Connect to OPC UA Server / Kepware

System Requirements

To make use of this feature, the following system requirements need to be matched.

- KepServerEx V5 (or higher).
- OPC UA Protocol

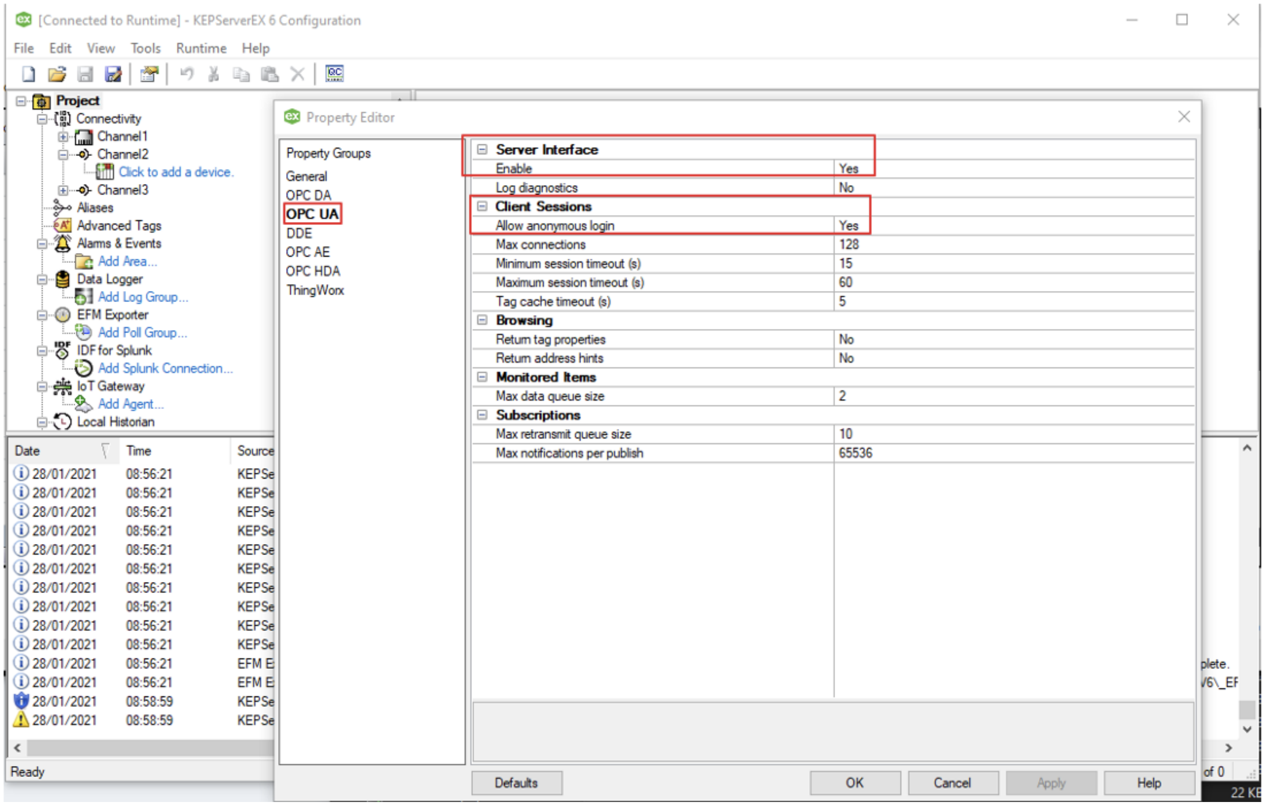
How to Use

The procedure for a successful OPC UA connection is divided into three main steps.

- KepServerEx OPC UA Server Configuration
- Creating certificates for Engineering and Runtime
- Importing client certificates on OPC UA

KepServerEx Configuration

At KepServerEx project properties, enable support for OPC UA. Use the command “Reinitialize” after changing the settings so they can be applied.



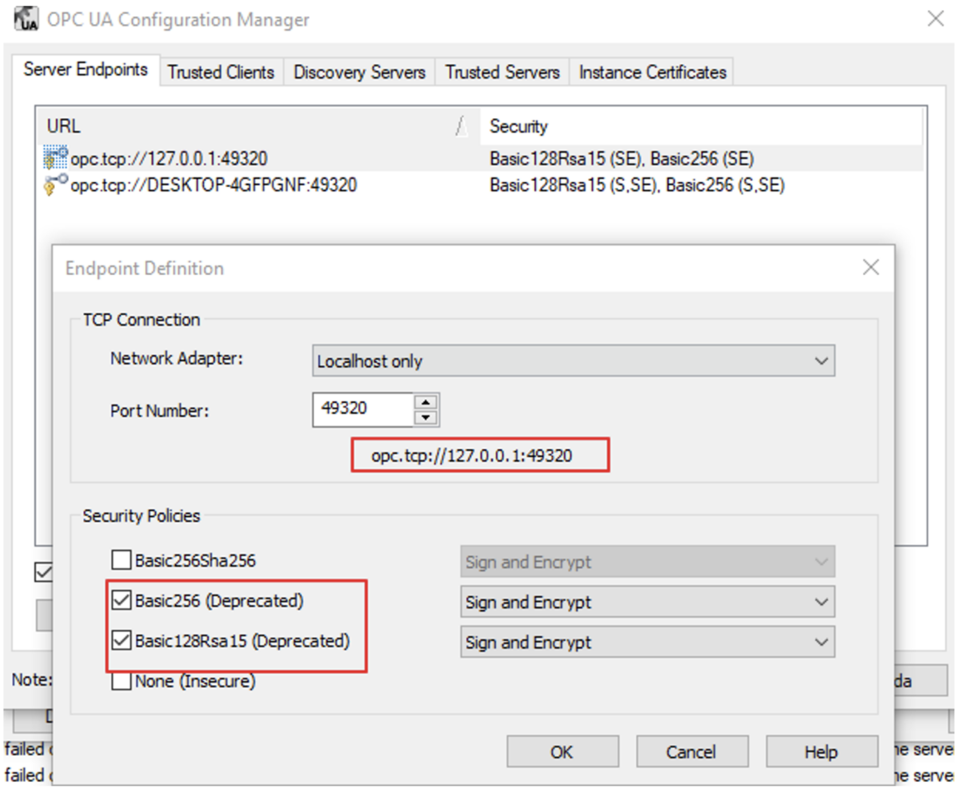
Server Interface	
Enable	Yes
Log diagnostics	No
Client Sessions	
Allow anonymous login	Yes
Max connections	128
Minimum session timeout (s)	15
Maximum session timeout (s)	60
Tag cache timeout (s)	5
Browsing	
Return tag properties	No
Return address hints	No
Monitored Items	
Max data queue size	2
Subscriptions	
Max retransmit queue size	10
Max notifications per publish	65536

Date	Time	Source
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	KEPSe
28/01/2021	08:56:21	EFM E
28/01/2021	08:56:21	EFM E
28/01/2021	08:58:59	KEPSe
28/01/2021	08:58:59	KEPSe

In the Server EndPoints tab, configure the endpoint parameters (network adapter, port number, and security policies) and copy the URL because it will be used later.

For the security policies configuration, you need to enable one (or both) of the following:

- Basic256.
- Basic128Rsa15.



OPC UA Configuration Manager

URL	Security
opc.tcp://127.0.0.1:49320	Basic128Rsa15 (SE), Basic256 (SE)
opc.tcp://DESKTOP-4GFPGNF:49320	Basic128Rsa15 (S,SE), Basic256 (S,SE)

Endpoint Definition

TCP Connection

Network Adapter: Localhost only

Port Number: 49320

opc.tcp://127.0.0.1:49320

Security Policies

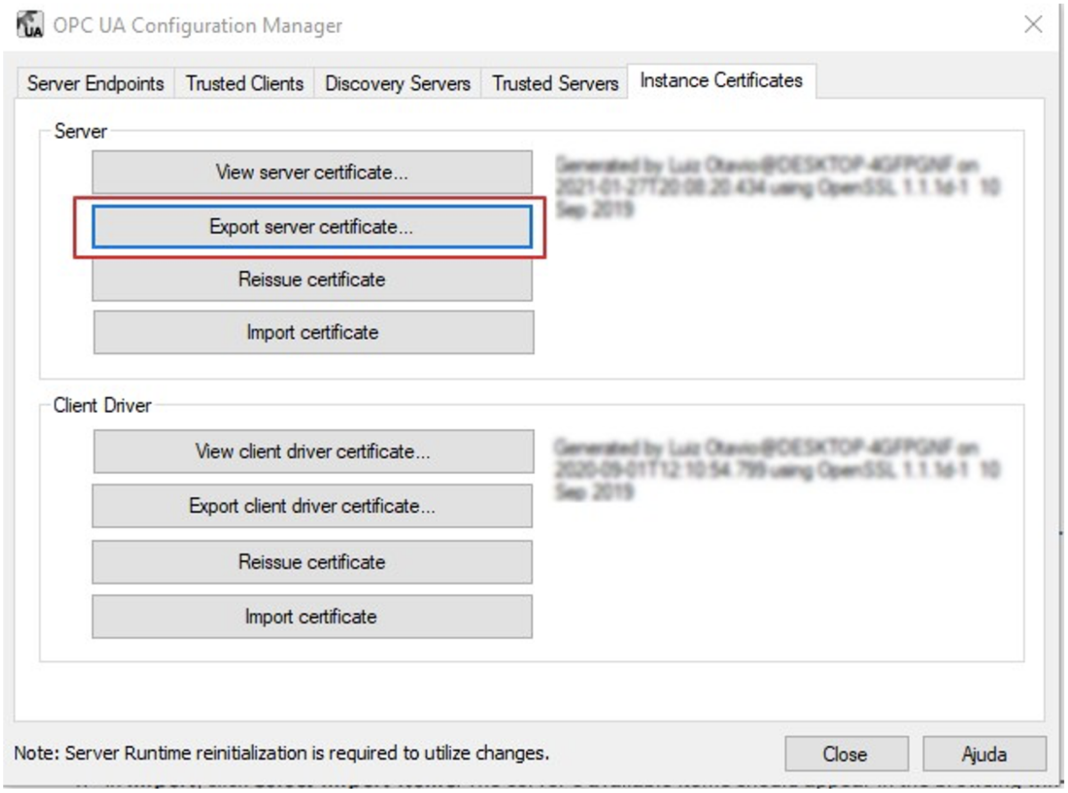
□ Basic256Sha256 — Sign and Encrypt

☑ Basic256 (Deprecated) — Sign and Encrypt

☑ Basic128Rsa15 (Deprecated) — Sign and Encrypt

□ None (Insecure)

On the Instance Certificates page, click on the Export Button and select a folder to save the certificate for the OPC UA Server.



OPC UA Configuration Manager

[redacted]

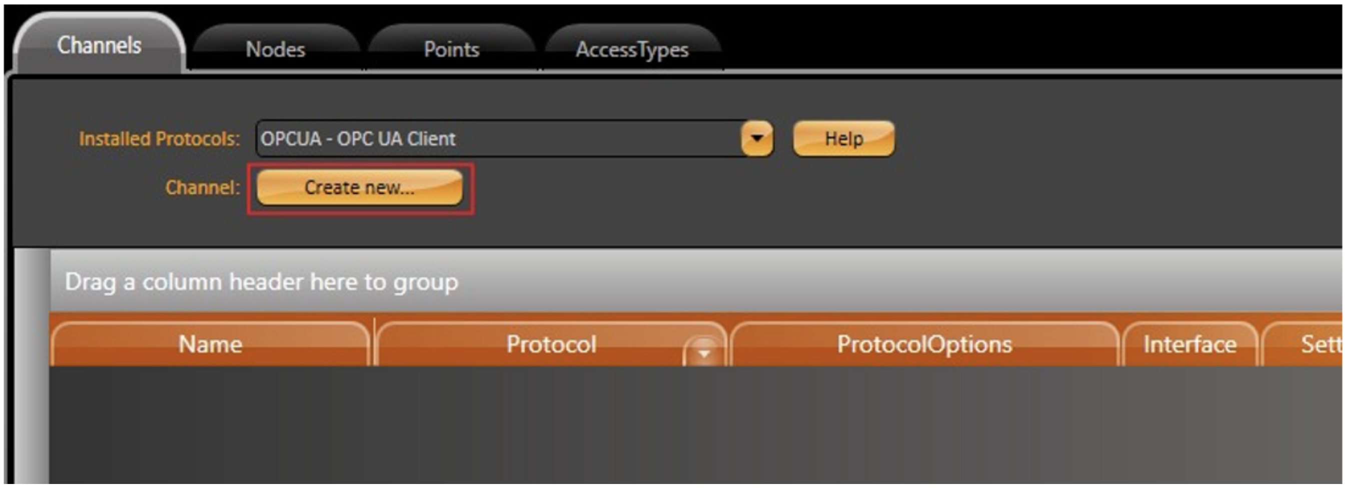
Client Driver
View client driver certificate...
Export client driver certificate...
Reissue certificate
Import certificate

[redacted]

Note: Server Runtime reinitialization is required to utilize changes.

Engineering and Runtime Configuration

In your Project, navigate to **Devices > Channels** and create a new OPC UA channel.



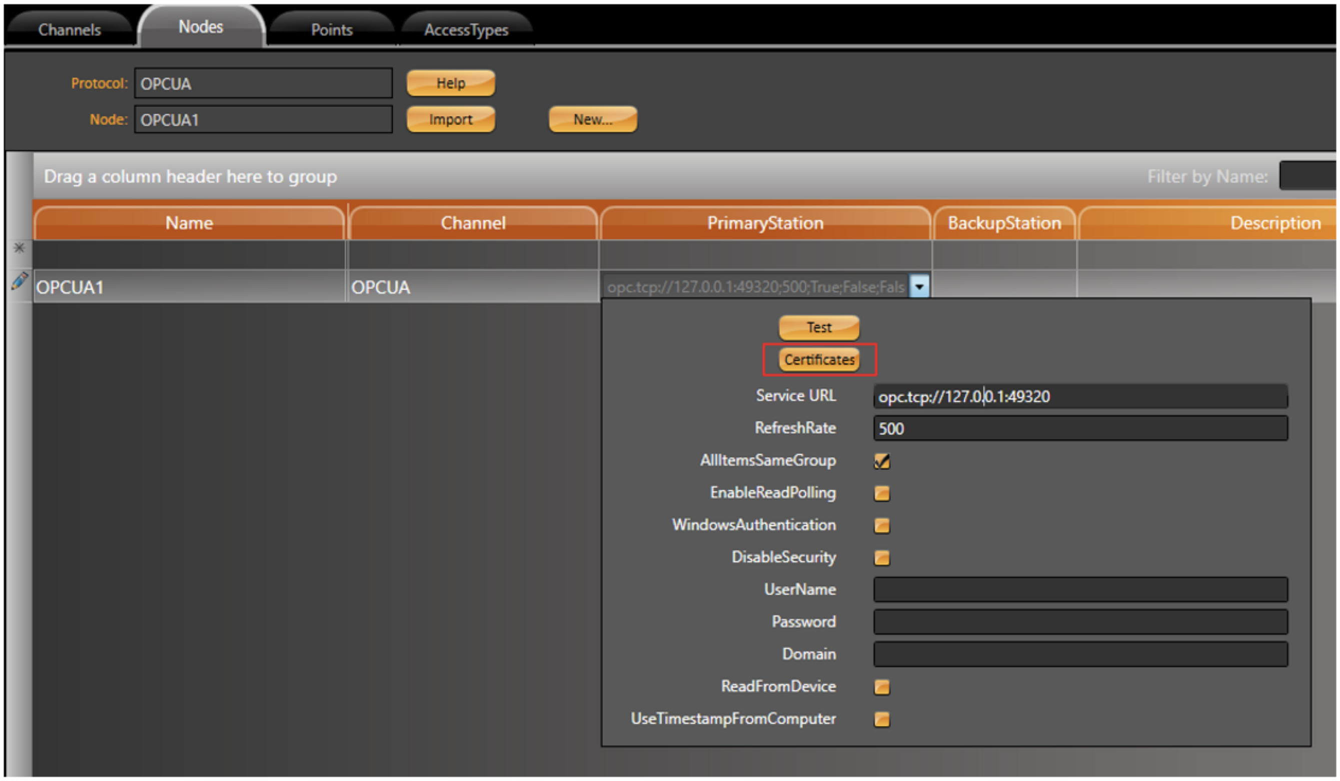
Installed Protocols: OPCUA - OPC UA Client

Channel: Create new...

In **Devices > Nodes**, paste the OPC URL (copied from the previous section) in the *PrimaryStation* configuration popup. Fill in the remaining parameters accordingly.

> ⚠ *For the Server Endpoint URL, you should **NOT** change from 127.0.0.1 to localhost. The Endpoint needs to be the same one used in the Server Instances Tab.*

Then, click on the *Certificates* button to launch the *UaClientConfigHelperNet4.exe* tool. Make sure the file is launched with Administrator privileges.



Protocol: OPCUA

Node: OPCUA1

Name	Channel	PrimaryStation	BackupStation	Description
OPCUA1	OPCUA	opc.tcp://127.0.0.1:49320;500;True;False;Fals		

Service URL: opc.tcp://127.0.0.1:49320

RefreshRate: 500

AllItemsSameGroup: ☑

EnableReadPolling: □

WindowsAuthentication: □

DisableSecurity: □

UserName:

Password:

Domain:

ReadFromDevice: □

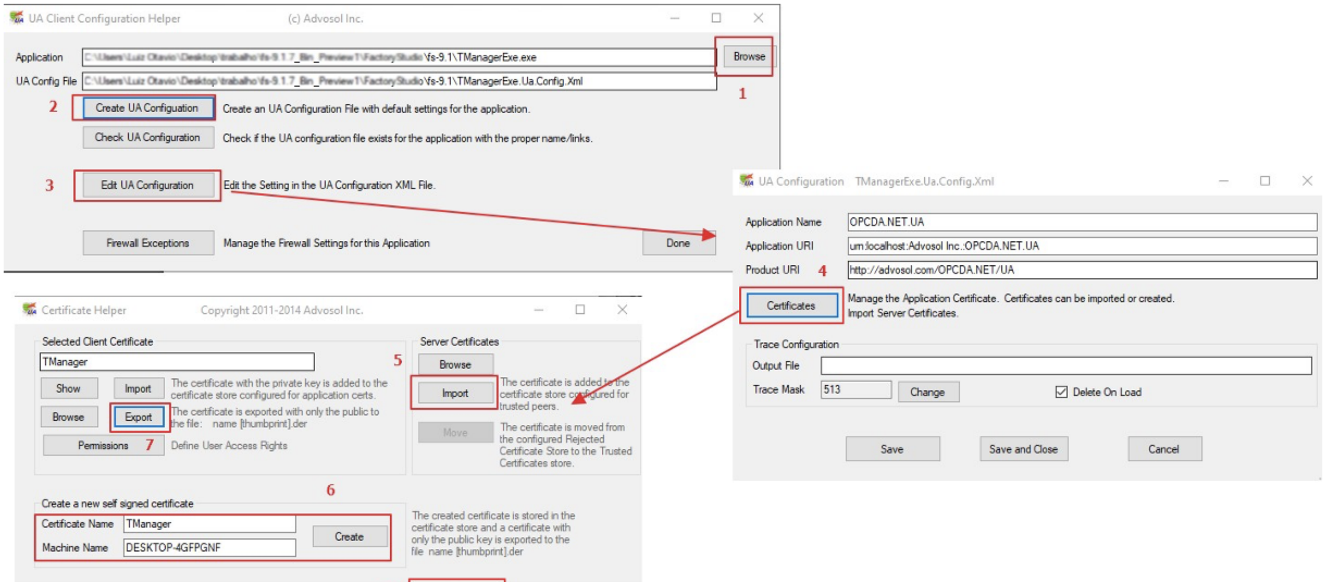
UseTimestampFromComputer: □

> ⚠ *The certification tool can also be launched (with admin rights) from the Product’s installation folder.*
>
> *..\fs-9.1\UaClientConfigHelperNet4.exe*.

The steps to create a certificate are described below:

- With the exe opened, browse for the application (\fs-9.1\TManagerExe.exe).
- Press Create UA Configuration, Edit UA Configuration, and press Certificates.
- Press the Create Button.
- Press “Server Certificates”, the “Import” button, and select the server certificate created by the Kepware application.
- Press “Export”.
- Press “OK”, and “Save and Close”.

The steps above are illustrated in the image below.



UA Client Configuration Helper (c) Advosol Inc.

Application: [redacted]\fs-9.1\TManagerExe.exe

UA Config File: [redacted]\fs-9.1\TManagerExe.Ua.Config.Xml

Create UA Configuation: Create an UA Configuration File with default settings for the application.

Check UA Configuration: Check if the UA configuration file exists for the application with the proper name/links.

Edit UA Configuration: Edit the Setting in the UA Configuration XML File.

Firewall Exceptions: Manage the Firewall Settings for this Application

UA Configuration TManagerExe.Ua.Config.Xml

Application Name: OPCDA.NET.UA

Application URI: urn:localhost:Advosol Inc.:OPCDA.NET.UA

Product URI: http://advosol.com/OPCDA.NET/UA

Certificates: Manage the Application Certificate. Certificates can be imported or created. Import Server Certificates.

Trace Configuration

Output File:

Trace Mask: 513

☑ Delete On Load

Certificate Helper Copyright 2011-2014 Advosol Inc.

Selected Client Certificate: TManager

Import: The certificate with the private key is added to the certificate store configured for application certs.

Export: The certificate is exported with only the public to the file: name [thumbprint].der

Permissions: Define User Access Rights

Server Certificates

Import: The certificate is added to the certificate store configured for trusted peers.

Move: The certificate is moved from the configured Rejected Certificate Store to the Trusted Certificates store.

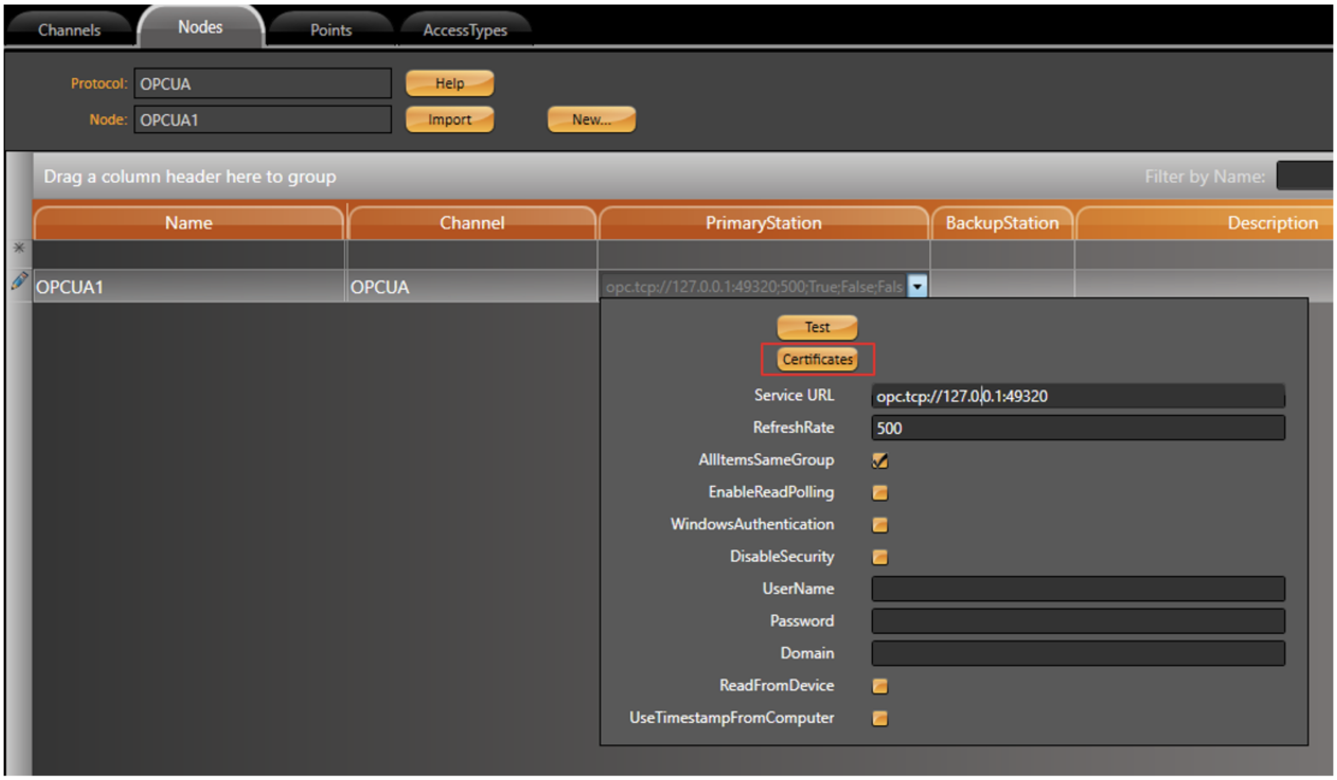
Create a new self signed certificate

Certificate Name: TManager

Machine Name: DESKTOP-4GFPGNF

The created certificate is stored in the certificate store and a certificate with only the public key is exported to the file name [thumbprint].der

⚠ *The same procedure must be repeated for the \fs-9.1\TRunModule.exe* application.



Protocol: OPCUA

Node: OPCUA1

Name	Channel	PrimaryStation	BackupStation	Description
OPCUA1	OPCUA	opc.tcp://127.0.0.1:49320;500;True;False;Fals		

Service URL: opc.tcp://127.0.0.1:49320

RefreshRate: 500

AllItemsSameGroup ☑

EnableReadPolling ☐

WindowsAuthentication ☐

DisableSecurity ☐

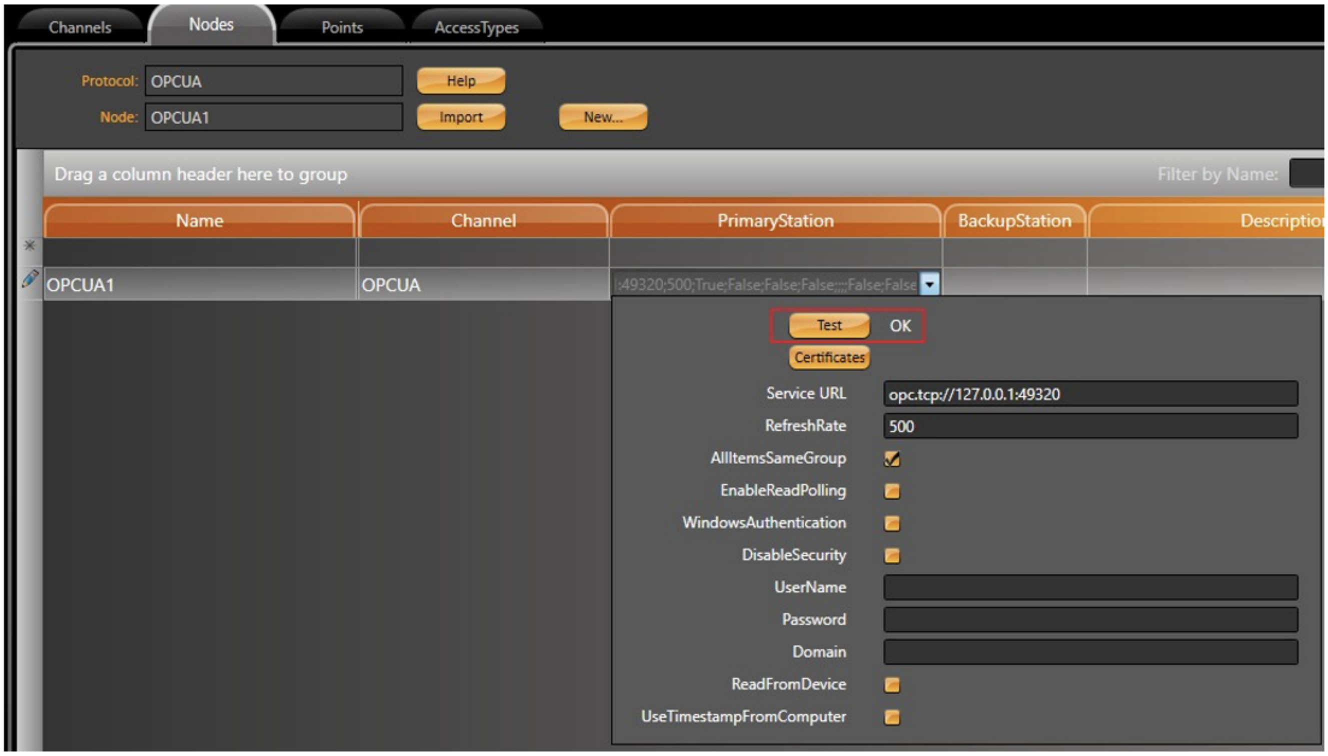
UserName

Password

Domain

ReadFromDevice ☐

UseTimestampFromComputer ☐



Protocol: OPCUA

Node: OPCUA1

Name	Channel	PrimaryStation	BackupStation	Descriptio
OPCUA1	OPCUA	:49320;500;True;False;False;False;;;;False;False		

Test OK

Service URL: opc.tcp://127.0.0.1:49320

RefreshRate: 500

AllItemsSameGroup ☑

EnableReadPolling ☐

WindowsAuthentication ☐

DisableSecurity ☐

UserName

Password

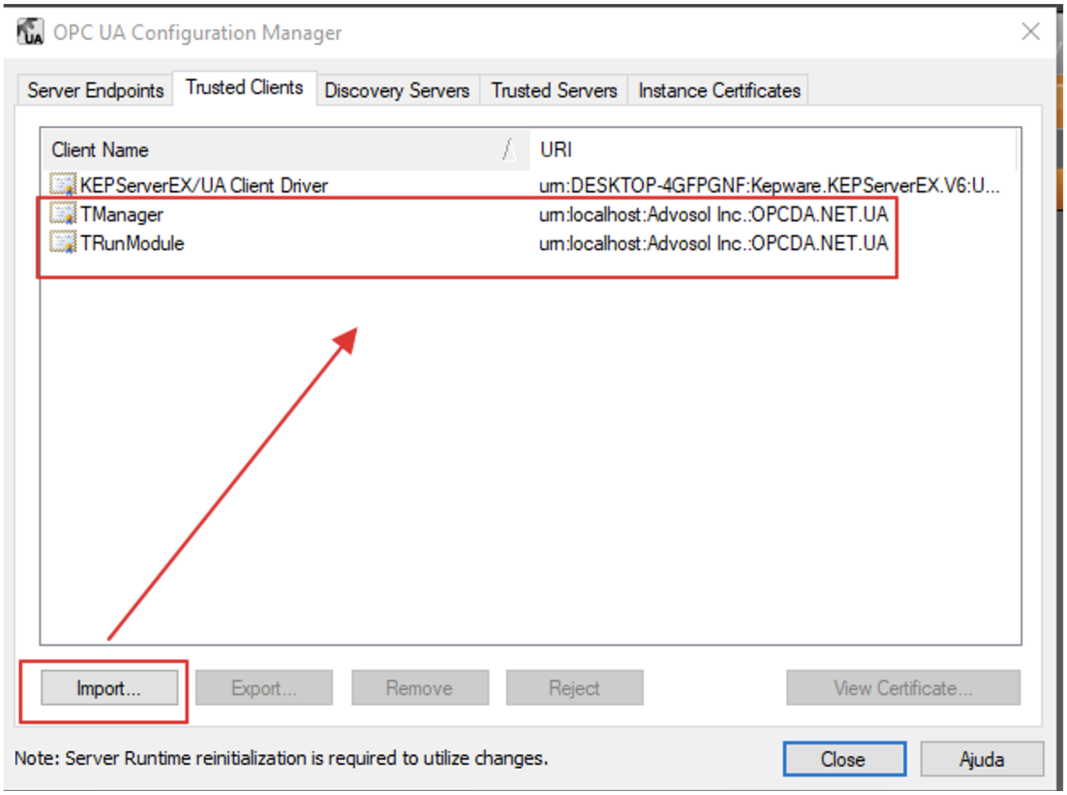
Domain

ReadFromDevice ☐

UseTimestampFromComputer ☐

Importing Client certificates and Testing Connection

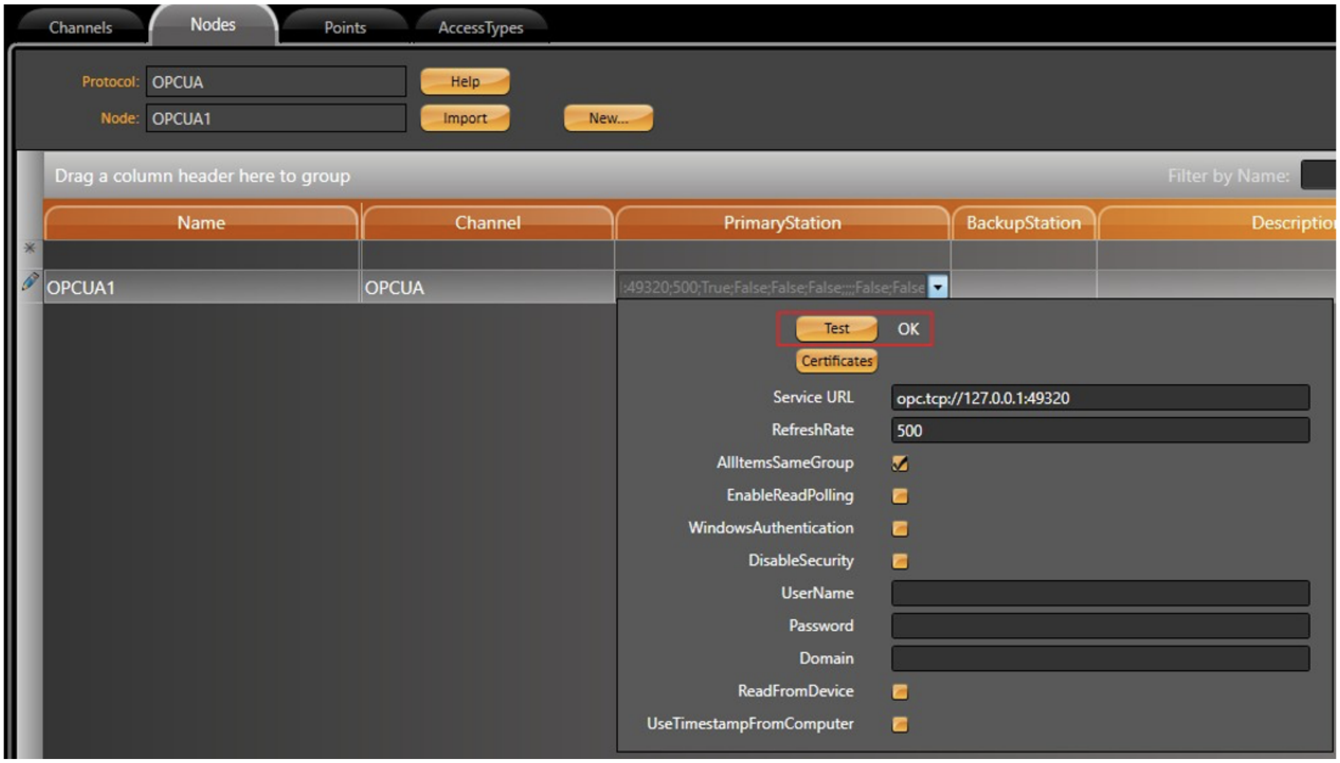
Back at KepServerEx, import the two certificates created in the previous section. Go to the OPC UA Configuration Manager - Trusted Clients Tab.



Client Name	URI
KEPServerEX/UA Client Driver	urn:DESKTOP-4GFPGNF:Kepware.KEPServerEX.V6:U...
TManager	urn:localhost:Advosol Inc.:OPCDA.NET.UA
TRunModule	urn:localhost:Advosol Inc.:OPCDA.NET.UA

Note: Server Runtime reinitialization is required to utilize changes.

Once the certifications have been trusted, we can test our connection. On the Project's **Devices > Nodes** page, open the PrimaryStation configuration popup and click on Test button. If this was done correctly, you should see an OK status.



Protocol: OPCUA

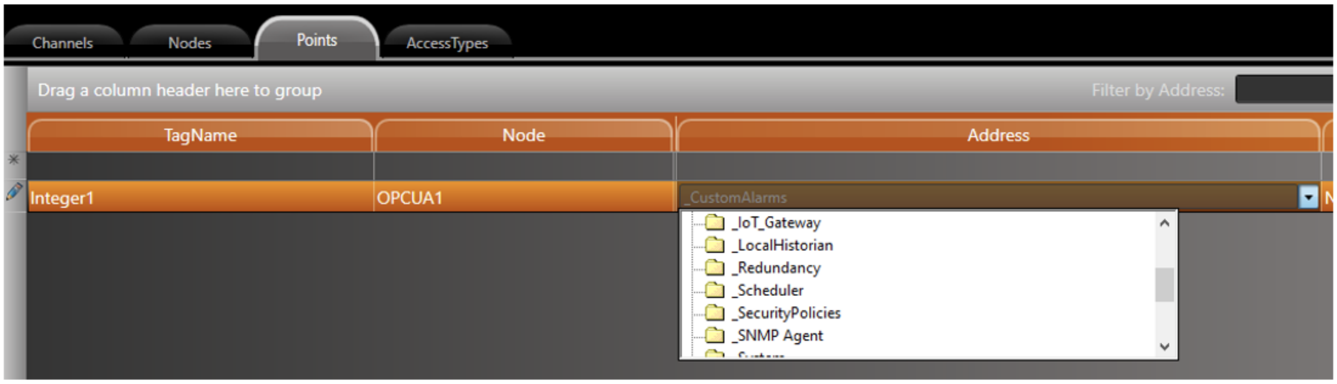
Node: OPCUA1

Name	Channel	PrimaryStation	BackupStation	Descriptio
OPCUA1	OPCUA	:49320;500;True;False;False;False;;;;False;False		

OK

Service URL: opc.tcp://127.0.0.1:49320
RefreshRate: 500
AllItemsSameGroup ☑
EnableReadPolling ☐
WindowsAuthentication ☐
DisableSecurity ☐
UserName
Password
Domain
ReadFromDevice ☐
UseTimestampFromComputer ☐

Lastly, on **Devices - Points**, create a row for our OPC Node and assign a Tag to it. In the *Address* column, you will be able to browse for every available Tag found on the Server in a TreeView style popup.



TagName	Node	Address
Integer1	OPCUA1	_CustomAlarms

OPCServer Available Data

If the available data in the OPCServer is from internal data (server information and diagnostics) or if the available data is from a simulation channel, the data can be exchanged by exception and the FS Node “Enable Read Polling” checkbox can be disabled.

If you are using the “Kepware OPC UA Client” or another device, you will need to enable the FS Node “Enable Read Polling” checkbox.

WE SUGGEST TESTING TO MAKING SURE THE CONNECTION AND DATA EXCHANGE IS WORKING PROPERLY and READING THE INTERNAL DATA FROM THE OPCSERVER KEPWARE. _System._Time_Second OR ANY SIMULATION VALUE.