# **OPCXmIDA – OPC Xml/DA Client and Server**

OPC Xml/DA Client implements communication with local and remote OPC servers. The communications blocks are dynamically created according to the pooling cycle defined on the Access Type for each Device Point.



Implementation DLL: T.ProtocolDriver.OPCXmlDA.dll

**Protocol:** OPC proprietary

Interface: OPC proprietary

OPC servers supported: Any OPC server compatible with OPC Xml/DA v2.05 or v3.0 specifications

Protocol Options: None

Max number of nodes: User defined

PC Hardware requirements: None

PC Software requirements: OPC Core components

Note
You can find the OPC Core components in the OPC Foundation website.

### **Channel Configuration**

There is no channel configuration for OPC Xml/DA Client channels.

## **Node Configuration**

#### **Station Configuration**

Service URL: Defines the location of the OPC Server. Example: OPCDAServer.2, \\192.168.1.201\ OPCDAServer.2, http://192.168.1.2:4200

Refresh Rate: Server update rate

AllitemsSameGroup: A Flag indicating if the driver should add all items at the same OPC group. Only one connection is created with OPC Server

EnableReadPolling: A Flag indicating if reading is by polling

ReadFromDevice: Forces all reads made from a device

UseTimestampFromComputer: Uses timestamp from a computer instead of a device

### **Point Configuration**

Choose the OPCServer item that will communicate with the tag.

You can type the OPC Server item's name into the textbox, or you can use the cell editor to browse the OPC Server items.

OPC Arrays: You should configure the Array field in the Modifiers column.

### Troubleshoot

The status of the driver's execution can be observed through the diagnostic tools, which are:

- Trace window
- Property Watch
- Module Information

The above tools indicate if the operations have succeeded or have failed. A status of 0 (zero) means communication is successful. Negative values indicate internal driver errors, and positive values indicate protocol error codes.

Consult your OPC Server documentation for the specific protocol error codes.

### Append – How to Configure DCOM

#### 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 not expose more than what is required for the application. Although multiple security layers exist, it is still possible that some part of the system will be compromised.

#### **Users and Groups**

To ensure that an OPC connection is secure, it is suggested to create users and groups that are exclusively for this use. These can be manually added by any user who has the proper credentials to do so.

A Note

The procedure described below must be executed on both the Client and Server. The User that is created in both computers must have the same name and password.

#### Adding a Local User

• Launch the Local User and Groups snap-in, which is part of the Microsoft Management Console. It can be viewed directly by selecting WindowsKey + R and typing 'lusrmgr.msc'.



• Next, click Users. Then, select Action > New User.

New User			?	×
User name:	OPCI	Jser1		
Full name:	B			
Description:	User	created for secure DCOM connection	ons	
				_
Password:		•••••		
Confirm password:				
User must cha	nge pa	ssword at next logon		
User cannot d	hange	password		
Password nev	er expi	es		
Account is dis	abled			
Help		Create	Clos	se

- Type the appropriate information in the dialog box.
   Change the following options as required:

   User must change password at next logon
   User cannot change password
   Password never expires
   Assert in disk back

  - Account is disabled
- Click, Create. Then, click Close.

#### Adding a Local Group

- Launch the Local User and Groups snap-in, which is part of the Microsoft Management Console. It can be viewed directly by selecting WindowsKey + R and typing 'lusrmgr.msc'.
  Click, Groups. Then, select Action > NewGroup.

New Group	?	$\times$
Group name:	OPCGroup	
Description:	Group created for secure DCOM connections	
Members:		
	€ <sup>2</sup>	
Add	Remove	
Help	Create	Close

- In Group Name, type a name for the new group.
- In Description, type a description of the new group.
- Click, Create. Then, Close.

#### Adding Users to a Group

- Launch the Local User and Groups snap-in.
- Select Groups.
- Right-click on the group in which a member will be added, and select All Tasks.
- Click, Add to Group > Add.

Select Users		×
Select this object type:		
Users or Built-in security principals		Object Types
From this location:		
DESKTOP-8UV53RB		Locations
Enter the object names to select (examples):		
OPCUser1		Check Names
Advanced	OK	Cancel

- In Object Types, select the types of objects it will find.
- In Locations, click the domain or the computer that contains the users it will add. Click, OK.
- Type the name of the user or group that will be added to the group. Click, OK.
- To validate the user or group names being added, click Check Names.

### **DCOM Configuration**

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

#### **Configuring the Application**

- Launch the Component Services snap-in, which is part of the Microsoft Management Console. It can be viewed directly by selecting Windows Key + R and typing 'dcomcnfg'.
- Under Console Root, go to Component Servers > Computers > My Computer > DCOM Config.



- Browse the DCOM enabled objects until the OPC server application is located. In this example, 'Tatsoft OPC DA Server' is displayed where the Right-click on the server application, and select Properties.
  Open the General tab, and verify that the Authentication Level is set to Default.

Tatsoft.OPCDAServer Tatsoft OPC DA Server Properties ?  $\times$ General Location Security Endpoints Identity General properties of this DCOM application Application Name: Tatsoft.OPCDAServer Tatsoft OPC DA Server {0F74F60C-E286-4978-A639-DE0DB478C37A} Application ID: Application Type: Local Server Authentication Level: Default  $\sim$ Local Path: Learn more about setting these properties. Cancel OK Apply

• Open the Security tab.

Tatsoft.OPCDAServer Tatsoft OPC DA Server Properties ? X
General Location Security Endpoints Identity
Launch and Activation Permissions
◯ Use Default
Customize     Edit
Access Permissions
◯ Use Default
Customize     Edit
L
Configuration Permissions
◯ Use Default
Customize     Edit
Loom many about particle these proportion
commore about <u>setting treas properties</u> .
OK Cancel Apply

• In Launch and Activation Permissions, select Customize. Here, users and groups can be granted permission to start the OPC server if it is not already running. Click Edit.

- In Launch and Activation Permissions, select Add

Select Users or Groups		×
Select this object type:		
Users, Groups, or Built-in security principals		Object Types
From this location:		
DESKTOP-8UV53RB		Locations
Enter the object names to select ( <u>examples</u> ):		
DESKTOP-8UV53RB\OPCGroup		Check Names
Advanced	ОК	Cancel

- In Object Types, select the desired object type.In Locations, click the domain or the computer that contains the users or groups that will be added.
- Then, click OK.
- Type the name of the user or group in the window. To validate the user or group names being added, click Check Names.
  After the account has been validated, click OK.
- Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the Group or user names list.
- Next, select the new user or group.

Launch and Activation Permission

$\sim$
~

?

Security		
Group or user names:		
SYSTEM Administrators (DESKTOP- INTERACTIVE CPCGroup (DESKTOP-8U	8UV53RB\Administra V53RB\OPCGroup)	ators)
	Add	Remove
Permissions for OPCGroup	Allow	Deny
Local Launch	$\mathbf{\nabla}$	
Remote Launch		
Remote Activation		
	OK	Cancel

#### Note ∕

To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

- Repeat the process for all accounts that have been added. Click OK.
  Select Customize in the Access Permissions group. Here, users and groups can be granted permissions to make calls to the OPC server. These calls include browsing for items, adding groups and items, or any other standard OPC call.
- Click Edit.
- Repeat the same procedure for the Access Permissions option. •
- Browse to the Identity tab and select The interactive user option.

Tatsoft.OPCDAServer Tatsoft	OPC DA Se	rver Prop	perties	?	×
General Location Security	Endpoints	Identity			
Which user account do you v	want to use to	o run this a	applicati	on?	
The interactive user.					
O The launching user.					
◯ This user.					
User:				Browse.	
Password:					
Confirm password:					
O The system account (serv	ices only).				
Learn more about <u>setting the</u> s	se properties.				
	OK			۸.	oh
	UK		ancer	~	Piy

• Select OK to close the Server Properties.

#### **Configuring the System**

- Under Component Services snap-in, go to Console Root > Component Services > Computers.
  Right-click on My Computer and select Properties.

Component Services File Action View Window Help		- C ×
🔶 🔿 📶 🗙 🖬 🍳 🕞 🛛 🛅 🏦		P
Console Root Name		Actions
Component Services	plications	My Computer 🔺
Wy Computer       DCOM Converted and the con	on Coordi	More Actions

- Select the Default Properties tab, and verify that the Enable Distributed COM on this computer option is enabled.
  Select Connect for the Default Authentication Level.
  Select Identify for the Default Impersonation Level.

### My Computer Properties

2	$\sim$
ſ	

Default Protocols	COM Security	MSDTC
General	Options	Default Properties
Enable Distributed COI	Mon this computer	
	or on this compater	
Enable COM Internet S	ervices on this comput	er
Default Distributed COM	Communication Prope	ties
The Authentication Leve	el specifies security at t	he packet level.
Default Authentication	Level:	
Connect		$\sim$
The impersonation level who is calling them, and	specifies whether appl whether the applicatio	ications can determine n can do operations
using the client's identity		
Default Impersonation	Level:	
Identify		$\sim$
Security for reference tra	acking can be provided	if authentication is used
Provide additional	security for reference tr	acking
	security for reference ti	acking
Learn more about setting t	hese properties.	
		0.1
	OK	Cancel Apply

- Select the COM Security tab.
  Select Edit Limits in the Access Permissions group.
  Select the ANONYMOUS LOGON group account in the Group or user names list.

#### Access Permission

ES KTOP-8UV53RB\ KTOP-8UV53RB\	Verformanc Distributed C
Add	Remove
Allow	Deny
N	
	]
	ES KTOP-8UV53RB\ CTOP-8UV53RB\ Add Allow

- In the Launch and Activation Permissions group, select Edit Limits.
  Add the created OPC Group to the Groups list.
  Next, select the new user or group, and allow the permissions.

#### Launch and Activation Permission

?

Security Limits					
Group or user names:					
Administrators (DESKTOP-8UV53RB\Administrators)  Performance Log Users (DESKTOP-8UV53RB\Performanc  Distributed COM Users (DESKTOP-8UV53RB\Distributed C  OPCGroup (DESKTOP-8UV53RB\OPCGroup)					
<		>			
L	Add	Remove			
Permissions for OPCGroup	Allow	Deny			
Local Launch Remote Launch Local Activation Remote Activation					
	ОК	Cancel			

Note Restart the computer to apply the changes.

### **Firewall Configuration**

In some cases, it is easier to turn off any firewalls that may be running on both the client and server machine before DCOM is setup. Once a connection has been successfully created, it is recommended that the firewall security is restored and the correct exceptions are added.

- Launch the Windows Firewall by selecting Windows Key + R and then typing 'firewall.cpl'.
  Browse to 'Allow an app or feature through Windows Firewall'.

	Windows Firewall				- 0	×	
÷	→ ~ ↑ 🔗 > Control Pa	anel  → System and Security  → Windows Firewall	~	Ō	Search Control Panel	Q	
	Control Panel Home	Help protect your PC with Windows	Firewall				
	Allow an app or feature through Windows Firewall	Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.					
	Change notification settings	Private networks			Connected	$\odot$	
	Turn Windows Firewall on or off	Networks at home or work where you know and trust the people and devices on the network					
	Restore defaults Advanced settings Troubleshoot my network	Windows Firewall state:	On				
		Incoming connections:	Block all connections to apps that are r list of allowed apps			not on the	
		Active private networks:	😰 N	etwor	k		
		Notification state:	Notify r app	me wł	hen Windows Firewall blocks a nev	N	
		Guest or public networks			Not connected	$\odot$	

Click on Allow another app, and browse for the file named DANSrvNet4.exe that is usually located at: C:\ProgramFiles(x86)\< CompanyName>\<ProductName>\<ProductVersion>

Change settings

### Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:			
Name	Privat	e Public	^
✓.NET4 OPC DA V2/V3 Professional Server Toolkit			
☑ 3D Builder	✓	✓	
Allow SQL	$\checkmark$	☑	
BranchCache - Content Retrieval (Uses HTTP)			
BranchCache - Hosted Cache Client (Uses HTTPS)			
BranchCache - Hosted Cache Server (Uses HTTPS)			
BranchCache - Peer Discovery (Uses WSD)			
Cast to Device functionality	$\checkmark$	$\checkmark$	
Complemento para Telefone Microsoft	$\checkmark$	✓	
Conector de aplicativos	$\checkmark$	☑	
Contact Support	$\checkmark$	$\checkmark$	
Core Networking	V	✓	Υ.
	Details	Remov	/e

The steps below must be executed on both the Client and Server.

- Click on Advanced Settings, right-click on Inbound Rules, and select add new rule.
- Select Port and click on Next.
  Apply the rule for TCP connections, and enter the port number, 135.

- Select Allow the connection, and click on next.
  Choose the domains that best suit your case.
  Enter a friendly name and description for the new rule.
  Repeat the procedure for Outbound Rules tab.

🔗 New Inbound Rule Wiza	ard	🗙 🔗 New Inbound Rule	🗙 🝘 New Inbound Rule Wizard			
Rule Type		Protocol and Ports	Protocol and Ports			
Select the type of firewall rule to	o create.	Specify the protocols and	Specify the protocols and ports to which this rule applies.			
Steps: Rule Type Protocol and Ports Action Profile Name	What type of rule would you like to create?         Pogram         Rule that controls connections for a program.         P Pol         Rule that controls connections for a TCP or UDP port.         Prodefined:         BanchCache - Content Retrieval (Uses HTTP)         Rule that controls connections for a Windows experience.         Costom         Qustom rule.	Steps: Protocol and Ports Action Profile Name	Does this rule apply to TCP or U	JDP? toots or specific local ports? T35 Example: 80, 443, 5000-5010 Cancel		
🔥 Note						

TCP Port 135 is commonly used for allowing clients to discover and utilize a DCOM service.