

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 information systems.

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 required 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

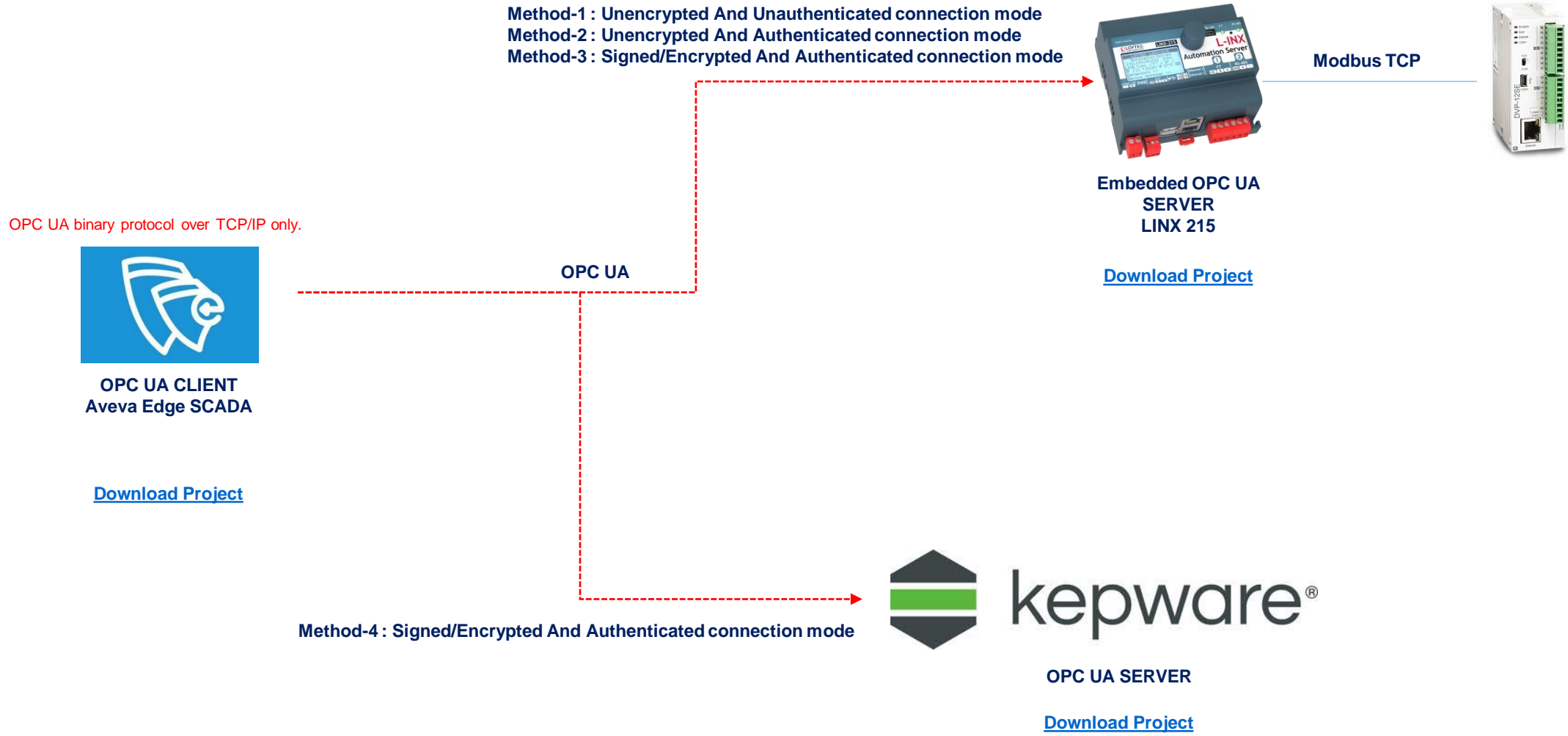
OPC UA Server

OPC XML-DA Server
OPC XML-DA Client

KEPServerEX

All others

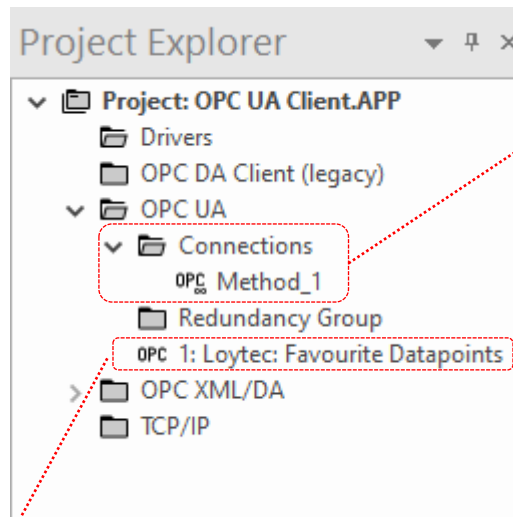
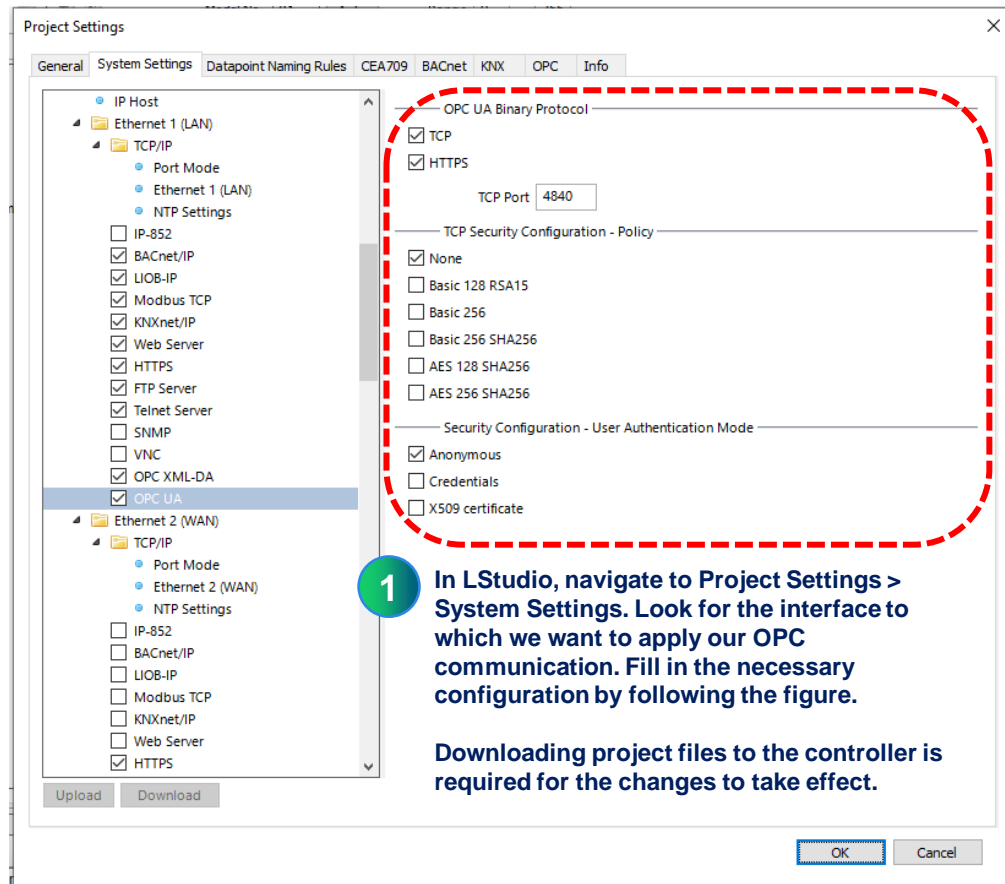
OPC UA Connections



Method 1 : Unencrypted And Unauthenticated connection mode

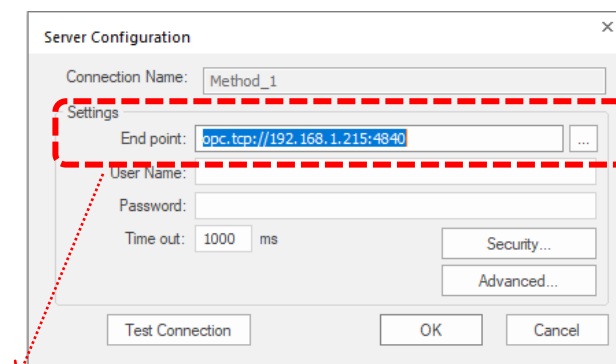
Security Policy : None

Authentication Mode : Anonymous



(Refer to next sheet for further details)

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



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

Asynchronous read trigger:

asynReadTrigger

5

Connection: **Select connection method that we previously created.**

Method_1

Status:

1000

6

Root node or view: **Browsing root node will make it much easier when selecting hierarchical OPC data points.**

/0:Objects/1:Loytec ROOT/1:Favorites

	Tag Name	Browse Path
	Filter text	Filter text
1	fav_bVar	/1:bFavVar
2	fav_iVar	/1:mFavVar
3	fav_rVar	/1:aFavVar
4	fav_sVar	
*		
*		
*		
*		
*		

7

Right click to browse OPC datapoints.

UA Browser

UA Server(/0:Objects/1:Loytec ROOT/1:Favorites)

- sFavVar
- mFavVar
- aFavVar
- bFavVar

Available OPC datapoints will show in this area.

Selected Item: /1:sFavVar

Element Type: Variable

Data Type: String

Node Id: ns=1;j=93792

Value: Hello World

Array Element:

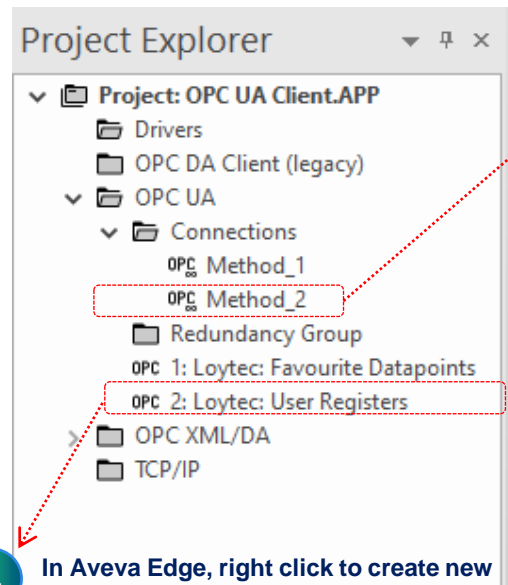
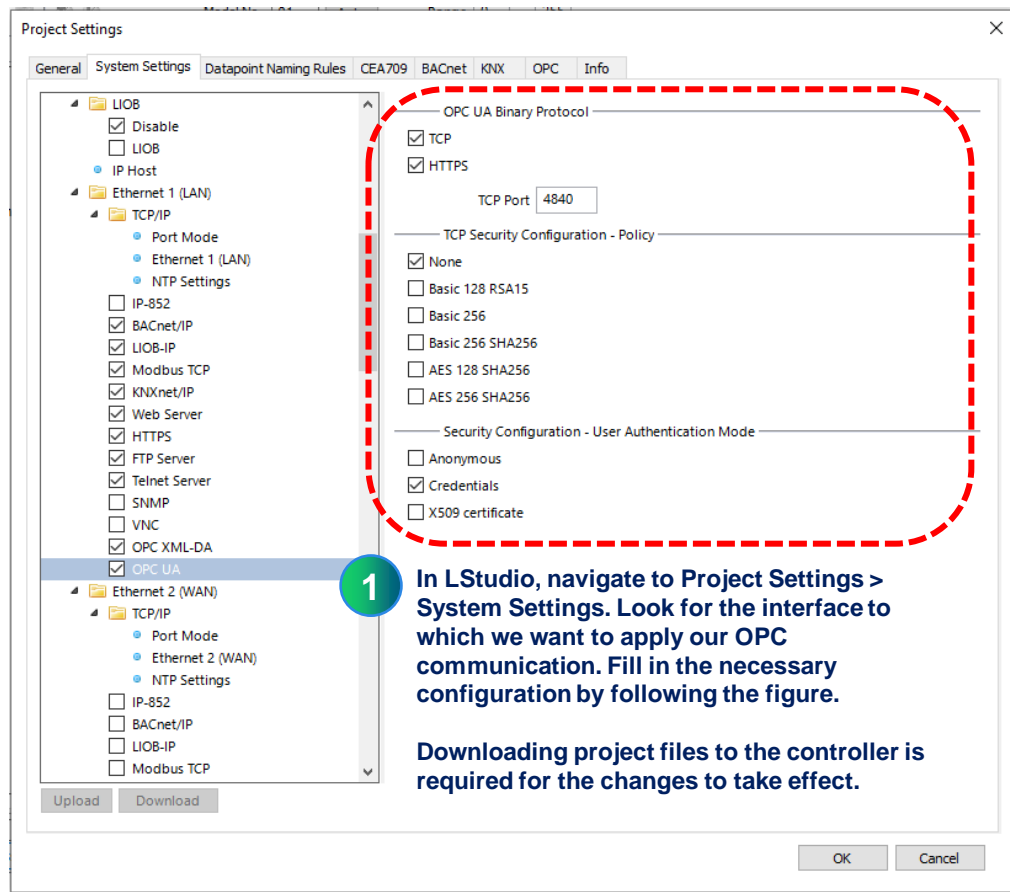
OK

Cancel

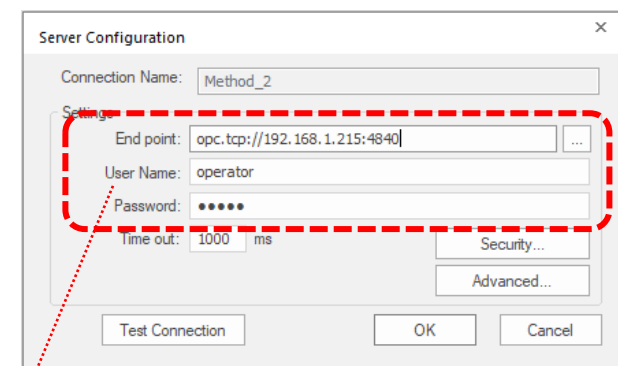
Method 2: Unencrypted And Authenticated connection mode

Security Policy : None

Authentication Mode: Credential



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



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.

Asynchronous read trigger:

asynReadTrigger

5

Connection: **Select connection method that we previously created.**

Method_2

Advanced...

Status:

Status Message:

Publish rate (ms):

1000

Disable:

6

Root node or view: **Browsing root node will make it much easier when selecting hierarchical OPC data points.**

/0:Objects/1:Loytec ROOT/1:User Registers

	Tag Name	Browse Path
	Filter text	Filter text
1	user_bVar	/1:bVar
2	user_iVar	/1:mVar
3	user_rVar	/1:aVar
4	user_sVar	
*		
*		
*		
*		
*		

7

Right click to browse OPC datapoints.

UA Browser

UA Server(/0:Objects/1:Loytec ROOT/1:User Register)

- sVar
- mVar
- aVar
- bVar

Available OPC datapoints will show in this area.

Selected Item: /1:aVar

Element Type: Variable

Data Type: Double

Node Id: ns=1;i=93328

Value: 18

Array Element:

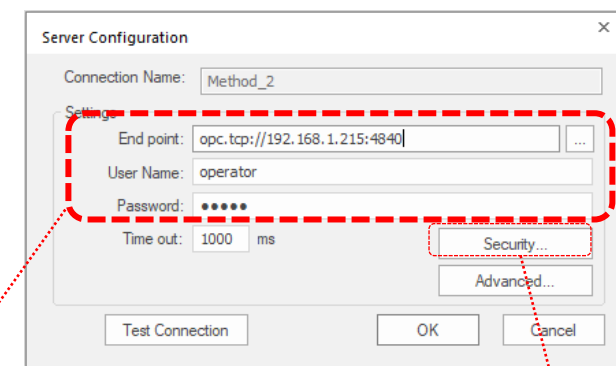
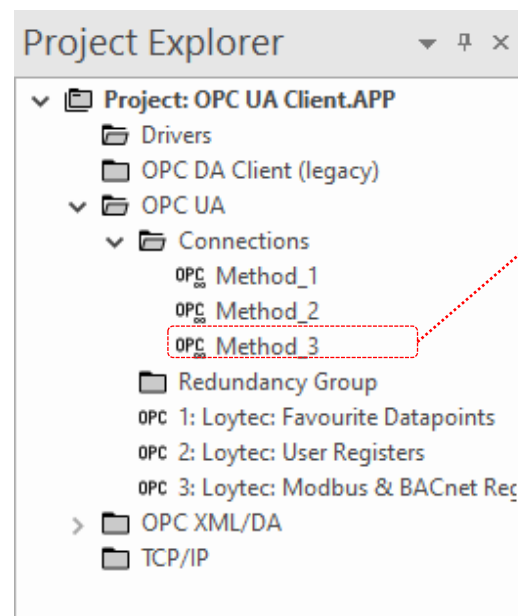
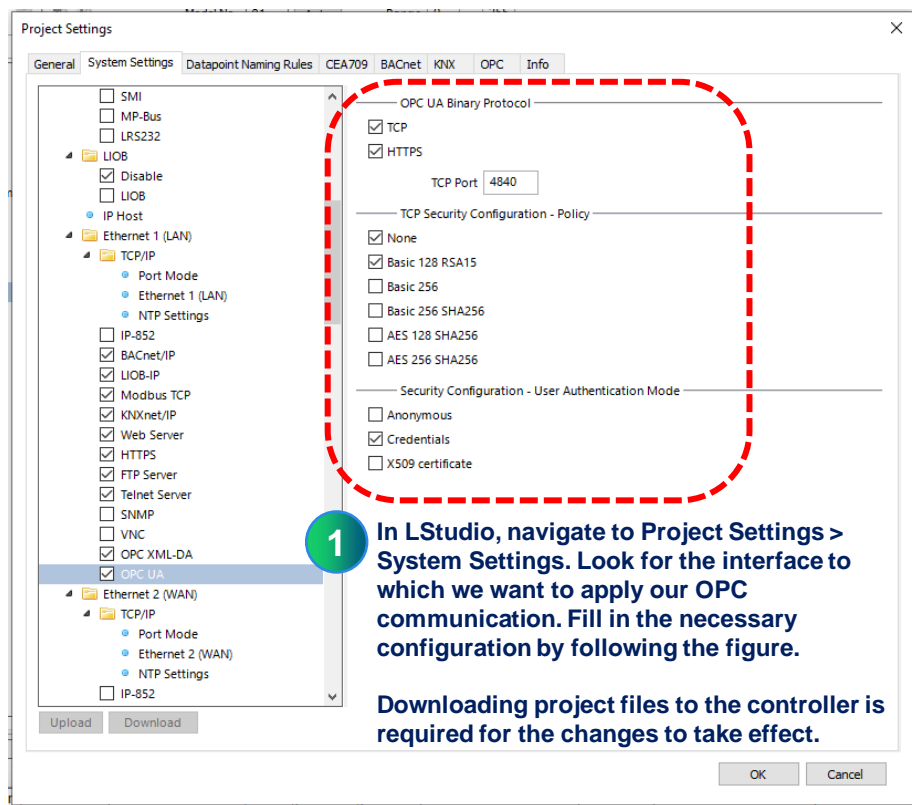
OK

Cancel

Method 3: Signed/Encrypted And Authenticated connection mode

Security Policy : Basic128Rsa15

Authentication Mode: Credential



Username : operator
Password : 12345

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

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

Security Settings

Message Security Mode: **Sign And Encrypt**

Security Policy: [Dropdown]

Endpoints

- opc.tcp://192.168.1.215:4840 - Sign And Encrypt
- opc.tcp://192.168.1.215:4840 - Sign - Basic128 Rsa15
- opc.tcp://192.168.1.215:4840 - None - None

Trust List (empty = Config\TrustList): [Empty list]

Issuer Certificate List (empty = Config\IssuerList): [Empty list]

☒ Automatically add server certificate to certificate store on the next connection

Buttons: Create self-signed certificate..., Trust server certificate, Session Security, OK, Cancel

Certificate Creation

Common Name: My company

Country (2 letters): US

Organization: Organization

Machine: linkwise-linn

Organization Unit: Unit

Client Uri: opc.tcp://linkwise-linn.Studio.Scada.Ua

Location Name: City

Expiration Date: 1/ 1/2074

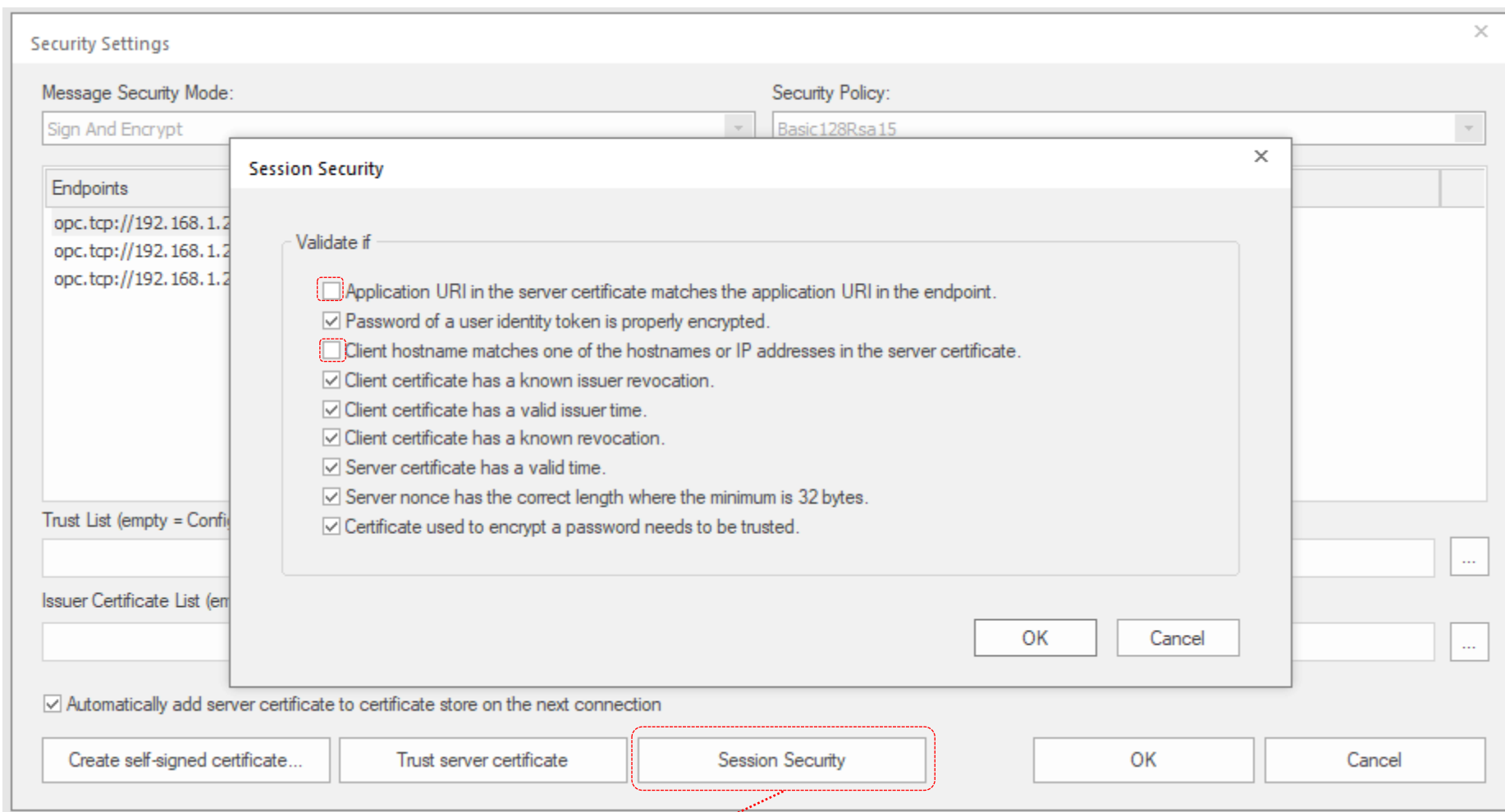
State/Province: State

RSA Key Size (Bits): 1024

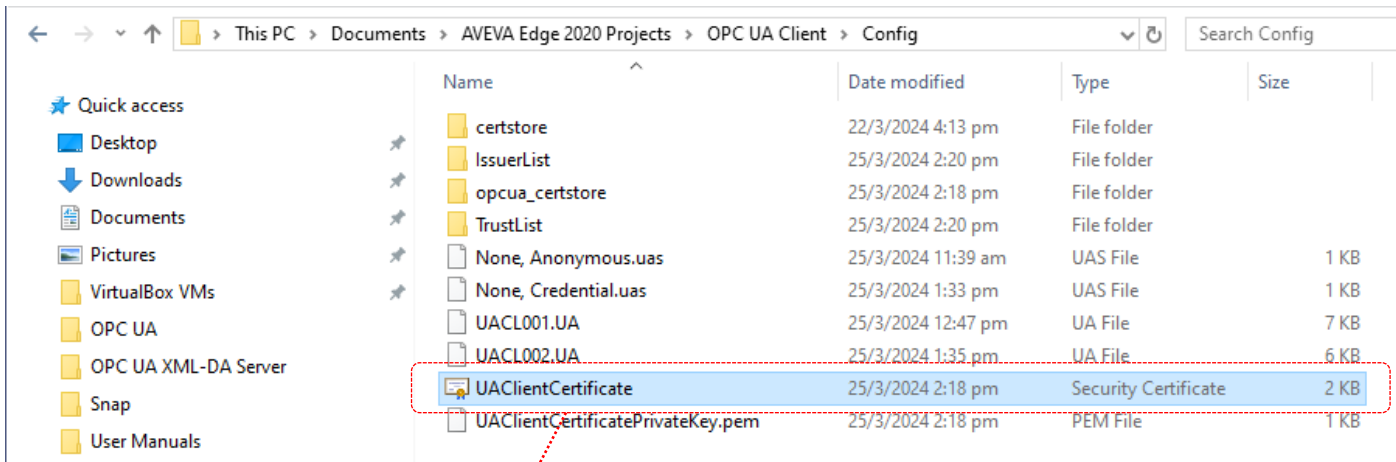
Buttons: Generate, Cancel

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)

Certificate Management

LINX-215
Logged in as
admin
2024-03-25 06:37:03

- Device Info
- Statistics
- Data
- Commission
- Config
- Programming
- Security**
 - Passwords
 - **Certificates**
 - User Management
- L-WEB
- L-IOB
- Documentation
- Maintenance
- Contact
- Logout

Warning: Managing certificates over an insecure connection is not recommended!

Installed Certificate
Create Certificate
Import Certificate
OPC UA

Get OPC UA Certificate: [Server certificate](#)

Add Client Certificate: Choose File No file chosen

Trusted List of OPC UA Clients:

Status	Common Name	Organization	Valid until	File name	Reject	Delete
✓	linkwise	linkwise technology	2073-12-31	UAClientCertific...der	<input type="checkbox"/>	<input type="checkbox"/>

Rejected List of OPC UA Clients:

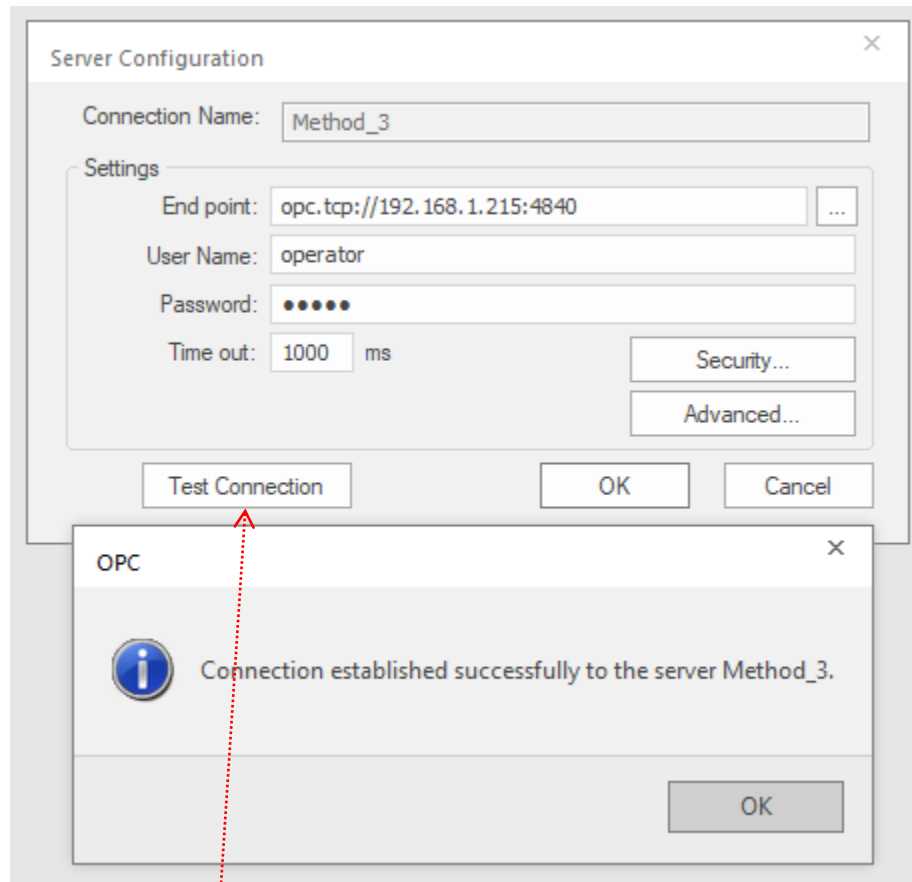
Status	Common Name	Organization	Valid until	File name	Trust	Delete
<div style="display: flex; justify-content: space-between; align-items: center; padding: 5px;"> 11 Save </div>						

10 Go to Security / Certificates / OPC UA

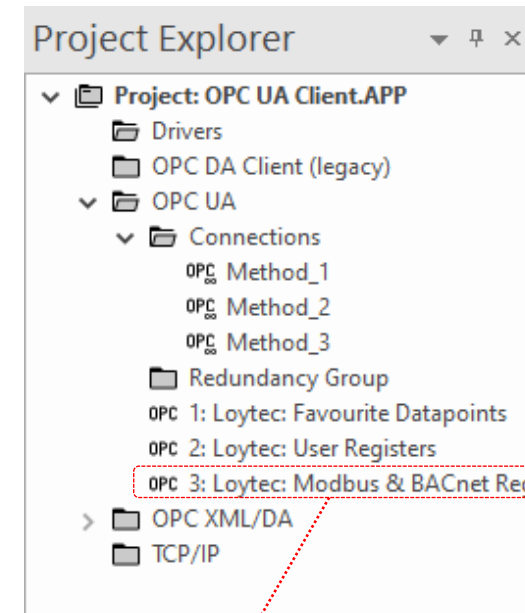
Click Add Client Certificate (Browse certificate file that we generated before)

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.

Asynchronous read trigger:

asynReadTrigger

Select connection method that we previously created.

14

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

15

OPC UA CL003.UA x Project Tags

Description:
Loytec: Modbus & BACnet Registers

Connection:
Method_3

Status:
Status Message:

Publish rate (ms):
1000

Disable:

Root node or view:
/0:Objects/1:Loytec ROOT

	Tag Name	
	Filter text	Filter text
1	modbus_M0	/1:Modbus Port T
2	modbus_X0	/1:Modbus Port T
3	modbus_Y0	/1:Modbus Port T
4	bacnet_AI	/1:BACnet Port/1:1
5	bacnet_AO	/1:BACnet Port/1:1
6	bacnet_AV	/1:BACnet Port/1:1
7	bacnet_BI	/1:BACnet Port/1:1
8	bacnet_BO	/1:BACnet Port/1:1
9	bacnet_BV	/1:BACnet Port/1:1
*		
*		
*		
*		
*		

16 Right click to browse OPC datapoints.

UA Browser

UA Server(/0:Objects/1:Loytec ROOT)

- > E-Mail
- > AlarmLogs
- > LIOB-IP
- > LIOB-FT
- > LIOB
- > Modbus Port TCP
- > CEA852 Port
- > BACnet Port
 - > Datapoints
 - multistateValue
 - analogValue
 - analogOutput
 - analogInput
 - binaryValue
 - binaryOutput
 - binaryInput
 - > CEA709 Port
 - > User Registers
 - > System Registers
 - > Favorites

Available OPC datapoints will show in this area.

Selected Item: /1:BACnet Port/1:Datapoints/1:binaryOutput

Element Type: Variable Data Type: Boolean

Node Id: ns=1;i=97344

Value: false

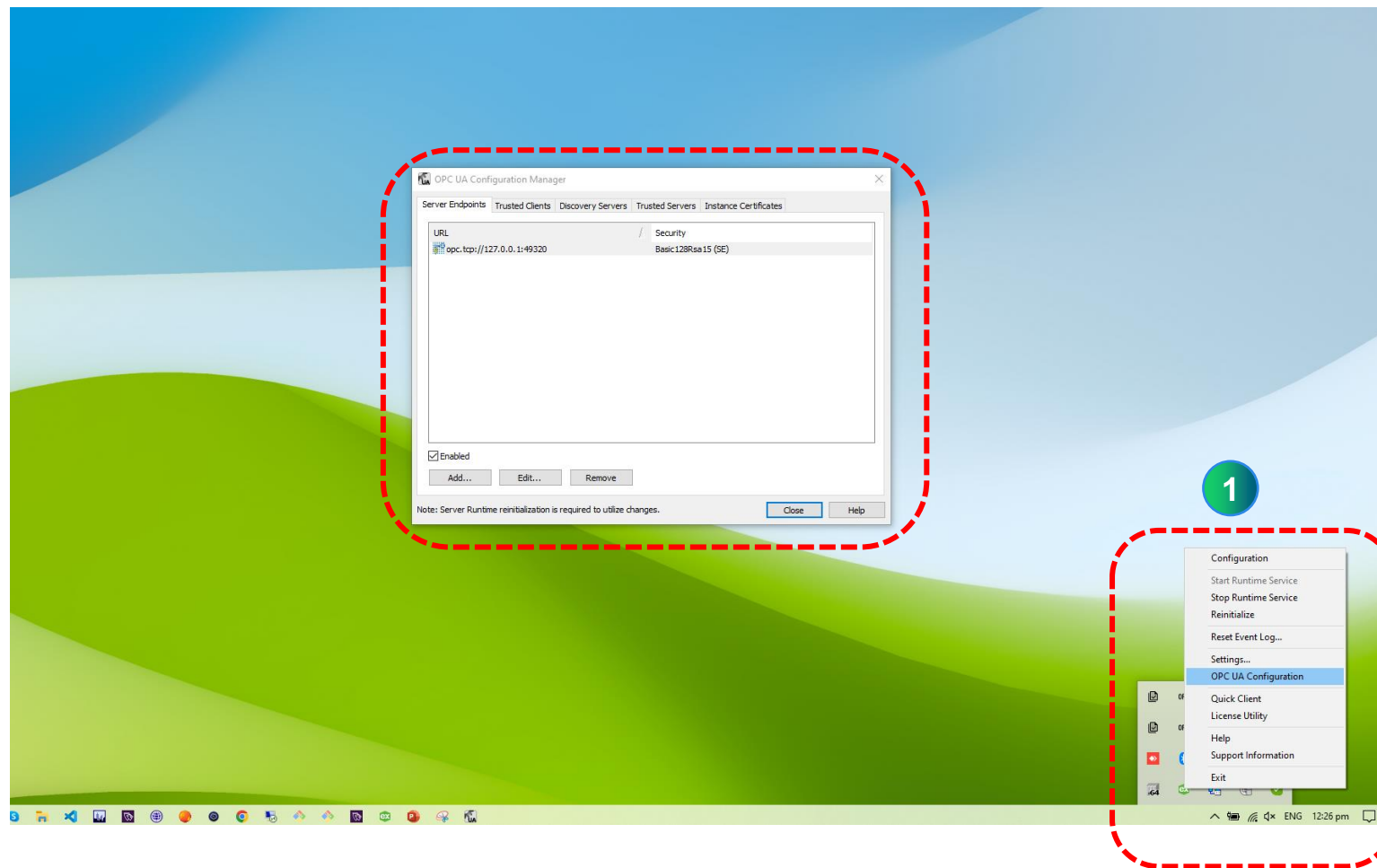
Array Element:

OK Cancel

Method 4: Signed/Encrypted And Authenticated connection mode

Security Policy : Basic128Rsa15

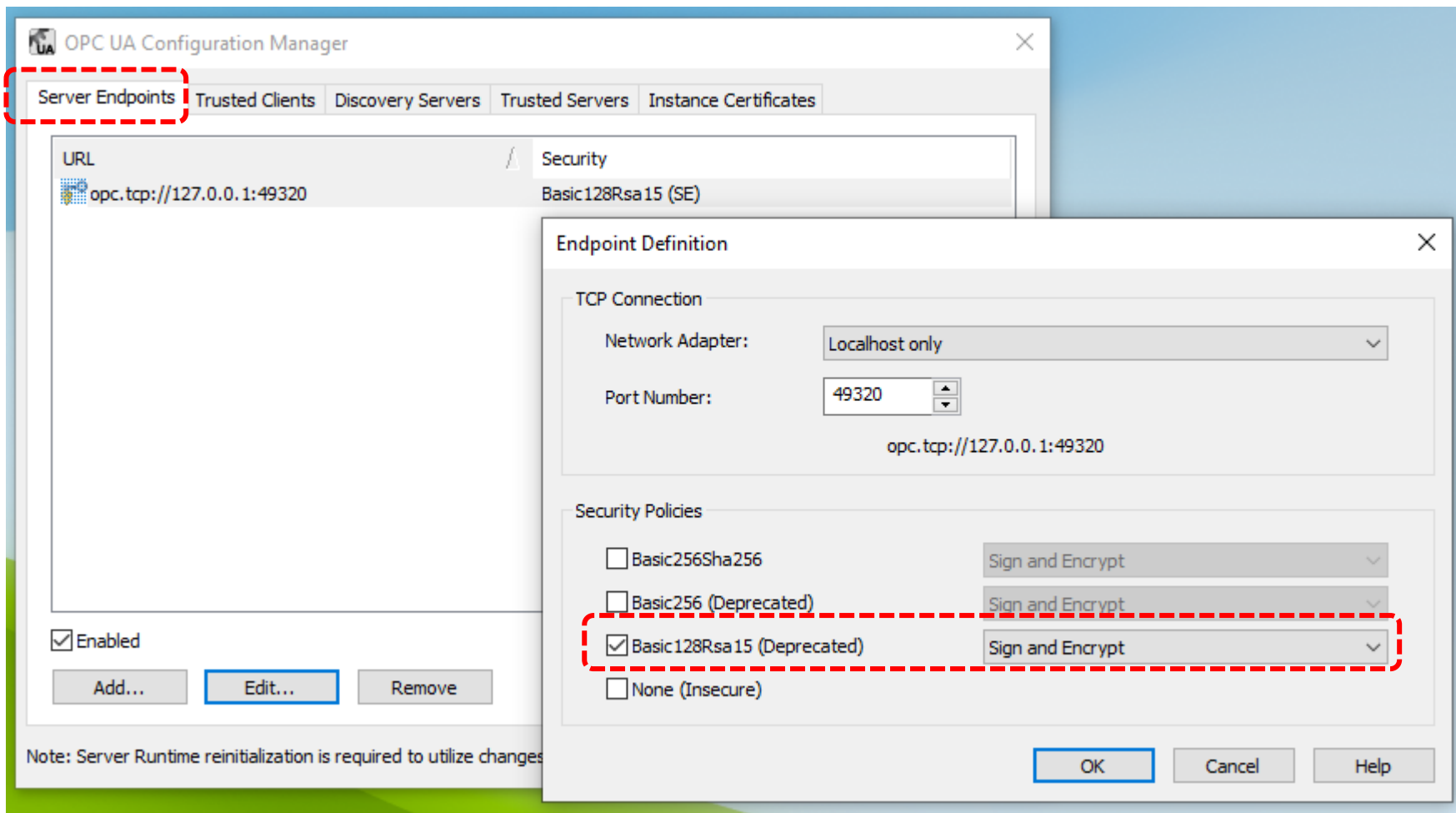
Authentication Mode: Credential



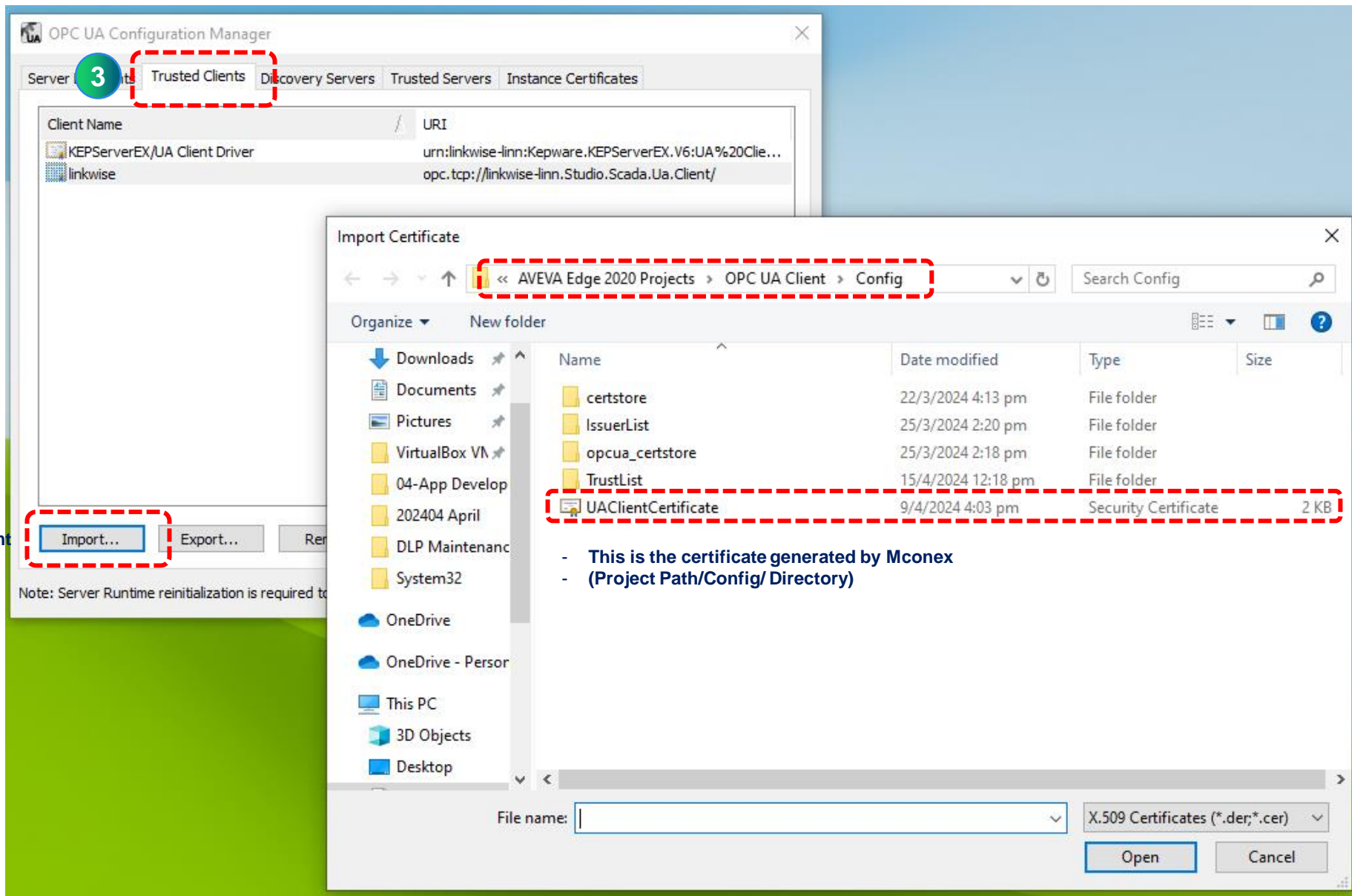
- Right click on the kepware icon in system tray to open the configuration menu
- Click on OPC UA Configuration

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

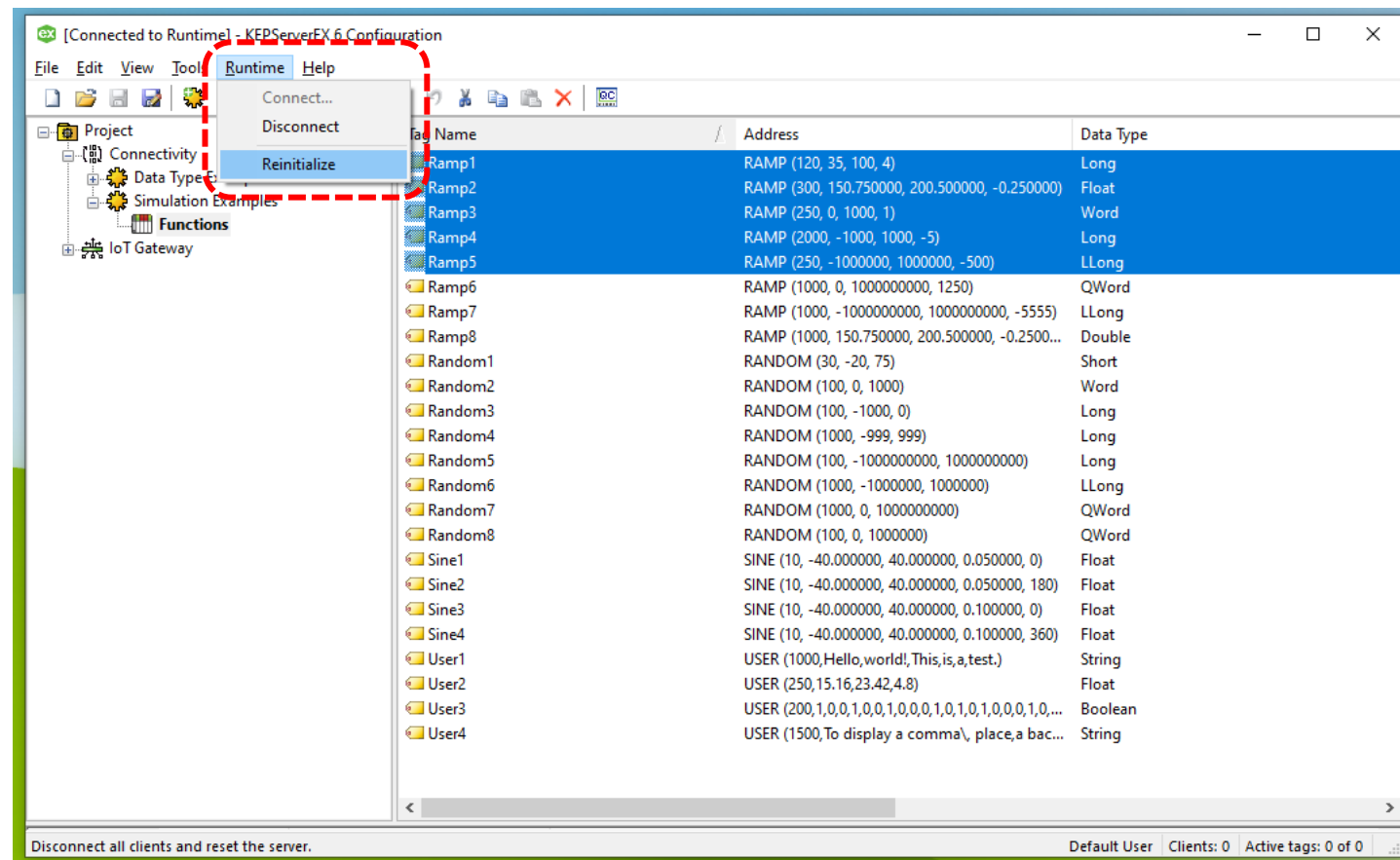
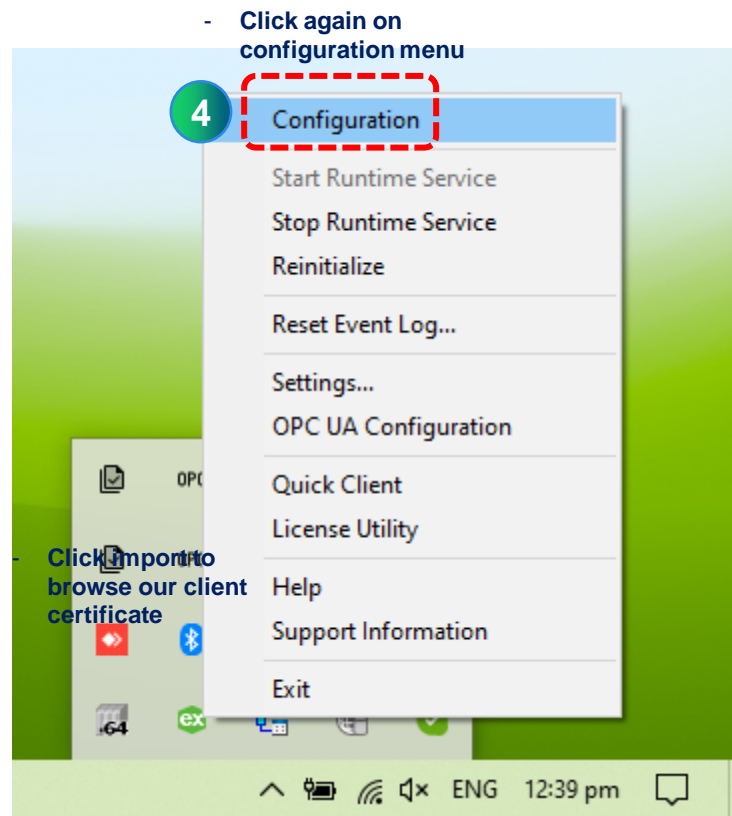
2

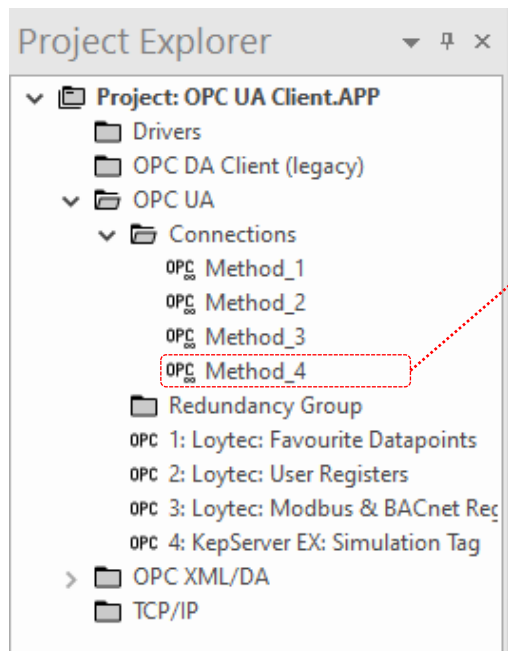


- Select connection mode
- (For production env, always consider for most secure encryption method and connection mode)

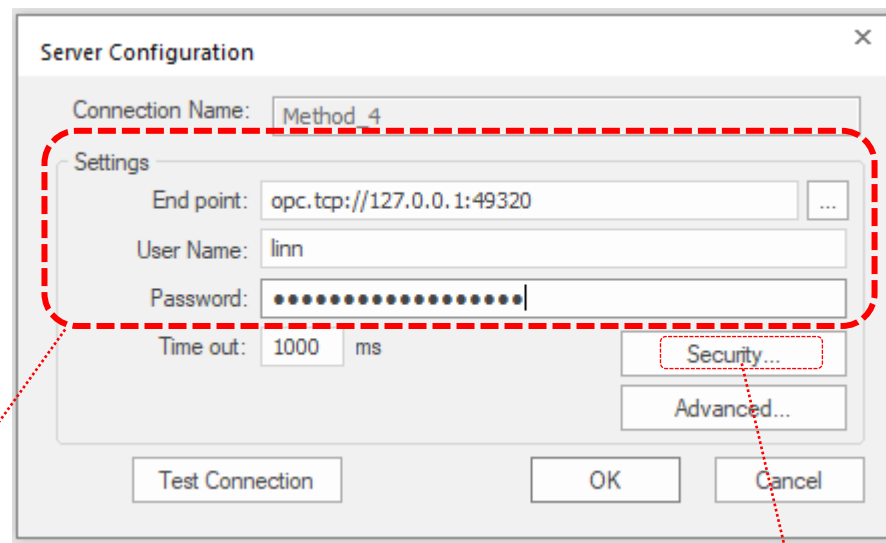


- Click Reinitialize in order to restart OPC UA Server Runtime Service





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

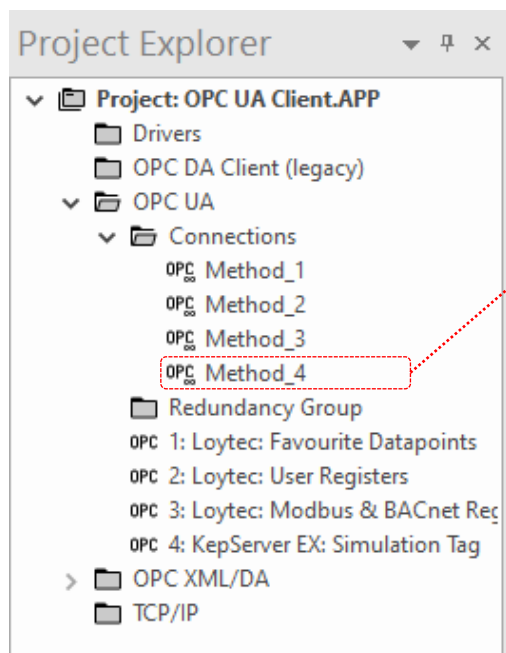


6

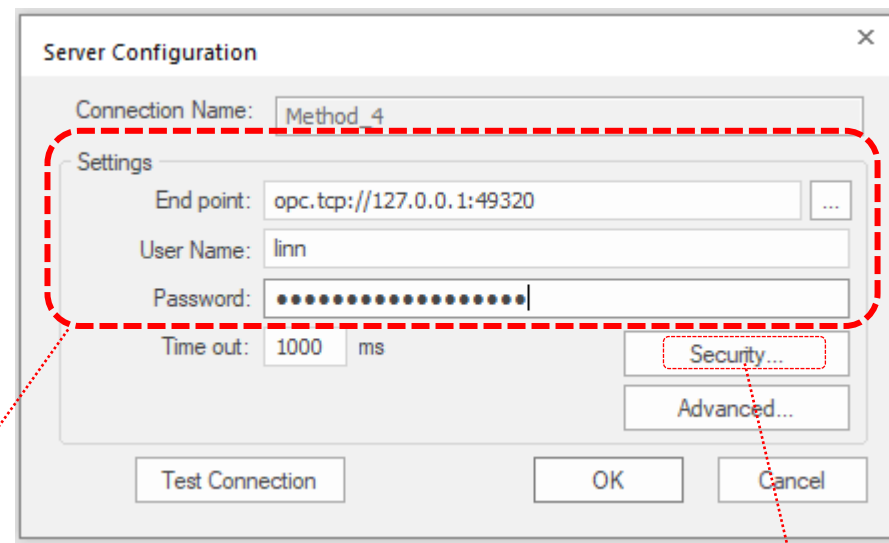
The endpoint URL for OPC TCP Binary communication should be `opc.tcp://ip_address:49320`. Alternatively, you can press the search icon to browse available OPC servers.

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]

Trust List (empty = Config\TrustList):

Issuer Certificate List (empty = Config\IssuerList):

☒ Automatically add server certificate to certificate store on the next connection

Create self-signed certificate...

Trust server certificate

Session Security

OK

Cancel

9 Select connection method.

Check this !

10

Select connection method that we previously created.

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

OPC UA004.UA x

Description:
KepServer EX: Simulation Tag

Connection:
Method_4

Status:
Status Mes

Publish rate (ms):
1000

Disable:

Root node or view:
/0:Objects/2:Simulation Examples/2:Functions

	Tag Name	
	Filter text	Filter text
1	keppure_Ramp1	/2:Ramp1
2	keppure_Ramp2	/2:Ramp2
3	keppure_Ramp3	/2:Ramp3
4	keppure_Ramp4	/2:Ramp4
5	keppure_Ramp5	/2:Ramp5
*		
*		
*		
*		
*		

Right click to browse OPC datapoints.

UA Browser

UA-Server(/0:Objects/2:Simulation Examples/2:Functions)

- _System
- Ramp1
- Ramp2
- Ramp3
- Ramp4
- Ramp5
- Ramp6
- Ramp7
- Ramp8
- Random1
- Random2
- Random3
- Random4
- Random5
- Random6
- Random7
- Random8
- Sine1
- Sine2
- Sine3

Available OPC datapoints will show in this area.

Selected Item: /2:Ramp5

Element Type: Variable Data Type: Int64

Node Id: ns=2;s=Simulation Examples.Functions.Ramp5

Value: -1000000

Array Element:

OK Cancel