

OPC UA®

PLC500, PLC500ED, PLC500MC PLC410

Application Note



Application Note

PLC410, PLC500, PLC500ED, PLC500MC

Document: 10013132265

Revision: 00

Publication Date: 04/2025

SUMMARY OF REVISIONS

The information below describes the reviews made in this manual.

Version	Revision	Description
1.4.2	R00	First edition.

CONTENTS

1	INTRODUCTION	1-1
1.1	ABBREVIATIONS AND DEFINITIONS USED	1-1
1.2	THE OPC UA PROTOCOL	1-2
1.3	REFERENCE DOCUMENTS	1-2
1.4	IMPORTANT NOTICE ABOUT CYBERSECURITY AND COMMUNICATIONS	1-2
1.5	TRADEMARKS	1-2
2	ETHERNET INTERFACE	2-1
2.1	INDICATION LEDS	2-2
2.2	OPC UA NETWORK INSTALLATION	2-2
2.3	OPC UA NETWORK TOPOLOGIES	2-3
3	SECURITY SETTINGS	3-1
3.1	CODESYS SECURITY AGENT	3-1
3.2	CODESYS RUNTIME	3-1
3.3	OPC UA SECURITY SETTINGS	3-3
3.4	CREATING A SELF-SIGNED CERTIFICATE	3-4
4	OPC UA SERVER - CODESYS	4-1
5	OPC UA CLIENT - UA EXPERT	5-1
5.1	FINDING SERVERS BY URL	5-1
5.2	ANONYMOUS CONNECTION	5-2
5.3	SECURE CONNECTION	5-3
6	OPC UA CLIENT - WES	6-1
6.1	ABOUT WES	6-1
6.2	PROJECT CREATION	6-1
7	OPC UA CLIENT - EASY BUILDER PRO	7-1
7.1	ANONYMOUS CONNECTION	7-2
8	OPC UA CLIENT - PLC500ED	8-1
8.1	ABOUT PLC500ED	8-1
8.2	QUICK CONFIGURATION	8-1
8.3	OPC UA PING PONG	8-2
8.3.1	OPC UA Server - PLC410	8-2
8.3.2	OPC UA Client - PLC500ED	8-3

1 INTRODUCTION

This Application Note is intended to assist in the use of the **OPC UA**® protocol on WEG PLCs, models PLC410, PLC500, PLC500ED, and PLC500MC. Throughout this document, the PLC500 is used as an example, but the information presented is equally applicable to the other mentioned models. It should be noted that the provided data may slightly change due to the continuous development and updating of products and tools.

In addition to providing an overview of the use of the OPC UA protocol, this document presents communication interfaces, installation recommendations, security configurations, network topology examples, and a guide to establishing OPC UA communication between PLCs and different devices and software, acting both as Server and Client. It is worth noting that all WEG PLCs with **CODESYS**® include support for the OPC UA Server. The OPC UA Client functionality is exclusively available on the PLC500ED, through programming on the WEGnology platform.

For more information regarding hardware, interfaces, and communication protocols, refer to the User Manual of the respective product, available on the [WEG](#) website. For a deeper and more detailed description of OPC UA, access the online help at [CODESYS Online Help](#).

**ATTENTION!**

This application note is intended for professionals trained in industrial networks. The installation and configuration of devices must be done according to the manufacturer's manual.

**NOTE!**

It is recommended to use **CODESYS** version **V3.5 SP19** or higher, as well as the latest version of the configuration libraries for OPC UA.

1.1 ABBREVIATIONS AND DEFINITIONS USED

CA: Public or private entity that is part of the digital certification trust chain, responsible for issuing, revoking, and renewing digital certificates (*Certificate Authority*).

CODESYS: Programming platform that allows the development, configuration, and monitoring of solutions for industrial automation and system integration.

Edge Agent: Container previously installed on the PLC500ED that allows the local execution of Edge Workflows.

IoT: Acronym referring to technologies that facilitate communication and data exchange between devices and the cloud, as well as between the devices themselves (*Internet of Things*).

IIoT: Application of IoT technologies in the industrial context, connecting devices, machines, and systems via the Internet for data collection, exchange, and analysis, aiming for greater efficiency, automation, and monitoring (*Industrial Internet of Things*).

OPC UA: Industrial communication protocol that ensures secure interoperability between devices and systems. It offers encryption, authentication, and support for complex data models, being widely used in automation and IIoT (*Open Platform Communications Unified Architecture*).

SCADA: System that monitors and controls industrial processes in real-time, collecting data from local and remote sensors and devices for centralized analysis and operation (*Supervisory Control and Data Acquisition*).

UAExpert: Software used as a general-purpose OPC UA Client for testing, supporting features such as DataAccess, Alarms & Conditions, Historical Access, and UA Method calling.

WEGnology: WEG's IIoT platform for monitoring, analyzing, and automating industrial processes, allowing device connection and real-time data management.

WES: WEGnology Edge Suite is a modern and advanced software for supervision, control, and automation of industrial processes and development of Edge IoT applications.

INTRODUCTION

1.2 THE OPC UA PROTOCOL

OPC UA (*Open Platform Communications Unified Architecture*) is a platform-independent industrial communication protocol that ensures secure and reliable interoperability between devices, machines, and systems from different manufacturers. Developed and maintained by the **OPC Foundation**, it was designed to replace previous versions of OPC, offering support for complex information models and advanced security, including encryption and authentication.

The OPC standard is a series of specifications developed by industry vendors, end-users, and software developers. These specifications define the interface between Clients and Servers, including real-time data access, alarm and event monitoring. Widely used in industrial automation, SCADA, IIoT, and system integration, OPC UA standardizes data exchange in various environments.

In **CODESYS**, OPC UA is integrated as a native Server, allowing OPC UA Clients to access device variables in a structured and secure manner. Configuration occurs in the **Symbol Configuration**, where shared data can have read and write access control. With support for encryption and authentication, this protocol facilitates communication between PLCs and industrial systems. For more details, refer to the official documentation on the [CODESYS](#) and [OPC Foundation](#) websites.

1.3 REFERENCE DOCUMENTS

It is recommended to consult the documents related to OPC UA shown in [Table 1.1 on page 1-2](#).

Table 1.1: Reference documents.

Document	Version	Source
Practical Security Recommendations for building OPC UA Applications	3	OPC Foundation

1.4 IMPORTANT NOTICE ABOUT CYBERSECURITY AND COMMUNICATIONS

WEG PLCs, models PLC410, PLC500, PLC500ED, and PLC500MC, have the capability to connect and exchange information through networks and communication protocols. Although they have been designed and tested to ensure proper operation with other automation systems using the protocols mentioned in this manual, it is essential that the customer understands the responsibilities associated with information and cybersecurity when using this equipment.

Therefore, it is the customer's sole responsibility to adopt defense-in-depth strategies and implement policies and measures to ensure the security of the system as a whole, including communications sent and received by the equipment. These measures include, but are not limited to, the installation of firewalls, antivirus and antimalware programs, data encryption, authentication control, and physical access control of users.

WEG and its affiliates are not responsible for damages or losses resulting from cybersecurity breaches, including, but not limited to, unauthorized access, intrusion, leakage and/or theft of data or information, denial of service, or any other form of security breach. The use of this product in conditions for which it was not specifically designed is not recommended and may cause damage to the product, network, and automation system.

In this regard, it is essential that the customer understands that external interventions through third-party programs, such as sniffers or similar programs, have the potential to cause interruptions or restrictions in the functionality of the equipment.

1.5 TRADEMARKS

OPC UA® is a registered trademark of the OPC Foundation.

All other trademarks are the property of their respective owners.

2 ETHERNET INTERFACE

OPC UA communication is carried out through Ethernet connections, indicated in [Figure 2.1 on page 2-1](#) for PLC500 and PLC410. Initially, each Ethernet port has the IP address indicated in [Table 2.1 on page 2-1](#), which can be changed at any time through the CODESYS software.

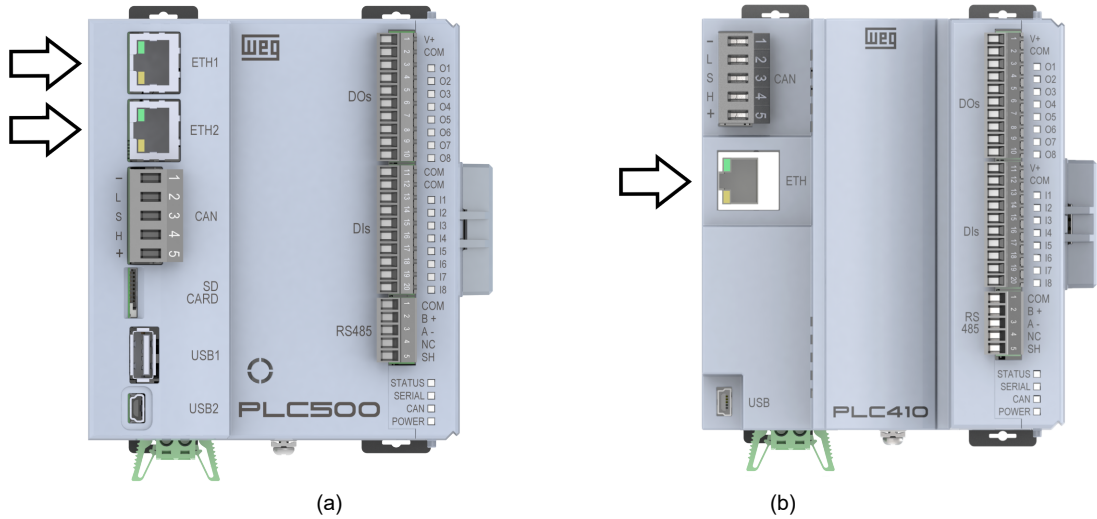


Figure 2.1: Indication of Ethernet connections of PLCs. (a) PLC500 and (b) PLC410.

Table 2.1: Default addresses for Ethernet ports.

PLC410	PLC500	Default IP address
ETH	ETH1	192.168.1.10
-	ETH2	192.168.2.10

The pin distribution of the connector follows the Ethernet 1000BASE-TX standard. The Ethernet interface of PLC410 supports speeds up to 100 Mbps, while the Ethernet interfaces of PLC500 reach up to 1000 Mbps.

PLC500, PLC500ED, and PLC500MC have two Ethernet interfaces, which can be configured in **Independent** mode, where the interfaces operate with distinct IPs, or in **Switch** mode, where the interfaces share the same IP address.

The Ethernet interfaces are compatible with various communication protocols, including OPC UA, and can be used simultaneously for multiple protocols. For instructions on how to configure these additional networks, refer to the Application Notes of the product available on the [WEG](#) website.

2.1 INDICATION LEDS

The Ethernet ports have LEDs to indicate speed and network link/activity, as indicated in [Figure 2.2 on page 2-2](#). These LEDs have the behavior described by [Table 2.2 on page 2-2](#) and [Table 2.3 on page 2-2](#).



Figure 2.2: Speed (S1) and link/activity (L1) LEDs of the Ethernet interface of PLC500.

Table 2.2: LED S1 - Speed.

State	Description
Off	Equipment off or 10 Mbps link
Green, solid	100 Mbps link

Table 2.3: LED L1 - Link/Activity.

State	Description
Off	Equipment off or no link
Amber, solid	With link and no network activity
Amber, blinking	With link and network activity

2.2 OPC UA NETWORK INSTALLATION

The OPC UA network, like many industrial communication networks, due to its application often in harsh environments with high exposure to electromagnetic interference, requires certain precautions to ensure a low communication error rate during its operation.



ATTENTION!

It is recommended to use passive components (cables, connectors, switches, hubs) certified for industrial applications.

The recommended characteristics for the cable used in the installation are:

- Standard Ethernet cable, 1000Base-TX, CAT 5e or higher.
- Shielded cable.
- Maximum length of 100 m for connection between equipment.

Proper grounding system connection is essential to minimize electromagnetic interference problems in industrial environments. It is important to avoid connecting the cable to multiple grounding points, especially in places where there are potential differences between the grounding points. Additionally, it is recommended that signal and communication cables be installed in dedicated routes, keeping a distance from power cables.



DANGER!

Inadequate grounding installations can cause failures in the OPC UA network and represent a risk of fatal electric shock.

2.3 OPC UA NETWORK TOPOLOGIES

Network topologies in an OPC UA system can vary according to project needs and installation architecture. In [Figure 2.3 on page 2-3](#) there is an example of a star topology, in which a central switch connects all OPC UA client and server devices.

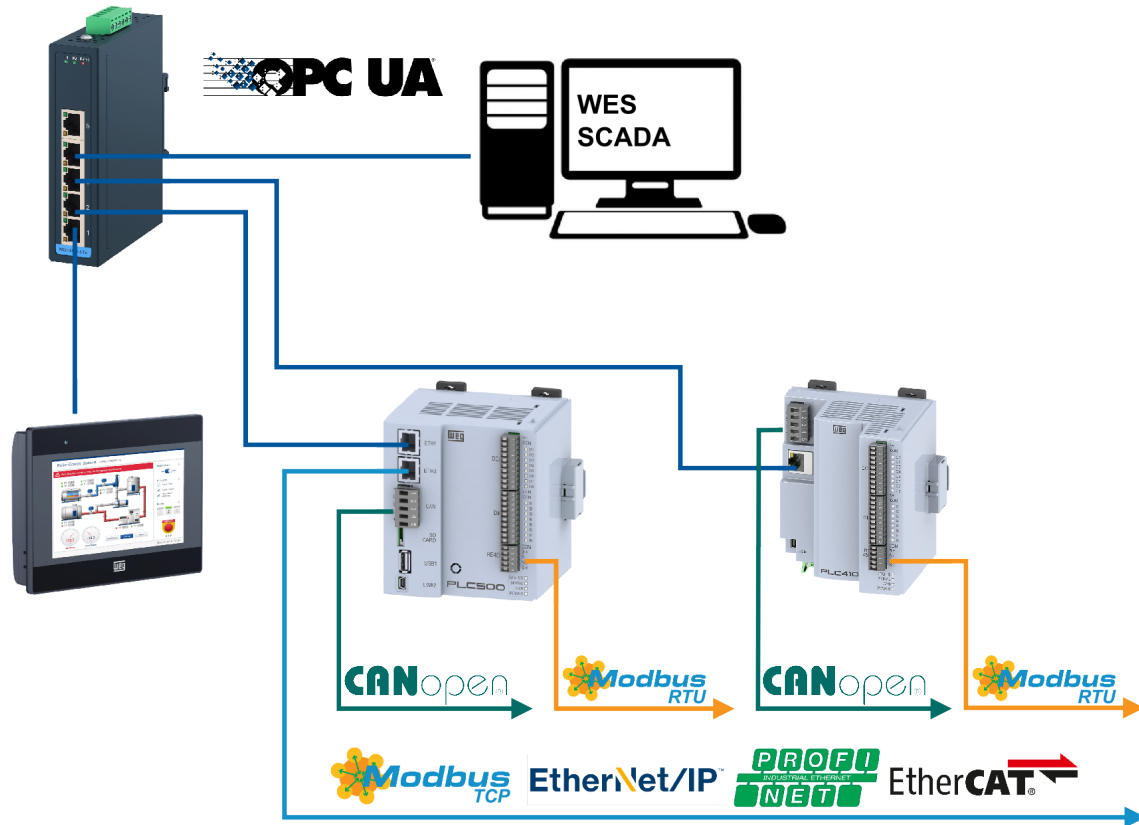


Figure 2.3: Example of OPC UA network topology integrated with other communication protocols used in industrial environments.

In the figure, the HMI can act as an OPC UA Server for a SCADA system, such as WES running on a computer, while behaving as a Client for PLC500 and PLC410. Additionally, it is possible to establish direct communication between PLCs, where one can be configured as a Server and the other as an OPC UA Client, allowing structured data exchange.

For control and monitoring of industrial devices, both PLC500 and PLC410 support various communication protocols, including CANopen, Modbus RTU, Modbus TCP, EtherNet/IP, PROFINET, and EtherCAT, ensuring integration with a wide range of equipment and industrial networks. This flexibility enables communication from sensors and actuators to integration with advanced distributed supervision and control systems.



NOTE!

For more information about the communication protocols of PLC500 and PLC410, refer to the Application Notes available on their respective product pages on the [WEG](#) website.

3 SECURITY SETTINGS

This section details the security options for OPC UA communication of the PLC500 in CODESYS. The settings can be adjusted according to the requirements of each application; however, it is always recommended to use the highest level of security available.

3.1 CODESYS SECURITY AGENT

The **CODESYS Security Agent** add-on allows configuring and managing essential security aspects in the CODESYS development environment. In the latest versions, it comes pre-installed. If it is not available on your system, follow the steps below to install it.

To install the add-on, go to **Tools** → **CODESYS Installer**. In the new window that opens, click on **Browse** and search for **Security**. Then, select **CODESYS Security Agent** and click on **Install**, as illustrated in [Figure 3.1 on page 3-1](#). Before installing new add-ons via the CODESYS Installer, make sure the CODESYS software is closed.

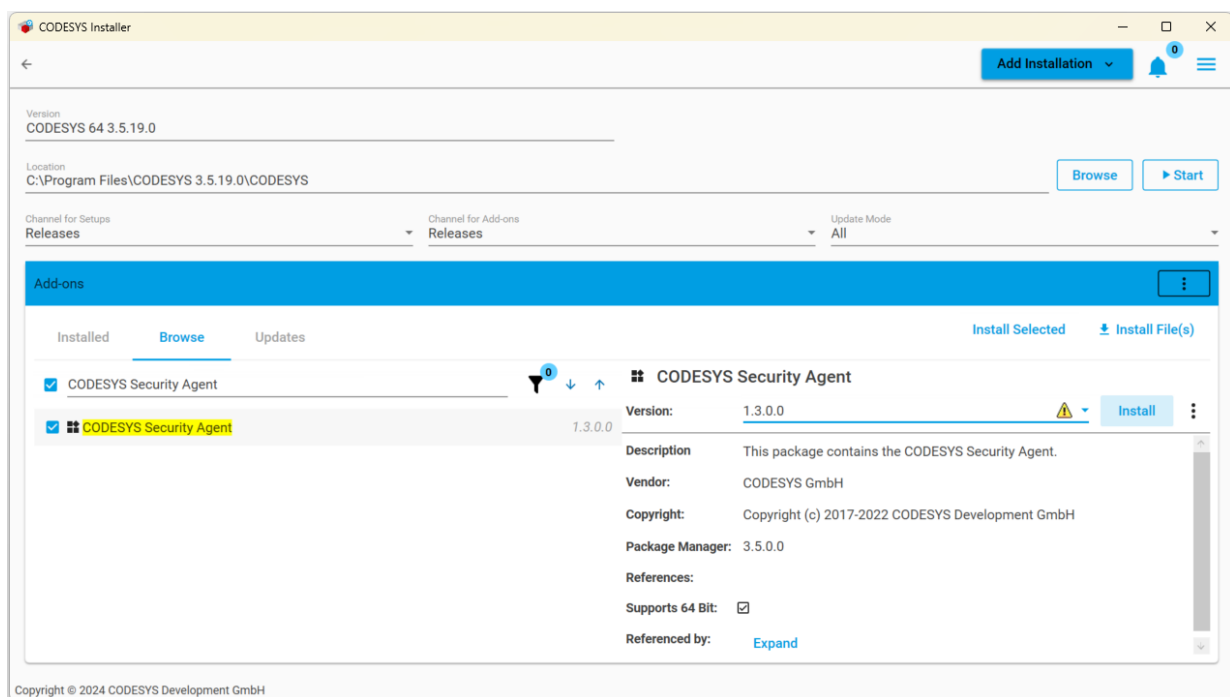


Figure 3.1: Installing the CODESYS Security Agent add-on.

3.2 CODESYS RUNTIME

The security settings of the CODESYS runtime can be changed by accessing **Communication Settings** → **Device** → **Change Runtime Security Policy**, as illustrated in [Figure 3.2 on page 3-2](#).

In the **Device User Management** section, it is possible to set user login management as optional (**Optional user management**) or mandatory (**Enforce user management**). Additionally, the **Allow anonymous login** option allows establishing an OPC UA connection without the need to provide user credentials and password.



CYBERSECURITY NOTE!

It is recommended not to allow anonymous connections via OPC UA, as this can expose the system to unauthorized access and security vulnerabilities. The OPC Foundation suggests that authentication be done through login with user and password (**Sign**) or with authentication and encryption (**SignAndEncrypt**).

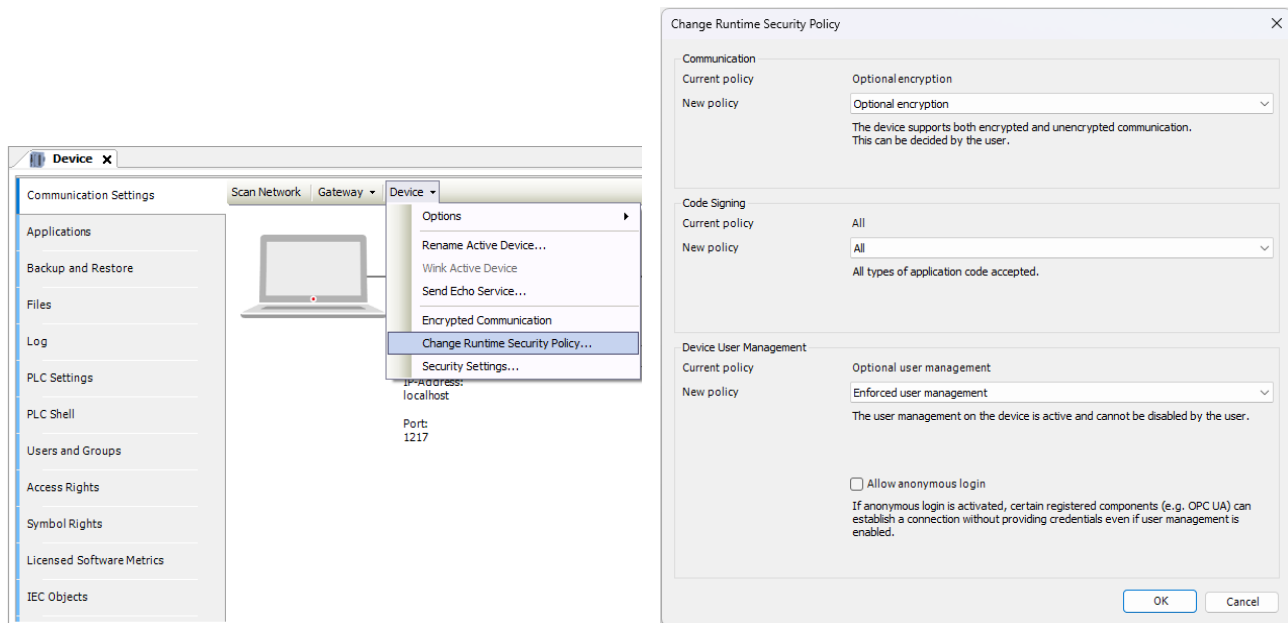


Figure 3.2: Accessing CODESYS runtime security settings.



CYBERSECURITY NOTE!

CODESYS offers various security features, including encryption in communication between the runtime and the PLC, application access control by users, certificate-based authentication, source code tampering protection, digital signatures for applications, among others. These measures ensure greater protection against unauthorized access and tampering. For more information, refer to the online help at [CODESYS Online Help](#).

If the **Enforce user management** option is enabled, it will be necessary to provide credentials to establish the Client connection with the OPC UA Server. If no user is configured on the PLC, the system will prompt for the creation of a new user and password on the next login attempt, as illustrated in [Figure 3.3 on page 3-2](#).

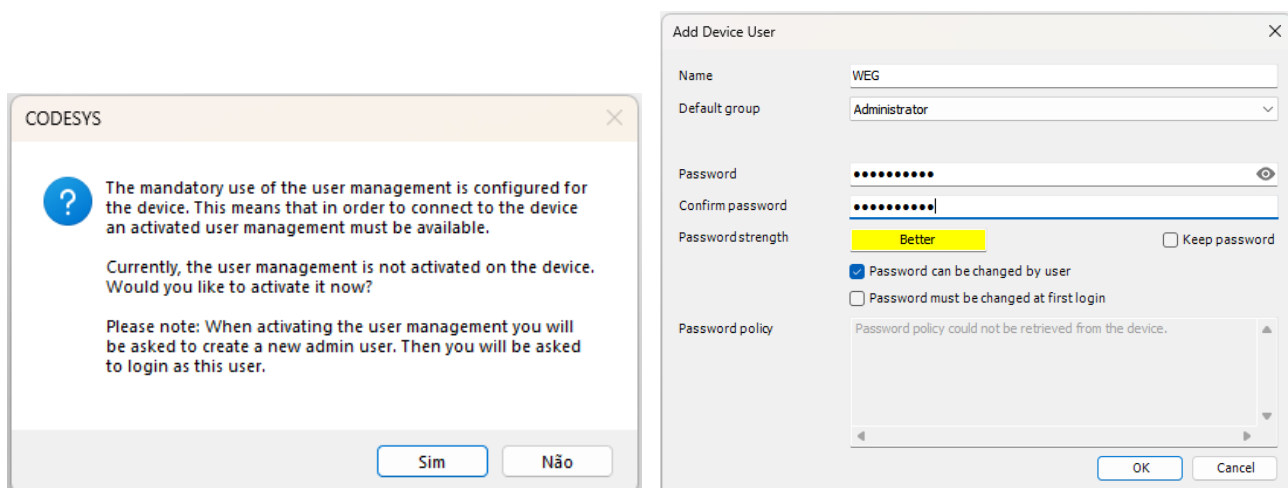


Figure 3.3: Mandatory user configuration to log in to the PLC.



CYBERSECURITY NOTE!

Always use strong passwords when logging into the PLC, combining uppercase and lowercase letters, numbers, and special characters. During commissioning, change any existing default passwords and establish a regular password change policy to enhance system security.

If the user and/or password for logging into the PLC are forgotten, access to the device can be recovered through **Factory Reset**, which restores the product's factory settings. This functionality is available via the web page, the PLC Shell in CODESYS, and also through SmartMedia. For more details, refer to the product manuals available on the [WEG](#) website.



ATTENTION! When performing a factory reset, **all CODESYS applications, logs, files stored on the PLC, and network settings will be erased**. The product will automatically restart after these operations are completed.

3.3 OPC UA SECURITY SETTINGS

The security settings of the OPC UA Server can be viewed in **Communication Settings** → **Device** → **Security Settings**, as shown in [Figure 3.4 on page 3-3](#). In this window, you can change the security policy used for authentication of communication between the OPC UA Client and Server.

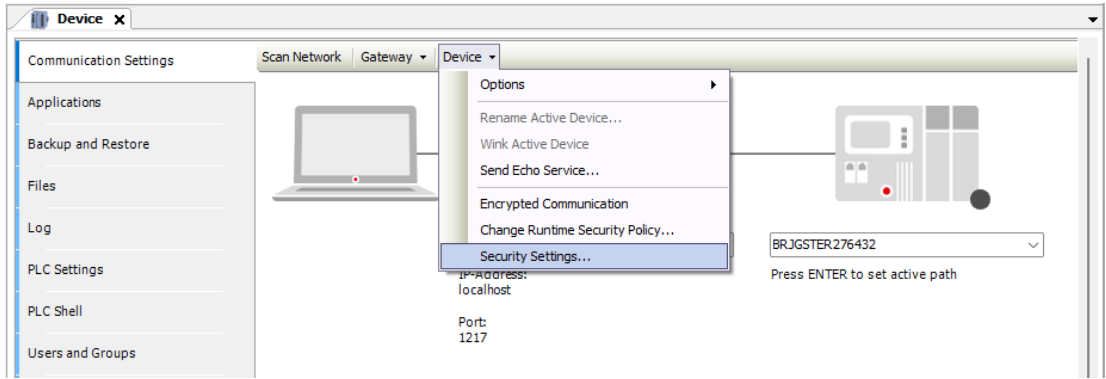


Figure 3.4: Accessing PLC500 security settings.

Through the **+** icon in **CmpOPCUAServer**, you have the possible security settings and information of the OPC UA Server, according to [Figure 3.5 on page 3-3](#).

Device Security Settings		
Setting	Value	Description
[-] CmpOPCUAServer		
[-] CommunicationPolicy	POLICY_AES128SHA256RSAOAE	Support for all policies beginning with Aes128Sha256RsaOaep (AES 128 with SHA256)
[-] CommunicationMode	SECURE_IF_POSSIBLE	Support all available modes, but deactivates None if it is possible to use secure endpoints (e.g. certificates created).
[-] Activation	ACTIVATED	Activates the OPC UA Server. [Default]
[-] UserAuthentication	ENABLED	Activates the user authentication for the OPC UA Server. [Default]
[-] AllowUserPasswordOnPlaintext	NO	Forbids to transit the password in a plaintext way.
[-] EnableCRLChecks	YES	Enable CRL checks. Verification will fail, if CRL for a CA are missing.
[-] EnableSelfSignedCertBackwardInteroperability	YES	Enable backward interoperability.
[-] CreateWithCAFlag	NO	Configuration to create self signed certificates with cA:FALSE as proposed by the RFCs for non CA certificates. (more secure).
[-] DeactivateSecurityPolicy		A comma separated list of security policies uris (e.g. http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256) which needs to be d
[-] ApplicationName	OPCUAServer@PLC500	The application name of the OPC UA server. This will be used for the certificate and the ApplicationName fields of the OPC UA Server.
[-] CompanyOrOrganizationName		The name of the organization running the OPC UA server. (If empty field is ignored)
[-] City		Will fill up the city field of the OPC UA Server certificate. If empty the field won't be used.
[-] State		Will fill up the state field of the OPC UA Server certificate. If empty the field won't be used.
[-] Country		Country field of the OPC UA Server certificate in alpha-2 code format according to ISO-3166 (e.g. DE for Germany). If empty the field wo
[-] CertificateIpAddresses		A comma separated list of IP addresses which should be added as alternative names to the X.509 certificate of the OPC UA Server. Spec
[+] CmpOpenSSL		
[+] CmpUserMgr		
[+] CmpApp		
[+] CmpSecureChannel		
[+] CmpWebServer		

Figure 3.5: OPC UA Server security settings.

SECURITY SETTINGS

The **CommunicationPolicy** field defines the security policy supported by the OPC UA Server. The available policies are: Aes256Sha256RsaPss, Basic256Sha256, and Aes128Sha256RsaOaep. The OPC Foundation recommends using at least the Basic256Sha256 policy. Outdated encryption algorithms that use SHA-1 should not be employed.

In **CommunicationMode**, it is possible to configure the connection mode allowed by the OPC UA Server. It is recommended to use the MIN_SIGNED option, which always requires a username and password.



NOTE!

To break AES-128 encryption by brute force, 2^{128} combinations would be required. With a supercomputer capable of performing 1×10^{18} operations per second, the estimated time for the task would be up to 10.8×10^{12} (trillion) years.

For more information on OPC UA security options, refer to the online help at [CODESYS Online Help](#).

3.4 CREATING A SELF-SIGNED CERTIFICATE

To create a self-signed certificate, go to **View** → **Security Screen** or click on the icon , located in the lower left corner of the CODESYS window, as illustrated in [Figure 3.6 on page 3-4](#).

In the window that opens, select the **Devices** tab, click on the refresh icon , and then click on the **Device** icon to view the available certificates, as demonstrated in [Figure 3.7 on page 3-4](#).

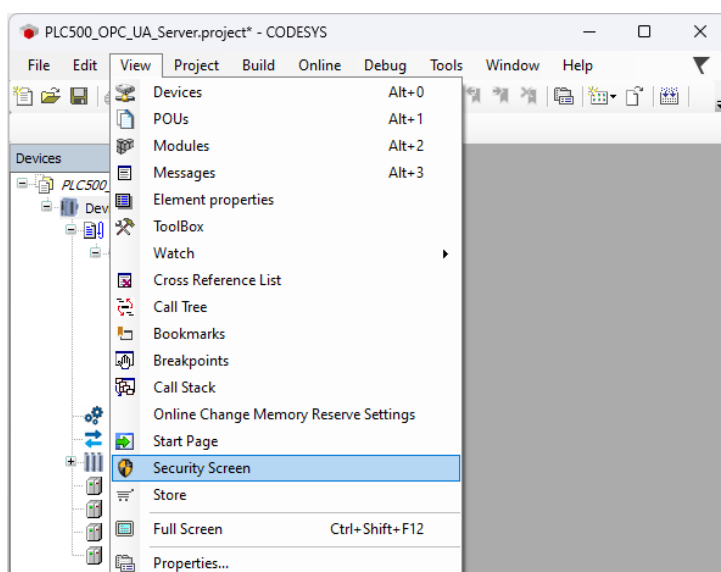


Figure 3.6: Opening the security screen in CODESYS.

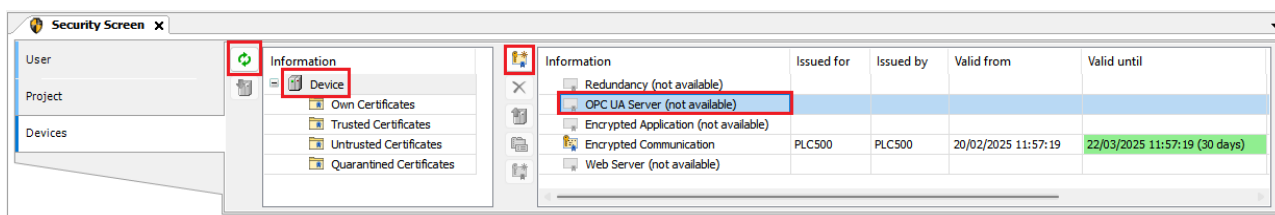


Figure 3.7: Device certificates screen.

To create a new certificate, go to **OPC UA Server** and click on the icon . Then, choose the key size, define the certificate validity, and click **OK**.

Wait for the certificate to be generated — the larger the key size, the more secure the certificate will be, but the creation process will take longer. After completion, the certificate can be viewed as illustrated in [Figure 3.8](#)

on page 3-5. Additionally, certificates created by PLC500 can be listed directly via PLC Shell using the **cert-getcertlist** command.



NOTE!

The certificate used for encrypting communication between CODESYS on the computer and the PLC is generated automatically, eliminating the need for manual creation.

Information	Issued for	Issued by	Valid from	Valid until
Redundancy (not available)				
OPC UA Server	OPCUAServer@PLC500	OPCUAServer@PLC500	20/02/2025 12:01:15	22/03/2025 12:01:15 (30 days)
Encrypted Application (not available)				
Encrypted Communication	PLC500	PLC500	20/02/2025 11:57:19	22/03/2025 11:57:19 (30 days)
Web Server (not available)				

Figure 3.8: New OPC UA Server certificate generated in CODESYS.



CYBERSECURITY NOTE!

Certificates generated by CODESYS do not have the authenticity of a Certificate Authority (CA), so any OPC UA Client wishing to establish secure communication must manually recognize the generated certificate.

4 OPC UA SERVER - CODESYS

This section presents an example of configuring an OPC UA Server in CODESYS using the PLC500.

Initially, add the **Symbol Configuration** to the application: right-click on **Application** → **Add Object** → **Symbol Configuration**, as illustrated in [Figure 4.1 on page 4-1](#). Check the **Support OPC UA features** option and click **Add**.

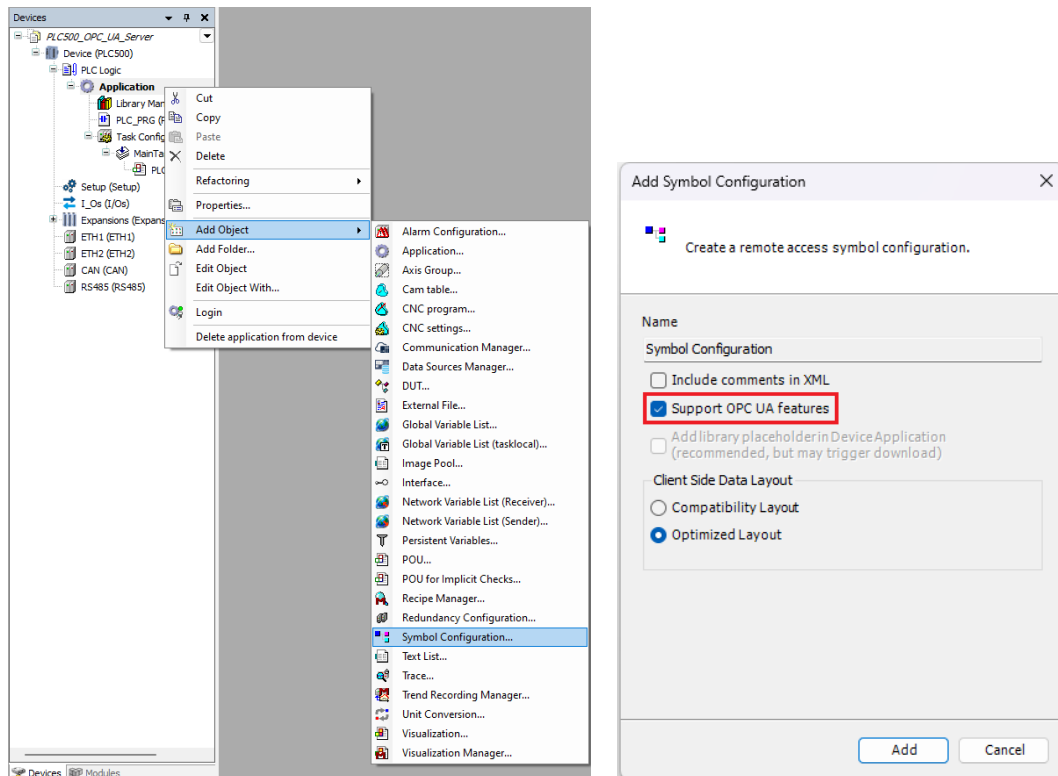


Figure 4.1: Adding Symbol Configuration to the application in CODESYS and enabling OPC UA features.

Next, in **Symbol Configuration**, click **Build**. Symbols will be created for all variables declared in the project. To select the data to be made available by the OPC UA Server, enable the checkboxes ☒ by left-clicking on the **Symbols** list, as demonstrated in [Figure 4.2 on page 4-1](#).

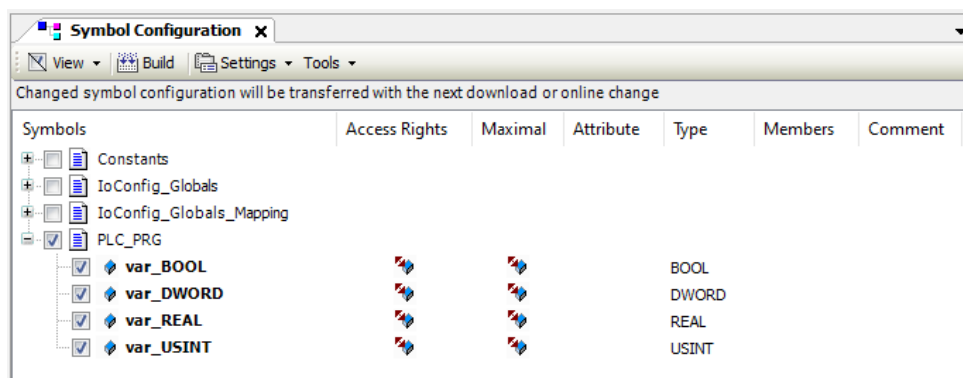


Figure 4.2: Variable configuration in Symbol Configuration.



NOTE!

By default, variables have read and write access rights for the OPC UA Client, as observed in the variable **var_DWORD**, indicated by the icon . Variables with read-only access have the icon , while those with write-only access have the icon . To modify the access type, left-click on the icons.

5 OPC UA CLIENT - UA EXPERT

This section presents an example of configuring an OPC UA Client in **UAExpert®**. The program is available for download on the [Unified Automation](#) website.

5.1 FINDING SERVERS BY URL

In UAExpert, click the **+** icon to add an OPC UA Server. Then, double-click the **+** in **Custom Discovery** and enter the URL corresponding to the IP of your OPC UA Server. For example, if the IP is 192.168.1.10, the URL will be **opc.tcp://192.168.1.10:4840**. [Figure 5.1 on page 5-1](#) shows the steps to add the OPC UA Server in UAExpert.

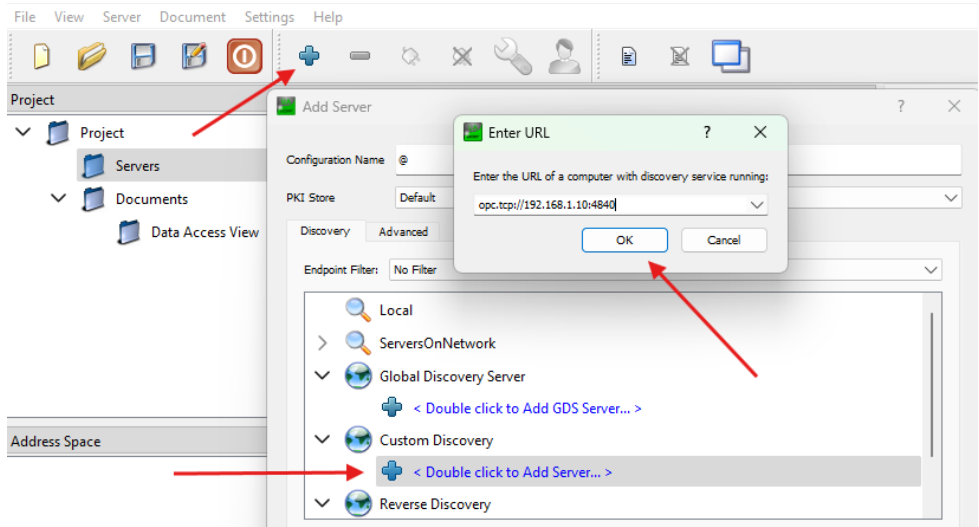


Figure 5.1: Adding the OPC UA Server in UAExpert.

Next, click on the URL and expand the icons until the available connections are displayed. Depending on the security configuration of the PLC500 OPC UA Server, not all options will be visible. Use the connection options that present an Endpoint URL with the IP address of the PLC500 OPC UA Server, as shown in [Figure 5.2 on page 5-1](#). Endpoint URLs with the hostname will generate a connection error.

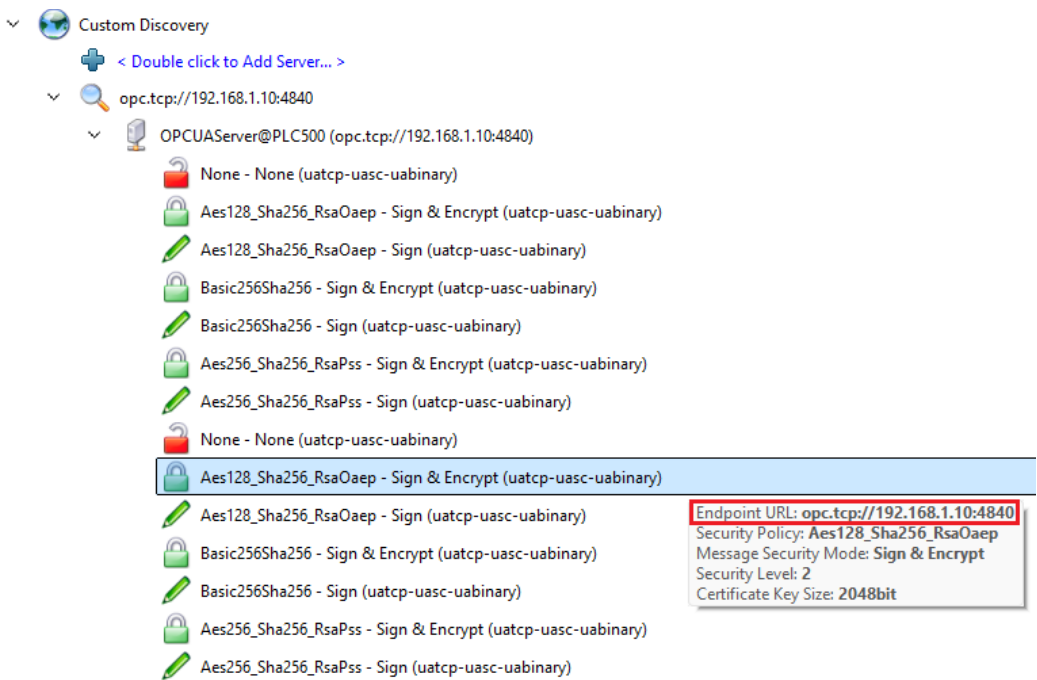


Figure 5.2: All connection options for the PLC500 OPC UA Server in UAExpert.



NOTE!

For all connection options to appear in UAExpert, a self-signed certificate for OPC UA needs to be created in the PLC500. Additionally, the **CommunicationMode** must be set to **ALL**. Check [Section 3 SECURITY SETTINGS](#) on page 3-1 for more information.

5.2 ANONYMOUS CONNECTION

For an anonymous connection to be possible, the **Allow anonymous login** option must be enabled in **Change Runtime Security Policy** and **CommunicationMode** must be set to **ALL** in **Device Security Settings**.



CYBERSECURITY NOTE!

The use of anonymous connection for regular application operation is not recommended due to cybersecurity issues. It should be restricted to testing, commissioning, or when other alternatives are not available.

Select the **None** connection option and click **OK**, as shown in [Figure 5.3](#) on page 5-2. The OPC UA Server will appear below the **Servers** folder. Right-click and select **Connect**, or click the corresponding icon in the toolbar, as shown in [Figure 5.4](#) on page 5-2.

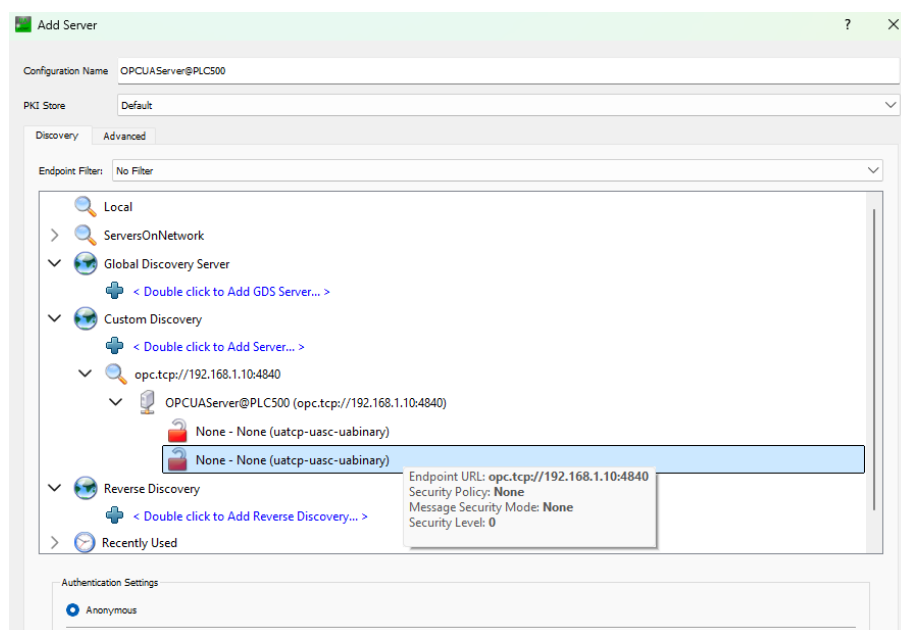


Figure 5.3: Selecting communication without encryption.

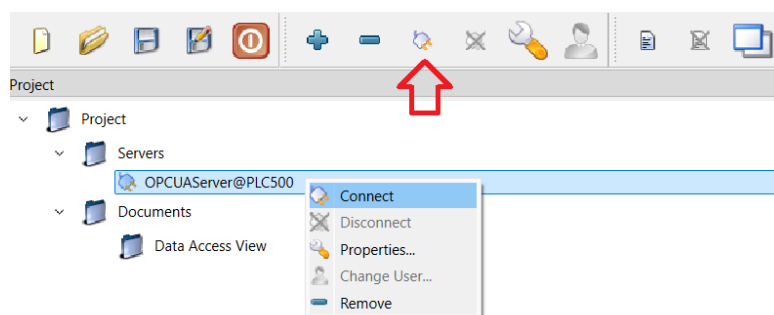


Figure 5.4: Establishing connection with PLC500 OPC UA Server in UAExpert.

The connection will be established, and the accessible variables will be present in **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**. These variables can be selected and dragged to the **Data Access View** window, where they can be monitored in real-time, as shown in [Figure 5.5 on page 5-3](#).

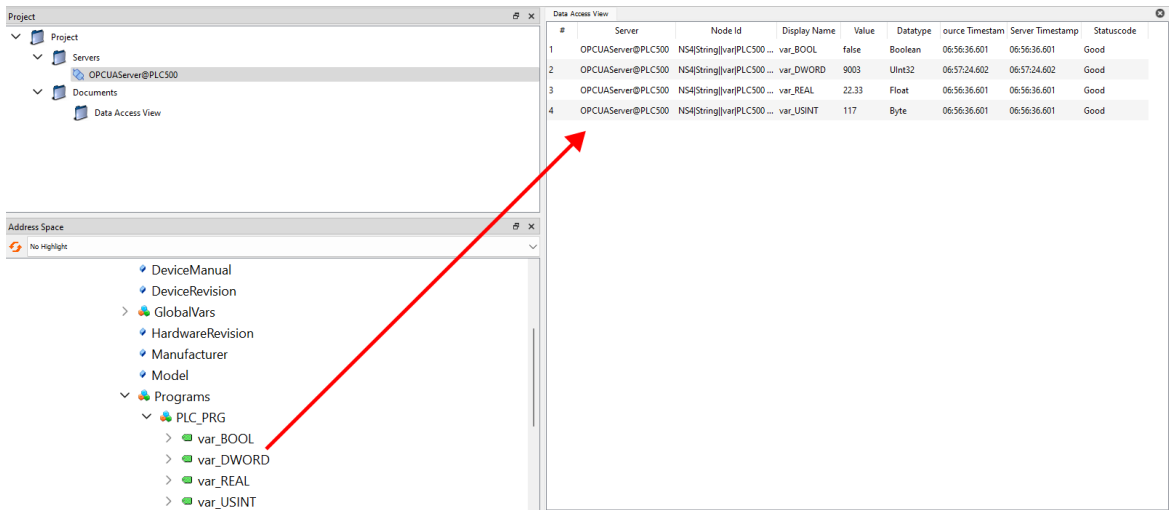


Figure 5.5: Monitoring variables in UAExpert.

5.3 SECURE CONNECTION

To establish a secure OPC UA connection with the PLC500 Server, a user and certificate must be configured in the PLC beforehand. For more details, refer to [Section 3 SECURITY SETTINGS on page 3-1](#).

Select a security option with credentials (**Sign**) or with credentials and encryption (**SignAndEncrypt**). Click the corresponding icon to enable authentication, enter the user configured in the PLC500, as shown in [Figure 5.6 on page 5-3](#), and click **OK**.

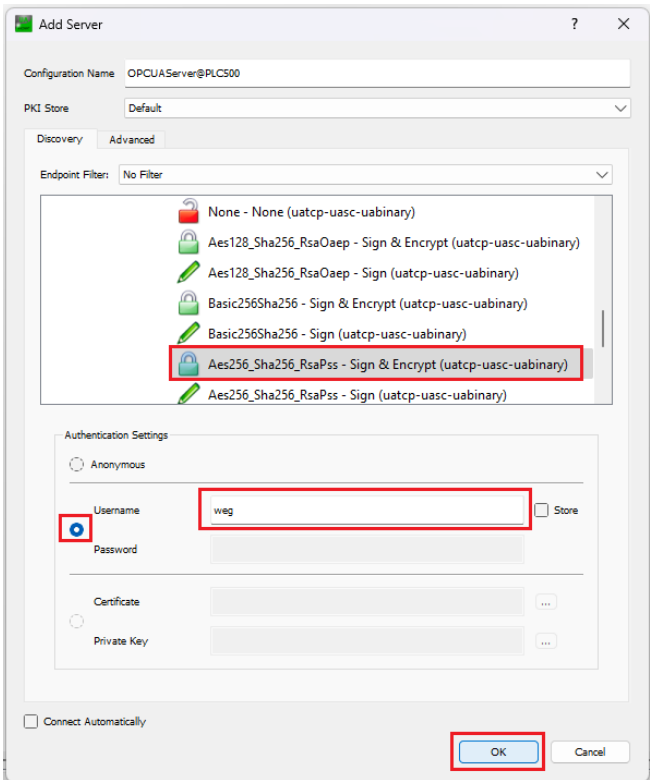
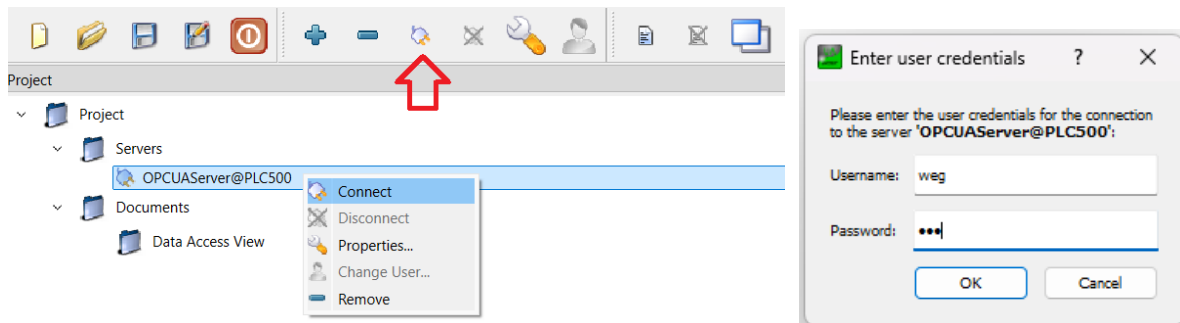


Figure 5.6: Selecting a secure OPC UA connection in UAExpert.

The OPC UA Server will appear below the **Servers** folder. Right-click on it and select **Connect**, or use the corresponding icon in the toolbar. In the window that opens, enter the user password and confirm.



NOTE!

The **BadCertificateHostNameInvalid** warning occurs when the hostname in the OPC UA Server certificate does not match the address used for the connection, such as when using an IP instead of a domain name. If the certificate is trusted and the user knows its origin, the warning can be ignored.

After clicking **OK**, a window will appear to trust the PLC500 certificate. Click **Trust Server Certificate** and then click **Continue** to complete the trust process and establish the secure connection. [Figure 5.7 on page 5-4](#) shows the certificate validation screens in UAExpert.

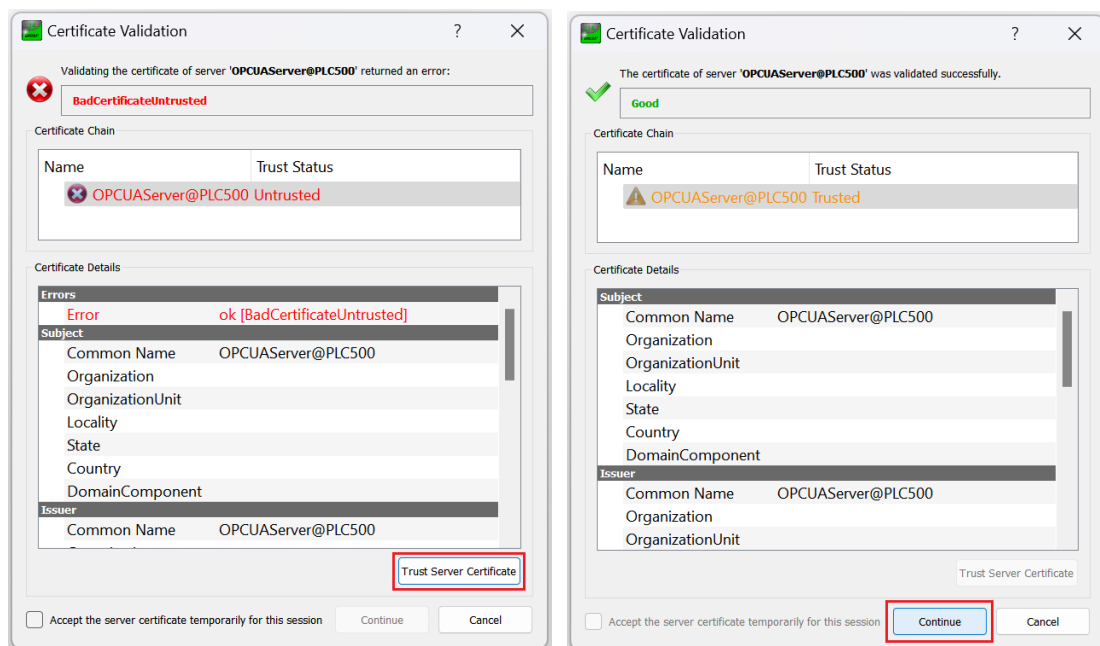
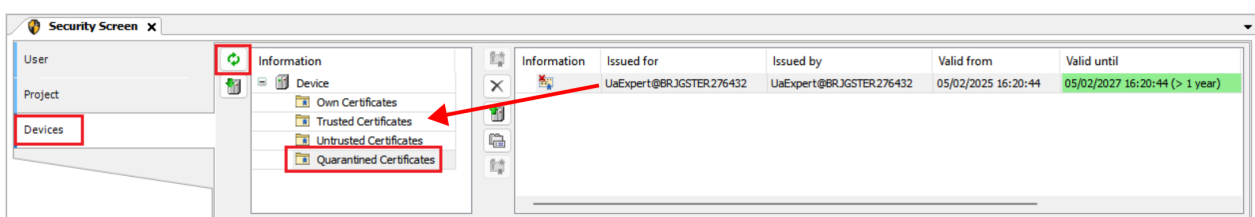
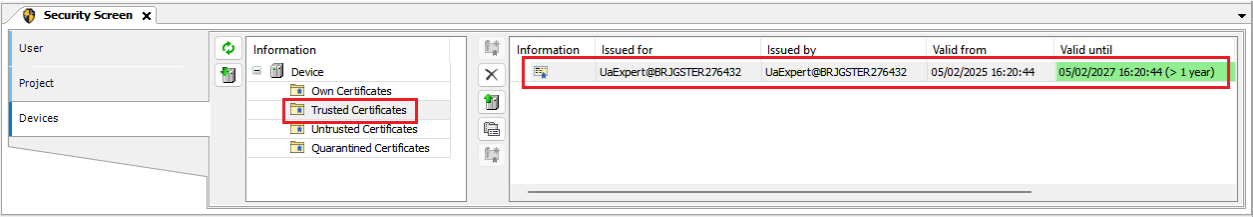


Figure 5.7: Certificate validation by UAExpert.

In CODESYS, go to the **Security Screen** and check if the UAExpert OPC UA Client certificate is in quarantine. Drag it to the **Trusted Certificates** folder to add it to the trusted certificates list.



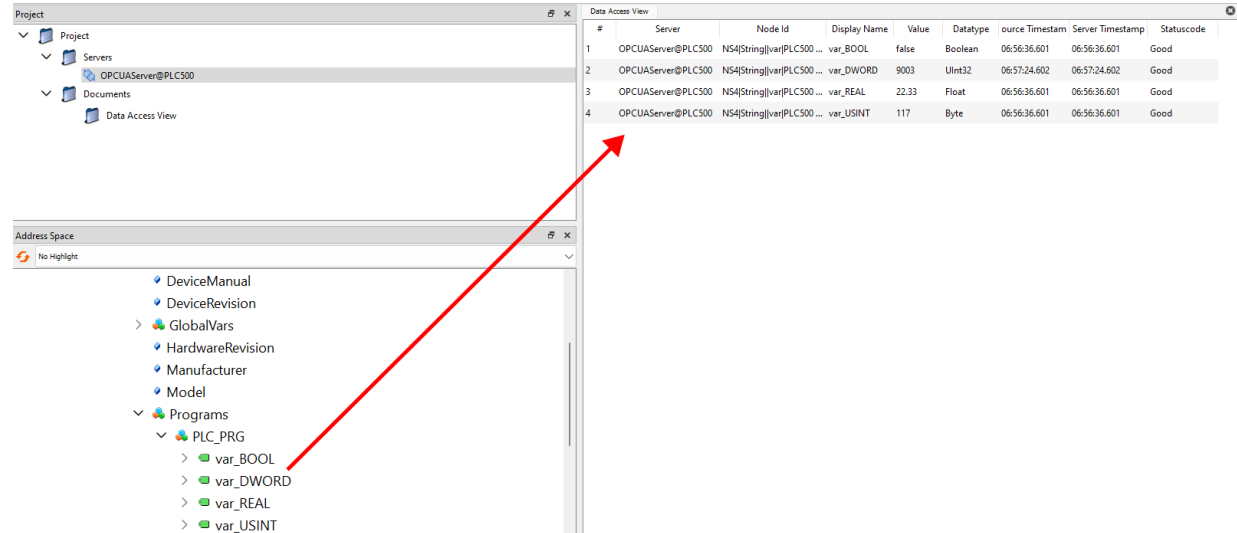
The UAExpert certificate should now appear in the trusted certificates window.



NOTE!

All created and trusted certificates of the PLC500 can also be viewed using the **cert-getcertlist** command in the PLC Shell.

After reconnecting the OPC UA Server in UAExpert, the connection should be established correctly. The variables located in **Tags** → **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs** can be dragged to the **Data Access View** window, allowing the variables to be read or modified as needed.



NOTE!

When a certificate is permanently trusted, it can be used to establish other secure connections in UAExpert until its expiration date.

6 OPC UA CLIENT - WES

This section presents an example of configuring an OPC UA Client in **WES (WEGnology Edge Suite)**. To access the WES page, visit the [WEG](#) website.

6.1 ABOUT WES

The WEGnology Edge Suite platform is a modern and advanced supervisory software for industrial process control and automation, and for developing edge IoT applications.

WES is a complete, secure, flexible, and scalable solution ranging from HMI applications to advanced SCADA systems, control centers, and supervision of distributed industrial processes for critical mission and high availability, including the WES-ELECTRICAL version for electrical systems, enabling applications in various industry segments, including OEMs.



6.2 PROJECT CREATION

In WES, create a new project in **Projects** → **New Project**. You can also check the current WES license in **License**. [Figure 6.1 on page 6-1](#) shows the WES initial screen.

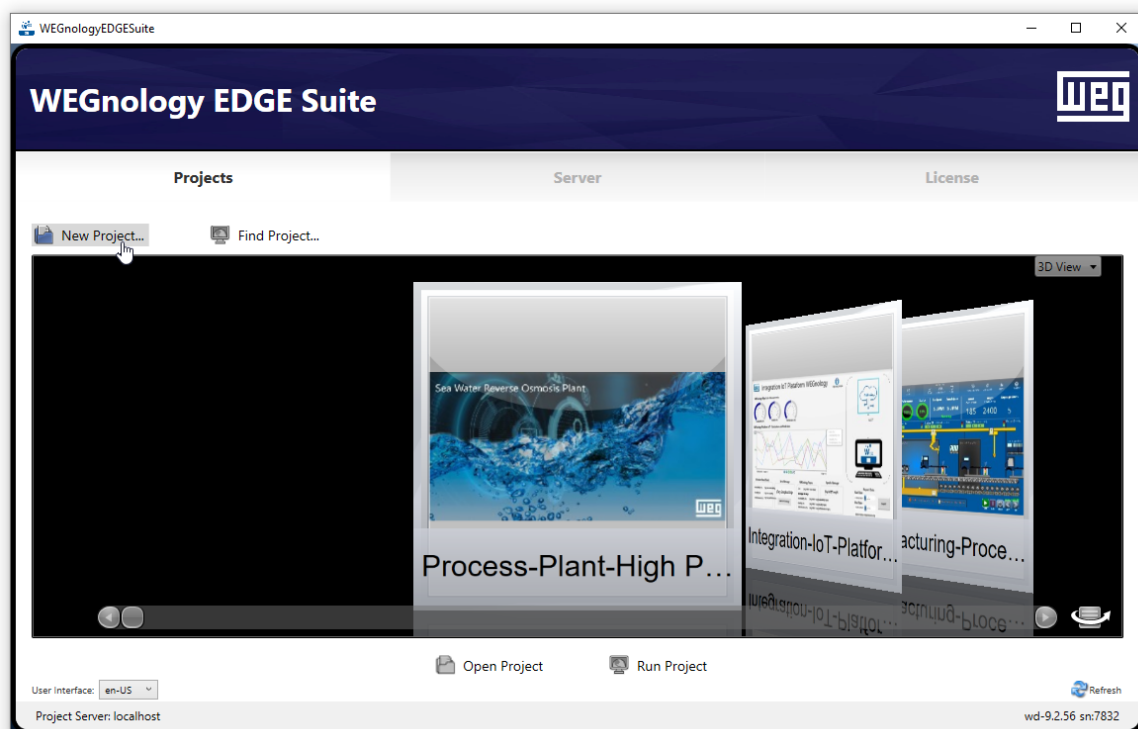


Figure 6.1: WES initial screen.

Once inside the created project, [Figure 6.2 on page 6-2](#) is presented, where the main fields **Edit**, **Draw**, and **Run** are found.

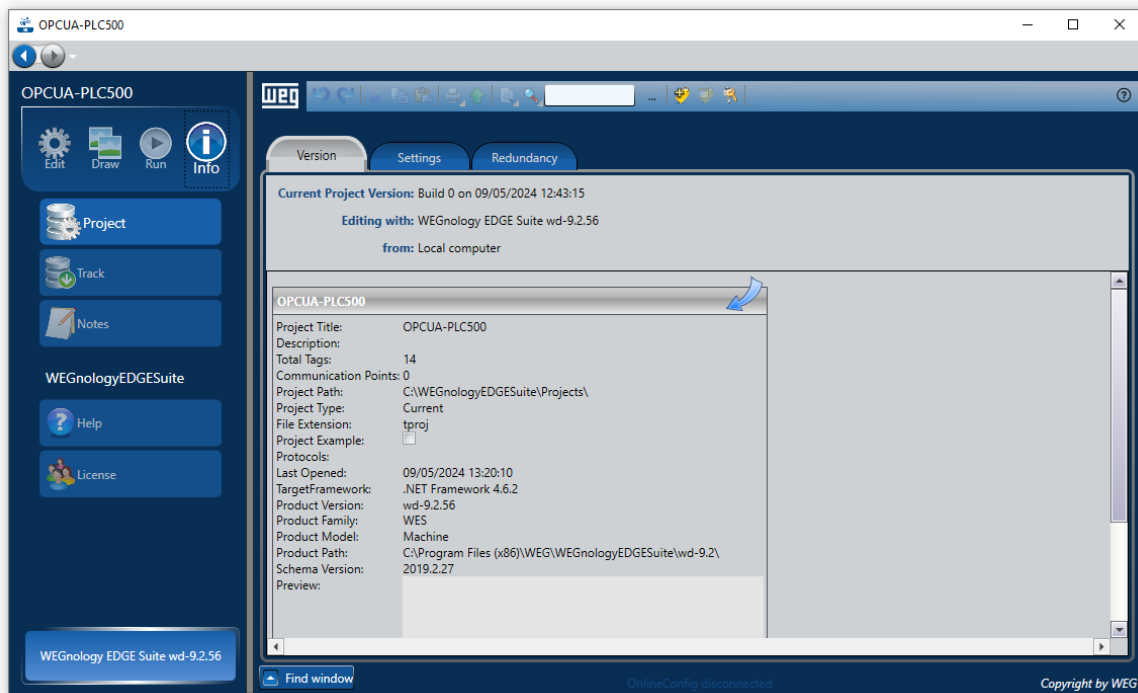


Figure 6.2: Project initial screen.

Go to **Edit** → **Devices** → **Channels** and choose **OPCUA - OPC UA Client** in **Installed Protocols**. Then, click on Channel: **Create new** and **Ok** to create a new channel. [Figure 6.3 on page 6-2](#) shows the created OPC UA channel.

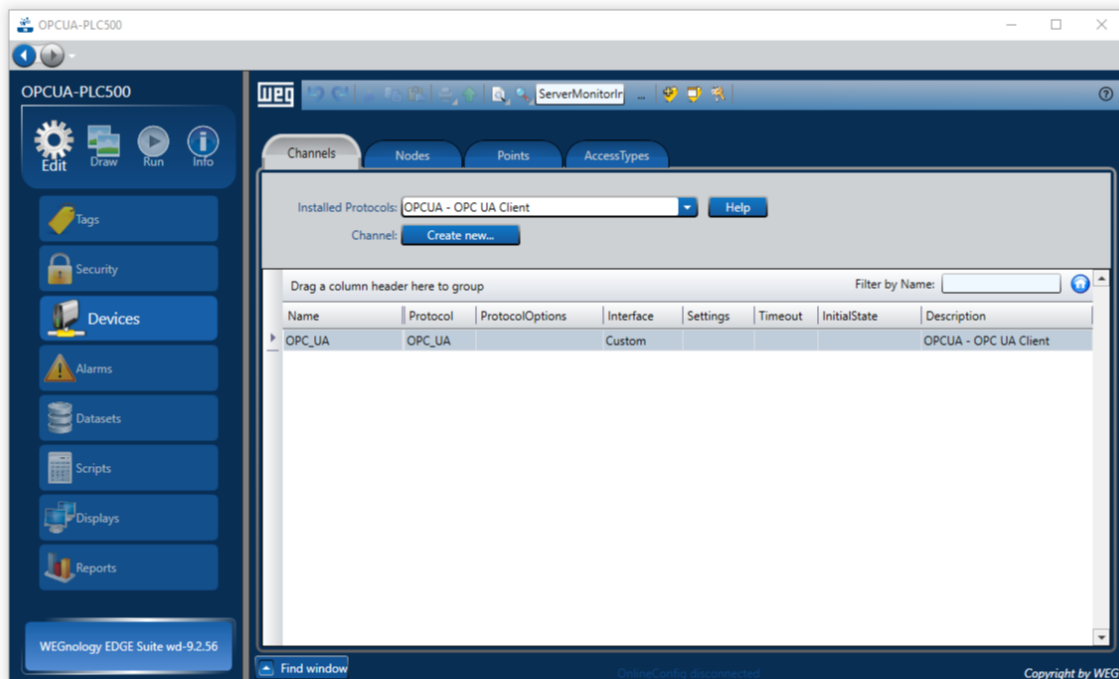


Figure 6.3: Creating a new channel.

To create a new node, go to **Edit** → **Devices** → **Nodes** → **New** and click **Ok**. In the same window, click on the blank field in **PrimaryStation** to open the arrow on the right. Click the arrow to open the configurator. In **Discovery**, enter the connection IP address in **IP Address** and click **Search**. Select the device and then click

Ok. Figure 6.4 on page 6-3 shows the screens for creating the new node.

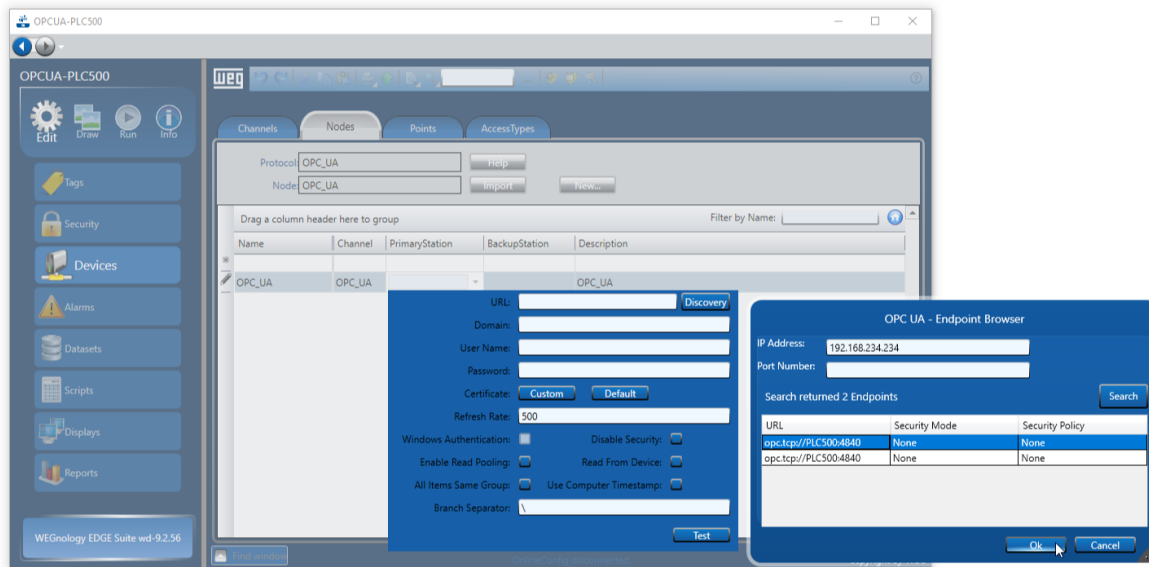


Figure 6.4: Creating and configuring a new node.

In the URL of the **Discovery** window, change the device name to the IP address of the OPC UA Server. For example, if the IP is 192.168.1.10, the URL will be **opc.tcp://192.168.1.10:4840**. Then, click **Test**. If everything goes well, the message **Connected** will be displayed next to the **Test** button. Figure 6.5 on page 6-3 shows the test for connecting a new OPC UA Server.

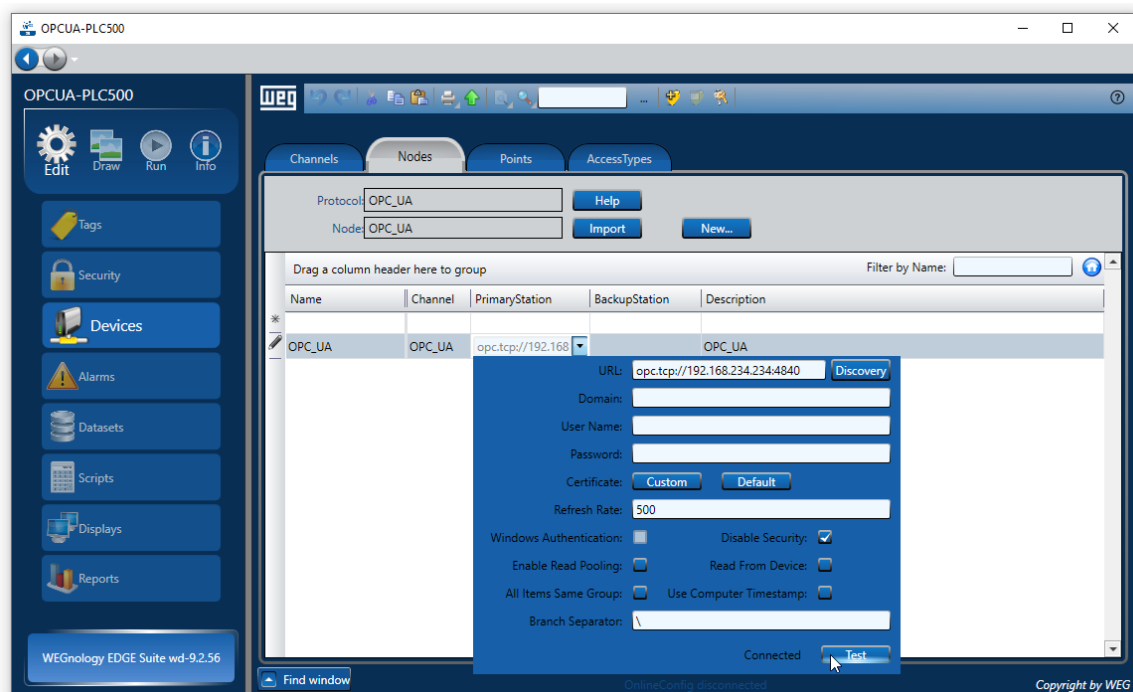


Figure 6.5: Testing and connecting a new OPC UA Server.

To select the variables of interest from CODESYS, go to **Edit** → **Devices** → **Nodes** → **Import** → **Update**. You can select a single variable, a group of variables, POU's, or entire programs. Figure 6.6 on page 6-4 shows the import of variables from the OPC UA Server.

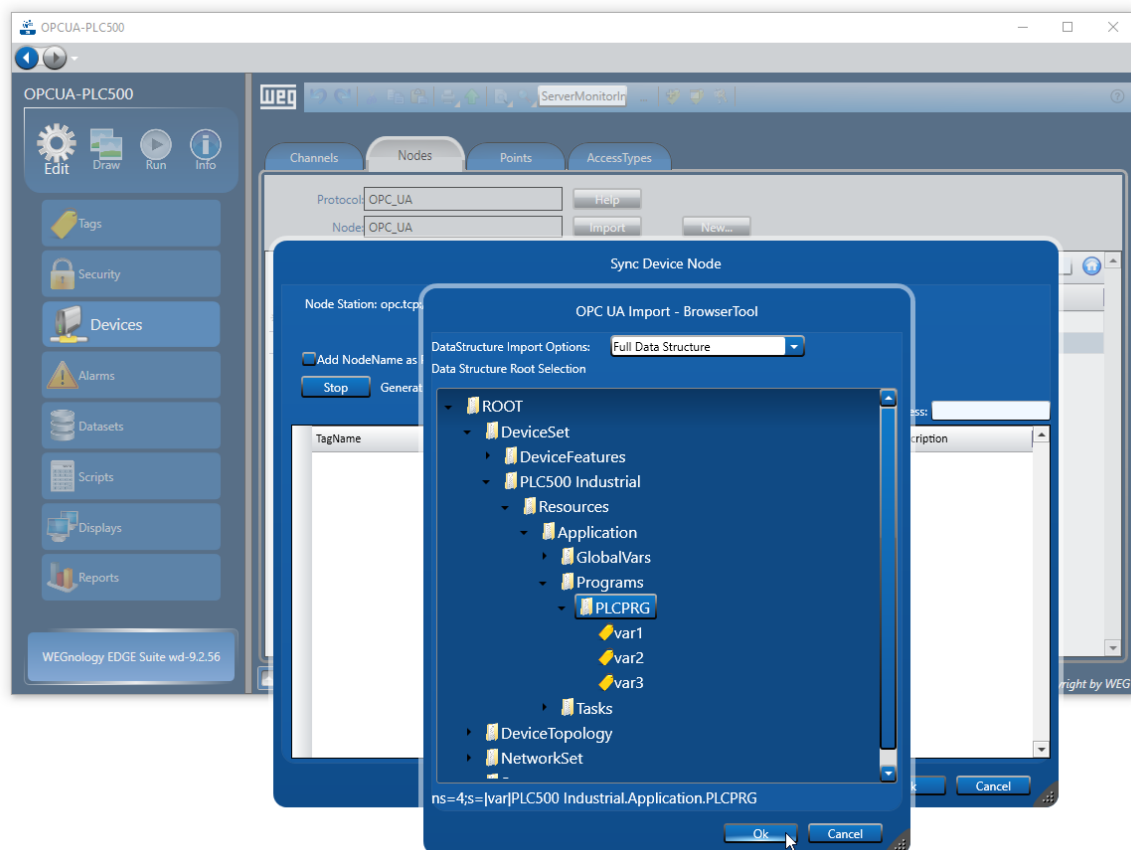


Figure 6.6: Importing variables from the OPC UA Server.

The previously selected variables can be viewed in **Edit** → **Devices** → **Points**. Their permissions can be modified in the **AccessType** option, changing between **Read**, **Write**, or **ReadWrite**. Figure 6.7 on page 6-4 shows the access permissions modification screen.

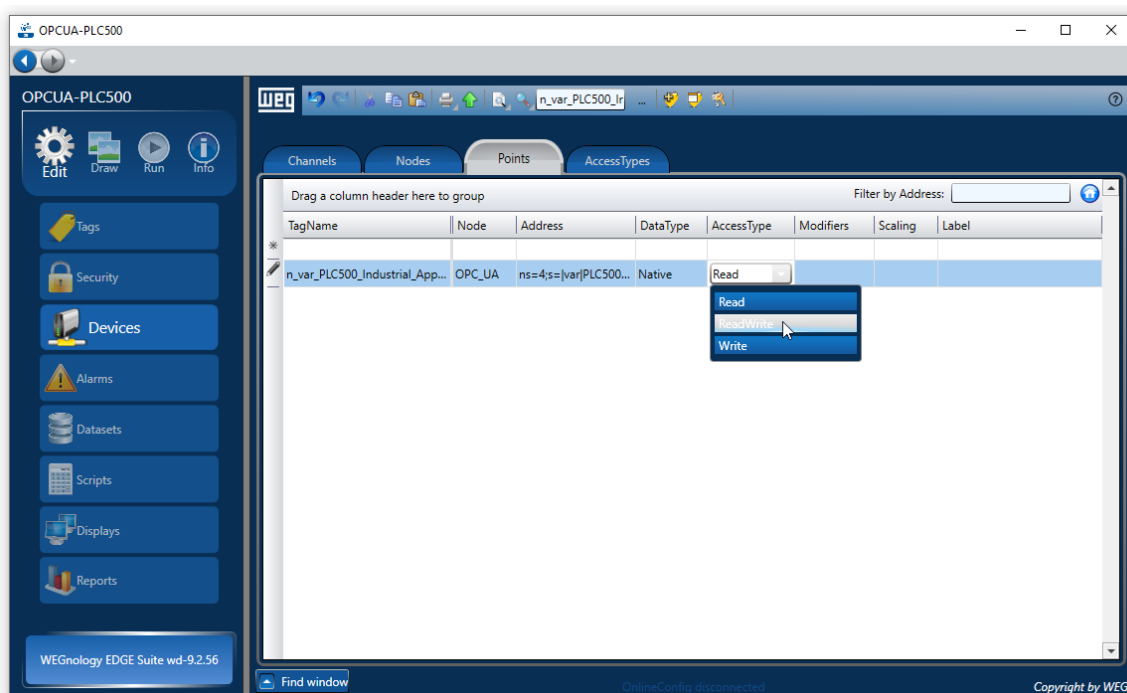


Figure 6.7: Changing access permissions.

The variables imported from CODESYS can now be used in the SCADA system. For example, go to **Draw** → **Drawing** → **TextBox**. Then, double-click the text box and go to **TextIO** → **ObjectName** → **Tag**, selecting the appropriate variable from CODESYS. [Figure 6.8 on page 6-5](#) shows how to select variables from CODESYS for use in WES.

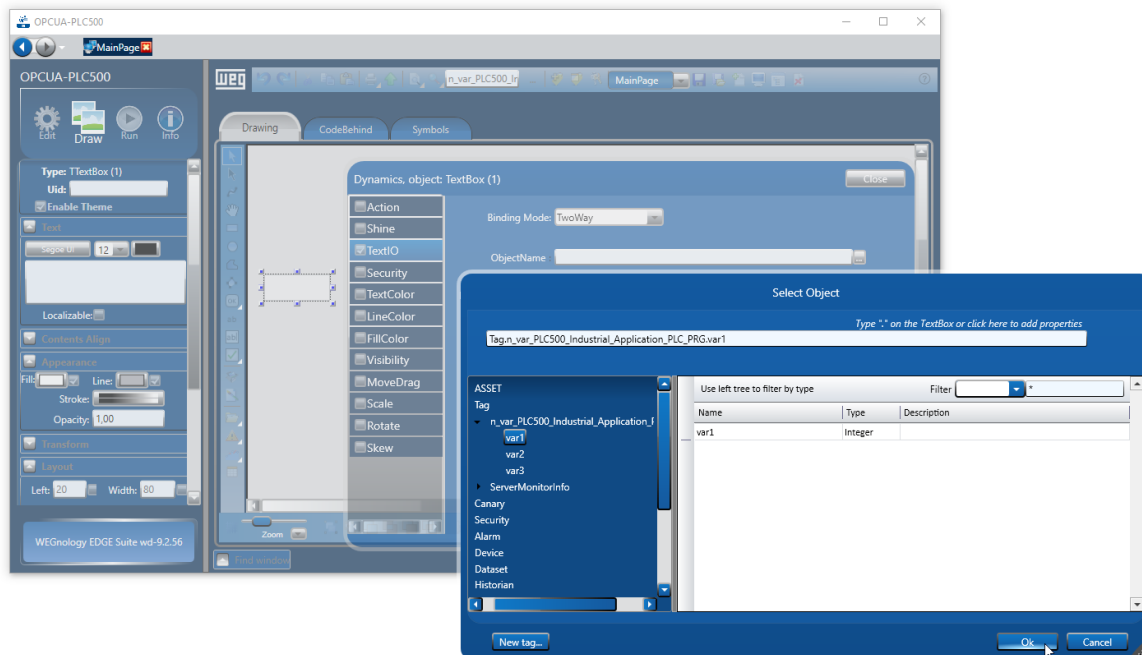


Figure 6.8: Using CODESYS variables in WES via OPC UA.

In **Execute** → **Initialization** → **Execute Initialization**, the window shown in [Figure 6.9 on page 6-5](#) opens, where the application's OPC UA variables can be monitored.

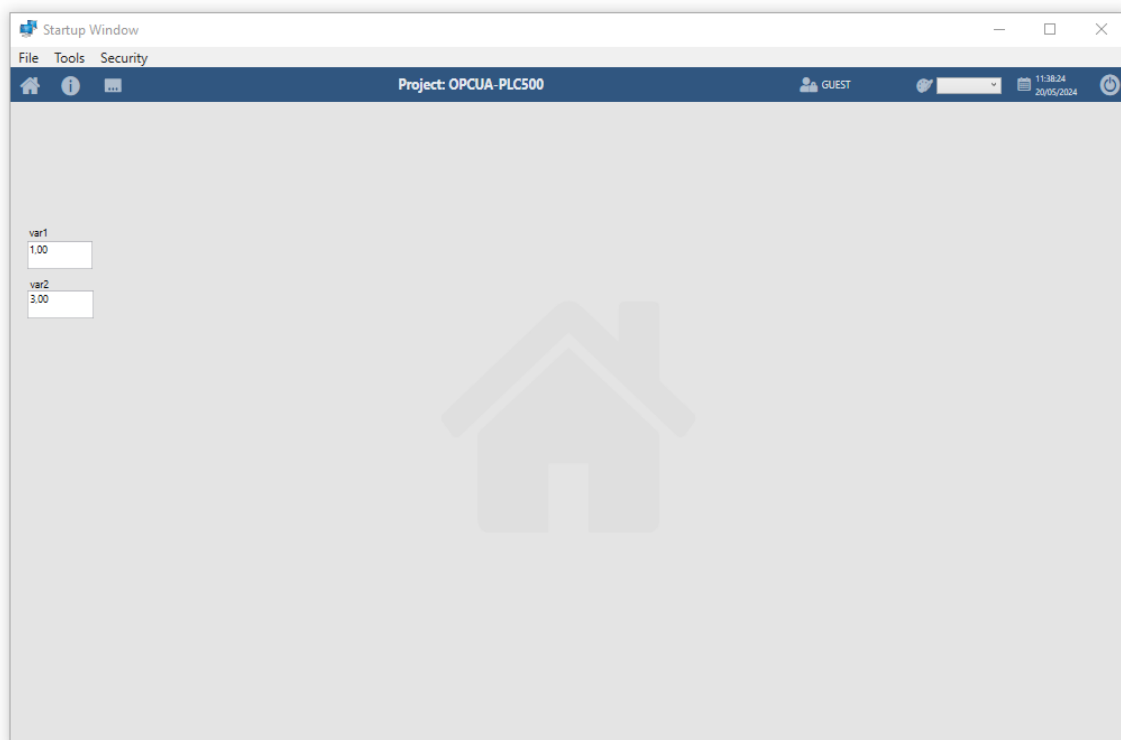


Figure 6.9: Monitoring OPC UA variables.

7 OPC UA CLIENT - EASY BUILDER PRO

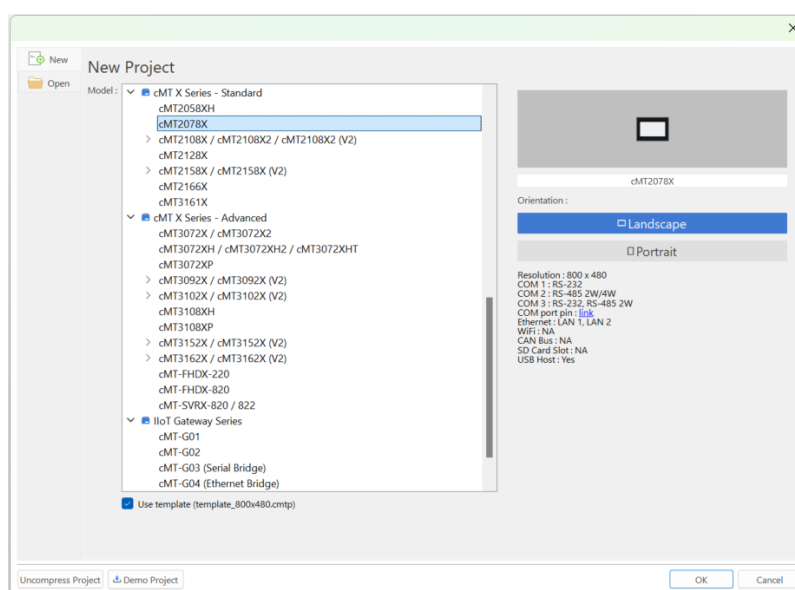
This section presents an example of configuring an OPC UA Client in Easy Builder PRO using a cMT2078X HMI. The program can be downloaded from the [Weintek](#) website.

To start, create a new project in Easy Builder PRO by accessing **File** → **New Project**, select your HMI model, and click **Ok**.

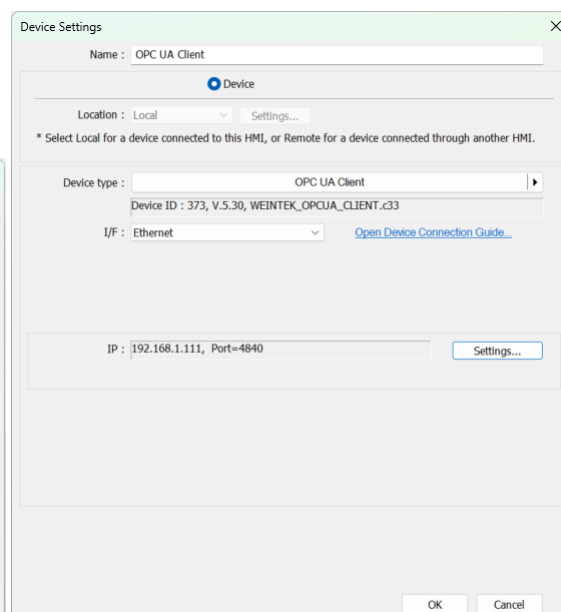
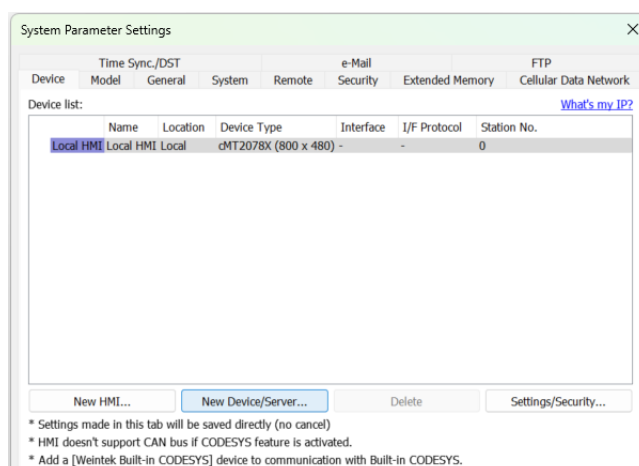


NOTE!

Currently, the WEG HMI models that support OPC UA Client are MT8051iP, MT8072iP, cMT2078X, cMT1106X, and cMT2108X2. For more information, consult the product page on the [WEG](#) website.



Next, the **System Parameter Settings** window will open. Add a new device in **New Device/Server**. In **Device Type**, select **OPC UA Client**. The **I/F**: interface should be set to **Ethernet** by default. Click **Settings** and define the IP address.



7.1 ANONYMOUS CONNECTION

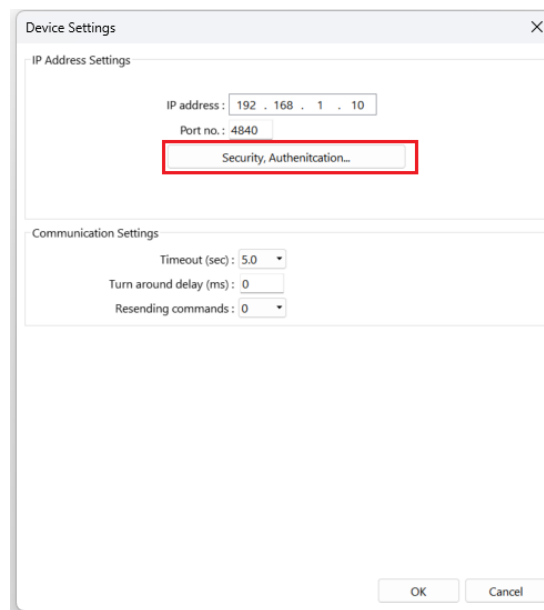
For an anonymous connection to be possible, it is necessary to enable **Allow anonymous login** in **Change Runtime Security Policy** in CODESYS. Additionally, **CommunicationMode** must be set to **ALL** for **CmpOPCUAServer** in **Device Security Settings**. Check [Section 3 SECURITY SETTINGS on page 3-1](#) for more information.



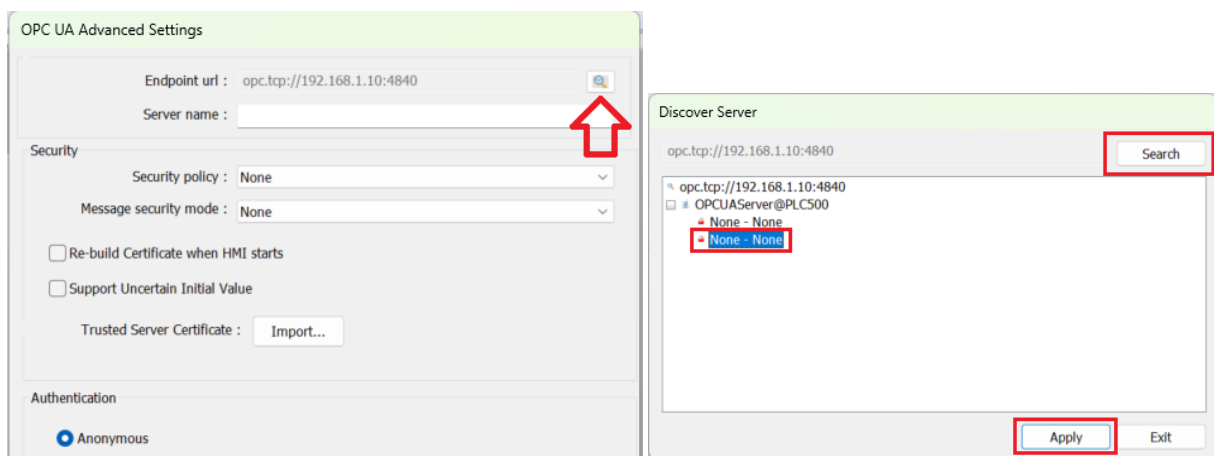
CYBERSECURITY NOTE!

The use of anonymous connection for regular application operation is not recommended due to cybersecurity issues. It should be restricted to testing, commissioning, or when other alternatives are not available.

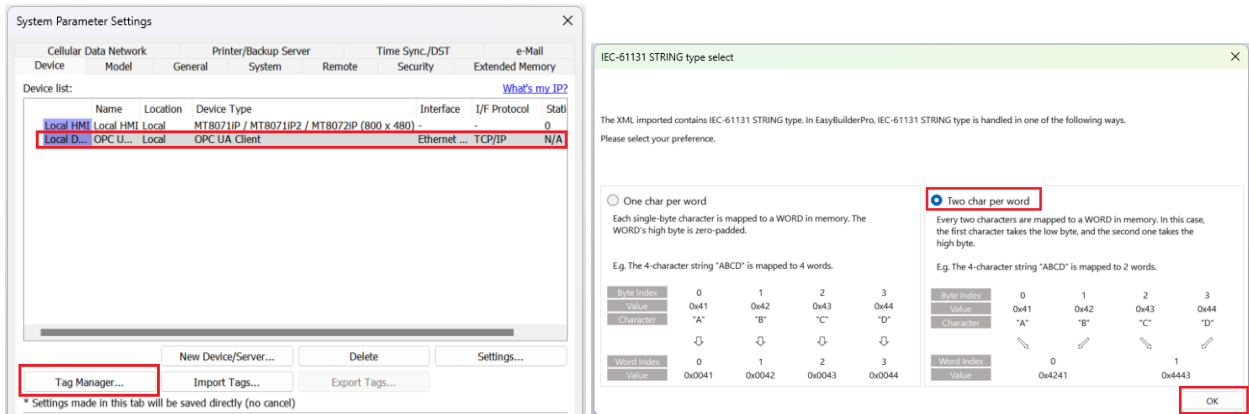
After configuring the IP of the OPC UA Server in PLC500, click **Security, Authentication**.



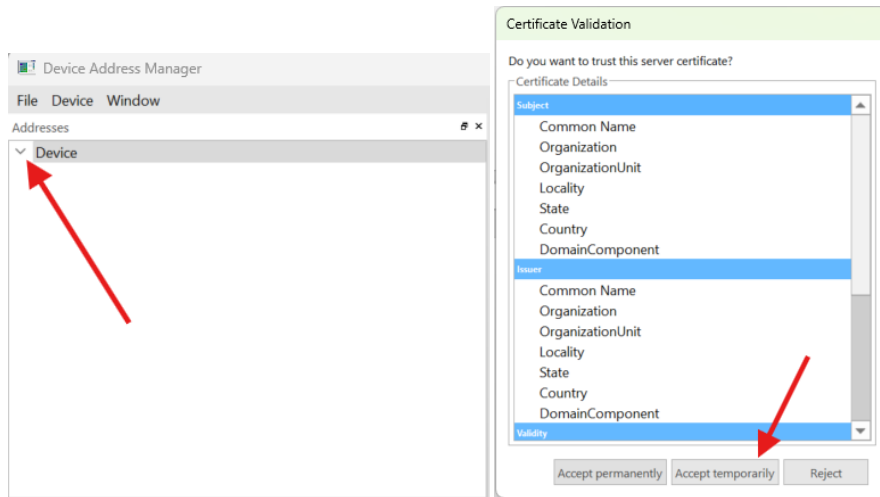
In the **OPC UA Advanced Settings** window, click the icon . Click **Search** to detect the available servers at the configured IP address. Select one of the anonymous connection options in **None** and click **Apply**. Keep the rest of the settings default and click **Ok** to close the windows until returning to **System Parameter Settings**.



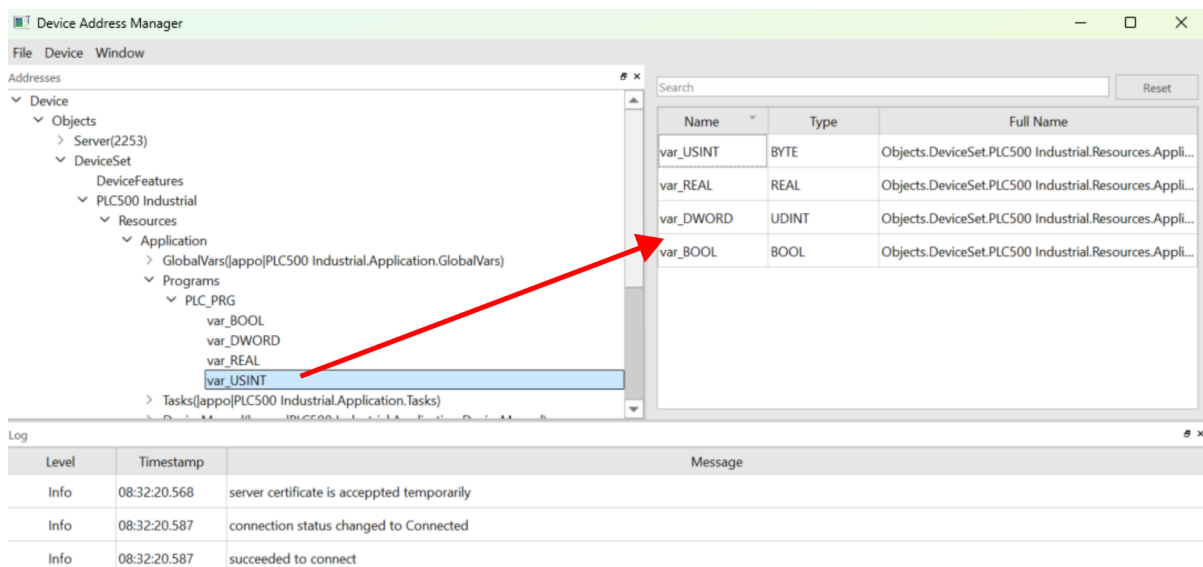
Select **OPCUA Client** and click **Tag Manager**. Select one of the variable mapping options and click **Ok**.



In the **Device Address Manager** window, ensure that the **Addresses** and **Log** options are enabled for viewing in **Window**. Click the arrow next to **Device**. A window to accept a certificate will open. Click **Accept Temporarily**.



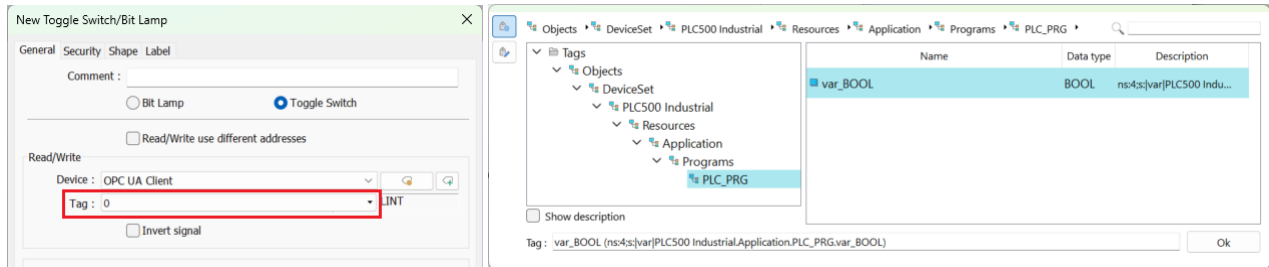
The anonymous connection with the OPC UA Server in PLC500 will be established. Click successively on the arrow in **Object** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**. All variables found in the CODESYS project programs will be displayed. In the example, the project has only one POU called **PLC_PRG**. Click the arrow next to the program to view the variables available for import into the HMI project. Drag each variable individually to the window on the side.



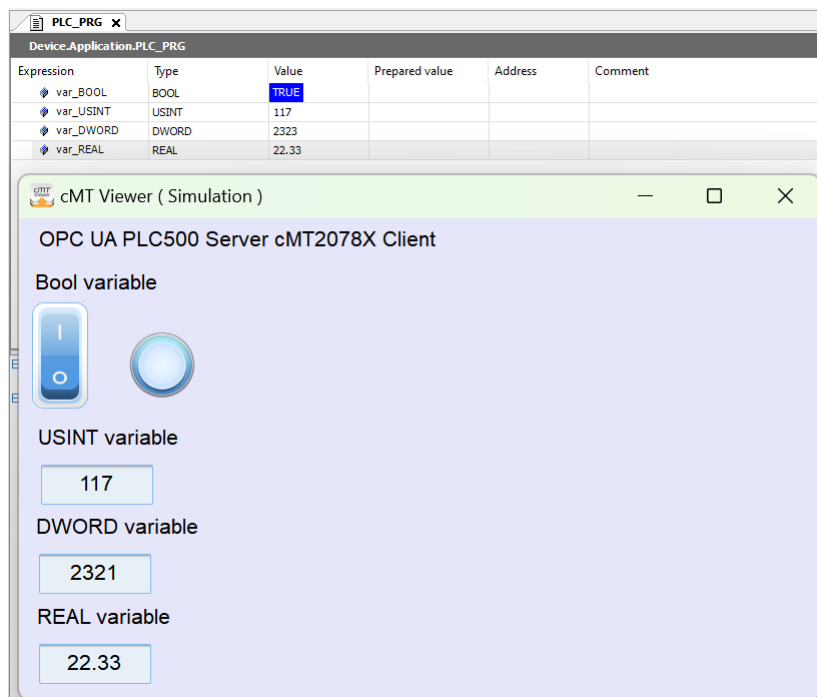
OPC UA CLIENT - EASY BUILDER PRO

After indexing all the project variables of interest, go to **File** → **Save** and then **File** → **Exit**. With the tags imported, click **Ok** in the **System Parameter Settings** window.

Add the desired objects to your interface and associate them with the variables from the PLC500 OPC UA Server by clicking **Tags**. Click successively on the icons **Tags** → **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**, and select the POU associated with the variable to be mapped.



After completing the HMI project with all the variables of interest, compile the project in **Compile** and load the program to the HMI in **Download (PC** → **HMI)**. The following image shows the online monitoring of variables in CODESYS and Easy Builder Pro through **Online Simulation**.



8 OPC UA CLIENT - PLC500ED

As highlighted at the beginning of this document, all WEG PLCs with CODESYS support the OPC UA Server. However, the **PLC500ED** also features the **OPC UA Client** functionality.

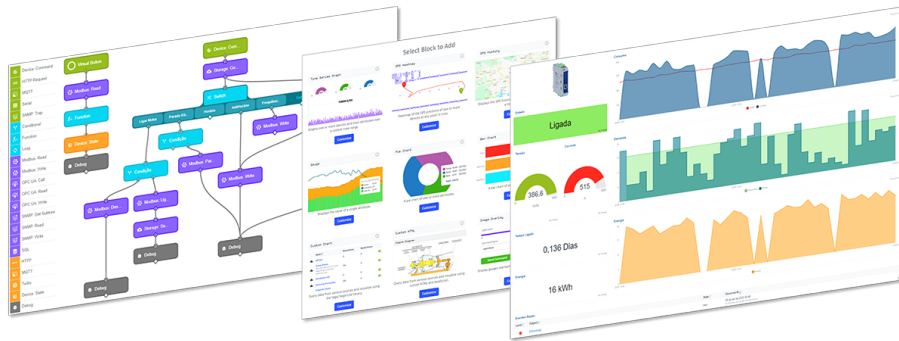


NOTE!

The use of the **OPC UA Client** protocol is only possible on the PLC500ED model through the **Edge Agent** container. This functionality cannot be used via CODESYS.

8.1 ABOUT PLC500ED

The PLC500ED retains all the functionalities of the PLC500, but with the added advantage of supporting edge computing through the **Edge Agent** container. This feature allows the connection of industrial equipment to WEG cloud platforms, such as **WEGnology** and **WEG Smart Machine**, enabling the implementation of advanced digital solutions like remote monitoring, predictive maintenance, and real-time data analysis. For more details about the product or the platforms, visit the [WEG](#) website.



8.2 QUICK CONFIGURATION

Here are the basic steps to quickly configure a WEGnology application through PLC500ED.

1. Create an application on the [WEGnology](#) website and save your credentials or obtain the credentials of a [WEG Digital Solution](#) application.
2. Connect the PLC500ED to the internet via the web page or CODESYS.
3. Enter the application data in the **Cloud Integration** tab of the web page.
4. Enable the **Edge Agent** container in the **Docker** tab of the web page.
5. Check if the device is automatically recognized as online on the platform. At this point, the **PLC500ED** will be ready to deploy the OPC UA Client application or any other workflow.

With all configurations correctly made, the PLC500ED status page should show that the product is connected to the internet, with an application also connected and the Edge Agent container running, as shown in [Figure 8.1 on page 8-2](#).

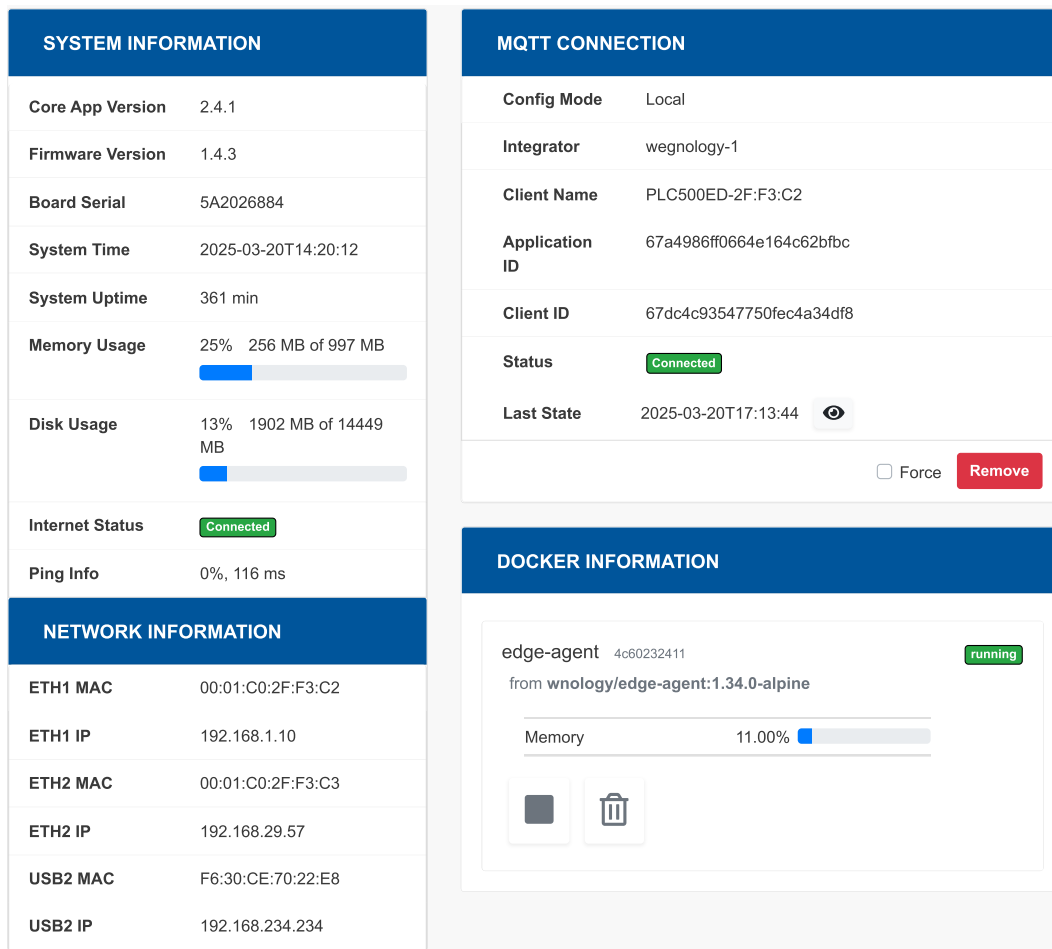


Figure 8.1: PLC500ED status page.

For more details, consult the PLC500ED Application Note, available on the [WEG](#) website.

8.3 OPC UA PING PONG

This basic application example uses a **PLC500ED** as an **OPC UA Client** and a **PLC410** as an **OPC UA Server**. Every 5 seconds, the Client reads the **iVar** variable from the Server. If the value is 1, the Client writes 0 to **iVar**. Meanwhile, the Server, through CODESYS, also reads **iVar**. If the value is 0, the Server writes 1 to **iVar** and increments **iCount**.



NOTE!

The **ETH1** interface of the **PLC500ED** must be connected to the **ETH** interface of the **PLC410**.

8.3.1 OPC UA Server - PLC410

The PLC410 must have the **ETH** configured with the IP address **192.168.1.20** and running an OPC UA Server application in CODESYS, with the **iVar** (INT) and **iCount** (INT) variables exported.



NOTE!

Any WEG PLC with CODESYS can be used as an **OPC UA Server**, as long as it is previously configured, as detailed in [Section 4 OPC UA SERVER - CODESYS on page 4-1](#).

[Figure 8.2 on page 8-3](#) shows the variable declaration and [Figure 8.2 on page 8-3](#) presents the structured text CODESYS program for the OPCUA_PingPong application.

```

OPCUA_PingPong
PROGRAM OPCUA_PingPong
VAR

    iVar : INT := 0;
    iCount : INT := 0;

END_VAR
    
```

Figure 8.2: OPCUA_PingPong variable declaration.

```

OPCUA_PingPong - Structured Text (ST)

    IF iVar = 0 THEN iVar := 1; iCount := iCount + 1; END_IF
    IF iCount > 1000 THEN iCount := 0; END_IF
    
```

Figure 8.3: OPCUA_PingPong structured text program.

8.3.2 OPC UA Client - PLC500ED

The PLC500ED must have **ETH1** configured with the IP address **192.168.1.10**, connected to the internet via **ETH2**, running the **Edge Agent** container, and with a properly configured WEGnology application. No CODESYS application is necessary.

On the main page of the WEGnology platform, go to **Workflows** → **Edge Workflows** → **Add**. Create the workflow shown in Figure 8.4 on page 8-3, composed of the blocks **Timer**, **OPC UA: Read**, **Conditional**, and **OPC UA: Write**.

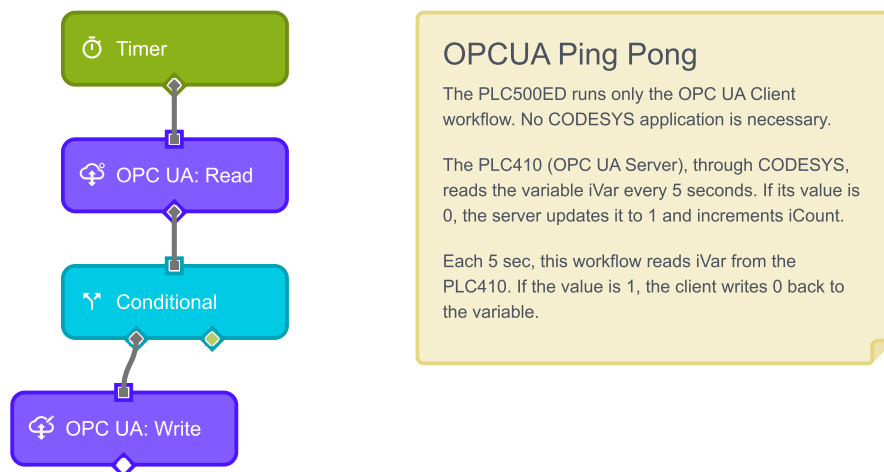


Figure 8.4: OPC UA Client Workflow.

Below is the description of the blocks and the respective configurations used:

Timer: defines the periodicity of the flow execution. Used: 5 seconds.

OPC UA: Read: reads variables from the OPC UA Server. The following configurations are used:

- OPC UA URI Template: opc.tcp://192.168.1.20:4840
- Namespace: 4
- Identifier Template: s=|var|PLC410 Industrial.Application.OPCUA_PingPong.iVar
- Result Key: iVar
- Destination Path: {data}

Conditional: evaluates a logical condition based on the values read. Condition used: {{iVar}} === '1'.

OPC UA: Write: writes variables to the OPC UA Server. The following configurations are used:

- OPC UA URI Template: opc.tcp://192.168.1.20:4840
- Namespace: 4
- Identifier Template: s=|var|PLC410 Industrial.Application.OPCUA_PingPong.iVar
- Value Source Type: 0

**NOTE!**

If it is necessary to confirm the **Namespace Index** or the **Identifier** of the variables, it may be useful to use **UAExpert**. In **UAExpert**, when accessing the OPC UA Server, it is possible to view the **NodeID**, which displays these variables in the format: ns=4;s=|var|PLC410 Industrial.Application.OPCUA_PingPong.

Upon completing the workflow, go to the upper right corner of the screen, click **Deploy**, select the device, and install the application in **Deploy Version**.



BRAZIL

WEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.

Av. Prefeito Waldemar Grubba, 3000

89256-900 - Jaraguá do Sul - SC

Phone: 55 (47) 3276-4000

Fax: 55 (47) 3276-4060

www.weg.net/br