

CONFIGURATION GUIDE

www.n3uron.com

Index

About this user guide	. 3
Machines configuration Install OPC Core Components Configure Users	.4 .4 .4
Assign Permissions	.4
Windows firewall configuration in the opc server machine	. 6
Network discovery	. 7
Dcom Configuration OPC Server Machine Configuration	. 8 . 8 15
Troubleshooting	16

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.

Distributed COM	Users Properti	ies		?	×
General					
Distribu	uted COM User	S			
Description:	Members are Distributed C	allowed to laur OM objects on t	nch, activate an this machine.	d use	
Members:					_
Add	Remove	Changes to are not effect user logs on	a user's group i ctive until the ne	members ext time th	ship ne
	OK	Cancel	Apply	He	lp

Select Users, Computers, Service Accounts or Groups							
Select this object type: Users, Service Accounts or Groups Object Types							
From this location ad.n3uron.com	From this location: ad.n3uron.com Locations						
Common Quer	ies						
Name:	Starts with ~				Columns		
Description:	Starts with ~				Find Now		
Disabled ad	ccounts				Stop		
□ Non expirin	g password				<u></u>		
Days since la	st log-on:				P		
Search results:				OK	Cancel		
Name	E-Mail Address	Description	In Folder				

N3uron

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.

each profil	le.
Private —	
Guest or Pu	ublic (
Netwo	ork discovery
W vi	Vhen network discovery is on, this computer can see other network computers and devices and is is is ble to other network computers.
	Turn on network discovery
	O Turn off network discovery
File ar	nd printer sharing
V b	Vhen file and printer sharing is on, files and printers that you have shared from this computer can we accessed by people on the network.
	Turn on file and printer sharing
	○ Turn off file and printer sharing
Domain —	
All Networ	ks (>)

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.

🖅 Run		×
	Type the name of a program, folder, document or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	dcomcnfg	~
	OK Cancel <u>B</u> rowse	

- 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.

My Computer Propertie	s		?	\times			
Default Protocols	COM Se	curity	MSDTC				
General	Options	Defau	It Properties				
☑ Enable Distributed CO □ Enable COM Internet	Ceneral Copions Constant reparate Constant reparate						
Default Distributed CO	OM Communication	Properties					
The Authentication Le	evel specifies security	at the packet	level.				
Default Authenticati	on Level:						
Connect		~					
who is calling them, a using the client's iden	nd whether the appli tity. on Level:	cation can do	operations				
Identify		~					
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.							
Learn more about <u>settin</u>	<u>g these properties</u> .						
	ОК	Cancel	Арр	ly			

- 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**.

Launch and Activation Permission		? ×				
Security Limits						
Group or user names:						
Kindp of user names. Everyone A A ALL APPLICATION PACKAGES S-1-15-3-1024-2405443489-874036122-4286035555-1823 Administrators (JGN-LAPTOP02\Administrators) Performance Log Users (JGN-LAPTOP02\Performance Log <						
	Add	Remove				
Permissions for Everyone	Allow	Deny				
Permissions for Everyone Local Launch	Allow	Deny				
Permissions for Everyone Local Launch Remote Launch	Allow	Deny				
Permissions for Everyone Local Launch Remote Launch Local Activation	Allow	Deny				
Permissions for Everyone Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny				
Permissions for Everyone Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny				

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.

KEPServerEX 6.10 Properties	?	×
General Location Security Endpoints Identity		
General properties of this DCOM application		
Application Name: KEPServerEX 6.10		
Application ID: {7BC0CC8E-482C-47CA-ABDC-0	FE7F9C6E	729}
Application Type: Local Service		
Authentication Level: Connect		\sim
Service Name: KEPServerEXV6		
Leam more about <u>setting these properties</u> .		
OK Cancel	Ap	ply

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

KEPServerEX 6.10 Properties	?	\times
General Location Security Endpoints Identity		
Launch and Activation Permissions		
Use Default		
O Customize	Edit	
Access Permissions		
◯ Use Default		
Customize	Edit	
Configuration Permissions		
◯ Use Default		
Customize	Edit	
Leam more about <u>setting these properties</u> .		
OK Cancel	Apj	ply

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**.

KEPServerEX 6.10 P	roperties			or 1	?	×
General Location	Security	Endpoints	Identity			
Which user accou	nt do you v	vant to use to	o run this applic	ation?		
O The interactive	user.					
O The launching	user.					
O This user.						
User:				Br	owse	
Password:						
Confirm passwor	d:					
The system according to the	count (serv	ices only).				
Learn more about	setting thes	e properties.				
	[ОК	Cancel		Арр	ly

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.

	New Inbound Rule Wizard		×
P	rogram		
Spe	ecify the full program path and e	executable name of the program that this rule matches.	
Ste	eps:		
۲	Rule Type	Does this rule apply to all programs or a specific program?	
۲	Program		
۲	Action	O All programs	
۲	Profile	Rule applies to all connections on the computer that match other rule properties.	
۲	Name	This program path:	
		%Program Files% (x86)\N3uron\bin\n3uron.exe Browse	
		Example: c:\path\program.exe	
		%ProgramFiles%\browser\browser.exe	
			_
		< Back Next > Cancel	

- 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

