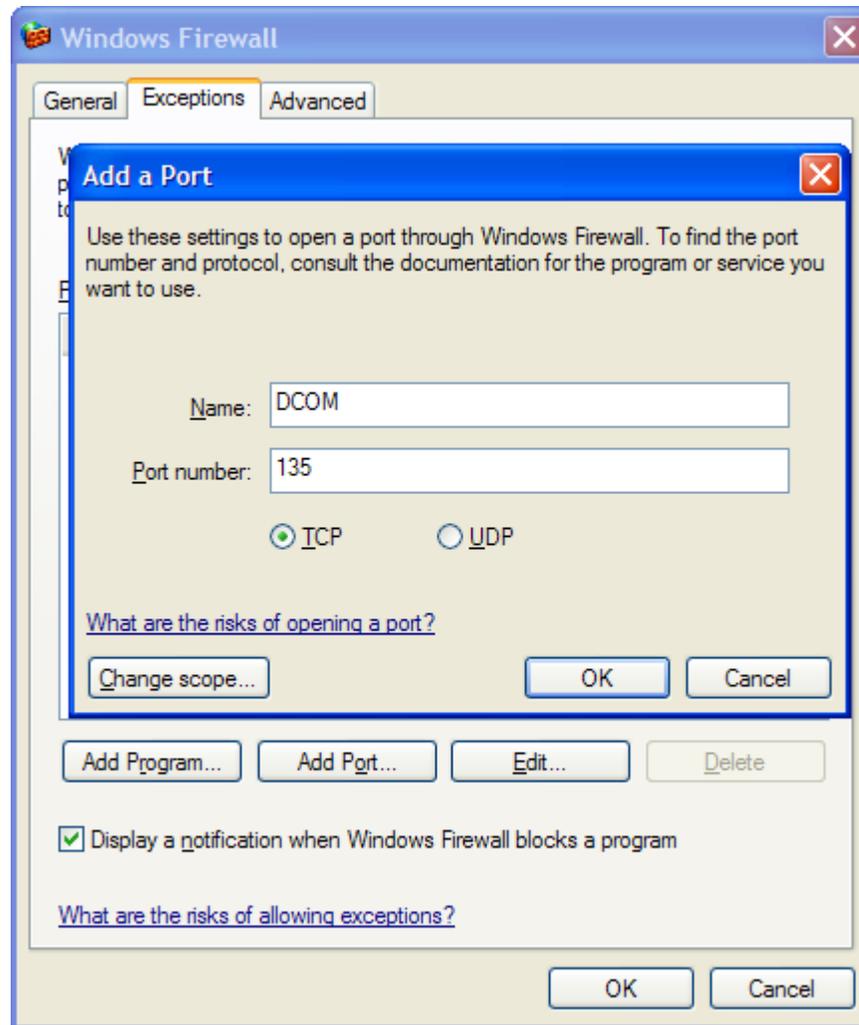
8. When all edits are complete, click **OK** to save the changes.
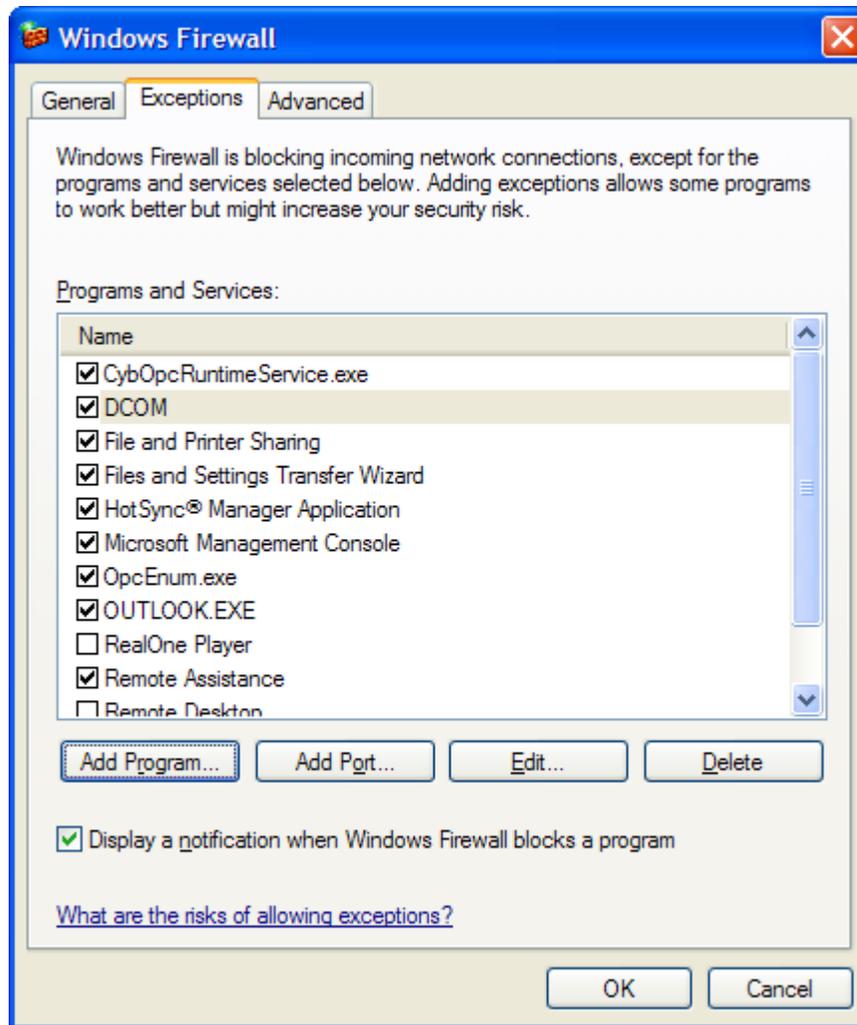
SYSTEM-WIDE DCOM CONFIGURATION ISSUES

This section covers configuration of the system-wide DCOM security settings. These settings must be applied to all systems running OPC client or server software. Remember that callback functions will cause the server system to appear as a client and vice-versa. This is why settings that appear to relate only to servers or only to clients must be applied to both types of systems.

Caution!

Changing the system-wide settings affects every COM application that does not have a custom configuration.

For each DCOM security property, a COM application can use either the system-wide setting or a custom setting. If an application has custom security settings, then the system-wide settings are disregarded. Applications that do not have custom settings use the system-wide settings.

The appearance of the dialog boxes may differ somewhat, depending upon the operating system in use. Where the differences are significant, this will be pointed out.

Opening DCOM Configuration

To open and change the DCOM settings:

1. Click on the **Start** menu, then select **Run**.

2. Type **dcomcnfg.exe** and click *OK*.
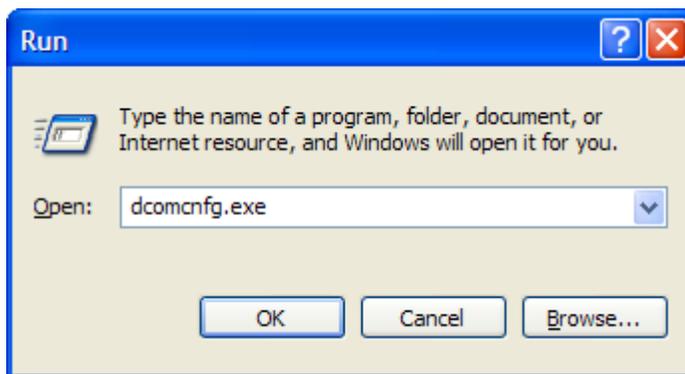
3. In the tree on the left side, open **Console Root**, then **Component Services** and then **Computers**.

4. Right-click on **My Computer** and select **Properties**.
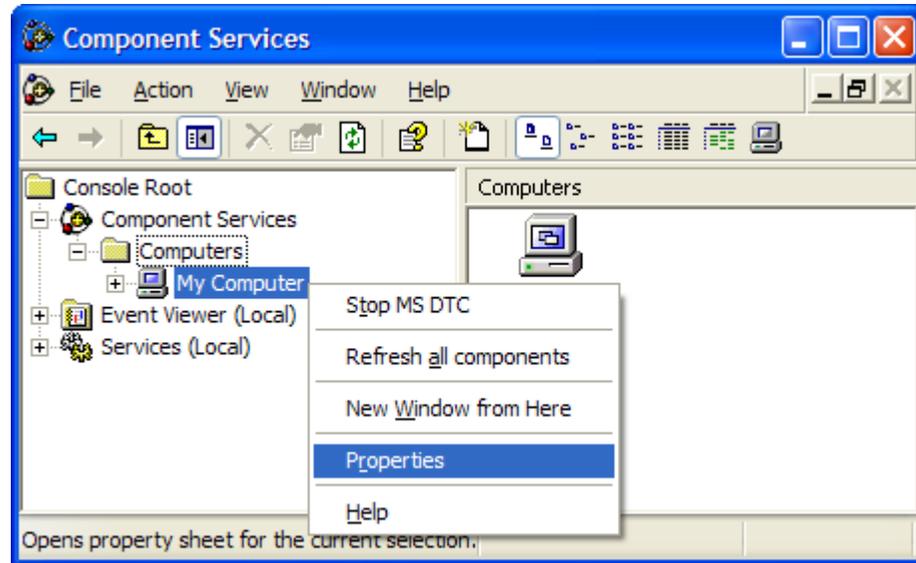
The DCOM configuration dialog box will open.

General, Options and MSDTC Tabs

No changes are needed on these tabs. The default settings will be correct for the OPC client system.

Default Protocols Tab

5.   Click on **Connection-oriented TCP/IP**.

6.   Click the **Move Up** button repeatedly until **Connection-oriented TCP/IP** is at the top position.

   This setting forces the use of TCP/IP as the preferred protocol for DCOM connections.
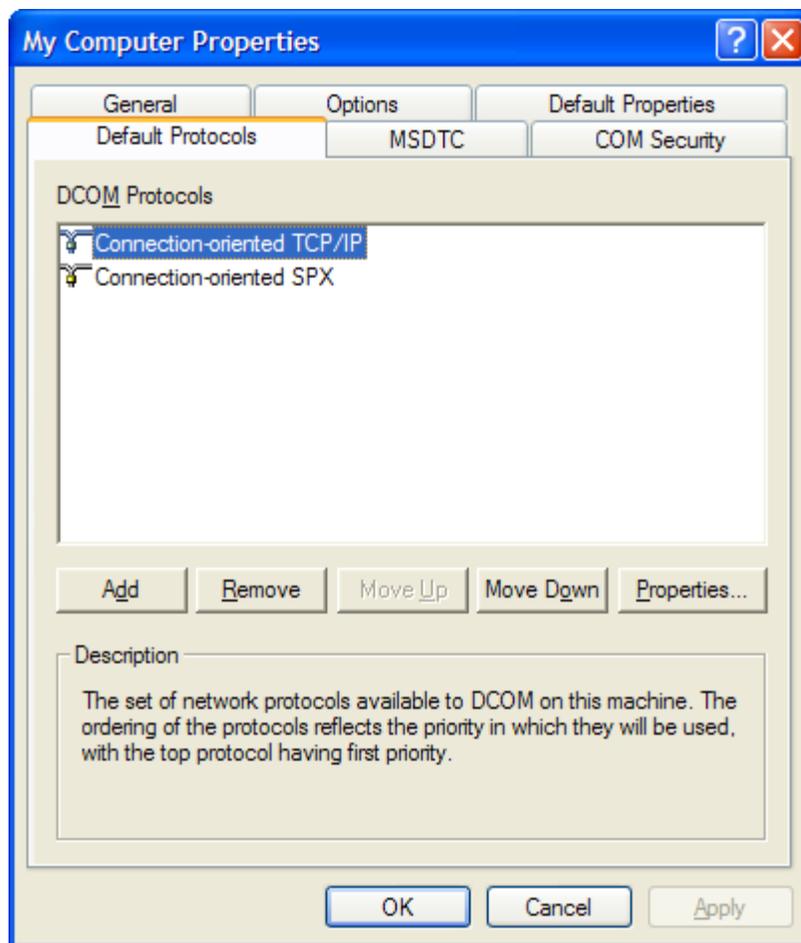
TCP/IP is the most commonly used transport protocol with DCOM. We recommend that you configure all of your client and server machines to use only TCP/IP, and remove other protocols from their DCOM Protocols lists. Doing so will reduce connection timeouts.

7. Select each protocol you want to remove and click the **Remove** button.

Default Properties Tab

8. Check the **Enable Distributed COM on this computer** box.

Caution!	If you change the setting of this check box, you must reboot the system for the change to take effect.
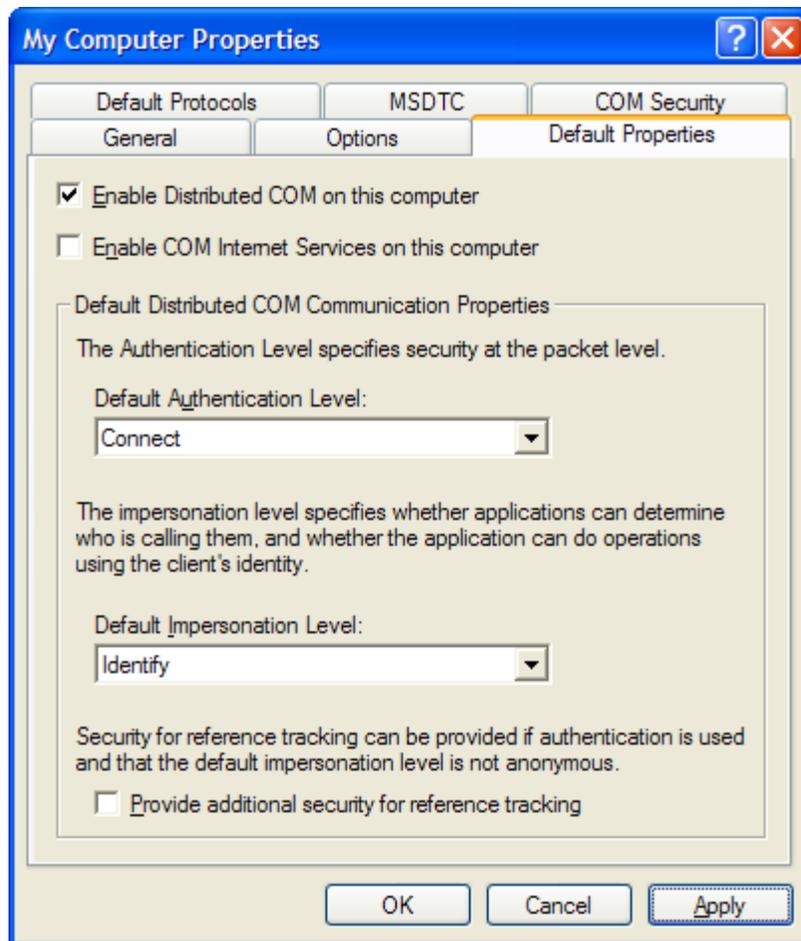
The Default Distributed COM Communication Properties settings will depend on your network configuration. A Domain configuration will have different settings than a Workgroup or mixed configuration.

Note   Cyberlogic's OPC Server and Client allow you to select preconfigured DCOM security settings that override the Default Distributed COM Communication Properties settings. If you decide to use one of these settings, it will not be necessary for you to change the Default Authentication Level or Default Impersonation Level here. Refer to Appendix A: Cyberlogic OPC Product DCOM Configuration for details.

Domain

If the client and server are both members of a Domain, use the following configuration:

9. Select **Connect** for the Default Authentication Level

    With **Connect** authentication, the server authenticates the credentials of the client only when the client connects to the server. Higher levels of authentication could be used, but performance might suffer.

10. Select **Identify** for the Default Impersonation Level.

With the **_Identify_** impersonation, the server can obtain the client's identity. The server can impersonate the client to do access-control list (ACL) checks, but it cannot access system objects as the client. This level of impersonation is sufficient for most servers.

Workgroup or Mixed Configuration

If the client, server or both are members of a Workgroup, user authentication and impersonation in DCOM is difficult to set up and does not work reliably. Therefore, we recommend that you use the following configuration:

11. Select **_None_** for the Default Authentication Level

12. Select **_Anonymous_** for the Default Impersonation Level.

Caution!	With authentication set to **_None_**, the server performs no authentication. With **_Anonymous_** impersonation, the client is anonymous to the server. After you confirm that DCOM communication is working, you may want to try changing these settings to **_Connect_** and **_Identify_** for better security.
Caution!	Remember that the client and server systems must both have User accounts with identical usernames and passwords.
Note	In Windows 2000, the Network Configuration icon will disappear if you set the DCOM security levels to **_None_** and **_Anonymous_**. The network will still work, but you will have no way to change the IP address of the network card. If you need to edit the IP address, temporarily change the DCOM settings to **_None_** and **_Delegate_**.

COM Security Tab

This tab allows you to configure the system-wide access, launch and activation permissions. On some systems, this tab is called **_Default COM Security_** and does not have the **_Edit Limits..._** buttons.
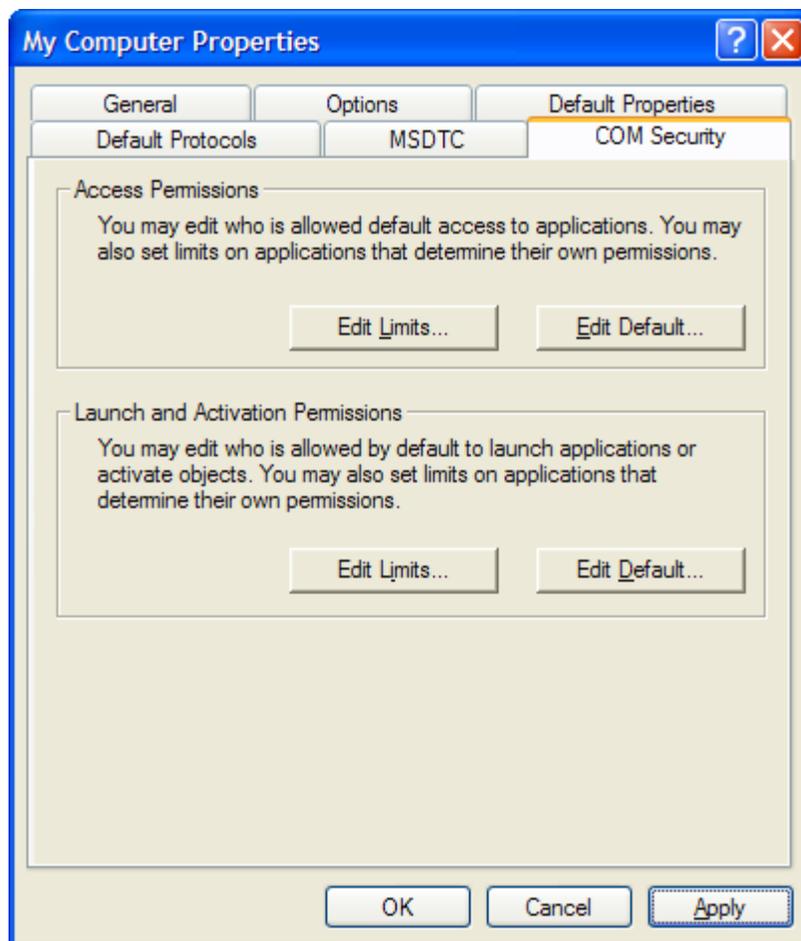
Note	Access permissions specify a list of Users who are granted or denied access to COM applications.
	Access permissions are divided into local access permission and remote access permission. Users with local access permission may access a COM application running on the same machine as the calling client. Users with remote access permission may access a COM application from other computers across a network connection.

Note	Launch permission is required to start a new COM application. Activation permission is required for a new client to use a COM application, even if the application has already been launched.
	Launch and activation permissions are divided into local and remote launch and activation permissions. Users with local launch or activation permission can start or use a COM application running on the same machine as the calling client. Users with remote launch or activation permission can start or use a COM application from other computers across a network connection.

Default Permissions

13. In the Access Permissions section, click the ***Edit Default...*** button.

Note	Cyberlogic's OPC Server and Client allow you to select preconfigured DCOM security settings that override the Default Access Permissions settings. If you decide to use one of these settings, you need not modify the Default Access Permissions in this section. Refer to Appendix A: Cyberlogic OPC Product DCOM Configuration for details.

14. For each user or group that will participate in OPC communication, check the ***Allow*** box for both Local Access and Remote Access. When you are finished, click ***OK***.

    If the User or Group you want to edit is not listed, refer to Appendix B: Adding Users or Groups for instructions on how to add to the listing.

Caution!	The example shown grants these permissions to ***Everyone***, which includes all authenticated users. You may wish to restrict this to a smaller group. The recommended way to do this is to create a group called ***OPC Users*** and add to this group all Users that will execute any OPC server or client. You would then grant the access, launch and activation permissions to the ***OPC Users*** group instead of ***Everyone***.

15. If the tab has a Launch and Activation Permissions section, click its **Edit Default...** button.

    Some systems have a Launch Permissions section instead of Launch and Activation Permissions. In such a case, you cannot edit the default Activation Permissions and you can skip this step.

16. For each user or group that will participate in OPC communication, check the **Allow** box for both Local Activation and Remote Activation. When you are finished, click **OK**.

    If the User or Group you want to edit is not listed, refer to Appendix B: Adding Users or Groups for instructions on how to add to the listing.

Note	The Local Launch and Remote Launch permissions need not be changed because the server-specific settings will provide their own custom permissions.

Access Permissions Limits

17. If the Access Permissions section has an **Edit Limits...** button, click it to open the edit screen.

18. Select the **ANONYMOUS LOGON** user and check the **Allow** boxes for Local Access and Remote Access. When you are finished, click **OK**.

    These settings are required to allow OPCEnum.exe to function and for some OPC servers and clients that set their DCOM authentication level to **None** to allow anonymous connections. Client applications use OPCEnum.exe to obtain a list of available servers on the local or remote machines. If your applications do not use OPCEnum.exe, you may not need to enable Remote Access for anonymous Users.
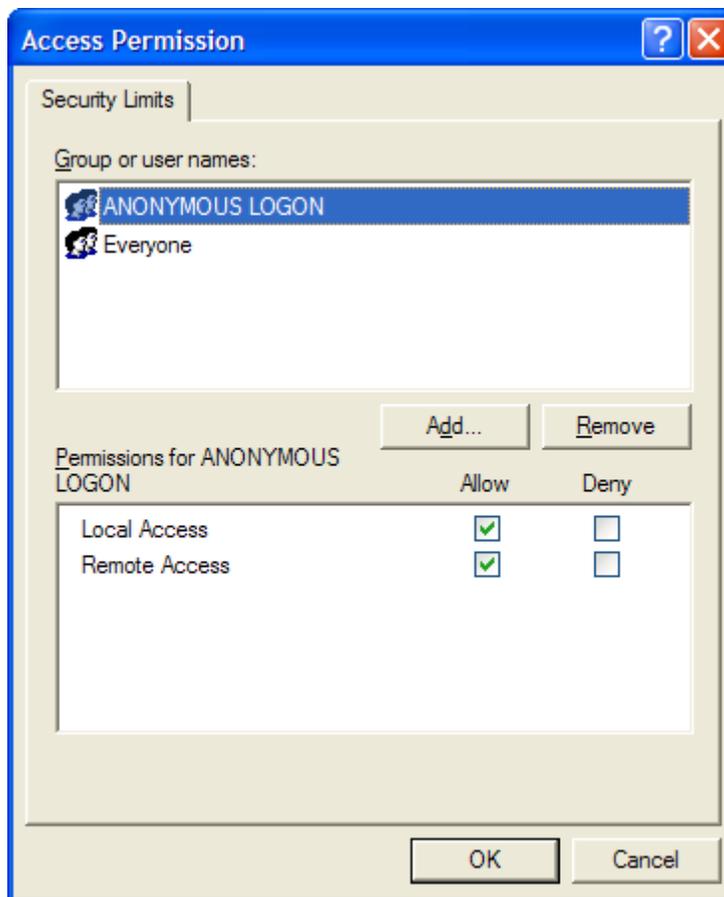
Launch and Activation Permissions Limits

19. If the Launch and Activation Permissions section has an **Edit Limits...** button, click it to open the edit screen.

20. For each User or Group that will participate in OPC communication, check the **Allow** box for all permission types: Local Launch, Remote Launch, Local Activation and Remote Activation. When you are finished, click **OK**.

    If the User or Group you want to edit is not listed, refer to Appendix B: Adding Users or Groups for instructions on how to add to the listing.

Caution! The example above grants these permissions to **Everyone**, which includes all authenticated users. You may wish to restrict this to a smaller group. The recommended way to do this is to create a group called **OPC Users** and add to this group all Users that will execute any OPC server or client. You would then grant the access, launch and activation permissions to the **OPC Users** group instead of **Everyone**.

SERVER-SPECIFIC DCOM CONFIGURATION ISSUES

This section covers configuration of the OPC server-specific DCOM security settings. As such, you need to apply the following procedures only to machines that have OPC server software installed and running.

<table>
<tr><td>Note</td><td>For each COM security property, a COM application can either use the system-wide setting or use a custom setting. Whenever an application has custom security settings, the system-wide settings are disregarded.</td></tr>
</table>

The appearance of the dialog boxes will differ somewhat, depending upon the operating system in use. Where the differences are significant, this will be pointed out.

Opening DCOM Configuration

1. Click on the **Start** menu, then select **Run**.

2. Enter **dcomcnfg.exe** and click **OK**.
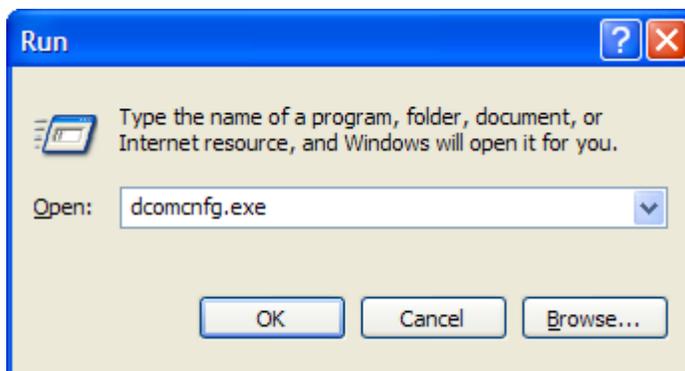
3. In the tree on the left side, open **Console Root**, then **Component Services**, then **Computers**, and then **DCOM Config**.

4. In the right pane, locate the OPC server. For the Cyberlogic OPC Server find **CybOpcRuntimeDA and CybOpcServerAE**.

5. Right-click on the server and select **Properties** from the context menu.
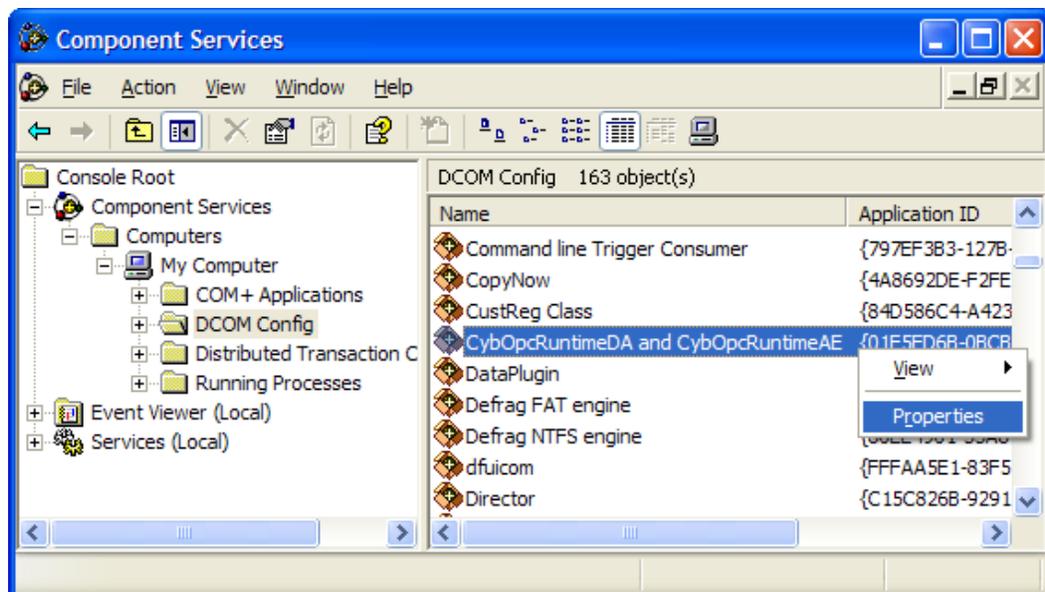
The DCOM configuration dialog box will open.

General, Location and Endpoints Tabs

No changes are needed on these tabs. The default settings will be correct for the OPC server system.

Security Tab

This tab allows you to change the launch, activation and access permissions for the server. The settings must be configured to grant these permissions for client applications using this server.

No changes are needed for the Configuration Permissions.
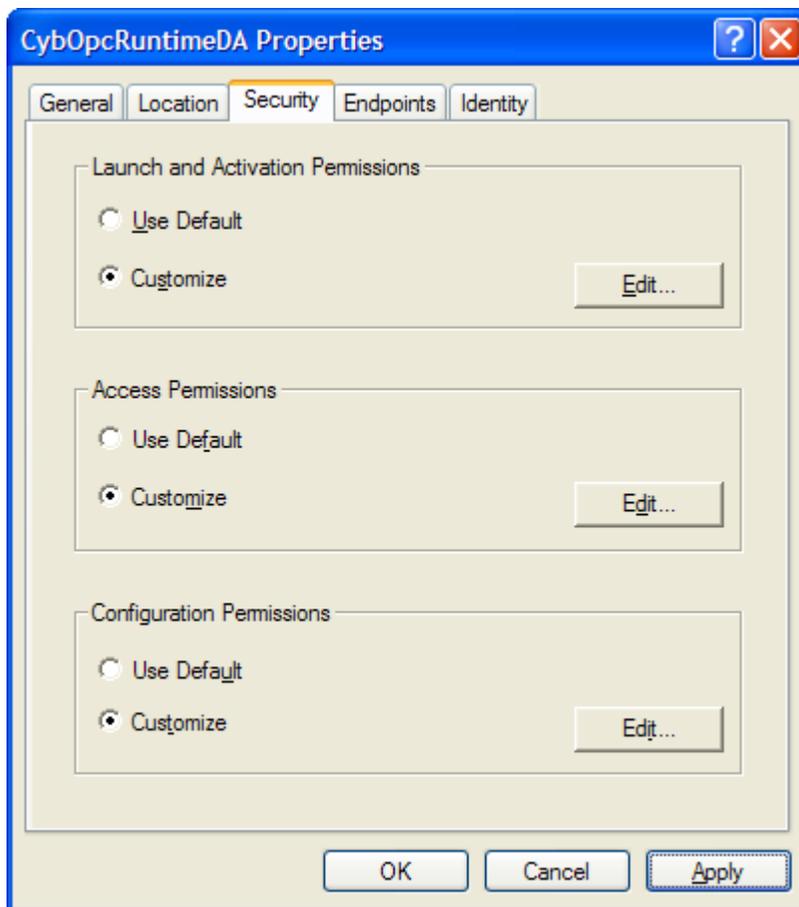
Launch and Activation Permissions

On some systems, this group is called Launch Permissions.

Launch permission is required to start a new COM application. Activation permission is required for a new client to use a COM application, even if the application has already been launched. Launch and activation permissions are divided into local and remote permissions. Users with local permission can start or use a COM application running on the same machine as the calling client. Users with remote permission can start or use a COM application from other computers across a network connection.

Because the OPC server will be launched by the OPC client application, the launch permission for the server must be granted for the security context in which the client is running.

6. In the Launch and Activation Permissions group, select the *Customize* option.

7. Click the *Edit...* button.

8. For each User or Group that will participate in OPC communication, check the **Allow** box for all permission types: Local Launch, Remote Launch, Local Activation and Remote Activation. When you are finished, click **OK**.

    If the User or Group you want to edit is not listed, refer to Appendix B: Adding Users or Groups for instructions on how to add to the listing.

| Caution! | The example shown grants these permissions to **Everyone**, which includes all authenticated users. You may wish to restrict this to a smaller group. The recommended way to do this is to create a group called **OPC Users** and add to this group all Users that will execute any OPC server or client. You would then grant the access, launch and activation permissions to the **OPC Users** group instead of **Everyone**. |

Access Permissions

Access permission grants a User or Group the right to communicate to an application. Access permissions are divided into local access permission and remote access permission. Users with local access permission may access a COM application running on the same machine as the calling client. Users with remote access permission may access a COM application from other computers across a network connection.

Because the OPC client application will call functions on the OPC server, the security context of the client must permit this.

Note   Cyberlogic's OPC server allow you to select preconfigured DCOM security settings that override the **Access Permissions** settings. If you decide to use one of these settings, you need not modify the **Access Permissions** here. Refer to Appendix A: Cyberlogic OPC Product DCOM Configuration for details.

9.   In the Access Permissions group, select the **Customize** option.

10. Click the **Edit...** button.

11. For each user or group that will participate in OPC communication, check the **Allow** box for Local Access and Remote Access. When you are finished, click OK.

If the User or Group you want to edit is not listed, refer to Appendix B: Adding Users or Groups for instructions on how to add to the listing.

Caution! The example above grants these permissions to **Everyone**, which includes all authenticated Users. You may wish to restrict this to a smaller group. The recommended way to do this is to create a group called **OPC Users** and add to this group all Users that will execute any OPC server or client. You would then grant the access, launch and activation permissions to the **OPC Users** group instead of **Everyone**.

Identity Tab

This tab allows you to specify the User account that will provide the security context for the server. There are four options:

- Recommended: **System Account**. Most OPC servers, including the Cyberlogic OPC Server run as a service, so the system account is selected by default. In most cases, this setting works well and should not be changed.

- Alternative: **This User**. If you have a special situation and need to set the exact security context to be used for the server, select **This User**. You must specify the desired User and that account's password in the Password and Confirm Password boxes.

Caution!	The User account you specify for this option must have access to the OPC server configuration file.

- Do not use: *Interactive User* and *Launching User*. The account that will actually be used with these selections is unpredictable, making it impossible to create a reliable configuration.
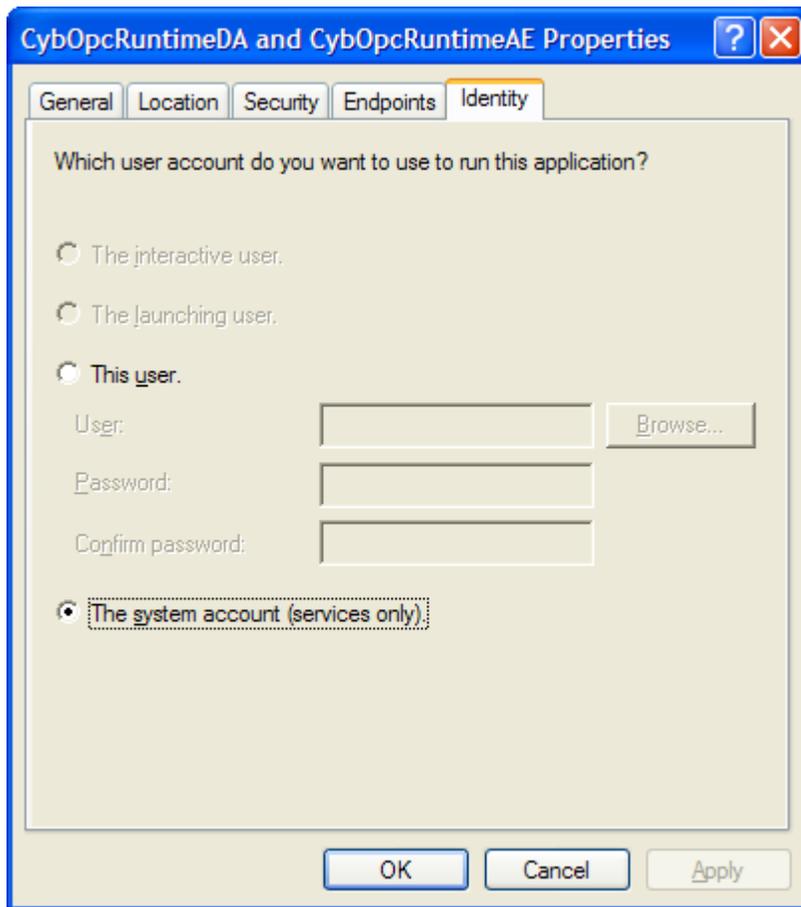
APPENDIX A: CYBERLOGIC OPC PRODUCT DCOM CONFIGURATION

Cyberlogic's OPC Server products provide a simple means to modify some of their DCOM security levels to meet the most commonly used configurations. In addition, the simple OPC client application provided with the servers includes the same capability.

Caution!	The preconfigured Low and Medium security settings override only the access permissions, authentication level and impersonation level for the Cyberlogic OPC Server or Client. The rest of the security settings must still be configured with the DCOMCNFG utility.

Using the Preconfigured Security Settings

When setting up DCOM security, you must take into consideration all of the OPC servers and clients that will communicate with each other. The servers must use the same security settings as the clients that will access their data. This, of course, implies that if you have multiple OPC servers that a client will access, then all servers must have the same security settings. Similarly, if you have multiple clients accessing the same server, all of the clients must have the same settings.

Some OPC applications—both clients and servers—have preset OPC security settings that specify their own access permissions, authentication level and impersonation level. These settings cannot be changed through the DCOMCNFG utility. If these applications are used with Cyberlogic's OPC products, you must configure the Cyberlogic products to match the other products' settings. There are two ways to do this.

- The Cyberlogic OPC Server and the test client have two preconfigured security levels that match the two most common settings used by OPC applications. It is likely that other OPC products you will use will work with one of these settings. You need only choose the proper setting for the Cyberlogic server or client, then restart it. The settings chosen for the Cyberlogic products will then be applied, overriding any different DCOM configuration in the system.

Caution!	The preconfigured settings selected in the Cyberlogic editors will apply only to the Cyberlogic product. All non-Cyberlogic products must be configured separately.

- If the other product you are using does not conform to either of the preconfigured settings in the Cyberlogic products, you can choose the *Custom* selection. This prevents the Cyberlogic software from overriding the system settings. You must then use the DCOM configuration editor to set the appropriate security levels. Refer to the System-Wide DCOM Configuration Issues and Server-Specific DCOM Configuration Issues sections for more information.

Preconfigured Server Security Settings

1. Open the Cyberlogic OPC Server Configuration editor **Tools** menu and select **Options...** .

2. When the Options dialog box opens, select the **Security** tab.

    Although there is no standard OPC security setting, the **Low** and **Medium** settings on this tab will match the requirements of most OPC clients, including Cyberlogic's.

| Caution! | If you change the selection on this tab, you must restart the Cyberlogic OPC Server for the new settings to take effect.

To restart the Server, open the Windows Control Panel, go to Administrative Tools and then Services. Right-click on **Cyberlogic OPC Server** and select **Restart**. |

3. If the **Low** or **Medium** security settings match your client application's settings, select the appropriate radio option. Refer to the Low and Medium sections for details on these settings.

4. If neither of the preconfigured settings are suitable for your installation, you must choose **Custom**.

    When the selection is **Custom**, the server does not override the default security values. Instead, the settings you edit with DCOMCNFG are used.

5. Click the **Launch DCOMCNFG...** button to edit the security settings manually.

    If you selected **Custom**, you must use DCOMCNFG to configure all of the security settings. If you selected **Low** or **Medium**, you must use DCOMCNFG to configure all

of the security settings except for the Cyberlogic OPC Server's access permissions, authentication level and impersonation level.

6. When you are finished, click *OK*.

Low

The **Low** selection overrides the default server-specific security values, giving them the following settings:

Security Parameter	Setting	Description
Access Permissions	All Users	Allows calls from anyone.
Authentication Level	None	No authentication occurs.
Impersonation Level	Identify	The server can obtain the client's identity. The server can impersonate the client to do access control list (ACL) checks, but it cannot access system objects as the client.

Note	When the Server starts, it will set the security level with the following call: CoInitializeSecurity(NULL, -1, NULL, NULL, RPC_C_AUTHN_LEVEL_NONE, RPC_C_IMP_LEVEL_IDENTIFY, NULL, EOAC_NONE, NULL);

Medium

The **Medium** selection overrides the default server-specific security values, giving them the following settings:

Security Parameter	Setting	Description
Access Permissions	All users	Allows calls from anyone.
Authentication Level	Packet	Authenticates credentials and verifies that all call data received is from the expected client.
Impersonation Level	Impersonate	The server can impersonate the client while acting on its behalf, but with restrictions. The server can access resources on the same computer as the client. If the server is on the same computer as the client, it can access network resources as the client. If the server is a computer different from the client, it can access only resources that are on the same computer as the server.

Note

When the Server starts, it will set the security level with the following call:

```
CSecurityDescriptor cSecurity;
cSecurity.InitializeFromThreadToken( );

CoInitializeSecurity(
cSecurity,
-1,
NULL,
NULL,
RPC_C_AUTHN_LEVEL_PKT,
RPC_C_IMP_LEVEL_IMPERSONATE,
NULL,
EOAC_NONE,
NULL);
```

Preconfigured Client Security Settings

1. Open the Cyberlogic OPC Client's **Tools** menu and select **Options…** .

2. When the Options dialog box opens, select the **Security** tab.

    Although there is no standard OPC security setting, the **Low** and **Medium** settings on this tab will match the requirements of most OPC servers, including Cyberlogic's.
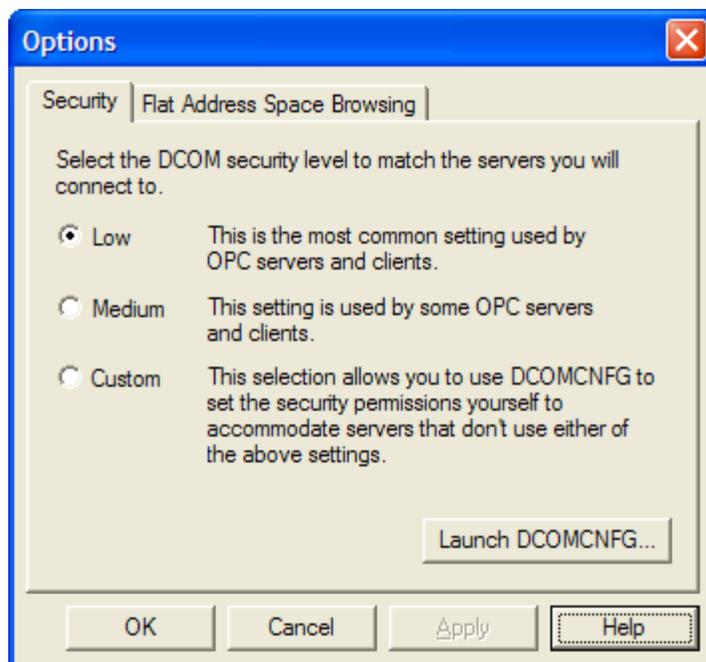
| Caution! | If you change the selection on this tab, you must restart the Cyberlogic OPC Client for the new settings to take effect. |

3. If the **Low** or **Medium** security settings match your server's settings, select the appropriate radio option. Refer to the server's Low and Medium sections for details on these settings.

4. If neither of the preconfigured settings are suitable for your installation, you must choose **Custom**.

   When the selection is **Custom**, the client does not override the default security values. Instead, the settings you edit with DCOMCNFG are used.

5. Click the **Launch DCOMCNFG...** button to edit the security settings manually.

   If you selected **Custom**, you must use DCOMCNFG to configure all of the security settings. If you selected **Low** or **Medium**, you must use DCOMCNFG to configure all of the security settings except for the Cyberlogic OPC Client's access permissions, authentication level and impersonation level.

6. When you are finished, click **OK**.

APPENDIX B: ADDING USERS OR GROUPS

When you are editing the default or limit permissions for launch, activation or access, you will modify these settings on the Security tab. This must be done for each User or Group you want to grant permission to. If the User or Group is not listed, you can use the following procedure to add them to the list.

1. From the Security tab for the permission you are editing, click the **Add...** button.
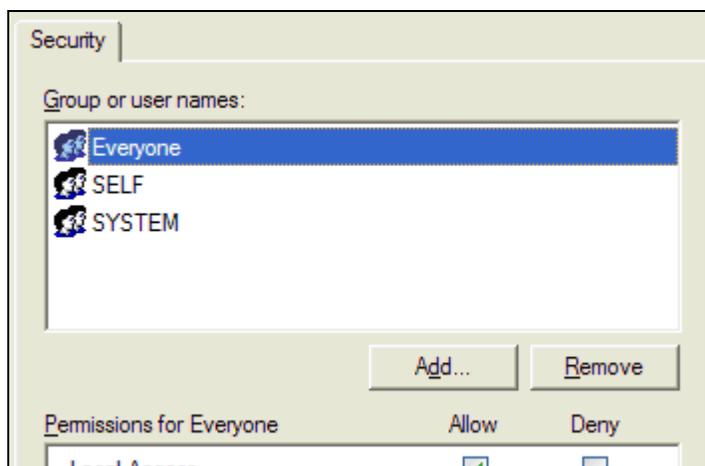
The Select Users, Computers, or Groups dialog box will open.

2. Click the **Advanced...** button.
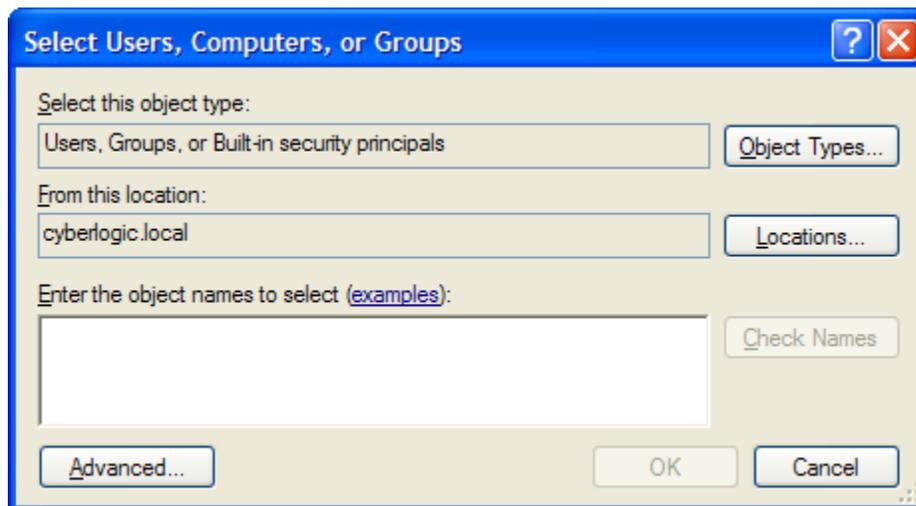
The advanced functions will then be available.

3. Click **Find Now**.

4. Select the desired User or Group from the list at the bottom of the dialog box

5. If you still do not see the User or Group you wish to add, you may need to look in a different location. Click the **Locations...** button to select the desired location, then repeat the **Find Now** operation.

6. When you have made your selection, click *OK* twice to return to the permissions edit screen.
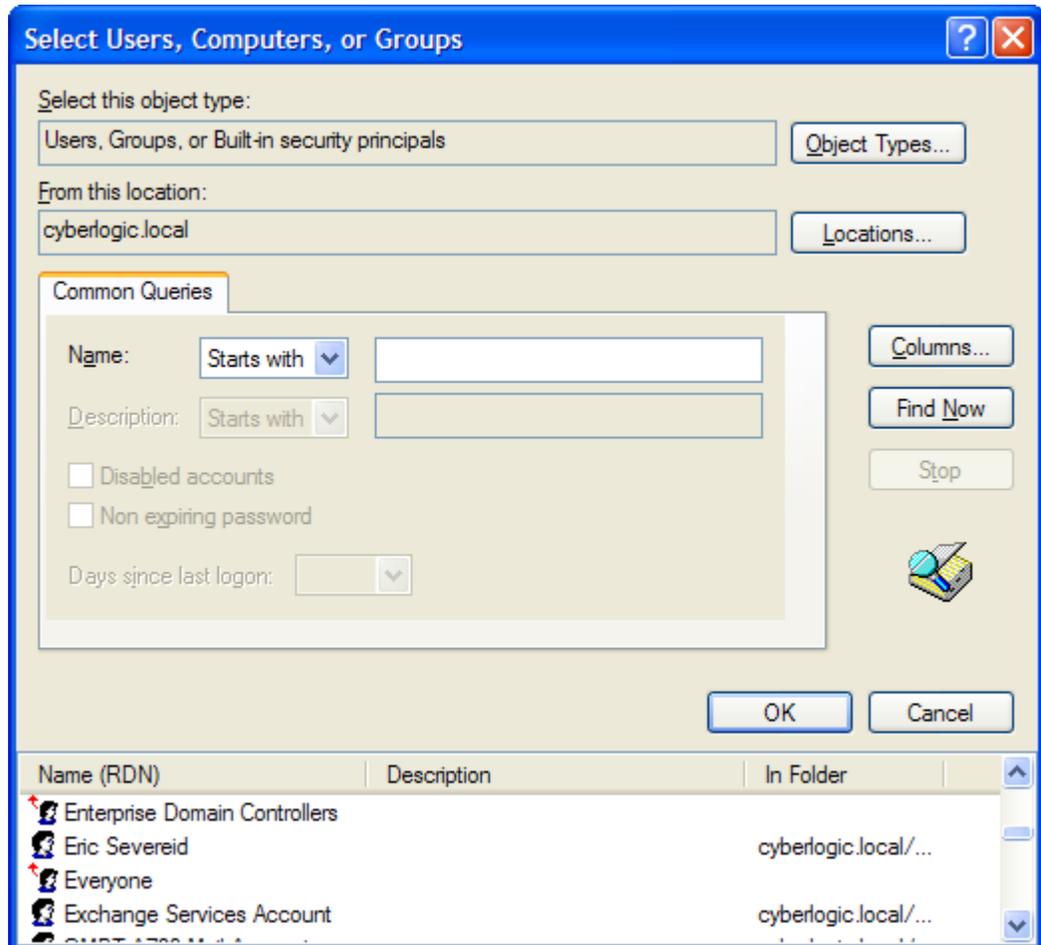
APPENDIX C: CONFIGURATION SETTING CHECKLIST

This appendix provides a summary of the typical security configuration settings used in OPC-based systems. It is intended for use by those who are thoroughly familiar with the material in this document and want a quick reference guide for configuring security.

Caution!	The body of this document contains important information on the procedures, options, risks and alternatives involved in configuring DCOM security. Be sure you are familiar with all of these discussions before attempting to use this checklist. This checklist does not cover all situations, so some of the settings shown here may not apply to your system.

Network Issues

- Domain: All systems in the same Domain or have Domains trust each other.

- Workgroup: All systems in the same Workgroup; identical user accounts on all systems.

- Mixed: Workgroup systems must have user accounts identical to those in the Domain.

Operating System Issues

- Windows 2000: Install SP3.

- Windows XP: Set network access local security setting to **Classic**. Add **TCP port 135, mmc.exe, OPCEnum.exe, CybOpcRuntimeService.exe,** and all other OPC clients and servers to the firewall exceptions list.

System-Wide DCOM Issues

- Make **TCP/IP** the preferred or only DCOM protocol.

- Enable DCOM.

- Set Default Authentication and Impersonation to **Connect / Identify** for Domain configurations, or **None / Anonymous** for Workgroup and Mixed configurations.

- For all Users or Groups that will use OPC communication, set defaults to allow Local and Remote Access and Local and Remote Activation.

- If Limit editing is available, set limits to allow Local and Remote Access for ANONYMOUS LOGON, and allow Local and Remote Launch and Activation for all Users and Groups that will use OPC communication.

Server-Specific DCOM Issues

- For all OPC servers, set Security Permissions to allow Local and Remote Launch, Activation and Access for all Users and Groups that will use OPC communication.

- Set the Identity to the *System account*.

WHERE CAN I GET MORE INFORMATION?

You can get detailed information on how to install, configure and use Cyberlogic's OPC servers by referring to the Help files for the DHX and MBX OPC Server Suites, DHX and MBX OPC Premier Suites, OPC Crosslink Suite and OPC Crosslink Premier Suite.

Cyberlogic's website, www.cyberlogic.com, has information on related products, news, software downloads and contact information.

Cyberlogic Technologies
5480 Corporate Drive
Suite 220
Troy, Michigan 48098 USA

Sales: 248-631-2200
                          sales@cyberlogic.com

Technical Support: 248-631-2288
                          techsupport@cyberlogic.com