Application Note

How to configure OPC UA driver communication!
Rev 1.1

Revision History

Rev1.0 : Initial Release

Rev1.1 : Add async trigger script

Conformance Testing

The following hardware/software configuration was used to test communication.

1. **Aveva Edge 2023 (Service Pack: 0, Path: 0, Build Number: 4801.2308.3105.0000)**
2. **Loytec LINX215 DDC Controller (Firmware: 8.2.4 2024-03-19 16:37:00)**
3. **KEPServerEX 6.15 (V6.15.132.0)**

OPC UA Introduction

OPC UA (Unified Architecture is a new International Standard designed for communication between informations system.

OPC UA involves with new features such as : Security based on certificate exchange, heartbeat for connections in both directions and acknowledgement of transmitted data.

The OPC UA server is accessible via two URL

opc.tcp://ip_address:4840

https://ip_address/UA

It is require to setup OPC UA server before establishing a connection with any OPC UA client.

OPC UA and Security Mode

Security Policy

1. None
2. Basic128Rsa15 (Sign + Sign&Encrypt)
3. Basic256 (Sign + Sign&Encrypt)
4. Basic256Sha256 (Sign + Sign&Encrypt)
5. Aes128Sha256RsaOaep (Sign + Sign&Encrypt)
6. Aes256Sha256RsaPss (Sign + Sign&Encrypt)

User Authentication Mode

1. Anonymous
2. Credentials
3. X509 Certificate

Available Drivers Interface

Aveva Edge 23

OPC UA Server
OPC UA Client

OPC XML-DA Client

OPC DA 2.05 Server
OPC DA 2.05 Client

OPC HDA Server

LOYTEC

OPC UA Server

OPC XML-DA Server
OPC XML-DA Client

KEPServerEX

All others

OPC UA Connections

Method-1 : Unencrypted And Unauthenticated connection mode
Method-2 : Unencrypted And Authenticated connection mode
Method-3 : Signed/Encrypted And Authenticated connection mode

Modbus TCP

Embedded OPC UA
SERVER
LINX 215

Download Project

OPC UA binary protocol over TCP/IP only.

OPC UA

OPC UA CLIENT
Aveva Edge SCADA

Download Project

Method-4 : Signed/Encrypted And Authenticated connection mode

kepware®

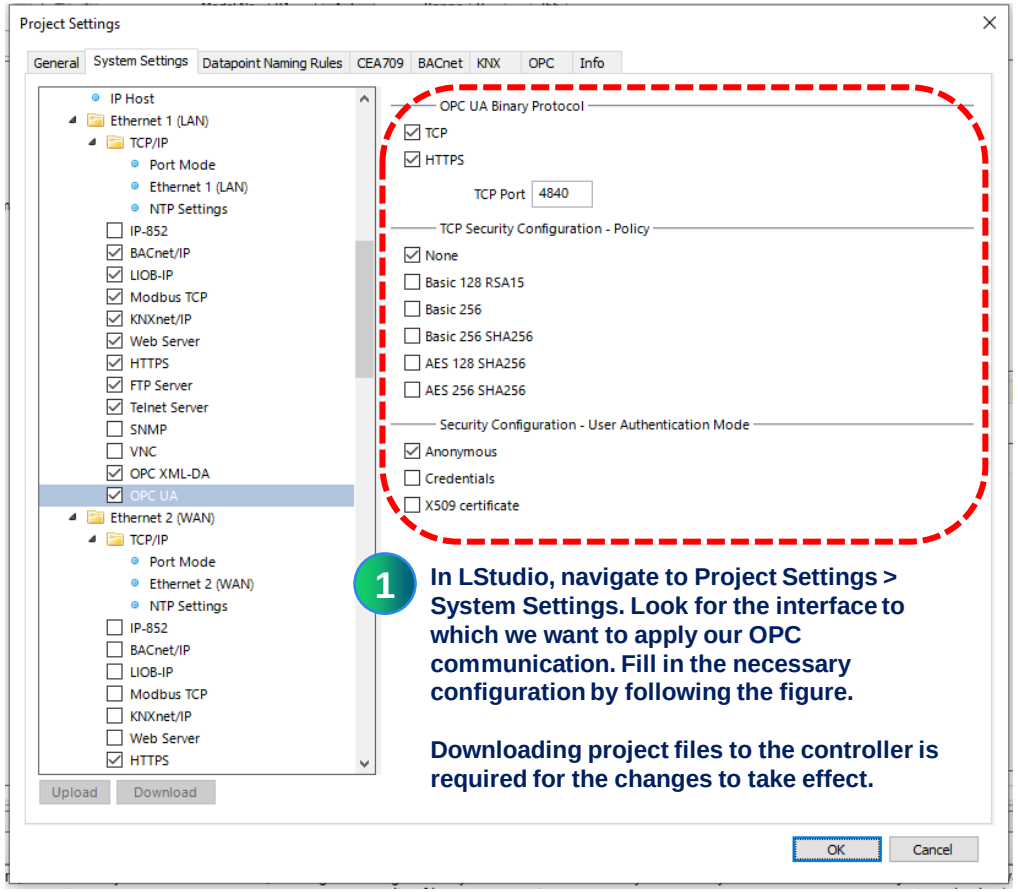
OPC UA SERVER

Download Project

Method 1 : Unencrypted And Unauthenticated connection mode

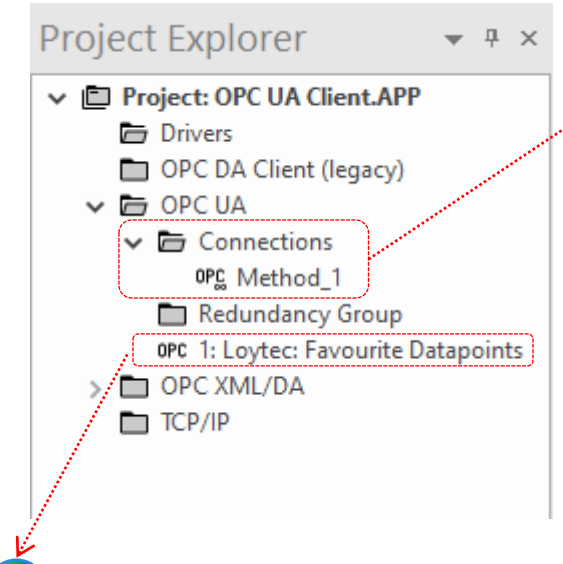
Security Policy : None

Authentication Mode : Anonymous



1 **In LStudio, navigate to Project Settings > System Settings. Look for the interface to which we want to apply our OPC communication. Fill in the necessary configuration by following the figure.**

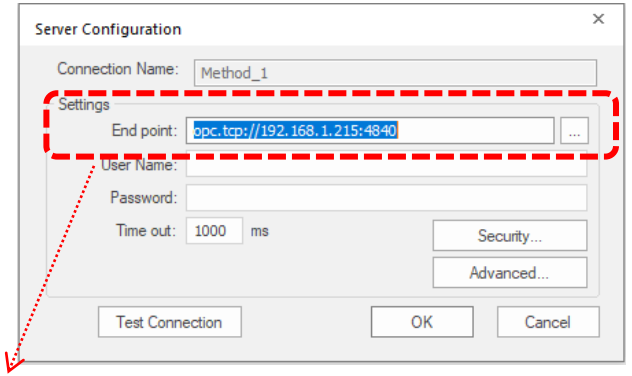
Downloading project files to the controller is required for the changes to take effect.



2 **Right click to create new *Connections* under OPC UA/Connections folder.**

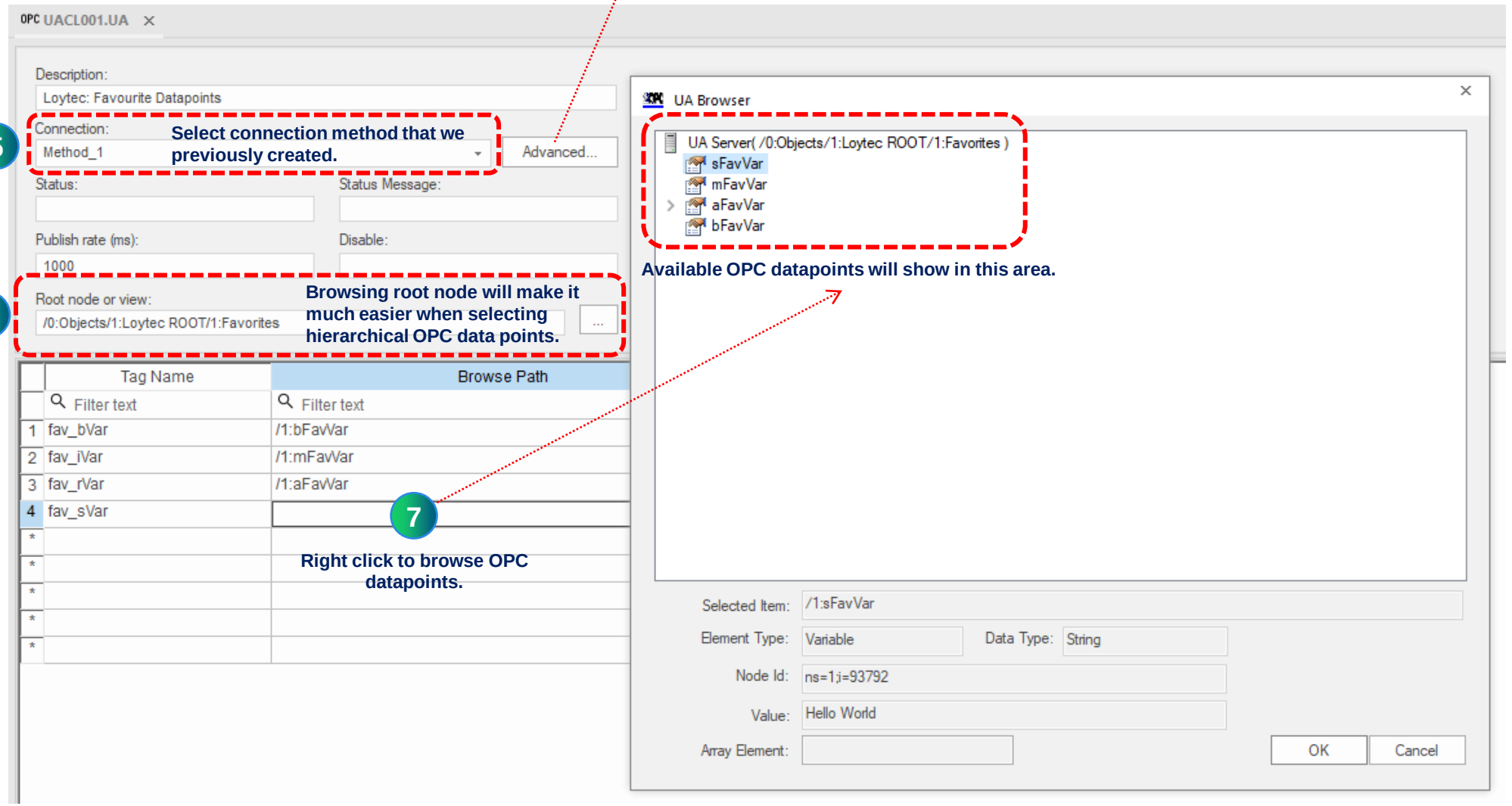
4 **In Aveva Edge, right click to create new *OPC driver worksheet* under UA folder.**

(Refer to next sheet for further details)



3 **The endpoint URL for OPC TCP Binary communication should be opc.tcp://ip_address:4840. Alternatively, you can press the search icon to browse available OPC servers. Please note that servers listening on the default port (4840) can only be found.**

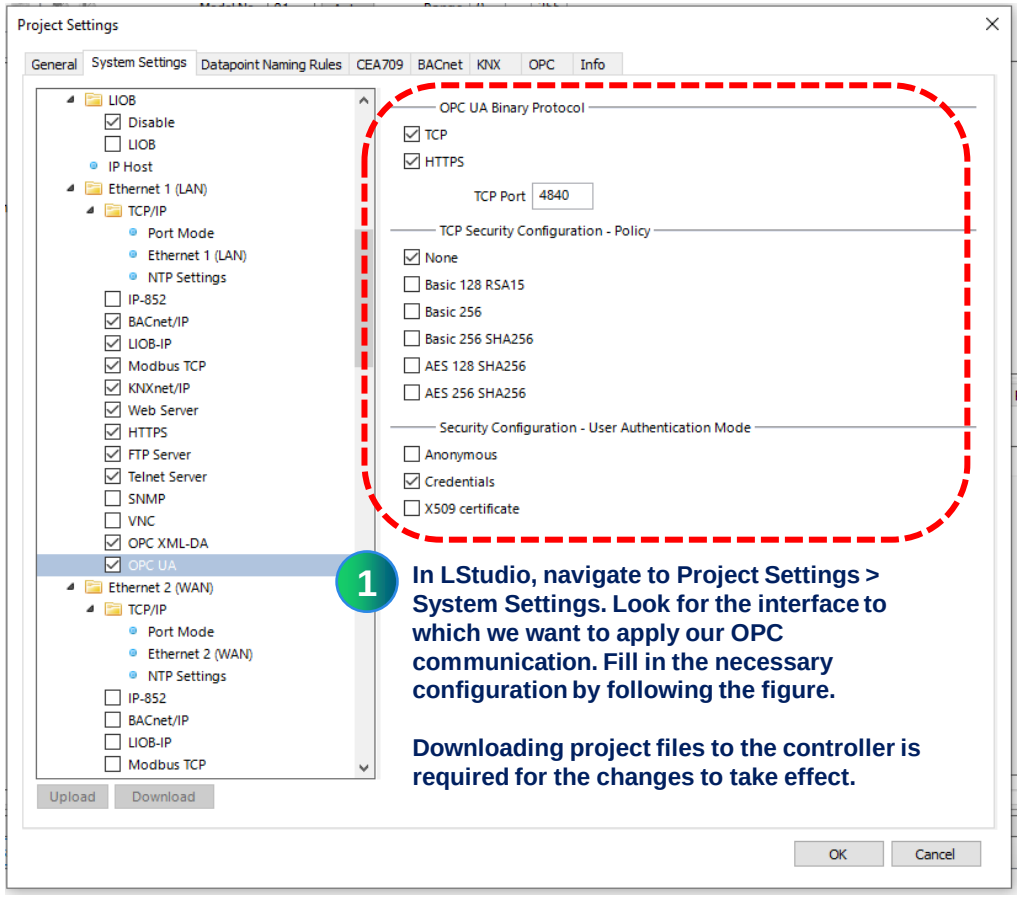
8 **Finally click on Advanced Button and assign asynReadTrigger Boolean Tag.**



Method 2: Unencrypted And Authenticated connection mode

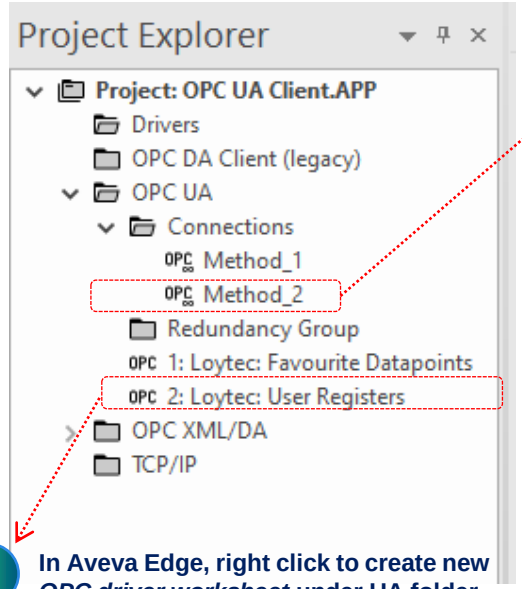
Security Policy : None

Authentication Mode: Credential



1 In LStudio, navigate to Project Settings > System Settings. Look for the interface to which we want to apply our OPC communication. Fill in the necessary configuration by following the figure.

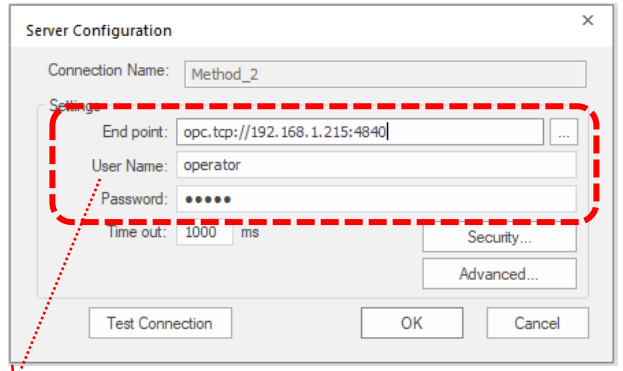
Downloading project files to the controller is required for the changes to take effect.



2 Right click to create new *Connections* under OPC UA/Connections folder.

4 In Aveva Edge, right click to create new *OPC driver worksheet* under UA folder.

(Refer to next sheet for further details)

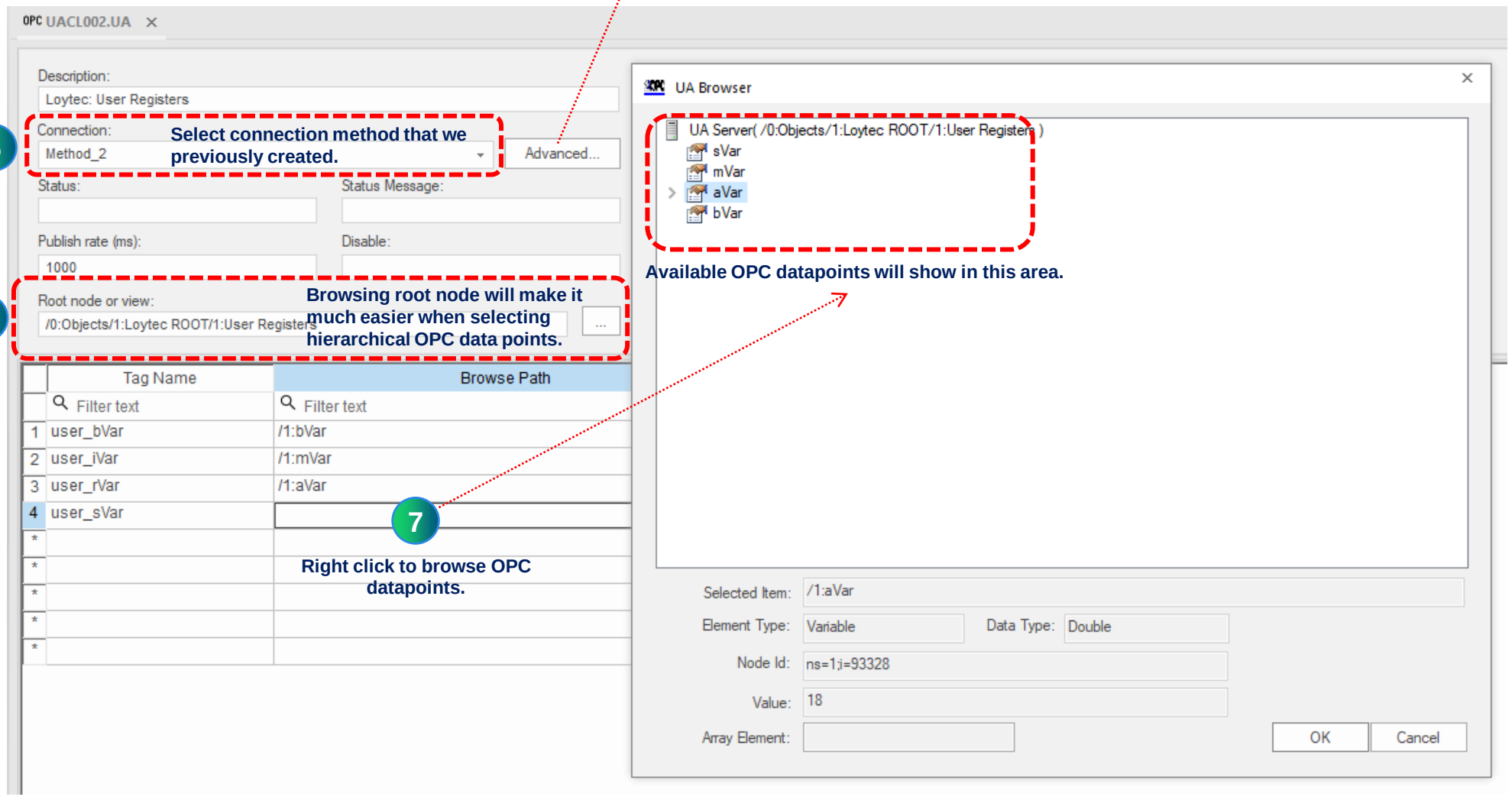


3 The endpoint URL for OPC TCP Binary communication should be opc.tcp://ip_address:4840. Alternatively, you can press the search icon to browse available OPC servers.

Username : operator
Password : 12345

Please note that servers listening on the default port (4840) can only be found.

8 **Finally click on Advanced Button and assign asynReadTrigger Boolean Tag.**



5 **Select connection method that we previously created.**

6 **Browsing root node will make it much easier when selecting hierarchical OPC data points.**

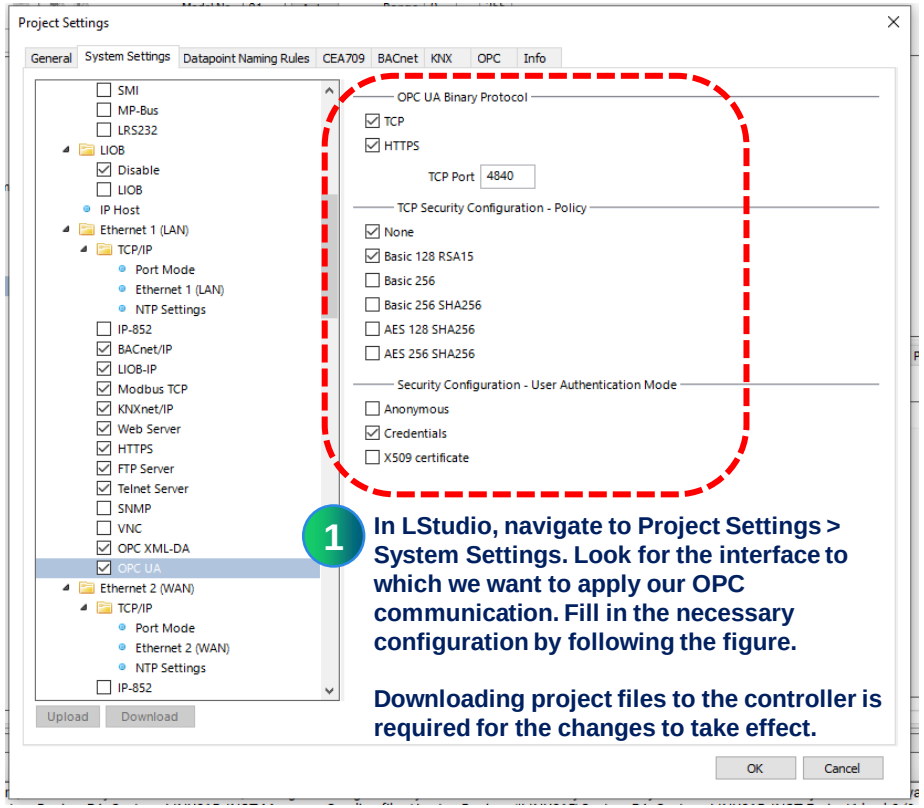
Available OPC datapoints will show in this area.

7 **Right click to browse OPC datapoints.**

Method 3: Signed/Encrypted And Authenticated connection mode

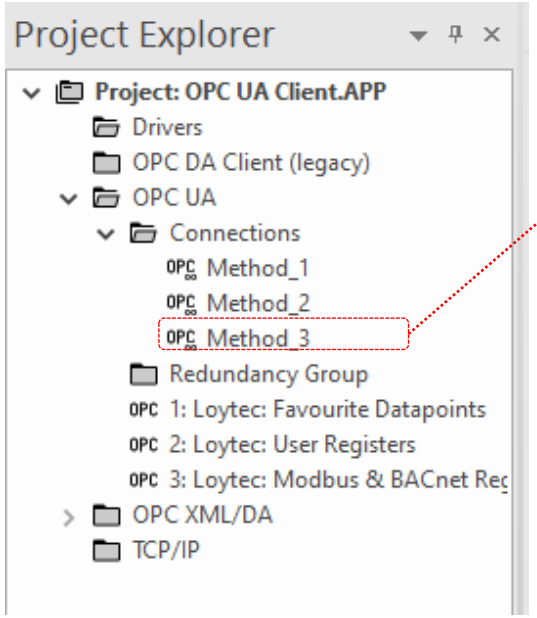
Security Policy : Basic128Rsa15

Authentication Mode: Credential

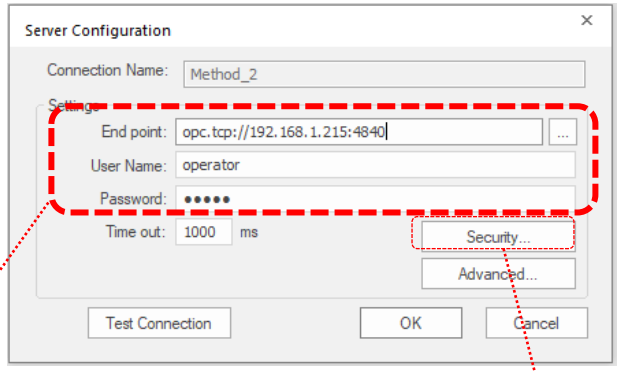


1 **In LStudio, navigate to Project Settings > System Settings. Look for the interface to which we want to apply our OPC communication. Fill in the necessary configuration by following the figure.**

Downloading project files to the controller is required for the changes to take effect.



2 **Right click to create new *Connections* under OPC UA/Connections folder.**



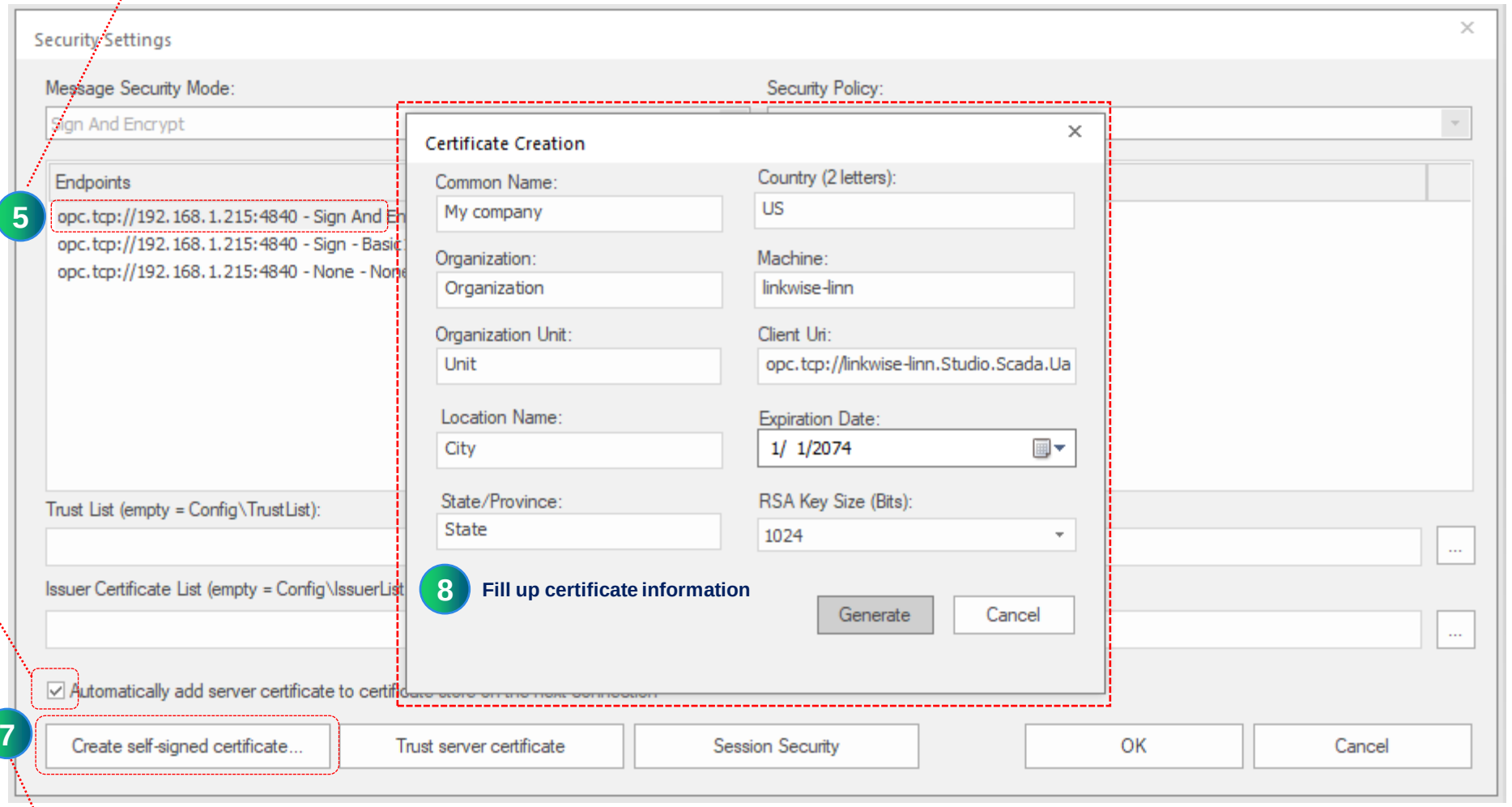
3 **The endpoint URL for OPC TCP Binary communication should be opc.tcp://ip_address:4840. Alternatively, you can press the search icon to browse available OPC servers.**

Username : operator
Password : 12345

Please note that servers listening on the default port (4840) can only be found.

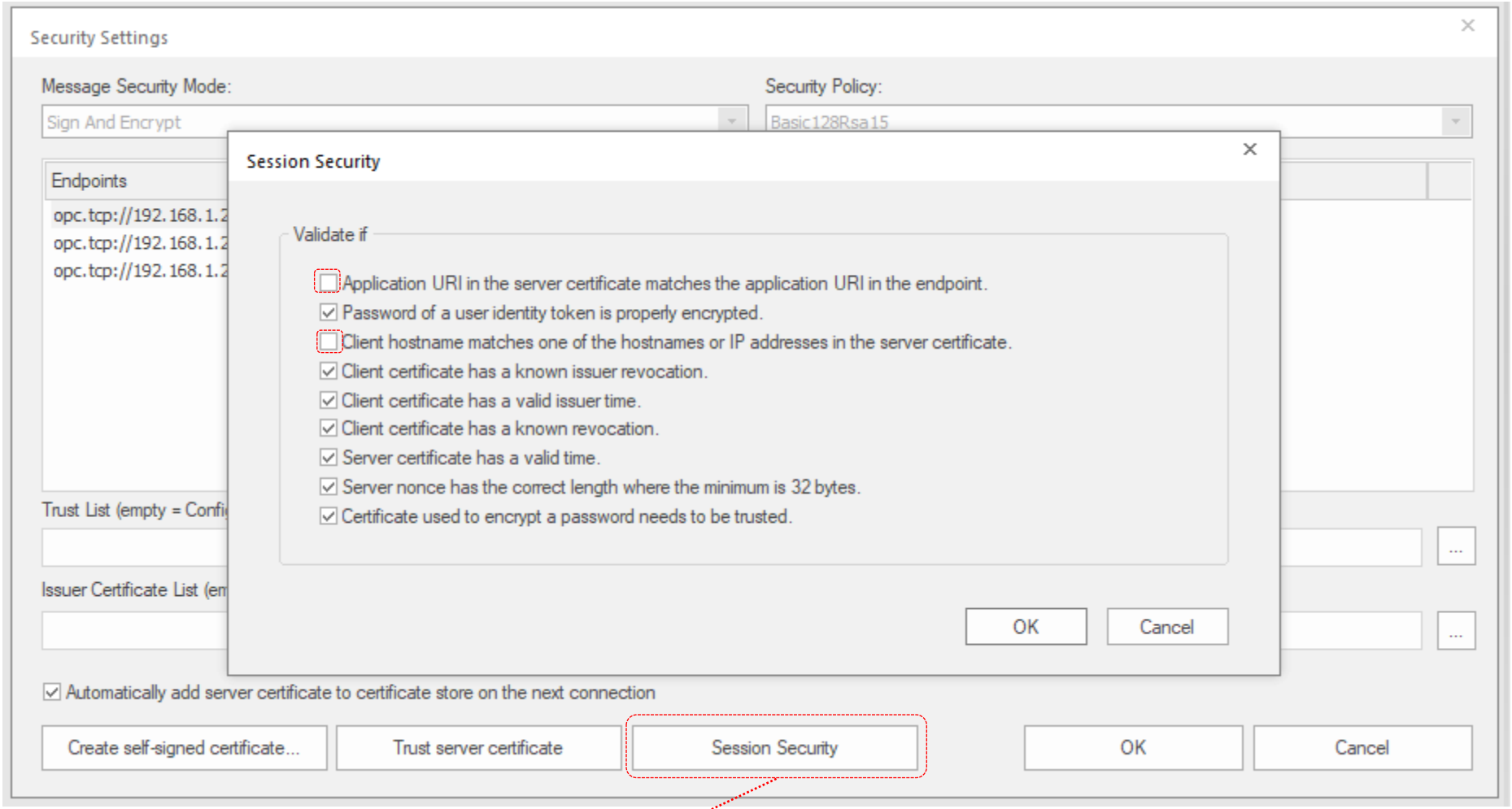
4 **Click the 'Security' button to configure a self-signed certificate and necessary encryption algorithms.**

Select Basic128 Rsa15 key pair method that we configured in Loytec OPC UA configuration.

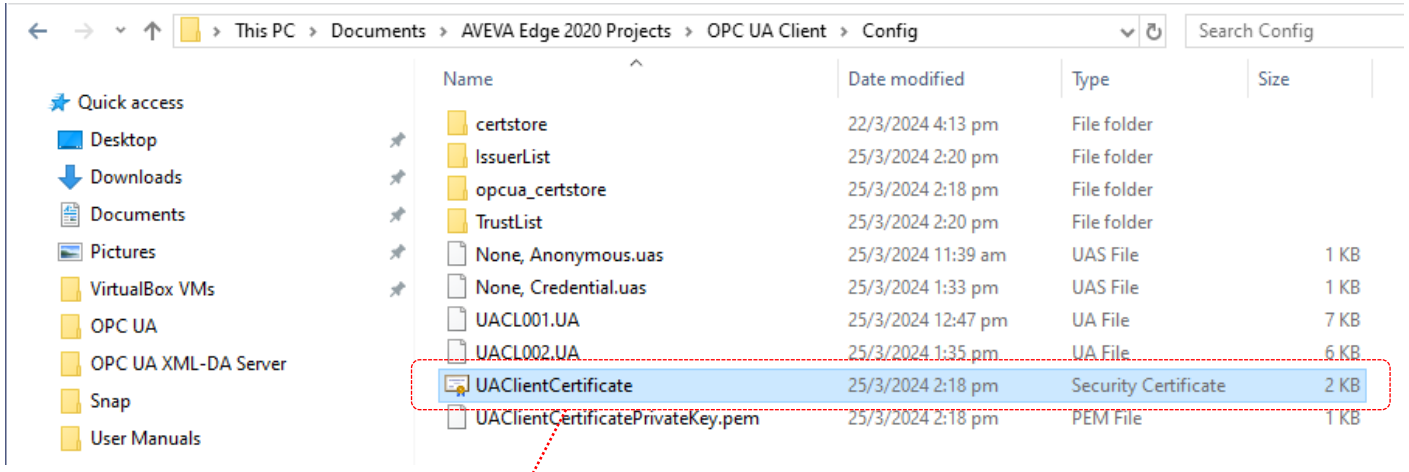


Check this box. (Then, Loytec OPC UA Server certificate will be trusted once we establish the connection.)

Next, we may need to generate a client self-signed certificate. (For this, the generated certificate will need to be copied to Loytec as a trusted certificate.)

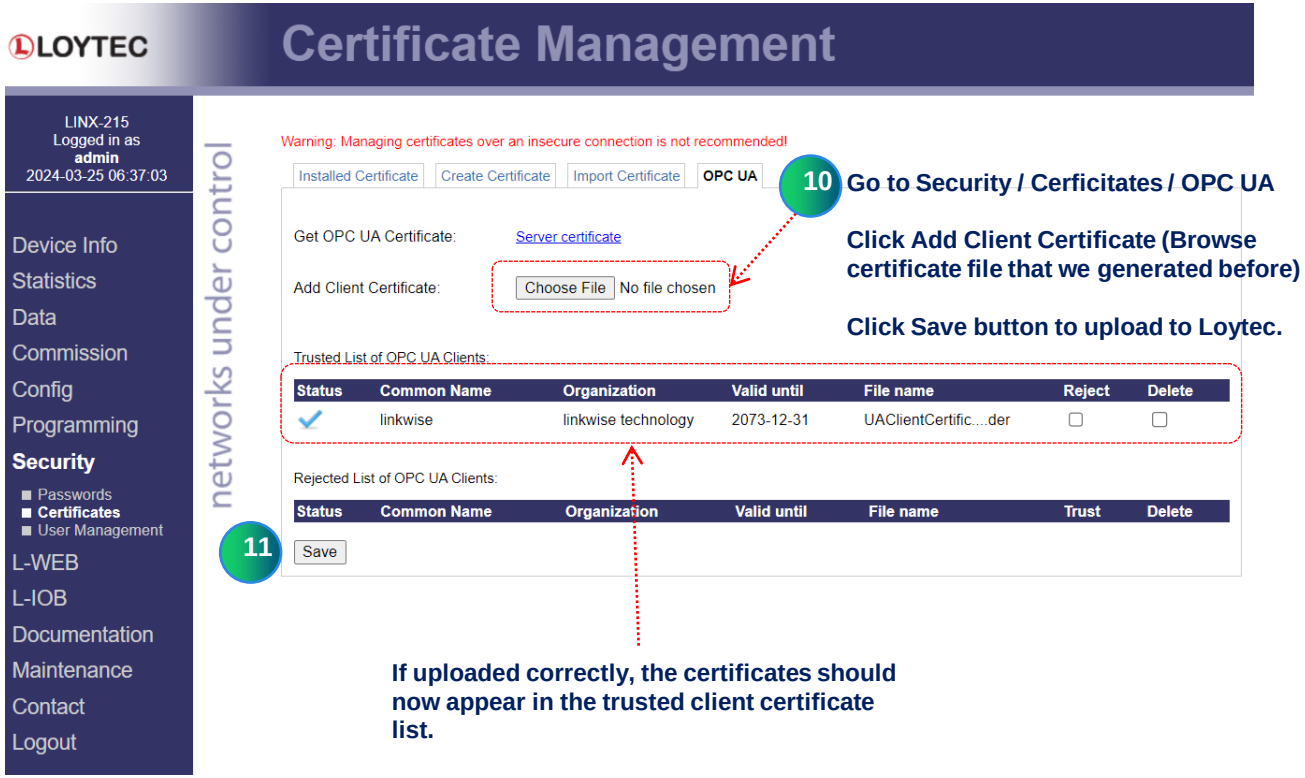


9 **click on session security, uncheck item 1 & 3.**



The exported certificate will be saved inside your project folder:

(xxx / Config / UAClientCertificate)

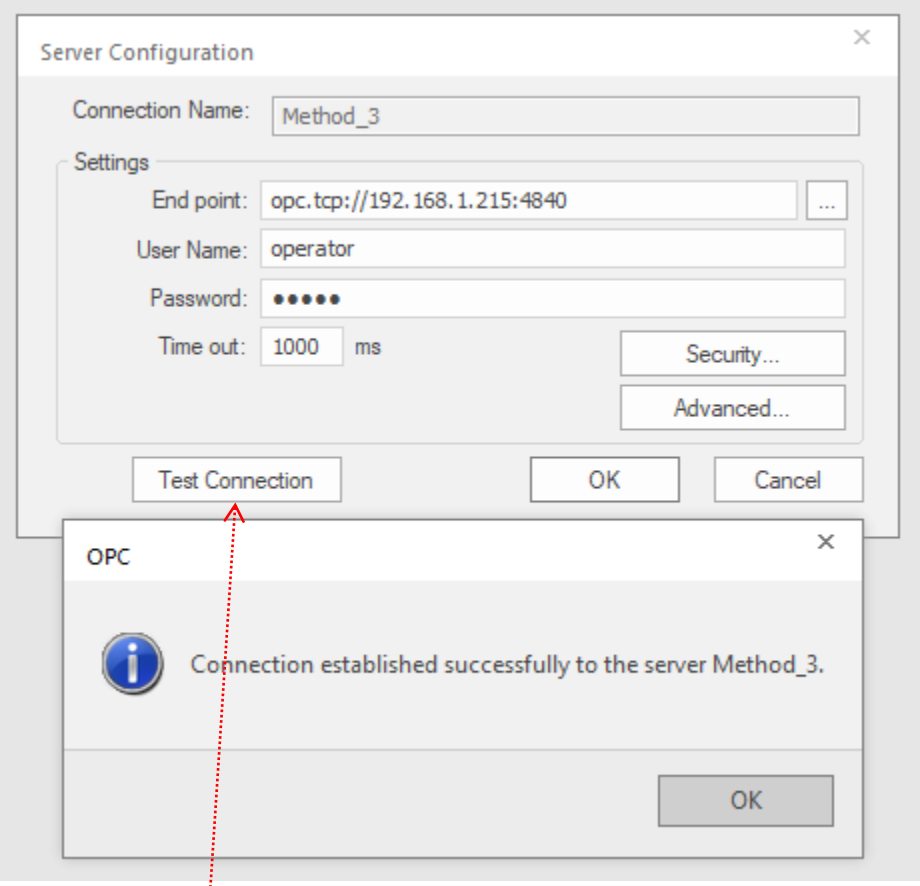


10 **Go to Security / Cerficitates / OPC UA**

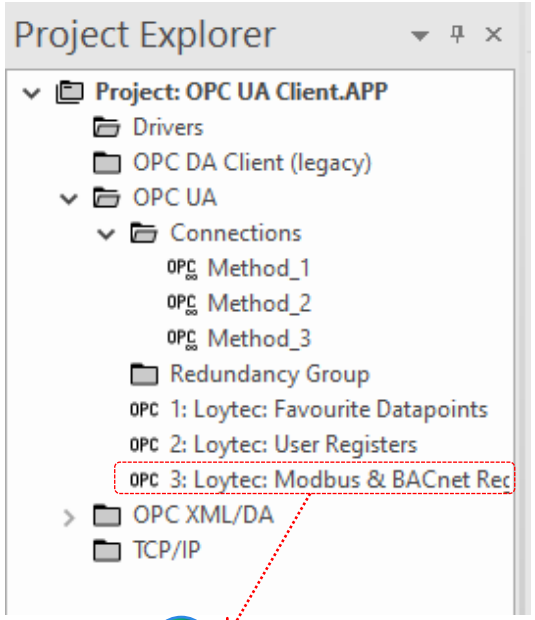
Click Add Client Certificate (Browse certificate file that we generated before)

Click Save button to upload to Loytec.

If uploaded correctly, the certificates should now appear in the trusted client certificate list.



12 **Click 'Test Connection' to check whether the connection status is good or bad.**



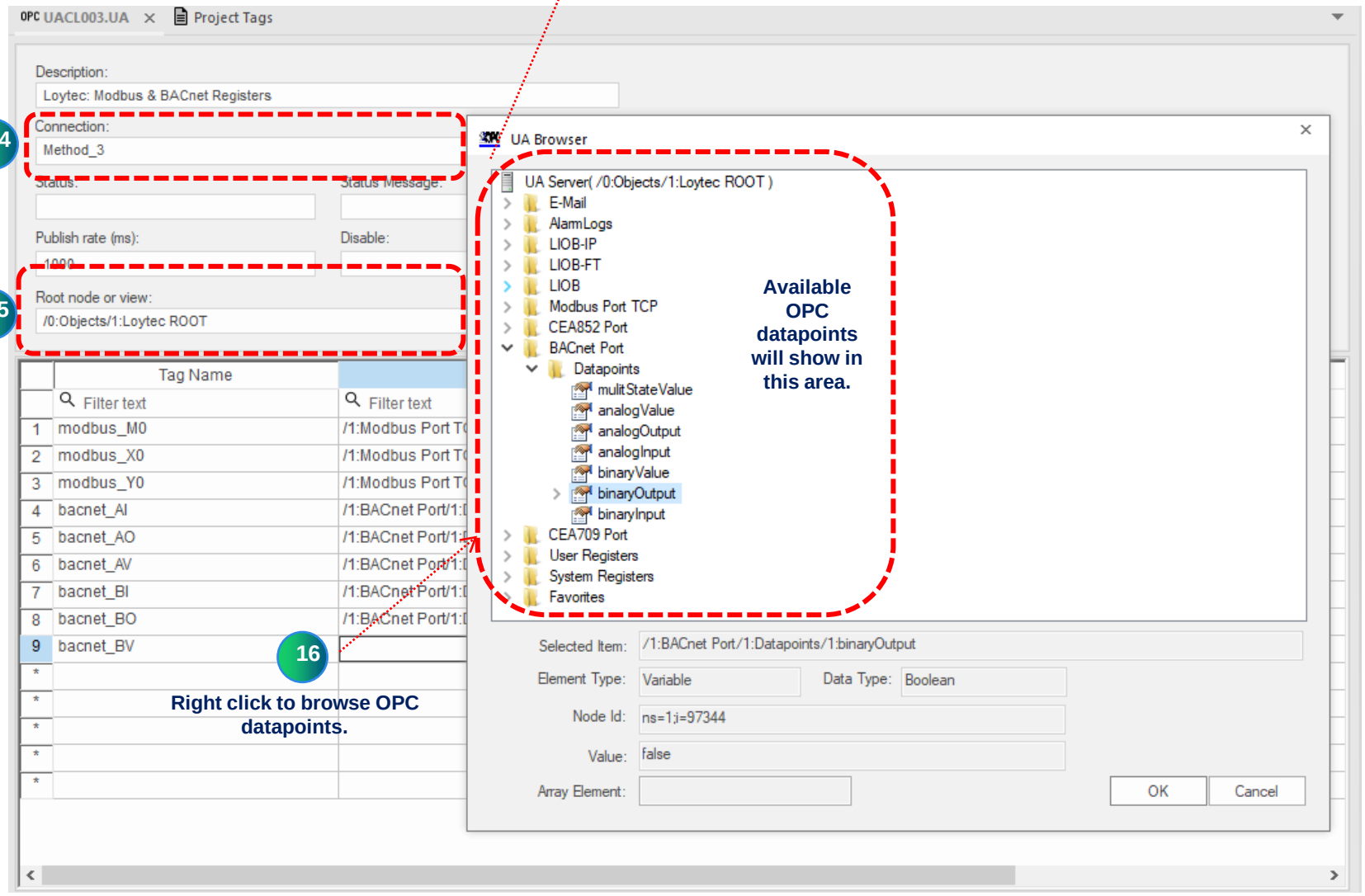
13 **In Aveva Edge, go to project explorer again and, right click to create new *OPC driver worksheet* under UA folder.**

(Refer to next sheet for further details)

17 **Finally click on Advanced Button and assign asynReadTrigger Boolean Tag.**

14 **Select connection method that we previously created.**

15 **Browsing root node will make it much easier when selecting hierarchical OPC data points.**

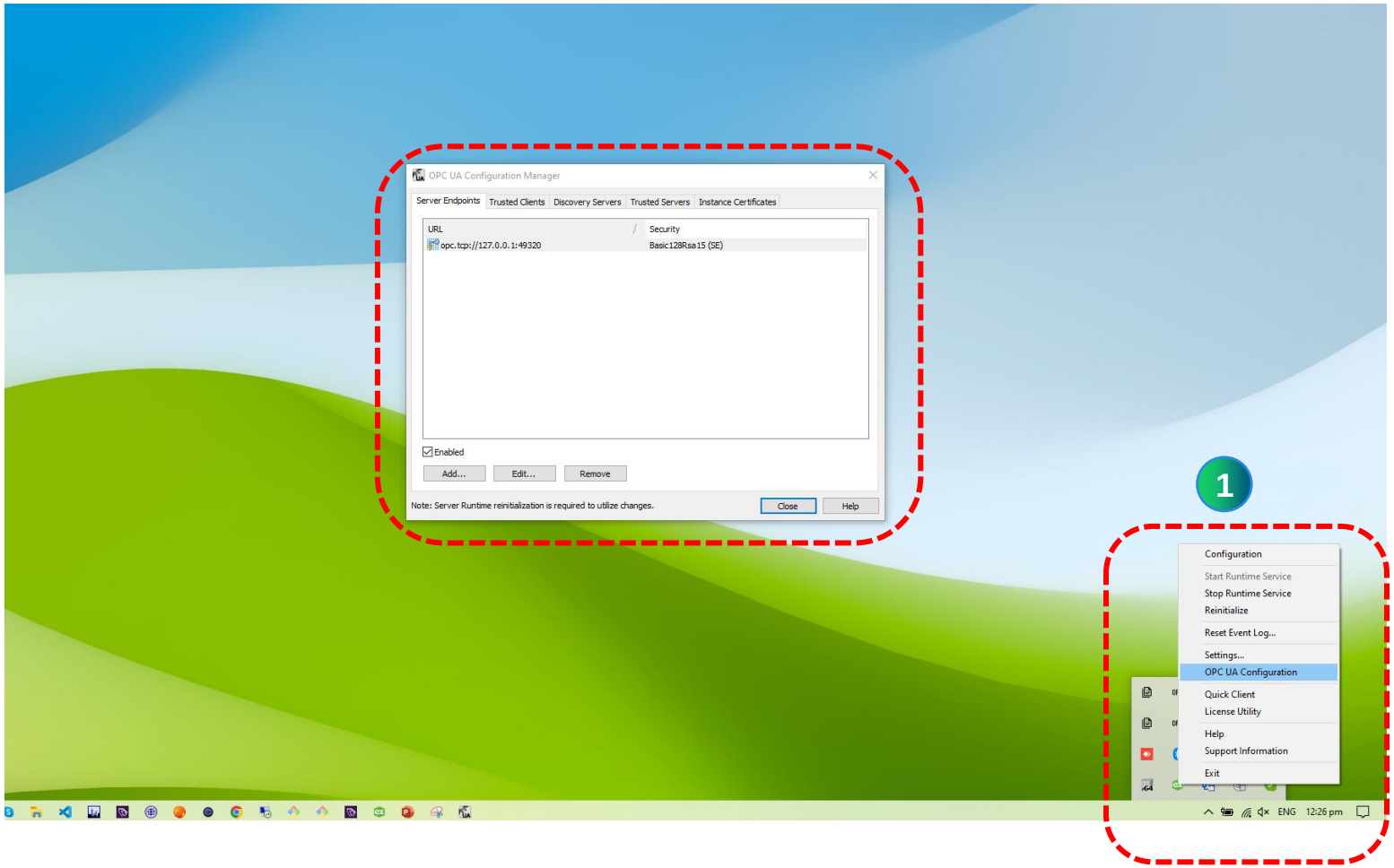


16 **Right click to browse OPC datapoints.**

Method 4: Signed/Encrypted And Authenticated connection mode

Security Policy : Basic128Rsa15

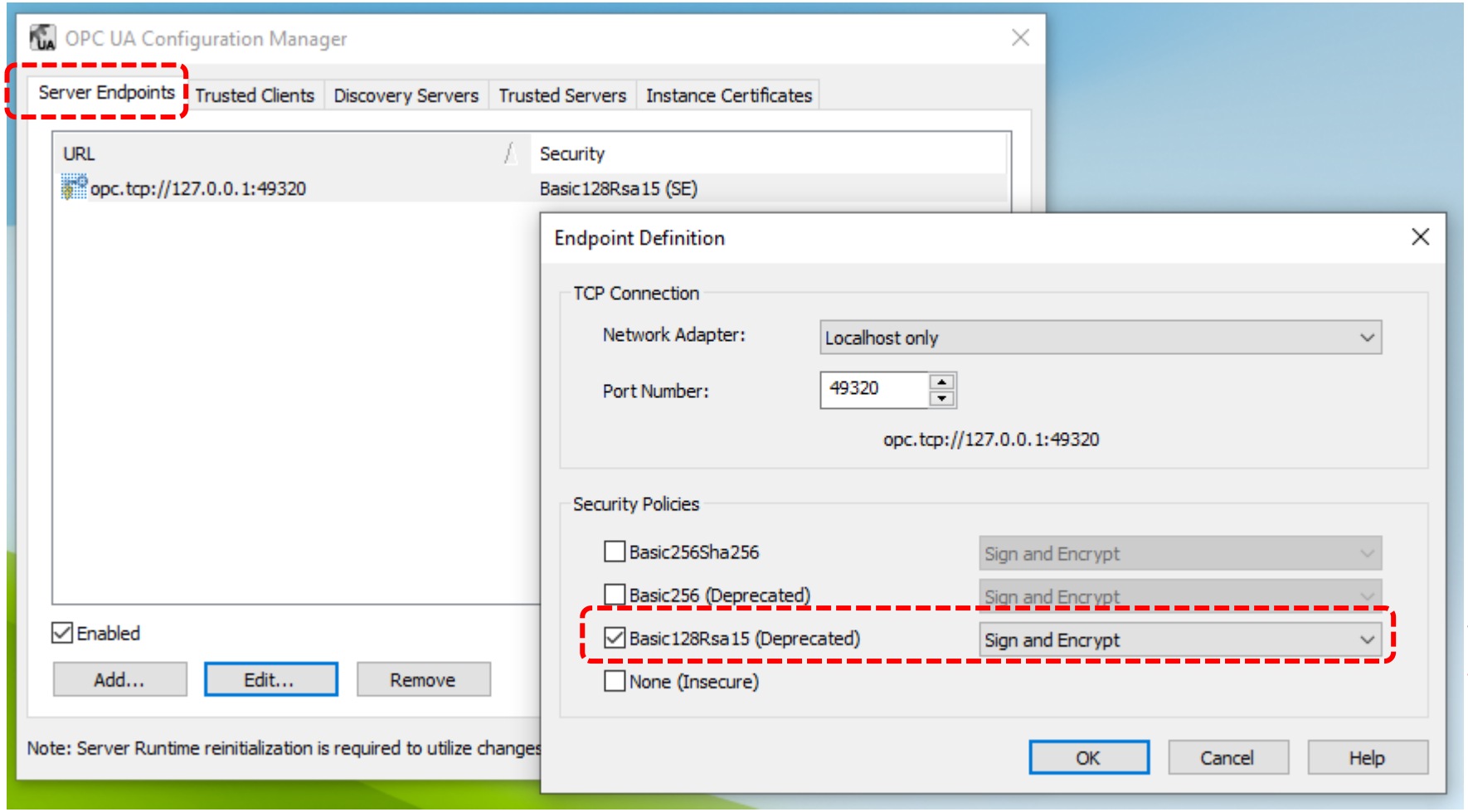
Authentication Mode: Credential



- **Right click on the kepware icon in system tray to open the configuration menu**
- **Click on OPC UA Configuration**

- Here, we may need to configure our OPC UA server settings

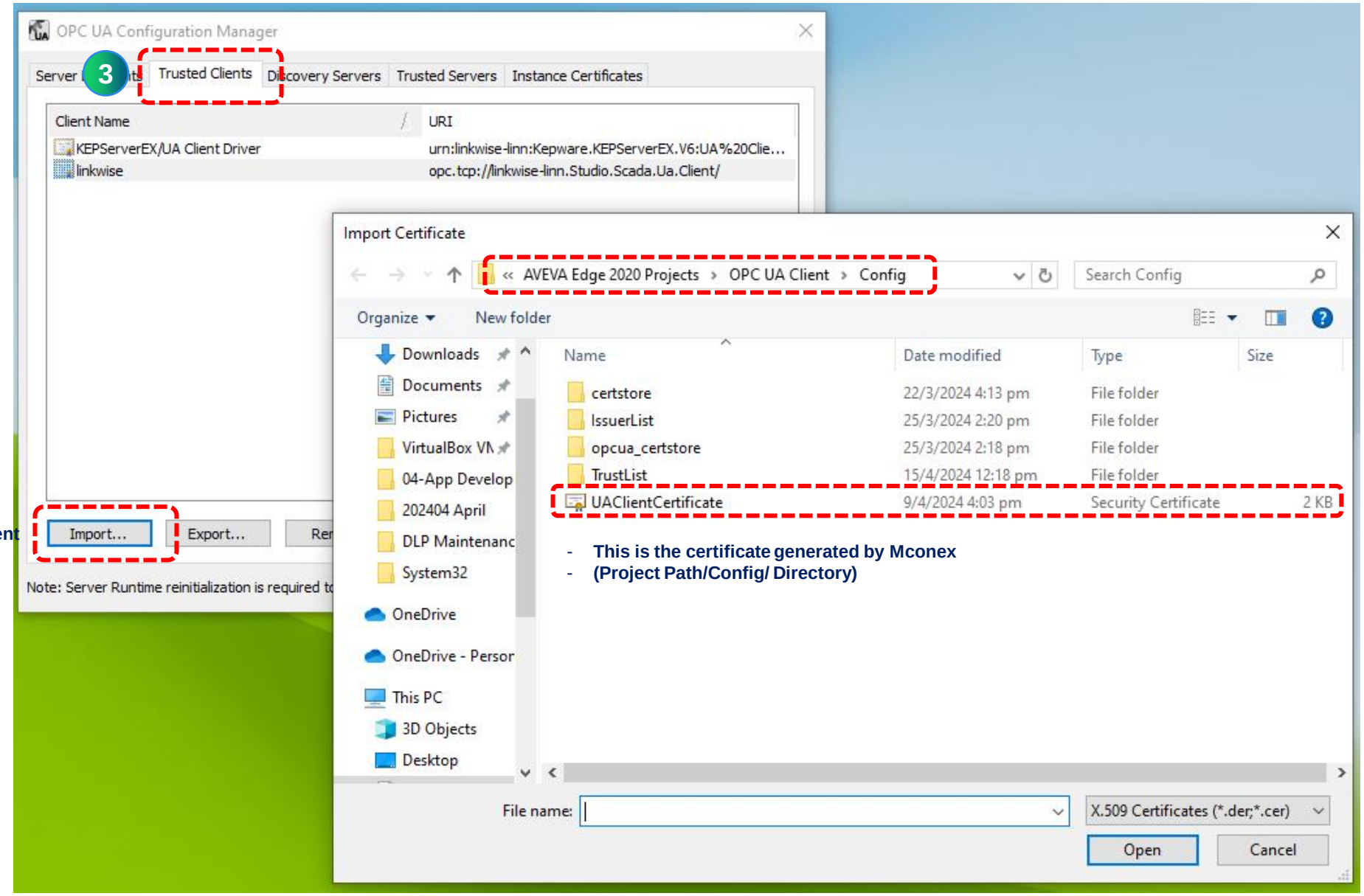
2



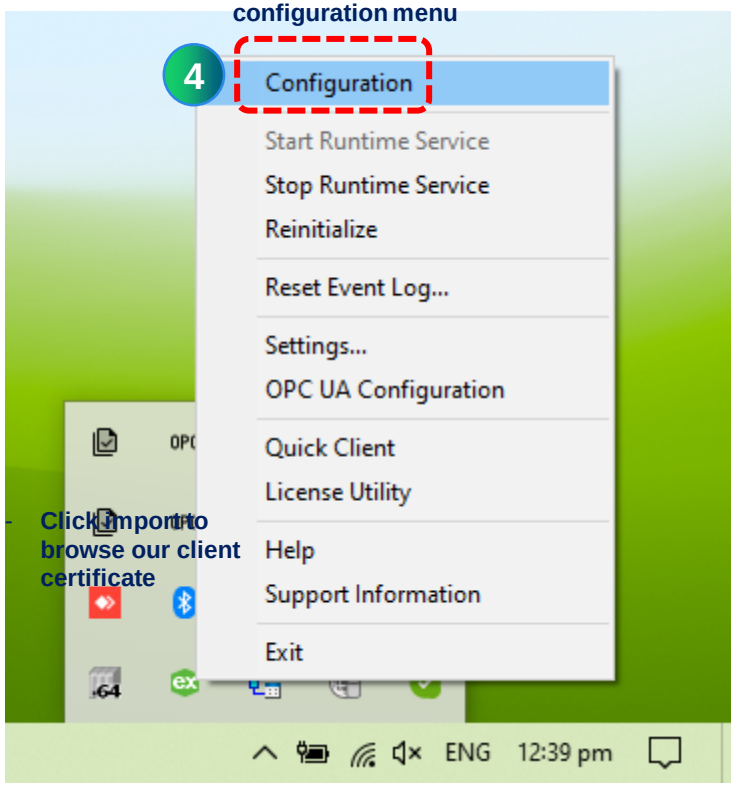
- Select connection mode
- (For production env, always consider for most secure encryption method and connection mode)

- Click Trusted Client Tab
- From here we may need to add our self signed certificate to OPC UA Server in order to get successful communication

- Click import to browse our client certificate

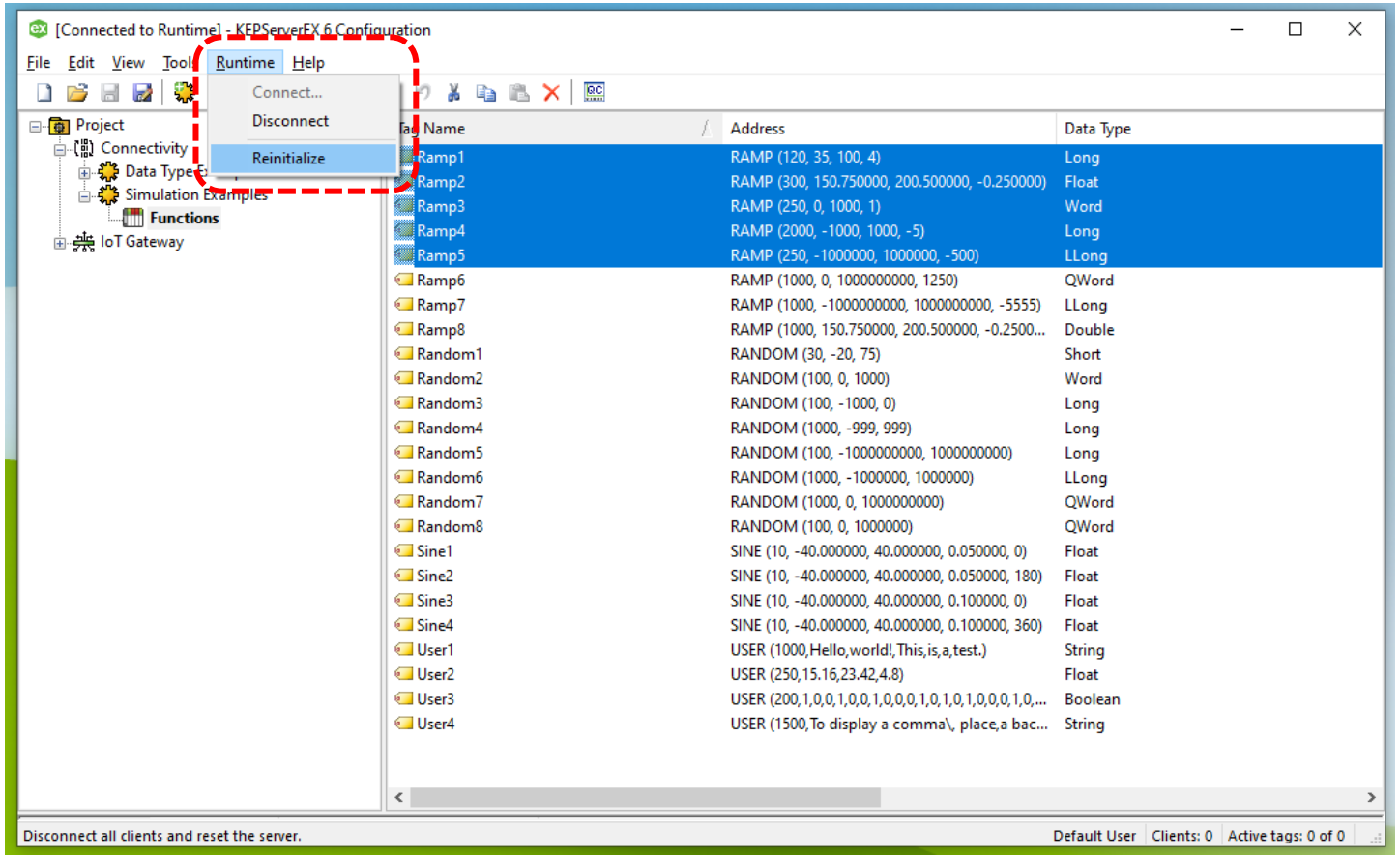


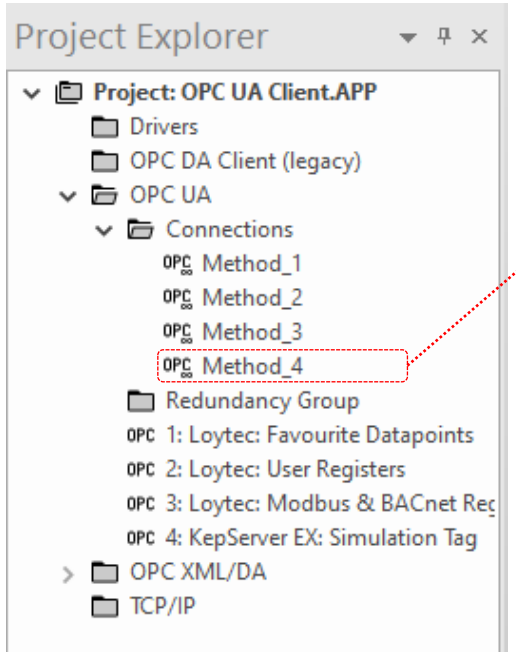
- Click again on configuration menu



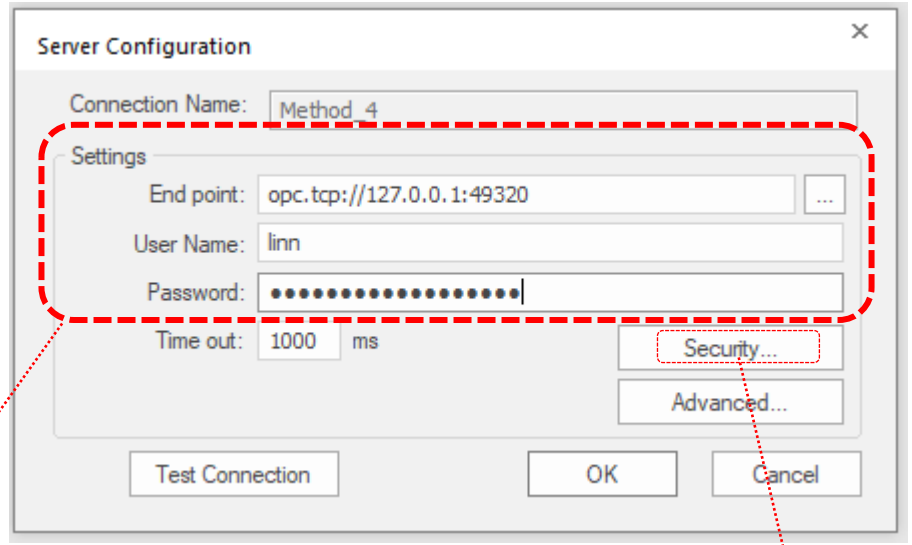
- Click import to browse our client certificate

- Click Reinitialize in order to restart OPC UA Server Runtime Service





5 **Right click to create new *Connections* under OPC UA/Connections folder.**

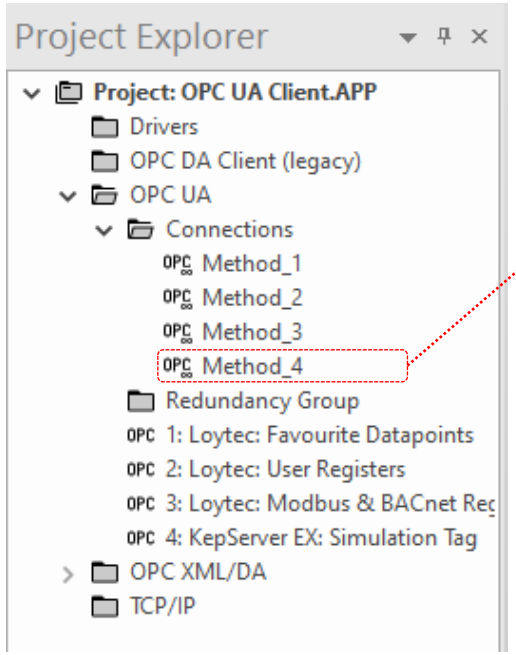


6

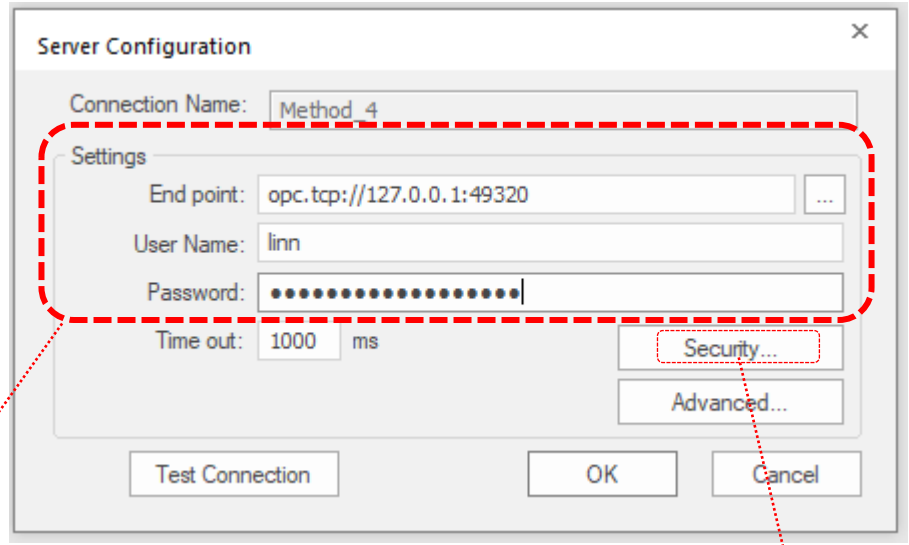
The endpoint URL for OPC TCP Binary communication should be opc.tcp://ip_address:49320. Alternatively, you can press the search icon to browse available OPC servers.

Username : auth from kepserver
Password : auth from kepserver

Click the 'Security' button to configure a self-signed certificate and necessary encryption algorithms.



7 **Right click to create new *Connections* under OPC UA/Connections folder.**

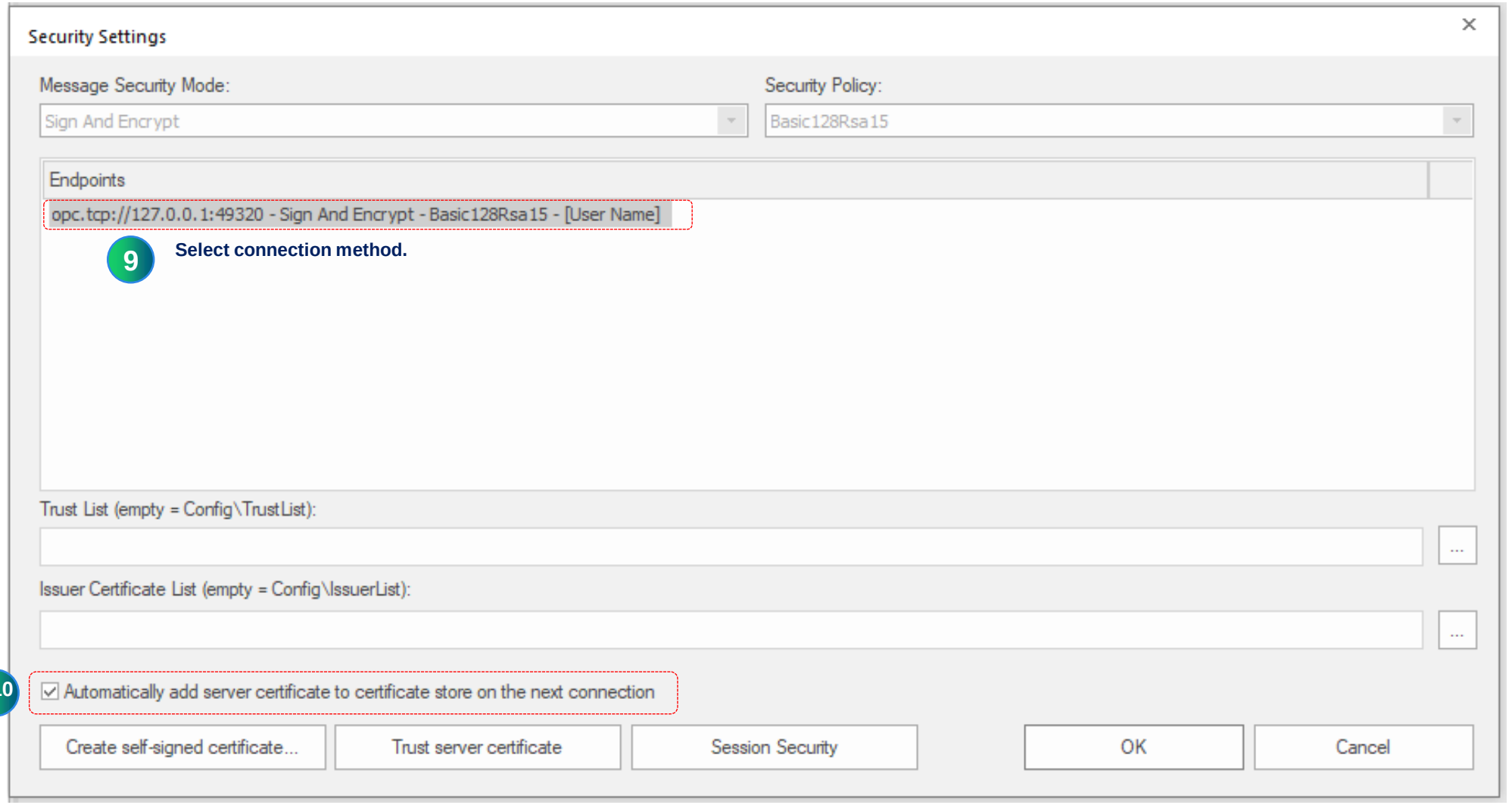


8

The endpoint URL for OPC TCP Binary communication should be opc.tcp://ip_address:49320. Alternatively, you can press the search icon to browse available OPC servers.

Username : auth from kepserver
Password : auth from kepserver

Click the 'Security' button to configure a self-signed certificate and necessary encryption algorithms.


Security Settings
Message Security Mode:
Sign And Encrypt
Security Policy:
Basic128Rsa15
Endpoints
opc.tcp://127.0.0.1:49320 - Sign And Encrypt - Basic128Rsa15 - [User Name]
9
Select connection method.
Trust List (empty = Config\TrustList):
Issuer Certificate List (empty = Config\IssuerList):
Check this !
10
Automatically add server certificate to certificate store on the next connection
Create self-signed certificate...
Trust server certificate
Session Security
OK
Cancel

Select connection method that we previously created.

Browsing root node will make it much easier when selecting hierarchical OPC data points.