N3uron

Industrial IoT connectivity solutions

CONFIGURATION GUIDE

DCOM

www.n3uron.com

Index

About this user guide

OPC Classic standard specifications rely on Microsoft's COM and DCOM to exchange data between automation hardware and software. DCOM needs to be configured properly in order to allow users to establish remote communications between their OPC client and server components.

In this document, we describe the necessary steps to get DCOM working properly under Windows in a Workgroup configuration, specifical adjustments will be required depending on the Windows version.

Machines configuration

Install OPC Core Components

OPC Core Components need to be installed on the OPC server and OPC client machines. You need to install OPC Core Components version according to the operating system version (64-bit or 32-bit). It can be downloaded from https://opcfoundation.org/developer-tools/samples-and-tools-classic/core-components.

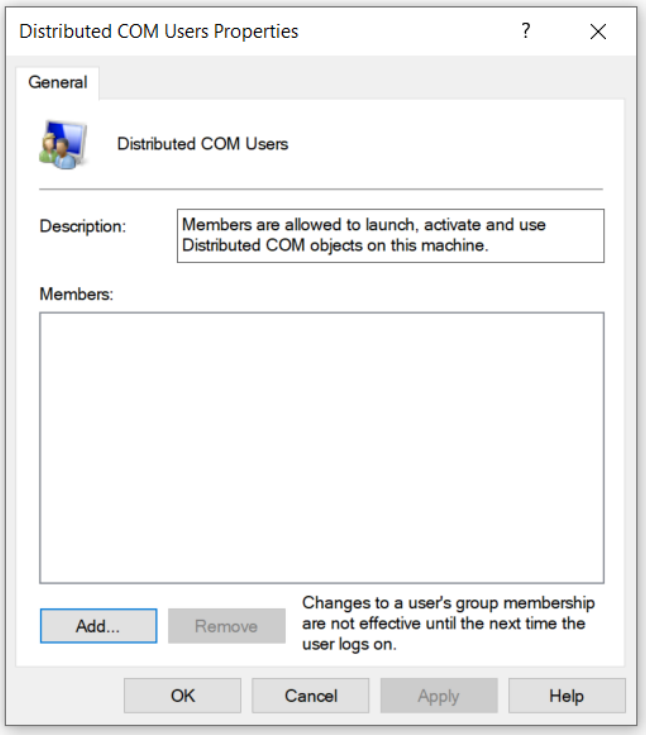
Configure Users

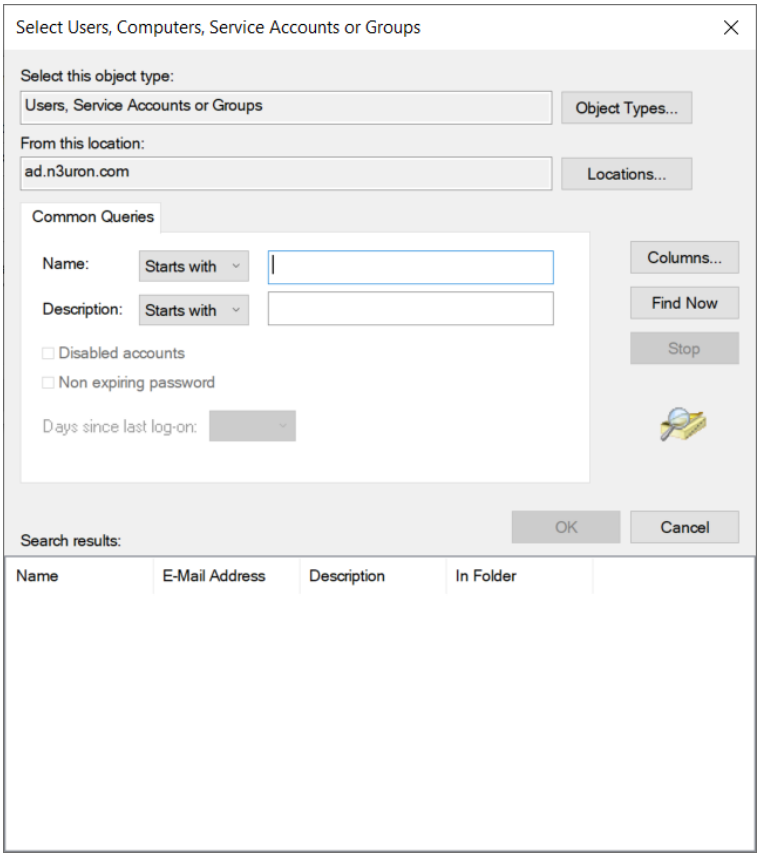
The created users in both, the client and server machines, must have the same name and password. Moreover, N3uron and the OPC Server should run using this user account.

Assign Permissions

In order to allow the users to work with DCOM, they require to be added to the corresponding "DCOM Users" group in both client and server machines. To do so:

- Go to **Local Users and Groups=> Groups.**
- Right click on **Distributed COM Users** nad click on **Properties.**
- On the properties tab, click on **Add=>Advanced=>Find Now** and select the user.




Select Users, Computers, Service Accounts or Groups
Select this object type:
Users, Service Accounts or Groups
Object Types...
From this location:
ad.n3uron.com
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last log-on:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
E-Mail Address
Description
In Folder

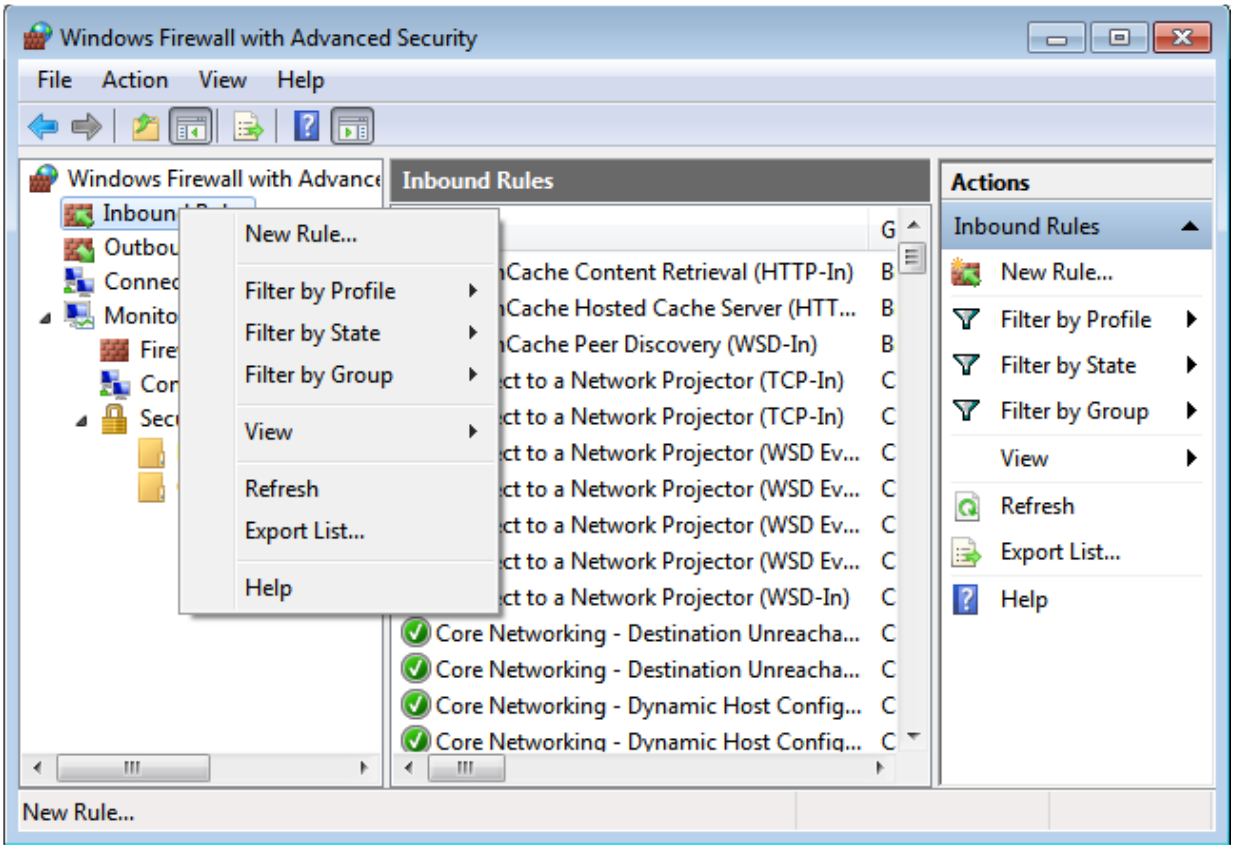
Windows firewall configuration in the opc server machine

By default, the Windows firewall does not allow any incoming requests across the network, therefore it is necessary to configure a **Program** inbound exception for the OPC Server application as well as a **Port** inbound exception for the TCP port **135**.

It will be also required to create another inbound rule for the **OPCEnum** program, whose executable file can be found in the following folder depending on the system version:

- **For 32-bit machine:** c:\Windows\system32\opcenum.exe
- **For 64-bit machine:** c:\Windows\SysWOW64\opcenum.exe.

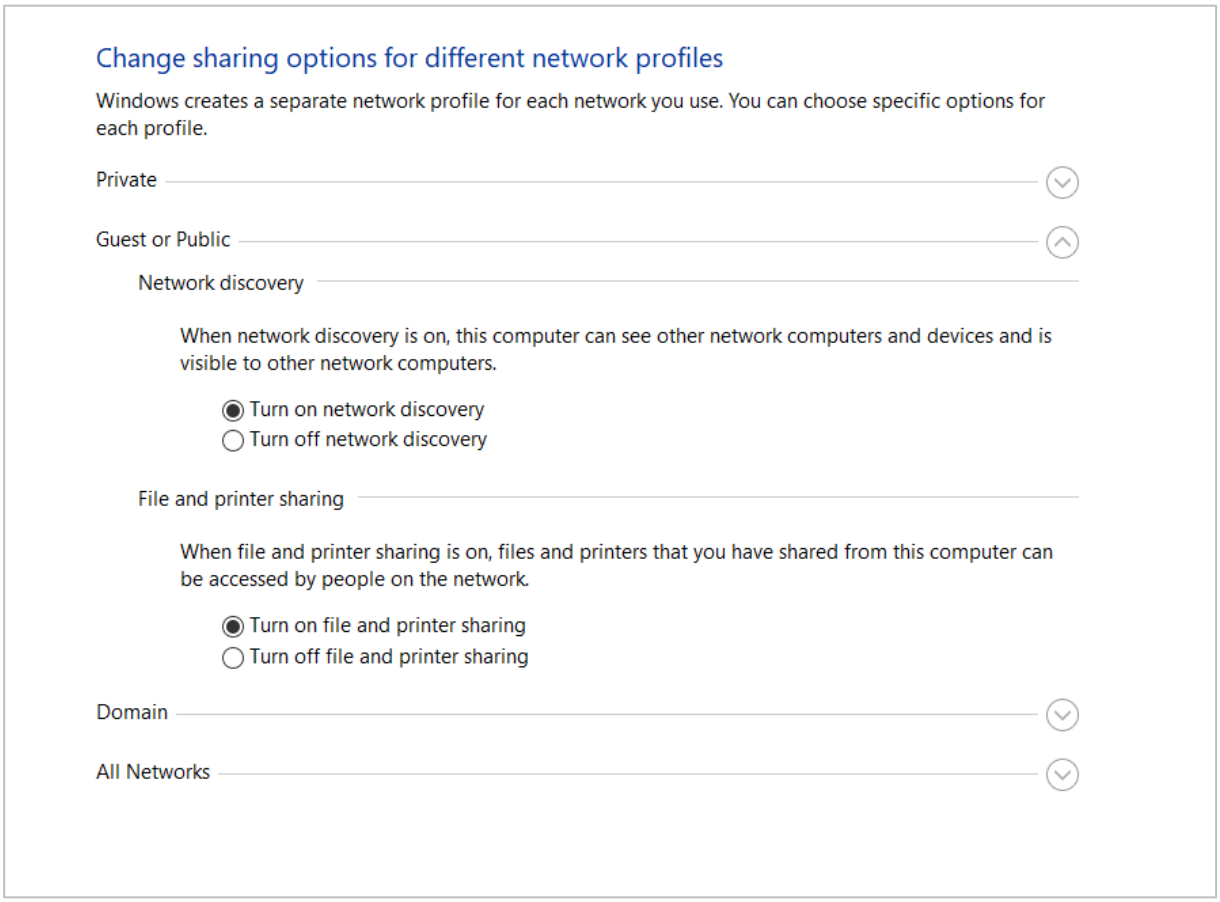
Make sure all the rules are enabled.



Network discovery

Make sure to apply the following Network Discovery steps on both server and client machines.

1. Go to **Control Panel=> Network and Internet => Network and Sharing Center**.
2. Select **Change advanced sharing settings**.
3. Click the **Turn on network discovery** radio button and save the changes.



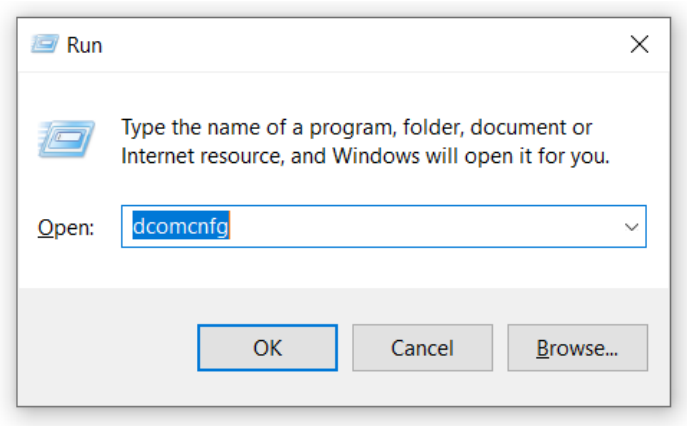
DCOM Configuration

OPC Server Machine Configuration

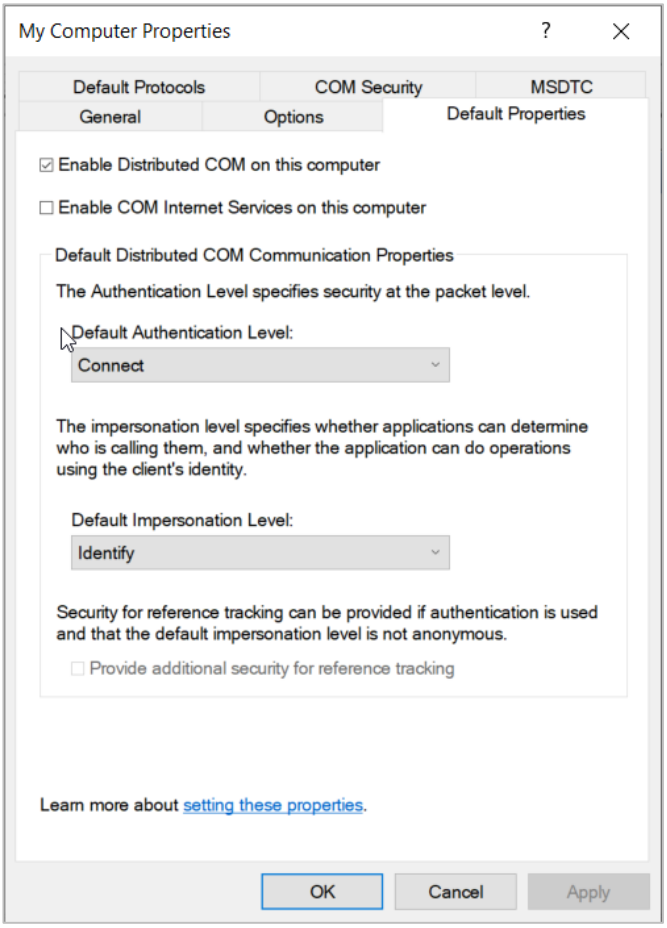
System-Wide DCOM settings

The system-wide DCOM settings affect all Windows applications that use DCOM, including OPC DA applications. In fact, any OPC DA Client application does not have its own DCOM settings, which make it affected by changes of the default DCOM configuration. This is why, system settings must be configured properly. To do so, follow the steps below:

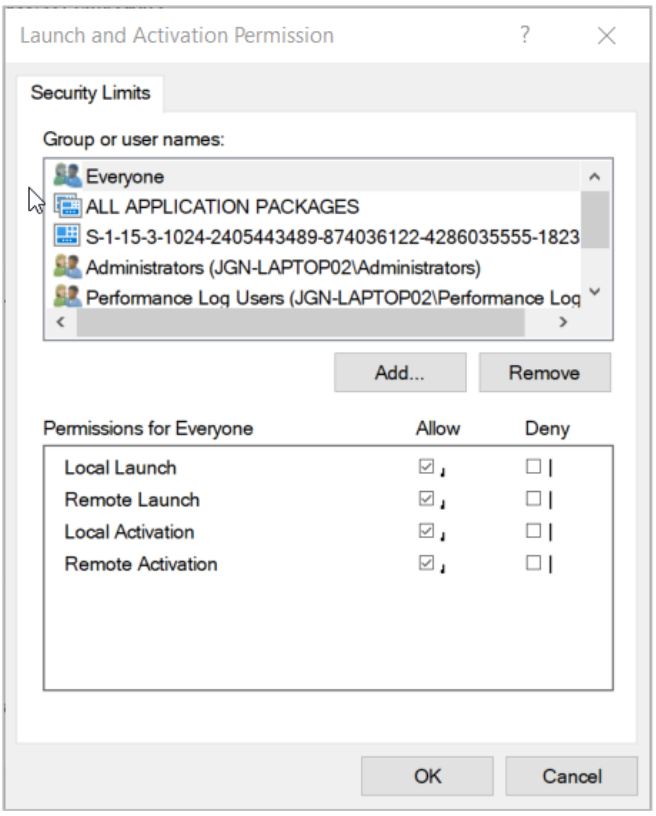
1. Click on the Windows Start button, and select Run and then type "**dcomcnfg**" to open the DCOM configuration dialog box.



2. Select **Component Services=>Computers.**
3. Right-click on **My Computer=>Properties=>Default Properties** tab.
4. Make sure to check the **Enable Distributed COM** on this computer check box. Set the **Default Authentication Level** to **Connect and the Default Impersonation Level** to Identify.



5. Right-click on **My Computer=>Properties=>COM Security** tab **=>Acces permissions=> Edit Limits.**
6. Add the user you are going to use to the list and give him all local and remote access rights.
7. It is necessary to check the **Remote Access** checkbox for the User **ANONYMOUS LOGON** as well as for the **Distributed Com Users.**

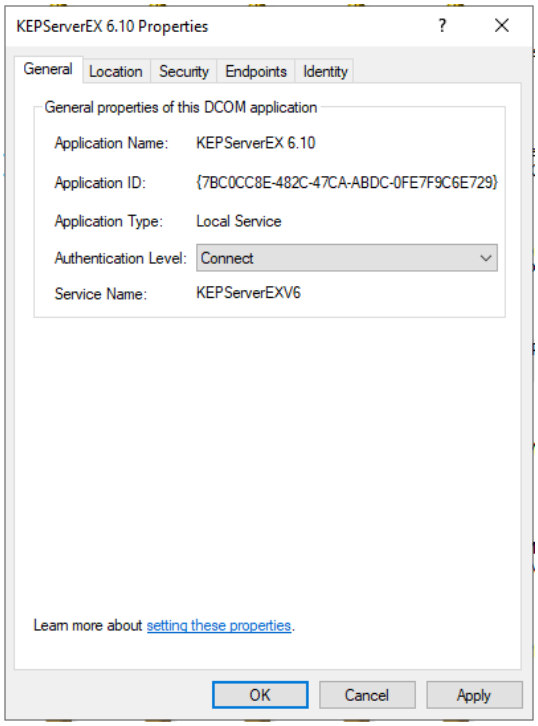


8. Under the **Launch and activation permissions** section, add the user you are going to use to the list and give him all local and remote access. It is also required to check the remote boxes for the User **Everyone**, as well as for the **Distributed Com Users.**

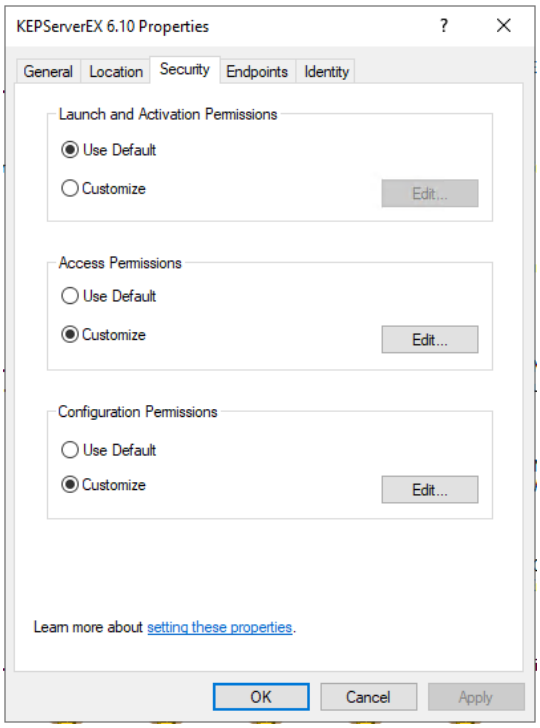
Server Specific DCOM settings

In this section, we will see how to configure the OPC server specific DCOM settings to allow access only for the user you are going to use.

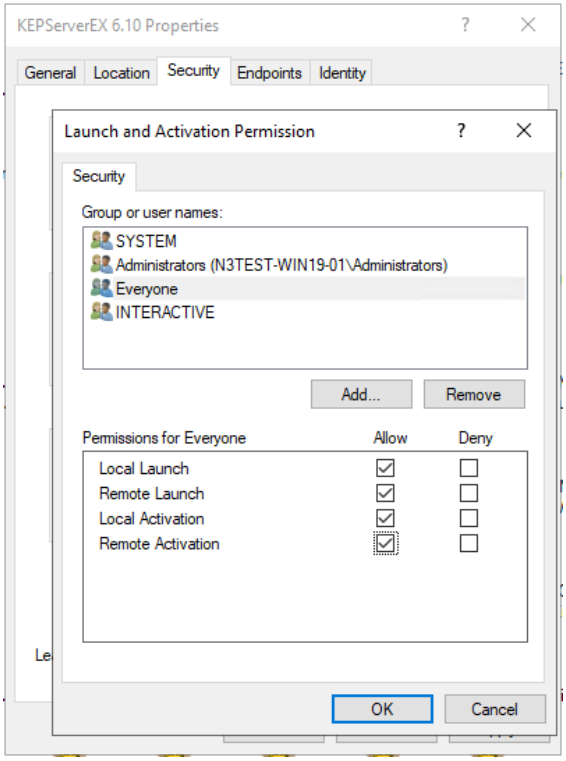
1. Go to Windows start button and type **dcomcnfg**.
2. Select **Component Services=>Computers**.
3. Click on **My Computer=>DCOM Config**.
4. Locate the OPC DA server, right click on it and select the **Properties** tab.
5. Go to **General** tab and set the **Authentication Level** to **Connect**.



6. Go to **Security** tab, for every permission type, select the **Customize** radio button and then click on **Edit**.

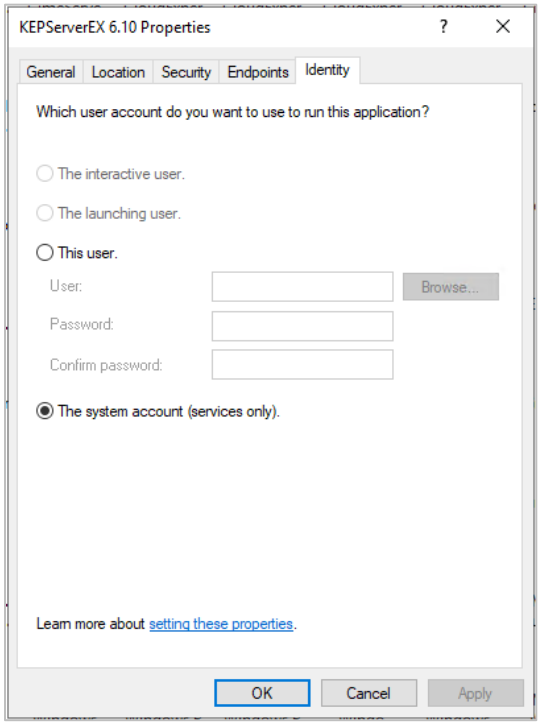


7. In **Launch and Activation Permissions**, add the user you are going to use to the **group or users names**, give him all the permissions for **(Local Launch, Remote Launch, Local Activation, Remote Activation)**, and make sure to add **Everyone**.

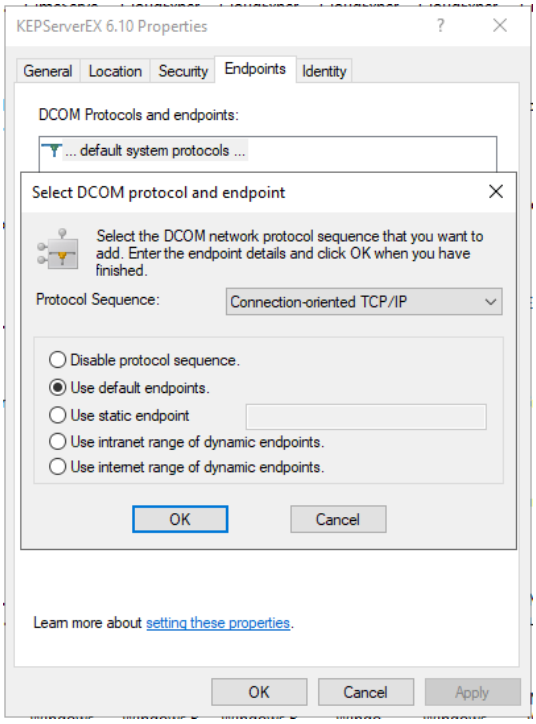


8. In **Access Permissions**, perform the same steps as in Launch and Activation Permissions for the user you are going to use and make sure to remove **Everyone** form the list.
9. In **Configuration Permissions**, perform the same steps as in Launch and Activation Permissions for the user you are going to use and make sure to remove **Everyone** form the list.

10. Go to the **Identity** tab, if the OPC DA Server is running as a service choose **The system account (service only)** option and make sure the logon for the service is the user you want to use. Otherwise, choose **The interactive user option**.



11. Go to the **Endpoints** taband choose **Connection-oriented TCP/IP**.



OPCEnum Configuration

1. Click on the Windows Start button, and select Run and then type "**dcomcnfg**" to open the DCOM configuration dialog box.
2. Select **Component Services=>Computers=>My Computer=>DCOM Config** and right click on **OpcEnum**.
3. In the **General tab**, select **Connect** as **Authentication Level**.
4. In **Launch and Activation Permissions**, add **Everyone** and **ANONYMOUS LOGON** and give them all permissions **(Local Launch, Remote Launch, Local Activation, Remote Activation)**.
5. In **Access Permissions**, add the user you are going to use to the **group or users names**, give him all the permissions for **(Local Launch, Remote Launch, Local Activation, Remote Activation)**, and make sure to remove **Everyone** from the list.
6. In **Configuration Permissions**, do the same as in **Access Permissions**.

OPC Client Machine Configuration

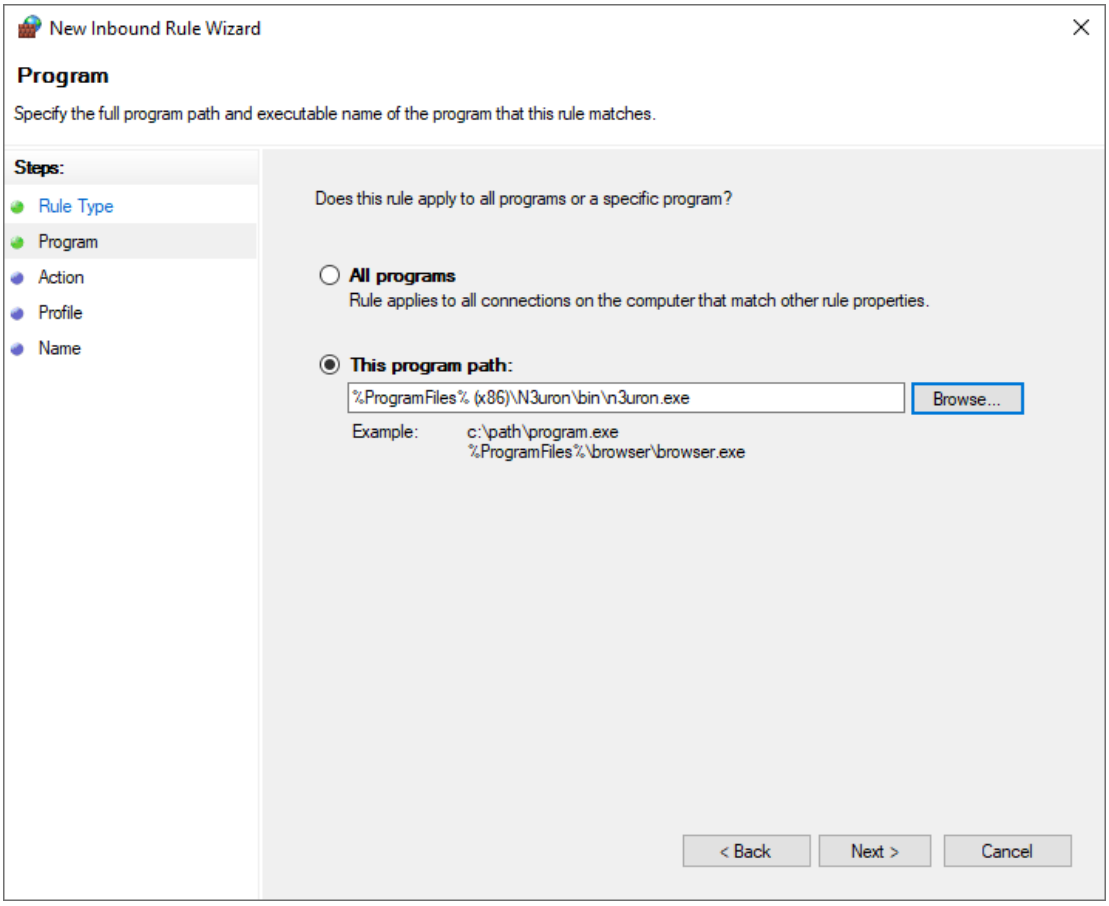
System-Wide DCOM settings

Perform the same steps as described in the section 5.1.1.

Windows Firewall

Make sure that OPC Core Components is installed and configure a new inbound rule for N3uron. For that proceed in the following way:

1. Go to **Control Panel=>System and Security=>Windows Defender Firewall=>Advanced Settings.**
2. Right click on **Inbound Rules**, select **Program**, click on **Browse** and select your N3uron.exe file usually located in C:\Program Files (x86)\N3uron\bin or C:\Program Files\N3uron\bin.



3. Select **Allow the connection**, click **Next**, give a name to the rule and click on **Finish**.
4. Restart both Client and Server Machines and verify everything is working properly.

Troubleshooting

Make sure there are no other firewall or antivirus blocking the communication between the server and client machines. In some cases, the client cannot connect to the remote OPC Server because it does not have access to browse the remote registry. It is recommended to prepare and apply a customized .reg file on the client computer in order to export Implemented categories and CLSID from the server machine registry database and add them to the client machine registry. To do so, proceed to the following steps:

1. On the server machine, click on the Windows Start button and type **Regedit** to open the **Registry Editor**.
2. Search your server CLSID under **HKEY_CLASSES_ROOT=>CLSID**.
3. Right click on your Sever CLSID, click on **Export** and save the **.reg** file.
4. Copy the **.reg** file in your client machine and double click on it.
5. Search your server ProgID under **HKEY_CLASSES_ROOT=>Server ProgID**.
6. Right click on your Sever ProgID, click on **Export** and save it.
7. Copy the Exported ProgID and execute it on the client machine
8. Search your server CLSID in AppID, go to **HKEY_CLASSES_ROOT=>AppID=>CLSID**.
9. Right click on on **Export**.
10. Copy the exported file and execute it on the client machine.

N3uron

Industrial IoT connectivity solutions

CONFIGURATION GUIDE

DCOM