OPCUA Server

straton user guide – Rev. 6

sales@straton-plc.com

straton

straton

Content

1. Overview

This document describes how to start with the straton OPC UA Server. It also describes how to test that OPC UA Server is working as expected, using a free OPC UA Client software.

Note: This tutorial concerns the OPC UA configurator from the version 11.0 (and newer) of straton.
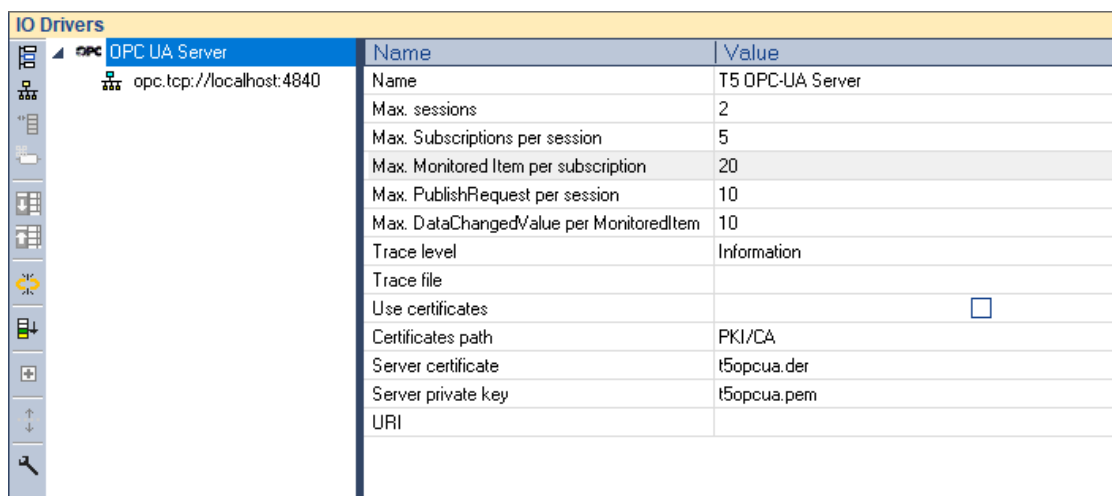
2. Requirement and setup

Download and install straton products from https://straton-plc.com/en/downloads/

3. Create and configure an application

3.1. Create configuration

Open the Fieldbus Configurations ( ) and add an "OPC UA Server" configuration.

If OPC UA certificates are used (check box "Use certificates"):

- The folder "PKI/CA" **must** be created in the working directory of the runtime.

- The certificate "t5opcua.der" (property "Server certificate") **must** be installed in "PKI/CA/certs" folder.

- Private key "t5opcua.pem" (property "Server private key") **must** be installed in "PKI/CA/private" folder.

- URI property : you have to write the same string as in your certificate "t5opcua.der".
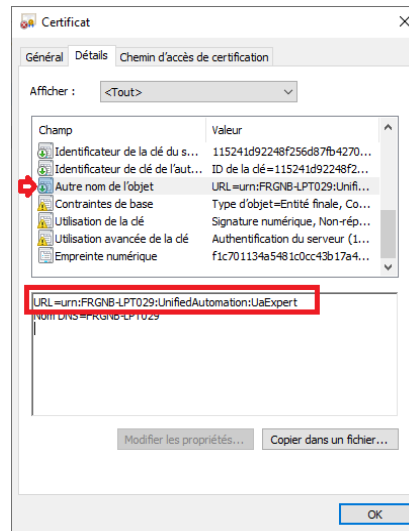
If the 'PKI' and 'CA' folders does not exist, straton will create it.

By default the runtime's working directory is the folder from where it is launched and where the application is downloaded (t5.cod etc.).

On Linux runtimes, it can be forced when launching the runtime. For OPC UA it corresponds to the `/pathopcua=xxx/` option.

For example:

```
# ./t5runtime /pathopcua=/home/workingpath/
```

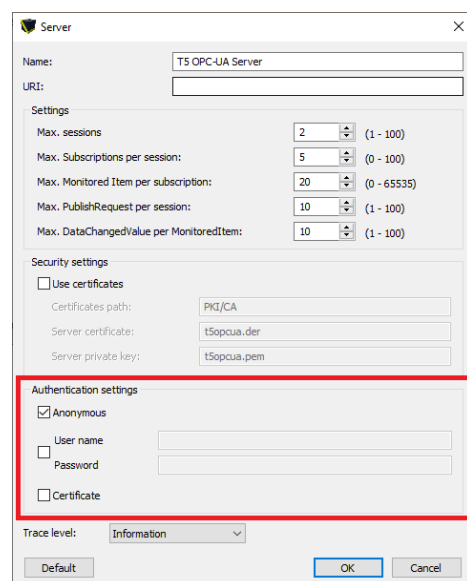Certificate will be installed here: "`/home/workingpath/PKI/CA/certs/`"

Private Key will be installed here: "`/home/workingpath/PKI/CA/private/`"

Authentication settings.

There are three ways for authentication:

- Anonymous
- User name / password
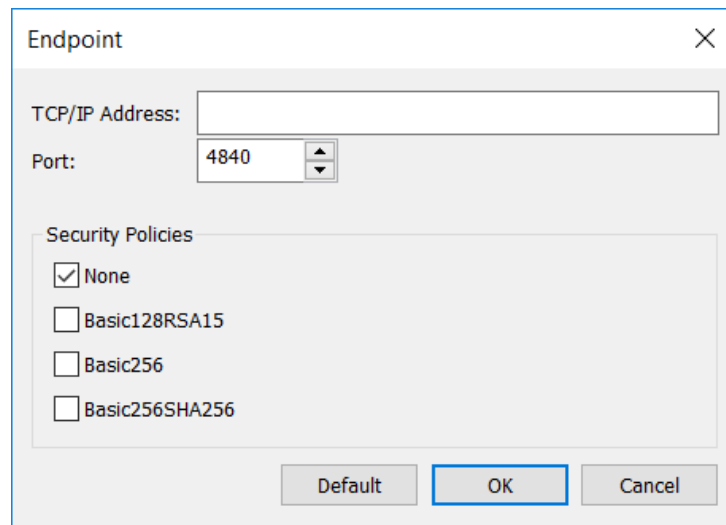- Certificates. Server allows client to authenticate with certificate.

These three methods can be cumulated.

3.2. Configure the application

Double-click on the second level of the configuration and configure:

▸ The TCP/IP Address of the runtime/target – It is advised to leave this field empty; in this case, the URL used by server will be the server host name.

▸ The Port that will be opened by the OPC UA Server

▸ If certificates are used (checkbox on the level 1 of the configuration), configure the Security Policies to be used by the Server.
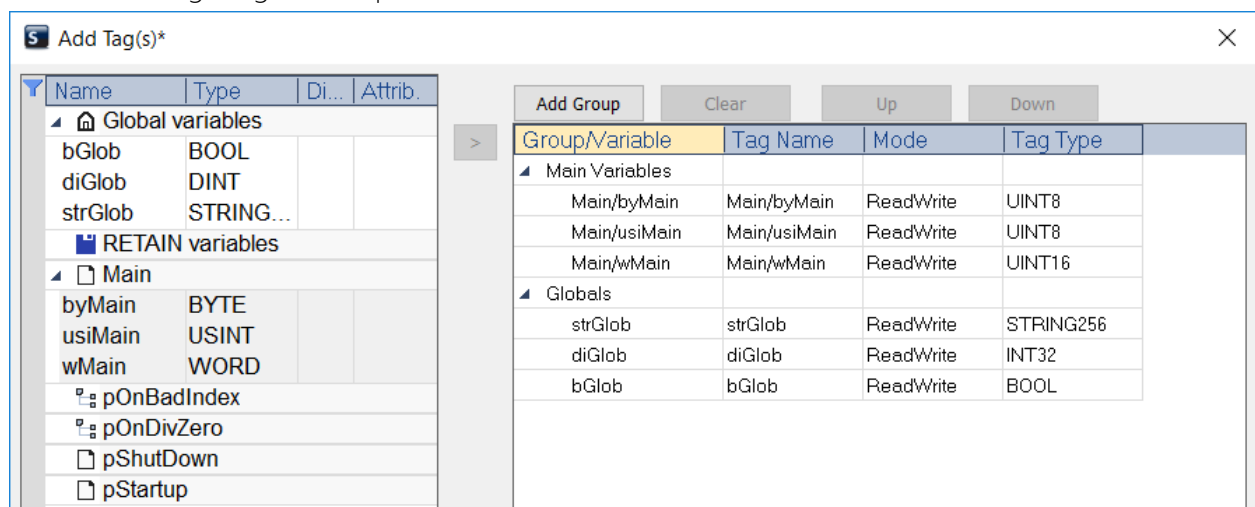

Once this is done, right-click on the level 2 of the configuration and 'Add Tags'

A popup window opens, simply map your variables from the left area to the right area, using the '>' button or doing drag and drops:

Note: Groups can be created in order to have a clear overview

After validating, the configuration tree is automatically created:
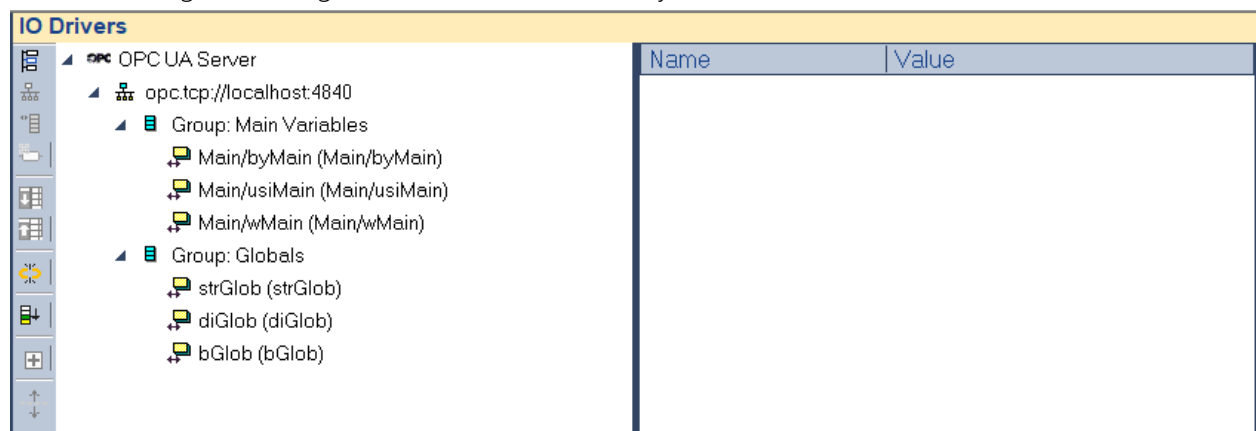
3.2.1. Server Parameters

In straton you can change some parameters of the OPC UA server.

Name	Value
Name	Straton Opc UA Server
Max. sessions	2
Max. Subscriptions per Session	5
Max. Monitored Item per Subscription	20
Max. PublishRequest per Session	10
Max. DataChangedValue per MonitoredItem	10
Trace Level	Information
Password	
Use certificates	☐
Certificates path	PKI/CA
Server certificate	stratonopc.der
Server private key	stratonopc.pem

Max. sessions: Maximum number of clients which can be connected to the server at the same time

Max. Subscriptions per Session: Maximum number of groups (subscriptions) that a client can use on his side

Max. Monitored Item per Subscription: Maximum number of item which can be monitored by a client in a single group

Max. PublishRequest per Session: Maximum number of active PublishRequests. Requests are send to the Server immediately after creating a Subscription.
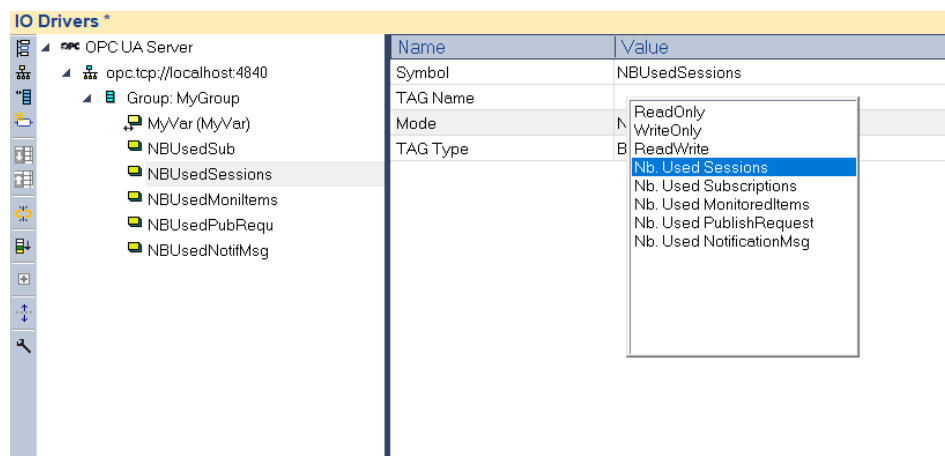
Max. DataChangedValue per MonitoredItem: Maximum number of value changes (for each monitored item) stored in the memory

Password: set a password

3.2.2. Status Variable

Some status variables are available in straton.

To add them to the application, create a new variable and change the desired mode:

Here is what the variables correspond to:

Nb. Use Sessions: displays the number of clients connected (sessions) to the server

Nb. Used Subscriptions: displays the number of groups (subscriptions) that a client use on his side

Nb. Used MonitoredItems: displays the number of monitored items to the server

Nb. Used PublishRequest: displays the current managed requests in the server

Nb. Used NotificationMsg: displays the current number of notification messages send by the server

3.3. Building and download the application

Download the application to the runtime:

▸   Select the communication parameters in menu Tools/Communication Parameters

▸   Establish the connection through menu Project/Online

RESULT IS:

The download is successful and application starts correctly.

The runtime is not started or communication parameters are wrong.

The application is not yet downloaded or an error occurs during startup. More detail can be found in the output view.

After downloading and starting the application, if no existing certificates were found in the "PKI" folder, then straton must have created it automatically.

IMPORTANT: If certificates already exists but these are not the straton ones, it is possible that the runtime does not manage to create the straton certificates.
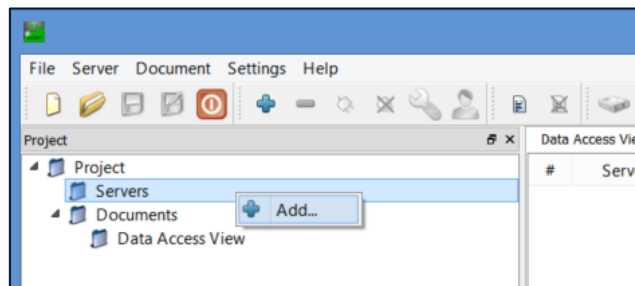
4. Connect to the Server via UA Expert

4.1. Case when certificates are not used

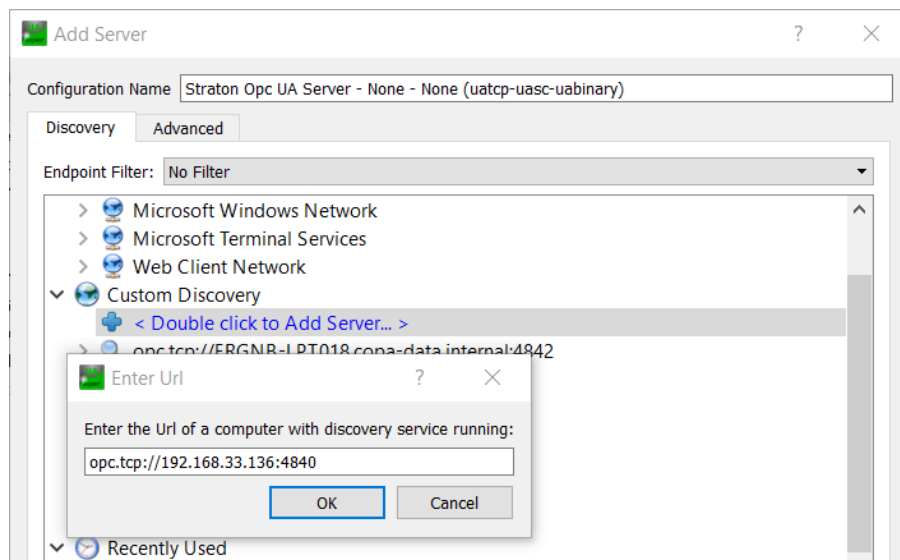In this example the OPC-UA Client is "UA Expert".

After installing UA-Expert and launching it, it will ask to create some OPC-UA certificates, press OK.
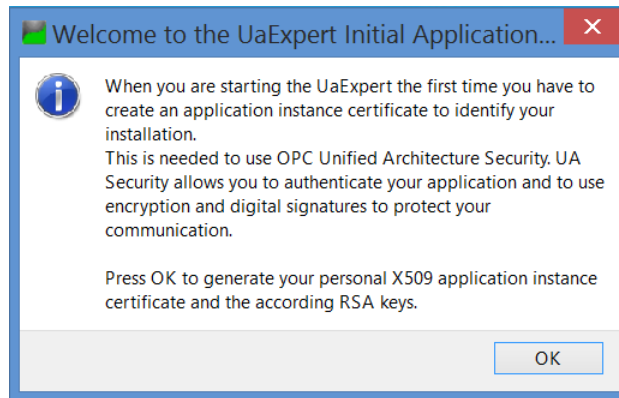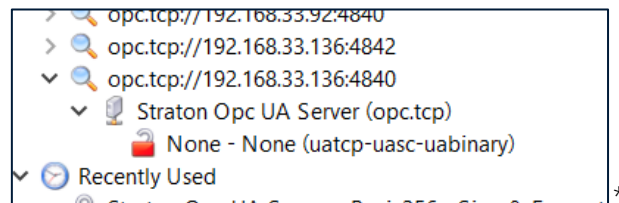

Right-click on the "Servers" to add your OPC-UA Server.

Double click in the Custom Discovery and fill the Server URL to add the OPC-UA Server
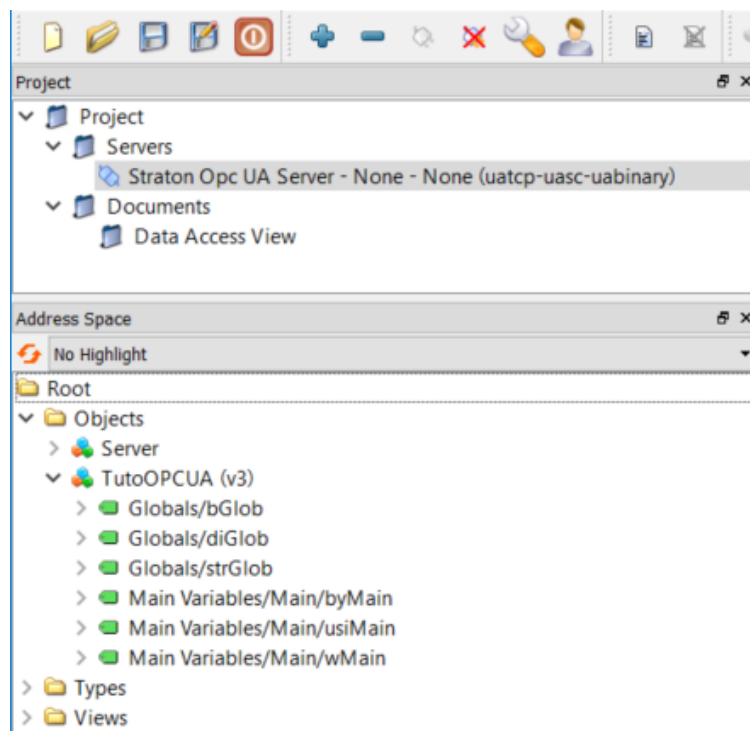
In this test case, no certificates are used, thus UA Expert shows:
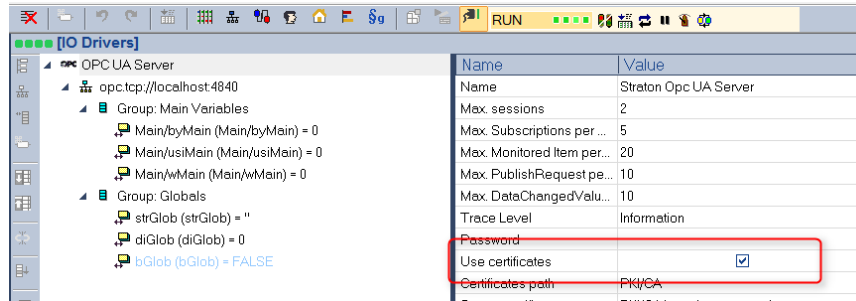

Double click on None.

The Server is now available in the UA Expert project.

Click on the Connect button ( ) to connect to the Server. Data are now available from the straton OPC UA Server:
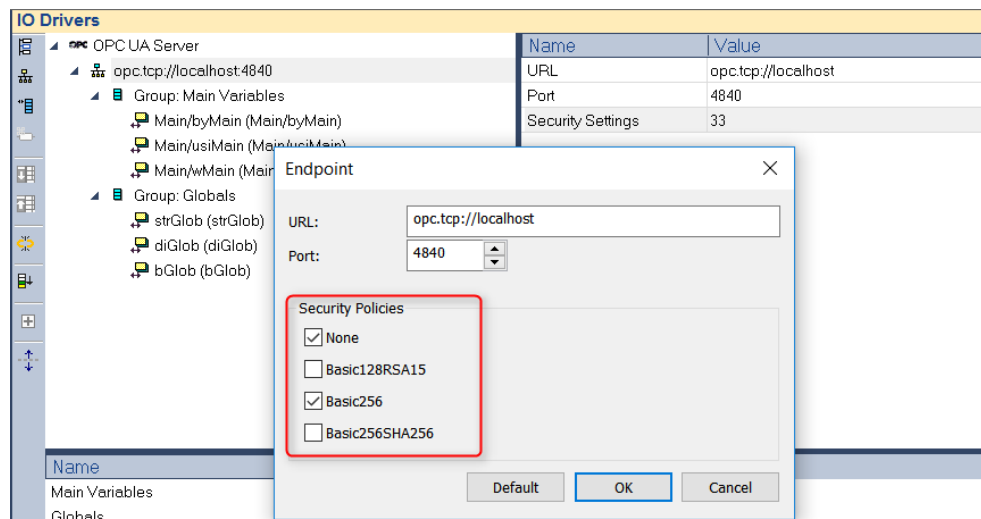
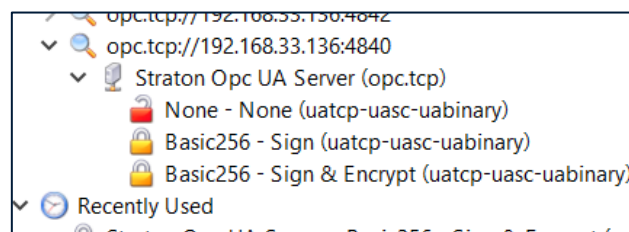## 4.2. Case when certificates are used

If certificates are used, read the previous part anyway in order to understand this one.

The default Security Settings in the straton OPC UA Server configuration must be changed, for example:
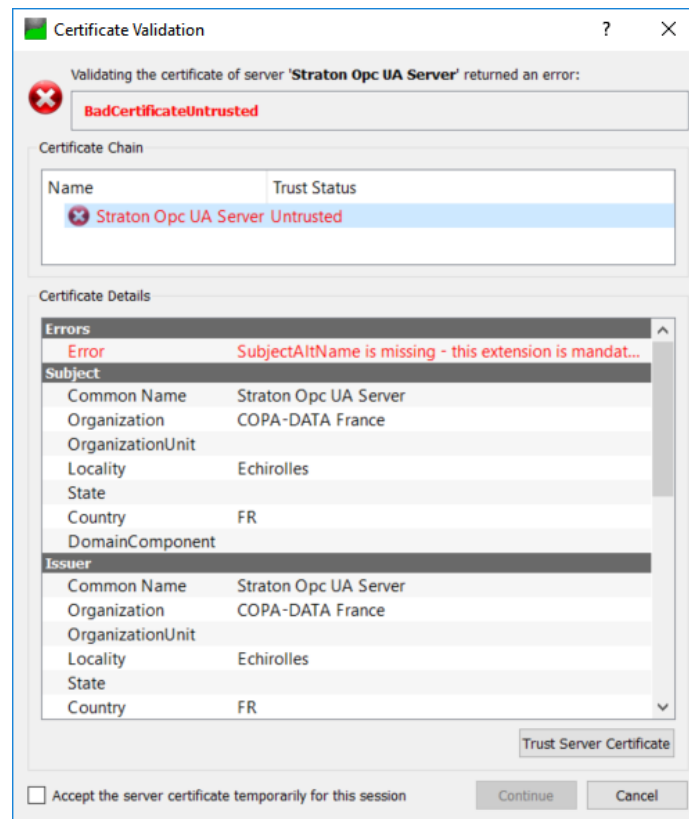

When browsing the Server, UA Expert will now show:

Double click on a Basic256 configuration to add the Server.

Click on the Connect button (   ) to connect to the Server.

If the Server certificate is untrusted, click on "Trust Server Certificate" and "Continue".

The Server is now available on the left side of the window, right-click on it and "Connect" (or use the connect button). The connection should fail because the Server does not recognize the Client. In this case, the Client certificate must be copied at the same place as the Server certificate. To do so in UA Expert, open the 'Settings > Manage certificates' and click on the 'Open certificates location' button
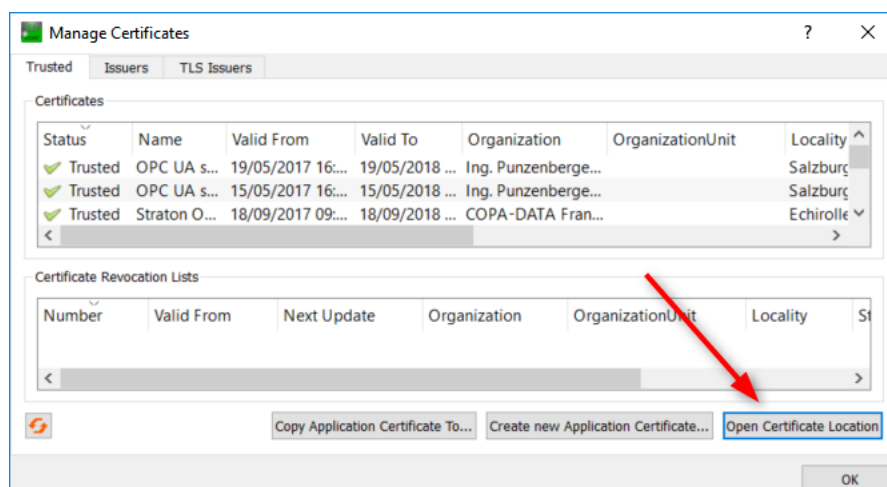
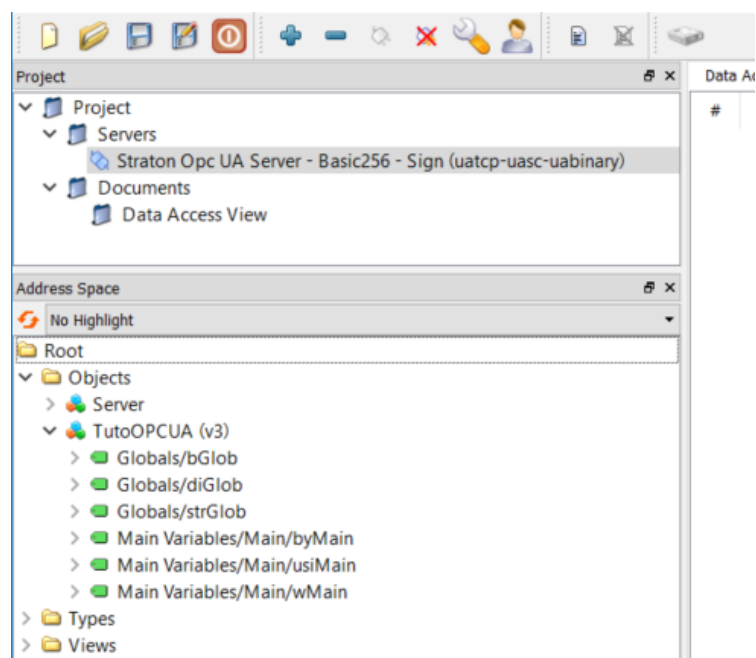The explorer opens the 'trusted' folder. Go two folders up in 'PKI' and open the 'own/certs' folder.
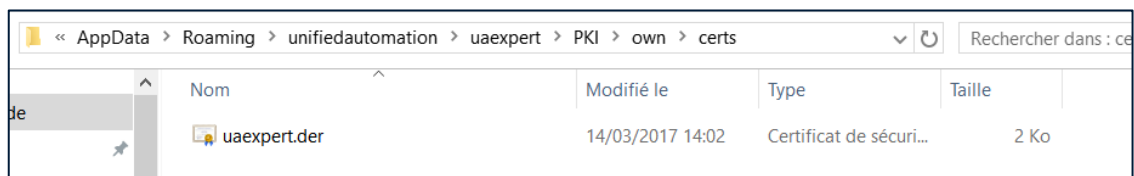
Copy this certificate and paste it in the 'PKI/CA/certs' folder on your runtime so the UA Expert Client certificate is at the same place as the straton OPC UA Server certificate.
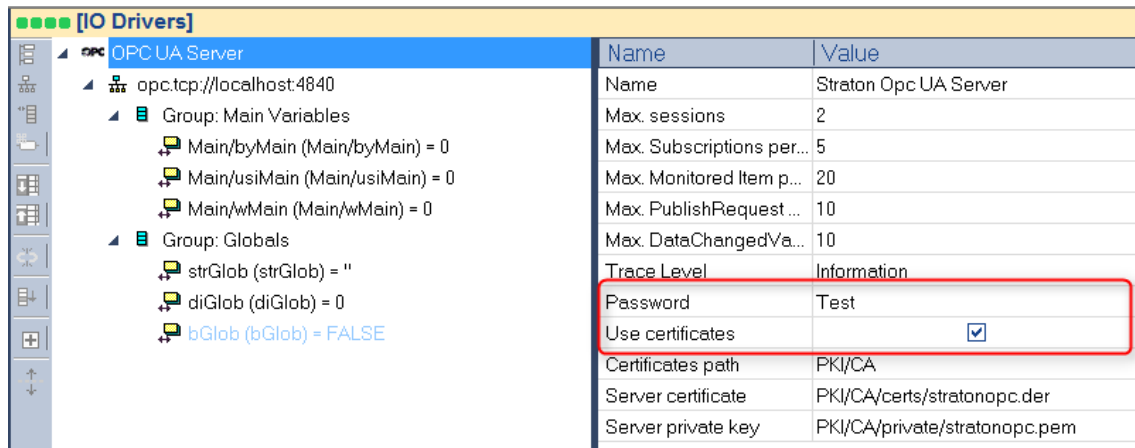
Once this is done, try to connect again to the Server, this must work:

4.3. Case when a password is used

If a password is used, read the previous part in order to understand this one.

Open the first level of the configuration and set a Password:

A password can be used only when using the Server certificates, indeed the 'Sign' and 'Sign & Encrypt' Message Security Mode are not available if Security Policy is 'None'.

In the Security Settings (level 2 of the straton configuration), a Security Policy different than 'None' must be chose.
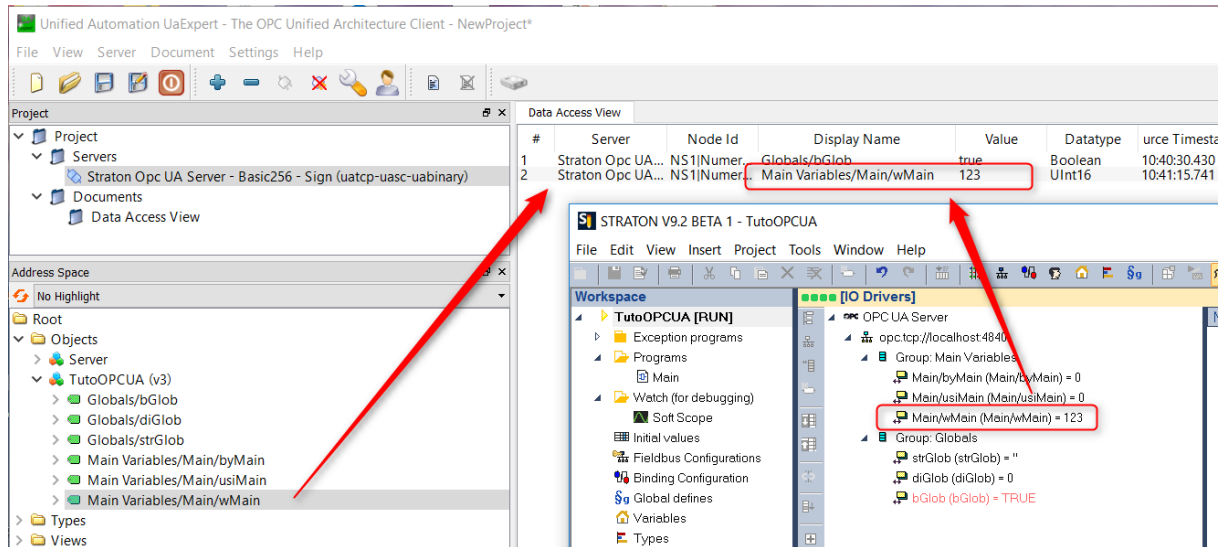
In the Client, here UA Expert, when browsing Servers, choose a security level different than 'None' then set the Password in the Authentication Settings:
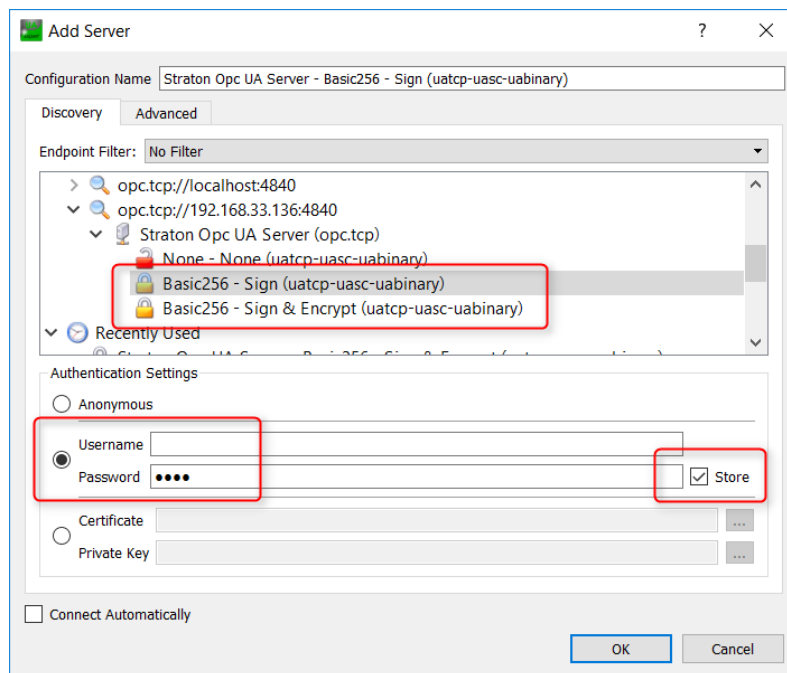
The Client must be able to connect to the Server if the Passwords corresponds.

4.4. Reading variables from UA Expert

Simply drag and drop variables from the 'Address space' area to the 'Data Access View' area:

5. Frequently Asked Questions

The OPC UA Client does not want to connect to the Server...

▸ If no certificates are used, check the Client's Endpoint URL parameter. For example if your Server is on another PC than the Client, the URL can't be 'opc.tcp://localhost:4840', it must be something like 'opc.tcp://192.168.33.136:4840' with the Server's IP address and port.

   ▪ Check that the port is well opened on the Server side

   ▪ Check that the Server can be reached using for example a 'ping' command

   ▪ Check that the Client certificate (*.der file) is copied in the Server certificate folder

▸ If a Password is used by the Server ('Password' field not empty), check that the configuration of the Client corresponds: the security policy must be different than 'None' and passwords must correspond.