

Configure encrypted opc-ua server from Phoenix Contact PlcNext PLC with Ignition

CODESYS North America

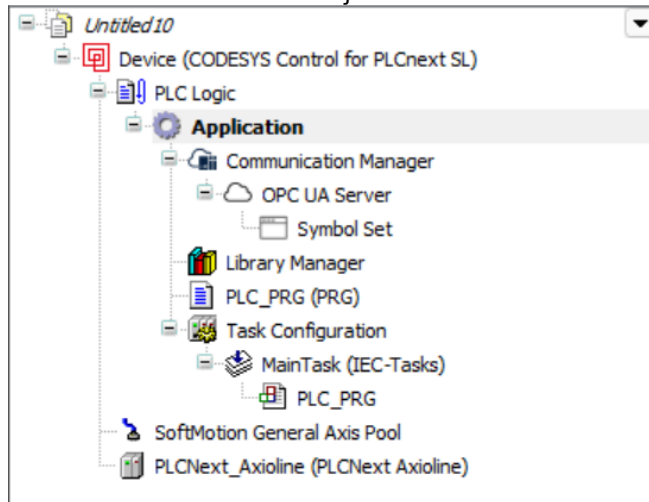
Exported on 09/12/2023

Table of Contents

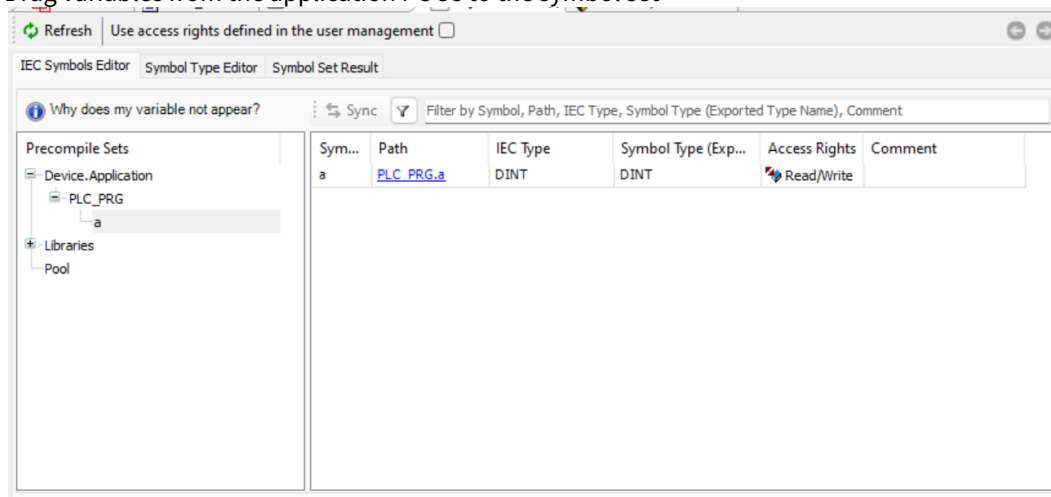
No headings included in this document

Description: this article describes the configuration details to set up encrypted OPC-UA

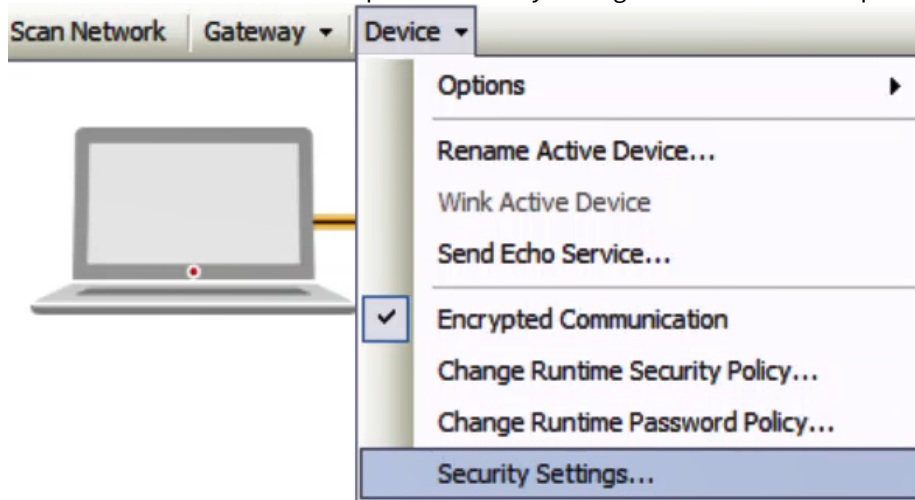
1. First add a communication manager object to project
2. Then add an OPC-UA server object to the communication manager



3. Drag variables from the application POU's to the symbol set



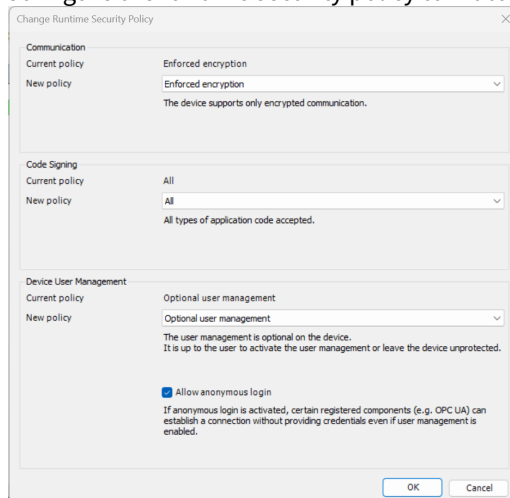
4. Double-click on the device and open the security settings from the device drop-down



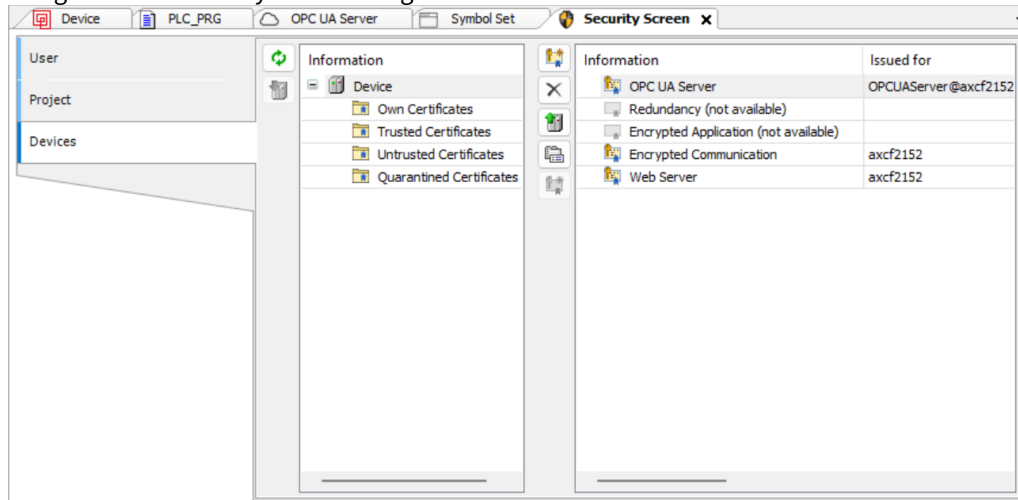
5. Configure the security settings to match the following:

Setting	Value
CmpOPCUAServer	
CommunicationPolicy	POLICY_BASIC256SHA256
CommunicationMode	ALL
Activation	ACTIVATED
UserAuthentication	ENABLED
AllowUserPasswordOnPlaintext	YES
EnableCRLChecks	YES
EnableSelfSignedCertBackwardInteroperability	YES
DeactivateSecurityPolicy	
ApplicationName	OPCUAServer@axcf2152
CompanyOrOrganizationName	
City	
State	
Country	

6. Open the "Change runtime security policy" settings from the device drop-down
 7. Configure the runtime security policy to match the following:



8. Navigate to the security screen and generate a certificate for the OPC-UA server



9. Create a new OPC connection from Ignition from the gateway configuration:

Name	Type	Description	Read Only	Status	
Ignition OPC UA Server	OPC UA	A "loopback" connection to the Ignition OPC UA server running on this gateway.	false	Connected	More edit
OPCUAServer@axcf2152	OPC UA		false	Connected	More edit

[→ Create new OPC Connection...](#)

Note: For details about a connection's status, see the [OPC Connection Status](#) page.

10. Choose OPC-UA

☒ **OPC UA**
Connect to a device or server that supports OPC UA.

☐ **OPC-DA COM Connection**
Provides access to legacy COM-based OPC-DA servers. Supports OPC-DA versions 2 and 3.

[Next >](#)

11. Enter the IP address of the PLCNext device followed by Port 4840:

[→ Skip to Advanced Configuration](#)

Server Discovery

Endpoint URL

192.168.1.10:4840

Example: opc.tcp://localhost:62541/discovery

[Next](#)

12. Select the OPC-UA server from the available list:

[→ Skip to Advanced Configuration](#)

Choose a Server

OPCUAServer@axcf2152

☒ **opc.tcp://192.168.1.10:4840**

[Previous](#) [Next](#)

13. Choose the Basic256Sha256 policy with SignAndEncrypt mode selected:

<input type="radio"/>	opc.tcp://192.168.1.10:4840	Security Policy: None Security Mode: None
<input checked="" type="radio"/>	opc.tcp://192.168.1.10:4840	Security Policy: Basic256Sha256 Security Mode: SignAndEncrypt
<input type="radio"/>	opc.tcp://192.168.1.10:4840	Security Policy: Basic256Sha256 Security Mode: Sign

14. Choose to trust the certificate from the Ignition side:

[Skip to Advanced Configuration](#)

Manage Certificate
Common Name: OPCUAServer@axcf2152 Organization: Organizational Unit: Locality: State or Province: Country: SHA-1 Fingerprint: d8241c64adb3fc81438cd142961d24e4b08e4263 Expiration: Fri Sep 09 06:19:26 PDT 2033
Trust certificate? <input type="radio"/> No <input checked="" type="radio"/> Yes

Previous

Next

15. Confirm the connection settings and click finish:

Confirm Connection Settings
Discovery URL: opc.tcp://192.168.1.10:4840 Endpoint URL: opc.tcp://192.168.1.10:4840 Endpoint Host Override: Endpoint Security Mode: SignAndEncrypt Endpoint Security Policy: Basic256Sha256
<p>Previous</p> <p>Finish</p>

16. Enter a unique name and clear out the password field:

Main	
Name	PhoenixContact
Description	
Enabled	<input checked="" type="checkbox"/> (default: true)
Read Only	<input type="checkbox"/> If selected, the connection to this OPC server will be read-only; all calls to write will fail. (default: false)
Authentication	
Username	
Password	
Password	Re-type password for verification.

☐ Show advanced properties

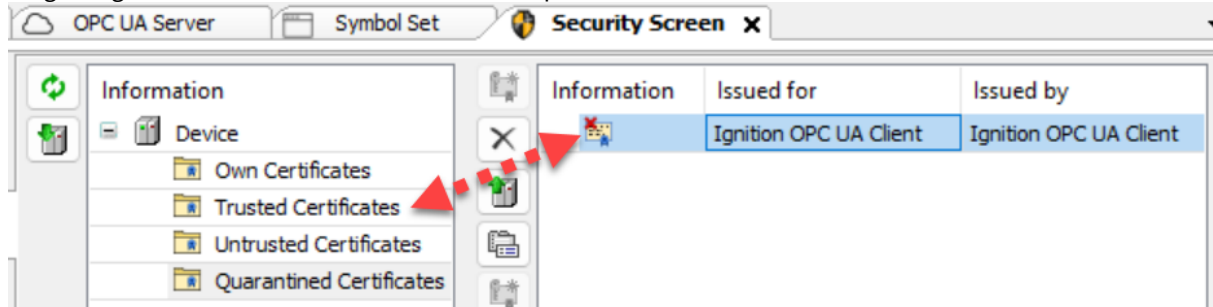
Create New OPC Connection

17. Click on create new OPC connection

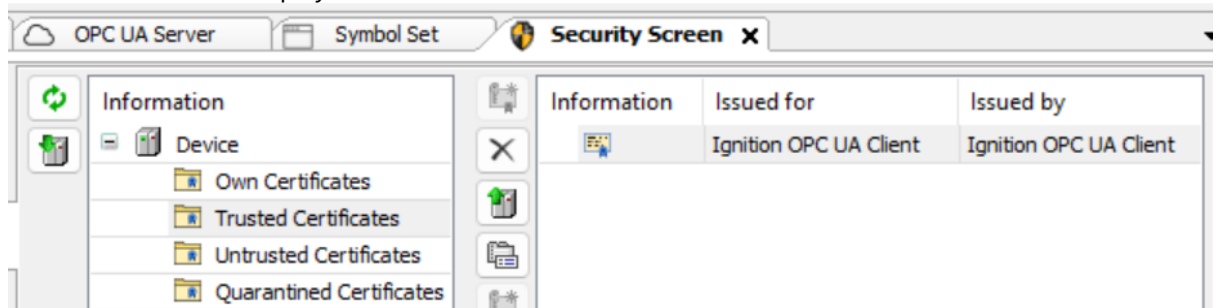
18. Now, you need to trust the certificate from the Codesys side
19. Open the security screen by double-clicking on the security icon



20. Drag the Ignition OPC client certificate from the quarantined certificates to the trusted certificates folder



21. The certificate will be displayed in the trusted certificates folder:



22. Login to the controller with the changes
23. Ignition will display a successful connection:

✓ Successfully updated OPC Connection "PhoenixContact"

Name	Type	Description	Read Only	Status	
Ignition OPC UA Server	OPC UA	A "loopback" connection to the Ignition OPC UA server running on this gateway.	false	Connected	More ▾ edit
OPCUAServer@axcf2152	OPC UA		false	Connected	More ▾ edit
PhoenixContact	OPC UA		false	Connected	More ▾ edit

[→ Create new OPC Connection...](#)

Note: For details about a connection's status, see the [OPC Connection Status](#) page.