

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

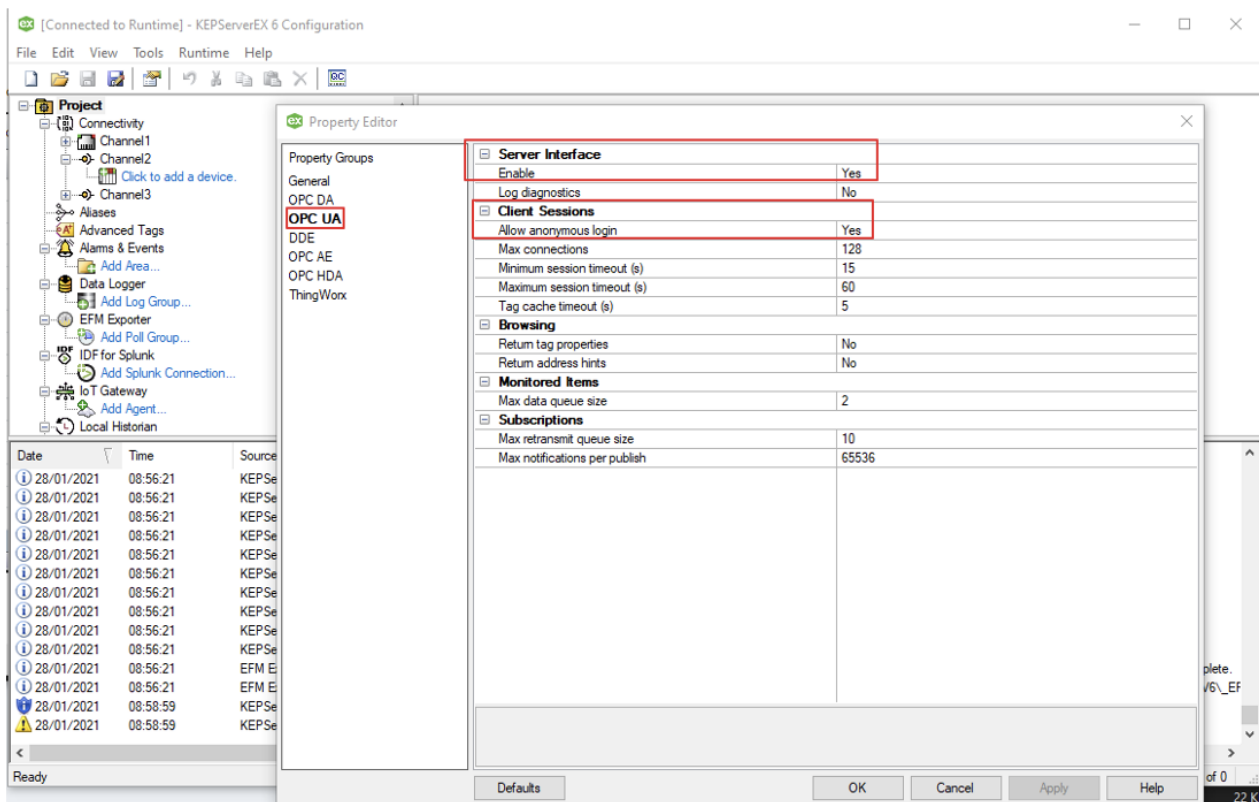
How to Use

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

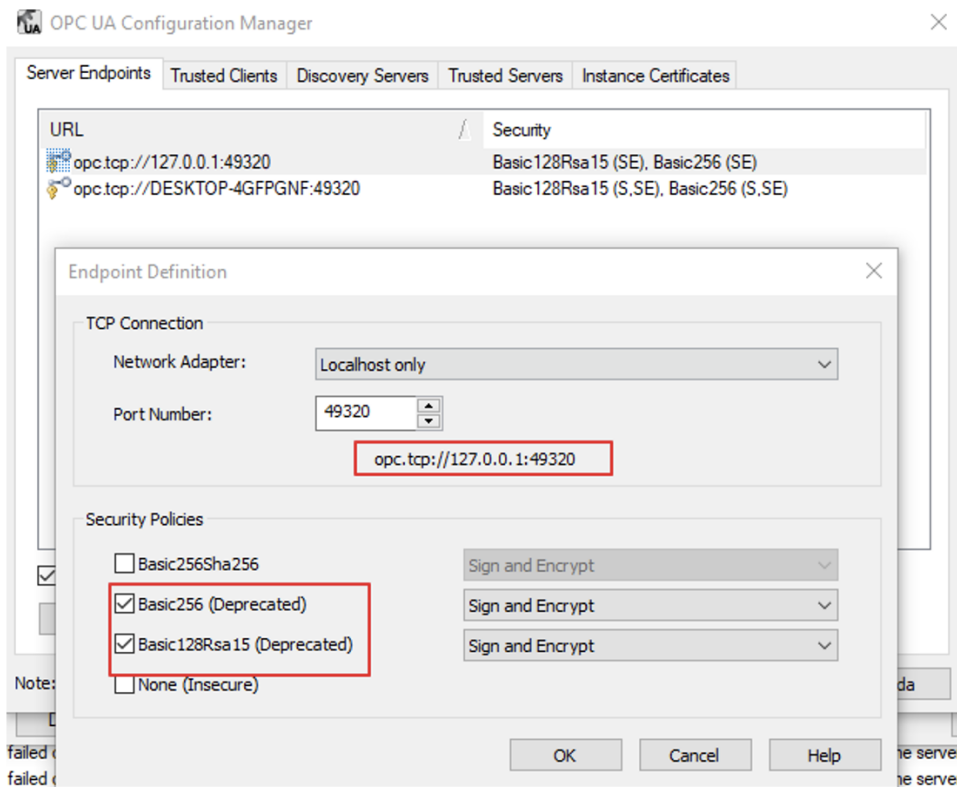
At KepServerEx project properties, enable support for OPC UA. Use the command "Reinitialize" after changing the settings so they can be applied.



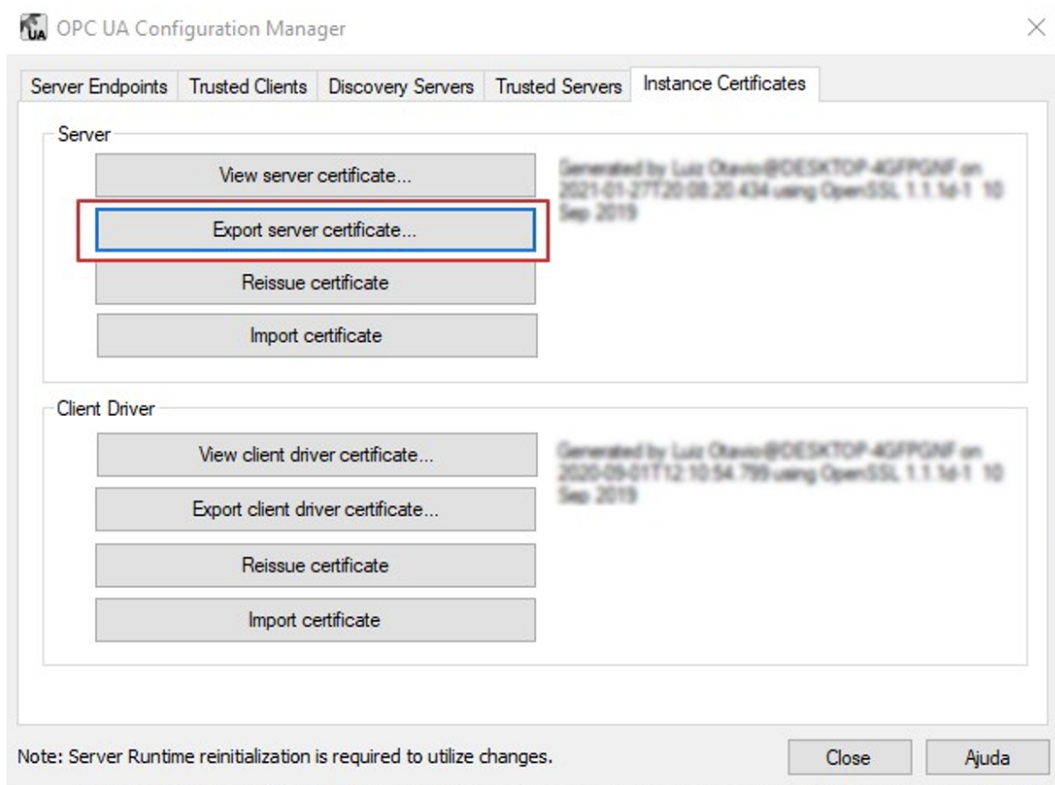
In the Server EndPoints tab, configure the endpoint parameters (network adapter, port number, and security policies) and copy the URL because it will be used later.

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

- Basic256.
- Basic128Rsa15.

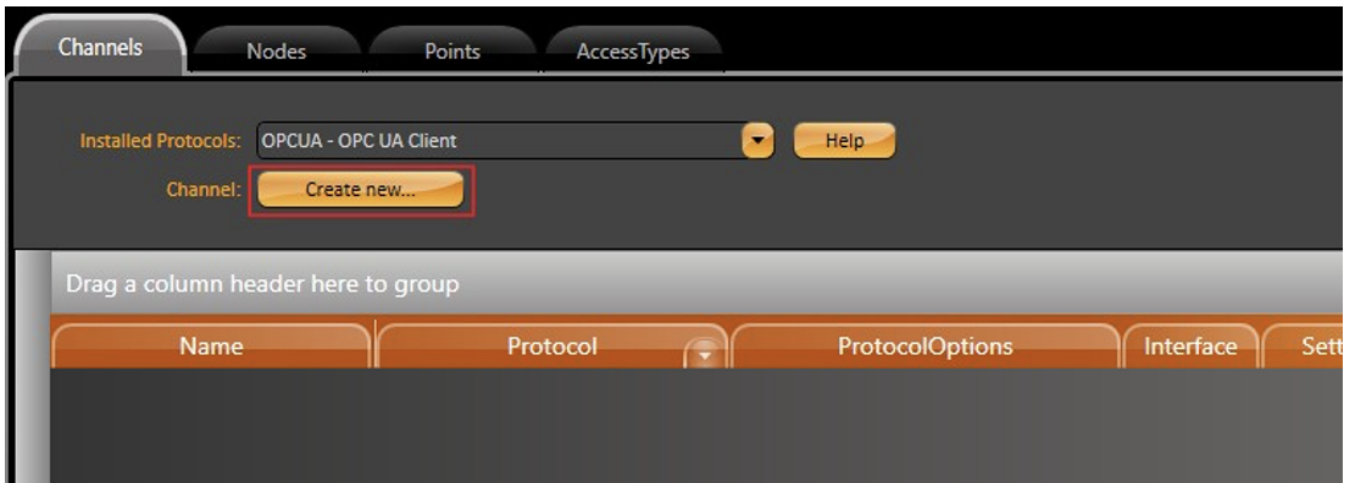


On the Instance Certificates page, click on the Export Button and select a folder to save the certificate for the OPC UA Server.



Engineering and Runtime Configuration

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

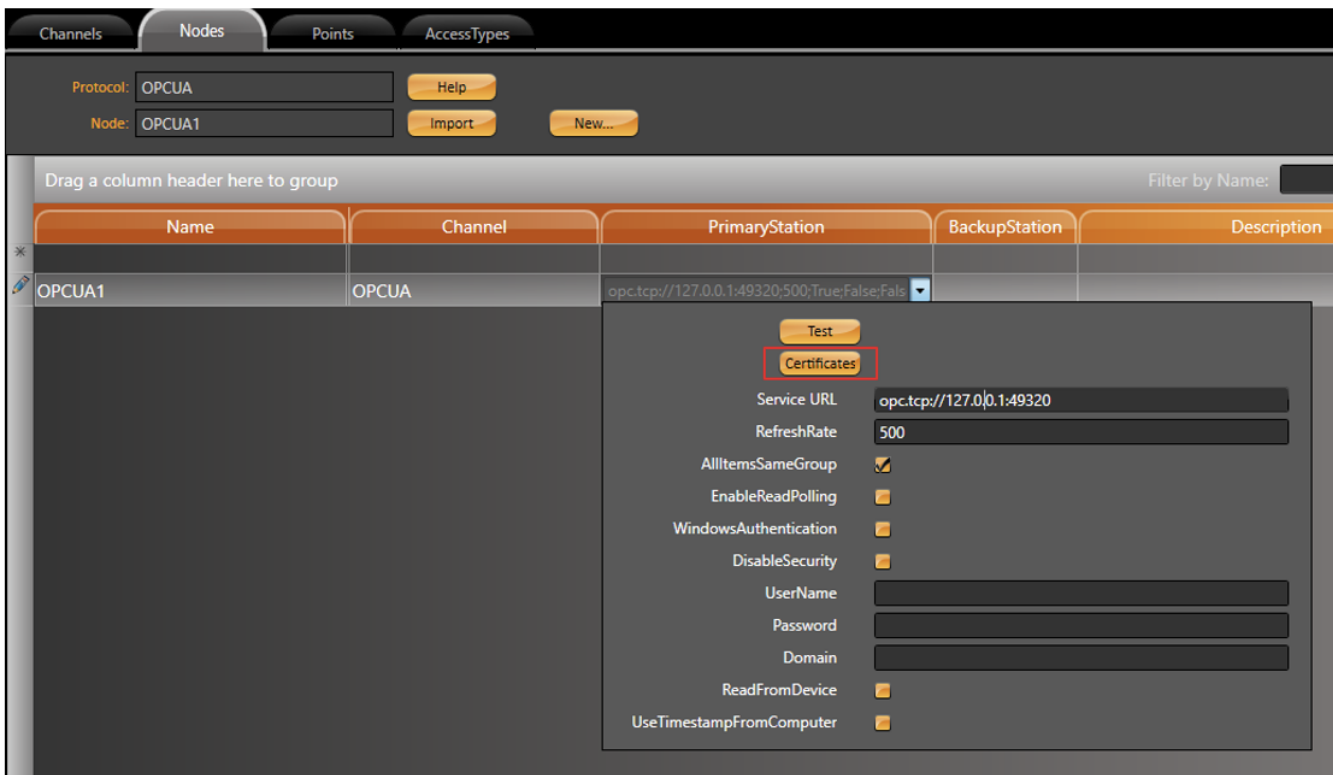


In **Devices > Nodes**, paste the OPC URL (copied from the previous section) in the *PrimaryStation* configuration popup. Fill in the remaining parameters accordingly.



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.



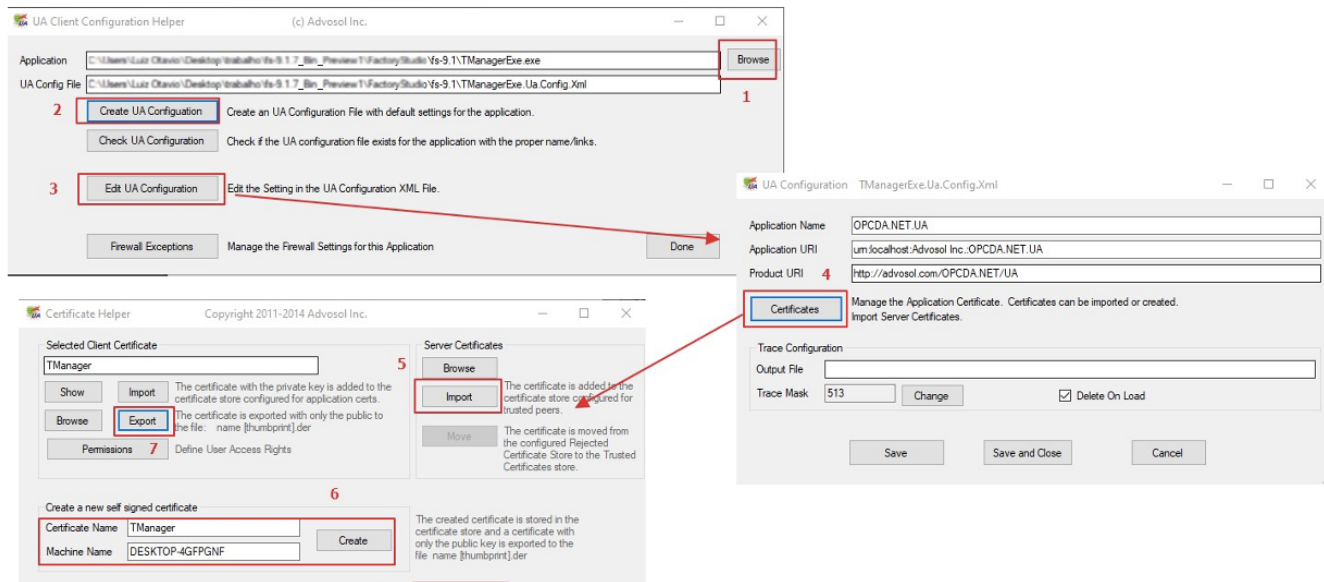
The certification tool can also be launched (with admin rights) from the Product's installation folder.

..\\fs-9.1\\UaClientConfigHelperNet4.exe.

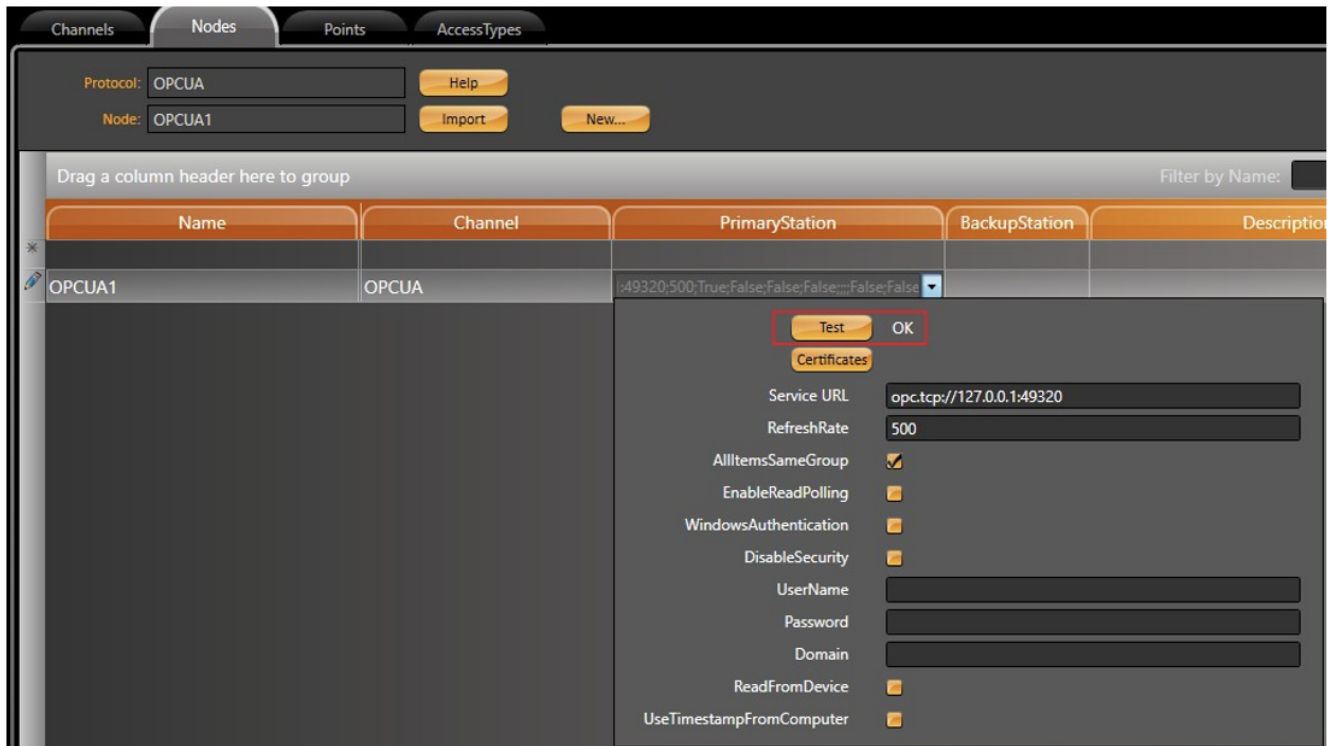
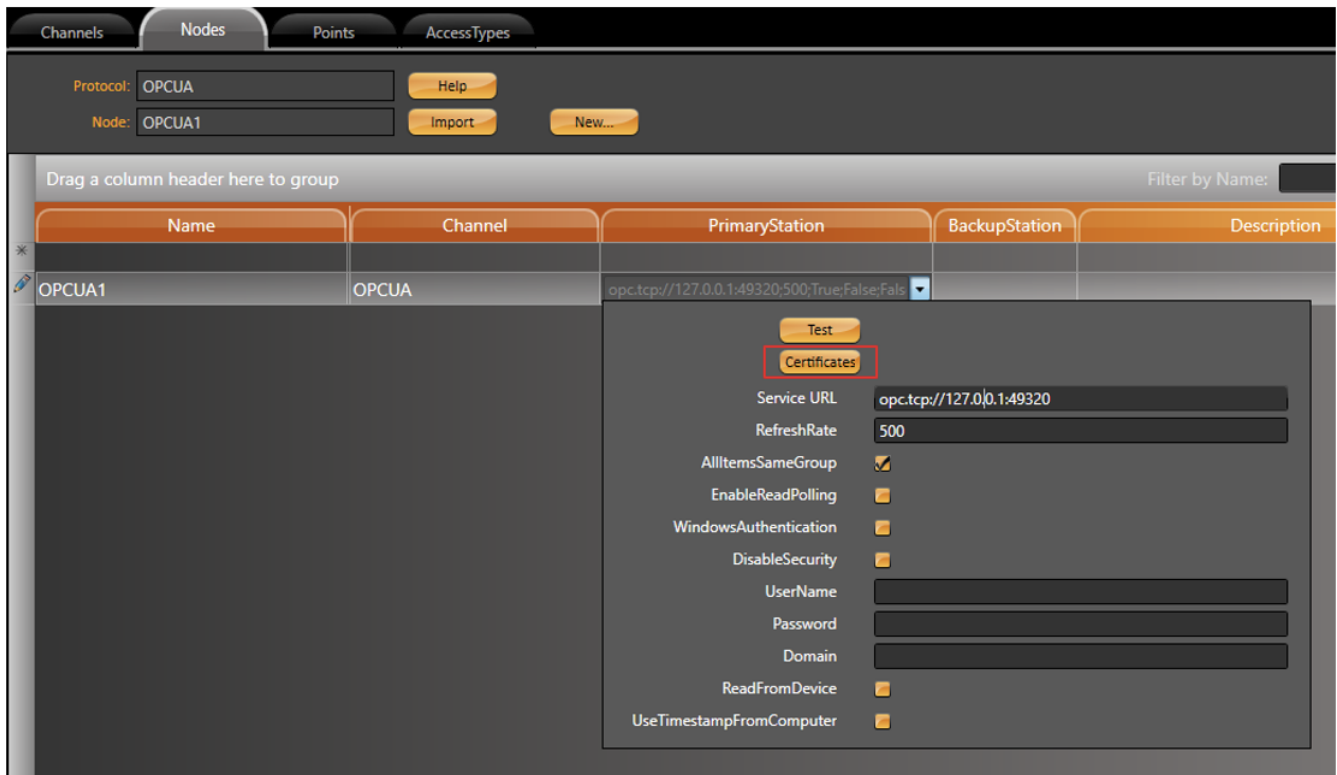
The steps to create a certificate are described below:

- 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.

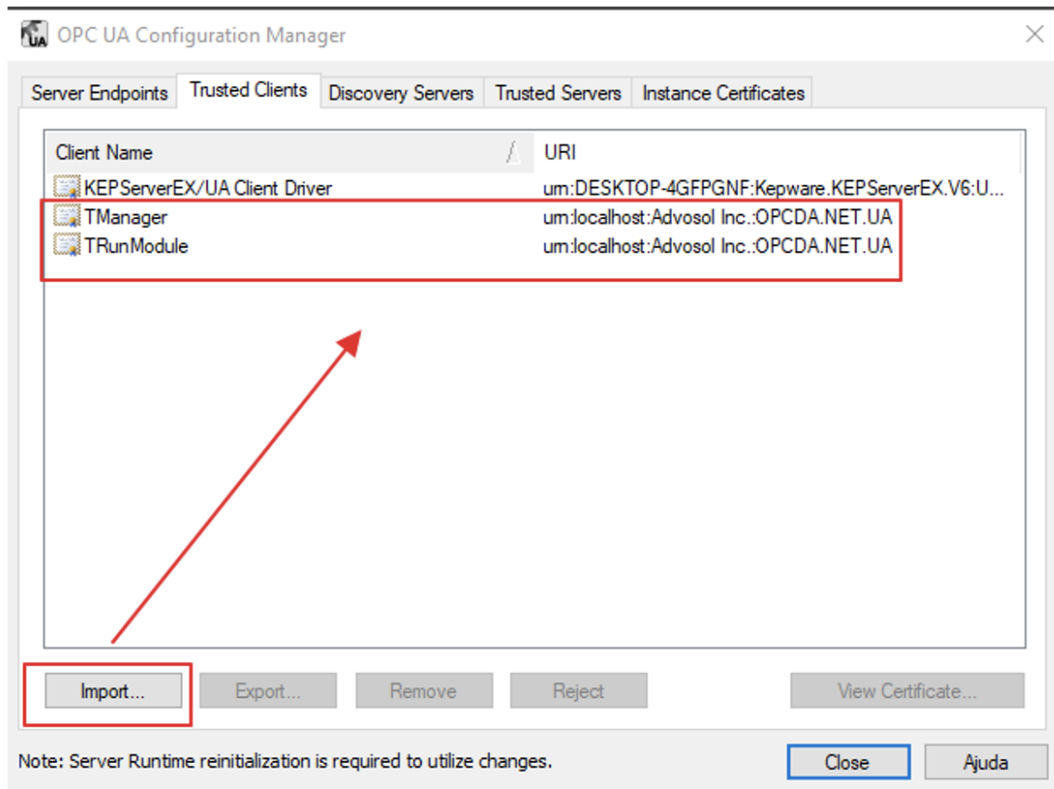


The same procedure must be repeated for the \\fs-9.1\\TRunModule.exe application.

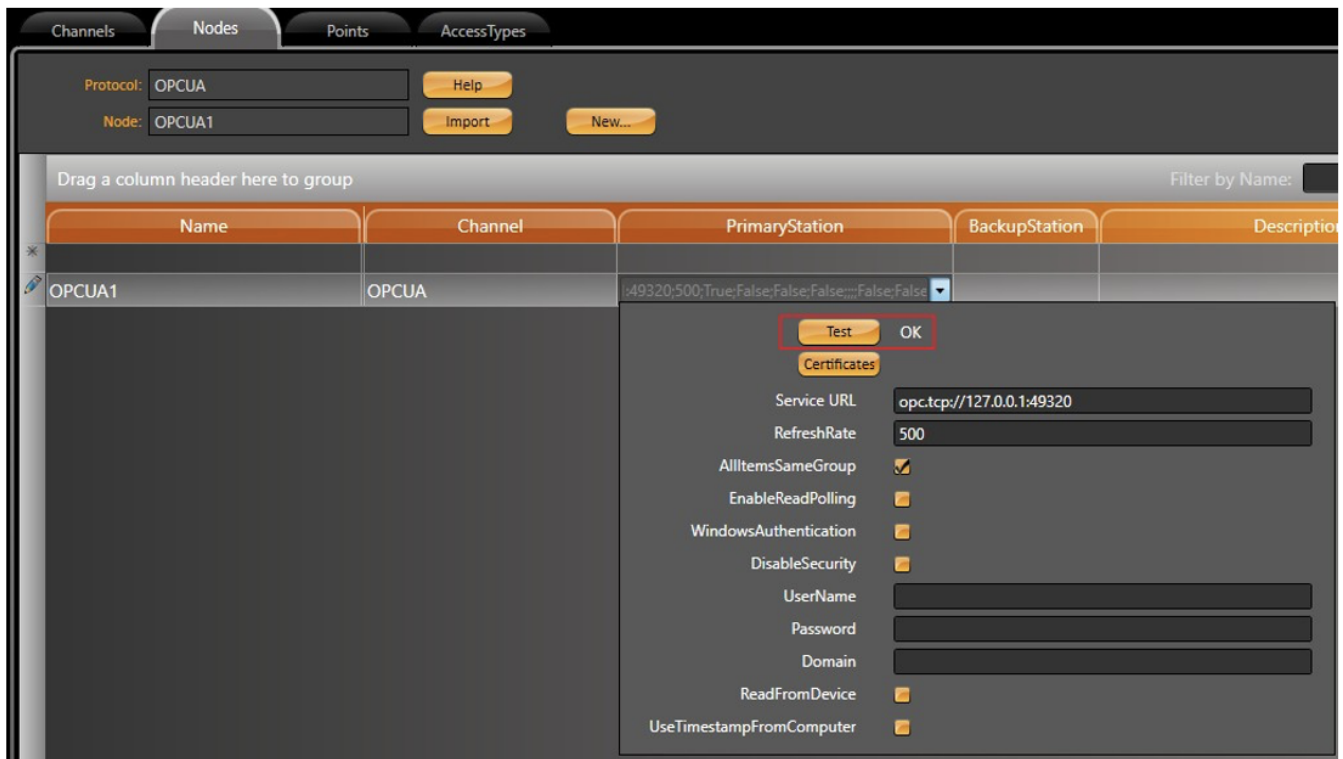


Importing Client certificates and Testing Connection

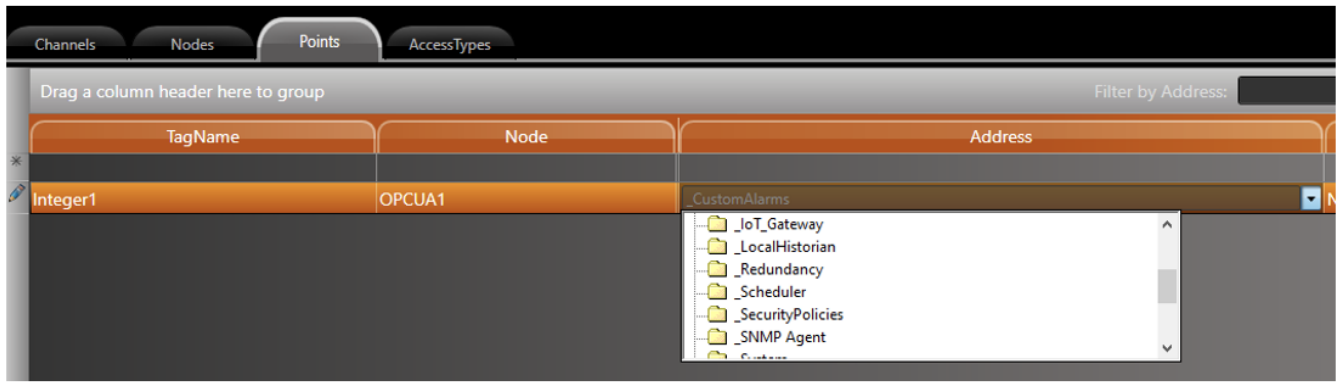
Back at KepServerEx, import the two certificates created in the previous section. Go to the OPC UA Configuration Manager - Trusted Clients Tab.



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.



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.



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.