

## OPC UA Client

Supported Series: Weineth OPC UA Server, Unified Automation, Prosys, Kepware

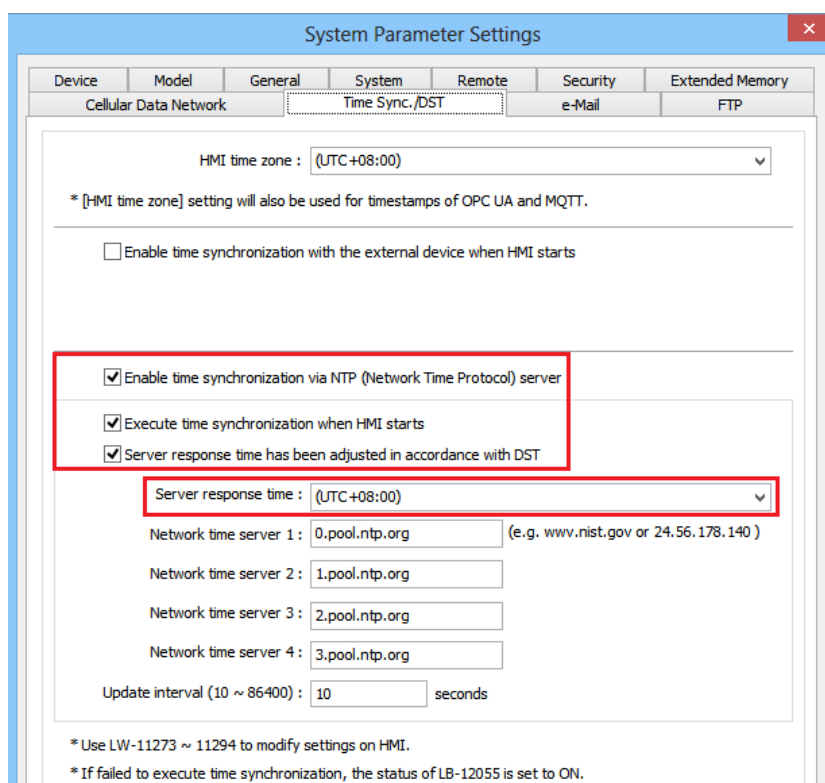
### HMI Setting:

Parameters	Recommended	Options	Notes
PLC type	OPC UA Client		
PLC I/F	Ethernet		
Port no.	4840		
Security policy	None	None / Basic128Rsa15 / Basic256 /	
Message security mode	None	None / Sign/ SignAndEncrypt	
Re-Build Certificate when HMI Starts			
Use sha-256 mode (default sha-1)			
Support Uncertain Initial Value			

On-line simulator	Yes	Multi-HMI connect	Yes
-------------------	-----	-------------------	-----

When you use opc ua client for the first time, you need to set time related settings, please refer to the settings below.

### System Parameter Setting -> Time Sync./DST



System Parameter Settings

Device Model General System Remote Security Extended Memory

Cellular Data Network Time Sync./DST e-Mail FTP

HMI time zone : (UTC+08:00)

\* [HMI time zone] setting will also be used for timestamps of OPC UA and MQTT.

☐ Enable time synchronization with the external device when HMI starts

☒ Enable time synchronization via NTP (Network Time Protocol) server

☒ Execute time synchronization when HMI starts

☒ Server response time has been adjusted in accordance with DST

Server response time : (UTC+08:00)

Network time server 1 : 0.pool.ntp.org (e.g. www.nist.gov or 24.56.178.140)

Network time server 2 : 1.pool.ntp.org

Network time server 3 : 2.pool.ntp.org

Network time server 4 : 3.pool.ntp.org

Update interval (10 ~ 86400) : 10 seconds

\* Use LW-11273 ~ 11294 to modify settings on HMI.

\* If failed to execute time synchronization, the status of LB-12055 is set to ON.

## Update Mode:

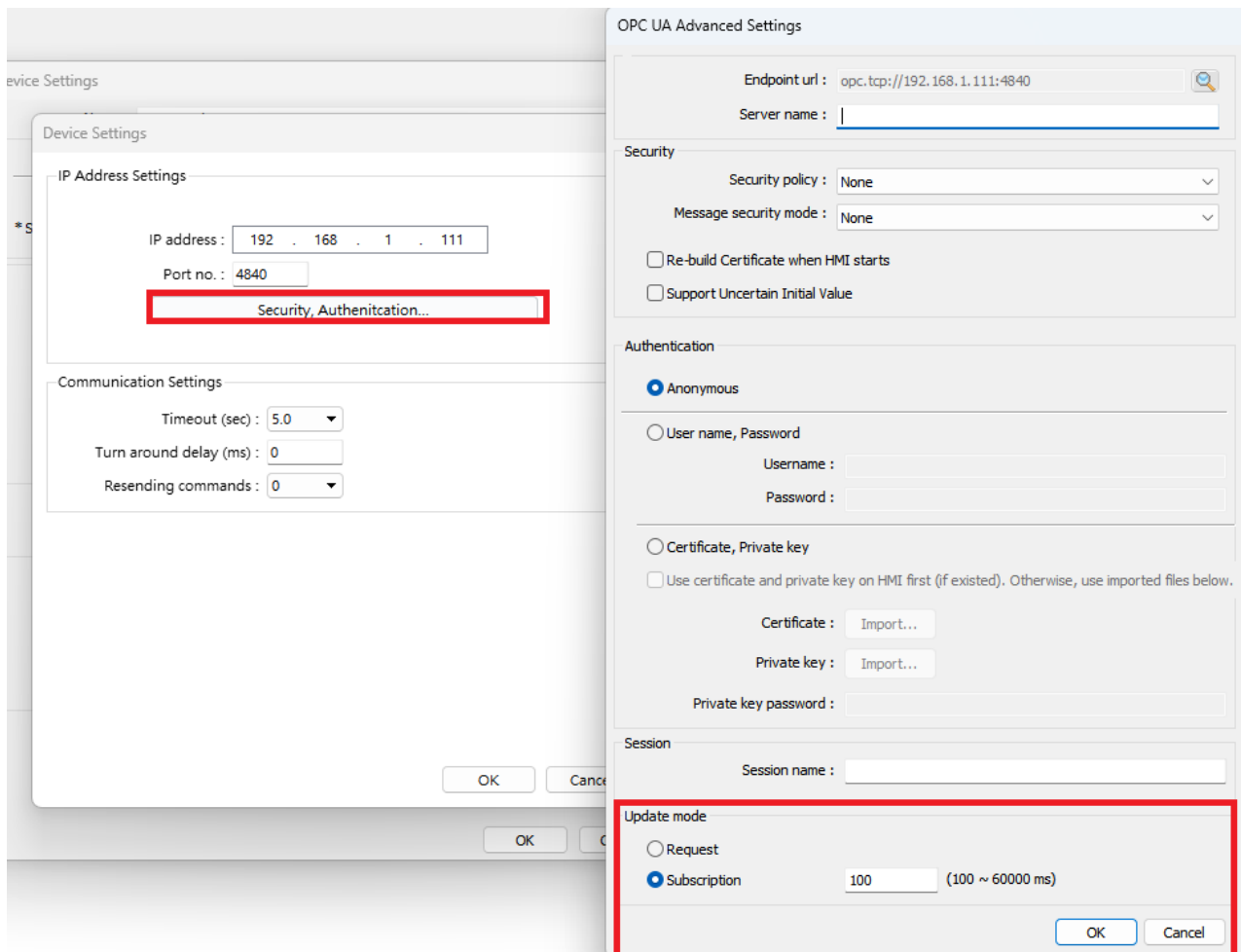
### [Request Mode]

The opcau client will actively send a ReadRequest packet to the opcau server. After the server receives the packet, it sends it back to the opcau client using a ReadResponse packet.

### [Subscription Mode]

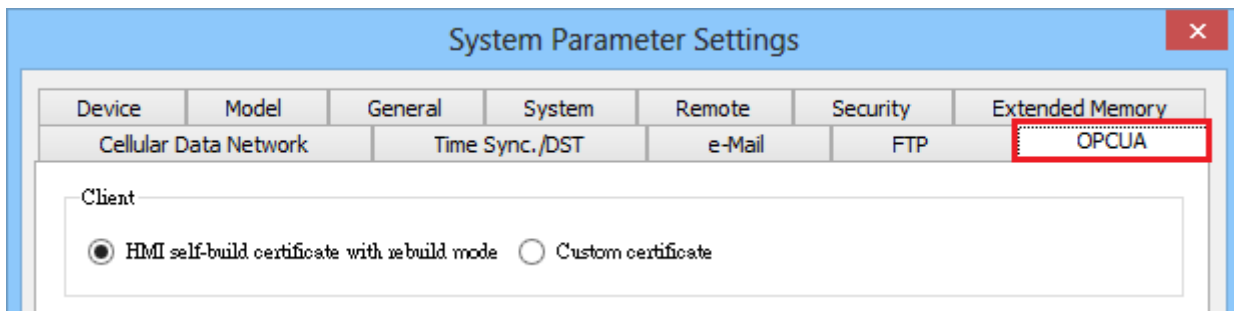
The server regularly performs tag sampling on the PLC.

1. If the "value" or "status" of the TAG changes, the PublishResponse will be sent to the client in the next Publishing tick.
2. If the values do not change, an empty PublishResponse will be sent to the client to ensure that the connection is still established, otherwise it will timeout.



## Certificate:

### HMI self-build certificate with rebuild mode:



#### [Re-build Mode]

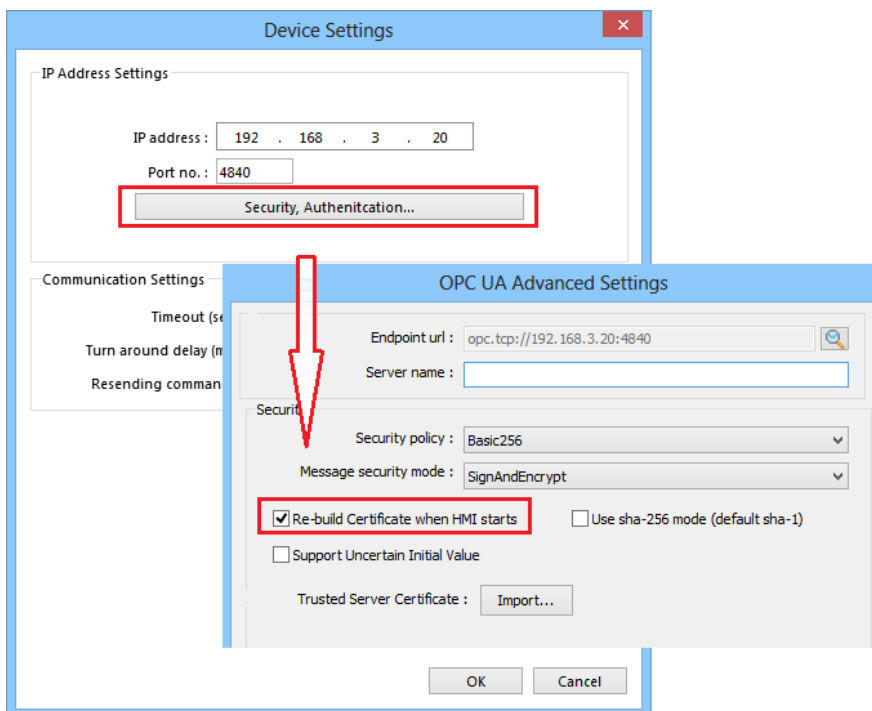
Does the certificate exist in the HMI?

1. Yes, overwrite the certificate and reload it.
2. No, create a new credential and load it.

#### [Not Re-build Mode]

Does the certificate exist in the HMI?

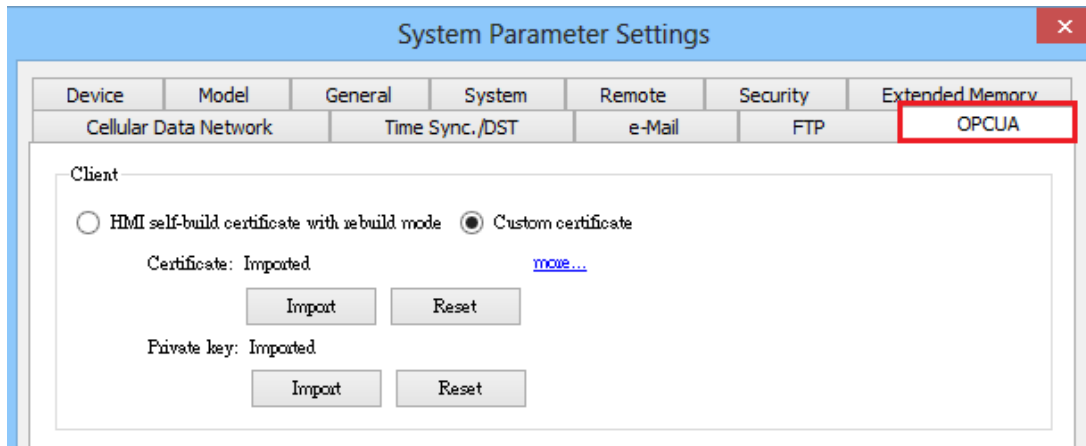
1. Yes, load the credentials existing in the HMI.
2. No, there is no certificate in the HMI and cannot communicate with the server.



## Custom Certificate:

Import custom certificate

\*Note: If you choose to import a custom certificate, you cannot check rebuild certificate, otherwise the certificate will be overwritten.



Note: The **[Custom Certificate]** function can only be downloaded to HMI and cannot be used for online simulation.

## Support Device Type:

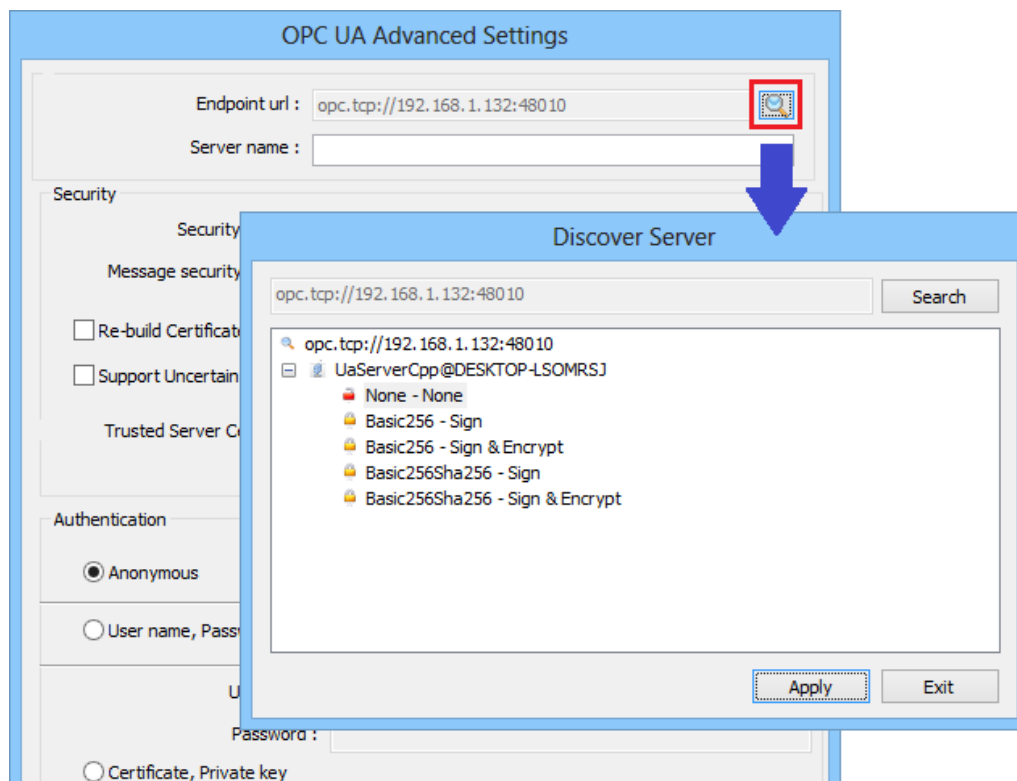
Data type	EasyBuilder data format	Memo
Bool	bit	
Int	16-bit BCD, Hex, Binary, Signed	16-bit
UInt	16-bit BCD, Hex, Binary, Unsigned	16-bit
DInt	32-bit BCD, Hex, Binary, Signed	32-bit
Real	32-bit Float	32-bit
UDInt	32-bit BCD, Hex, Binary, Unsigned	32-bit
LInt	64-bit Signed	64-bit
ULInt	64-bit Unsigned	64-bit
Double	64-bit Float	64-bit

**Note:** EBPro V6.03.02 or later supports 64 bits data type (**cMT Series only**), but please note that the address limit range is 48 bits in maximum..

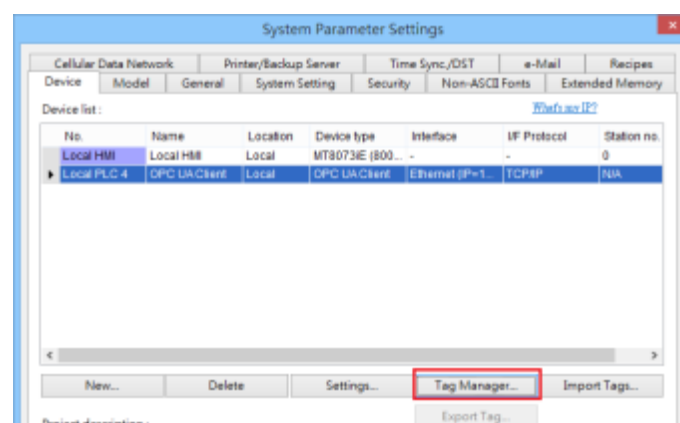
## Tag Manager:

1. In EasyBuilder Pro, add OPC UA Client into the device list, set **[IP address]**, **[Port no.]**, and then open **[Security, Authentication]**.

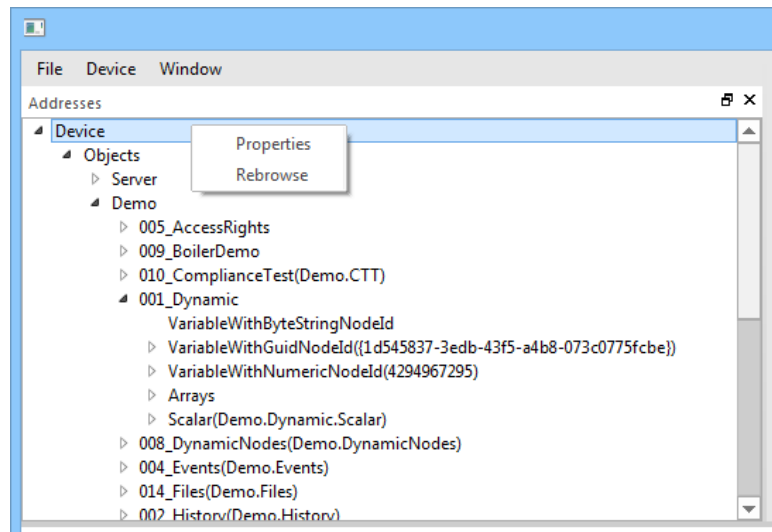
2. Click the magnifier icon near the **[Endpoint url]** field to open Discover Server window. In the window the security parameters of OPC UA Server can be found. Click **[Apply]**, the parameters will be automatically filled into the fields in Security group box in OPC UA Settings window. Finish the rest of the settings and then click **[OK]** to leave.



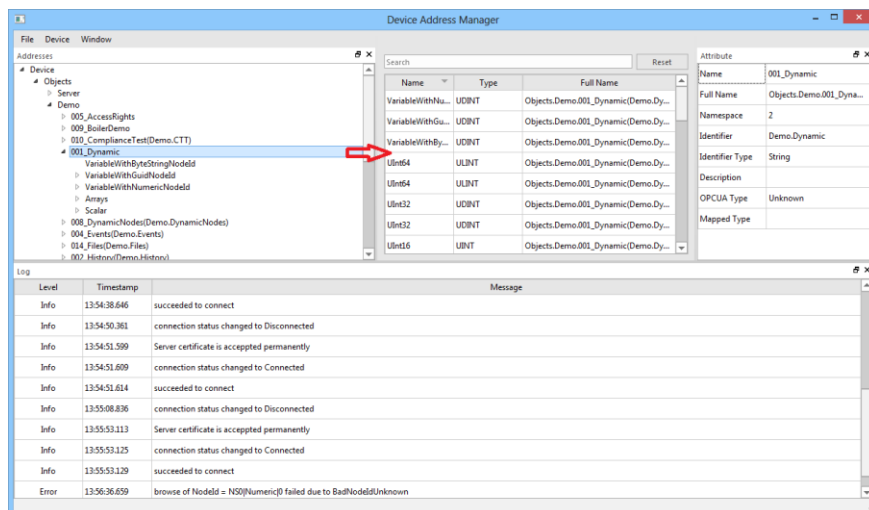
3. Click Tag Manager. If **“Connection failed.”** message appears, please check the communication parameters.



#### 4. Device (right click) -> Rebrowse -> Expand node

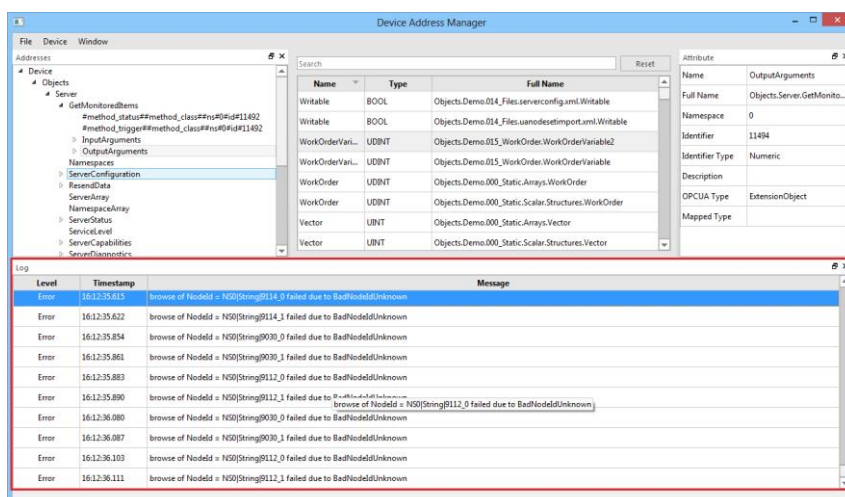


5. Drag the address to be added to the right area. If the node has child nodes, they will be added as well.



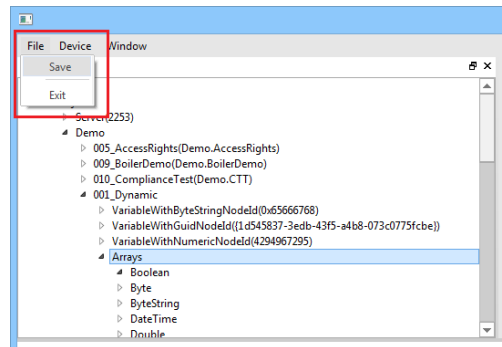
6. Log will display the import results, and unsupported data types will display a message in this field.

UaStatus code: <https://www.opcti.com/common-error-codes.aspx>



7. After importing the address, save it and leave. The specific operations are as follows:

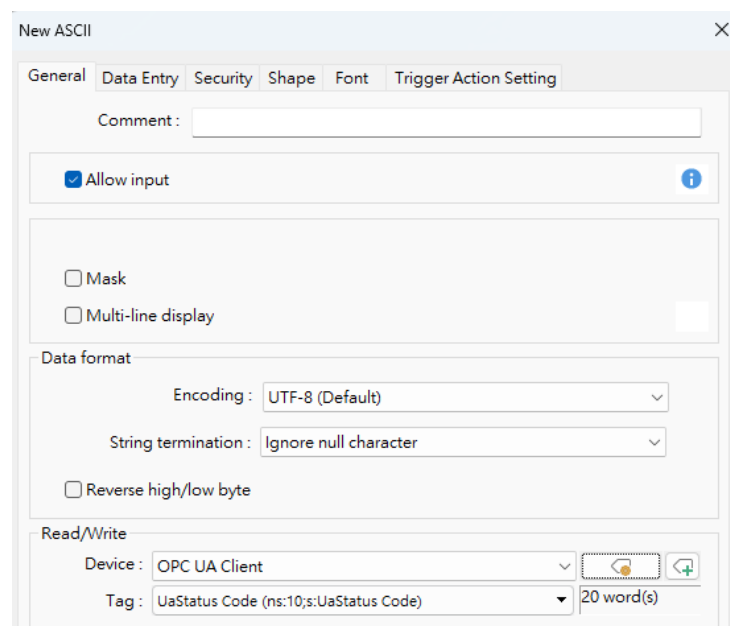
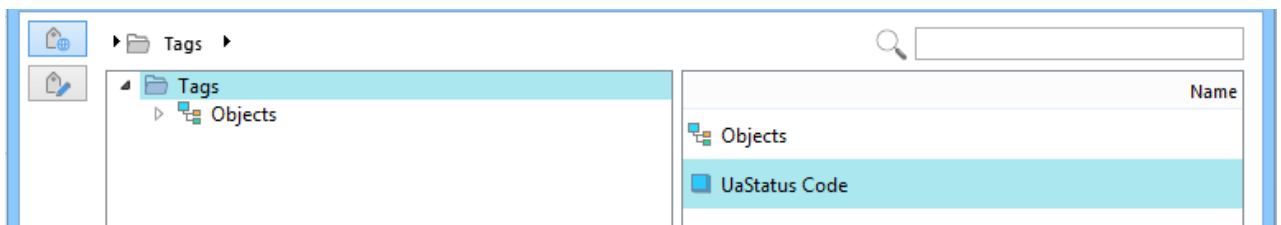
**[File] -> [Save] -> [Exit]**



## Connection Diagnostics:

The UaStatus Code address can be used to diagnose communication connection problems. If the project was created earlier, this address may not be found. The user can enter the tag manager to get the tag again, and then use the ASCII object to read the data. The information that can be obtained is as follows:

- Error code for failed connection
- “GOOD” will be displayed if the connection is successful.



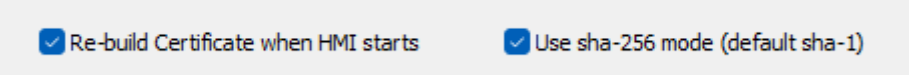
The following describes common Error Codes and solutions.

### 1. BadCertificateHostNameInvalid

**[Reason]:** client-certificate does not match the HMI.

**[Solution]:**

1.1 Check the following two options and download the project again.



☒ Re-build Certificate when HMI starts      ☒ Use sha-256 mode (default sha-1)

1.2 If the user needs to import client-certificate, please make sure the created client-cert matches the HMI name.


### 2. BadCertificateTimeInvalid

**[Reason]:** The server checks whether the client- certificate on the HMI has expired or has not yet taken effect.

**[Solution]:**

2.1 Check the time setting of the HMI.

2.2 Confirm whether the time when the client-certificate was generated is normal. If the time is abnormal, please check the following two options and re-download the project. After the download is complete, confirm the client-cert again.



☒ Re-build Certificate when HMI starts      ☒ Use sha-256 mode (default sha-1)

2.3 How to confirm client-cert

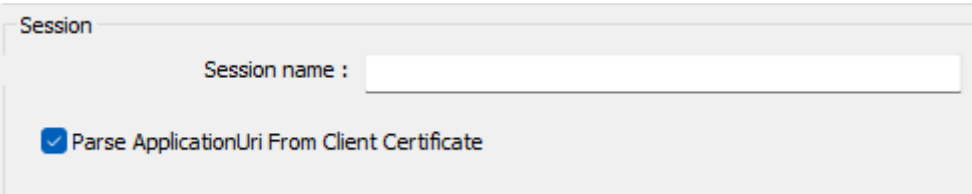
2.3.1 Confirm from the OPC UA Server's Credential Management System UI.

2.3.2 If the OPC UA server is a Weintek HMI, users can confirm the client- certificate of the OPC UA client from Easyweb.

### 3. BadCertificateUriInvalid

**[Reason]:** This is common when you import your own client-cert. When the client-certificate uri created by the user has a problem.

**[Solution]:** Check the following options to download again



Session

Session name :

☒ Parse ApplicationUri From Client Certificate



## 4. BadCommunicationError

**[Reason]:** Network communication failed

**[Solution]:**

- 4.1 Check the target IP/Port no. settings are correct, ping to see if it works.
- 4.2 Check that the network cable is plugged into the HMI and the network indicator is displayed correctly, and check that the HMI network settings are correct.
- 4.3 After confirmation, the user can re-download the project or restart the HMI to re-confirm communication.

## 5. BadSecurityChecksFailed

**[Reason]:** The OPC UA server does not trust the client-certificate sent by the opcua client yet

**[Solution]:** Open the server management certificate page and trust the corresponding client- certificate.

### Example1: UA Demo Server

1.1 UA Demo Server management page, find the corresponding credentials.

UA Server Administration - C:/Program Files (x86)/UnifiedAutomation/UaCPPServer/bin/ServerConfig.xml

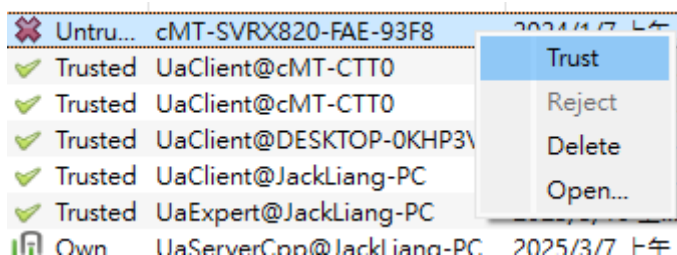
UA Endpoints Trace Certificates

Trusted Issuers

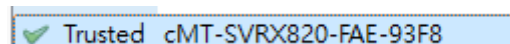
Certificates

Status	Name	Valid From	Valid To	Organization	OrganizationUnit	Locality	State	Country	AppURI	DomainName	IP	Filename
Untr...	cMT-SVRX820-FAE-93F8	2024/1/7 上午...	2029/1/7 ...	Weintek	OPCUAClient	Taipei	Taiwan	TW	urn:cMT-S...	cMT-SVRX820-FA...		C:/Program...
Trusted	UaClient@cMT-CTT0	2024/1/7 上午...	2029/1/7 ...	Weintek	OPCUAClient	Taipei	Taiwan	TW	urn:cMT-C...	cMT-CTT0	192.1...	C:/Program...
Trusted	UaClient@cMT-CTT0	2024/1/7 上午...	2029/1/7 ...	Weintek	OPCUAClient	Taipei	Taiwan	TW	urn:cMT-C...	cMT-CTT0	192.1...	C:/Program...
Trusted	UaClient@DESKTOP-0KHP3VD	2025/5/19 下...	2093/5/2 ...	Weintek	OPCUAClient	Taipei	Taiwan	TW	urn:DESKT...	DESKTOP-0KHP3...	172.2...	C:/Program...
Trusted	UaClient@JackLiang-PC	2025/5/13 上...	2093/4/27 ...	Weintek	OPCUAClient	Taipei	Taiwan	TW	urn:JackLia...	JackLiang-PC	192.1...	C:/Program...
Trusted	UaExpert@JackLiang-PC	2025/5/13 上...	2030/5/12 ...	Weintek	driver	New Taipei	x	TW	urn:JackLia...	JackLiang-PC		C:/Program...
Own ...	UaServerCpp@JackLiang-PC	2025/3/7 上午...	2030/3/6 ...	Organization	Unit	LocationN...		DE	urn:JackLia...	JackLiang-PC		C:/Program...

1.2 Trust the certificate.



1.3 Trusted Certificates.



## Example2: Weintek OPC UA Server

2.1 Open the easyweb of opcua server, find **OPC UA / Certificates**, and switch to the **[Trusted Clients]**

The screenshot shows the Weintek OPC UA EasyWeb interface. The left sidebar contains a navigation menu with items like System, Network, Project, Data, Features, WebView Setting, CODESYS, OPC UA (highlighted with a red box), FTP, Weincoud, and Administration. The main area displays the 'OPC UA' status as 'Running' with 'Start' and 'Stop' buttons. Below this, the 'Certificates' tab is selected, showing a 'Trusted Clients' dropdown menu and a table of certificates. The table has columns for Name, Valid From, Valid To, Organization, Organization Unit, URI, Filename, and Signature Algorithm. One certificate is listed with a red 'Untrusted' label.

<input type="checkbox"/>	Name	Valid From	Valid To	Organization	Organization Unit	URI	Filename	Signature Algorithm
<input type="checkbox"/>	<div>Untrusted</div> UaClient@tony-PC	2025/07/10 17:07:31	2093/06/23 17:06:31	Weintek	OPCUAClient	urn:tony-PC:Weintek:OPCUAClient	UaClient@tony-PC [912D31DE23080FD520883718BD99022DDD7B9EB9].der	SHA1-RSA

2.2 Select the untrusted certificate and click **[Trust]**.

This block shows a close-up of the 'Trusted Clients' table. The first row, which was previously marked as 'Untrusted', now has a blue checkmark in the first column, indicating it is trusted. Below the table, the 'Trust' button is highlighted with a red box, along with 'Reject', 'Remove Certificate', and 'Export Certificate' buttons.

<input checked="" type="checkbox"/>	Name	Valid From	Valid To	Organization	Organization Unit	URI	Filename	Signature Algorithm
<input checked="" type="checkbox"/>	<div>Untrusted</div> UaClient@tony-PC	2025/07/10 17:07:31	2093/06/23 17:06:31	Weintek	OPCUAClient	urn:tony-PC:Weintek:OPCUAClient	UaClient@tony-PC [912D31DE23080FD520883718BD99022DDD7B9EB9].der	SHA1-RSA

## 6. BadCertificateUntrusted

**[Reason]:** The OPC UA Server does not trust the user-certificate exchanged by the OPC UA Client

**[Solution]:**

6.1 The certificate management to the server accepts user- certificate. Take the client connecting to the Weintek OPC UA Server as an example, switch to the **[Trusted Users]** and trust it.

The screenshot shows the Weintek OPC UA Server interface. The left sidebar contains a menu with 'System', 'Network', 'Project', 'Data', 'Features', 'WebView Setting', 'CODESYS', 'OPC UA' (highlighted), 'FTP', 'Weincloud', and 'Administration'. The main area displays the 'OPC UA' configuration. The 'OPC UA Server' status is 'Running'. The 'Certificates' tab is selected, showing a table of trusted users. The table has columns: Name, Valid From, Valid to, Organization, OrganizationUnit, URI, Filename, and Signature Algorithm. A user certificate is listed with the name 'user-1' and a status of 'Untrusted'. The 'Trust' button is highlighted.

<input checked="" type="checkbox"/>	Name	Valid From	Valid to	Organization	OrganizationUnit	URI	Filename	Signature Algorithm
<input checked="" type="checkbox"/>	user-1	2025/02/01 00:02:00	2035/02/01 00:02:00			urn:user-1:Weintek:OPCUAClient	BC1317410F5C080C2B2F2420DB2DEB4864361641.der	SHA256-RSA

6.2 Another way is to import the user-cert into the HMI in advance, switch to the **[Trusted Users]** page, and import the certificate.

The screenshot shows the Weintek OPC UA Server interface. The left sidebar contains a menu with 'System', 'Network', 'Project', 'Data', 'Features', 'WebView Setting', 'CODESYS', 'OPC UA' (highlighted), 'FTP', 'Weincloud', and 'Administration'. The main area displays the 'OPC UA' configuration. The 'OPC UA Server' status is 'Running'. The 'Certificates' tab is selected, showing a table of trusted users. The table is currently empty, displaying 'No Data'. The 'Import Certificate' button is highlighted.

<input type="checkbox"/>	Name	Valid From	Valid to	Organization	OrganizationUnit	URI	Filename	Signature Algorithm
No Data								

## 7. BadTooManySessions

**[Reason]:** There are multiple devices/sessions connected to the server at the same time, and the server's upper limit is reached

**[Solution]:**

7.1 Close other OPCUA CLIENT software used for testing.

7.2 Do not connect online simulation and HMI to the server at the same time.

## Wiring Diagram:

Ethernet cable:

