Configuration Guide

Remote OPC DA (DCOM)

July 2022
Ref. 3.13

Table of Contents

1. Overview 1
   - 1.1 What is DCOM? 1
   - 1.2 What is OPCEnum? 1
2. Users and Groups 1
   - 2.1 Domains and Workgroups 1
   - 2.2 Adding a Local User 2
   - 2.3 Adding a Local Group 2
   - 2.4 Adding Users to a Group 3
3. Server Runtime 4
   - 3.1 OPC Connection Security 4
   - 3.2 Setting the Identity When Running as a Service 4
4. DCOM Configuration 6
   - 4.1 Configuring the Application 6
   - 4.2 Configuring the System 10
   - 4.3 Applying Changes 13
5. Firewalls 14
   - 5.1 Server-Side Exceptions 14
   - 5.2 Client-Side Exceptions 16
6. Network Discovery (Optional) 18
7. Local Security Policies 19
   - 7.1 Server-Side Policies 19
   - 7.2 Client-Side Policies 20

1. Overview

This document provides information for setting up a secure DCOM connection between an OPC server and a client running on a supported Microsoft operating system.

1.1 What is DCOM?

Distributed Component Object Model (DCOM) is an extension of Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network, which in turn allows COM to communicate beyond the boundaries of the local machine.

- Because DCOM poses a security threat, care should be taken to expose only what is required for the application. Although multiple security layers exist, it is still possible that some part of the system can be compromised.

1.2 What is OPCEnum?

The OPC server stores OPC-specific information in the registry. Since OPC clients must be able to discover servers running on the same machine and remote machines, there needs to be a standard method for accessing this registry information (which is not available for remote access). To do so, a component called OPCEnum is provided by the OPC Foundation. OPCEnum is an executable typically installed on a computer with the OPC server. It runs as a system service and provides a means to browse the local machine for OPC servers and exposes the resulting list to the OPC client.

2. Users and Groups

To ensure that an OPC connection is secure, create users and groups exclusively for this use. These can be manually added by any user with the proper credentials.

2.1 Domains and Workgroups

When working within a workgroup, each user needs to be created locally on each computer involved in the connection. Furthermore, each user account must have the same password for authentication to occur. A blank password is not valid in most cases.

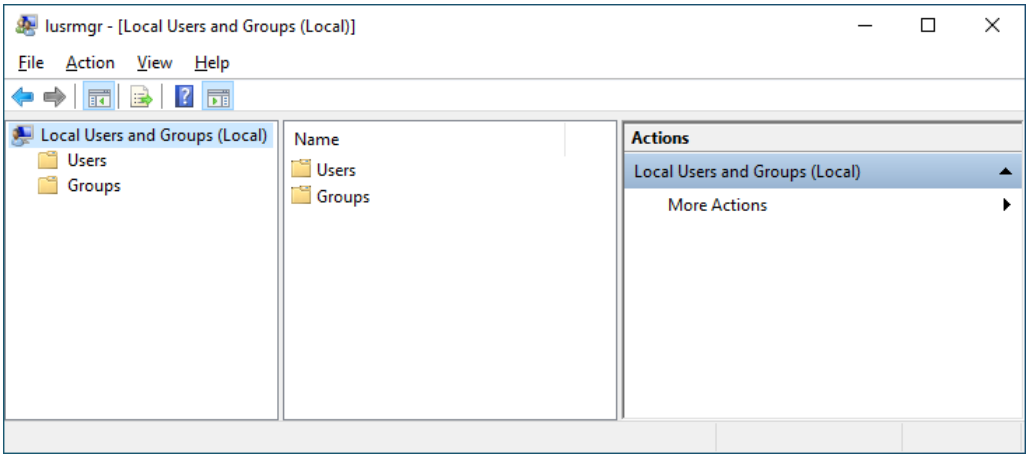
When working within a domain, local users and groups are not required to be added to each computer. If working within a domain is preferred, a network administrator may have to implement changes.

Mixing domains and workgroups requires both computers to authenticate with the lesser of the two options. As such, local user accounts must be added to the domain computer.

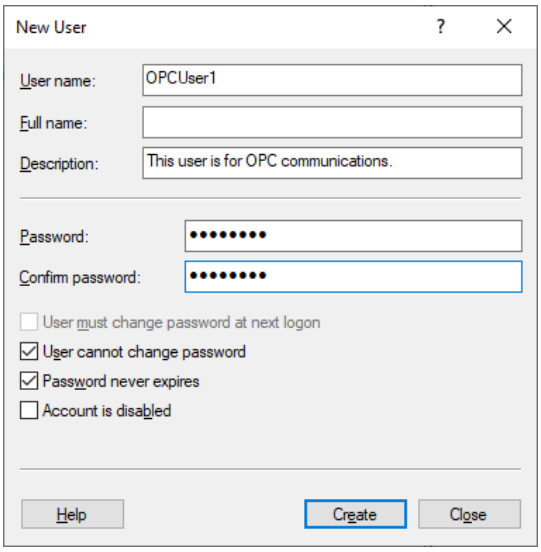
- **Note**: The client application must run as the authenticated user.

2.2 Adding a Local User

1. Launch Local User and Groups, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "lusrmgr.msc".



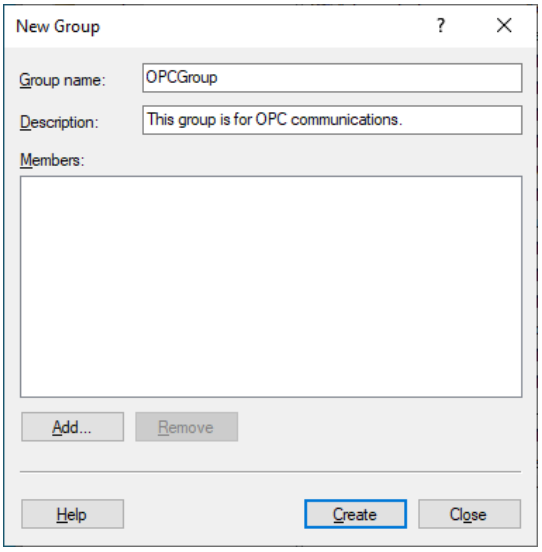
2. Click **Users**.
3. Select **Action | New User**.
4. Type the appropriate information in the dialog box.



5. Click **Create**.
6. Click **Close**.

2.3 Adding a Local Group

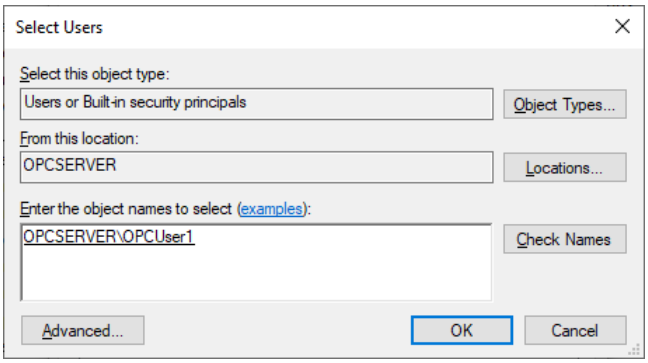
1. Launch Local User and Groups, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "lusrmgr.msc".
2. Click **Groups** and select **Action | New Group**.
3. In Group name, type a name for the new group.



4. In Description, type a phrase to identify the new group.
5. Click **Create**.
6. Click **Close**.

2.4 Adding Users to a Group

1. Launch Local User and Groups.
2. Select **Groups**.
3. Right-click on the new group and select **Add to Group**, then select **Add**.



4. In Object Types, select the types of objects to find.
5. In Locations, click the domain or the computer that contains the users to add.
6. Click **OK**.
7. Type the name of the user or group to be added to the group.
8. To validate the user or group names being added, click **Check Names**.
9. Click **OK**

3. Server Runtime

Before DCOM is configured on the server computer, the process mode should be chosen. *For more information on which process mode is appropriate for the specific application, refer to the server's help file*.

- **Caution**: Application-level DCOM settings are reset when the server's process mode is changed.

3.1 OPC Connection Security

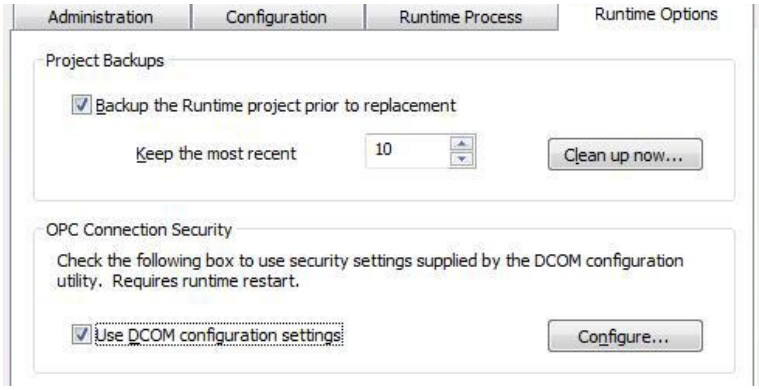
To provide the highest level of security, DCOM must be enabled in the Runtime. This option, which is enabled by default, ensures that DCOM settings are enforced and user authentication is performed.

- **Caution**: Disabling the option is not recommended and is not supported by Microsoft operating systems updated after June 2022.

1. Right-click on the Server Administration icon in the system tray.
2. Select **Settings**.

- **Tip**: If the Administration icon is not present, access it from the **Start** menu.

3. Select the **Runtime Options** tab.
4. Check **Use DCOM configuration settings** (if it is not already enabled).



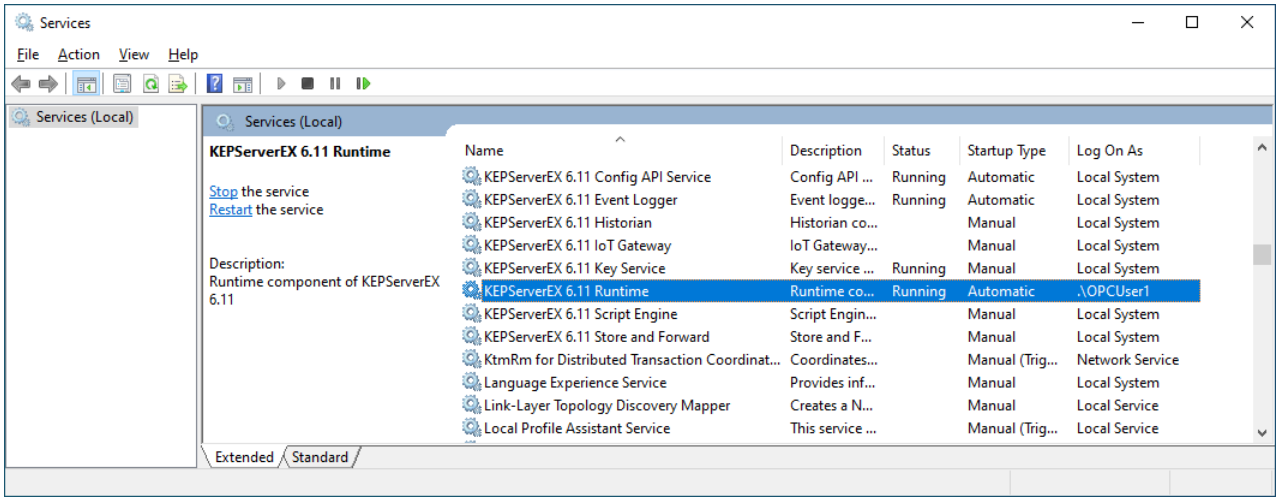
5. Click **OK**.

- **Tip**: If prompted to restart the Runtime, choose **Yes**.

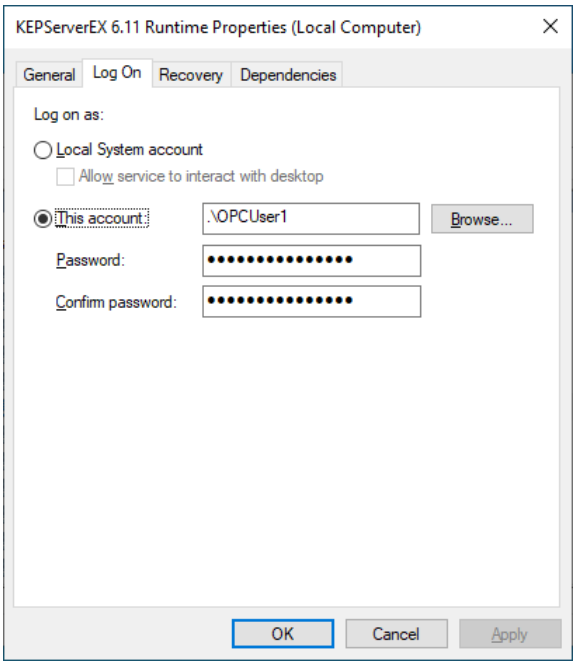
3.2 Setting the Identity When Running as a Service

When the OPC server's process mode is set to run as a service, the service must be set to run as a specific user so that the client can authenticate the callbacks sent from the server.

1. Launch Windows Services. To view it directly, select **Start | Run** and type "services.msc".
2. Locate the OPC server runtime and view **Properties**. In this example, "KEPServerEX Runtime" is displayed, but this can apply to other OPC servers.



3. In the Properties dialog, select the **Log On** tab.
4. Click the **This account** radio button.



5. Enter the username or click **Browse** to launch the Select User dialog to assist in selecting a valid username.

Note: The specified user must be part of the Administrators group.

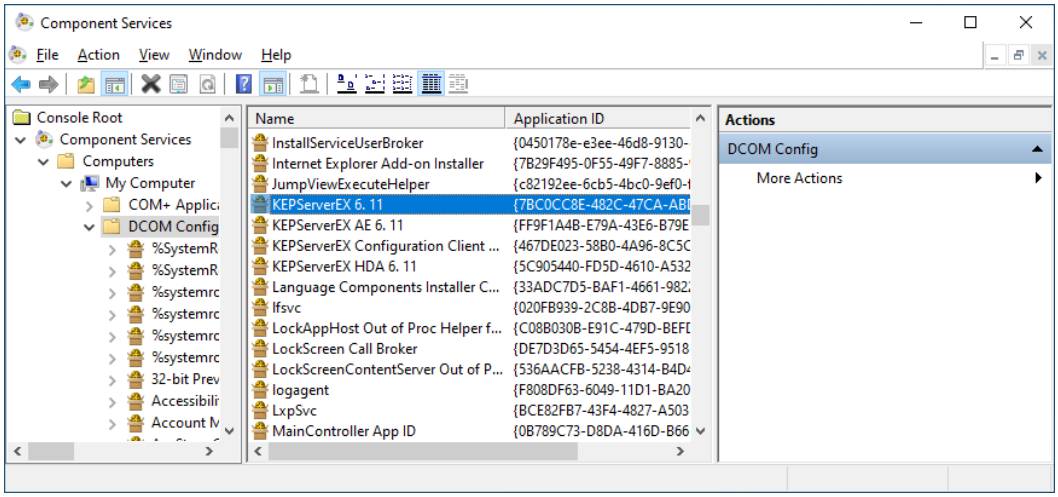
6. Enter and confirm the password of the user chosen to run the server application.
7. Click **OK** to return to Services.
8. Restart the OPC server service to apply changes.

4. DCOM Configuration

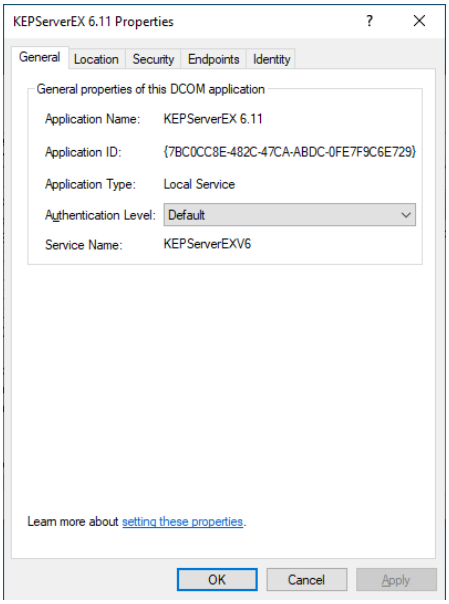
The computer running the OPC server requires changes to the application and system levels to setup DCOM correctly.

4.1 Configuring the Application

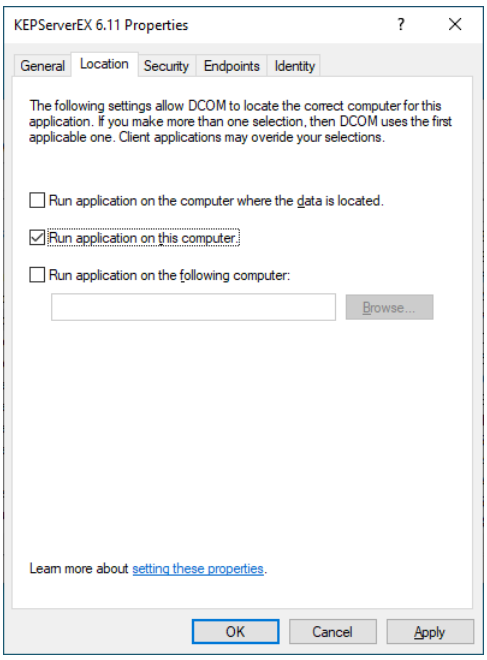
1. Launch Component Services, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "dcomcnfg".
2. Under Console Root, expand Component Services, Computers, My Computer, and DCOM Config.
3. Browse the DCOM-enabled objects until the OPC server application is located. In this example, “KEPServerEX” is displayed, but this can apply to other OPC servers.



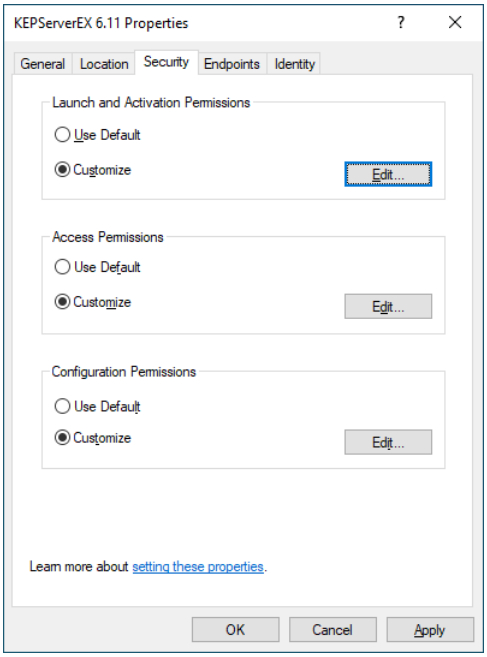
4. Right-click on the server application and select **Properties....**
5. View the **General** tab.
6. Verify that the Authentication Level is set to **Default**.



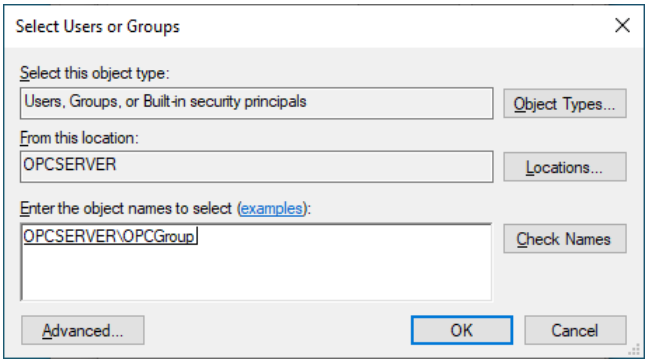
7. View the **Location** tab.
8. Verify that only the **Run application on this computer** option is enabled.



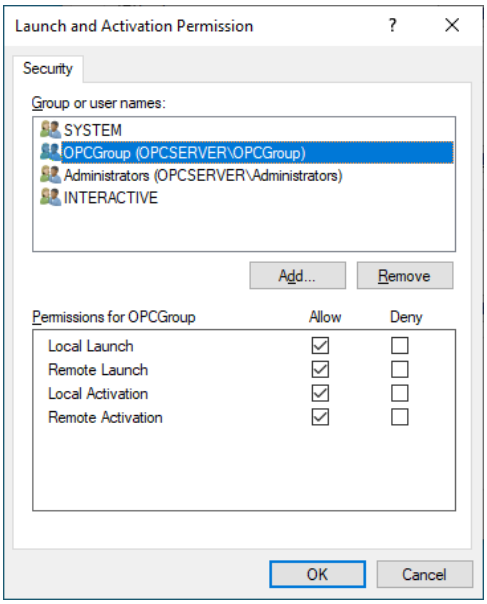
9. View the **Security** tab.
10. In the **Launch and Activation Permissions** area, select **Customize** (so users and groups can be granted permission to start the OPC server if it is not running).
11. Click **Edit...**.



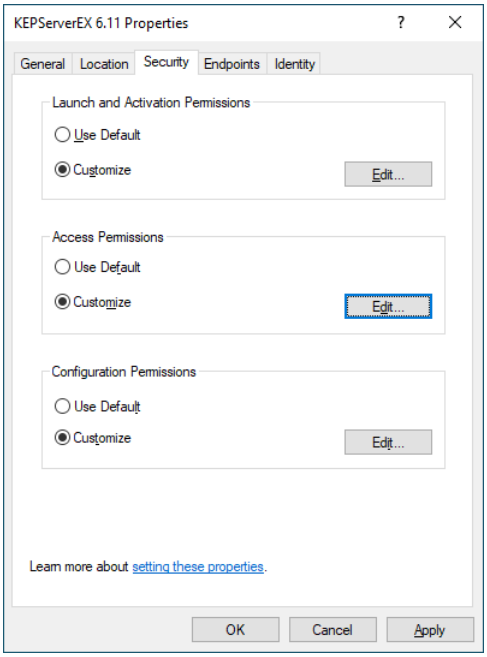
12. In Launch and Activation Permissions, select **Edit...**.



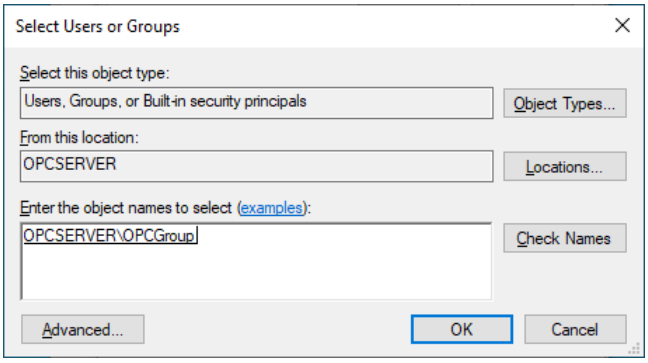
13. In Object Types, select the desired object type.
14. In Locations, click the domain or the computer that contains the users or groups to be added, then click **OK**.
15. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.
16. After the account has been validated, click **OK**.
17. Select the new user or group.



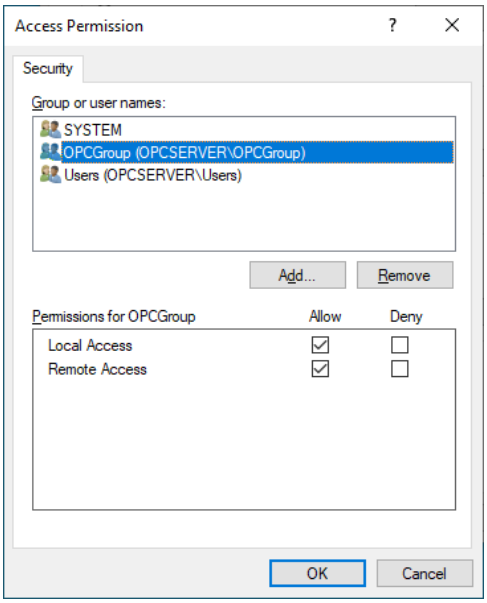
18. Enable the local and remote permissions for this user or group and click **OK**.
19. In the Access Permissions group, select **Customize** (so users and groups can be granted permissions to make calls to the OPC server, such as browsing for items, adding groups and items, or any other standard OPC call).
20. Click **Edit...**.



21. In Access Permissions, select **Edit...**.



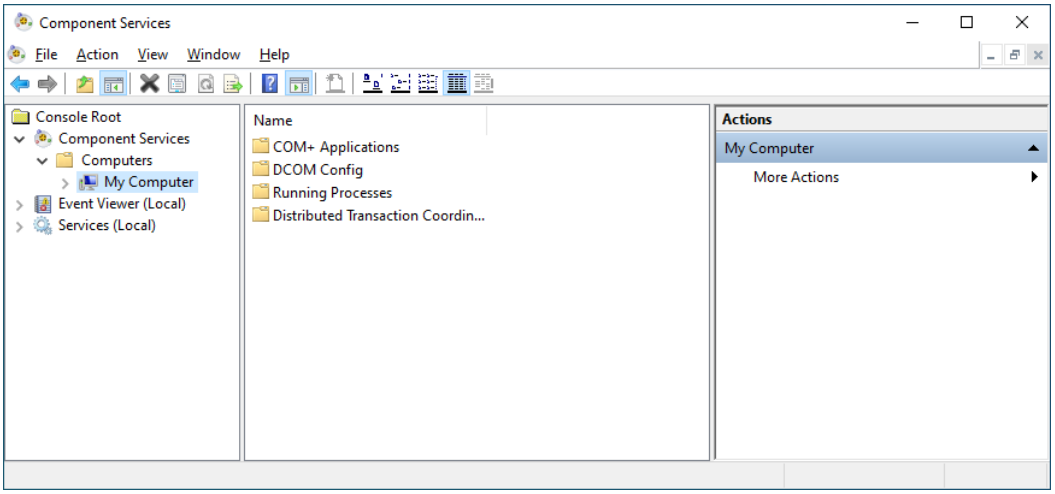
22. In Object Types, select the desired object type.
23. In Locations, click the domain or the computer that contains the users or groups to be added, then click **OK**.
24. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.
25. After the account has been validated, click **OK**.
26. Select the new user or group.



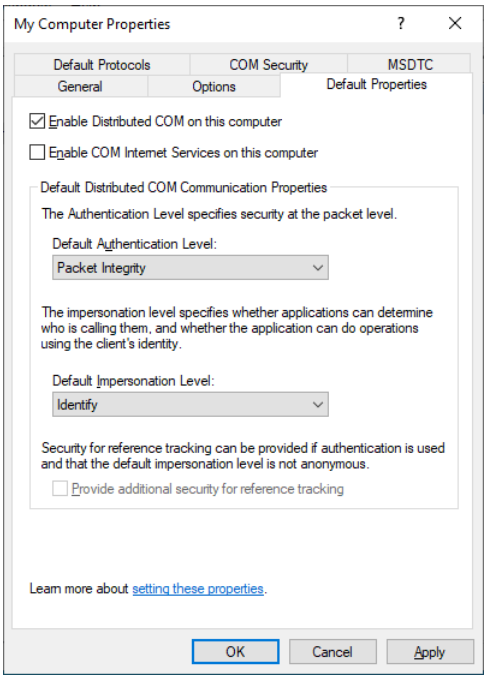
27. Enable the local and remote permissions for this user or group.
28. Click **OK**.

4.2 Configuring the System

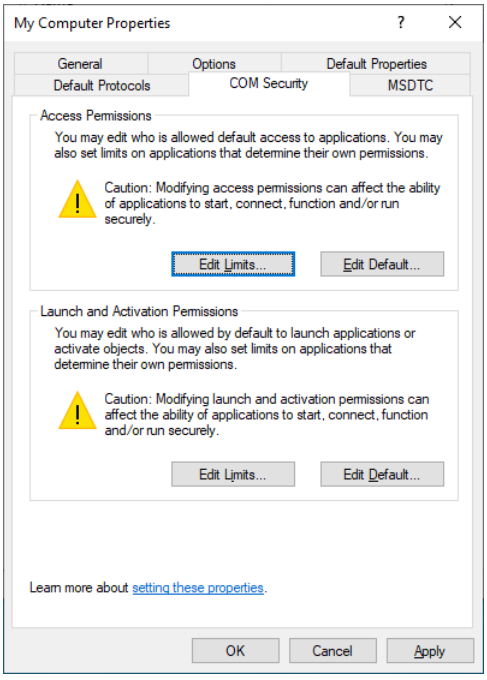
1. Launch Component Services, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "dcomcnfg".
2. Under Console Root, expand Component Services and Computers.



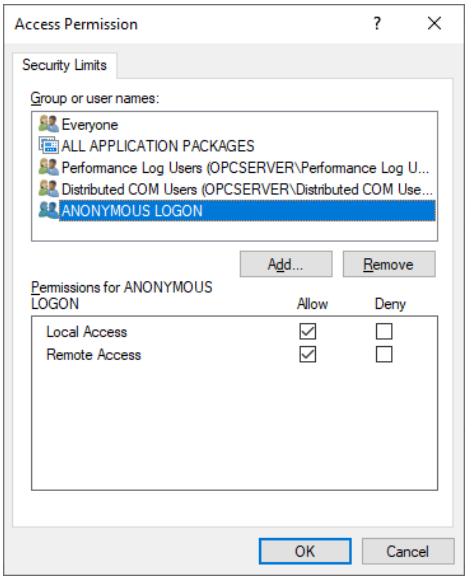
3. Right-click on My Computer and select **Properties...**.
4. Select the **Default Properties** tab.
5. Verify that the **Enable Distributed COM on this computer** option is enabled.
6. Select **Packet Integrity** for the Default Authentication Level.
7. Select **Identify** for the Default Impersonation Level.



8. Select the **COM Security** tab.
9. Select **Edit Limits** in the Access Permissions group.



10. Select the **ANONYMOUS LOGON** group account in the Group or user names list.

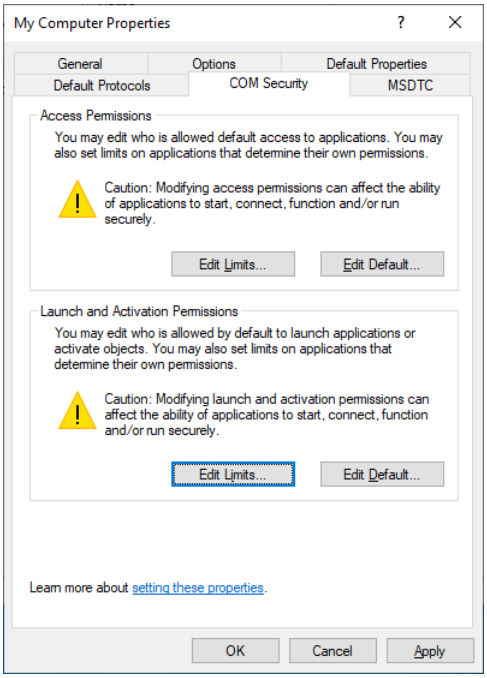


11. Enable the Local Access and Remote Access permissions for this group.

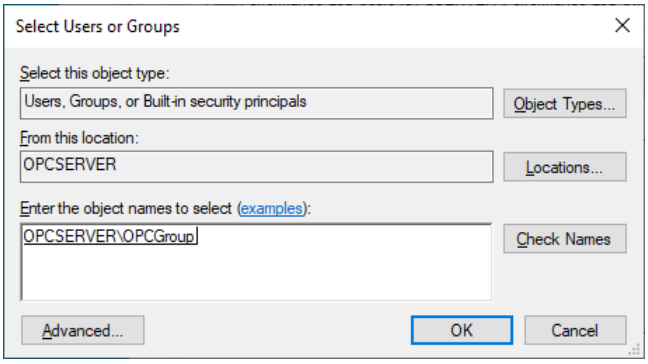
Note: OPCEnum overrides DCOM settings and opens accessibility to everyone. This step is required because applications are not permitted to perform this action without user interaction.

12. Click **OK** to return to COM Security.

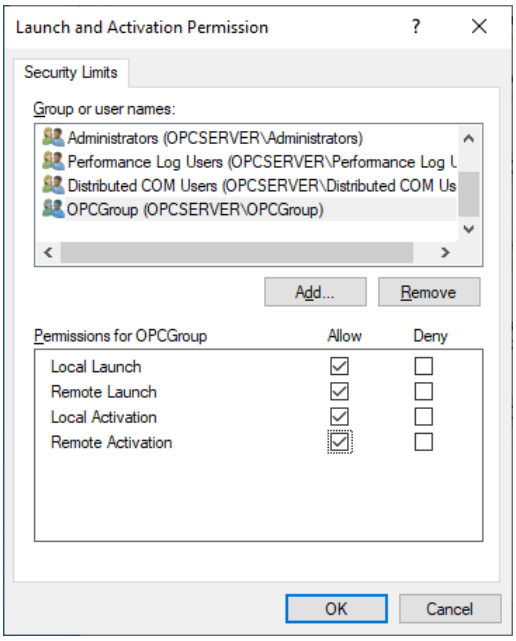
13. In the Launch and Activation Permissions group, select **Edit Limits...**



14. In Launch and Activation Permissions, select **Add.**



15. In Object Types, select the desired object type.
16. In Locations, click the domain or the computer that contains the users or groups to be added and click **OK**.
17. Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.
18. After the account has been validated, click **OK**.
19. Next, select the new user or group.



20. Enable the local and remote permissions for this user or group.
21. Click **OK** to close the My Computer properties window.

4.3 Applying Changes

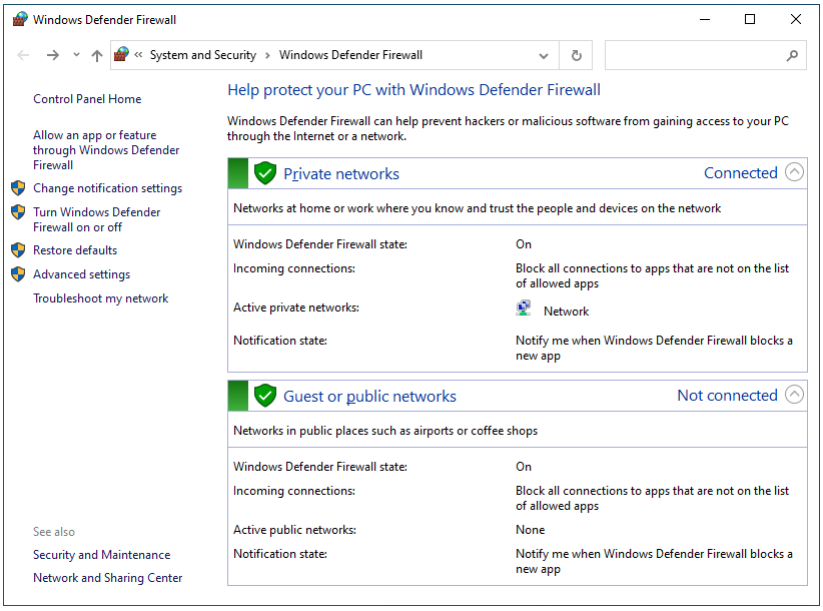
After DCOM settings have been modified, the changes may not be applied immediately. Some operating systems require a reboot for DCOM changes to take effect.

5. Firewalls

It may be easier to turn off any firewalls that may be running on both the client and server machine while configuring DCOM. Once a connection has been successfully established, it is recommended that the firewall security is restored and the correct exceptions are added.

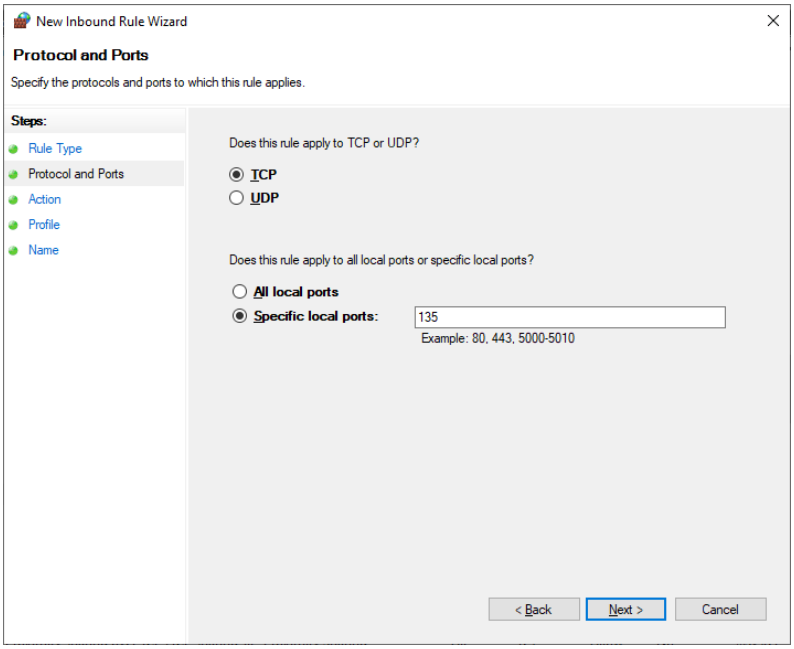
5.1 Server-Side Exceptions

1. To launch the Windows Firewall, select **Start | Run** and type "firewall.cpl".

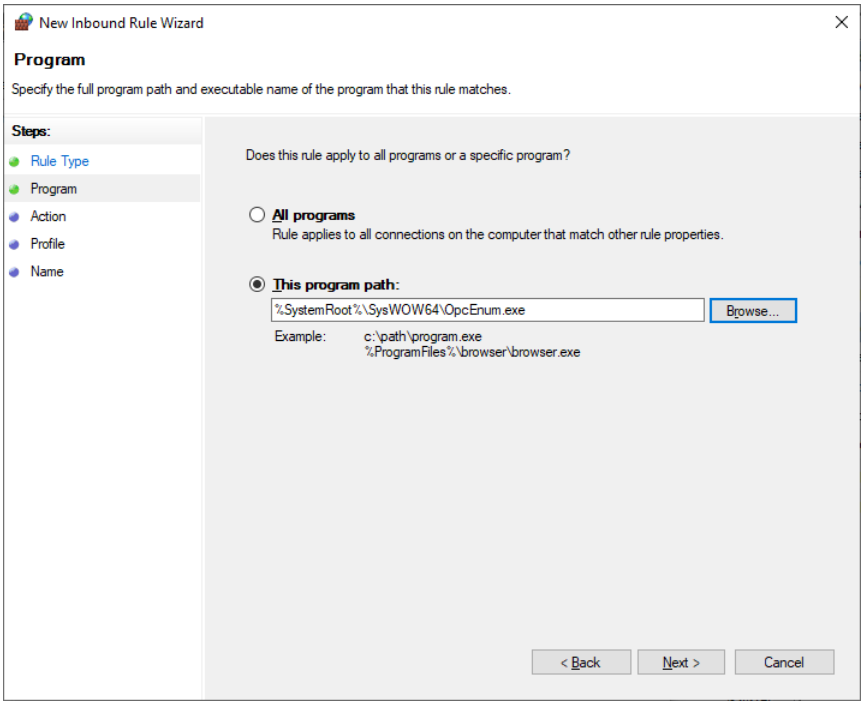


2. Verify that the firewall is enabled. If needed, select **Turn Windows Defender Firewall** on or off and customize as needed.

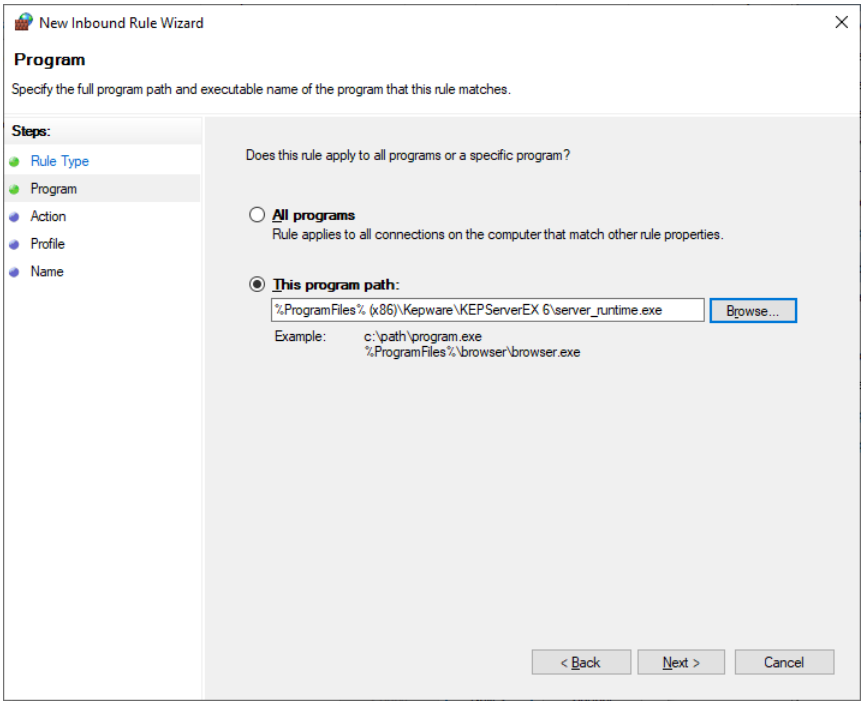
3. Add **TCP Port 135** to the firewall and allow the connection.



4. Add **OPCEnum** to the firewall and allow the connection.

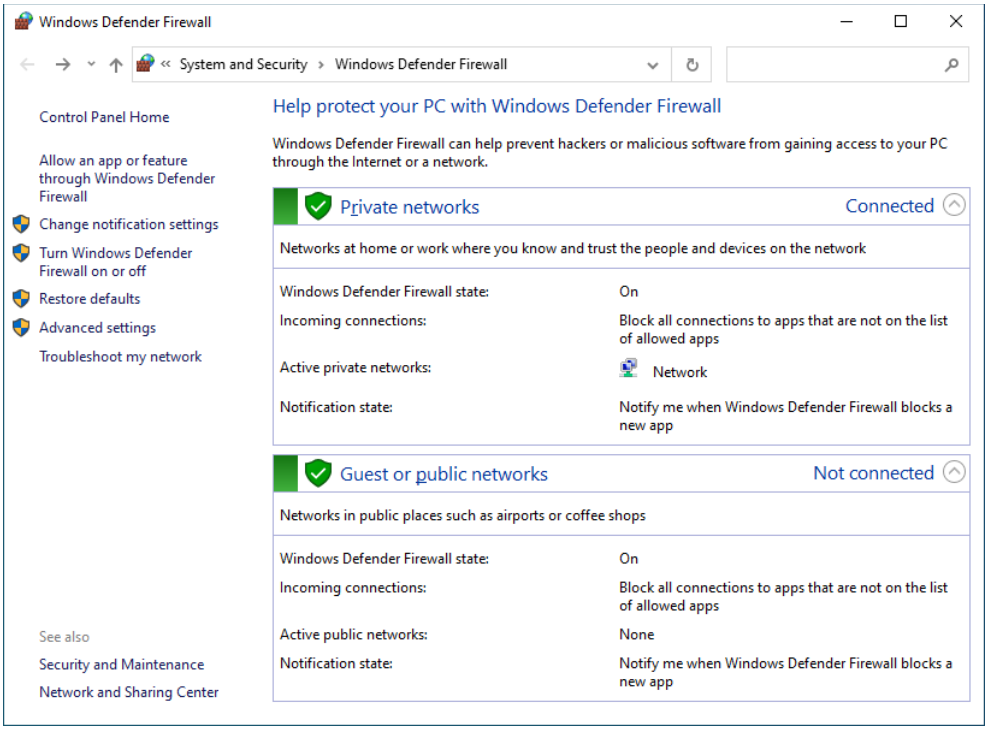


5. Add the server application executable to the firewall and allow the connection.



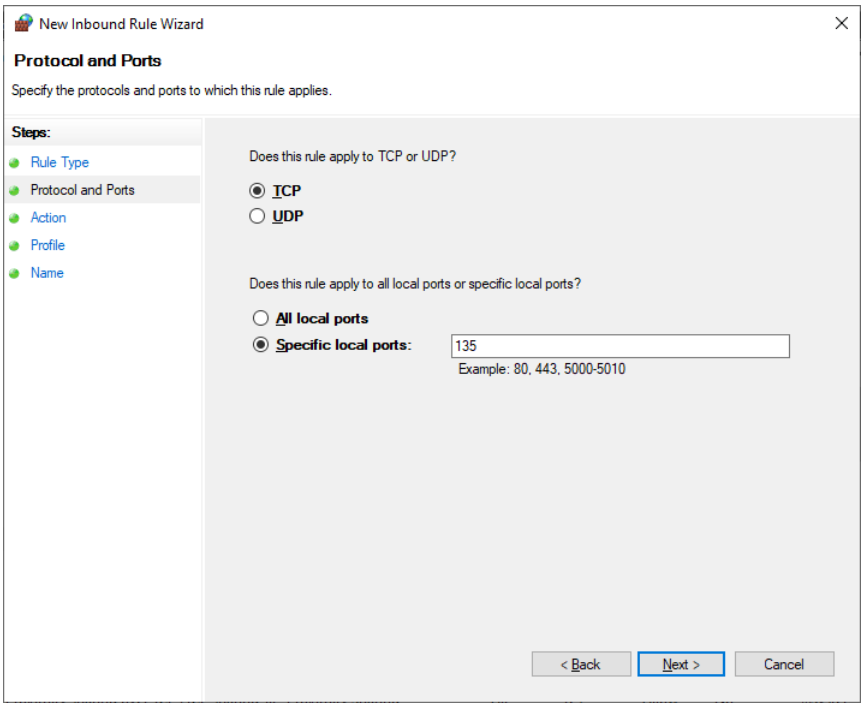
5.2 Client-Side Exceptions

1. To launch the Windows Firewall, select **Start | Run** and type "firewall.cpl".

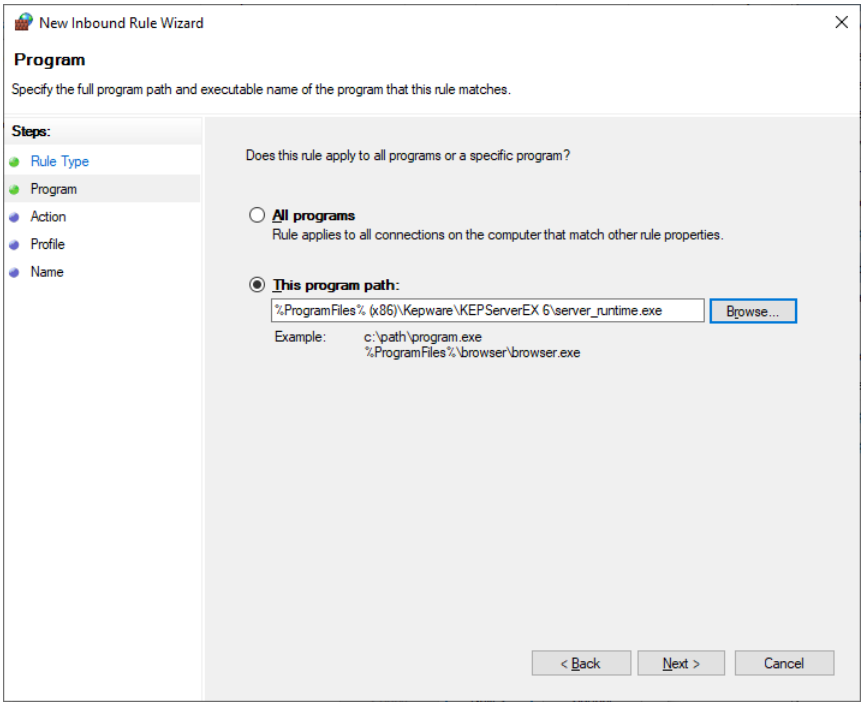


2. Verify that the firewall is enabled. If needed, select **Turn Windows Defender Firewall on or off** and customize as needed.

3. Add 135 as the **Specific local ports** to the firewall and allow the connection.



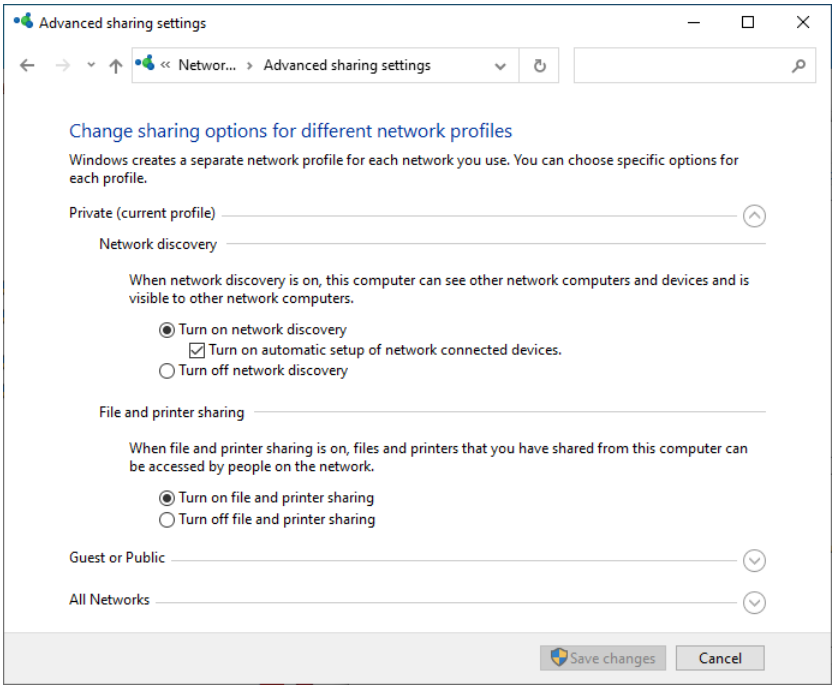
4. Add the client application to the firewall and allow the connection. In this example, the client is the OPC DA Client driver running within the Runtime service.



6. Network Discovery (Optional)

The Network Discovery setting allows or prevents the computer to detect or be detected by other computers on the network. OPC clients might not be able to browse for the server depending on how Network Discovery is configured. If the OPC server's ProgID is known and can be manually entered into the client application, browsing is not necessary and often not configured.

1. Click **Start | Control Panel | Network and Internet | Network and Sharing Center | Advanced sharing settings**.
2. Under the Network Discovery section, select the radio button to **Turn on network discovery**.
3. Click **Save changes**.



Note: Network Discovery may also require additional firewall configuration as well as additional configuration to some of the required services, such as Function Discovery Provider Host, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host.

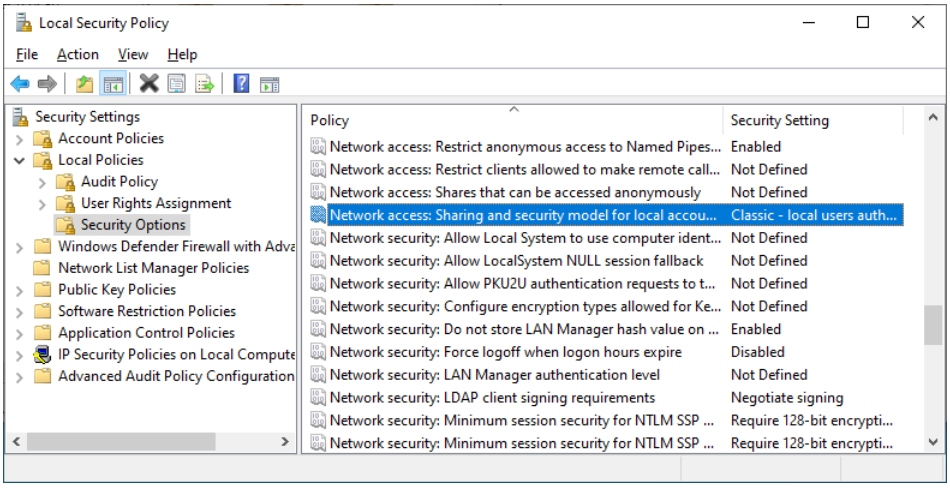
7. Local Security Policies

When computers involved in the remote connection are part of a workgroup, it may be necessary to edit the Local Security Policy. This should only be done if it is necessary. In most cases, the server computer may require changes to the authentication model whereas the client computer needs to have access to browse for servers.

7.1 Server-Side Policies

This setting determines how local users are authenticated. When the setting is set to **Classic**, remote logons use the same level of access that is set for the local account given that it has the same username and password. The Sharing and Security Model may need to be set to **Classic** on the server computer only.

1. Launch Local Security Policy, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "secpol.msc".
2. Under Security Settings, expand Local Policies.
3. Select **Security Options**.
4. In the list, right-click on Network access: Sharing and security model for local accounts and select **Properties...**.



5. Choose **Classic – local users authenticate as themselves**.
6. Click **OK**.

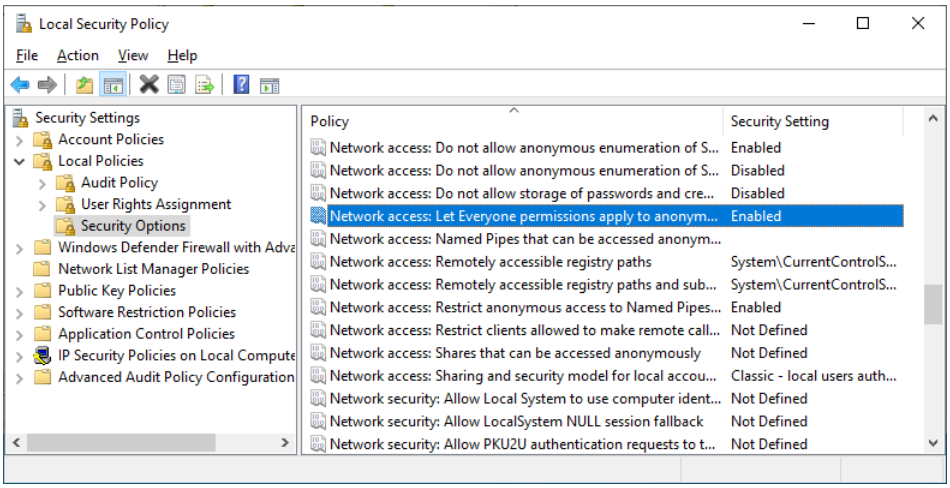
Note: An error code (HR=80070005) is returned to the client when attempting to add items if this is required.

7.2 Client-Side Policies

This setting determines the additional permissions granted for anonymous logons. When the option is disabled, the permissions granted to the Everyone security identifier do not apply to anonymous users. If the option is enabled, anonymous users are given the same permissions as the Everyone group.

Note: The Everyone permissions setting must be enabled on the client computer only.

1. Launch the Local Security Policy snap-in, which is part of the Microsoft Management Console. To view it directly, select **Start | Run** and type "secpol.msc".
2. Under Security Settings, expand Local Policies.
3. Select **Security Options**.
4. In the list, right-click on Network access: Let Everyone permissions apply to anonymous users and select **Properties**.



5. Choose **Enable** and select **OK**.

Note: If clients cannot browse for the remote server even after DCOM has been set up, this setting is required.