

Unified-E OPC-UA Adapter User Manual

Configure OPC-UA Endpoints and Datapoints

Software version 3.1.0.0, last updated: July 2025

Publisher: Unified-E AG, Winterthur, Switzerland



Content

1	General.....	3
1.1	Introduction	3
1.2	Encrypted communication	3
2	Adapter Parameters in Unified-E.....	3
2.1	Endpoint Address.....	4
2.2	Adapter Parameters	4
3	Add datapoints	5
3.1	Selecting Datapoints Online	5
3.2	Addressing Datapoints	6

1 General

1.1 Introduction

OPC UA (Open Platform Communications Unified Architecture) is a platform-independent, standardized protocol for industrial communication. It enables the secure and reliable exchange of data between machines, controllers and HMI visualizations.

The OPC UA adapter allows process data from an OPC UA server (e.g. a controller) to be used in a Unified-E HMI app. For this purpose, datapoints are configured that can be read and written via the adapter.

More and more PLC control manufacturers are now offering an OPC UA interface as standard (e.g. Codesys controllers, B&R controllers)

1.2 Encrypted communication

OPC-UA enables encrypted communication. The communication participants each authorize themselves with an SSL certificate.

The SSL certificate must be trusted by the communication partner. This can be done in the following ways:

1. The SSL certificate has been trusted on the gateway PC via standard mechanisms or has been issued by a trusted certificate authority (recommended only for experienced administrators)
2. The SSL certificate (only the public key) is copied to a defined location that contains all trusted certificates

Location of your own client certificates:

%ProgramData%\OPC Foundation\CertificateStores\MachineDefault\certs

%ProgramData%\OPC Foundation\CertificateStores\MachineDefault\private

The OPC-UA adapter uses these certificates to sign data packets, for example.

Location of the trusted server certificates:

%ProgramData%\OPC Foundation\CertificateStores\UA Applications\certs

Copy the certificates of the trusted OPC UA servers to this directory.

2 Adapter Parameters in Unified-E

The endpoint address and the adapter parameters can be set in the Unified-E App Designer or in the Unified-E App Manager.

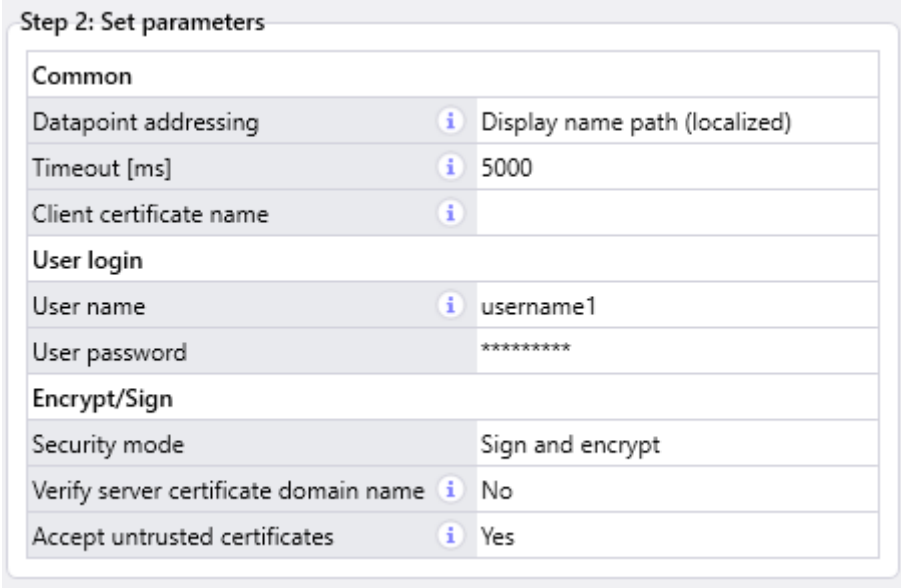
2.1 Endpoint Address

The endpoint address uniquely identifies the OPC UA server on the network.

Examples of addresses:

- `opc.tcp://192.168.1.20:48020`
- `opc.tcp://13.250.XXX.XXX:5220/RMS343/DataAccessServer`

2.2 Adapter Parameters



Step 2: Set parameters	
Common	
Datapoint addressing	Display name path (localized)
Timeout [ms]	5000
Client certificate name	
User login	
User name	username1
User password	*****
Encrypt/Sign	
Security mode	Sign and encrypt
Verify server certificate domain name	No
Accept untrusted certificates	Yes

General:

- **Datapoint Addressing:** Specifies how an OPC variable is addressed. The following options are available:
 - **Display name path (localized):** The address path consists of segments such as "Demo/Static/Scalar/Boolean". If multiple nodes have the same name, the first matching node is used. The segments are multilingual
 - **Browse name path:** The address path consists of segments such as "Demo/Static/Scalar/Boolean". If multiple nodes have the same name, the first matching node is used. The segments denote the node's browse name
 - **Node ID (fast):** The variable is identified directly by the unique NodeID, e.g. « ns=4; s=SimulationSpeed". This method is the most performant and is recommended when the node ID is known and no longer changes
- **Timeout [ms]:** Specifies how long it waits for a response from the server (for example, when connecting or reading values). The value is given in milliseconds
- **Client certificate name:** Subject name of the client certificate to use
 - This certificate must be located in the %ProgramData%\OPC Foundation\CertificateStores\MachineDefault\certs directory

- If no name is specified, a temporary client certificate is automatically generated

User Login:

- Username / User password: Optional – if the OPC UA Server requires authentication via username and password.
 - The password is stored encrypted

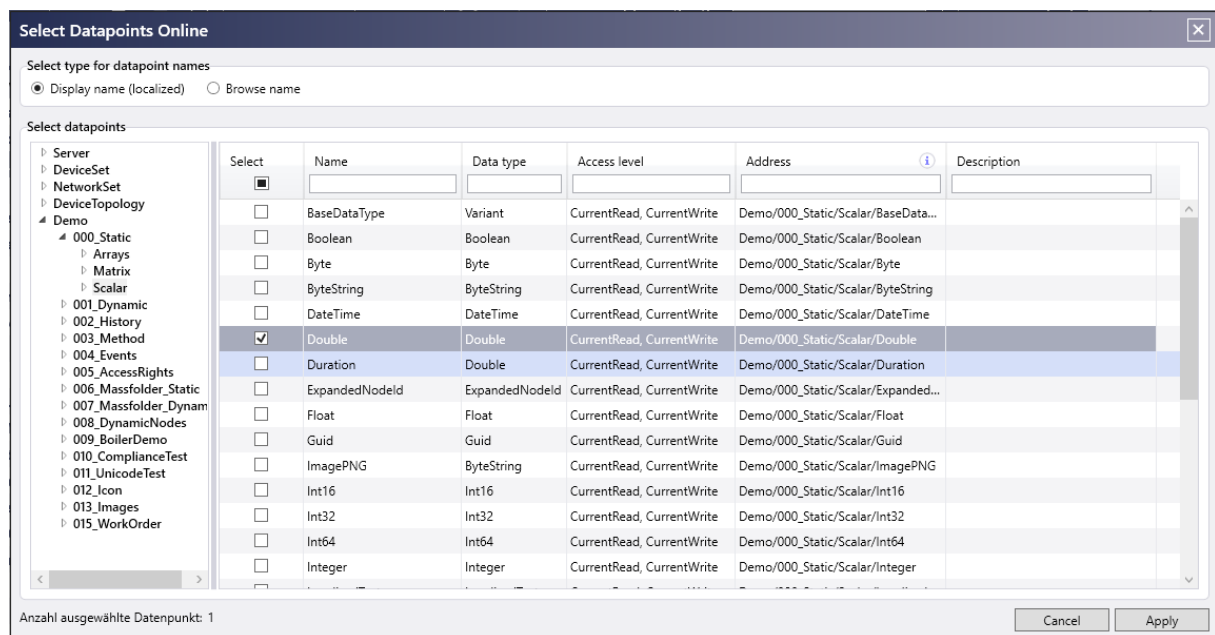
Encrypt / Sign:

- Security mode: Determines how data communication is secured:
 - None: Data is transmitted unencrypted. No other parameters required
 - Sign: The data is signed with the client certificate, but not encrypted
 - Sign and Encrypt: The communication is fully secured – both signed and encrypted
- Verify server certificate domain name: If active (value «Yes»), it checks whether the domain name in the server certificate matches the actual server address
 - This option increases security, but can be disabled for internal networks
- Accept untrusted server certificates: If active (value "Yes"), certificates that have not been signed by a trusted certificate authority will also be accepted
 - This setting is required in test environments or for self-signed certificates

3 Add Datapoints

3.1 Selecting Datapoints Online

The easiest way to add new datapoints in the Unified-E App Designer in the Endpoint Editor is to use the "Select datapoints online" button (see App Designer user manual). Clicking this button opens a dialog to select the desired datapoints of the connected OPC UA server. The selected datapoints are automatically transferred to the Datapoints table. There is no need to manually enter the datapoint address – the address is automatically entered according to the "Datapoint addressing" parameter (see above).



3.2 Addressing Datapoints

The address of a datapoint depends on the selected addressing type, which is determined by the "Datapoint addressing" parameter – see above.

In the following, the different datapoint addresses are examined in more detail.

Datapoint Addressing: « Browse name path »:

- **Advantage:** The address is easy to read, e.g. "Demo/000_Static/Scalar/Byte".
- **Disadvantage:** Initially, when establishing a connection, the node ID of the browse name path must always be determined first – which requires communication with the OPC UA servers and can lead to performance problems with many datapoints and a slow connection.

Datapoint Addressing: «Node ID (fast)»:

- **Advantage:** Fast connection, the browse path does not have to be resolved, as the node ID, which is necessary for communication, is already available.
- **Disadvantage:** The node ID is less readable depending on the OPC UA server and could already change if new variables are added in the OPC UA server or the PLC program changes.

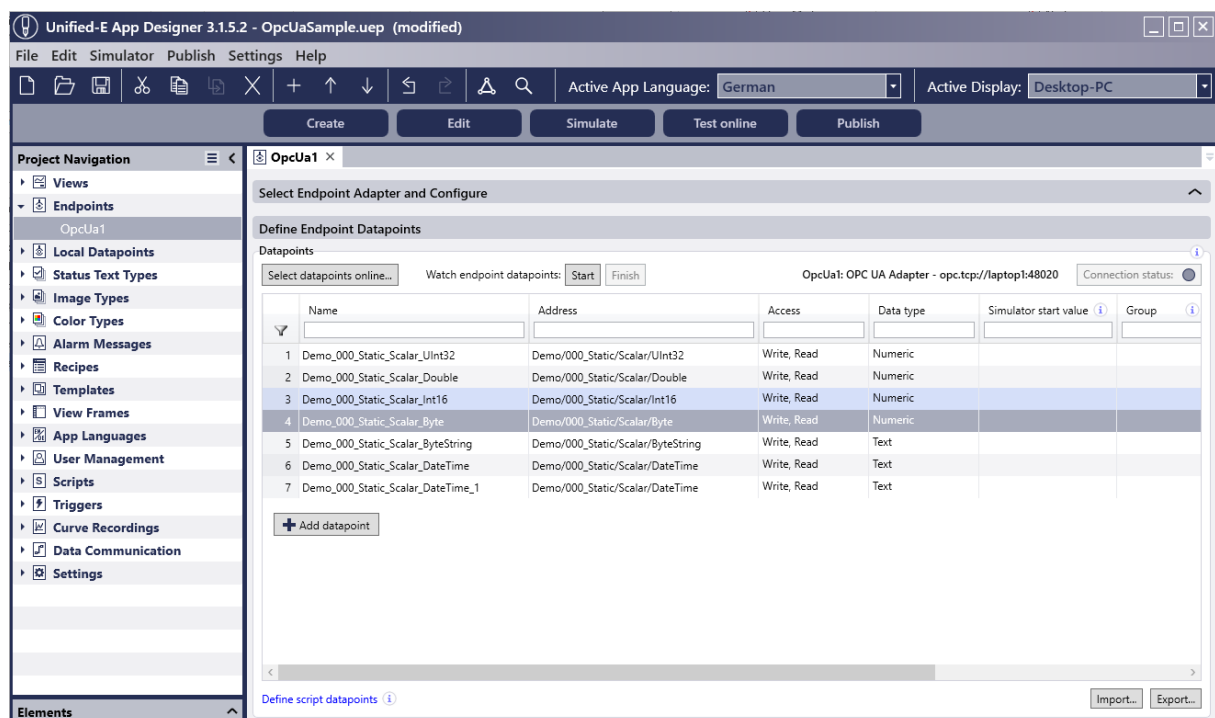
Datapoint Addressing: «Display name path (localized)»:

This type of addressing is not recommended – it should only be used if the OPC UA server only supports names in one language and the browsing name is not sufficiently meaningful.

Possible data types:

- BOOL (Boolean)
- BYTE (Byte)
- SINT (SByte)
- WORD, UINT (UInt16)
- DWORD, UDINT (UInt32)
- INT (Int16)
- DINT (Int32)
- LINT (Int64)
- ULINT (UInt64)
- REAL (Float)
- LREAL (Double)
- STRING
- DATETIME
- Array
- History Lists for Time Charts

Example addresses in the Unified-E App Designer:



Bit addressing for numeric variables:

Example: Demo/Static/Byte.0 addresses the first bit.