# Kepware Technologies
# DCOM – Secure by Default

## For Kepware Server and Client Products

May, 2009
Ref. 50.08

# Table of Contents

# Table of Figures

# Tables

# 1. Overview

This white paper intends to provide users with information and instruction on how to configure the Distributed Component Object Model (DCOM) for use with OPC clients and servers. The information discussed will include the following:

- DCOM Security settings for Windows XP and higher operating systems.
- The security that DCOM provides and why it is important.
- Basic Windows/network security and how it relates to DCOM Security.
- User Groups and User Types and how they relate to DCOM Security.
- Configuring a secure DCOM connectivity using common Windows User, Security and Policy Management tools.

Furthermore, this white paper will focus on setting DCOM Security in domains where user security is centrally located and controlled by the domain server. Differences in settings and actions between Domain and Workgroup setups will be noted where applicable.

**Note:** Although OPC applications run on the home versions of Windows XP and Vista, these operating systems are not designed with Network/Domain security requirements in mind. We recommend that OPC applications be run in Business, Professional or Enterprise/Server Class operating systems in a production environment.

**Important:** Consult with your IT Manager before making any changes to the Windows Security settings or policies.

# 2. What is DCOM Security?

OPC DA is based on Microsoft's Component Object Model (COM) technology. Remote connectivity is accomplished using Distributed COM (DCOM), which contains a Security Layer. DCOM Security is used to determine which users have Access and Launching rights in DCOM-enabled applications on either the local PC or on PCs in the local network/domain.

DCOM is depends on Remote Procedure Calls (RPC) for remote connections. Any connection made to applications running under different accounts on a local PC is treated as a remote procedure call. This is important to remember when configuring the security settings.

DCOM was intended for use in domains, in which it is much easier to configure and manage connectivity. When connecting between Workgroup PCs or Domain and Workgroup PCs, the process becomes much more difficult.

## 2.1 Why is DCOM Security Important?

DCOM Security is important because it protects the process and data. Without security entailing permission for different actions, anyone with access to the network would be able to access your processes and make changes. Today, security is usually achieved by removing any ability for an outside connection at the facility.

## 2.2 How is DCOM Security Set?

DCOM Security is tied to the PC and Network/Domain Security. In a Domain, any user account on any machine in the Domain can be authorized. In Workgroups, each user on each PC must be added.

# 3. Windows Security

Windows Security specifies what a user can and cannot access and what can or cannot be done on a PC or Network. This is most noticeable when logging in to a PC or when sharing a folder that only allows certain users access. The ability to perform actions, run programs or change system settings on a PC or Network is also controlled by user security. Authorization is given with permissions.

At this point, the relationship between DCOM, OPC and security may still be unclear. It is important to understand, however, that Windows Vista and Windows 2008 Server operating systems contain new security features that directly impact the OPC servers' and clients' ability to run. Thus, if intending to run on these operating systems, the operating instructions may need to be updated to account for the new features.

## 3.1 What are Permissions?

Permissions are rules associated with objects (such as files or folders) on a computer or network: they determine if a user can access an object and what can be done with it. For example, a user may be able to access a document on a shared folder on a network, but can only read it and not make any changes. System administrators and users with administrator accounts can assign permissions to both individual users and groups.

The table below displays the permission levels that are normally available for files and folders.

| Permission Level | Description |
|---|---|
| Full Control | Users can view the contents of a file or folder, change existing files and folders, create new files and folders and also run programs in a folder. |
| Modify | Users can change existing files and folders, but cannot create new ones. |
| Read & Execute | Users can view the contents of existing files and folders and can also run programs in a folder. |
| Read | Users can view the contents of a folder and also open files and folders. |
| Write | Users can create new files and folders and also make changes to existing files and folders. |

**Table 1: Permission Levels for Files and Folders**

The following table displays the permission levels that are normally available for DCOM-Enabled applications.

| Permission Level | Description |
|---|---|
| Local Access | Allows the Group or Account on the local PC to access the application. |
| Remote Access | Allows the Group or Account on a remote PC access to the application. |
| Local Launch | Allows the Group or Account on the local PC to launch the application if it is not running. |
| Remote Launch | Allows the Group or Account on a remote PC to launch the application if it is not running. |
| Local Activation | Allows the Group or Account on the local PC to activate the application if it is not active. |
| Remote Activation | Allows the Group or Account on a remote PC to activate the application if it is not active. |

**Table 2: Permission Levels for Applications**

## 3.2 User Groups in Windows

A User Group is a collection of user accounts that have the same security rights. They are sometimes referred to as Security Groups.

The two most common user groups are the **Standard User Group** and the **Administrator Group**. A user account is often referred to by the user group it is in; thus, an account in the standard user group is called a standard account. An administrator account can create custom user groups, move accounts from one group to another and add or remove accounts from different groups. Rights are assigned when a custom user group is created.

**Note:** A user account can be a member of more than one group.

### 3.2.1 What is a User Account?

A User Account is a collection of information that tells Windows what files and folders can be accessed, what changes can be made to the computer and also the user's personal preferences (such as desktop background and color theme). User accounts make it possible to share a computer with several people while retaining individual files and settings. Each person accesses their user account with a user name and password.

The table below displays the kinds of accounts associated with the different operating systems.

| Vista and Win 2008 | XP and Win 2008 |
|---|---|
| Administrator | Administrator<br>Power User |
| Standard User | User/Restricted User |
| Guest | Guest |

**Table 3: Account Types by Operation System**

Each account type provides a different level of control. The Administrator Account, which should only be used when necessary, has the most control over the computer's programs and security. The Standard Account, which is preferable for everyday computing, has access to most programs and files installed on the computer. The Guest Account, which can be used by people who don't have a permanent account, provides temporary access to the computer.

**Note:** In Windows XP and 2003 operating systems, the **Power User** has most of the same privileges as an administrator, but not all. In Vista and Windows 2008, administrators run as users and are only elevated to administrator status when an action requires that level of user privilege.

### 3.2.2 What is an Administrator Account?

An Administrator Account is a user account that can make changes that affect other users. Administrators can change security settings, install software and hardware, change other user accounts and access all files on the computer.

When setting up Windows, you'll be required to create a user account. This, the administrator account, will allow you to setup the computer and install any programs that will be used. Microsoft recommends that a standard user account be used for everyday computing, however, as it is more secure.

### 3.2.3 What is a Standard User Account?

A Standard User Account allows access to most of the computer's capabilities, but requires permission from an administrator to make changes that will affect the computer's security (or other users).

A standard account allows users to access most programs that are installed on the computer. It does not, however, allow users to do the following:

- Install or uninstall software and hardware.
- Delete files that are required for the computer to work.
- Change settings on the computer that affect other users.

When using a standard account, some programs might require an administrator password before certain tasks can be performed.

### 3.2.4 What is a Guest Account?

A Guest Account is for users who don't have a permanent account on the computer or domain. It allows people to use the computer without having any access to personal files. This account cannot install software or hardware, change settings or create a password.

**Note:** The guest account must be turned on before it can be used.

### 3.2.5 A Standard User Account vs. an Administrator Account

The standard account helps protect the computer by preventing users from making any changes that will affect everyone who uses the computer. A standard account can do anything that an administrator account can do, barring making changes that will affect other users. If attempting to install software or change the security settings, Windows may prompt for an administrator account password.

**Note:** We recommend that a standard account be created for all users.

# 4. User Account Control Overview

In Windows 2008 and Vista, processing can also be affected by **User Account Control (UAC),** which is a new set of infrastructure technologies that help prevent malicious programs (malware) from damaging the system. UAC also helps organizations to manage the desktop more efficiently.

With UAC, applications and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC stops the automatic installation of unauthorized applications and prevents inadvertent changes to system settings.

## 4.1 How Does UAC Work?

In Windows 2008 and Vista, there are two levels of users: standard users and administrators. Standard users are members of the Users Group and administrators are members of the Administrators Group. Unlike previous versions of Windows, both standard users and administrators can access resources and run applications in the security context of standard users by default. When any user logs on to a computer, the system creates an **access token**, which contains information about the level of access that the user is granted. This includes specific **Security Identifiers (SIDs)** and Windows privileges.

When an administrator logs on, two separate access tokens are created: a standard user access token and an administrator access token. The standard user access token contains the same user-specific information as the administrator access token, but removes the administrative privileges and SIDs. The standard user access token is used to start applications that do not perform administrative tasks.

When the administrator needs to run applications that do perform administrative tasks, the operating system will prompt for a change or elevation in the user's security context (from a standard user to an administrator). This default administrator user experience is called **Admin Approval Mode**. In this mode, applications require specific permission to run as an administrator application, which an application that has the same access as an administrator.

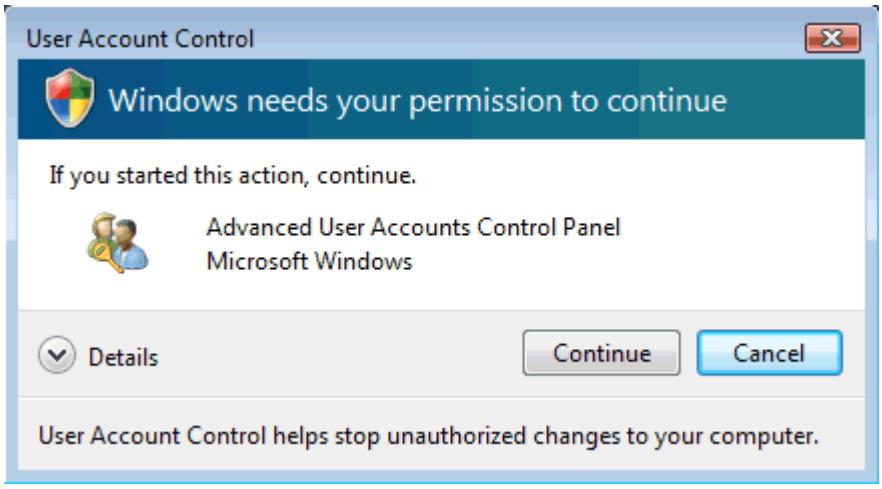


**Figure 1: User Account Control Message Dialog**

A User Account Control message is invoked by default when an administrator application starts, giving the user a choice to start or cancel the application. If the user is a standard user, they can enter the user name and password of an account that is a member of the local Administrators group to continue.

**Note:** The Group Policy parameter can be used to change the User Account Control message's behavior.

While designing an application, the software developer should identify it as either an administrator application or a standard user application. If it has not been identified as an administrator application, it will be treated as a standard user application. Administrators can also mark applications to be treated as administrator applications.

## 4.2 UAC Permission Prompts

When a permission or password is needed to complete a task, UAC will invoke one of the following messages.

### 4.2.1 Windows needs your permission to continue

A Windows function or program that may affect other users on this computer needs permission to start. Check the name of the action to ensure that it's a function or program you want to run.

### 4.2.2 A program needs your permission to continue

A program that's not part of Windows needs permission to start. It has a valid digital signature that indicates its name and publisher, which helps to ensure authenticity. Make sure that this is a program that you intended to run.

### 4.2.3 An unidentified program wants access to your computer

An unidentified program is one that doesn't have a valid digital signature from its publisher to ensure authenticity. Although this doesn't necessarily indicate danger (since many older, legitimate programs lack signatures) you should use extra caution and only allow this program to run if it was obtained from a trusted source (such as the original CD or a publisher's website).

### 4.2.4 This program has been blocked

This is a program that the administrator has specifically blocked from running on the computer. To run this program, you must contact the administrator and ask to have the program unblocked.

## 4.3 How UAC affects DCOM OPC?

UAC affects DCOM OPC by impacting the user's ability to set DCOM Security or change the Security settings. If UAC is on and you are a Standard User with no administrator credentials, you will neither be able to change DCOM Security nor be able to turn UAC off.

**Note:** Many manufacturers recommend that UAC be turned off in the Production environment. For KEPServerEX 5.x, this is not required once DCOM has been configured. For KEPServerEX 4.x, UAC must be disabled. To do so, follow the instructions below.

1. Open the **User Accounts Manager** in the **Control Panel**.
2. Click on **Turn User Account Control On or Off**.

# 5. Creating Users and User Groups

The best way to ensure secure OPC connections is to create an OPC-Specific User Group and OPC-Specific Users. These can be manually created on any PC on which you have Administrator level privileges. The Groups and Users will be Local to that PC. If working on a domain, contact the IT/Network Administrator to have these changes made.

## 5.1 User Groups in Windows

A User Group is a collection of user accounts that contain the same security rights. User groups are sometimes referred to as Security Groups. A user account can be a member of more than one group. The two most common user groups are the standard user group and the administrator group.

The following steps demonstrate how to create a local user group to which local and domain users can be added.

### 5.1.1 Creating a User Group

These steps cannot be completed on Home or Starter versions of Windows operating systems.

1. In the **Command Line**, type "MMC.exe" to launch the Microsoft Management Console.

   **Note:** Only users with administrator privileges can use the MMC. On operating systems with UAC enabled, you may be prompted for an administrator password or confirmation. If so, type the password or provide confirmation.

2. Next, click **Local Users and Groups**.

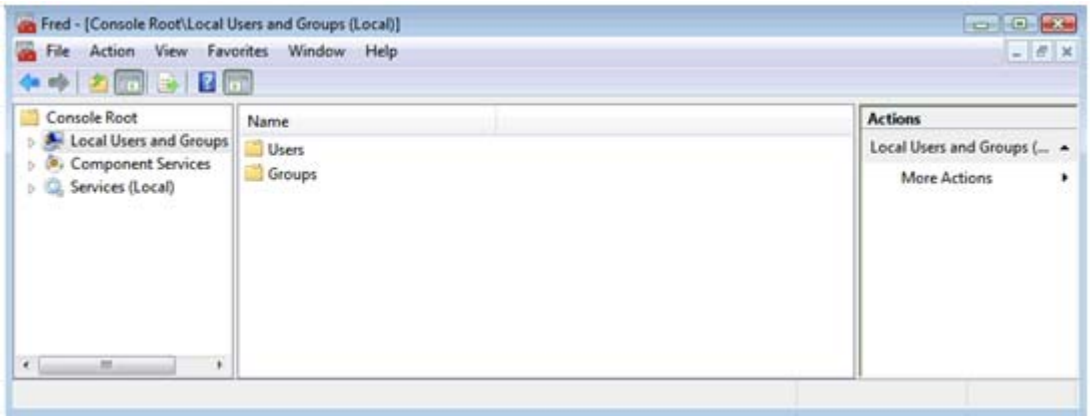


**Figure 2: Microsoft Management Console**

**Note:** If Local Users and Groups is not visible, the snap-in may not have been added to the Microsoft Management Console. Follow the instructions below for information on how to install it.

a. In the Microsoft Management Console, click **File** | **Add/Remove Snap-in**.

b. Next, click **Local Users and Groups** and then select **Add**.

c. Click **Local Computer** and then select **Finish**.

d. Click **OK**.

3. Double-click on **Groups** and then select **Action**.
4. Click **New Group** and then specify a group name and a description.

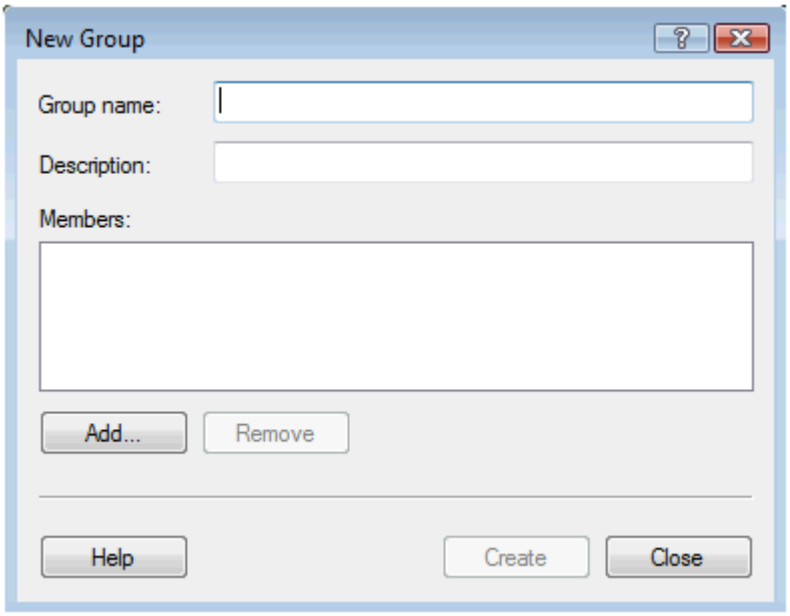


**Figure 3: New User Group Dialog**

5. Click **Add** to open the **Select Users, Computers or Groups** dialog.
6. Next, assign the user account a name.
7. Click **Check Names** and then select **OK**.
8. Click **Create**.

## 5.2 Adding a User Account to a Group

Adding a user account to a group can bypass needing to grant the same access and permission to users individually. Group members can make the same types of changes to settings and have the same access to folders, printers and other network services.

**Note:** These steps cannot be completed on Home or Starter versions of Windows operating systems.

1. Click to open the **Microsoft Management Console**. Enter the administrator password or provide confirmation if prompted.
2. Next, click **Local Users and Groups** and select the **Groups** folder.
3. Double-click on the group to which the user account will be added. Then, click **Add**.

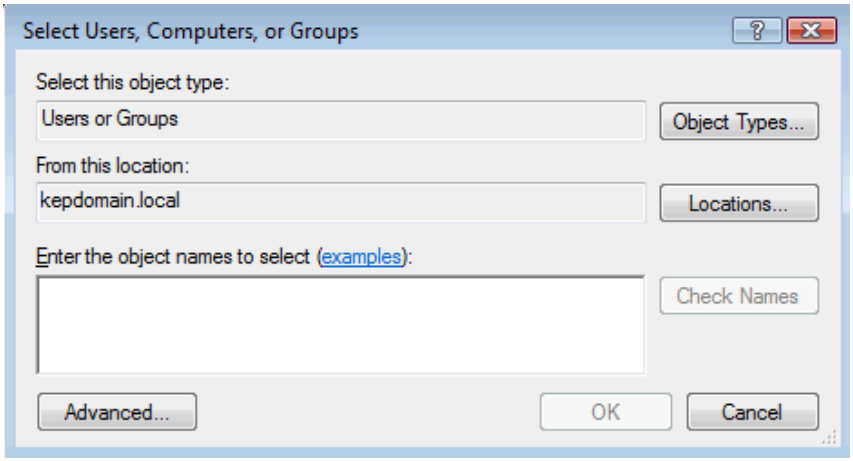


**Figure 4: User Account Select Dialog**

4. Type in the name of the user account that will be added to the group.

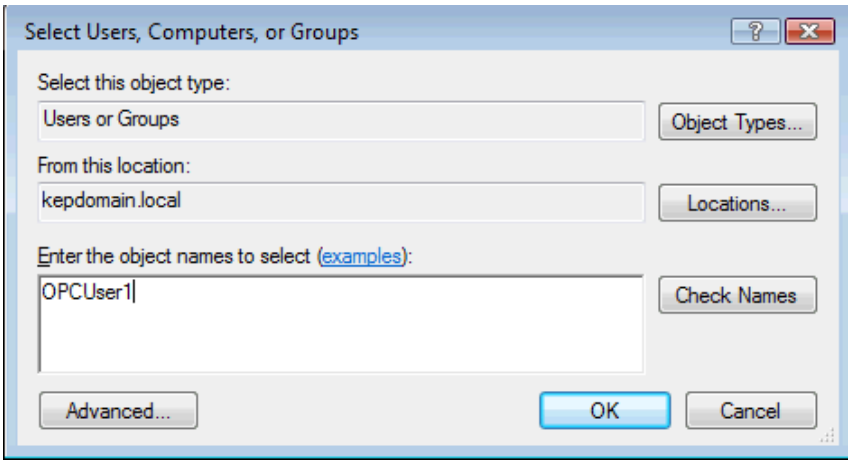


**Figure 5: User Account Select Dialog With Selected User**

5. Click **Check Names** to verify that the user account exists.

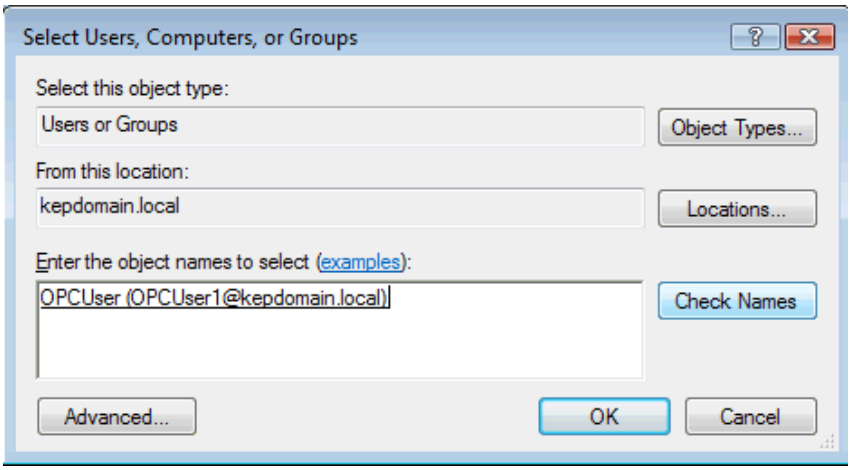


**Figure 6: User Account Select Dialog with Verified User Account**

6. Click **OK** to accept.

**Note:** For a higher level of security, be sure to only add a user to the Administrators Group if it is necessary. Users in this group have complete control over the computer: they can see all files, change all user passwords and install any software.

## 5.3 Creating a User Account

User accounts allow several people to share a single computer. Each person can have a separate account containing their unique settings and preferences. User accounts also control access to files and programs as well as the type of changes that can be made to the computer. Standard accounts are normally made for most computer users. For more information, follow the instructions below.

1. Open the **Windows Control Panel**.
2. Click **User Accounts** in order to open the **User Account Manager**.

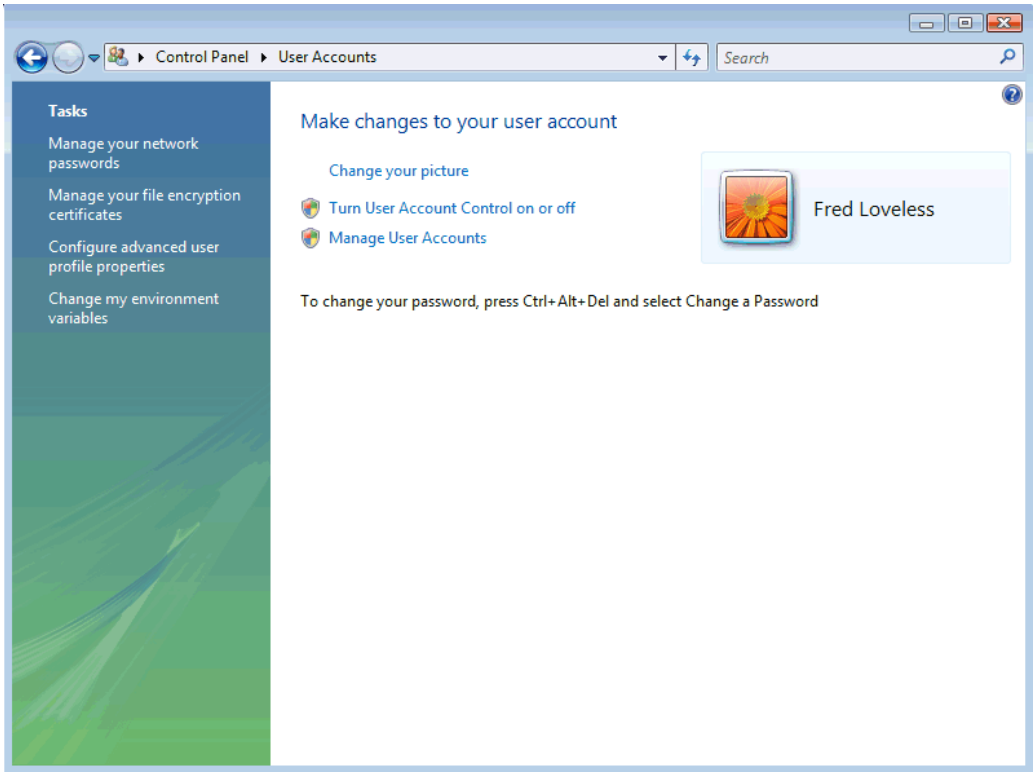


**Figure 7: User Account Manager**

3. Click **Manage Another Account**.

   **Note:** Provide an administrator password or confirmation if prompted.

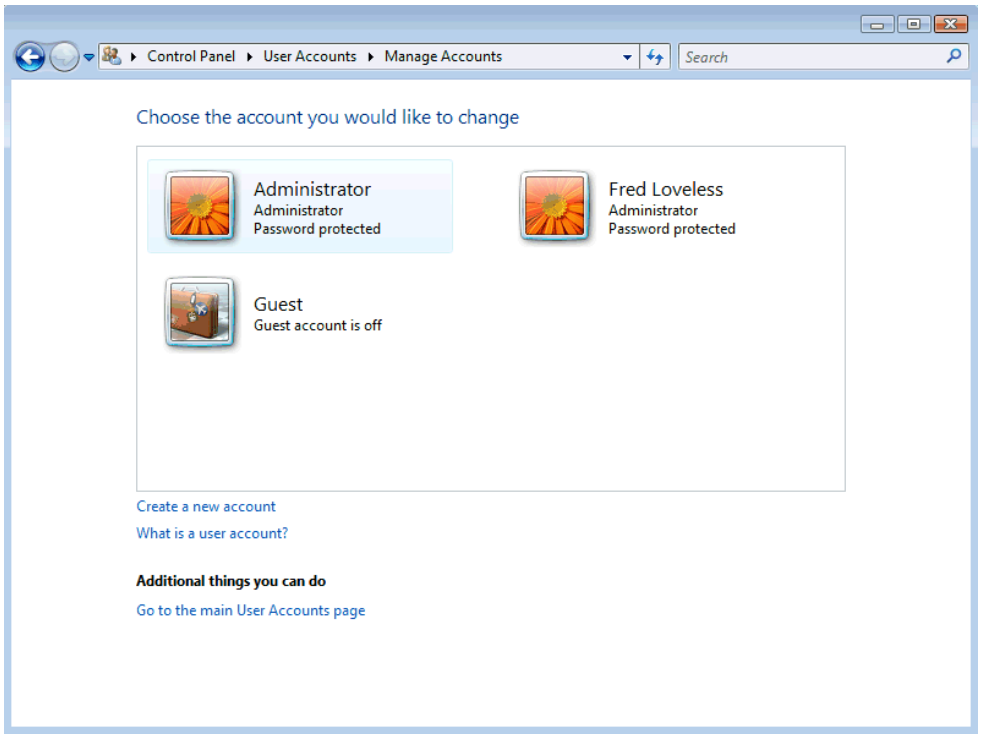


**Figure 8: User Accounts List**

4. Select **Create a new account**.

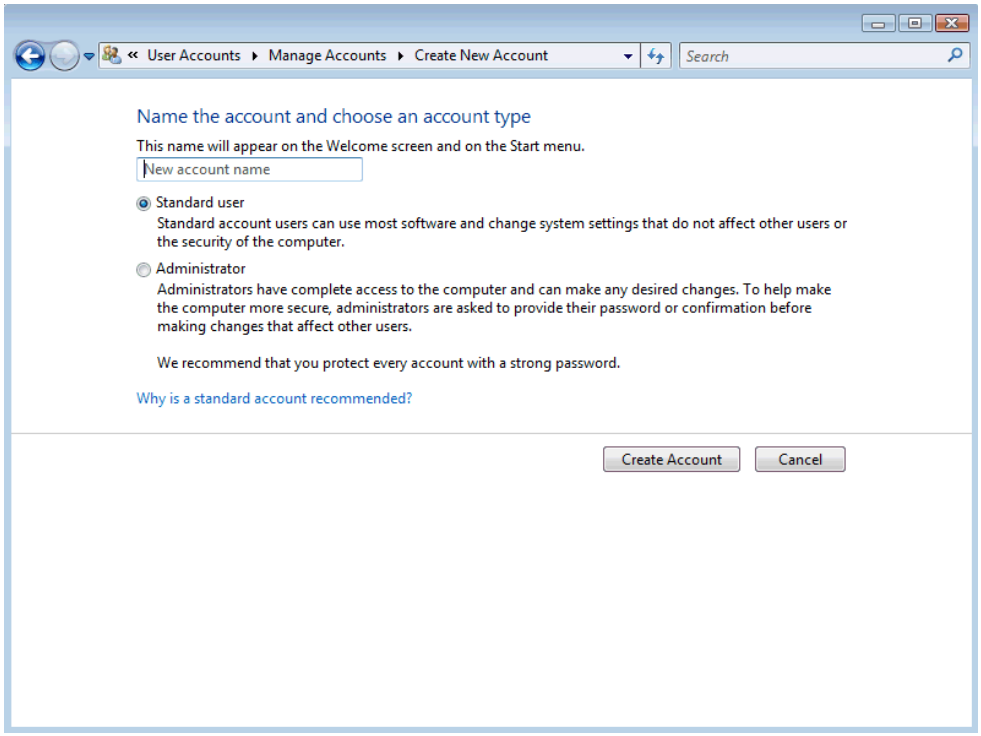


**Figure 9: New User Account Dialog**

5. Specify a name for the user account.

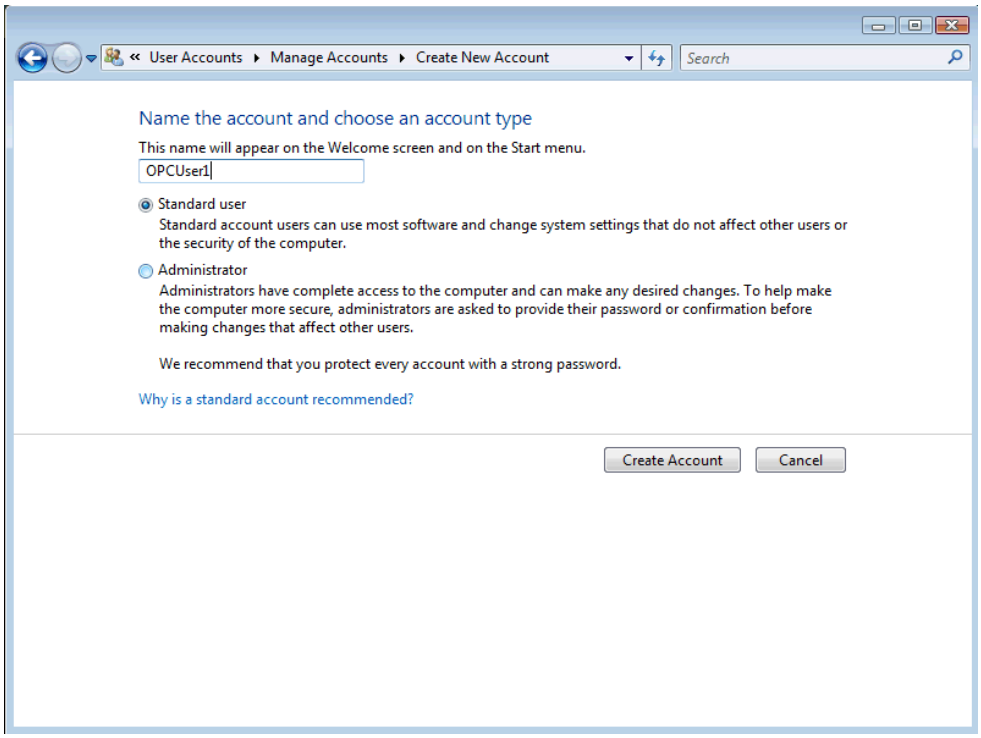


**Figure 10: New User Account Dialog With New User**

6. Select an account type that will be assigned to the user.
7. Click **Create Account**.

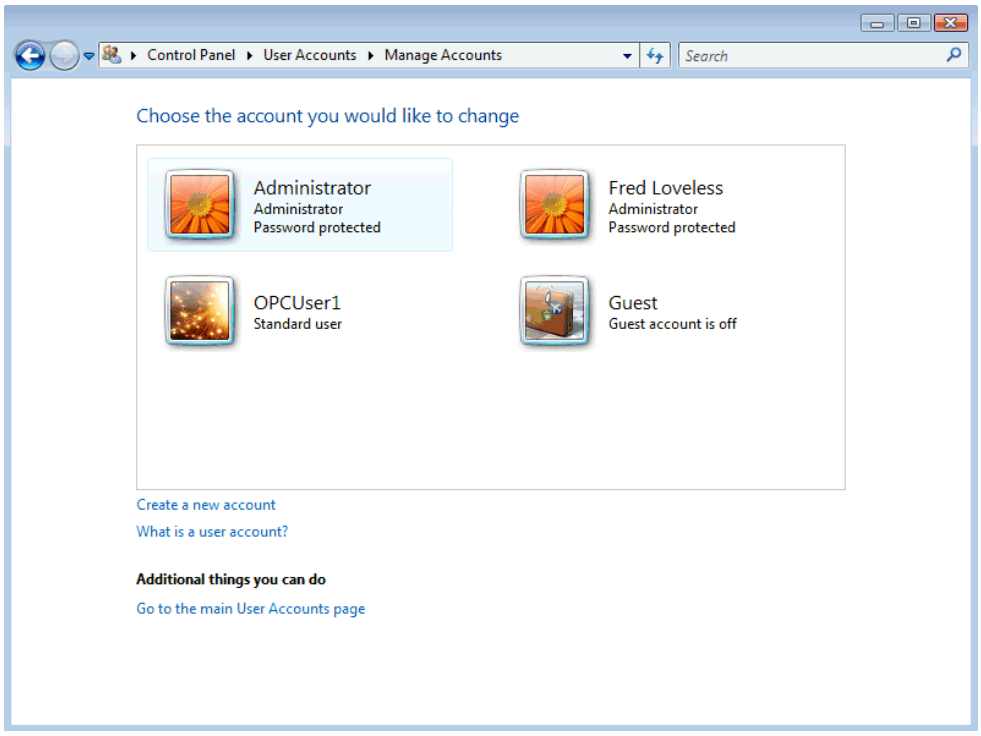


**Figure 11: User Accounts List With New User**

8. Repeat the process until all accounts are added.

### 5.3.1 Changing a User's Account Type

The administrator account was initially created to finish Windows setup and program installation. After this initial setup, we recommend that a standard account be created for everyday computing. All new user accounts should be made into standard accounts in order to keep the computer secure from unauthorized changes.

1. Open the **Windows Control Panel**.
2. Click **User Accounts** to open the **User Account Manager**.
3. Click **Manage another account**.

   **Note:** Provide an administrator password or confirmation if prompted.

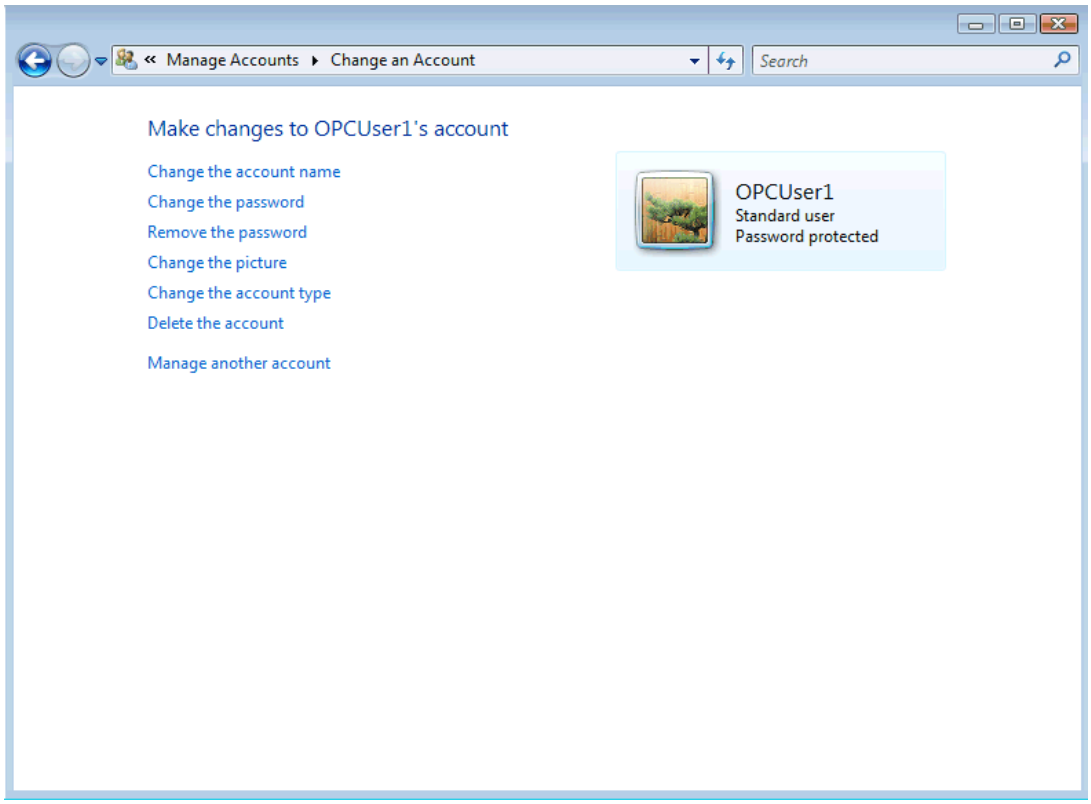


**Figure 12: User Account Property Settings**

4. Select the account that will be changed and then click **Change the account type**.

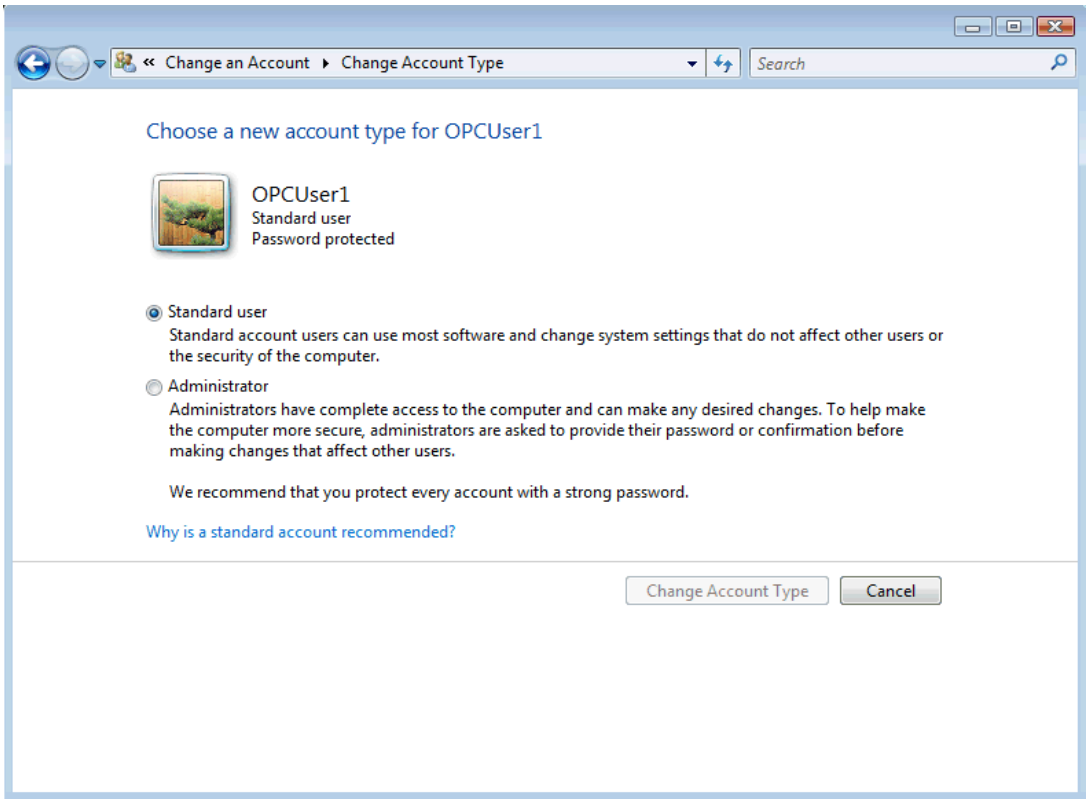


**Figure 13: Change User Account Type**

5. Select the desired account type and then click **Change Account Type**.

**Note:** Windows requires at least one administrator account on a computer. If you only have one, you will not be able to change it to a standard account.

# 6. Configuring DCOM Security

DCOM Security is one of the more difficult aspects of OPC Products. Many manufacturers have opened DCOM Security as wide as they can on their networks in order to ease connectivity between DCOM-enabled applications. With a little planning, however, you can achieve secure connections easily. The rest of this document focuses on the following:

- How DCOM Security works.
- How to set up DCOM Security for secure access between clients and servers.
- How to set DCOM Security wide open.
- Local Security Policies.
- The Windows Firewall, and how it is configured.
- What is needed for DCOM when User Switching is being used.
- How DCOM is affected when applications are run as a service.

## 6.1 How DCOM Security Works

An important aspect of DCOM is its associated permissions. When assigning DCOM permissions for a specific Account or User Group on a particular application, you can specify whether other applications running under that group can access it. DCOM defines the user accounts that have access to the application, as well as the user accounts from which an application can accept responses.

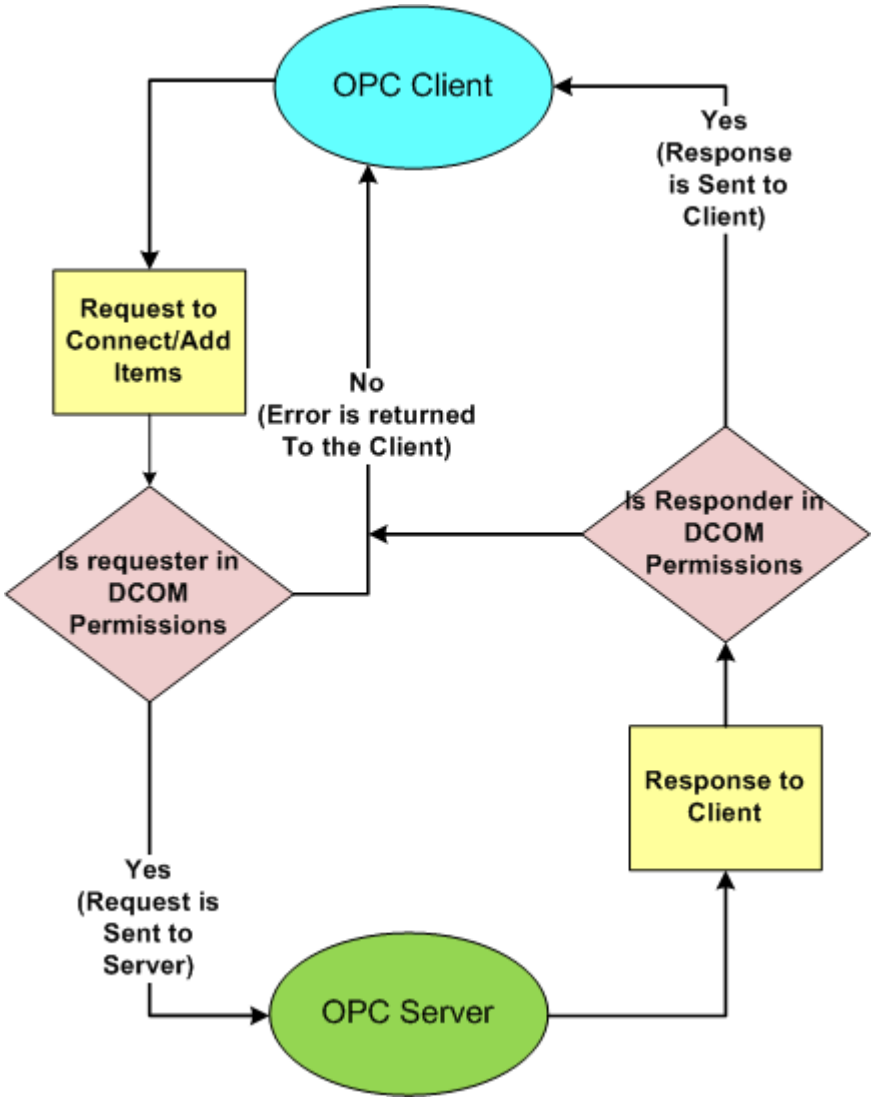


**Figure 14: DCOM Security Working Flow Model**

## 6.2 Setting Secure DCOM by Application

To make DCOM secure by default, set security for the application rather than for the entire operating system.

### 6.2.1 Starting the DCOM Configuration Utility

There are four ways that users can launch the DCOM Configuration. Choose from the methods below to open component services.

1. For KEPServerEX or LinkMaster, click on the **Launch DCOM Configuration button** .
2. In the server, click on **Tools** | **Launch DCOM Configuration**.
3. In the **Start** menu, type **DCOMcnfg.exe** in the run command. Then, click **OK**.

   **Note:** Alternatively, launch the **Control Panel** and then double-click on **Administrative Tools**. Finally, select **Component Services**.

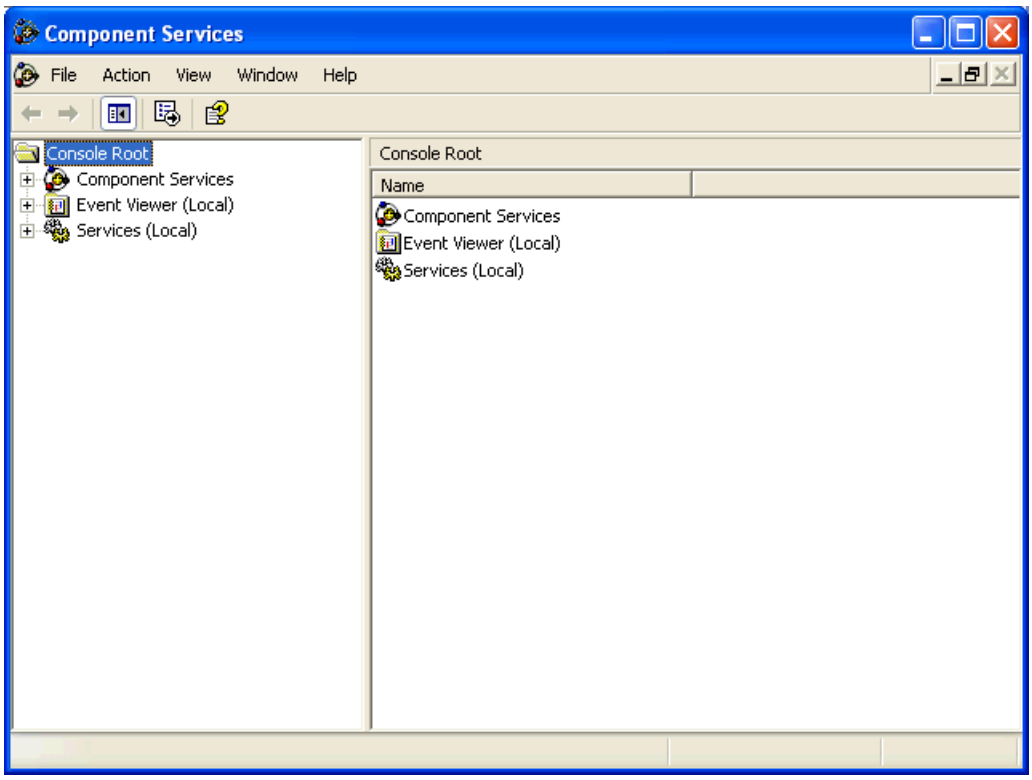


**Figure 15: Component Services Console**

4. Once the DCOM Configuration is open, double-click on **Component Services**. Open the **Computers** folder.
5. Expand **Computers** and then select **My Computer**.

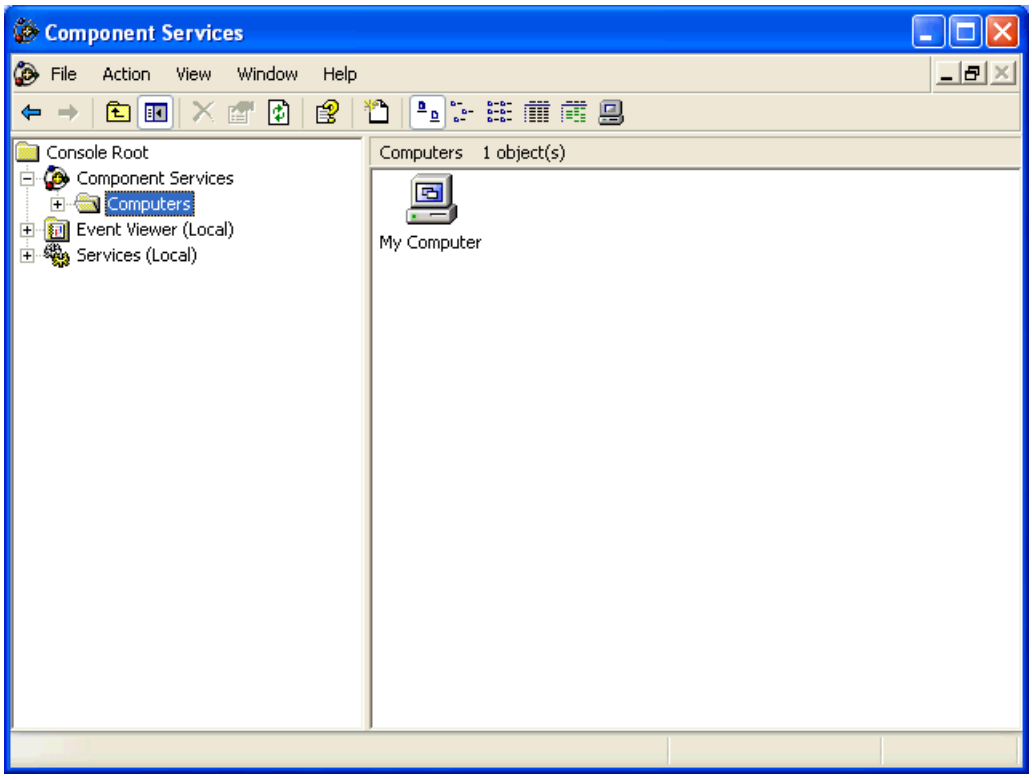


**Figure 16: Component Services Console - Computers**

### 6.2.2 Selecting a DCOM Enabled Application

Follow the instructions below for information on selecting a DCOM-enabled application.

1. Expand the **My Computer** folder and then select the **DCOM Config** folder.
2. Browse the DCOM enabled applications until the one that will be configured is located.

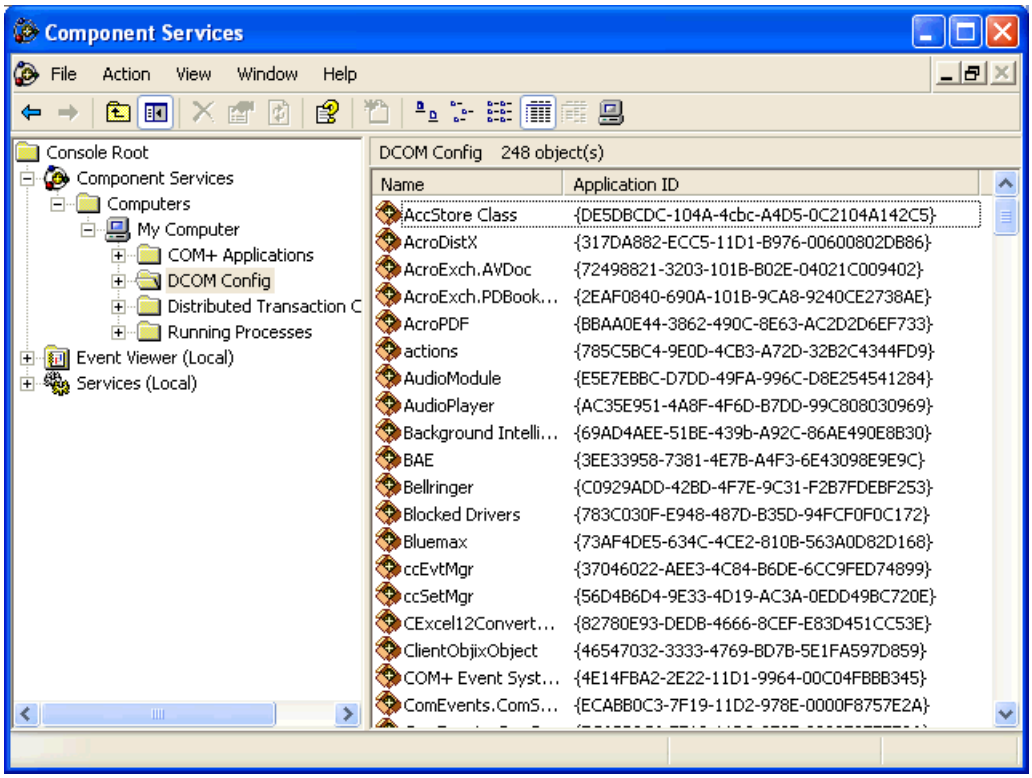


**Figure 17: DCOM Enabled Applications on the Computer**

3. Then, right-click on the application and select **Properties**.

### 6.2.3 A DCOM Application's General Properties

The Property Window will open to the General tab. The Authentication level will be set to default, but can be changed. The three most important settings are as described below.

a. **Default:** This setting tells the application to use whatever the default is for all DCOM enabled applications. If the application is running as a service, it will use the authentication of the user that it is running as.

b. **None:** This setting tells the application to use no authentication. This is not recommended.

c. **Connect:** This setting tells the application to authenticate using the connecting application.

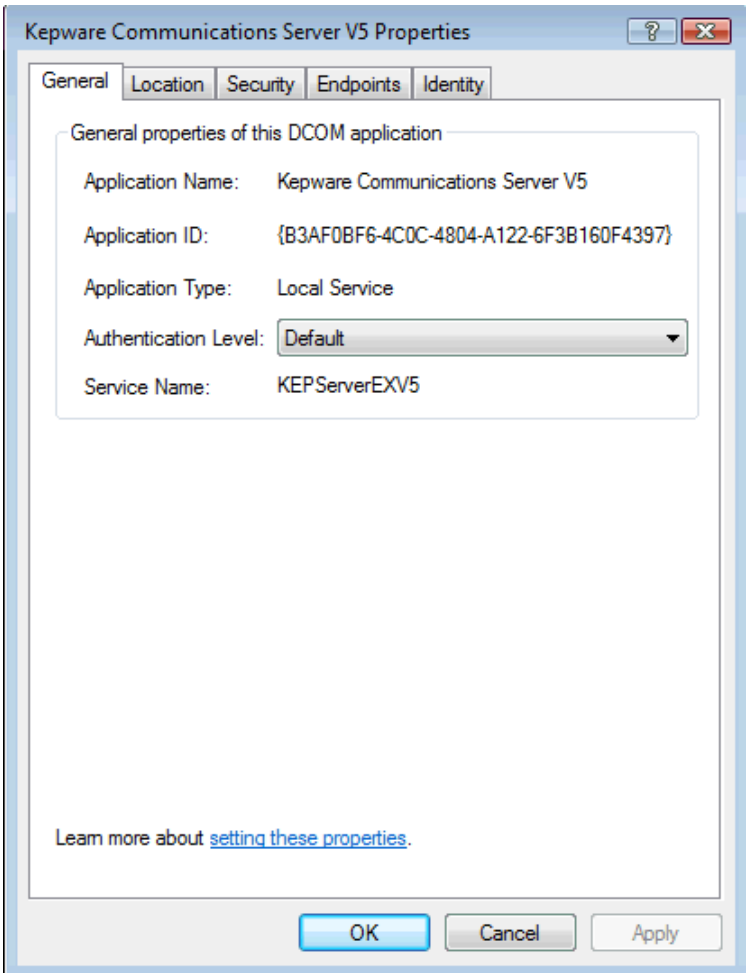


**Figure 18: DCOM Properties for KEPServerEX 5**

**Note:** For this example, leave the Authentication Level at Default. Then, select the Location tab.

### 6.2.4 A DCOM Application's Location Properties

The Location Tab directs the client connection to where the server application is running. For OPC 2.0 and higher applications **Run application on this computer** should be checked.

**Note:** There should only be one selection checked at one time.

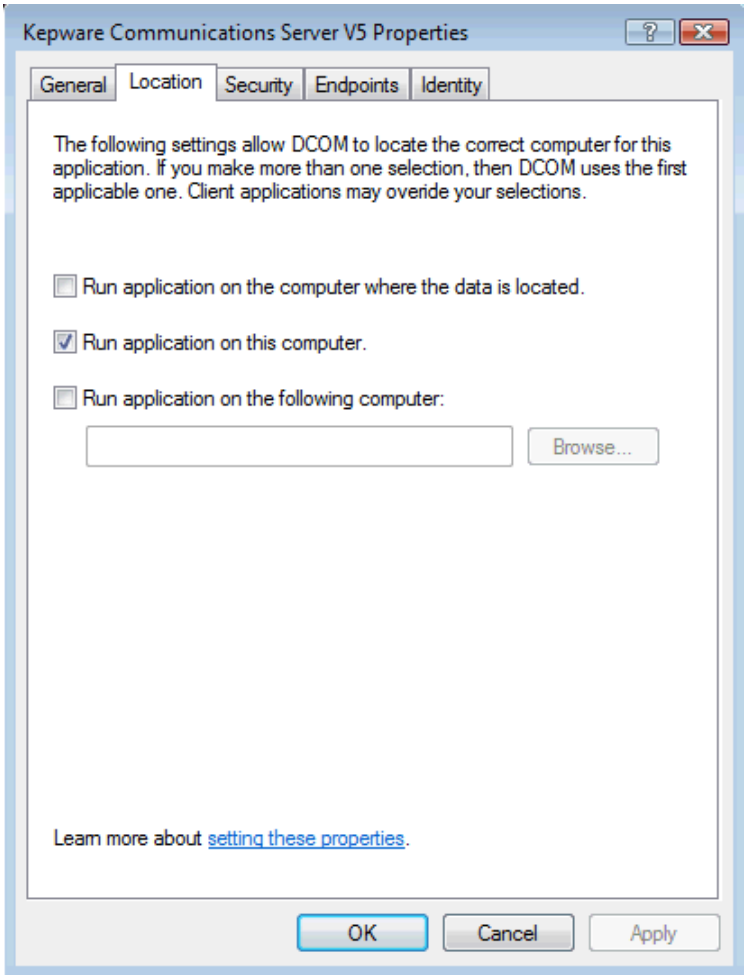


**Figure 19: Application DCOM Location Properties**

**Note 1:** For this example, leave the setting at Default. Then, select the Identity tab.

**Note 2:** The OPC 1.0 Specification did not support the Remote Browsing and Connectivity of OPC servers. To do a remote connection, the local registry requires an entry for the server. Users must then select "Run application on the following computer:" and then provide the computer name or the IP of the PC running the server to which a connection is desired. A local connection to the server by the client would then be routed to the remote PC.

### 6.2.5 A DCOM Application's Identity Properties

The Identity Tab specifies what user account the application will run under when it is started. Descriptions of the options are as follows.

a. **Interactive User:** A user running interactively on the desktop.

b. **Launching User:** The user that makes the initial connection request to an application that is not running, but is then launched.

c. **Specified User:** A specified user account on the PC. If the server is running as a service on a Windows XP or 2003 server OS, the account will not be able to be opened on the desktop.

d. **System Account:** This is the default for applications that are running as a service.

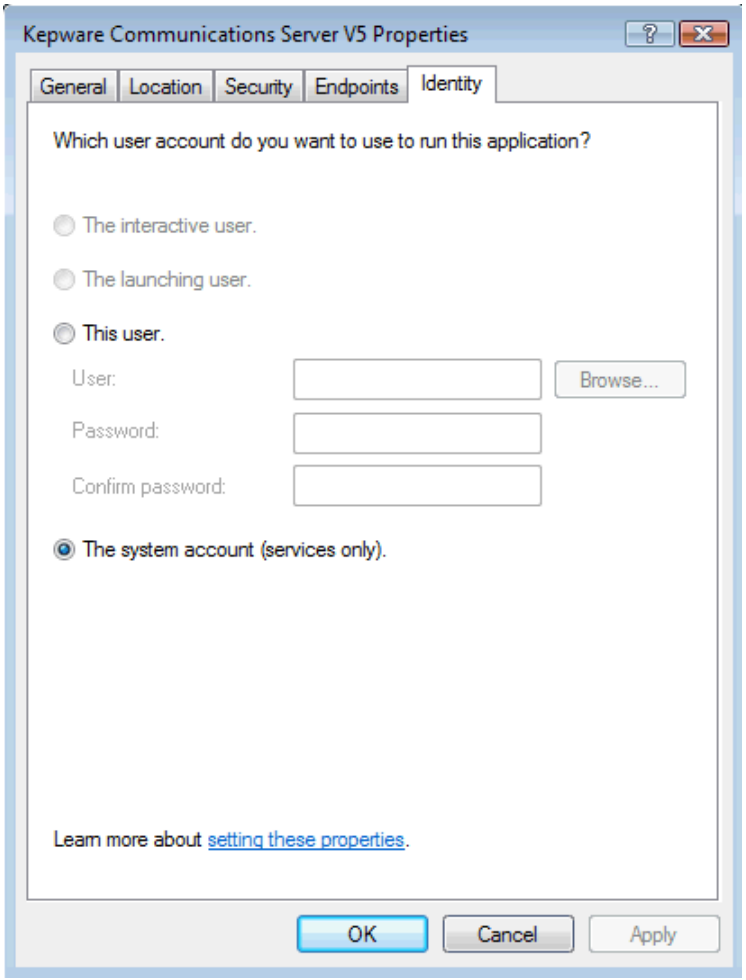


**Figure 20: Application DCOM Identity Properties**

**Note:** Leave the tab unedited. Then, open the Security Tab.

### 6.2.6 A DCOM Application's Security Settings

The Security tab specifies which users can Launch, Activate and Access the application. Descriptions of the options are as follows.

a. **Default:** This setting tells the application to use the System Defaults.

b. **Customize:** This setting tells the application to use the custom settings that are being specified in this dialog.

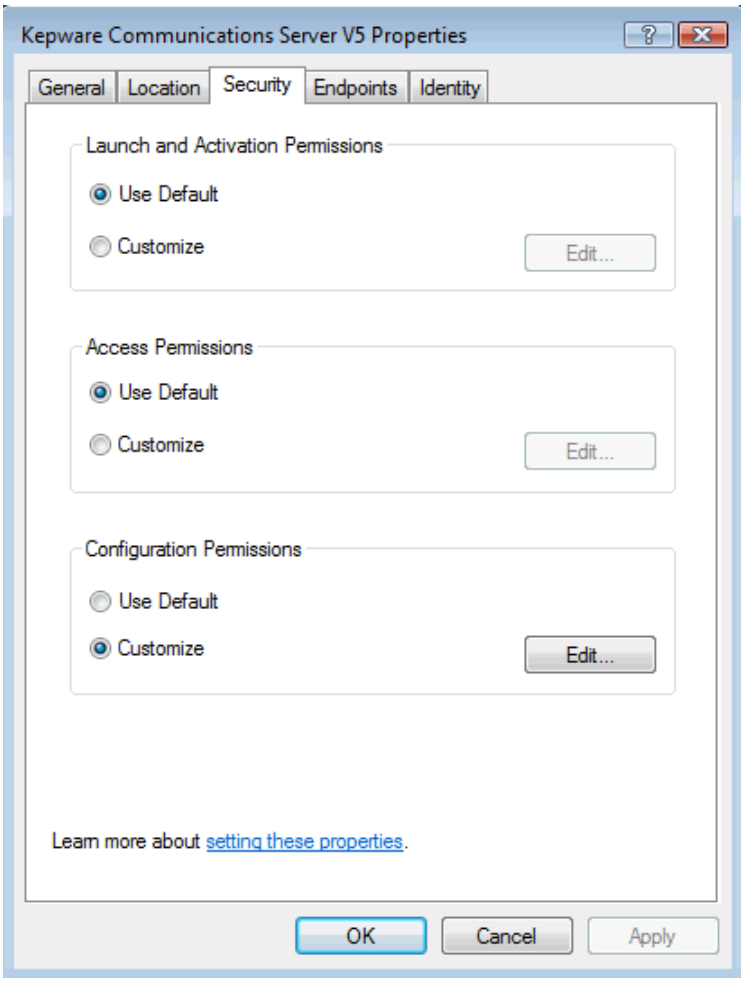


**Figure 21: Application DCOM Security Properties**

**Note:** Set Launch and Activation Permissions first. To do so, click Customize to set local permissions. Then, click Edit to set permissions for users.

## 6.3 Launch and Activation Permissions

The Launch and Activation Permissions window will open to default settings. Since we are making the Application DCOM Secure, we only want certain accounts to work with the application. For Kepware products, applications must always be running under the **System Account and local Administrators** to have permissions. Leave them as they are but remove the **Interactive Account**.

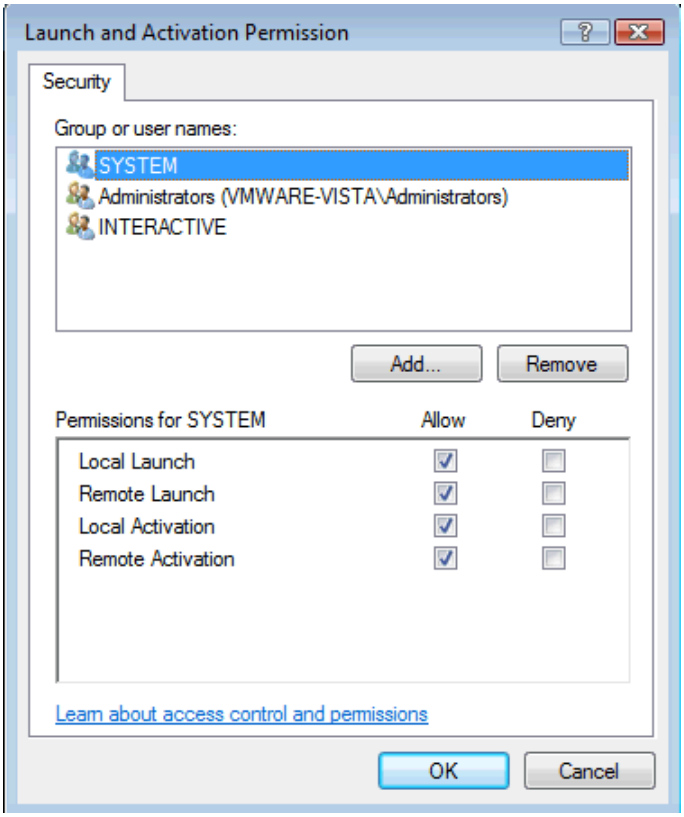


**Figure 22: DCOM Launch and Activation Permissions by Group and Account**

To add new users or groups, follow the instructions below.

1. Click **Add**.

   **Note:** The process of creating local user groups and accounts was described earlier. If on a domain, have the domain administrator create a user group with all of the accounts that will need DCOM security.

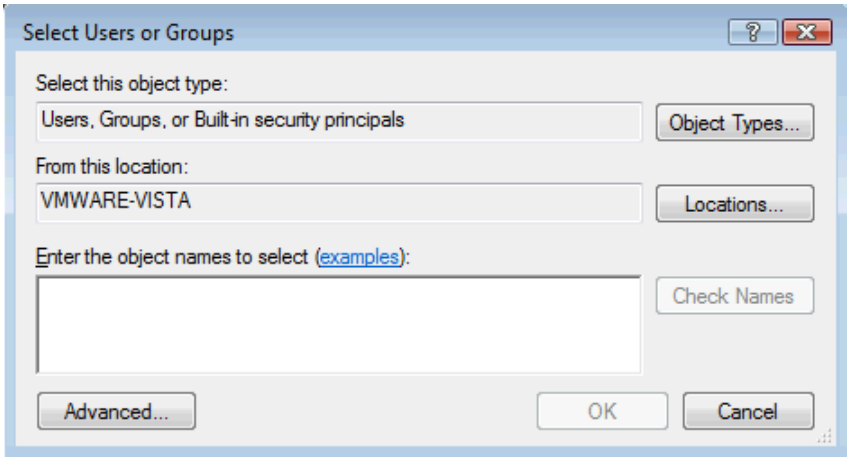


**Figure 23: User and Group Selection Dialog**

2. In **Enter the object names to select field**, specify the name of the Account or User Group name that will be added.

   **Note:** In this example, the name of the User Group created earlier has been entered.

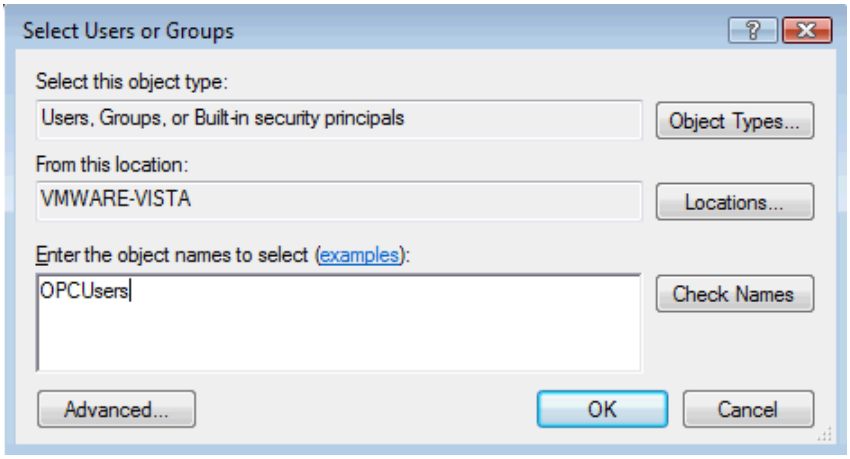


**Figure 24: User and Group Selection Dialog With Selected Group**

3. Next, click **Check Names** in order to validate the group or account that has been entered.
4. After the account has been validated, click **OK**.
5. Repeat Steps 1-4 until all the desired groups or accounts that permissions will be assigned to have been added.

   **Note:** If unsure of the accounts that should be added, click on **Advanced**. Then, select **Find Now** and all of the local group accounts in a work group (or if on a domain, all the domain accounts and groups) should be visible.

6. The new account or group should be visible in the **Group or user names** list.

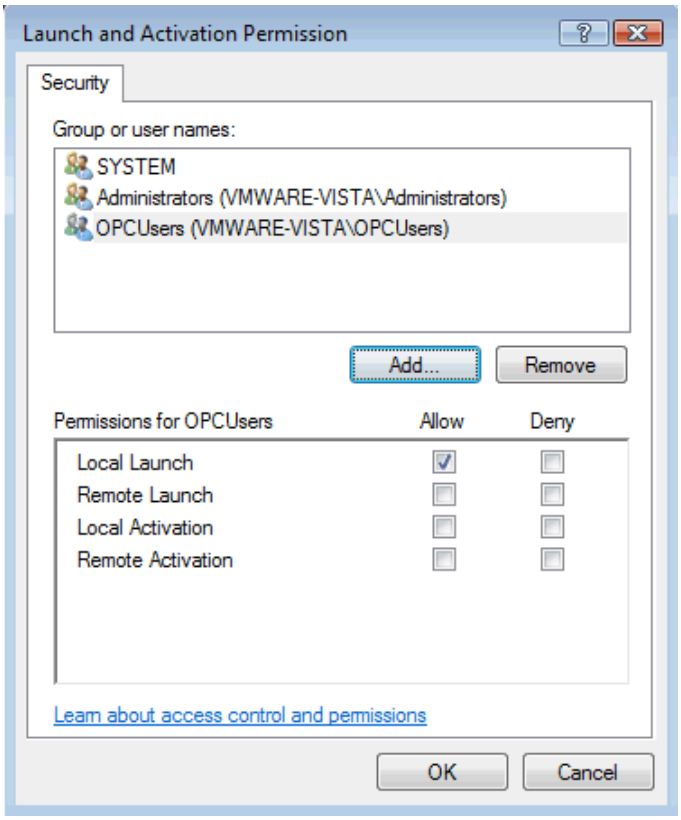


**Figure 25: Group or User Account Permissions Settings**

7. Next, select the new group or account.

   **Note: O**nly Local Launch permissions are enabled for it by default.

8. To allow local applications only to connect, then only enable the local permissions for the account. In this example, we want both local and remote connections; thus, we check all boxes.

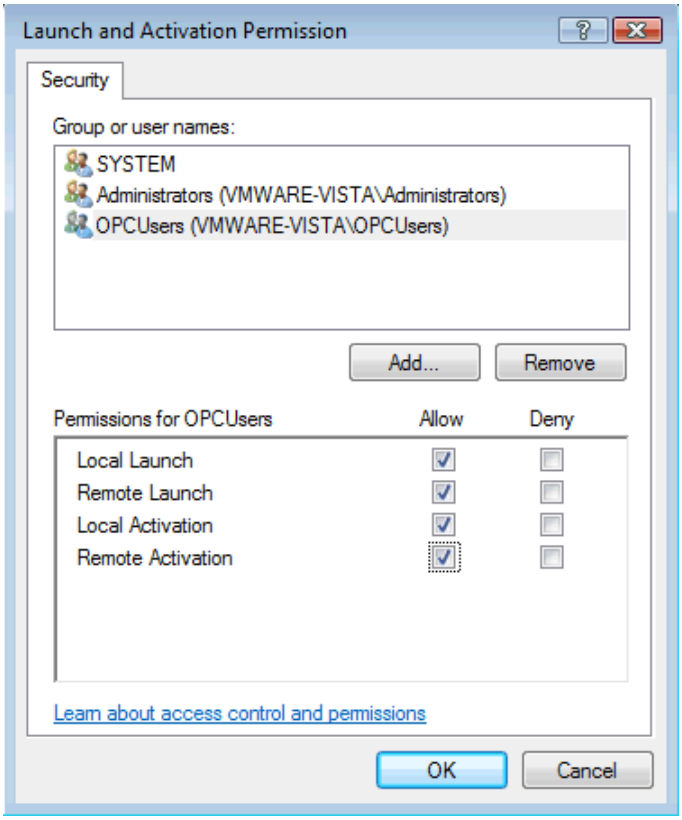


**Figure 26: Completed Group or User Account Permissions Settings**

9. Repeat the process for all accounts that have been added. Then, click **OK**.

### 6.3.1 Access Permissions

The Access Permissions window opens to default settings. Since we are making the Application DCOM Secure, we only want certain accounts to work with the application. For Kepware products, applications running under the System Account (and local Administrators) must always have permissions. Leave them as they are and remove the Interactive Account.

To set Access Permissions, follow the instructions below.

a. Click **Customize** to set local permissions.

b. Click **Edit** to set permissions for users.

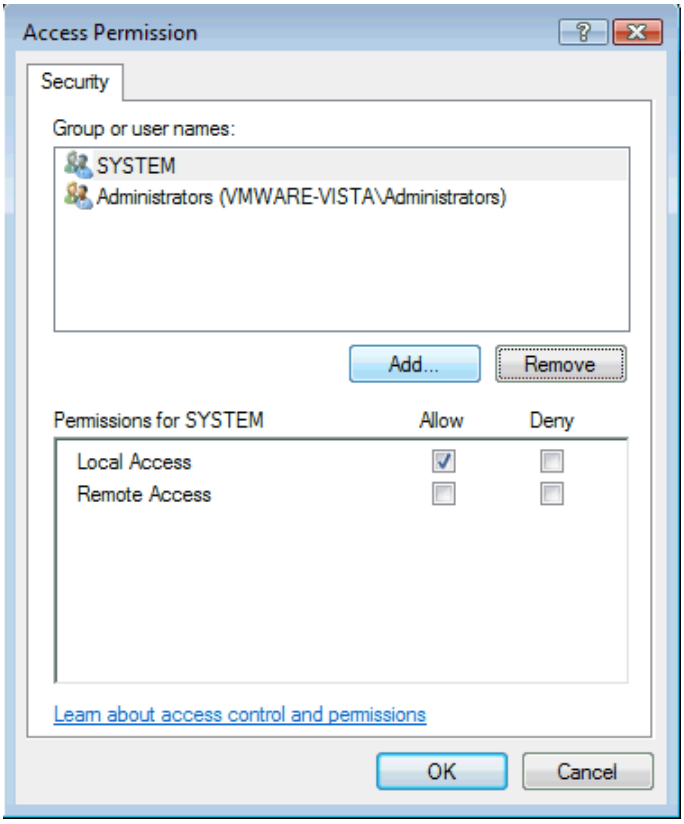


**Figure 27: DCOM Access Permissions Dialog**

1. Repeat the previous steps to add and enable Access permissions for all desired accounts and groups.
2. When finished, click **OK**.

**Note:** For a list of the groups and accounts that should always be used, refer to Required Accounts and Groups for OPC.

3. Return to the Security tab and then click **Apply** to set all of the selected permissions settings.

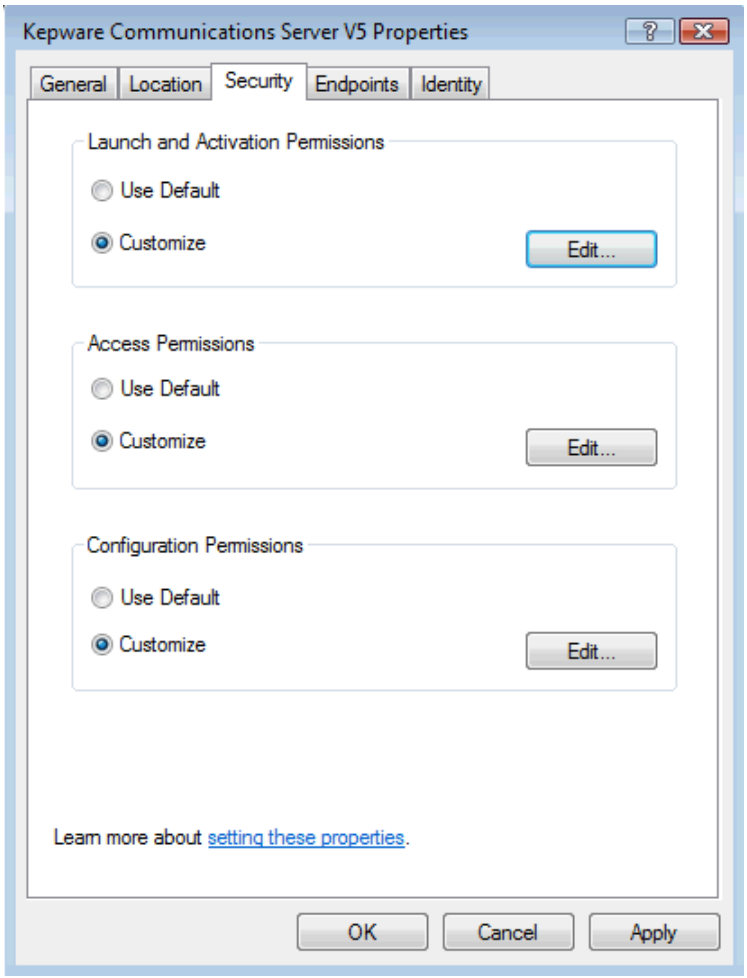


**Figure 28: Application DCOM Security Property Page**

4. Close the application's **Properties** by clicking **OK**.

   **Note:** DCOM Security has now been set for this application. The process will need to be repeated for other applications that require Secure DCOM Security.

## 6.4 Setting DCOM Security Open for All Applications

Some end users do not want to manage Secure DCOM Settings and would rather open OPC DCOM Security wide. For more information on how this is completed, refer to the instructions below.

### *6.4.1 Starting the DCOM Configuration Utility*

To launch DCOM Configuration, perform one of the following tasks.

1. For KEPServerEX or LinkMaster click on the Launch **DCOM Configuration** icon .
2. In the server, click **Tools** | **Launch DCOM Configuration**.
3. From the **Start** menu, type **DCOMcnfg.exe** in the run command and then click **OK**.

**Note:** Alternatively, open the **Control Panel** from the **Start** Menu and then double-click on **Administrative Tools**. Then, click on **Component Services**.

4. Double-click on **Component Services** and then select the **Computers** folder.
5. Expand the folder and locate **My Computer**.

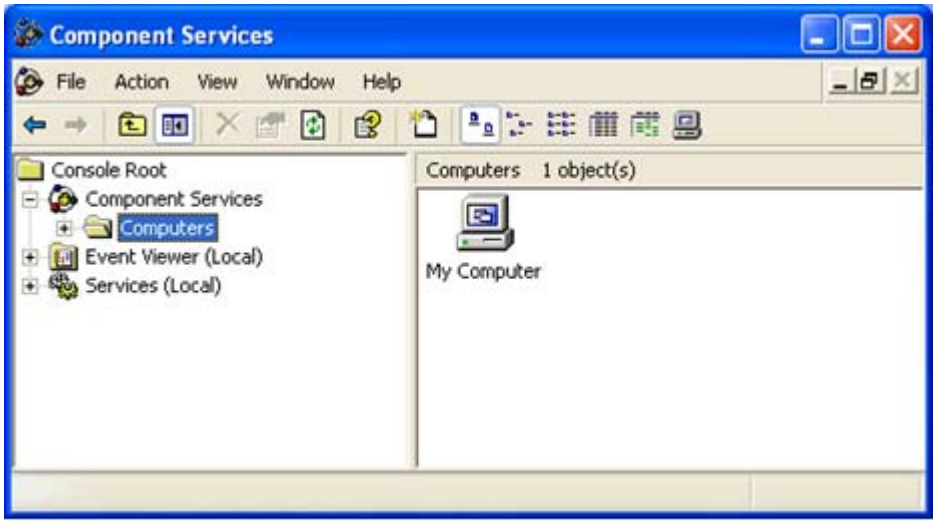


**Figure 29: Global DCOM Settings for Local Computer**

## 6.4.2 Opening the Computer's Properties

My Computer Properties will open to the General Tab.

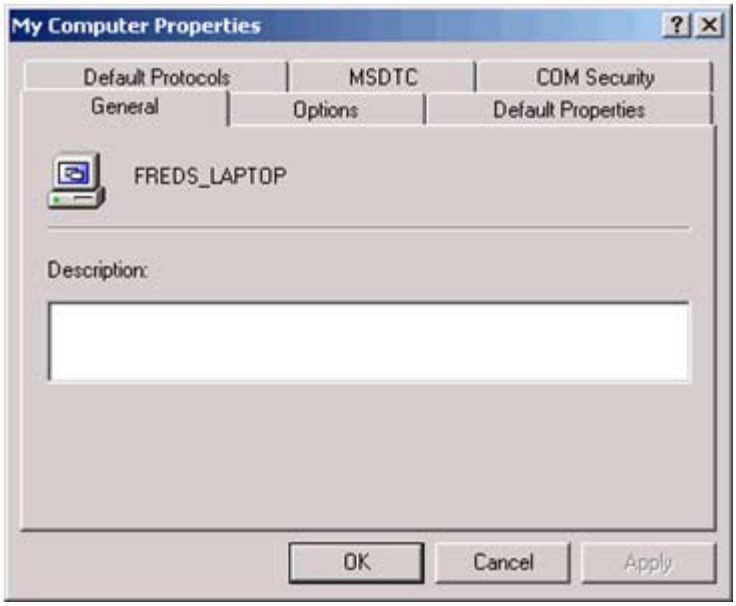


**Figure 30: My Computer Properties – General Tab**

**Note:** Click on the Default Properties tab.

### 6.4.3 The Computer's Default COM Properties

The Default COM Properties dialog is used to enable or disable DCOM for the PC. The PC's Default Authentication Level for COM and DCOM can also be specified in this dialog.

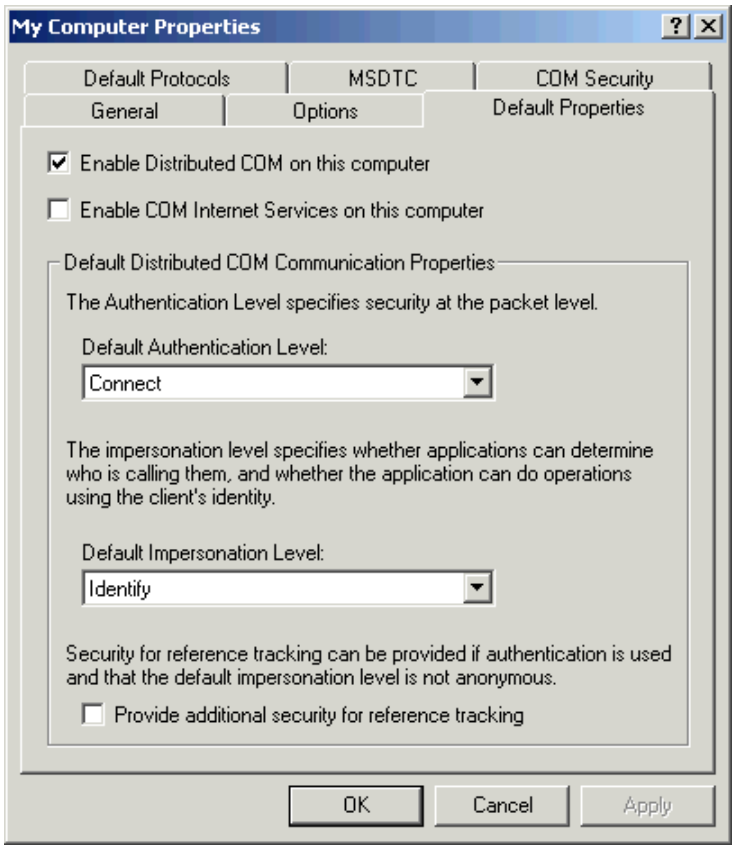


**Figure 31: My Computer Properties – Default COM Properties Tab**

1. Check **Enable Distributed COM**.
2. Leave the **Authentication** and **Impersonation** levels at the defaults.
3. Then, click on the **COM Security** tab.

### 6.4.4 The Computer's COM Security

Set the Default COM security for the computer in the COM Security dialog. The following steps demonstrate the order in which Security should be opened for the computer.

**Note:** Each Permissions section has a **Default** and a **Limits Edit** button. These are used to enable user groups and then limit permissions for certain users in those groups. Since this is setting DCOM permissions for the entire computer, ensure that all the users can access the applications.

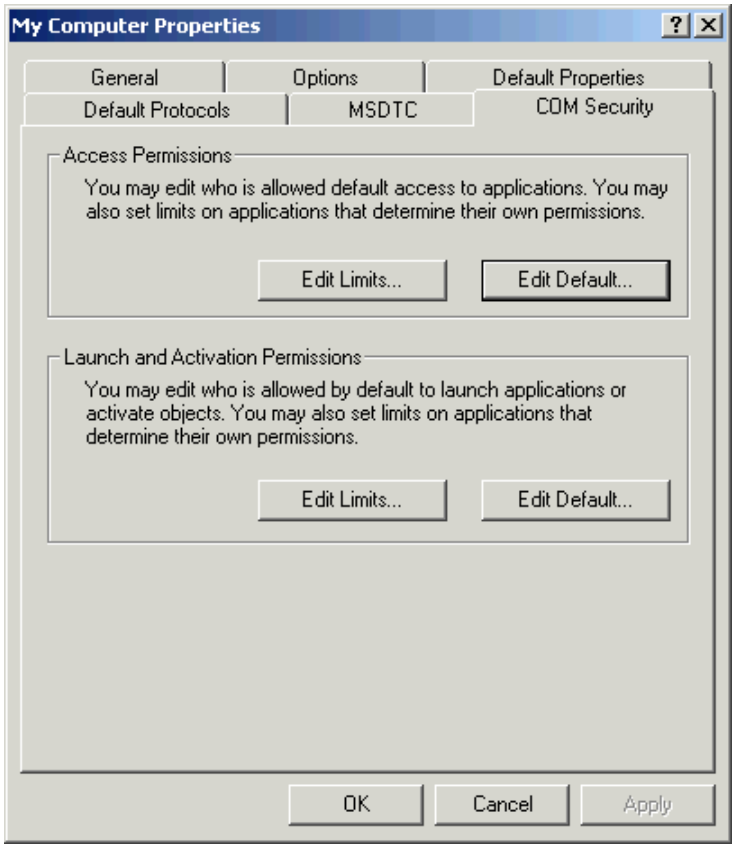


**Figure 32: My Computer Properties – Default COM Security Tab**

## 6.5 Access Permissions

To open the Access Permissions dialog, click **Edit Defaults** | **Access Permissions**. Once open, several accounts and groups that were already added should be visible.

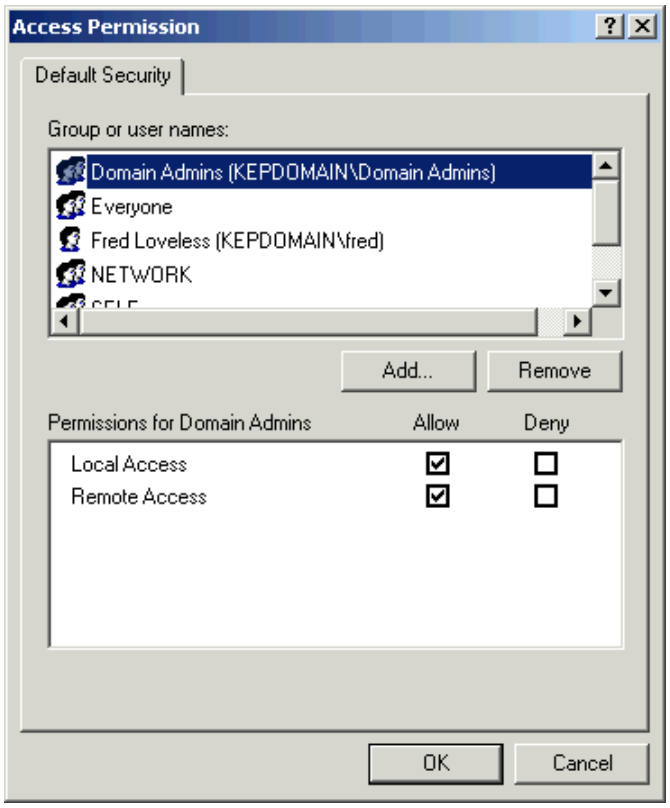


**Figure 33: My Computer Properties – Global DCOM Access Permissions**

1. To add a new group or account, click **Add**.
2. The **Select Users, Computers, or Groups** window will be invoked.

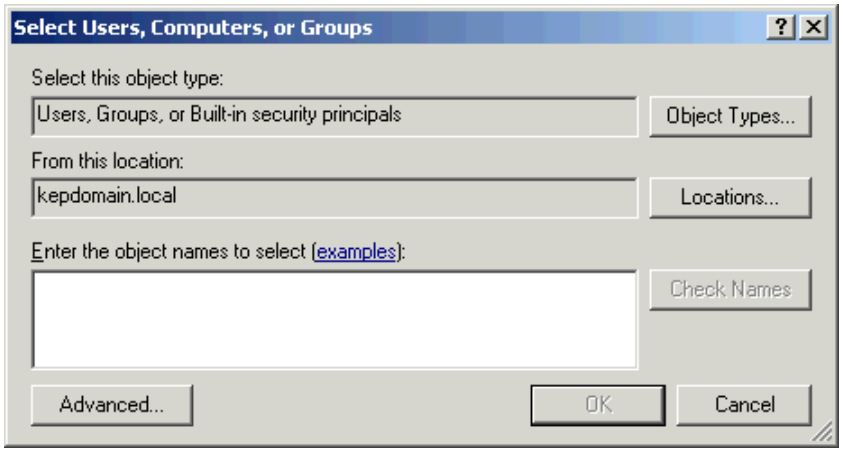


**Figure 34: User Account and Group Selection Dialog**

3. Browse the available users list in order to locate the groups or accounts that will be added.

4. Next, click **Advanced** and then click **Find Now**.

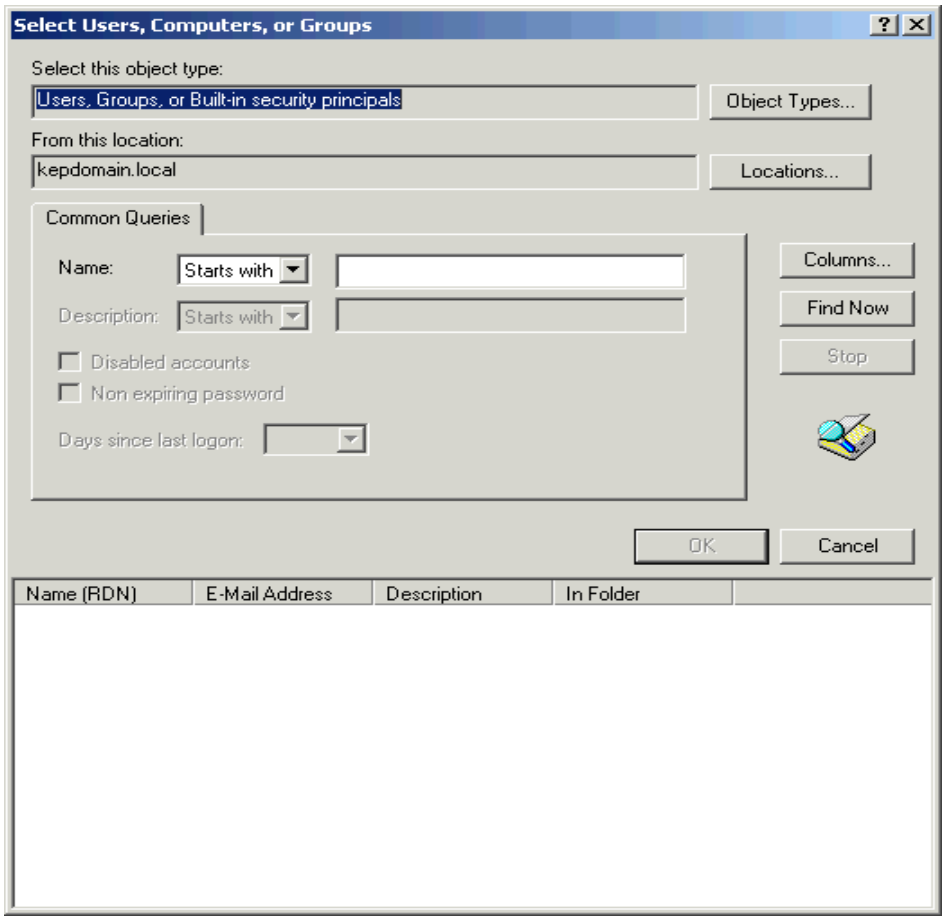


**Figure 35: User Account and Group Selection Dialog - Advanced**

5. If on a Domain, a list of all the domain groups and accounts should be visible. For a work group PC, a list of the Local Groups and Accounts should be visible.

   **Note:** If you have a Workgroup PC and are using an Account Login that has been granted access rights to the domain, the domain can be browsed in the Advanced window.

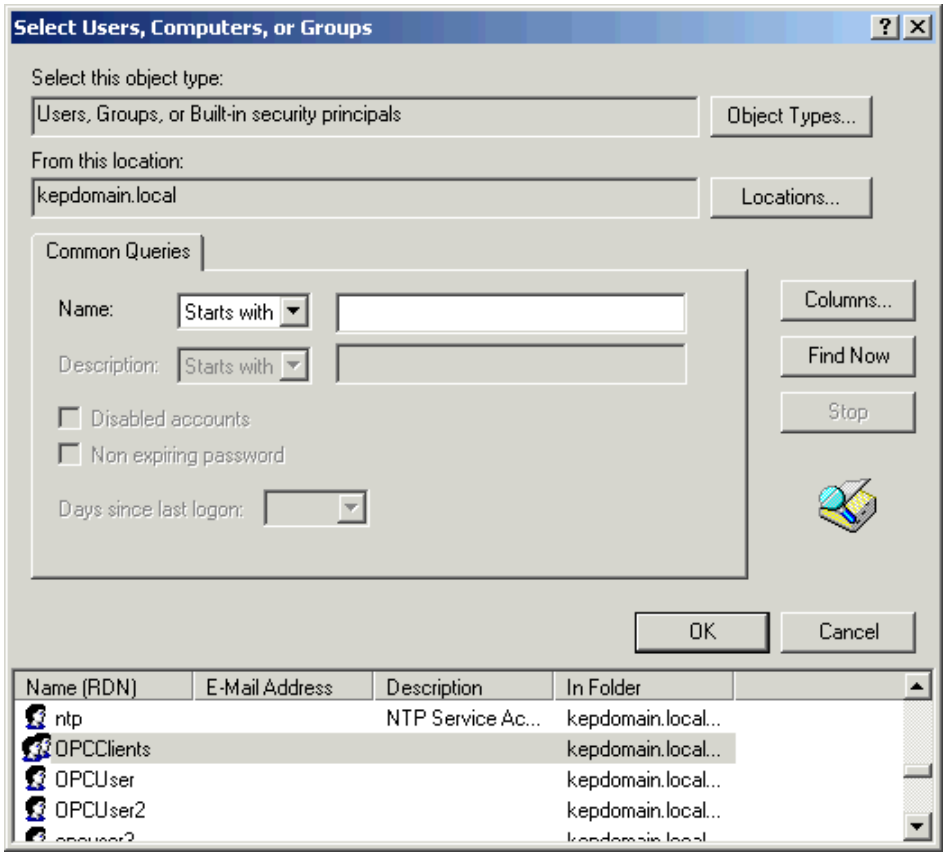


**Figure 36: User Account and Group Selection Dialog – Found Accounts**

6. Next, select the accounts and groups that permissions will be given to and then click **OK**.

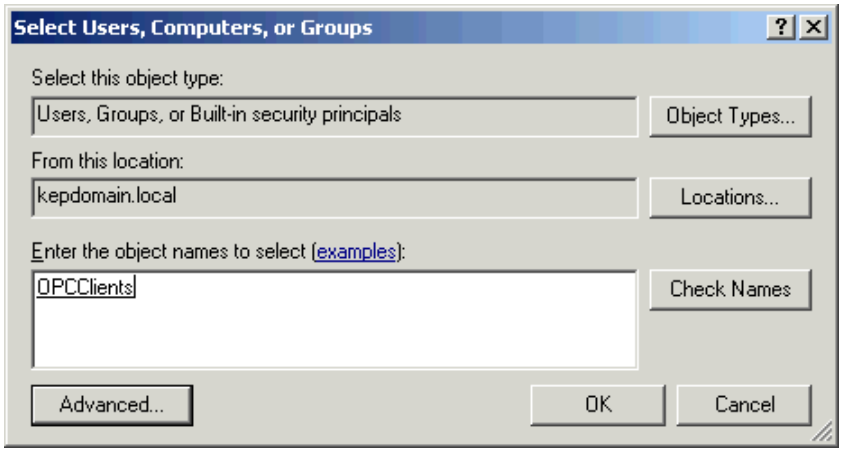


**Figure 37: User Account and Group Selection Dialog – Selected Group**

7. Verify that all the desired accounts have been selected and then click **OK**.


**Figure 38: Global DCOM Access Permissions by Account or Group**

8. Select an added account or group.

   **Note:** When new groups and accounts are added, only Local Permissions are enabled by default.

9. Click **Remote Access** to enable Remote Connectivity.

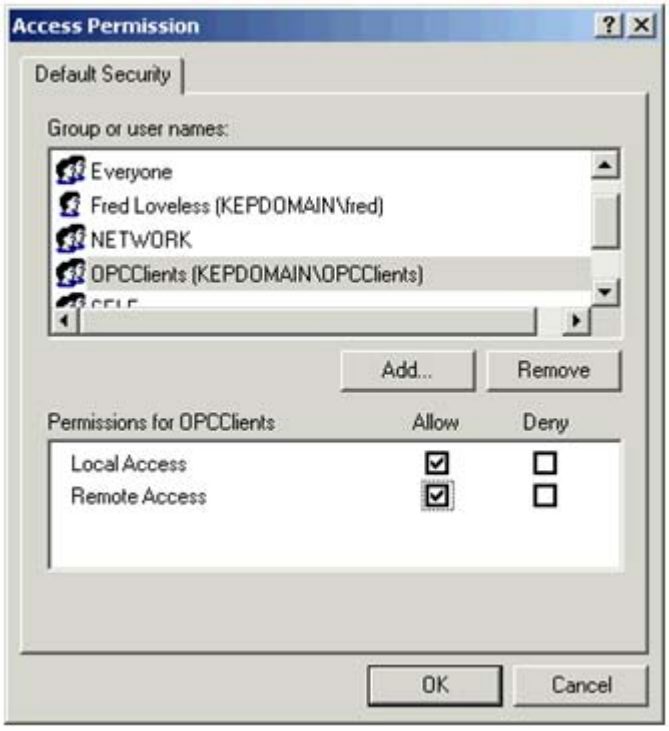


**Figure 39: Completed Global DCOM Access Permissions**

10. Repeat the process until permission has been assigned to all of the groups and accounts that were previously added.
11. To close the Default Access Permission window, click **OK**.

**Note:** Click the Access Permissions Edit Limits button.

### 6.5.1 Access Permission Limits

Now that DCOM security is enabled, you can limit what users can and cannot do. This works the same way as setting the permissions, except that the permissions are being accepted or denied as required by IT or Plant Mangement.

**Note:** All accounts are allowed unless otherwise specified using the Limit parameter.

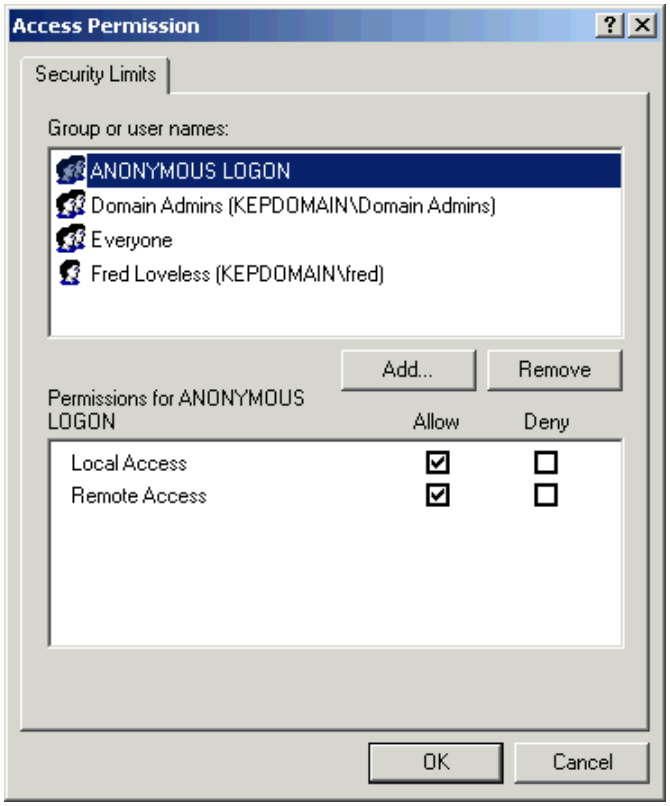


**Figure 40: Global DCOM Access Permission Limits by Account or Group**

1. Add or remove accounts to the **Edit Limits** list in the same manner as when setting permissions.
2. Select each account or group and click to allow or deny permissions.
3. To close, click **OK**.
4. For Launch and Activation Permissions, click **Edit**.

### 6.5.2 Launch and Activation Permissions

When the Access Permissions dialog opens, several Accounts and Groups that were already added should be visible.

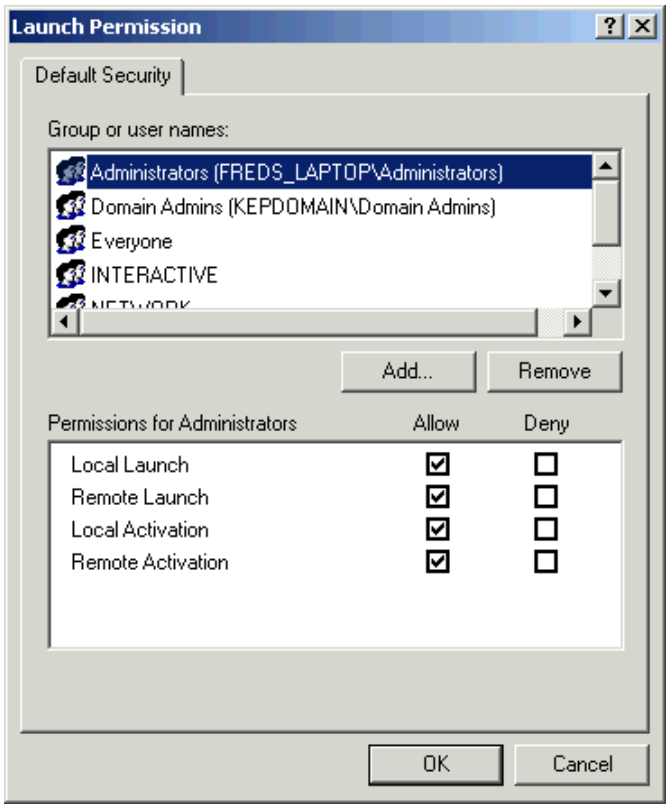


**Figure 41: My Computer Properties - Global DCOM Launch and Activation Permissions**

1. To add a new group or account, click **Add**.
2. Repeat the previous steps to add new groups and accounts.

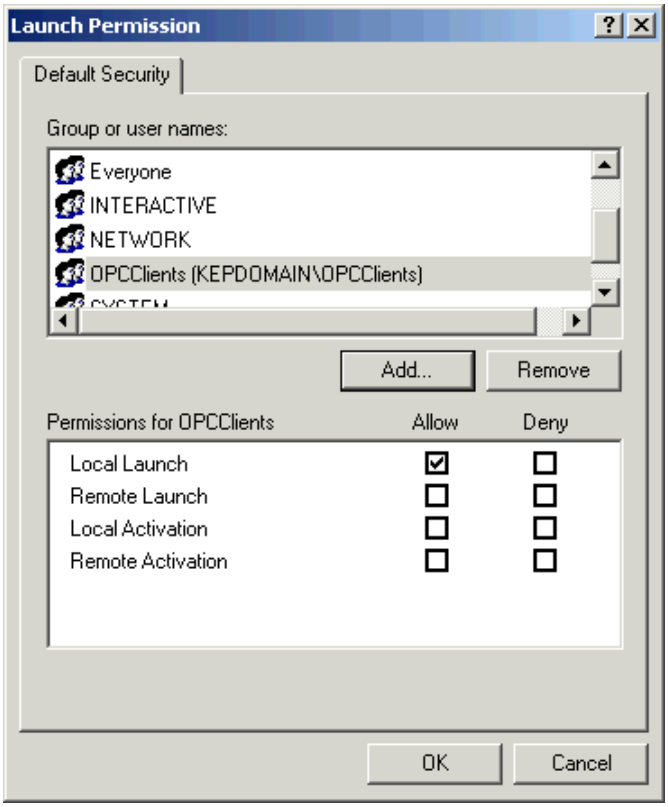


**Figure 42: Global DCOM Launch and Activation Permissions by Account or Group**

3. Select an Account or Group.

**Note:** When new groups or accounts are added, only Local Permissions are enabled by default.

4. Click **Remote Launch and/or Activate** to allow remote launch or activate for this account or group.

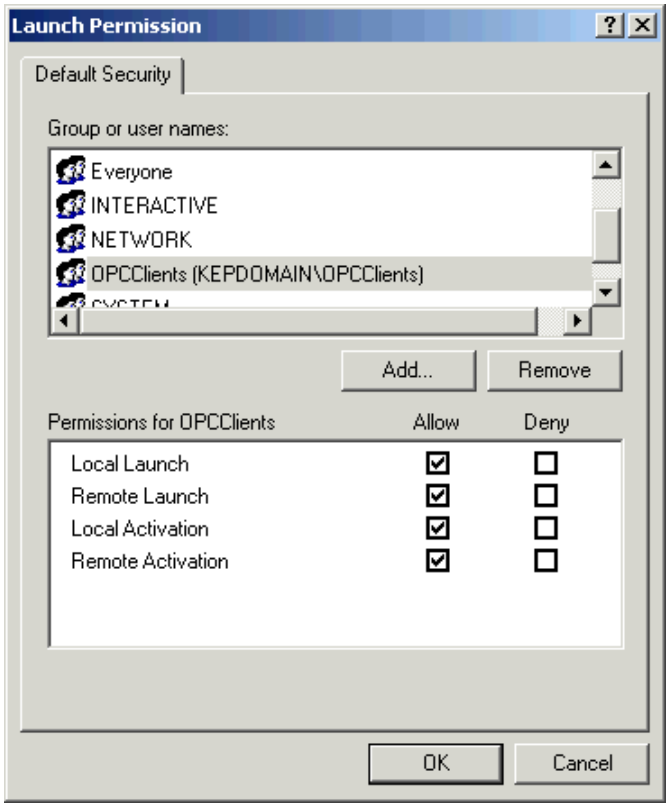


**Figure 43: Completed Global DCOM Launch and Activation Permissions**

5. Repeat the process until permission has been assigned to all of the groups and accounts.
6. To close the Default Launch and Activation Permission window, click **OK**.

**Note:** Next, click the Launch and Activation Permissions Edit Limits button.

### 6.5.3 Launch and Activation Permission Limits

Now that DCOM security, you now have the Option to limit what users can and cannot do. This works the same way as setting the permissions did except that you are allowing and denying those permissions as required.

**Note:** By default, all accounts are allowed unless otherwise specified with the Limits settings.

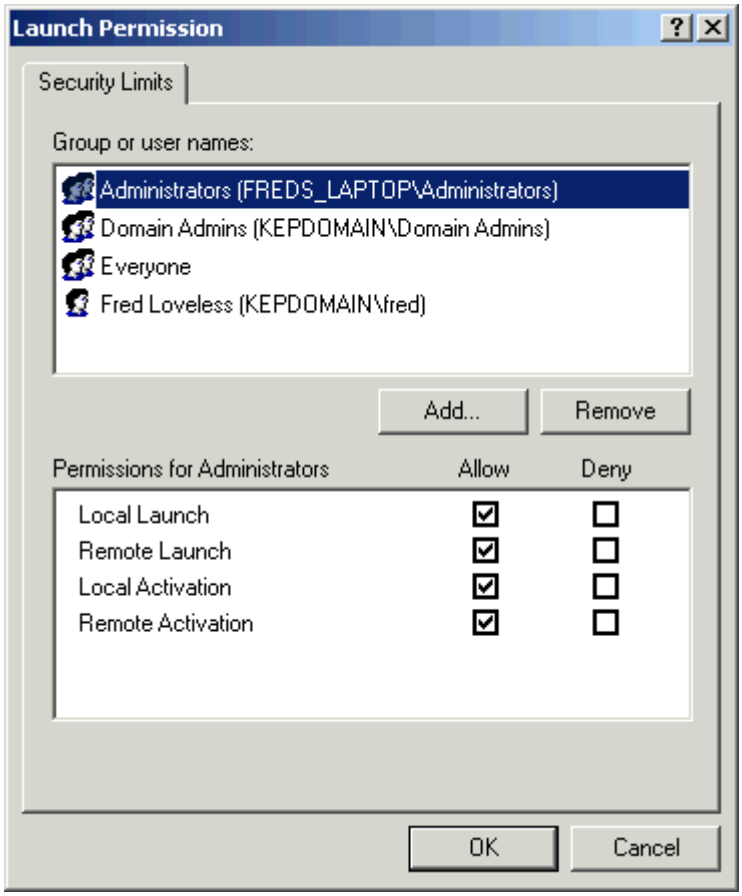


**Figure 44: Global DCOM Launch and Activation Permission Limits**

7. Add or remove accounts to the Edit Limits list as you did when setting permissions.
8. Select each Account or Group and click to allow our deny permissions for it.
9. Click OK to close.

**Note:** For a list of the groups and accounts that should always be used, refer to "**Required Accounts and Groups for OPC**."

10. Click **Apply** to set all of the newly configured COM Security settings.

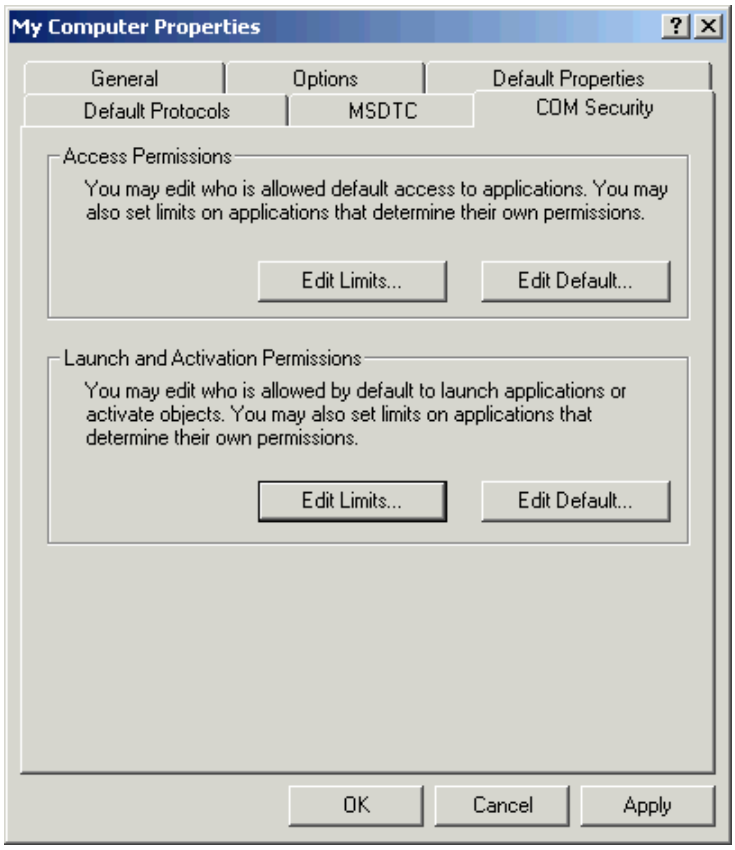


**Figure 45: My Computer Properties – COM Security**

11. To close the **My Computer** properties window, click **OK**.

# 7. Local Security Policies

In order for DCOM to work properly, some of the Local Security Polices will need to be addressed. In managed networks, you will most likely need a Network or IT administrator set the policy settings.

## 7.1 Opening the Local Security Policies Console

For information on accessing the Local Security Policy Console, follow the instructions below.

1. In the **Start** menu, open the **Control Panel**. Then, double-click on **Administrative Tools**.

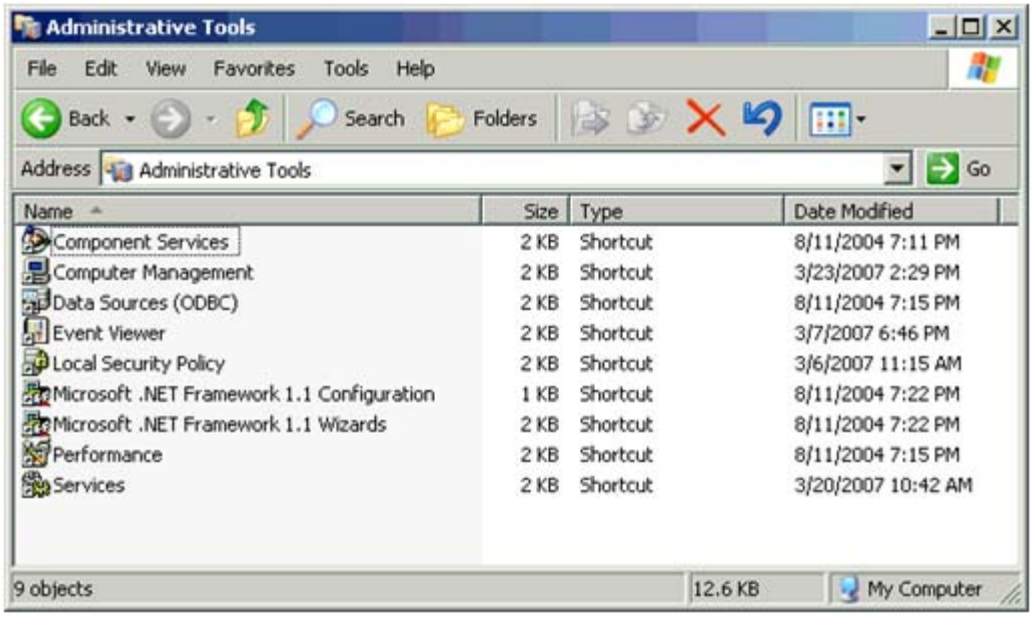


**Figure 46: Local Computer Administrative Tools**

2. Next, double-click on **Local Security Policy**. This will invoke the Microsoft Management Console for Security Settings.
3. Expand the **Local Polices** folder.
4. Select **Security Options**.

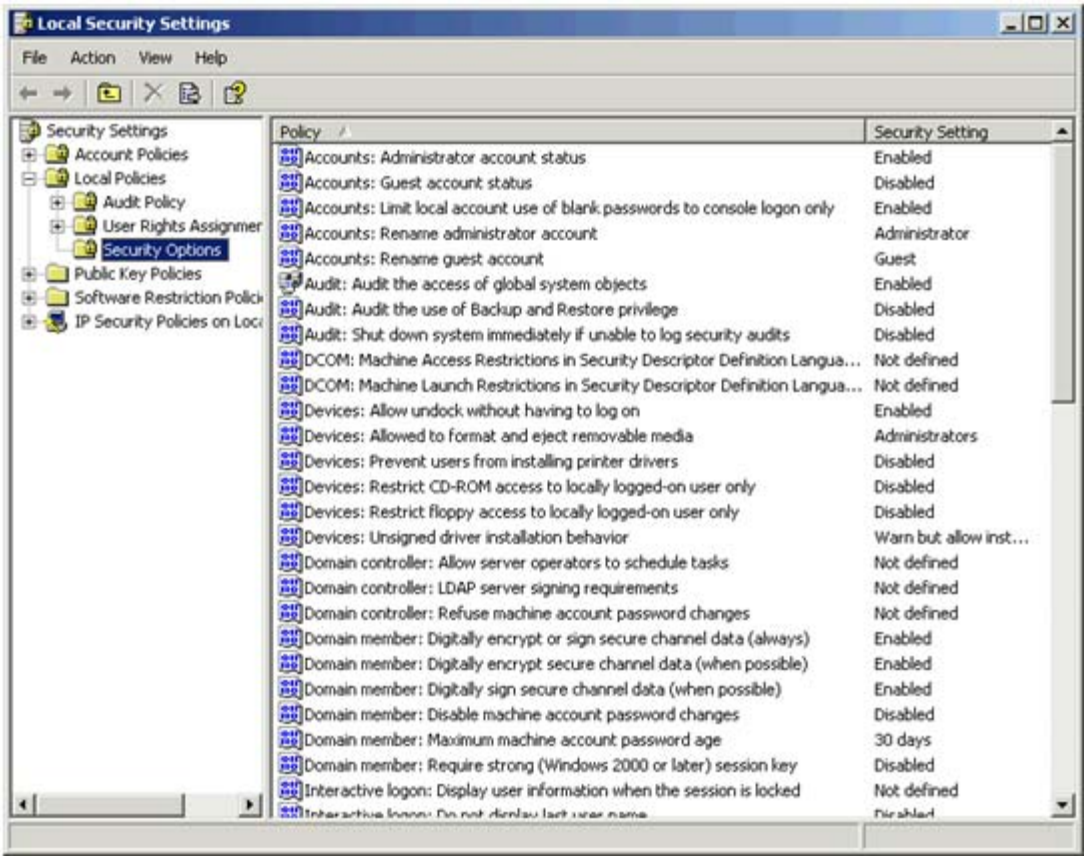


**Figure 47: Local Security Settings**

## 7.2 Everyone Permissions for Anonymous Users

This security setting determines what additional permissions are granted to anonymous users when on the computer.

1. Scroll down the Security options list until "**Network access: Let Everyone permissions apply to anonymous users**" is visible.
2. Next, double-click on it to open **Properties**.
3. This property is disabled by default. If setting up a secure system, this should not be enabled.

**Note 1:** Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. By default, the Everyone Security Identifier (SID) is removed from the token created for anonymous connections. Therefore, permissions granted to the Everyone group do not apply to anonymous users. If this option is set, anonymous users can only access those resources for which they have been given permission.

**Note 2:** If this policy is enabled, the Everyone SID is added to the token created for anonymous connections. In this case, anonymous users are able to access any resource for which the Everyone group has been given permissions.

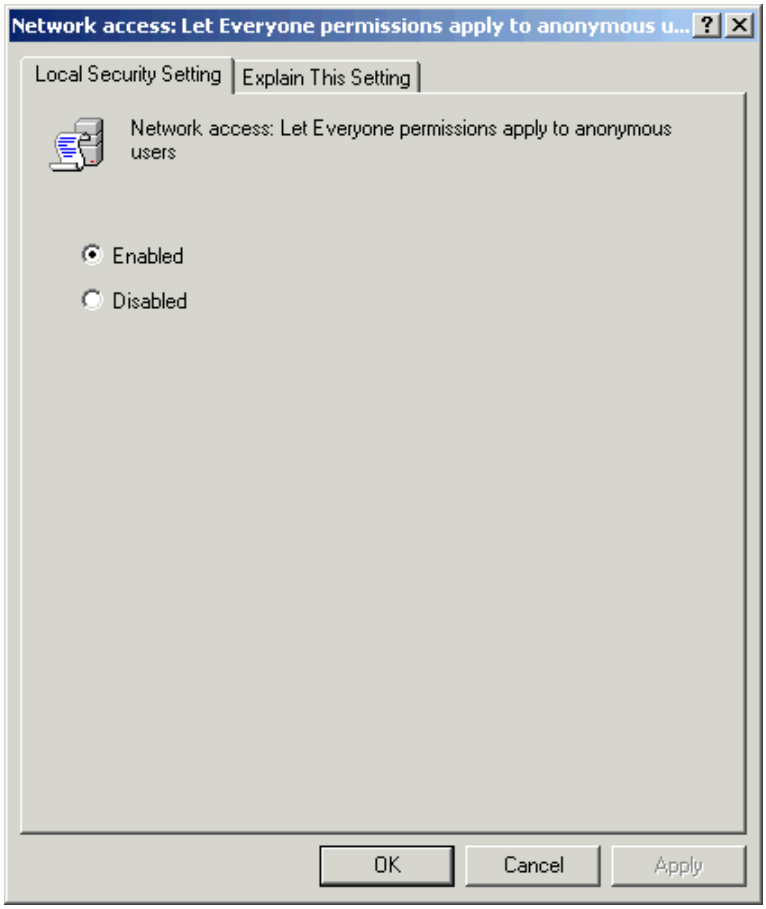


**Figure 48: Local Security Settings – Let Everyone Permission Apply to Anonymous Users - Enabled**

4. Check the setting that is required for this particular setup.
5. Click **OK**.

## 7.3 Sharing Model for Local Accounts

This next setting must be set regardless of which type of DCOM is being setup.

1. Scroll down the list until "**Network access: Sharing and security model for local accounts**" is visible.
2. Double-click on it to open **Properties**.
3. This setting is set to "**Local users authenticate as Guest**" by default. For safety reasons, the Guest account should always be disabled on any PC on the plant floor.

**Note 1:** This security setting determines how network logons that use Local accounts are authenticated. If this setting is set to **Classic**, the network logons that use local account credentials authenticate by using those credentials. If this setting is set to **Guest Only**, the network logons that use Local accounts are automatically mapped to the Guest account.

**Note 2:** The Classic and Guest Only models provide different levels of control over access to resources. By using the Classic model, different types of access can be granted to different users for the same resource. By using the Guest Only model, all users are treated equally. All users authenticate as Guest, and all receive the same level of access to a given resource (which can be either Read Only or Modifty).

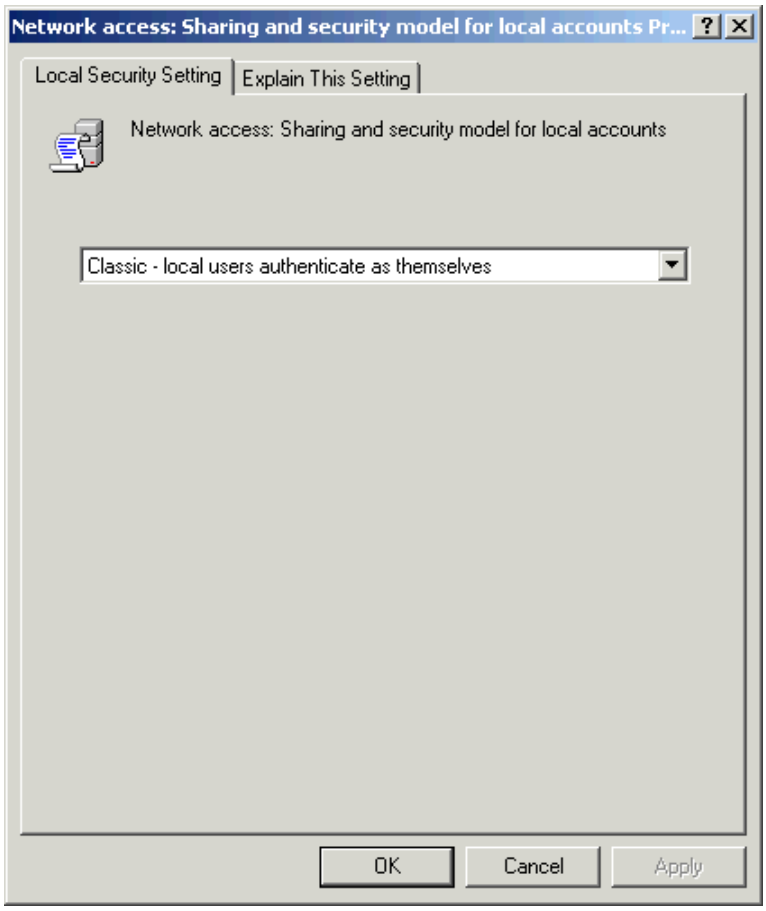


**Figure 49: Local Security Settings – Sharing and Security Model Set to Classic**

4. Next, select the "**Classic: Local users authenticate as themselves**" setting.
5. To close, click **OK**.

**Important:** With the Guest Only model, any user who can access the computer over the network (including anonymous internet users) can access the shared resources. Thus, to protect the computer from unauthorized access, use the Internet Connection Firewall (ICF) or another similar device. Similarly, when using the Classic model, local accounts must be password protected. Otherwise, those user accounts can be used by anyone in order to access shared system resources.

# 8. Firewalls

Firewall settings are the last that need to be considered. The example below will demonstrate what settings to use if the Windows Firewall is set. You will need to consider the same settings for 3rd party firewall software or for firewall hardware.

## 8.1 The Windows Firewall

1. To open the Windows Firewall, open the **Control Panel**.
2. Double-click on **Windows Firewall** in order to open the **Firewall Properties** window.

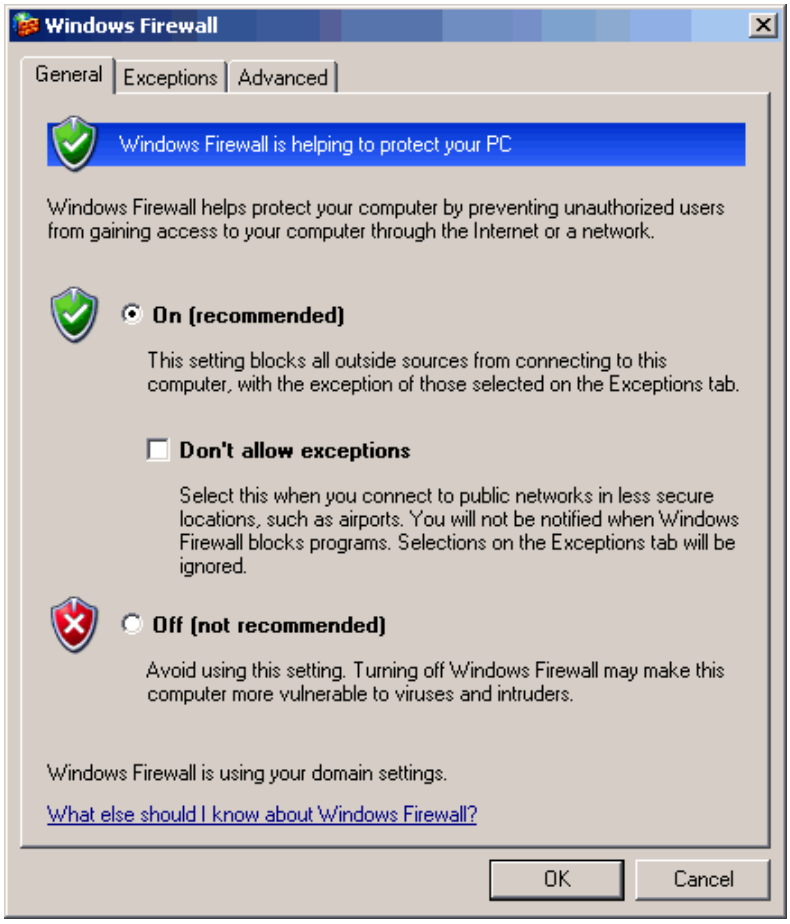


**Figure 50: Windows Firewall Settings - General Tab - Enabled**

1. If connections can be made to the outside world, make sure to turn the Firewall **On**.
2. If the network is protected from the outside world, the Firewall can be safely turned **Off**.

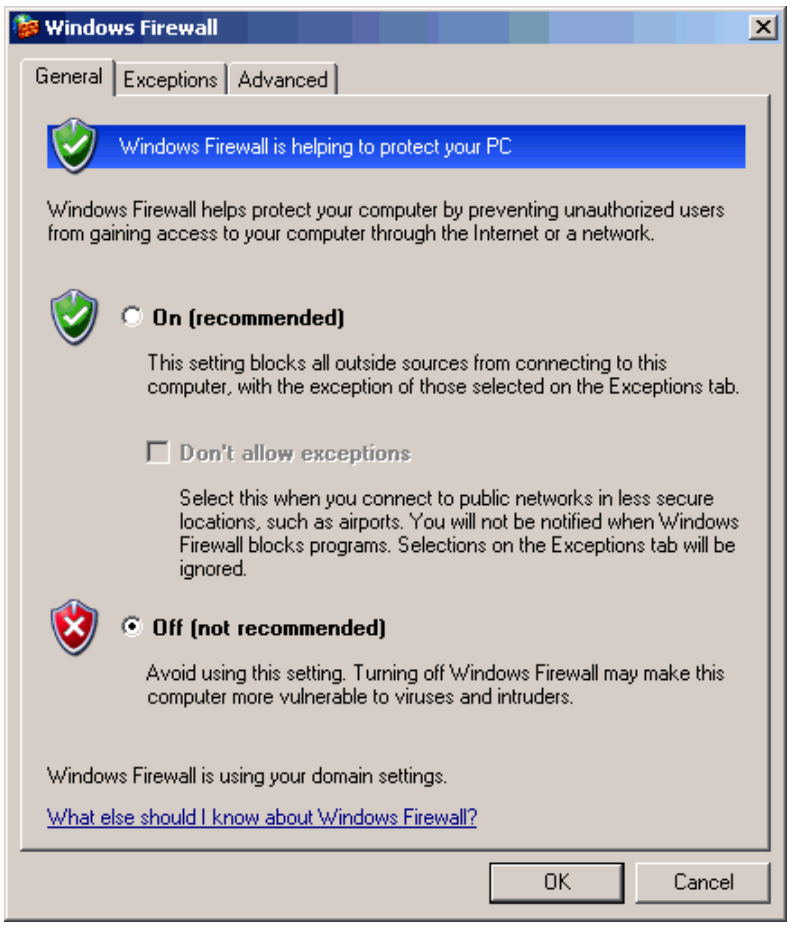


**Figure 51: Windows Firewall Settings - General Tab - Disabled**

3. If the Firewall is turned on, exceptions will need to be set in order to allow DCOM connections and application to connect through it.

## 8.2 Firewall Exceptions

4. To set exceptions, click on the **Exceptions** tab.

   **Note:** Exceptions set in the Firewall specify which applications can connect through it and what TCP and UDP Ports can pass traffic through it. Every application or port enabled is a potential hole in the security, however, and so use caution when setting exceptions.

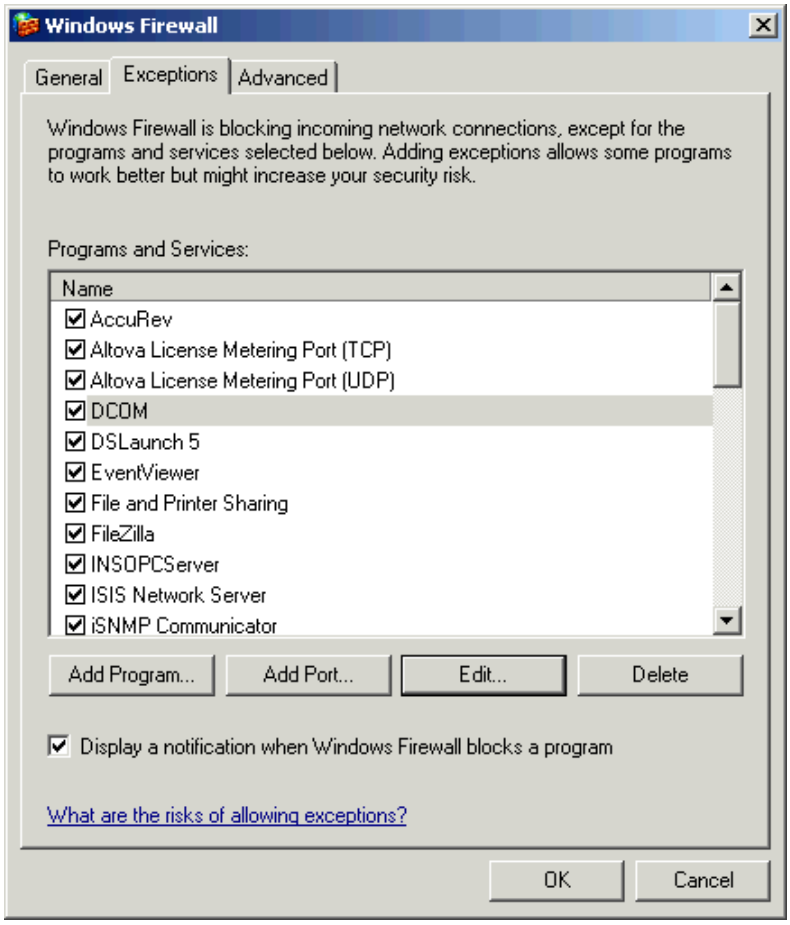


**Figure 52: Windows Firewall Settings – Exceptions Tag**

### 8.2.1 Adding a Program to the Exception List

To add a program to the Exception list, follow the instructions below.

1. Click **Add Program**.
2. Browse the PC's list of available programs.

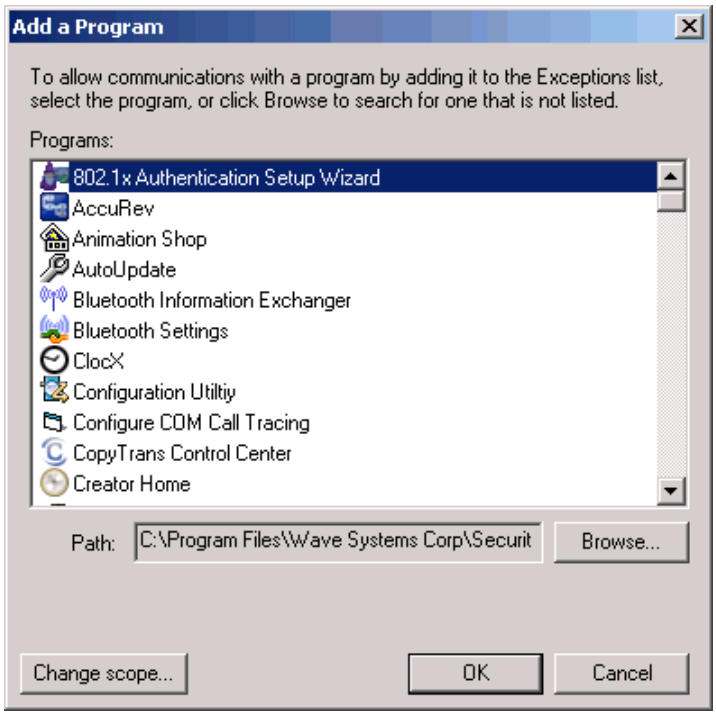


**Figure 53: Add Program List of Local Programs for Program Firewall Exceptions**

3. Once the desired program is located, click on it and then click **OK** to add it to the list.

### 8.2.2 Add a Port to the Exception List

To add a port to the Exception list, follow the instructions below.

1. Click **Add Port**.

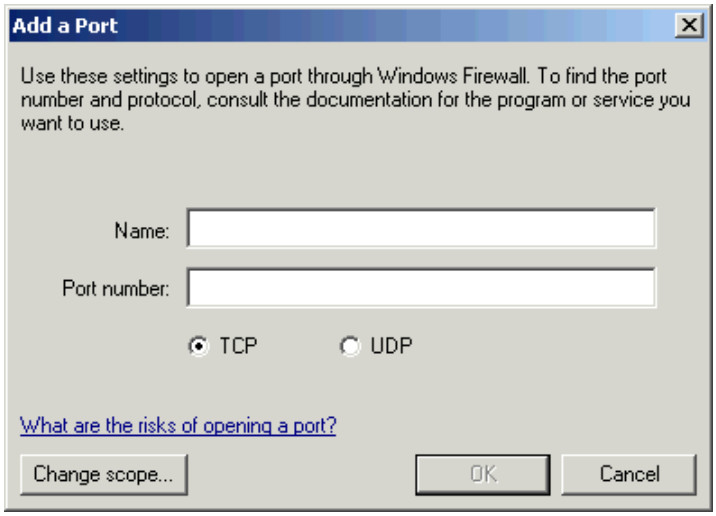


**Figure 54: Add TCP/UDP Port Firewall Exceptions**

2. In the **Add Port** dialog, specify the port's name.
3. Next, specify the **Port number**.
4. Specify whether it is a **TCP** or **UDP** port.

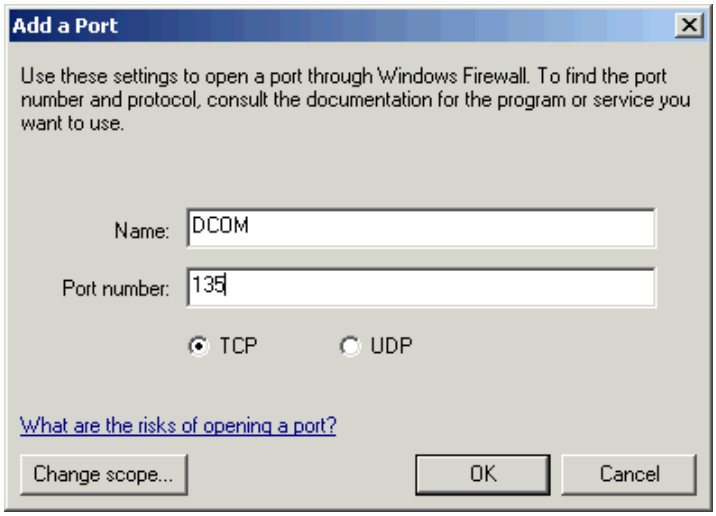


**Figure 55: Firewall Exception for DCOM**

5. In this example, DCOM Port 135 has been added.
6. Click **OK** to finish.

**Note:** Once a program or port has been added, it can be disabled again by simply unchecking it in the Exception list.

### 8.2.3 Kepware Programs and Ports for the Exception List

The table below displays the Kepware programs and ports that may need to be added to the Exception list.

| Programs | Ports |
|---|---|
| Servermain.exe - KEPServerEX 4.0 | TCP Port 135 DCOM<br>TCP Port 56233 - KEPServerEX 5.0 Event Log |
| OPCQuickClient.exe | TCP Port 32390 - KEPServerEX 5.0 Configuration Utility |
| LinkMaster.exe | |
| RedundancyMaster.exe | |
| Server_runtime.exe - KEPServerEX 5.0 | |
| OPCEnum.exe | |

**Table 4: Programs and Ports that Should Be Added to the Firewall Exception List**

# 9. Required Accounts and Groups for OPC

The table below displays the groups and accounts are usually required for OPC to work on Domains or Work Groups.

| Account or Group | Purpose |
|---|---|
| System | This is the default account that many applications running as a service will run under. OPCEnum.exr, which is used by all OPC applications to browse for and access applications on remote PCs, runs under this account. Whether using an open or secure setup, this account should have local and remote access, launch and activation permissions. |
| Local Administrator | Local access, launch and activation permissions should always be given to this account. |
| Everyone | This account/group is used in wide open DCOM to enable access for all users. |
| Network Users | This is used in Workgroups to aid remote users in connecting. |

**Table 5: Required Accounts and Groups for OPC**

# 10. Summary

You should now understand how to configure the Distributed Component Object Model (DCOM) for use with OPC clients and servers, as well as how to achieve security using DCOM Security. For questions regarding the OPC portion of this DCOM configuration project, contact Kepware Technical Support via e-mail at Technical.Support@kepware.com, via phone at 1-207-775-1660 x211 or via our Technical Support feedback form on www.kepware.com.