TECHDOCS

Technical Information

WAGO I/O System 750

750-8xxx

OPC UA Server

750-8xxx

Version 1.1.0, FW Version 03.06.09(18), OPC UA Server Version 1.2.5

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Notes about this Documentation

➔ **Note**

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation applies to the functionality “OPC UA Server” used together with the ***e!****COCKPIT* software and WAGO PFC100 or PFC200 Series Controllers.

This documentation is only applicable from FW Version 03.06.09(18), OPC UA Server Version 1.2.5.

Die vorliegende, geräteübergreifende Dokumentation umfasst Funktionen und Eigenschaften, die nicht auf allen Geräten vorhanden sind.

➔ **Note**

Observe other Applicable Documentation!
In addition to this documentation, also observe additional instructions and information provided in the operating instructions for the software and devices used. Download the operating instructions for the ***e!****COCKPIT* software and controller used (PFC100/PFC200) from the download area of the Internet site http://www.wago.com.

1.2 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO Kontakttechnik GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.

1.3 Property rights

Third-party trademarks are used in this documentation. This section contains the trademarks used. The “®” and “TM” symbols are omitted hereinafter.

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- AS-Interface® is a registered trademark of AS-International Association.
- BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of the Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI is a registered trademark of Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology of Beckhoff Automation GmbH.
- EtherNet/IP™ is a registered trademark of Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc.
- PROFIBUS® is a registered trademark of Siemens AG.
- PROFINET® is a registered trademark of Siemens AG.
- Subversion® is a registered trademark of Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

1.4 Symbols

⚠ DANGER

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ DANGER

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

NOTICE

Damage to Property!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.

ℹ **Information**

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).

1.5 Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.6 Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
“Value”	Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

2 Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1 Legal Bases

2.1.1 Subject to Changes

WAGO Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2 Personnel Qualifications

All sequences implemented on WAGO I/O System 750 devices may only be carried out by electrical specialists with sufficient knowledge in automation. The specialists must be familiar with the current norms and guidelines for the devices and automated environments.

All changes to the coupler or controller should always be carried out by qualified personnel with sufficient skills in PLC programming.

2.1.3 Use of the 750 Series in Compliance with Underlying Provisions

Fieldbus couplers, controllers and I/O modules found in the modular WAGO I/O System 750 receive digital and analog signals from sensors and transmit them to actuators or higher-level control systems. Using controllers, the signals can also be (pre-) processed.

The devices have been developed for use in an environment that fulfills the requirements of protection type IP20 and are designed for use in dry interior spaces. Protection against finger injury and solid impurities up to 12.5 mm diameter is assured; protection against water damage is not ensured. Unless otherwise specified, operation of the devices in wet and dusty environments is prohibited.
Use without additional protective measures in environments within which dust, corrosive fumes, gases or ionized radiation can occur is considered improper use.

Operating the WAGO I/O System 750 devices in home applications without further measures is only permitted if they meet the emission limits (emissions of interference) according to EN 61000-6-3. You will find the relevant information in the section “Device Description” > “Standards and Guidelines” in the manual for the used device.

Appropriate housing (per 2014/34/EU) is required when operating the WAGO I/O System 750 in hazardous environments. Please observe the installation regulations! Please note that a prototype test certificate must be obtained that confirms the correct installation of the system in a housing or switch cabinet.

The implementation of safety functions such as EMERGENCY STOP or safety door monitoring must only be performed by the F I/O modules within the modular WAGO I/O System 750. Only these safe F I/O modules ensure functional safety in accordance with the latest international standards. WAGO's interference-free output modules can be controlled by the safety function.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO Kontakttechnik GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO Kontakttechnik GmbH & Co. KG.

2.2 Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

⚠ DANGER

Do not work on devices while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

⚠ DANGER

Install device in only one suitable enclosure!
The device is an open system. Install the device in a suitable enclosure. This enclosure must:

- Guarantee that the max. permissible degree of pollution is not exceeded.
- Offer adequate protection against contact.
- Prevent fire from spreading outside of the enclosure.
- Offer adequate protection against UV irradiation.
- Guarantee mechanical stability
- Restrict access to authorized personnel and may only be opened with tools

⚠ DANGER

Ensure disconnect and overcurrent protection!
The device is intended for installation in automation technology systems. Disconnect protection is not integrated. Connected systems must be protected by a fuse.
Provide suitable disconnect and overcurrent protection on the system side!

⚠ DANGER

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

NOTICE

Ensure proper contact with the DIN-rail!
Proper electrical contact between the DIN-rail and device is necessary to maintain the EMC characteristics and function of the device.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

NOTICE

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Clean only with permitted materials!
Clean housing and soiled contacts with propanol.

NOTICE

Do not use any contact spray!
Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

NOTICE

Do not reverse the polarity of connection lines!
Avoid reverse polarity of data and power supply lines, as this may damage the devices involved.

NOTICE

Avoid electrostatic discharge!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded.

2.3 Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.
- In the control components (e.g., for WAGO I/-CHECK and CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
  Only open ports and services during commissioning and/or configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.
- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.
- If remote access to control components and control networks is required, use a Virtual Private Network (VPN).
- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.
- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.

3 Overview

OPC Unified Architecture is a platform-independent, service-oriented architecture used to describe and transport data. Because the services are independent, devices from different manufacturers can be interconnected.
The described server can release PFC100 and PFC200 Series runtime data to a product in the network when it meets the required preconditions. The device must have an ETHERNET interface that can be used for communication, and have the memory capacity and processing time required by the server.

4 Properties

4.1 Technical Data

- The OPC UA Server supports the ***e!****Runtime* runtime environment variables. The variables to be monitored must be released through the symbol configuration.

- The server supports 1000 “Monitored Items.”

- The following data types are available:
  `BOOL, BYTE, WORD, DWORD, LWORD, SINT, INT, DINT, LINT, USINT, UINT, UDINT, ULINT, REAL, LREAL, TIME, LTIME, TIME_OF_DAY, DATE, DATE_AND_TIME, STRING, WSTRING, ENUM, ARRAY, STRUCT`

Note

Einschränkungen für Strukturen und Arrays
Strukturen, die Enumerationen enthalten, werden nicht unterstützt. Arrays, die einen Enumerations-Datentyp enthalten, werden nicht unterstützt.

- The server supports user-defined IEC data types (structures and enumerators).

- The server can be operated without a runtime system; however, its rights within the system are limited (security).

- Der Server läuft unabhängig vom Laufzeitsystem und kann somit separat gestartet und gestoppt werden.

- The server supports encrypted communication.

- Login can be anonymous or with user name and password.

- The server can be operated with trusted certificates.

- Up to one thousand OPC UA 1-bit nodes can be displayed, read or written.

- The total number of OPC UA nodes is related to the device resources. Up to one thousand variable values (1 byte) are ensured.

- The server can be operated in parallel with up to 7 clients.

- The server can manage client certificates; although requests from unknown clients are refused.

Note

Anzahl der OPC-UA-Knoten abhängig von Systemleistung
Die Anzahl der OPC-UA-Knoten, die der OPC-UA-Server zur Verfügung stellen kann, ist abhängig von der verfügbaren Systemleistung. Daher kann hier keine pauschale Aussage getroffen werden.
Sowohl die IEC-Applikation als auch sonstige Systemfunktionen beeinflussen diese Anzahl. So kann z. B. eine ressourcenschonende Programmierung des Gerätes die mögliche Anzahl der OPC-UA-Knoten deutlich steigern.

4.2 Identifying the OPC UA Server Versions

The server consists of different parts. Each part has its own version ID, as listed in the table below.

Table 3: OPC UA Server Parts

OPC UA Server Parts	Version Request
WAGO OPC UA Server	The version can be requested via ServerExecutable (/usr/bin/opcua-server -v).
SDK Version Used in Server	The version can be requested via ServerExecutable (/usr/bin/opcua-server -s).
WAGO OPC UA Configuration Tool	The version can be requested via the configuration tool (/etc/config-tool/config-opcua -v).

All versions can be requested via an SSH Shell. The WAGO OPC UA Server version ID is displayed in the WBM. This version ID implies a specific SDK (Software Development Kit) version.

The configuration tool has no relevance to server operation. The build information stated in the OPC UA protocol gives the WAGO OPC UA Server version.

4.3 Differences between the WAGO OPC UA Server and the 3S OPC UA Server

The following differentiates the WAGO OPC UA Server from the 3S OPC UA Server:

- The variable parameter ”MinimumSamplingInterval” cannot be read out for any variables.
- The PLC open data types BYTE, WORD, DWORD, LWORD, DT, TOD are not available.
  IEC variables with these data types are mapped to OPC standard data types with the same dimensions.
- The run-time system data is saved in the folder “DeviceSet.” This is the only data mapping possible in the “Server” directory.
- Enumerations (Enum) use a reference type from the directory “BaseDataVariableType.” These reference types are written in the “BaseVariableType” directory by the originally installed server.
- Der 3S OPC-UA-Server verwendet standardmäßig einen anderen Namespace als der WAGO OPC-UA-Server.

5 Functions

5.1 Network

5.1.1 Network Security

5.1.1.1 Authentication

The OPC UA Server works with the users authorized to log on defined in the system under Linux. As delivered, this includes:

- root
- admin
- user

5.1.1.2 Authorization

There is no authorization concept at this time. Consequently, even if the configuration restricts user access, currently there are no restrictions for “anonymous” users.

5.1.1.3 Certificates

The server is delivered with a certificate.
Please note: The delivered certificate only offers limited security.

Therefore, exchanging this certificate with a more suitable certificate and the higher level of security it offers is recommended.

The GDS Push method can be used to exchange certificates.

For a more detailed description of certificate exchange with UAExpert, see Section “Service” > “Install New Certificate.”

5.2 Influence of Variable Types and Their Effect on Execution and Run Times

The ratio of log data to user data affects the data flow rate. Normally, the user data amount in an OPC UA node is fixed. If, for example, an OPC UA node is used with data type “byte,” the user data amount when this node is queried is 1 byte. There are three ways to increase the amount of user data:

- Combining several nodes in one query (Listen).
- Combining the same data types under a node (Arrays).
- Combining different types of data under a node (Structures).

5.2.1 List Requests

When OPC UA nodes are compiled in a list, the information of each individual node is transported and evaluated in response to the request. Because the ratio of the user data amount to the node is the same, the ratio of user data amount to query improves.

5.2.2 Array Requests

When arrays are used as OPC UA nodes, the user data amount increases according to the size of the array used. The individual elements are always the same size. The logical naming is restricted to the node names.

5.2.3 Structure Requests

When structures are used as OPC UA nodes, the user data amount increases according to the size of the structure used. To interpret the structure variable values – which are encoded for transport – in the client, additional information is needed. This information is filed in the server's “Data Type Dictionary,” and can be separately requested by the client. Thus, the information required for decoding can be requested once and reused when new data arrives.

5.2.4 Effect of Runtime Data Types on OPC UA Nodes

The runtime variable data types are like the data types the OPC UA Server offers. As a result, the selection of data types for runtime has a significant influence on the processing load (CPU load required) of the released OPC UA data.

For example, ten individual values (released by OPC UA) entail a greater processing load than a structure variable with ten fields.

6 Commissioning

6.1 Initial Connection to the OPC UA Server

6.1.1 Establishing an Unsecured Connection

An OPC UA Client is needed to establish an connection with a OPC UA Server. The following description involves a “UAExpert” client from the company “Unified Automation GmbH.”

The WAGO OPC UA server has a specific commissioning mode for initial commissioning. It is enabled as long as there are no trusted certificates on the server.

Note

Synchronize date and time on server and client!
To establish a (secured by certificate) connection between client and server, the date and time must be identical on both units.
If necessary, update the date and time on the controller.

PC with OPC UA Client

1. Start the “UAExpert.”

2. Create a new project.

3. Click **[+]** in the client menu bar to add a server.

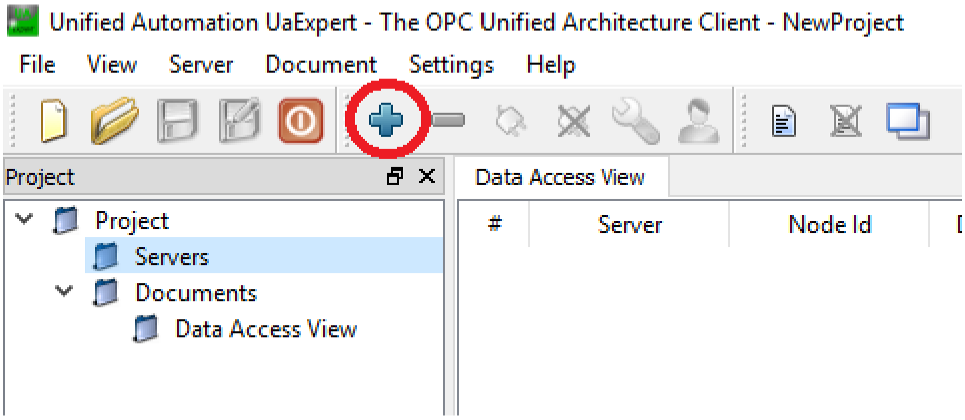


Figure 1: UAExpert User Interface

4. To open the input window for the Server URL, double-click the entry “**+ <Double Click to Add Server>**.”

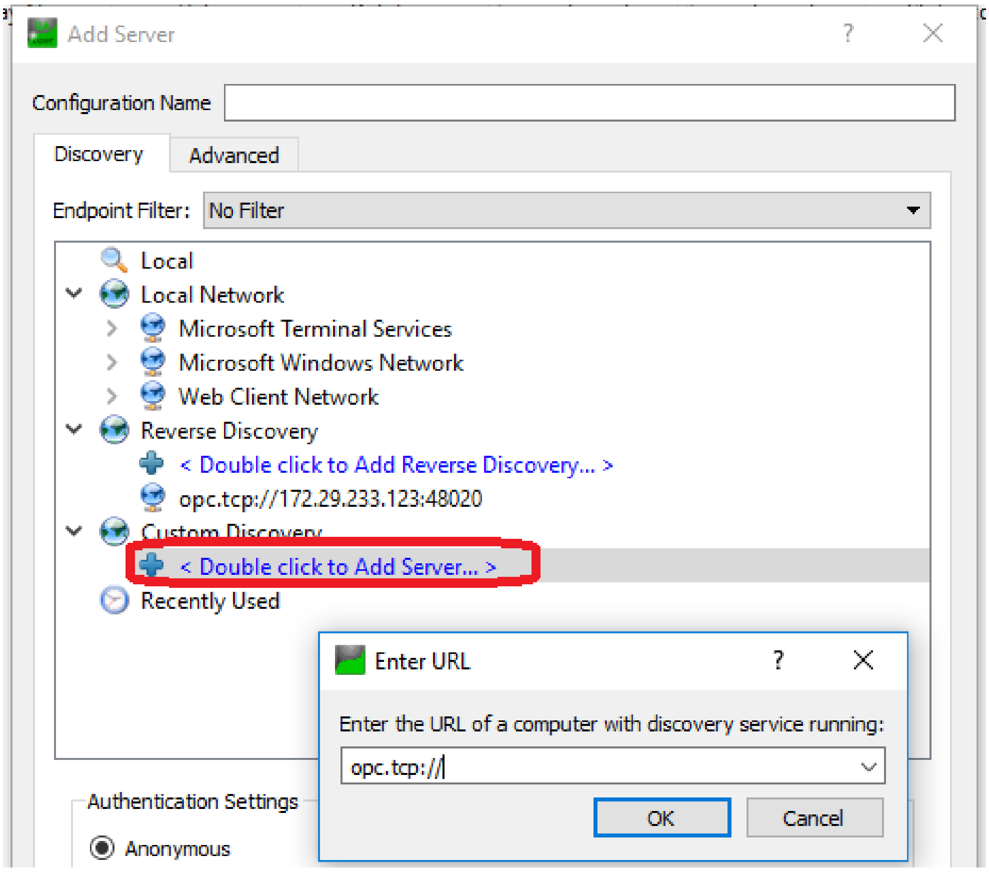

Add Server
Configuration Name
Discovery
Advanced
Endpoint Filter:
No Filter
Local
Local Network
Microsoft Terminal Services
Microsoft Windows Network
Web Client Network
Reverse Discovery
< Double click to Add Reverse Discovery... >
opc.tcp://172.29.233.123:48020
Custom Discovery
< Double click to Add Server... >
Recently Used
Authentication Settings
Anonymous
Enter URL
Enter the URL of a computer with discovery service running:
opc.tcp://
OK
Cancel

Abbildung 2: Hinzufügen eines Servers

Figure 3: Adding a Server

5. Enter “opc.tcp://[Domain name or IP address]” as the URL.

6. Click **[OK]** to confirm the entry.

7. Select the URL that was just entered.

8. Select the OPC UA Server under the URL list.

9. Confirm the prompt in the message window.

10. Select the secured connection (“Basic256Sha256”).

11. Select the option “**Username/Password**” in the “**Authentication Settings**” area.

12. Enter the user name (delivery default: “root”).

13. Tick the control field “**Store**.”

14. Enter the password (delivery default: “wago”).

15. Click **[OK]** to accept the entries.

Another approach is to create or change the user name and password through the properties dialog as described below.

16. In the project tree under “**Project**” > “**Server**,” right-click the server that was just created to open its context menu.

17. Select the menu item “**Properties**.”

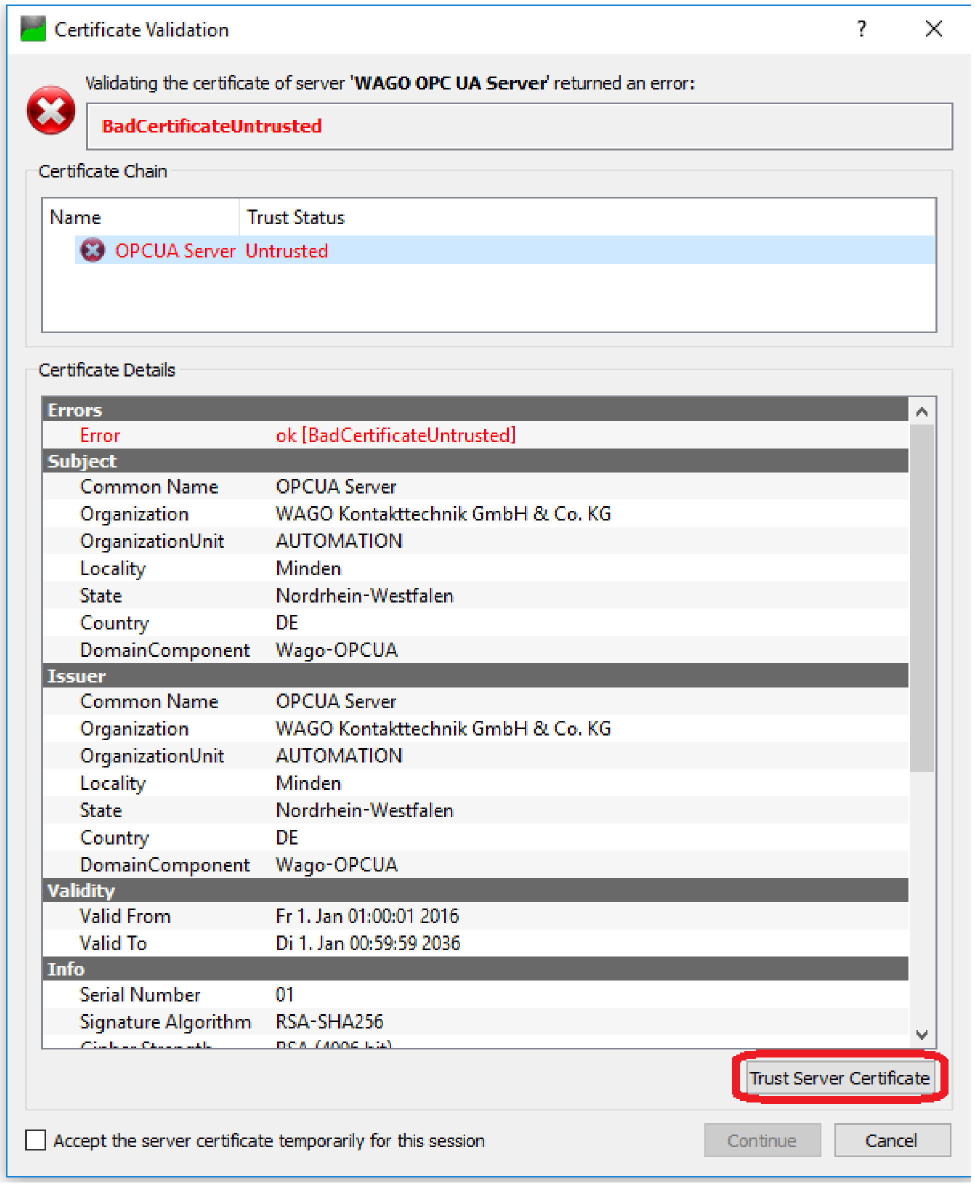
18. Enter the user name and password as described above.

19. Click **[OK]** to confirm the entries.

→ The connection parameters have been created.

20. In the project tree under “**Server**,” open the context menu of the server that was just created and select the menu item “**Connect**.”

To establish the first connection with the server, transfer the certificate delivered with the server to the list of trusted client certificates.



Validating the certificate of server '**WAGO OPC UA Server**' returned an error:

BadCertificateUntrusted

Certificate Chain

Name	Trust Status
OPCUA Server	Untrusted

Certificate Details

Errors	
Error	ok [BadCertificateUntrusted]
Subject	
Common Name	OPCUA Server
Organization	WAGO Kontakttechnik GmbH & Co. KG
OrganizationUnit	AUTOMATION
Locality	Minden
State	Nordrhein-Westfalen
Country	DE
DomainComponent	Wago-OPCUA
Issuer	
Common Name	OPCUA Server
Organization	WAGO Kontakttechnik GmbH & Co. KG
OrganizationUnit	AUTOMATION
Locality	Minden
State	Nordrhein-Westfalen
Country	DE
DomainComponent	Wago-OPCUA
Validity	
Valid From	Fr 1. Jan 01:00:01 2016
Valid To	Di 1. Jan 00:59:59 2036
Info	
Serial Number	01
Signature Algorithm	RSA-SHA256

☐ Accept the server certificate temporarily for this session

Figure 4: Confirming the Server Certificate

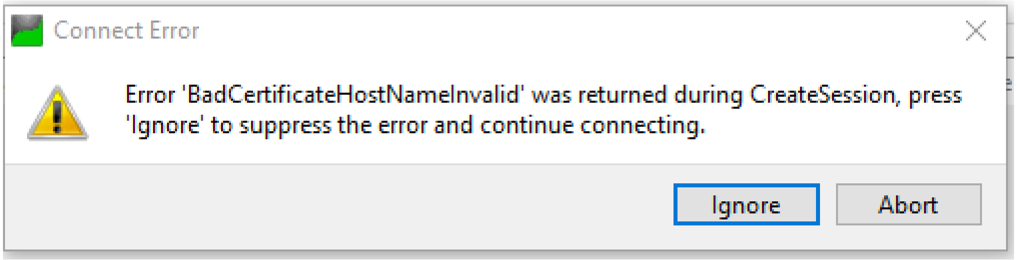
21. To transfer the certificate, click the button **[Trust Server Certificate]** in the "**Certificate Validation**" window.

22. Click **[Continue]** to close the window and establish the connection.

Note

Exchange the certificate!
This certificate is delivered with all servers and only offers limited security. Exchange the delivered certificate for one with a higher security level.

When an encrypted connection is established, the host name and the entries in the certificate are checked.
The following message is displayed if the entries do not agree.



Error 'BadCertificateHostNameInvalid' was returned during CreateSession, press 'Ignore' to suppress the error and continue connecting.

Figure 5: Message for Successful Connection

23. To establish the connection despite mismatched entries, click **[Ignore]** in the message window.

→ Then an initial, unsecured connection is established.

6.1.2 Establishing and Configuring a Secured Connection

To set up a secure connection, the certificate must still be changed. Please proceed as follows:

1. To open the associated context menu, right-click **“Documents”** under “**Projects**” in the project tree.
2. Select the “**Add …**” menu item to add a “GDS Push View” document.
3. Click the **[Add]** button in the window that appears to confirm the addition.
4. Open the “**GDS Push View**” tab.
5. Click the **[Create Certificate …]** button in the right “**Server Certificate**” section.
6. Click **[OK]** to confirm the following notice.
7. Make the required settings.
8. Click **[OK]** to confirm the settings.
9. Click the button **[Download]** to load the certificate to the controller.

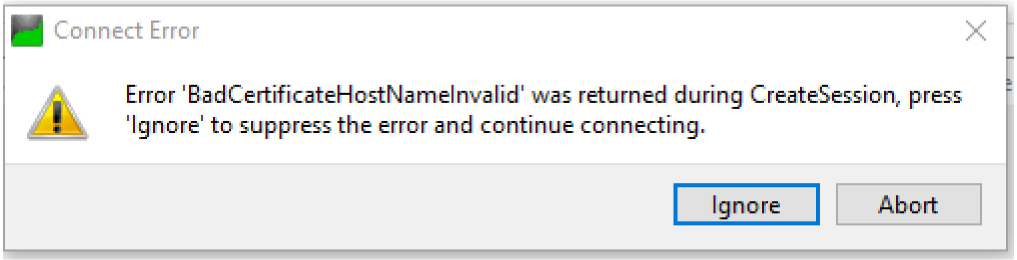
→ A message window with a prompt appears.

10. Click the button **[No]** to take over the certificate without any changes and close the message window.

→ Another message window with a reminder appears.

11. Click the **[OK]** button to confirm the reminder and close this message window.
12. To transfer the certificate, click the button **[Trust Server Certificate]** in the “**Certificate Validation**” window.
13. Click **[Apply Settings]** to finish the process.
14. Click **[Disconnect]** to break the connection.
15. Click **[Connect]** to reestablish the connection.

When an encrypted connection is established, the host name and the entries in the certificate are checked.
The following message is displayed if the entries do not agree.



Error 'BadCertificateHostNameInvalid' was returned during CreateSession, press 'Ignore' to suppress the error and continue connecting.

Figure 6: Message for Successful Connection

16. To establish the connection despite mismatched entries, click **[Ignore]** in the message window.

→ In the “**GDS Push View**” window, area “**Server Certificate Groups**,” now the **“Trusted”** tab contains a certificate created by “UAExpert” that has not yet been ranked as trusted. This certificate is marked with a red “X.”

17. Right-click to open the context menu of this certificate entry.

18. Select the menu item “**Trust**.”

→ The certificate on the server has been exchanged. The exchanged certificate is marked with a green checkmark.

19. Save the settings for later use in a new project.

→ After this step, only a connection secured with a corresponding certificate can be made to the server. The commissioning mode is terminated automatically. No further clients can access the server unless they have a corresponding certificate.

6.2 Configuration

The WAGO OPC UA Server can be configured through the Web-Based Management (WBM).

6.2.1 Web-Based-Management (WBM)

Die Informationen und Einstellungen für den WAGO OPC-UA-Server sind auf den WBM-Seiten „**OPC UA Status**“, „**OPC UA Configuration**“ und „**OPC UA Information Model**“ dargestellt.

Die Seiten sind über das Register „**Fieldbus**“ und den Auswahlpunkt „**OPC UA**“ erreichbar.

6.2.1.1 “Fieldbus” Tab

6.2.1.1.1 Seite „OPC UA Status“

Auf der Seite „OPC UA Status“ finden Sie Statusinformationen zum OPC-UA-Dienst.

Gruppe „OPC UA Server“

Tabelle 4: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server“

Parameter	Bedeutung
State	Hier wird der aktuelle Status (enabled/disabled) des WAGO OPC-UA-Servers angezeigt.
Version	Hier wird die installierte Version des WAGO OPC-UA-Servers angezeigt.
License	Hier wird eine ggf. vorhandenen OPC-UA-Server-Lizenz angezeigt. Einige Features des WAGO OPC-UA-Servers setzen eine spezielle kostenpflichtige Lizenz voraus.

6.2.1.1.2 Seite „OPC UA Configuration“

Auf der Seite „OPC UA Configuration“ finden Sie die Einstellungen zum OPC-UA-Dienst.

Gruppe „General OPC UA Server Configuration“

Tabelle 5: WBM-Seite „OPC UA Configuration“ – Gruppe „General OPC UA Server Configuration“

<table>
<tr><th>Parameter</th><th colspan="2">Bedeutung</th></tr>
<tr><td>Service enabled</td><td colspan="2">Hier aktivieren oder deaktivieren Sie den WAGO OPC-UA-Server.</td></tr>
<tr><td>Ctrl Configuration name</td><td colspan="2">Hier geben Sie den Konfigurationsnamen an, den der Controller innerhalb des PLC Open Device Sets erhält.</td></tr>
<tr><td>Log level</td><td colspan="2">Hier wählen Sie den Log-Level aus. Folgende Werte sind einstellbar: Info / Debug / Warning / Error.
Mit dem Log-Level „Error“ werden nur Fehlermeldungen ausgegeben, mit dem Log-Level „Info“ auch Statusmeldungen. Die Auswahl des Log-Levels beeinflusst die Reaktionszeit des Servers. Wählen Sie daher nur den minimal benötigten Level aus, z. B. „Debug“ nur für tiefgreifende Analysen.</td></tr>
<tr><td rowspan="3">Unlimited anonymous access</td><td colspan="2">Hier stellen Sie die Rechte für den Zugriff auf die vom Server bereitgestellten Daten ein.</td></tr>
<tr><td>Enabled</td><td>Ein nicht registrierter Benutzer kann alle Variablen sehen, lesen und schreiben.</td></tr>
<tr><td>Disabled</td><td>Für den Vollzugriff auf die Daten ist ein Benutzer-Login mit den passenden Rechten erforderlich.</td></tr>
</table>

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „OPC UA Endpoints“

Tabelle 6: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Endpoints“

Parameter	Bedeutung
Security Policy - None	Hier aktivieren oder deaktivieren Sie den OPC-UA-Endpoint „None“. Dieser ermöglicht, eine ungesicherte Verbindung zum OPC-UA-Server aufzubauen.
Security Policy - Basic128Rsa15	Hier aktivieren oder deaktivieren Sie die Security-Policy „Basic128Rsa15“. **Hinweis:** Diese Policy wird nicht mehr als sicher eingestuft.
Security Policy - Basic256Sha256	Die Security-Policy „Basic256Sha256“ ermöglicht, eine gesicherte Verbindung mit dem OPC-UA-Server aufzubauen.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „OPC UA Security Settings“

Tabelle 7: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Security Settings“

Parameter	Bedeutung	
Trust all clients	Hier aktivieren oder deaktivieren Sie die Verifikation.	
	Enabled	Es wird eine Verbindung zu allen Clients erlaubt. → Keine Sicherheit!
	Disabled	Es wird nur eine Verbindung zu Clients mit sichern Zertifikaten zugelassen.
Application URI Check	Hier aktivieren oder deaktivieren Sie die URI-Prüfung. Eine deaktivierte URI-Prüfung ermöglicht es, eine Verbindung zu einem OPC-Server aufzubauen, auch wenn dessen URI sich von der in den Zertifikaten hinterlegten URI unterscheidet.	
Error Certificate Time	Hier aktivieren oder deaktivieren Sie die Zeitüberprüfung. Zertifikate können ein Ablaufdatum besitzen. Dieses Datum wird mit der aktuellen Zeit des Gerätes überprüft. Wenn das Gerät eine falsch eingestellte Zeit besitzt, kann die Prüfung nicht erfolgreich durchgeführt werden.	
Certificate Issuer Time Invalid	Hier aktivieren oder deaktivieren Sie die Überprüfung des Zeitstempels. CA-Zertifikate enthalten einen Zeitstempel bzw. eine Gültigkeit vom Aussteller. Dieser wird mit Hilfe der Zeit auf der Server-Hardware überprüft. Durch eine fehlerhafte bzw. nicht vorhandene Zeiteinstellung auf der Server-Hardware kann es dazu kommen, dass das Zertifikat als ungültig gekennzeichnet wird.	
Certificate Revocation Unknown	Hier aktivieren oder deaktivieren Sie die Überprüfung der Erreichbarkeit des Speicherortes für zurückgezogene Zertifikate. Jedes Zertifikat kann einen Ort für zurückgezogene Zertifikate besitzen. Falls der angegebene Ort z. B. durch Netzwerkprobleme nicht erreicht werden kann, wird das Zertifikat nicht akzeptiert.	
Certificate Issuer Revocation Unknown	Hier aktivieren oder deaktivieren Sie die Überprüfung der Erreichbarkeit des Ablageortes für zurückgezogene Zertifikate. Jedes Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) kann eine Angabe für den Ablageort von zurückgezogenen Zertifikaten enthalten. Kann dieser Ort nicht erreicht werden, wird das Zertifikat vom Server nicht akzeptiert.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

6.2.1.1.3 Seite „OPC UA Information Model“

Auf der Seite „OPC UA Information Model“ finden Sie die Einstellungen zum OPC-UA-Informationsmodell.
Die Seite ist nur sichtbar bei Controllern der 2. Generation (750-821x/xxx-xxx), die Softwarekomponenten unterstützen, die einer Lizenzprüfung unterliegen (Runtime-Lizenzen).

Gruppe „OPC UA Server Information Model“

Tabelle 8: WBM-Seite „OPC UA Information Model“ – Gruppe „OPC UA Server Information Model“

Parameter	Bedeutung
Feature enabled	Hier aktivieren oder deaktivieren Sie das OPC UA Server-Informationsmodell.
informationmodel.xml	Hier wählen Sie eine XML-Beschreibungsdatei für das anzuwendende Informationsmodell aus. Die Verwendung eines spezifischen Informationsmodells setzt eine erweiterte OPC UA Lizenz voraus!

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um die ausgewählte Beschreibungsdatei auf den Controller zu übertragen, klicken Sie die Schaltfläche **[Upload]**.

Um die installierte Beschreibungsdatei vom Controller zu löschen, klicken Sie die Schaltfläche **[Delete]**. Nach dem Löschen wird wieder das standardmäßig installierte PLC-Open-Informationsmodell verwendet.

7 Service

7.1 Installing a New Certificate

An encrypted, authenticated connection is required to make changes to the certificates.

Note

Nur temporär alle Clients zulassen!
Wenn der Aufbau einer verschlüsselten Verbindung zum OPC-UA-Server nicht möglich ist, aktivieren Sie die Option **Trust all Clients** im WBM, damit der OPC-UA-Server eine Verbindung mit allen Clients akzeptiert. Deaktivieren sie die Option, nachdem Sie die nachfolgenden Schritte vollständig durchgeführt haben!

PC with UAExpert

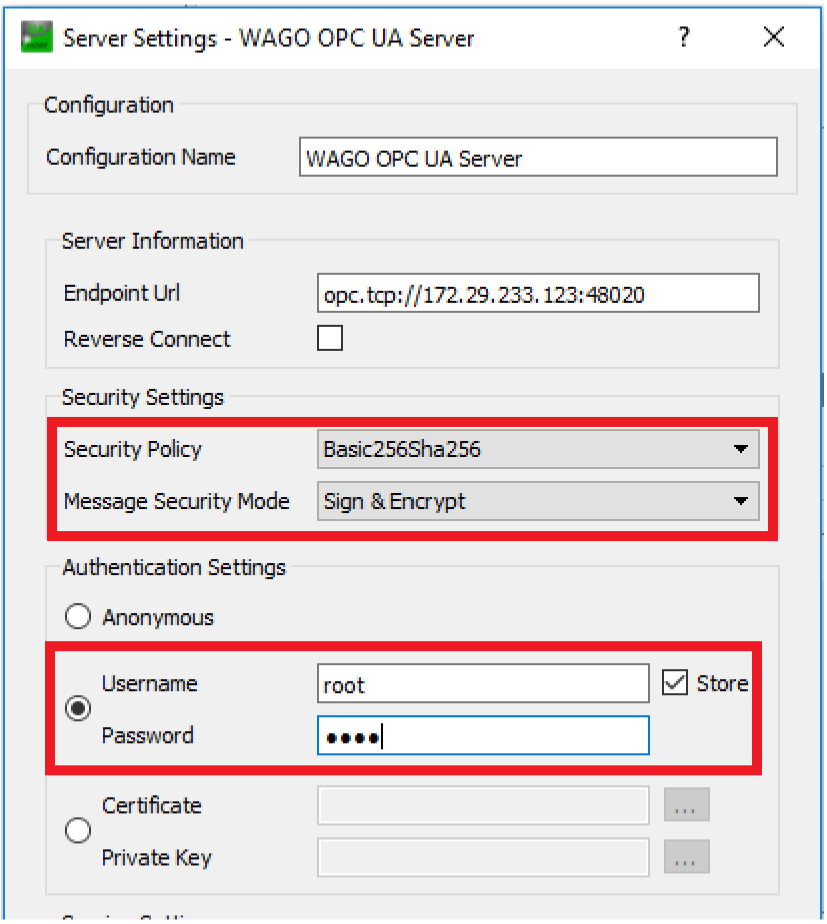
1. Start the “UAExpert.”

2. Open the project with the current settings.

3. In the project tree under “**Project**” > “**Server**,” open the WAGO OPC UA Server context menu with a right click.

4. Select the menu item “**Properties**.”

5. Check the following settings; adapt as necessary.



Server Settings - WAGO OPC UA Server

Configuration
Configuration Name: WAGO OPC UA Server

Server Information
Endpoint Url: opc.tcp://172.29.233.123:48020
Reverse Connect: □

Security Settings
Security Policy: Basic256Sha256
Message Security Mode: Sign & Encrypt

Authentication Settings
○ Anonymous
● Username: root ☑ Store
Password: ••••
○ Certificate
Private Key

Figure 7: Opening Connection Settings

“UAExpert” has a special view (GDS Push View) for the certificate exchange. If there is a connection to the server, a new server certificate can be created in this view. Certificates created from another site can be loaded too.

Follow these steps to open this view:

PC with UAExpert

6. To open the associated context menu, right-click **“Documents”** under “**Project**” in the project tree.

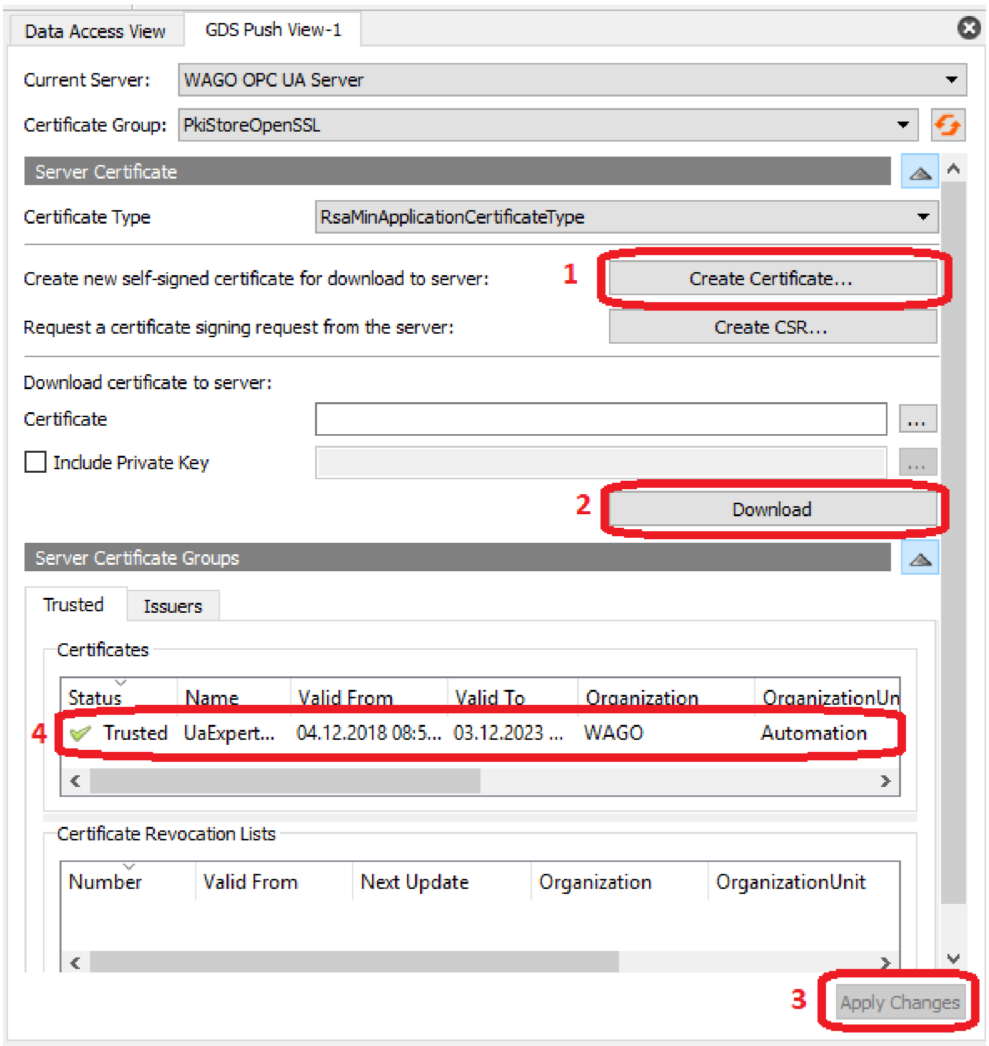
7. Select the “**Add …**” menu item.

→ The “**Add Document**” dialog appears.

8. In the “**Document Type**” selection field, select the value “GDS Push View.”

9. Click **[Add]** to close the dialog window and save the view.

→ The following tab is opened (Fig. “GDS Push View”).



Current Server: WAGO OPC UA Server

Certificate Group: PkiStoreOpenSSL

Certificate Type RsaMinApplicationCertificateType

Create new self-signed certificate for download to server:

Request a certificate signing request from the server:

Download certificate to server:

Certificate

□ Include Private Key

Status	Name	Valid From	Valid To	Organization	OrganizationUn
✓ Trusted	UaExpert...	04.12.2018 08:5...	03.12.2023 ...	WAGO	Automation

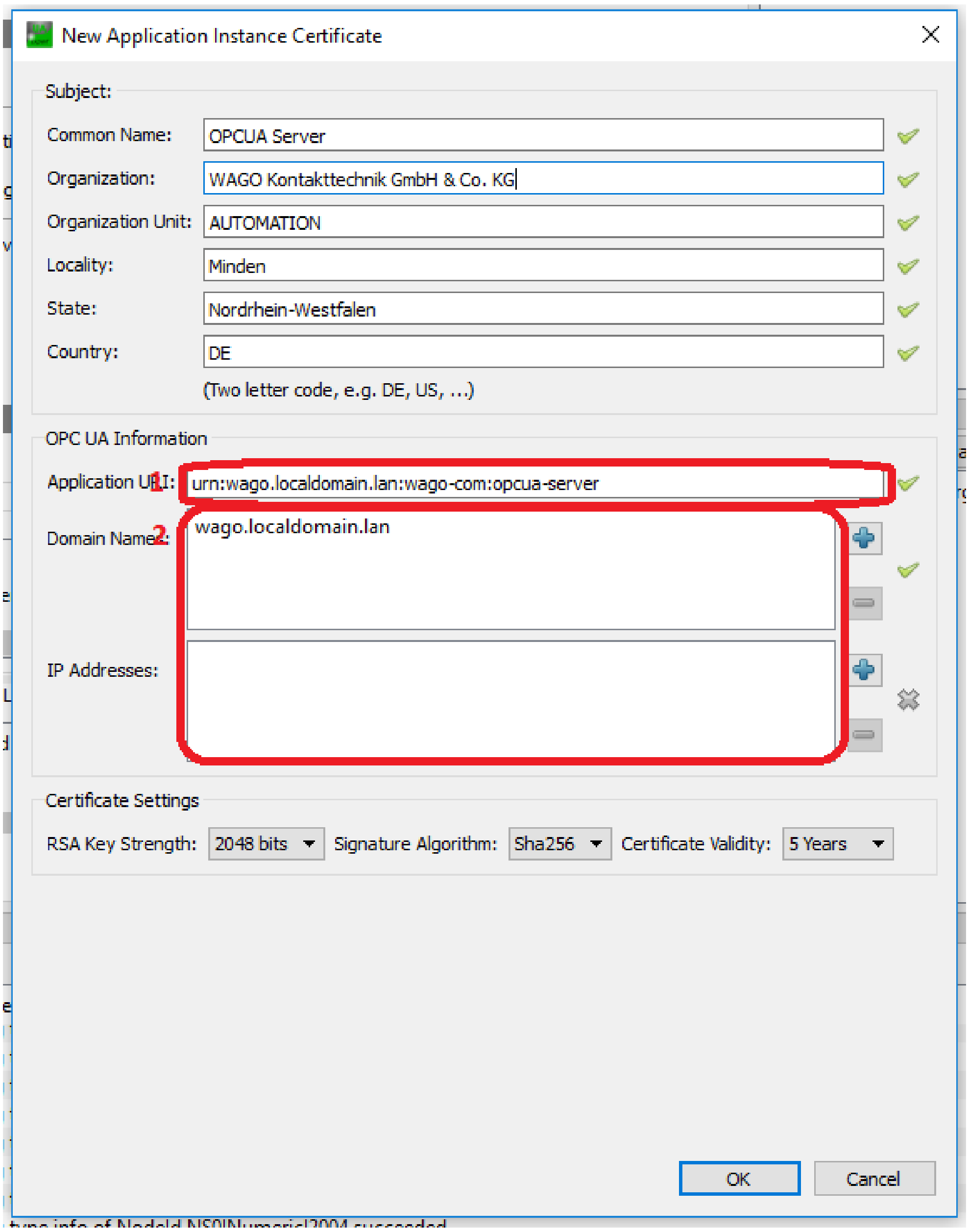
Number	Valid From	Next Update	Organization	OrganizationUnit

Figure 8: GDS Push View

When the “UAExpert” certificate is renewed, it must be created, signed by the server and downloaded to the server.

10. To create a new certificate, click the **[Apply Changes]** button (Fig. “GDS Push View,” Area 1).

→ The following dialog appears:



New Application Instance Certificate

Subject:

Common Name: OPCUA Server ✓
Organization: WAGO Kontakttechnik GmbH & Co. KG ✓
Organization Unit: AUTOMATION ✓
Locality: Minden ✓
State: Nordrhein-Westfalen ✓
Country: DE ✓
(Two letter code, e.g. DE, US, ...)

OPC UA Information

Application URI: urn:wago.localdomain.lan:wago-com:opcua-server ✓
Domain Names: wago.localdomain.lan ✓
IP Addresses:

Certificate Settings

RSA Key Strength: 2048 bits
Signature Algorithm: Sha256
Certificate Validity: 5 Years

Figure 9: Certificate Settings

The presettings displayed in this dialog window were previously read from the current certificate used on the device.

11. Adapt the “Application URI” to the existing environment (Fig. “Certificate Settings,” Area 1). The format required is: “urn:[Hostname].[Domain Name]:wago-com:opcua-server.”

12. Extend the connection information through “Domain Name” or “IP Addresses” (Fig. “Certificate Settings,” Area 2). For example, the connection information is added to the image as host name and domain name. An IP address can also be used.

13. Click **[OK]** to save the settings and close the dialog window.

14. Click the button **[Download]** in the “GDS Push View” tab to load the certificate to the controller (Fig. “GDS Push View,” Area 2).

→ A message window with a prompt appears.

15. Click the button **[No]** to take over the certificate without any changes and close the message window.

→ Another message window with a reminder appears.

16. Click the **[OK]** button to confirm the reminder and close this message window.

17. Click the button **[Apply Changes]** to activate the certificate loaded in the controller (Fig. “GDS Push View,” Area 3).

→ After activation, the current client-server connection is canceled because the certificate currently used on the server no longer matches the certificate used in the connection.

18. In the project tree under “**Project**” > “**Server**,” open the WAGO OPC UA Server context menu with a right click.

19. To disconnect the connection, select the “**Disconnect**” menu item.

20. In the project tree under “**Project**” > “**Server**,” open the WAGO OPC UA Server context menu with a right click.

21. To restore the connection, select the menu item “**Connect**.”

→ If the connection is no longer possible, check the settings (Fig. OPC UA Settings in Web-Based Management”).

→ If the connection is reestablished, the certificate for the current connection is used (Fig. “GDS Push View”; Area 4).

22. Right-click to open the context menu of this certificate entry.

23. Select the menu item “**Trust**.”

→ The certificate is now added to the trusted certificates list.

To allow additional server-client constellations, start a new connection attempt for this constellation.
This attempt fails, since the client certificate is not accepted.

The connection can be added to an accepted server-client constellation after the failed attempt. Continue as described above.

7.2 Adding OPC UA Clients

The section describes the steps needed to add additional clients for the OPC UA Server connection structure.

Prerequisites:

- UAExpert with version >= 1.4.4.
- A PFC100 or PFC200 Controller with a running OPC UA Server
- Certificates for the additional clients

Note

The first startup under the certificate must be completed!
Because a certificate has already been created for this constellation, use the client (e.g., UAExpert) through which the first startup was run to add OPC UA Clients.

Explanation:

There are several ways to add clients.

- A client attempts to connect to the server and is refused. Thus, the certificate is in the unaccepted certificate area. The connection is added as “trusted” via a trusted client.
- A client certificate is loaded to the server via a trusted connection.

Only the process for adding through the two clients is written here.

PC with OPC UA Client to Add

1. Start UAExpert on the client to be added.
2. In the “Project” window, open the “Project/Servers” tree.
3. Right-click on “Server” to open the associated context menu.
4. Select the “Add …” menu item.
5. Under “Configuration Name,” enter a unique name for the server(e.g., “WAGO OPC UA Server”).
6. Select the “Advanced” tab.
7. Enter the connection to the server (e.g., “opc.tcp://172.29.233.206”) in the “Endpoint URL” field in the “Server Information” group.
8. In the “Security Policy” selection field, select the entry “Basic256Sha256” in the “Security Settings” group and in the “Message Security Mode” field, select “Sign & Encrypt.”

9. Select the option “Username/Password” in the “Authentication Settings” group.

10. In the “**Username**” field, enter the user name “root” and enter the password in the “**Password**” field (delivery password: “wago”).

11. Tick the control field “Store” and close the window with **[OK]**.

12. In the “Project” window, open the “Project/Servers” tree.

13. Right-click on “Server” to open the context menu of the server that was just created.

14. Select the menu item “Connect.”

→ A connection to the server cannot yet be established.

PC with Trusted OPC UA Client

15. Start UAExpert on the trusted client.

16. In the “Project” window, open the “Project/Servers” tree.

17. Right-click to open context menu of the desired server.

18. Select the menu item “Connect.”

19. In the “Project” window, open the “Project/Documents” tree.

20. Select the “Add …” menu item.

21. In the “Document Type” group, select the entry “GDS Push View.”

22. Close the window with **[Add]**.

23. Select the desired server from the “Current Server” selection field in the “GDS Push View” tab.

→ In the group “Server Certificate Groups” in the “Trusted” tab, the certificate from the previous connection attempt is displayed as “Untrusted.”

24. Right-click to open the context menu for this certificate.

25. Select the menu item “Trust.”

→ The certificate is now displayed as “Trusted.”

26. In the “Project” window, open the “Project/Servers” tree.

27. Right-click on “Server” to open the context menu of the server that was just created.

28. Select the “Disconnect” menu item.

→ The connection to the server is canceled.

List of Figures

List of Tables

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • D - 32385 Minden
Hansastraße 27 • D - 32423 Minden
Phone: +49 571 887 – 0
Fax: +49 571 887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com