TURCK

Your Global Automation Partner

# TN-UHF-...-OPC-UA
# UHF Reader

Instructions for Use

# Contents

# 1 About these Instructions

These instructions describe the setup, functions and use of the product and help you to operate the product according to its intended purpose. Read these instructions carefully before using the product. This will prevent the risk of personal injury and damage to property. Keep these instructions safe during the service life of the product. If the product is passed on, pass on these instructions as well.

## 1.1 Target groups

These instructions are aimed at qualified personal and must be carefully read by anyone mounting, commissioning, operating, maintaining, dismantling or disposing of the device.

## 1.2 Explanation of symbols

The following symbols are used in these instructions:

| | |
|---|---|
|  | **DANGER**<br>DANGER indicates a hazardous situation with a high level of risk, which, if not avoided, will result in death or serious injury. |
|  | **WARNING**<br>WARNING indicates a hazardous situation with a medium level of risk, which, if not avoided, will result in death or serious injury. |
|  | **CAUTION**<br>CAUTION indicates a hazardous situation with a medium level of risk, which, if not avoided, will result in moderate or minor injury. |
|  | **NOTICE**<br>CAUTION indicates a situation which, if not avoided, may cause damage to property. |
|  | **NOTE**<br>NOTE indicates tips, recommendations and important information about special action steps and issues. The notes simplify your work and help you to avoid additional work. |
| ▶ | **MANDATORY ACTION**<br>This symbol denotes actions that the user must carry out. |
| ⇨ | **RESULT OF ACTION**<br>This symbol denotes the relevant results of an action. |

## 1.3 Other documents

Besides this document the following material can be found on the Internet at www.turck.com:

- Data sheet
- Approvals
- Configuration manual

## 1.4 Naming convention

Read/write devices in the HF are called “read/write heads” and “readers” in the UHF area. “Tag”, “transponder” and “mobile data memory” are common synonyms for “data carriers”.

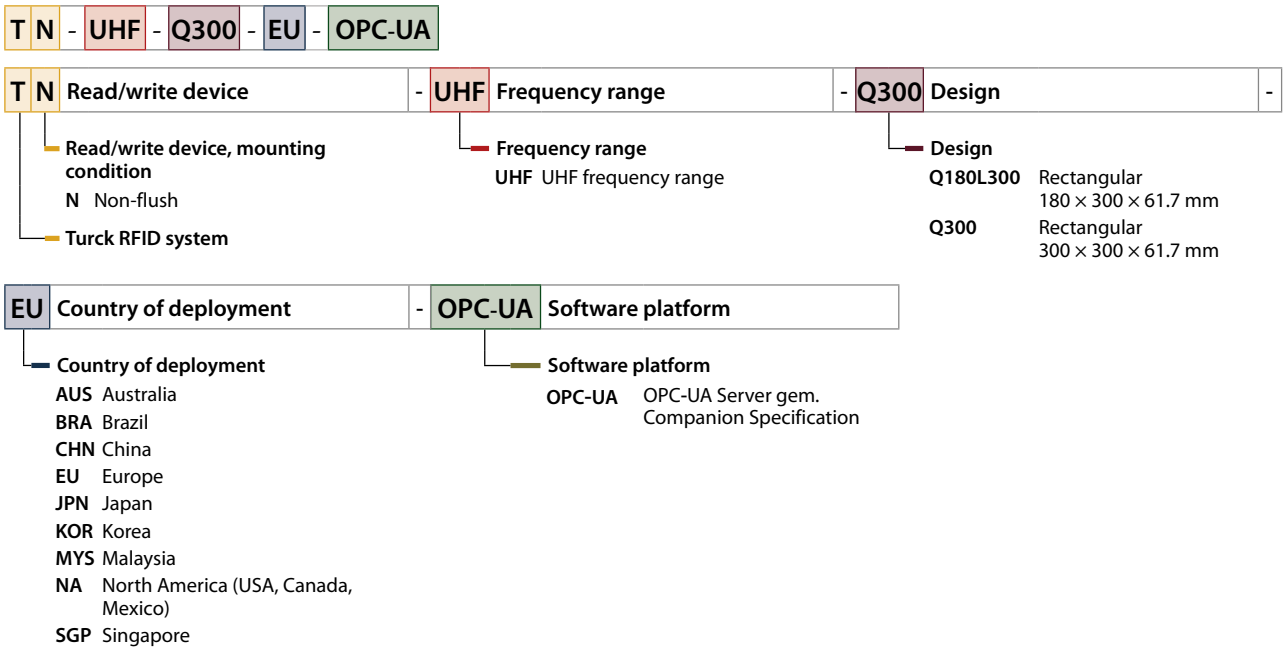
## 1.5 Feedback about these instructions

We make every effort to ensure that these instructions are as informative and as clear as possible. If you have any suggestions for improving the design or if some information is missing in the document, please send your suggestions to techdoc@turck.com.

# 2 Notes on the product

## 2.1 Product identification

These instructions apply to the following UHF readers:




## 2.2 Scope of delivery

The delivery consists of the following:

- UHF reader
- Wall bracket (metal rail)
- Quick Start Guide

## 2.3 TURCK service

TURCK supports you in your projects — from the initial analysis right through to the commissioning of your application. The TURCK product database at www.turck.com offers you several software tools for programming, configuring or commissioning, as well as data sheets and CAD files in many export formats.

For the contact details of our branches worldwide, please see page [▷ 80].

# 3 For your safety

The product is designed according to state of the art technology. Residual hazards, however, still exist. Observe the following safety instructions and warnings in order to prevent danger to persons and property. TURCK accepts no liability for damage caused by failure to observe these safety instructions.

## 3.1 Intended use

The readers with an integrated RFID interface are used for contactless data exchange with the RFID tags in the TURCK UHF RFID system. The following table shows the operating frequency of the devices:

| Type designation | Operating frequency | Region |
|---|---|---|
| TN-UHF-…-AUS-OPC-UA | 920…926 MHz | Australia, New Zealand |
| TN-UHF-…-BRA-OPC-UA | 915…928 MHz | Brazil |
| TN-UHF-…-CHN-OPC-UA | 920.5…924.5 MHz | China and Thailand |
| TN-UHF-…-EU-OPC-UA | 865.6…867.6 MHz | Europe, Turkey, India |
| TN-UHF-…-JPN-OPC-UA | 916.7…920.9 MHz | Japan |
| TN-UHF-…-KOR-OPC-UA | 917…920.8 MHz | Korea |
| TN-UHF-…-MYS-OPC-UA | 919…923 MHz | Malaysia |
| TN-UHF-…-NA-OPC-UA | 902…928 MHz | North America (USA, Canada, Mexico) |
| TN-UHF-…-SGP-OPC-UA | 920…925 MHz | Singapore |

These devices may only be started up under the following conditions:

- The particular frequency range is permissible for the use of UHF-RFID.
- The operating frequency range of the devices is compliant with the permissible UHF RFID range of the region.
- A valid certification and/or approval is available for the region of use.

The module can communicate with third-party systems such as ERP systems via an integrated OPC UA server compliant with the AutoID Companion Specification.

Four configurable digital channels are also provided for connecting digital sensors and actuators.

The device must only be used as described in these instructions. Any other use is not in accordance with the intended use. TURCK accepts no liability for any resulting damage.

## 3.2 General safety notes

- The device meets the EMC requirements for the industrial areas. When used in residential areas, take measures to prevent radio frequency interference.
- The device must only be fitted, installed, operated, parameterized and maintained by trained and qualified personnel.
- Only use the device in compliance with the applicable national and international regulations, standards and laws.
- Any extended stay within the area of radiation of UHF readers may be harmful to health. Observe a minimum distance of > 0.35 m from the actively radiating surface of the UHF reader.
- The radiation of the UHF readers may have an adverse effect on the operation of electrically controlled medical equipment. Keep an additional distance from active radiation sources up to the maximum transmission distance.
- Change the default password of the integrated web server after the first login. TURCK recommends the use of a secure password.

## 3.3 Notes on EU Directive 2014/53/EU (RED Directive)

For safe and proper use of the device, ensure the following physical and logical safety measures in accordance with DIN EN 18031-1 in the environment:

- Access control: Enable access to security-related data and settings only to authorized persons, devices and services. Especially protect cryptographic keys in the device.
- Authentication: Manage access to security-related data and settings through appropriate authentication mechanisms. This also includes the regular verification and adjustment of passwords and other authentication methods.
- Firmware management: Regularly check the availability of new firmware versions at **www.turck.com** and carry out updates promptly. Check the integrity of firmware updates by comparing them with the hash values provided on the TURCK website.
- Data protection and communication: Protect the data stored in the device for integrity and confidentiality. Secure communication with the device against manipulation, unauthorized access and listening in.
- Attack protection: Take measures to prevent successful replay, denial of service or brute force attacks.
- Vulnerability management: Ensure that known vulnerabilities cannot be exploited.
- Interface control: Only send valid and authorized data to the device interfaces.

# 4 Product Description

The devices are designed with an aluminum housing and degree of protection IP67. The active face is made out of plastic. Devices are available with an integrated antenna (Q300) or for connecting external antennas (Q180). Both device variants are suitable for connecting up to four external passive UHF RFID antennas.

The terminals for the Ethernet and for digital I/Os are M12 sockets. The device has an M12 plug connector for connecting the power supply. Terminals are provided for up to four external antennas.

## 4.1 Device overview

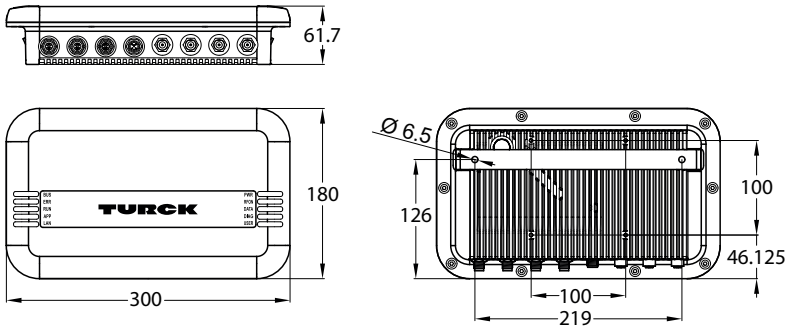



Fig. 1: Dimensions – TN-UHF-Q180L300…

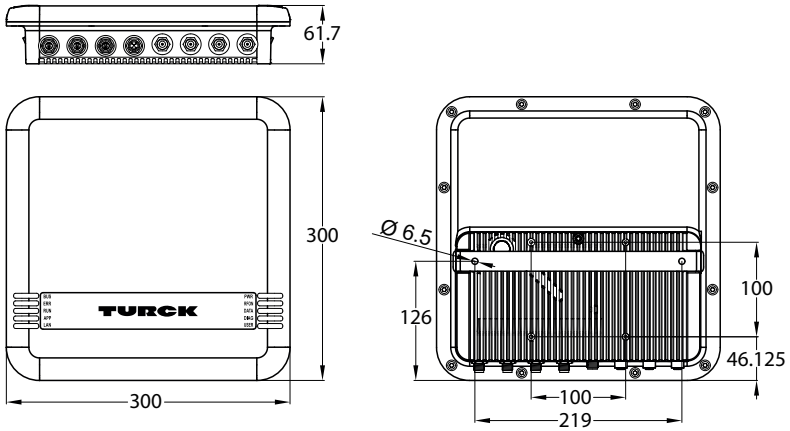



Fig. 2: Dimensions – TN-UHF-Q300…

### 4.1.1 Indication elements

The device has the following LED indicators:

- Power supply
- Group and bus errors
- Status
- Diagnostics

An acoustic signal can also be set using software tools.

## 4.2 Properties and features

- Integrated OPC UA server standardized in accordance with AutoID Companion Specification
- Calling of data via OPC UA clients
- Universal interface offers interoperability
- Supports security mechanisms and authentication
- Rectangular, height 180 or 300 mm
- Active front face, UV-resistant
- Four terminals for passive UHF RFID antennas
- Four configurable digital channels, which can be configured as PNP inputs and/or 0.5-A outputs
- 2 W (ERP) maximum output power
- Close-to-control integration in PLC systems without the use of a special function module
- Integrated web server
- LEDs and diagnostics

## 4.3 Operating principle

The readers are used for contactless data exchange with tags. For this the controller sends commands and data via the interface to the reader and receives the corresponding response data from the reader. The reading of the IDs of all RFID tags in the read area and the writing of an RFID tag with a specific production date are examples of typical commands. To communicate with the tag, the data of the reader is coded and transferred via an electromagnetic field, which at the same time supplies the tags with power.

A reader contains a transmitter and a receiver, an interface to the interface module and a coupling element (coil and dipole antenna) for communicating with the tag. Electromagnetic wave propagation is used for the transmission between reader and tag on devices for the UHF range.

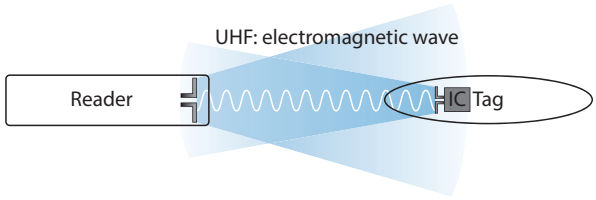



Fig. 3: Operating principle of UHF-RFID

The antenna of the reader generates electromagnetic waves. This produces a transmission window as a so-called air interface in which the data exchange with the tag takes place. The size of the transmission window depends on the combination of readers and tags, as well as on the relevant environmental conditions.

Each reader can communicate with a number of tags. This requires the reader and the tag to operate in the same frequency range. Depending on their power and the frequency in use, the devices have a range of a few millimeters up to several meters. The specified maximum distance between the read/write heads represents values measured under laboratory conditions, free from any influences caused by surrounding materials. Attainable distances may vary due to component tolerances, mounting conditions, ambient conditions and influences caused by surrounding materials (especially metal and liquids).

The OPC UA interface is used to connect the reader to the higher-level system via Ethernet. Up to four additional antennas can be connected via the RFID interfaces. During operation, the process data is exchanged between the higher-level system and RFID system. The OPC UA server integrated into the reader communicates with the OPC UA client of the higher-level system to do this.

## 4.4 Functions and operating modes

### 4.4.1 Operating frequency

The TURCK UHF system operates at country-specific operating frequencies between the tags and the readers. These national operating frequencies for UHF are the frequency ranges that are individually specified by the national regulation bodies.

For example, the operating frequencies of the devices in the UHF band are 865.6…867.6 MHz for Europe and 902…928 MHZ for the USA. The UHF readers can only be used in the particular designated regions and must not be commissioned outside these regions. Since UHF tags do not emit their own radio waves, they may be used worldwide.

In order to achieve the biggest possible communication range, TURCK offers tags which are optimally tuned to country-specific frequency bands. Alternatively, broadband multi-area tags are also available for international use.

The different TURCK readers support the following operating frequencies:

- 920…926 MHz (e.g. Australia and New Zealand)
- 915…928 MHz (e.g. Brazil)
- 920.5…924.5 MHz (e.g. China and Thailand)
- 865.6…867.6 MHz (e.g. Europe, Türkiye, India)
- 916.7…920.9 MHz (e.g. Japan)
- 917…920.8 MHz (e.g. Korea)
- 919…923 MHz (e.g. Malaysia)
- 902…928 MHz (e.g. USA, Canada, Mexico)
- 920…925 MHz (e.g. Singapore)

All the country-specific details concerning UHF, such as frequency band, power supply, and any national regulations are available at:
**https://www.gs1.org/docs/epc/uhf_regulations.pdf**

For more detailed information please contact the regulation authorities of the country where you wish to use the UHF RFID system.

HF RFID systems can be operated in parallel with UHF RFID systems in a single system.

### 4.4.2 Compatible OPC UA clients

The device is compatible with all OPC UA clients that support the method execution and data model according to the AutoID Companion Specification. For example, the following OPC UA clients can be used:

- UAExpert – Unified Automation
- dataFeed OPC UA Client – Softing
- OPC Router – Inray

It is also possible to capture RFID data with any OPC UA client by setting variables (ScanStart and Read), without the client having to support a method execution.

A specific OPC UA client can be programmed with the OPC UA Stack of the OPC Foundation. It is also possible to use the OPC UA SDKs of other manufacturers. TURCK recommends the use of the ".NET based OPC UA client/server SDK". The OPC Foundation provides an overview of the available clients.

### 4.4.3 Authentication and encryption

For secure communication, the OPC UA interface offers authentication by the signing of certificates and the encryption of messages on the transport level. The OPC UA server of the device makes it possible to perform authentication and authorization on the application level by means of user levels and passwords.

### 4.4.4 RFID commands (methods)

The RFID functionality is defined in accordance with the AutoID Companion Specification. A complete description of the methods is provided in the specification. The methods are also described in the "Setting" chapter.

The device can perform the following methods and functions:

- Scan
- ScanStart
- ScanStop
- ReadTag
- WriteTag
- KillTag
- LockTag
- SetTagPassword
- WriteTagID

# 5 Installing

The device is designed for mounting on a bracket based on the VESA 100 × 100 standard. The device is provided with four M4 threaded holes spaced 100 mm apart (horizontally and vertically). The maximum length of the screws is 8 mm plus the thickness of the VESA bracket. The devices can be mounted in any position.

- ▶ Fasten the device with four M4 screws to a bracket in accordance with VESA 100 × 100.

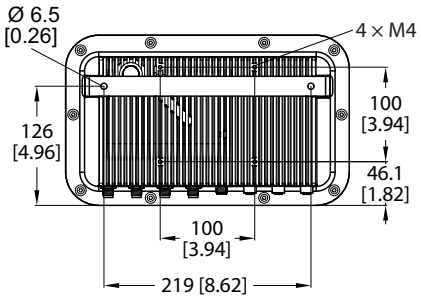



Fig. 4: Rear view – TN-UHF-Q180…

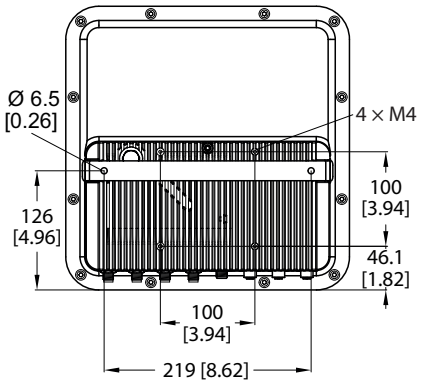



Fig. 5: Rear view – TN-UHF-Q300…

# 6 Connecting

## 6.1 Connecting devices to Ethernet

The device has a 4-pin M12 female connector for connection to an Ethernet system.

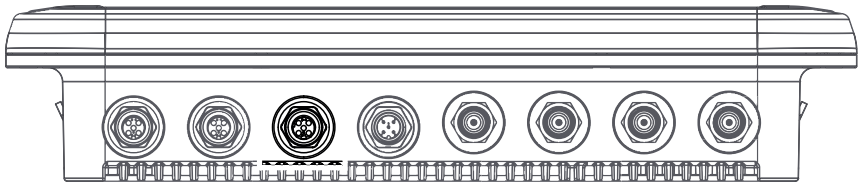


Fig. 6: M12 Ethernet connector

- ▶ Connect the device to Ethernet in accordance with the pin assignment below (max. tightening torque: 0.8 Nm).

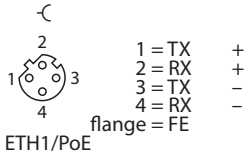



Fig. 7: Pin assignment for Ethernet connections

**NOTE**
With PoE, the supply voltage is transmitted via PoE Mode A with 4-wire cables.
The use of PoE and 24 VDC simultaneously is not supported.

## 6.2 Connecting the power supply

The device is provided with a 5-pin M12 plug connectors for connecting the power supply.

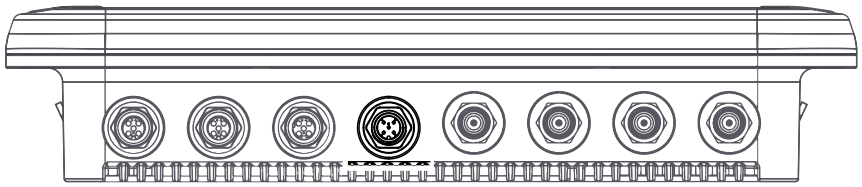


Fig. 8: M12 plug connector for connecting the power supply

- ▶ Connect the device to the power supply as per the following pin assignment (max. tightening torque 0.8 Nm).

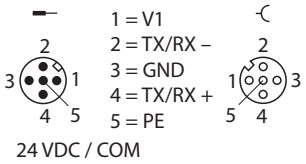



Fig. 9: Pin assignment of the power supply terminals

## 6.3 Connecting digital sensors and actuators

The device has two 5-pin M12 plug connectors for connecting digital sensors and actuators.

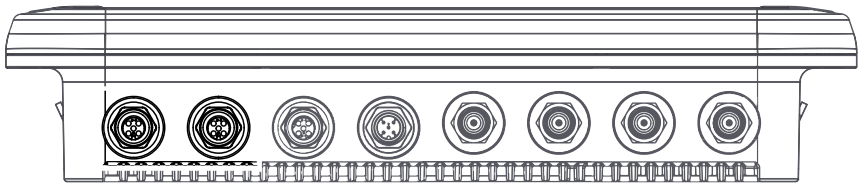


Fig. 10: M12 plug connectors for connecting digital sensors and actuators

**NOTE**
When operating via PoE (Power over Ethernet) the digital channels cannot be used as outputs.

- Connect sensors and actuators to the device as per the following pin assignment (max. tightening torque 0.8 Nm).

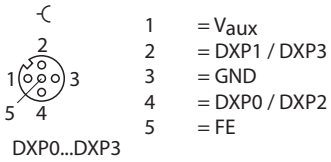



Fig. 11: Connections for digital sensors and actuators – pin assignment

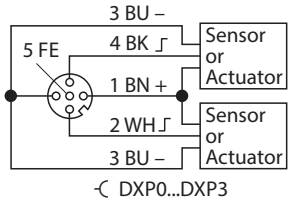



Fig. 12: Connections for digital sensors and actuators – wiring diagram

## 6.4 Connecting external antennas

The device is provided with four RP-TNC sockets for connecting up to four external antennas. The input impedance is 50 Ω.

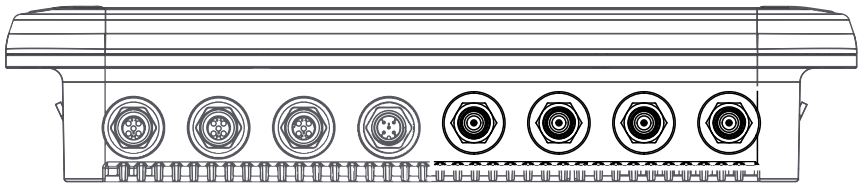


Fig. 13: RP-TNC sockets for connecting external antennas

- ▶ Connect external antennas with an RP-TNC antenna cable to the device (max. tightening torque 0.8 Nm).

# 7 Commissioning

## 7.1 Parameterizing the reader using the web server

The integrated web server can be used to set the devices and send commands to the devices. In order to be able to open the web server with a PC, the device and the PC must be in the same IP network.

### 7.1.1 Opening the web server

The web server can be opened from a web browser or from the TURCK Automation Suite (TAS). Accessing the web server via TAS is described in the section entitled "Adjusting network settings."

The device is factory set to IP address 192.168.1.254. To open the web server via a web browser, enter **http://192.168.1.254** in the address bar of the web browser.

### 7.1.2 Editing settings in the web server

A login is required to edit settings via the web server. The default password is "password".

**NOTE**
TURCK recommends changing the password after the first login for security reasons.

- Open the device's web server.
- Enter **Username** and **Password**.
- Click **Login**

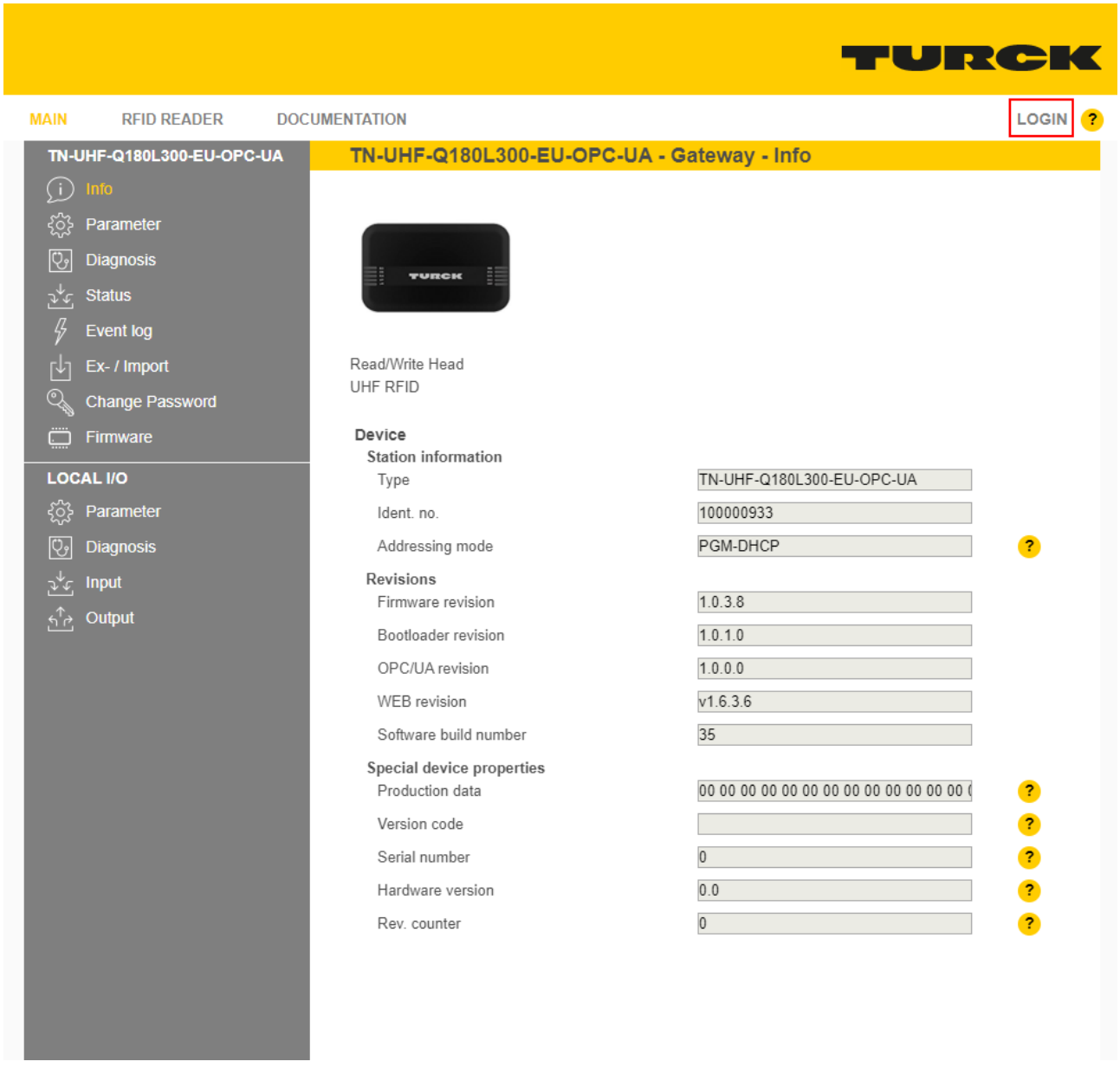



Fig. 14: Web server — login

▶ Change the password after the first login.

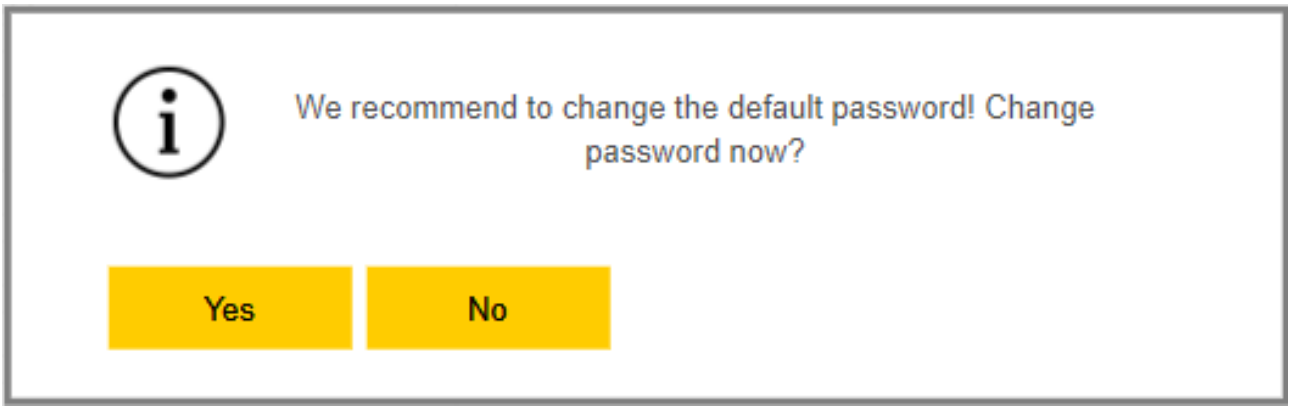



Fig. 15: Web server — password change dialog

⇨ The start page is displayed with the device information after the login.

▶ Click **RFID READER** to display and set the device parameters.

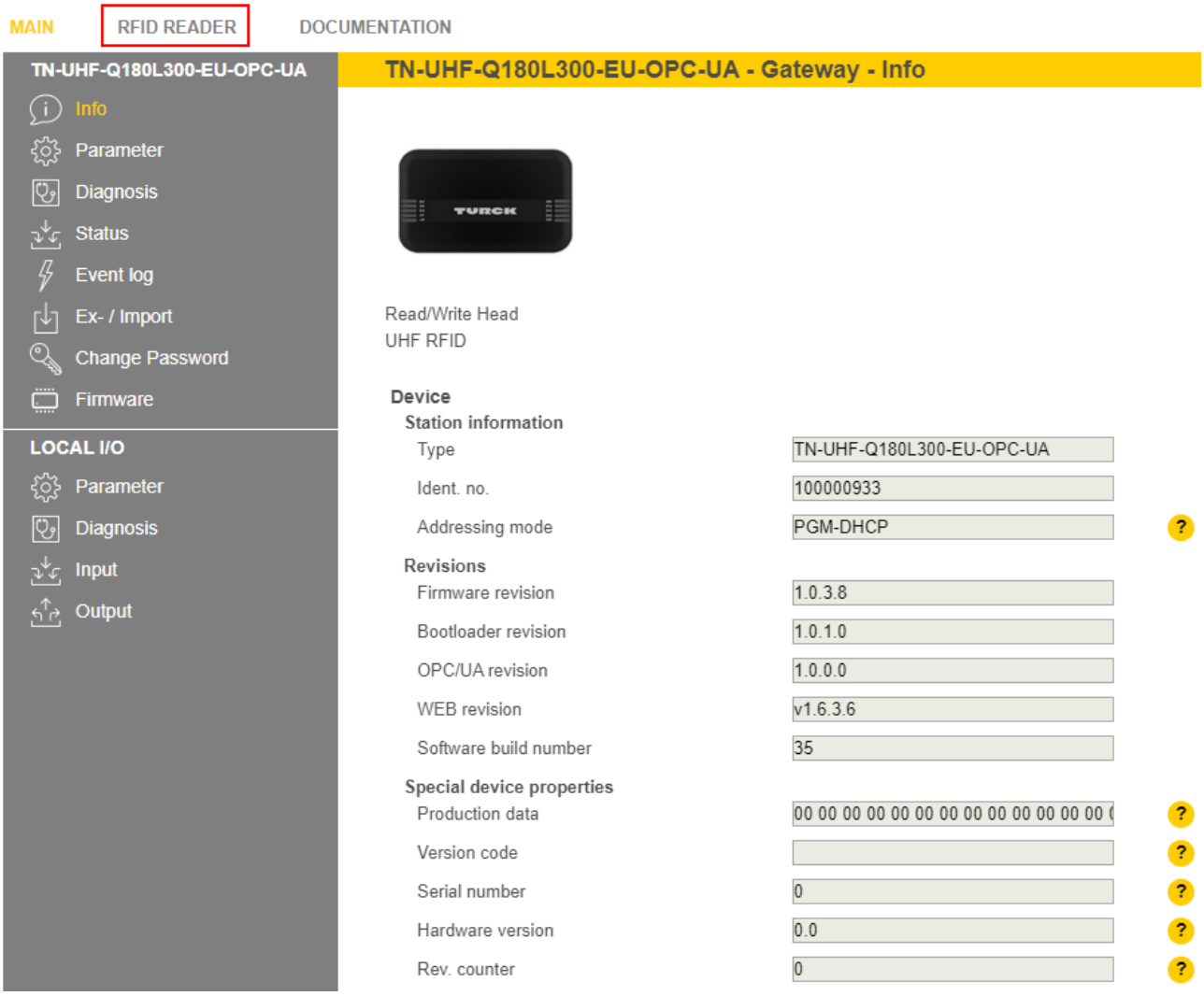



Fig. 16: Web server — home page

▶ Click **Parameter** in the navigation bar on the left of the screen.

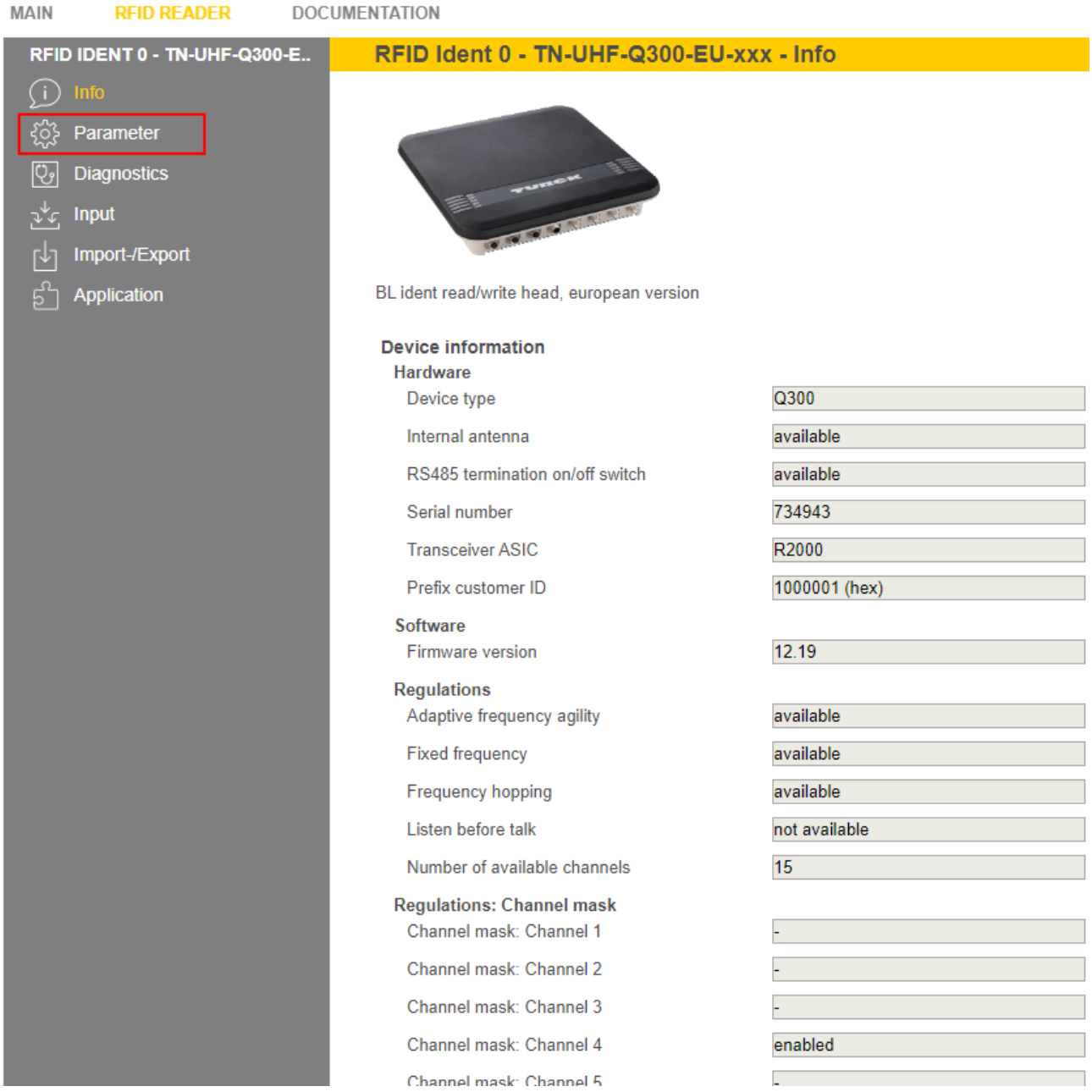



Fig. 17: Web server — RFID Reader — Info

⇨ All parameters of the device are displayed.

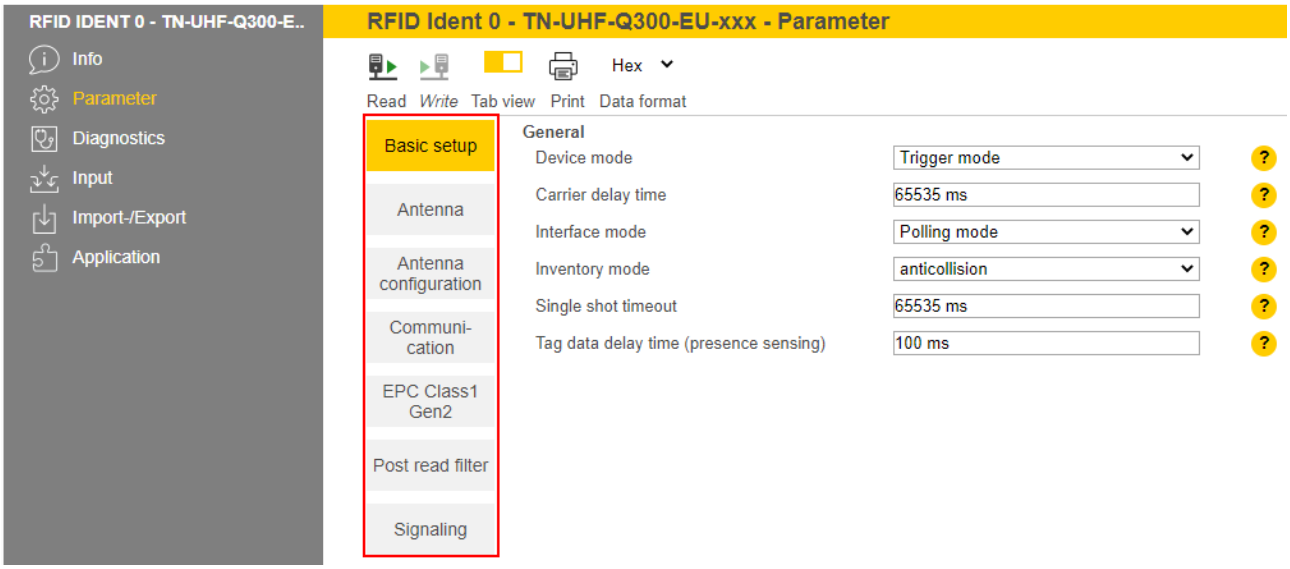



Fig. 18: Web server — RFID Reader — Parameter

The following setup windows can be called up:

- Basic setup
- Antenna
- Antenna configuration
- Communication
- EPC Class1 Gen2
- Post read filter
- Signaling

▶ Set the parameters: Click **Write**.

**NOTE**
While a parameter is being set, the ERR LED lights up red and automatically turns green.

## 7.2 Testing the reader using the web server

The **Application** function enables the devices to be tested with the web server.

▶ Click **RFID READER** → **Application**

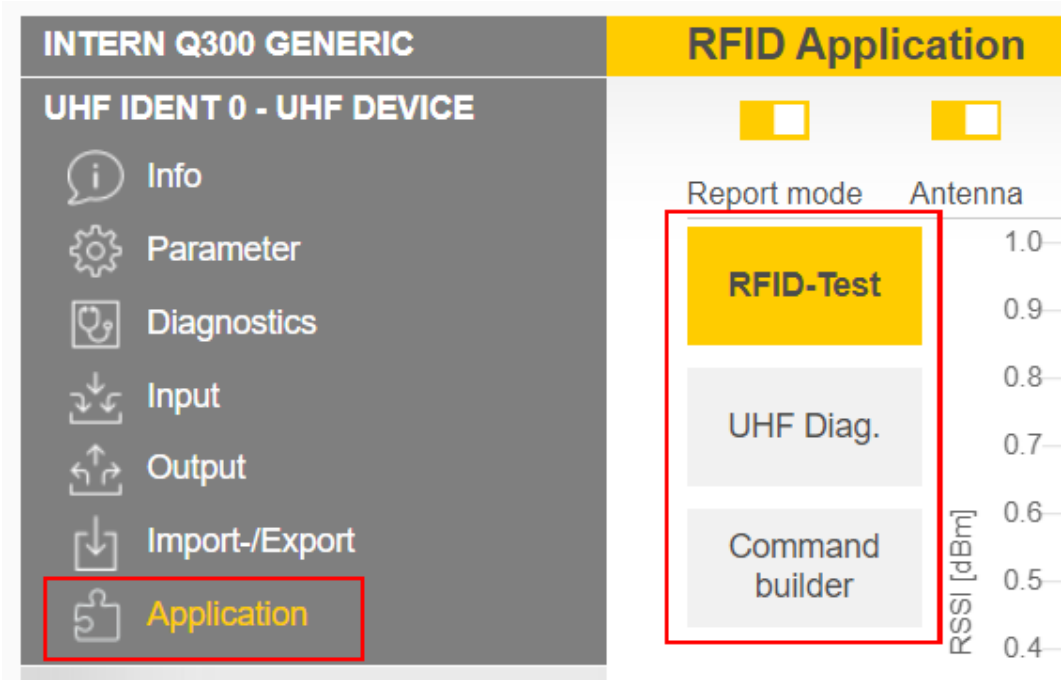



Fig. 19: Web server — RFID Application

The RFID test, the UHF diagnostics and the command builder are provided in the application area:

- RFID-Test: If the trigger is set to ON, the RF field is activated and tags can be read.
- UHF Diag: The diagrams show the interference frequencies of all channels used.
- Command builder: Use of the command builder is reserved for TURCK Support and is not designed for setting device parameters or device operation.

**RFID-Test** allows EPC information from tags to be displayed and read out in single-tag and multi-tag mode. The received RSSI values are displayed as a curve in relation to time.

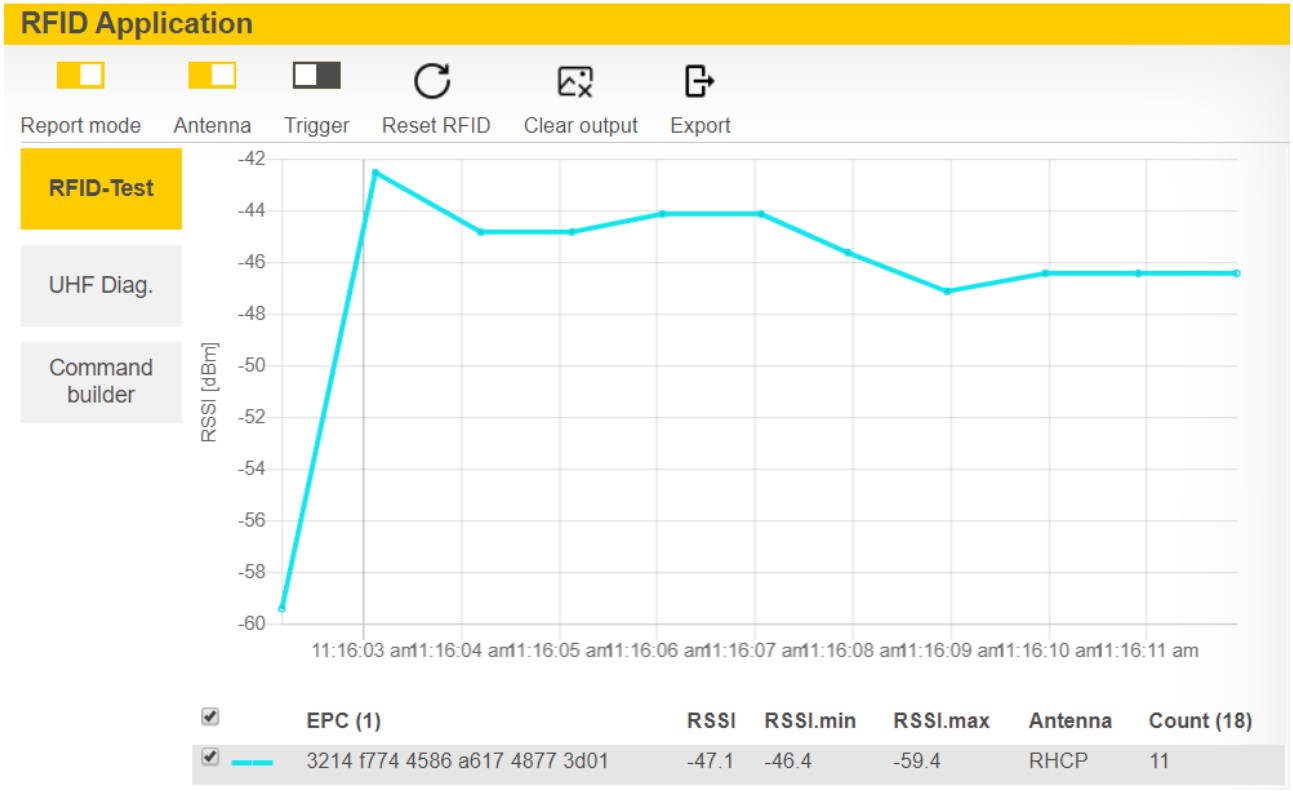



Fig. 20: Example of RFID test: Record of a tag with the received RSSI values over time and the number of read operations

The **UHF diagnostics** display the current power level being received by the reader per channel.

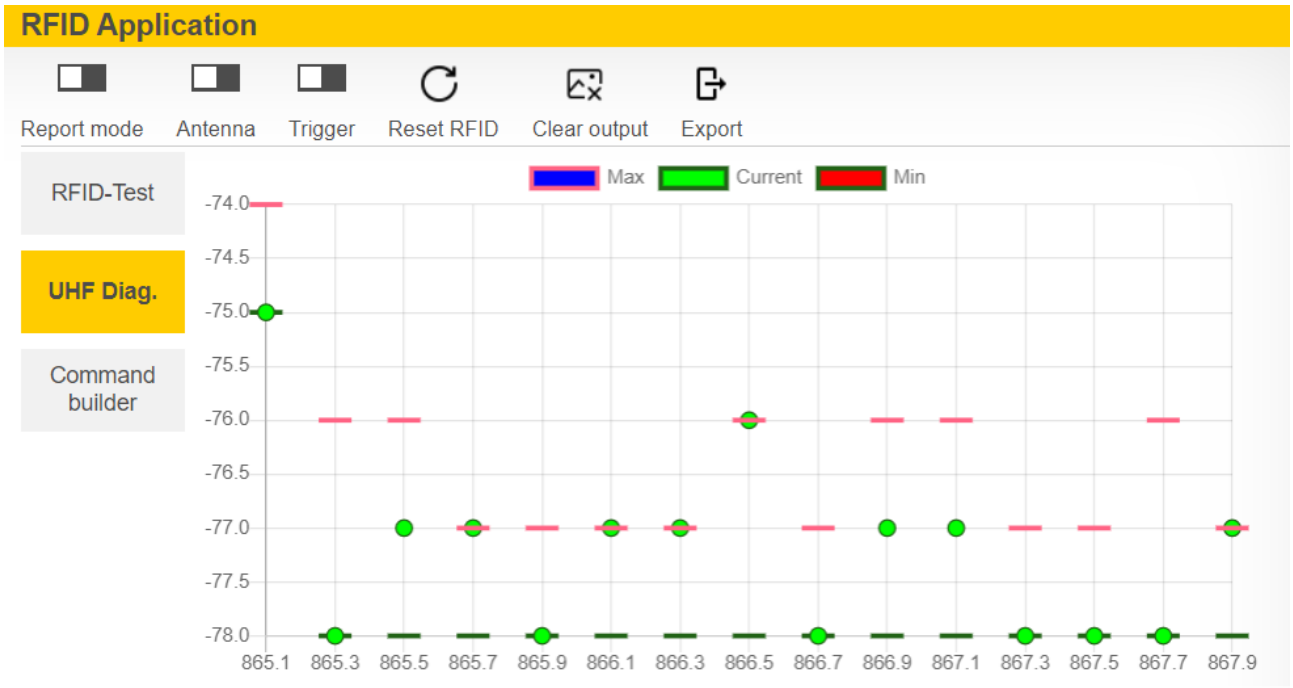



Fig. 21: Example of UHF diagnostics: Received power level per channel

## 7.3 Adjusting network settings

### 7.3.1 Adjusting network settings via TAS (TURCK Automation Suite)

In the delivery state the device has the IP address 192.168.1.254. The IP address can be set via TAS (TURCK Automation Suite). TAS is available free of charge at www.turck.com.

- ▶ Connect the device to the PC via the Ethernet interface.
- ▶ Open TAS.
- ▶ Click **Scan network**.

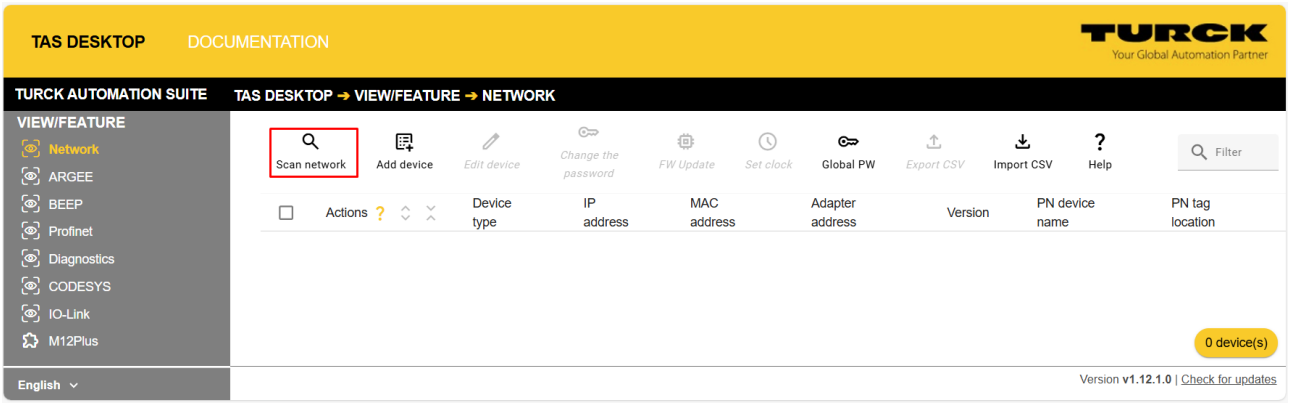



Fig. 22: Home screen in TAS

⇨ TAS shows the connected devices.

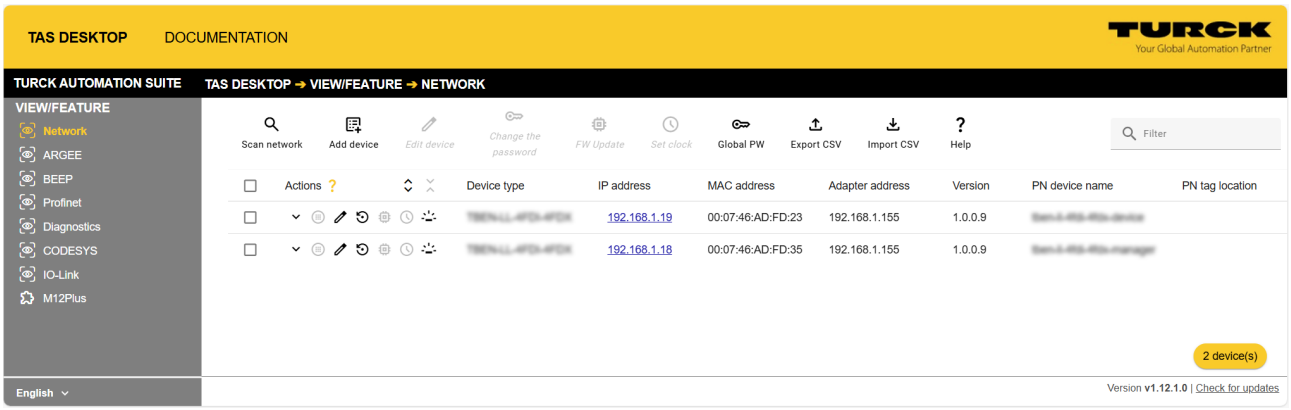



Fig. 23: Found devices in TAS

- ▶ Select the relevant device (check box).
- ▶ Click **Edit device**.

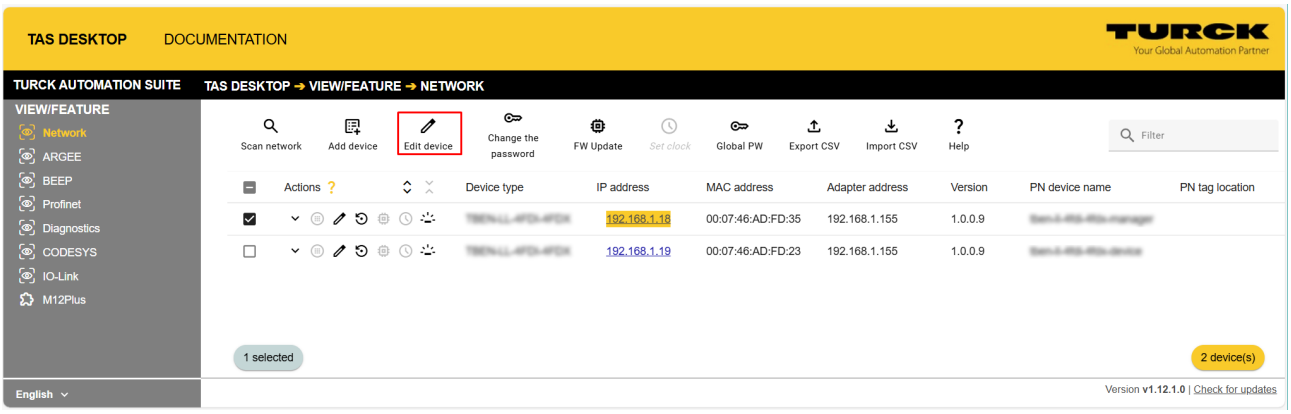



Fig. 24: Selecting the device in TAS

**NOTE**
By clicking on the IP address of the device, the configuration view of the device can be opened either in TAS or on the device website.

- ▶ Enter the device password and click **Login** The default password is "password".
  Note: TURCK recommends changing the password after the first login for security reasons.

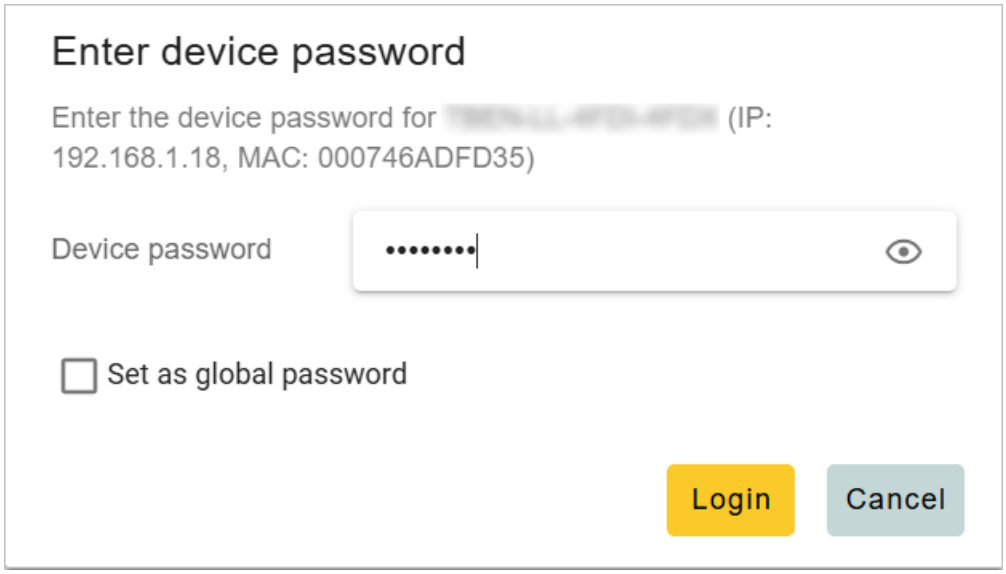



Fig. 25: Entering the device password

- Change the PN device name, IP address and, if necessary, the default gateway, subnet mask and PN tag location.
- Save changes by clicking on **Apply** .

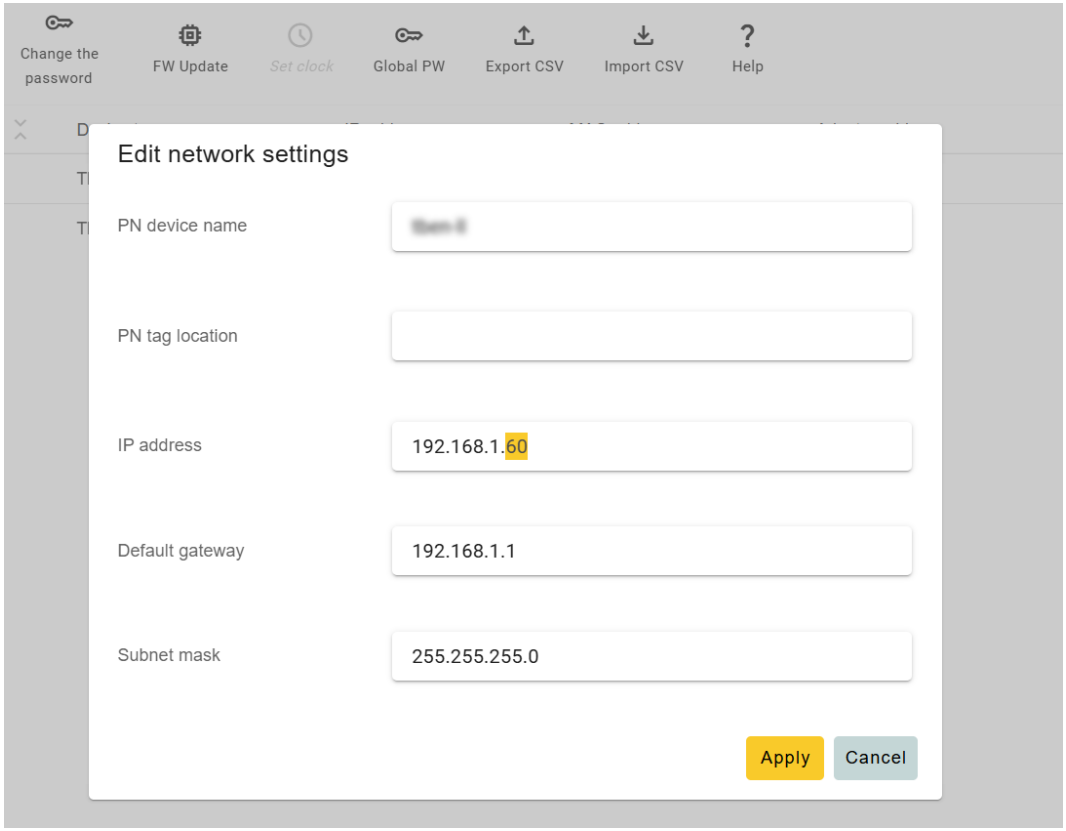



Fig. 26: Changing network settings in TAS

### 7.3.2 Adjusting network settings via the web server

**NOTE**
The device must be in PGM mode in order to set the IP address via the web server.

- Open the web server.
- Log into the device as administrator.
- Click **Parameter → Network**.
- Change the IP address and if necessary also the subnet mask and default gateway.
- Write the new IP address, subnet mask and default gateway via **SET NETWORK CONFIGURATION** to the device.

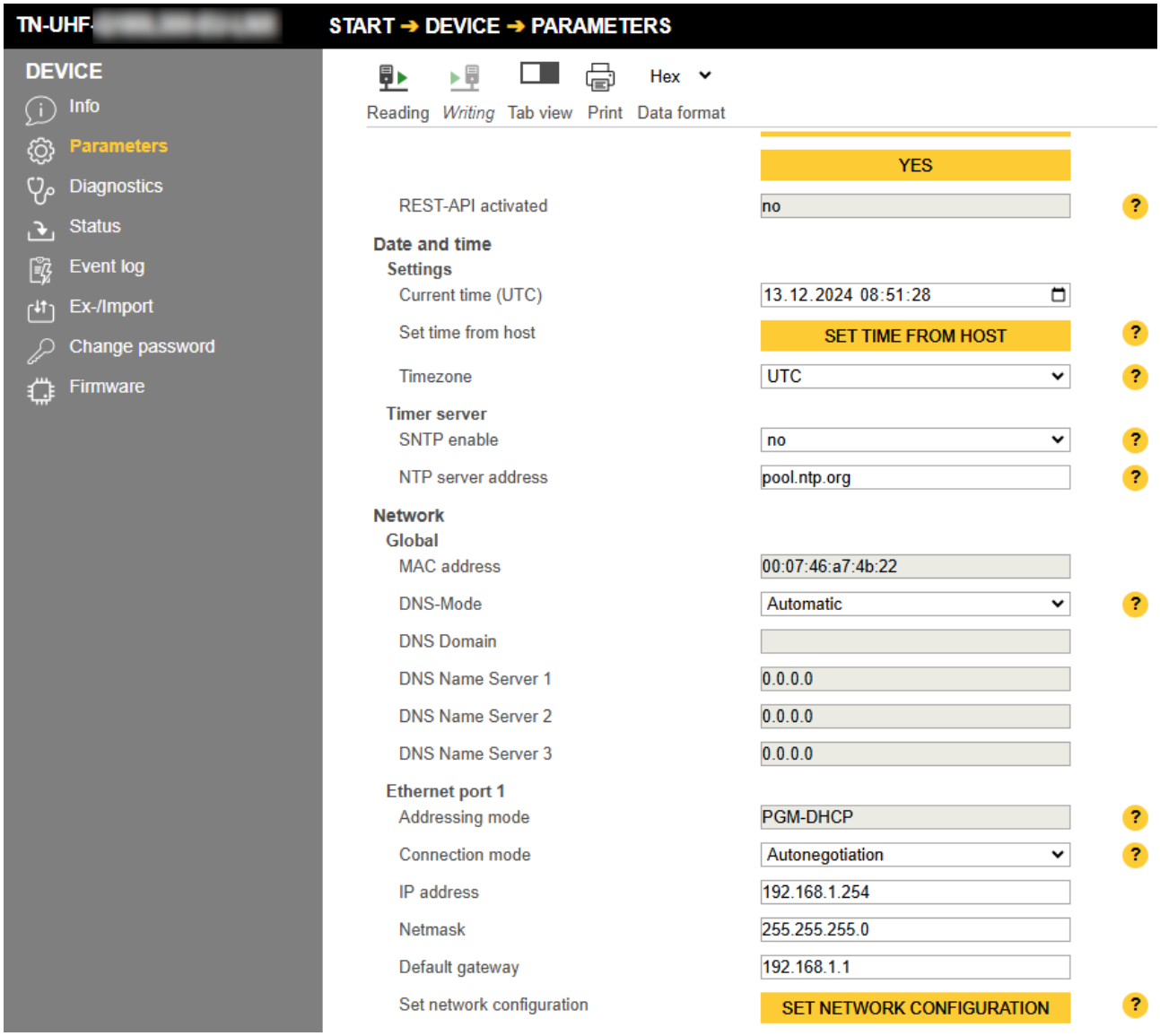


Fig. 27: Adjusting network settings via the web server

## 7.4 Preparing the device for commissioning via the web server

**NOTE**
The web server always displays all setting options. All values are shown as decimal values.

The integrated web server can be used to set the device and send commands to the device. In order to be able to open the web server with a PC, the device and the PC must be in the same IP network.

### 7.4.1 Opening the web server and editing the settings

The web server can be opened from a web browser or from the TURCK Automation Suite (TAS). Accessing the web server via TAS is described in the section entitled "Adjusting network settings."

Status information and network settings are displayed on the home page.

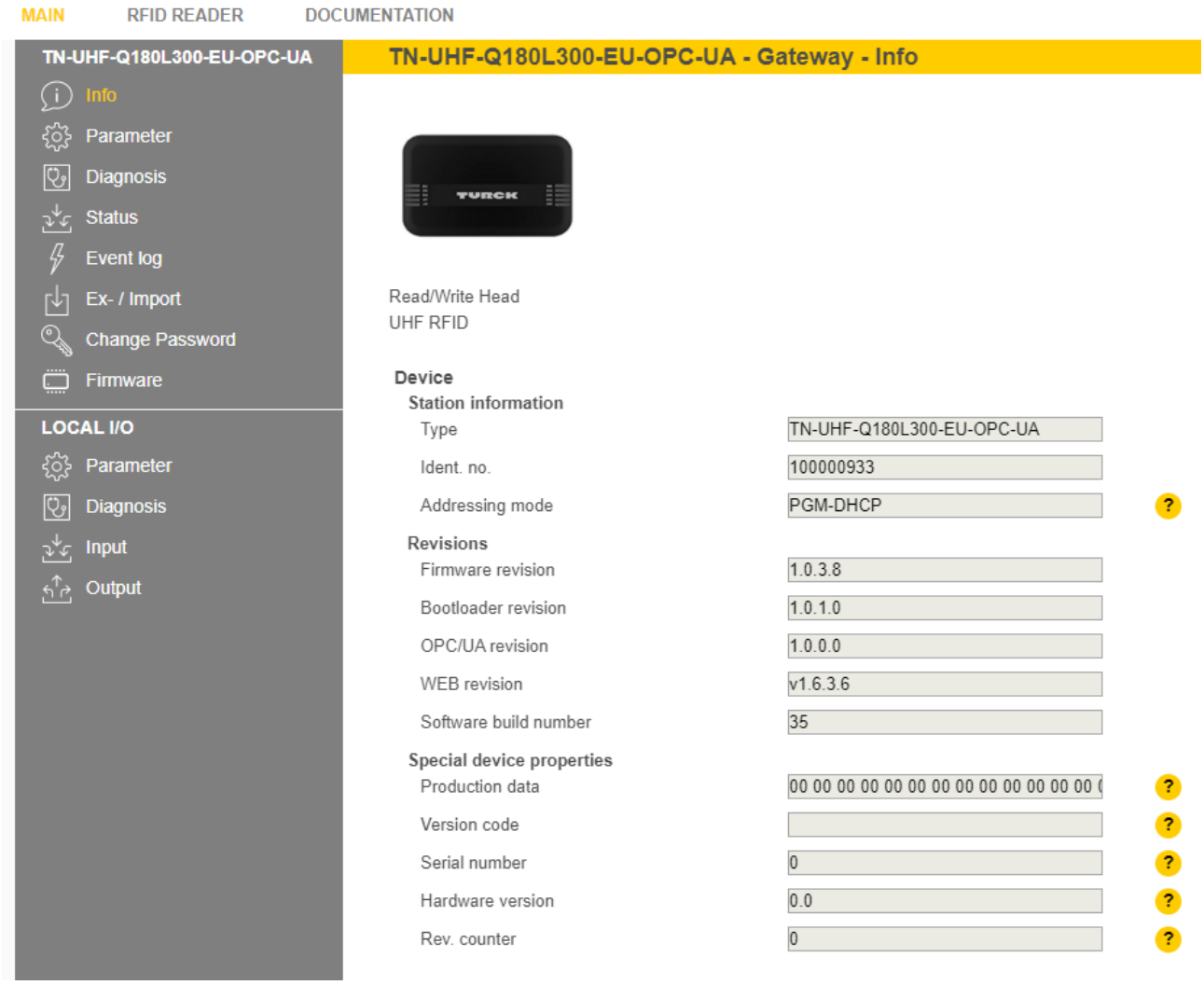



Fig. 28: Web server — home page

A login is required to edit settings via the web server. The default password is "password".

**NOTE**
TURCK recommends changing the password after the first login for security reasons.

- Open the device's web server.
- Enter **Username** and **Password**.
- Click **Login**

Write access to the parameter data of the module is possible after the login.

To access OPC UA-specific parameters, enter the OPC UA root password. The default password is "Turck."

**NOTICE**
Insufficiently secured devices
**Unauthorized access to sensitive data**
- Change the password after the first login. TURCK recommends the use of a secure password.

- **Parameter** → **OPC UA**: Enter the password in the **OPC UA root password** field.
- Click **AUTHENTICATE**.

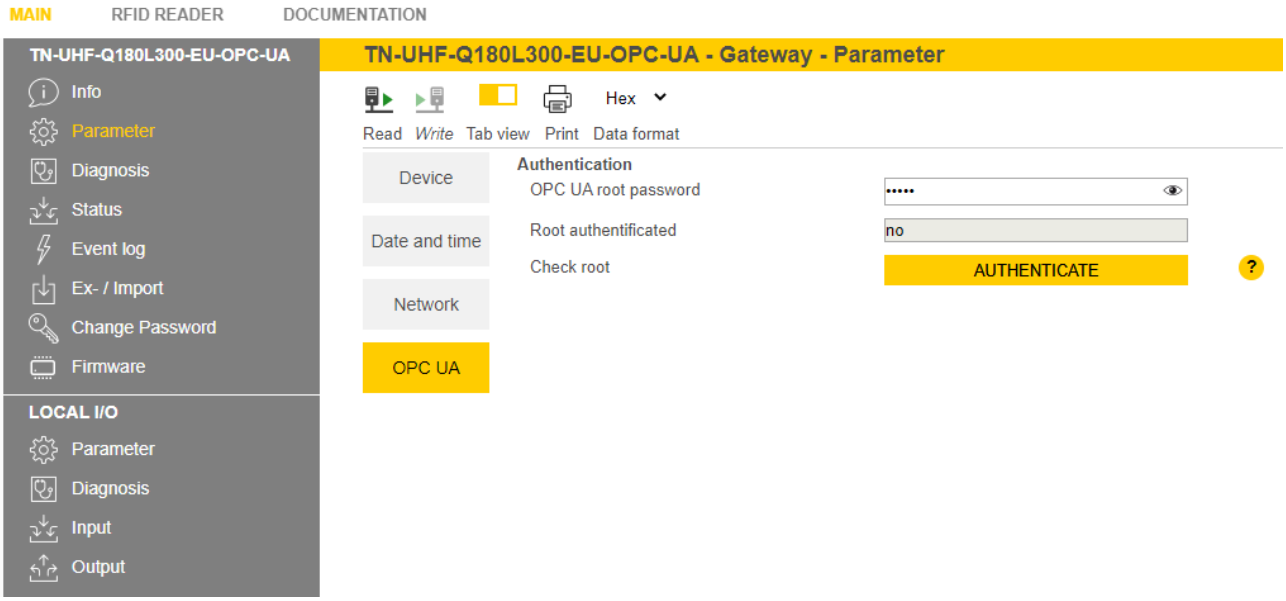



Fig. 29: Entering the OPC UA root password

➪ The parameters for the OPC UA-specific configuration are shown.

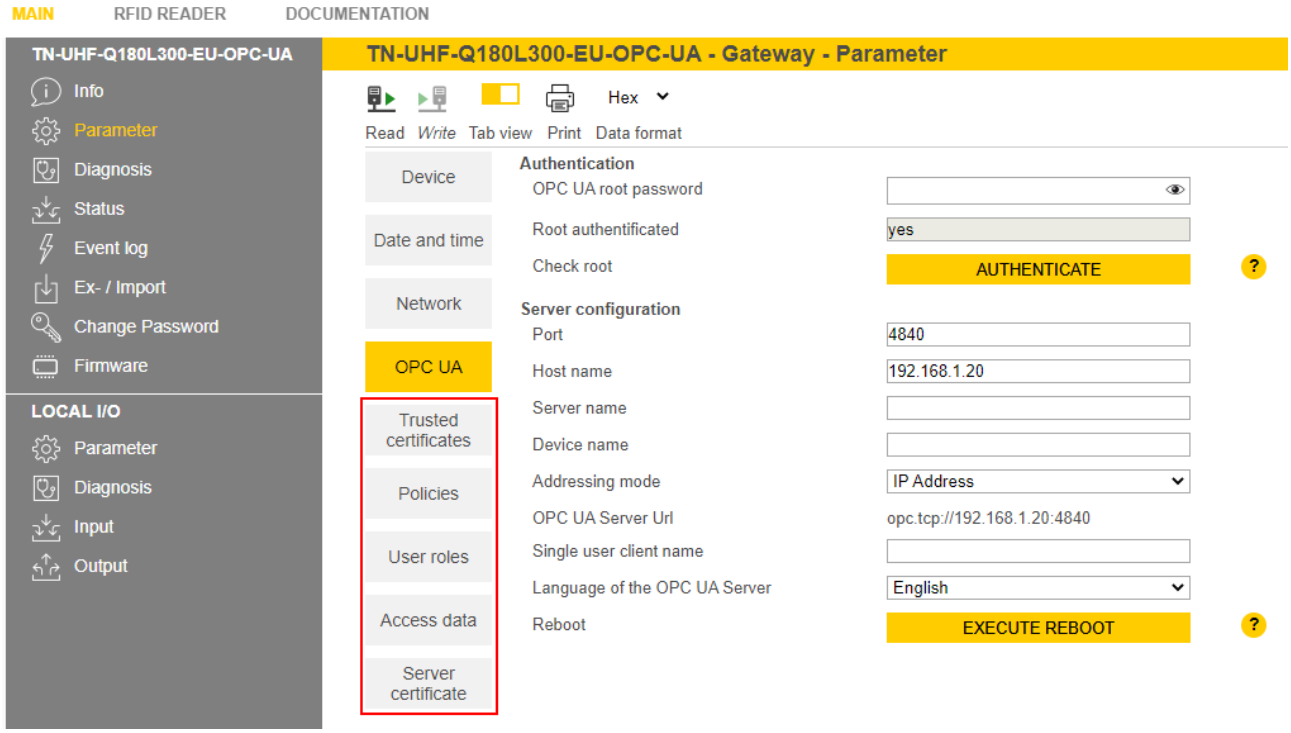



Fig. 30: Parameters for the OPC UA-specific configuration

The root password can be changed via **Access data**.

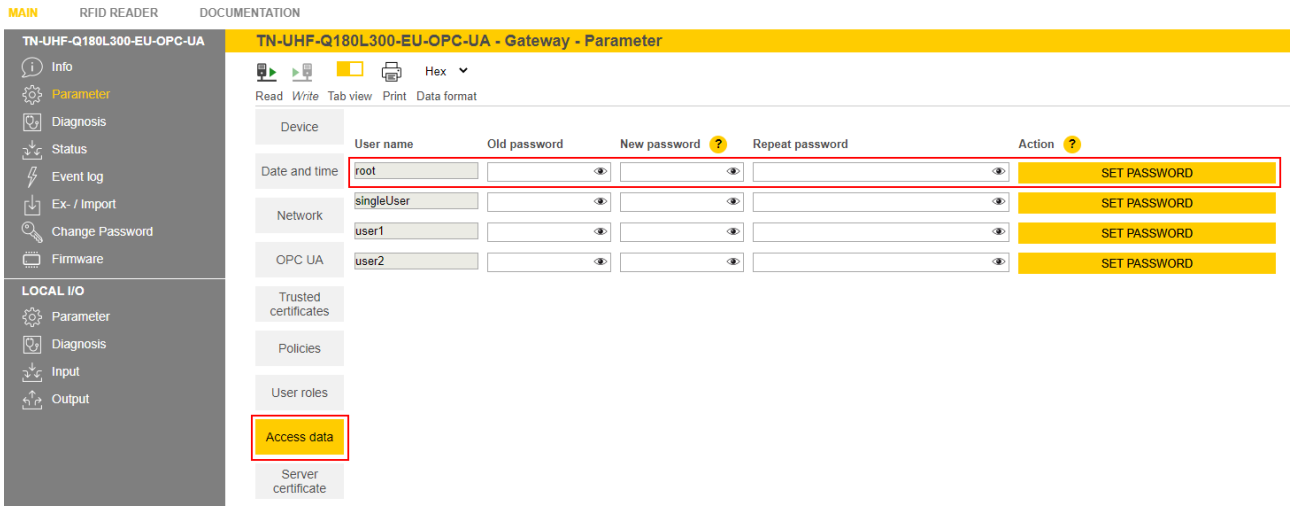



Fig. 31: Changing the root password

### 7.4.2 Establishing the connection between the OPC UA server and OPC UA client

The following example uses UAExpert as the OPC UA client.

- ▶ Add the OPC UA server in the OPC UA client used.
- ▶ Enter in the following window the OPC UA server URL and the required **Security Settings**.
- ▶ Confirm entries with **OK**.

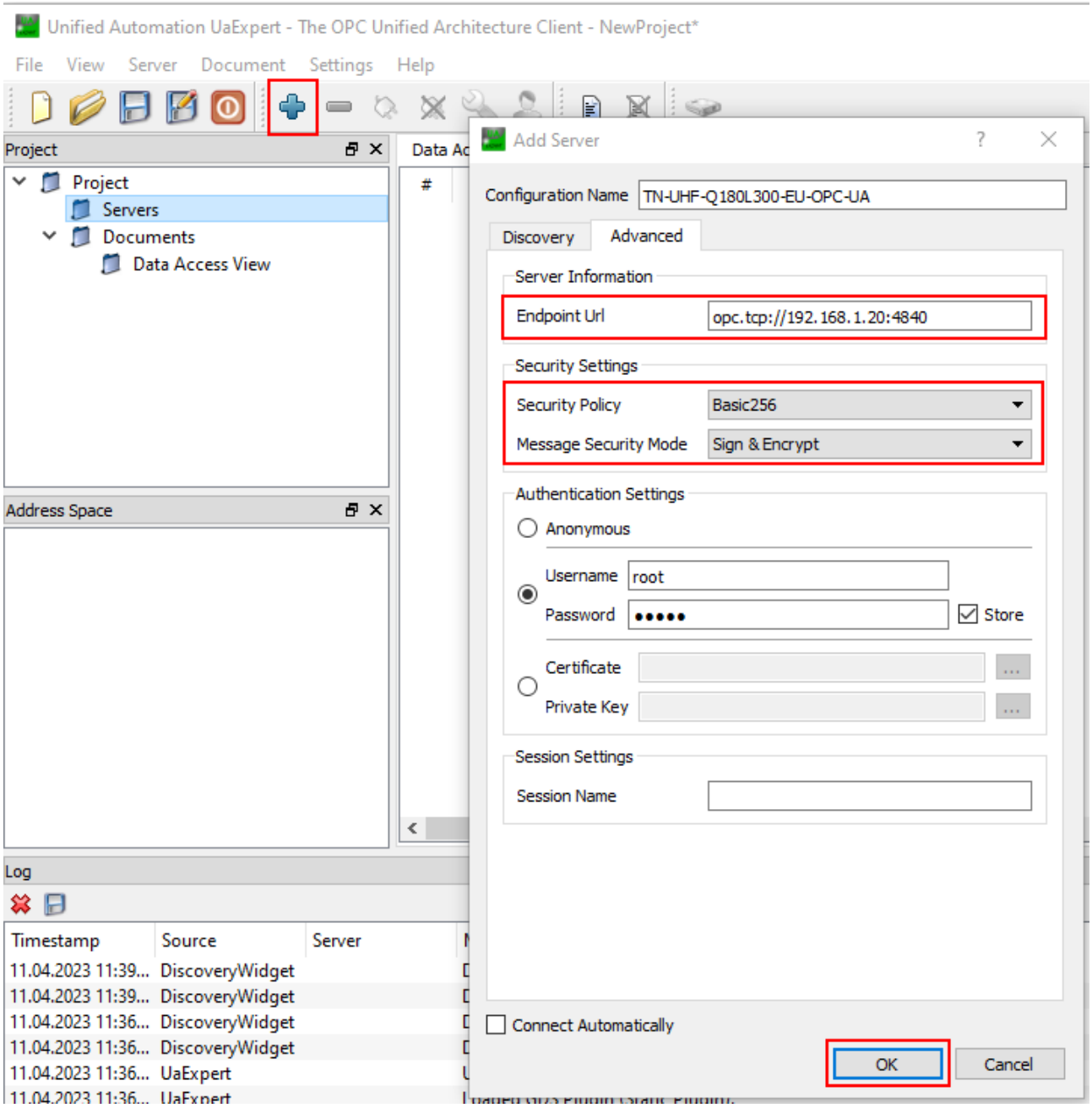



Fig. 32: Enter the OPC UA server URL and choose the Security Settings

⇨ The OPC UA server is added to the project tree.

- ▶ Right-click the server in the project tree.
- ▶ Click **Connect**.

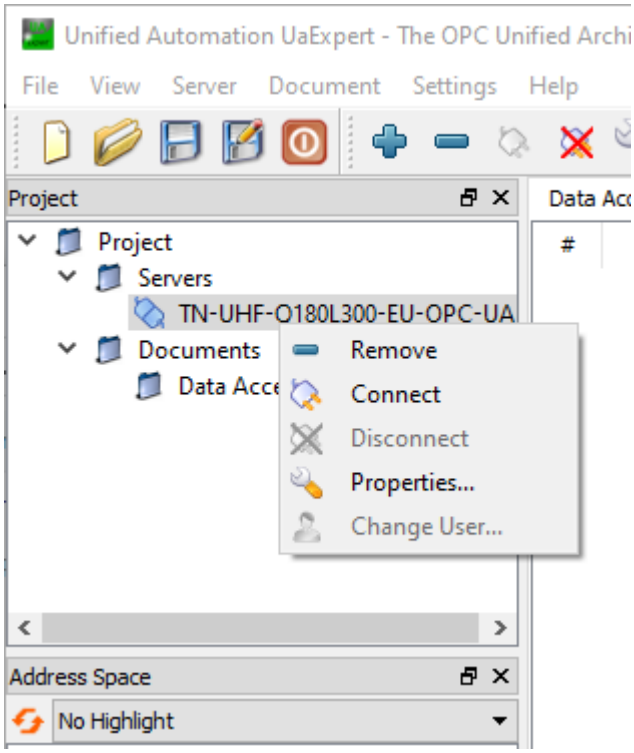



Fig. 33: Connecting the OPC UA server

⇨ The OPC UA client requests a connection and a security certificate from the server. If encryption is activated, the security certificate appears in the web server at **Parameter → Rejected certificates**.

- ▶ Click **TRUST** to add the security certificate to the list of trustworthy certificates.

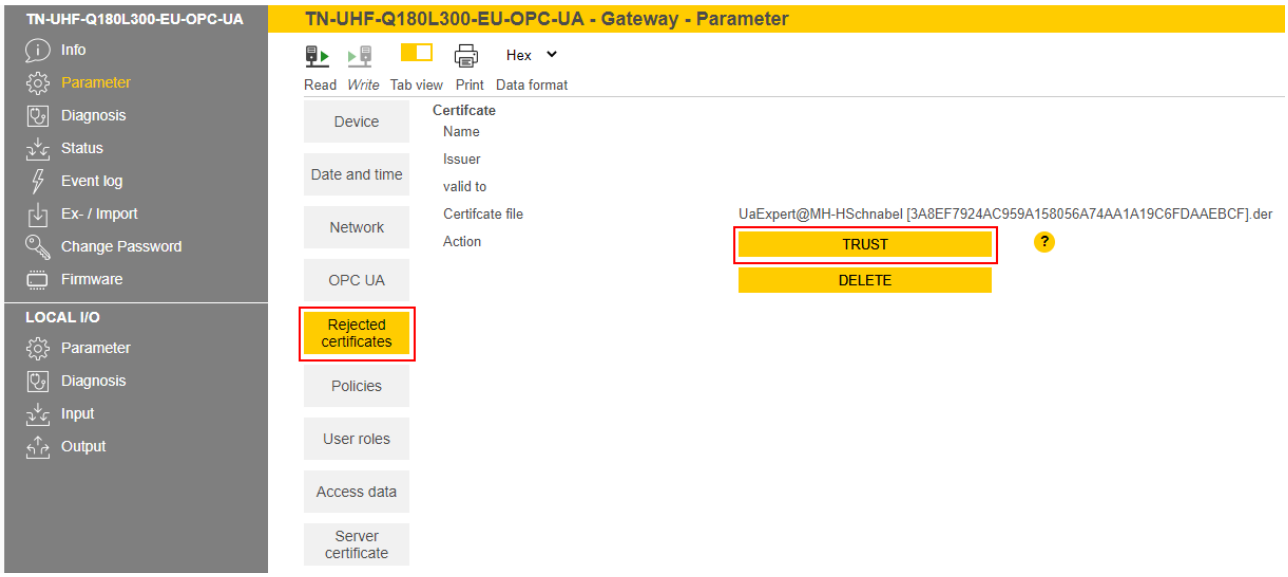



Fig. 34: Trusting security certificates

- ▶ In the OPC UA client, right-click the server and click **Connect**.

⇨ The connection between the OPC UA server and OPC UA client is established and the **Address Space** in the client is created.

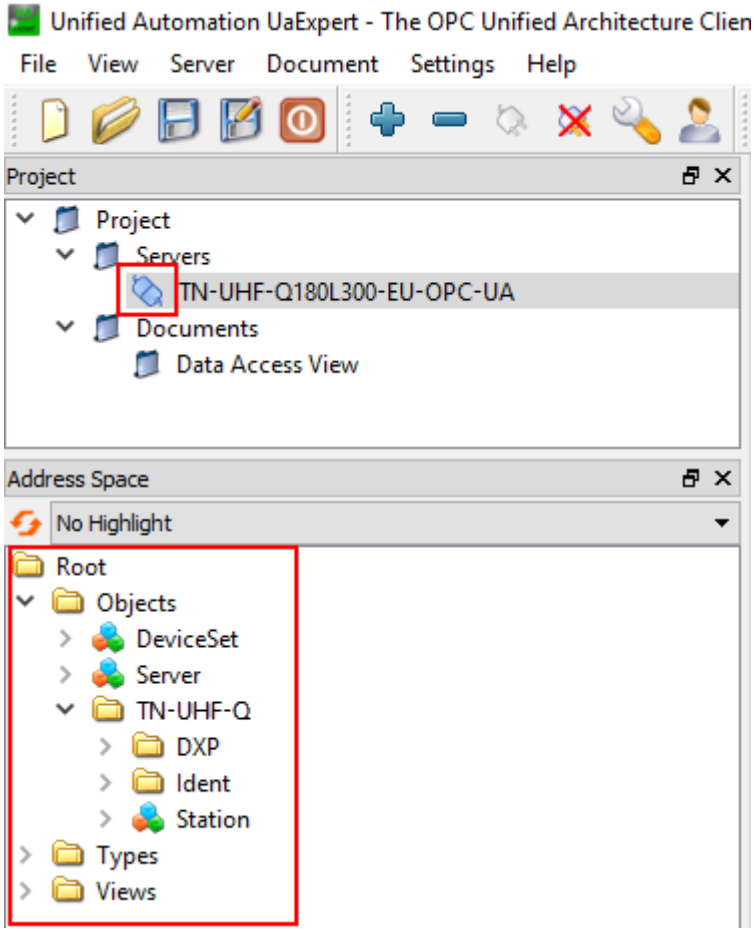



Fig. 35: Connection established, address space created

### 7.4.3 Validating security certificates

Security certificates must be accepted by the server before communication. The OPC UA client sends its certificate when the client is connected to the server via a secured connection. A separate security certificate is sent for each security level. The security certificates can be validated via the web server.

If the OPC UA client sends its security certificate when it is establishing a connection, the security certificate appears in the web server at **Parameter** → **Rejected certificates**.

- ▶ Trust security certificates: Click **TRUST**.
- ⇨ The security certificate is added to the list of trusted certificates.

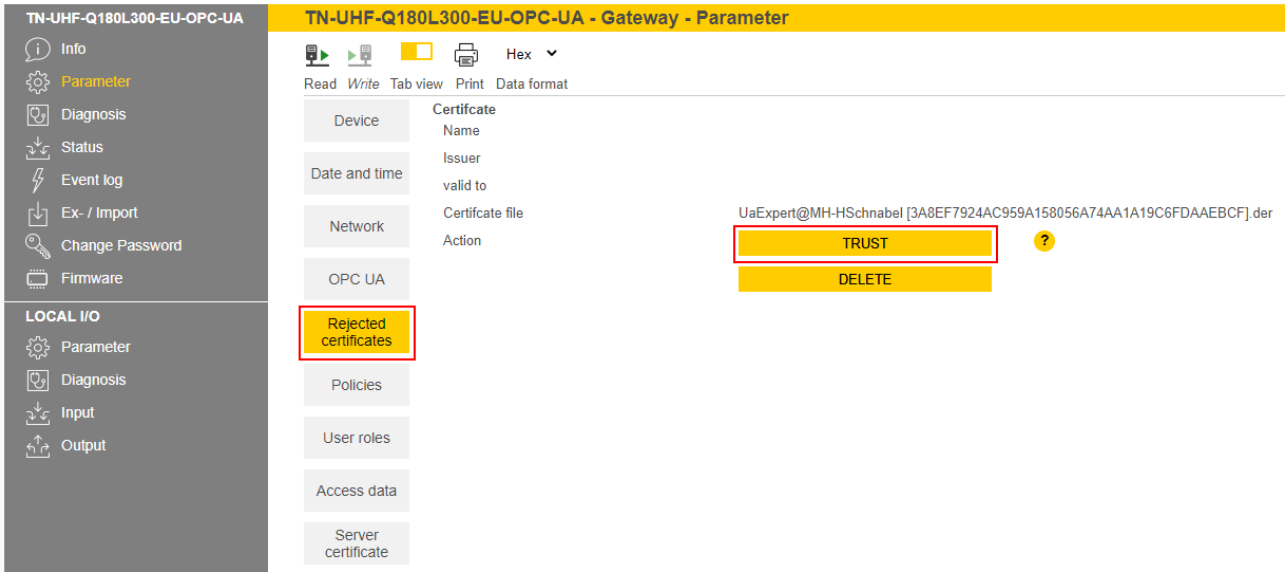



Fig. 36: Trusting security certificates

The **Trusted certificates** area lists the trusted certificates and can be rejected by clicking **REJECT**.

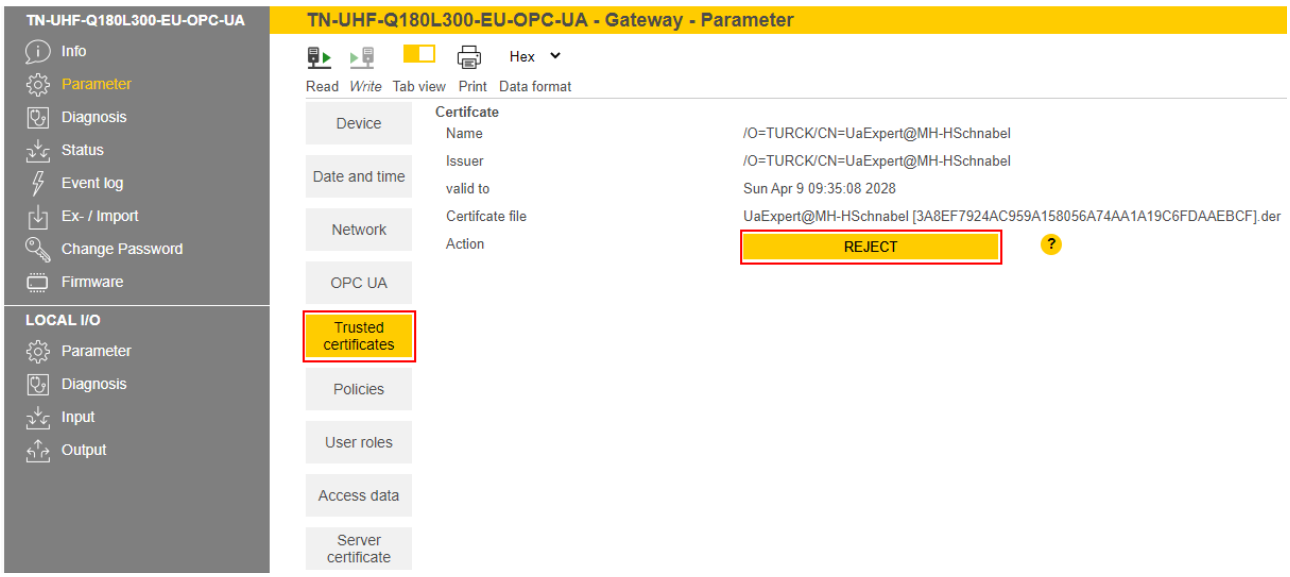



Fig. 37: Rejecting a certificate

## Creating a specific security certificate

The user can create a specific security certificate via **Update own server certificate**. The OPC UA clients must accept the new generated certificate. During the generation, the current IP address and host name are automatically added to the certificate. The certificate can also be edited via an OPC UA client if the highest security level is activated.

- ▶ Create a specific security certificate: Click **Parameter** → **Server certificate** → **UPDATE CERTIFICATE**.

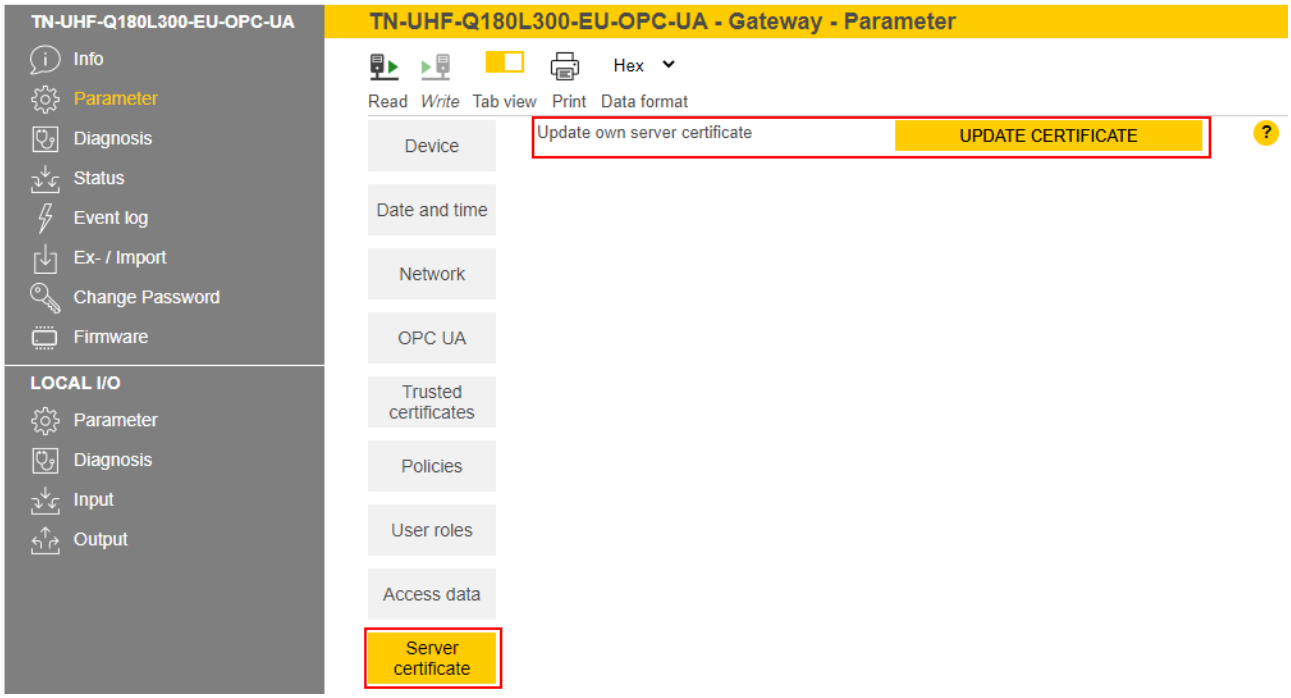



Fig. 38: Creating a specific security certificate

### 7.4.4 Adapting settings for OPC UA communication — set endpoints

**NOTE**
Changes to the settings are accepted after a voltage reset.

#### Changing the security settings

The device is provided with three security levels for OPC UA communication. The security levels Sign and Sign & Encrypt require the confirmation of the security certificate in the web server.

| Security level | Description |
|---|---|
| None | No protection |
| Sign | Communication with security certificate, no encryption |
| Sign & Encrypt | Communication with security certificate, encryption |

The security levels for the individual security policies can be set at **Parameter** → **Policies**. The SecurityPolicy describes the algorithm type and the key length used for a SecureChannel between the client and the server application.

If **Anonymous** is activated, a connection is allowed without a user login.

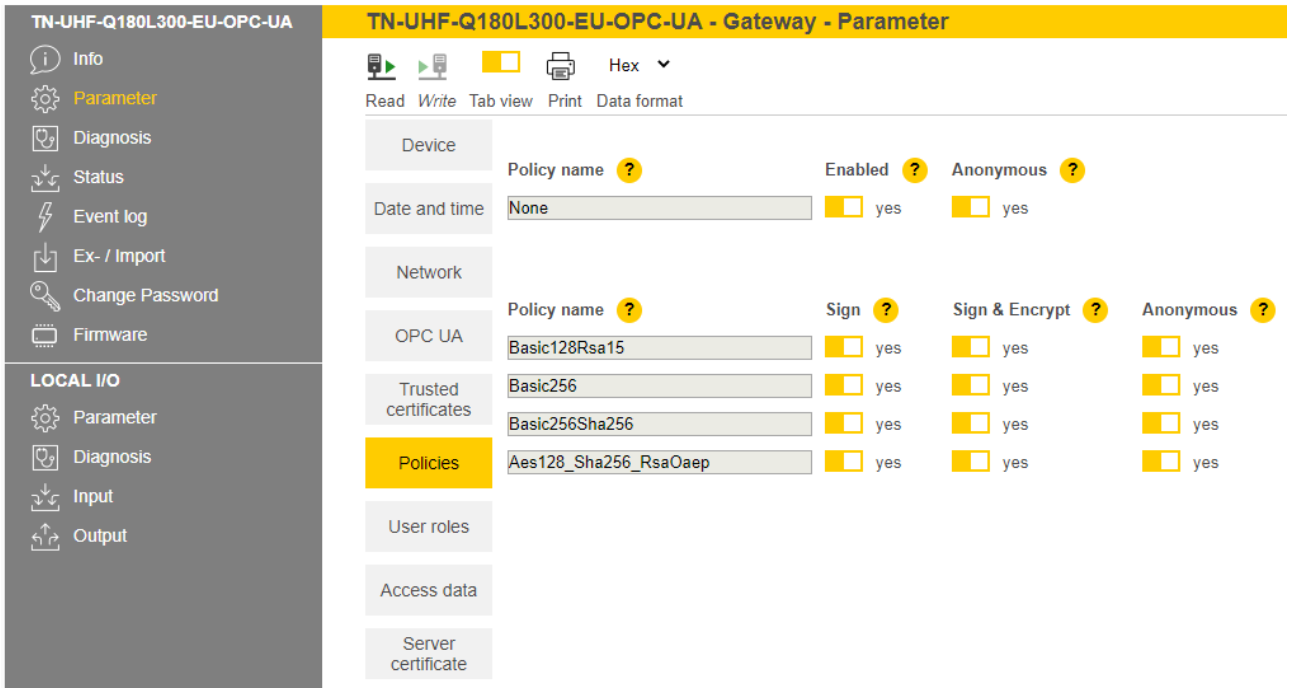



Fig. 39: Setting security levels for SecurityPolicies

## Issuing authorizations

The users (Anonymous, root, singleUser, user1, user2) can be assigned different rights at **Parameter → User roles**.

- **Observer**: authorized to search, read and receive events
- **Operator**: authorized to search, read, write and receive events and call up methods
- **Engineer**: authorized to search, read and configure safety-related parameters and methods (e.g. SetTagPassword, LockTag)
- **Administrator**: all authorizations
- **Single user**: authorized to use variables for limited clients (ScanActive, ScanSettings variables) (only singleUsers)

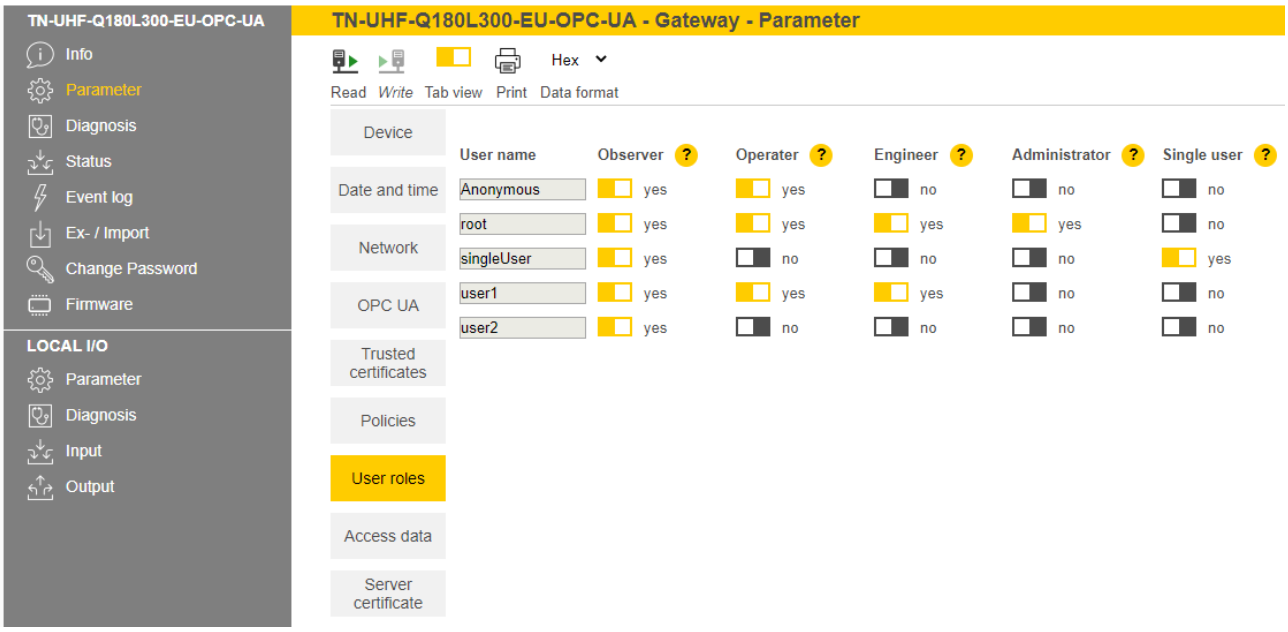



Fig. 40: User roles

## Configuring endpoints — server configuration

Settings including those listed below can be changed in the **Parameter → OPC UA → Server configuration** area:

- Port
- Host name
- Name of the OPC UA server

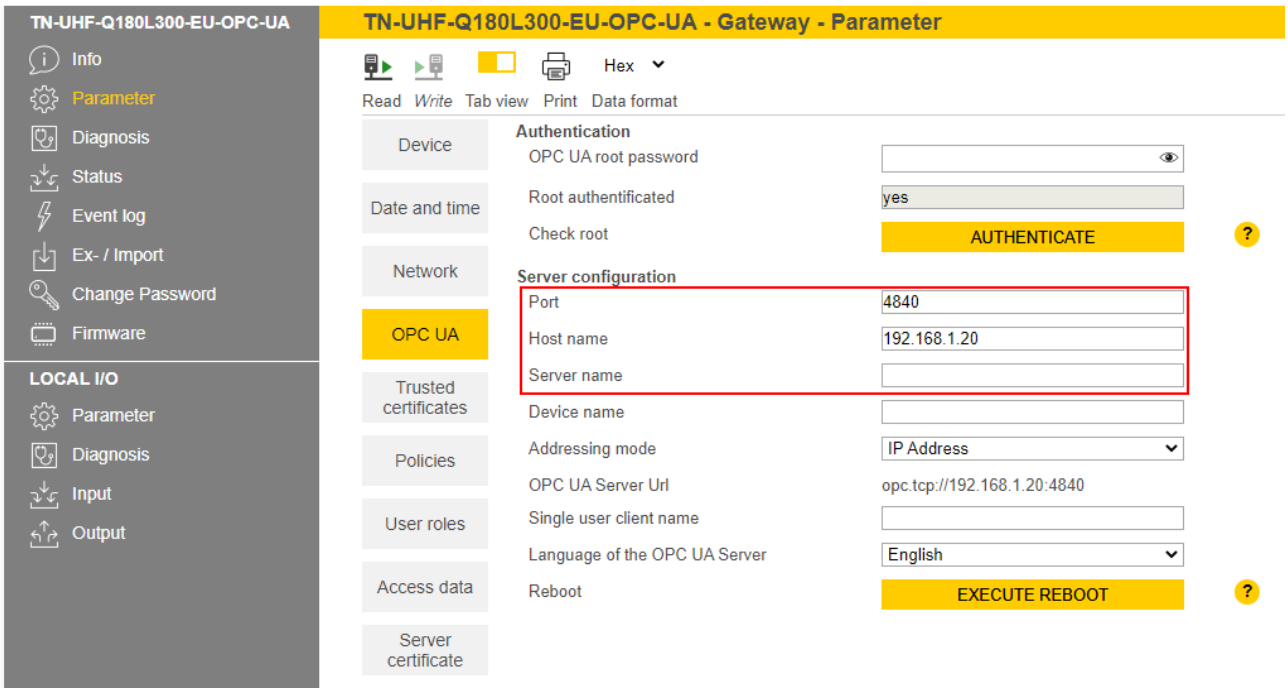



Fig. 41: Server configuration

### Changing the name resolution on the OPC UA server endpoint — Choose NodeName for Endpoint Resolution

In order to identify the endpoint uniquely, the OPC UA client checks the host name for the specified IP address. Identification problems can occur if DHCP and DNS are not available in a network. In order to avoid identification problems, a fixed IP address can be assigned for the name resolution or the host name can be set statically.

In networks with a DHCP server, the host name can be set via the NodeName variable.

In local networks without DHCP, the server can provide the DNS name via mDNS. In this case, Avahi (Linux network service) adds the ".local" suffix to the host name. In Windows systems, the Bonjour service can be used for the name resolution.

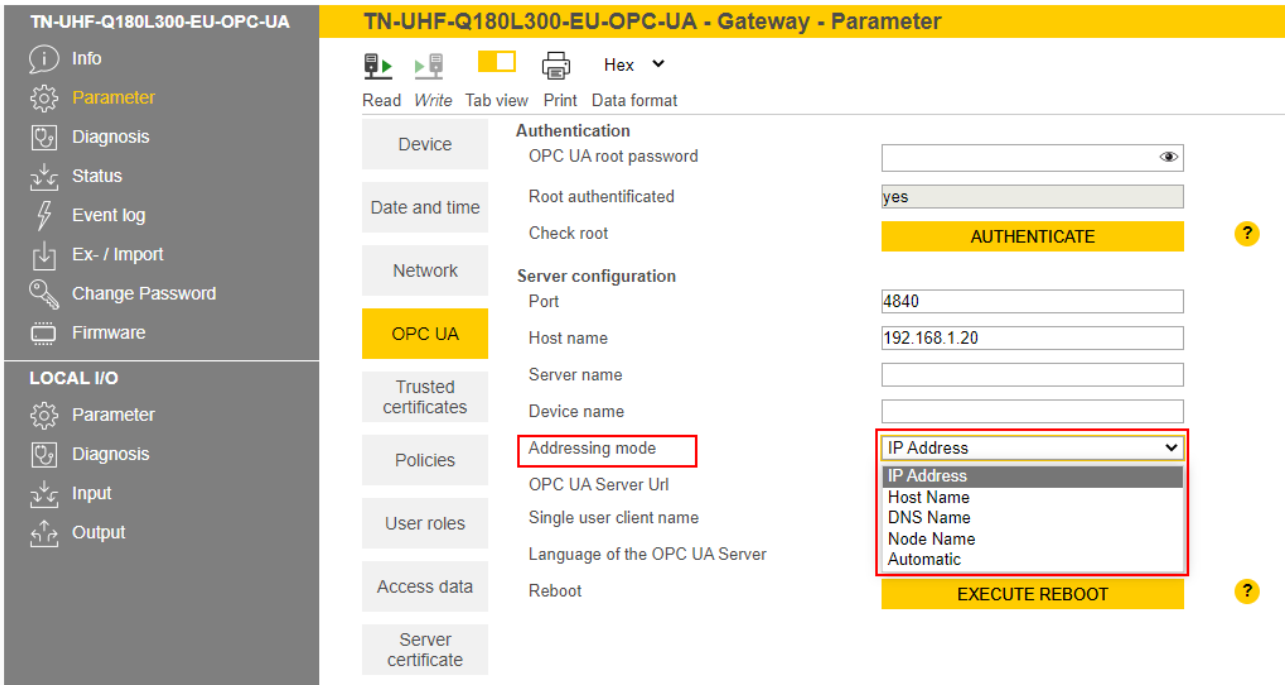



Fig. 42: Changing the name resolution for server endpoints

### Changing the language setting of the OPC UA server — Language of the OPC UA Server

OPC UA provides the opportunity to create a description (Description) for each object. The language of the description can be set at **Parameter → OPC UA → Language of the OPC UA Server**. German and English are the available languages.

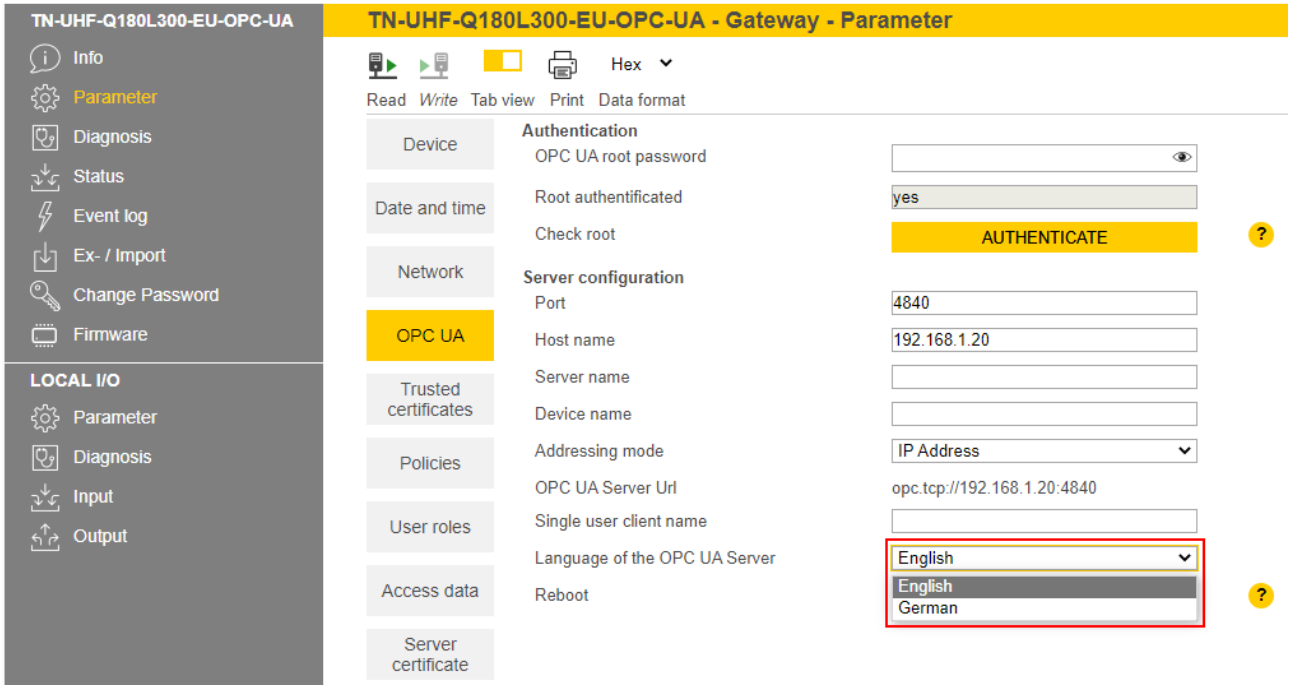



Fig. 43: Changing language settings of the OPC UA server

### 7.4.5 Setting the OPC UA password

To access OPC UA-specific parameters, enter the OPC UA root password. The default password is "Turck".

**NOTICE**
Insufficiently secured devices
**Unauthorized access to sensitive data**
- ▶ Change the password after the first login. TURCK recommends the use of a secure password.

- ▶ **Parameter → OPC UA**: Enter the password in the **OPC UA root password** field.
- ▶ Click **AUTHENTICATE**.

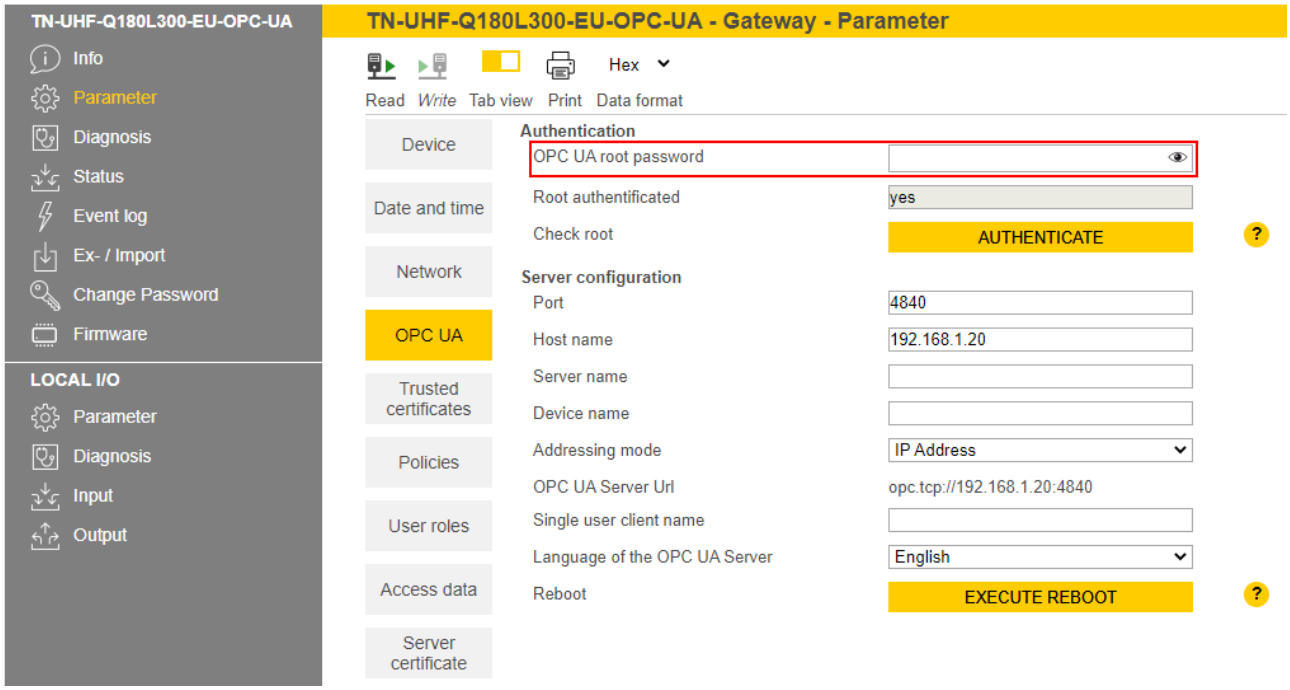



Fig. 44: Entering the OPC UA root password

A separate OPC UA password can be assigned and changed for each user. The default passwords for the different users are shown in the following table:

| User | Default password |
|---|---|
| root | Turck |
| user1 | password |
| user2 | password |
| singleUser | singlepassword |

- ▶ **Parameter → Access data**
- ▶ Enter the old password in the line of the required user.
- ▶ Enter the new password.
- ▶ Repeat the new password.
- ▶ Write the new password to the device via **SET PASSWORD**.

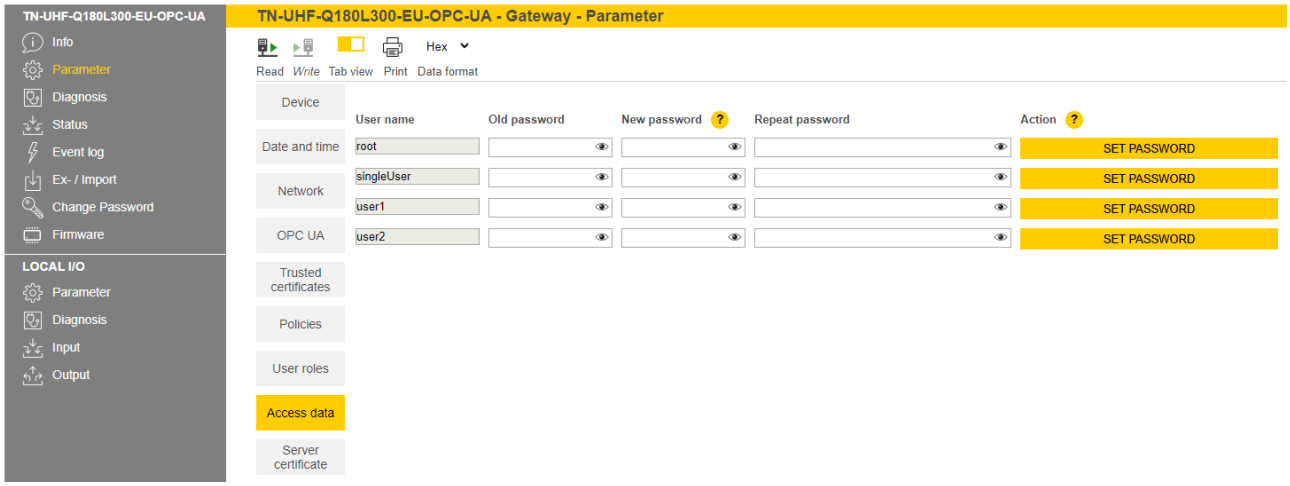



Fig. 45: Web server — changing OPC UA passwords

## Web server — resetting a password for the OPC UA server

The device can be reset to the factory settings via the F_Reset function (rotary coding switch at switch position 90, DIP switch [MODE] at position 1) without entering a password. All other possibilities to fully reset to the default settings, including the OPC UA passwords, are blocked.

### 7.4.6 Setting up an OPC UA client via an SDK

The OPC UA client must be set up in order to connect the OPC UA server of the device to an OPC UA client. The following software is required for the setup:

- Client SDK, e.g. from www.unified-automation.com (for C++, .net, ANSI C or Java)
- UaModeler, e.g. from www.unified-automation.com

The client SDK requires a chargeable license from www.unified-automation.com. The license supplied with the software always only lasts for an hour.

#### Creating application frames

- ▶ Install the client SDK and UaModeler.
- ▶ Launch the development environment and create a new project.

**NOTE**
An example of how to create a new application and the first steps required are provided in the documentation supplied with the client SDK.

- ▶ Download the license applied for and incorporate it in the project.
- ▶ Create the structured data types with the UaModeler.

**NOTE**
Examples and further information on handling structured data types are provided in the documentation supplied with the UaModeler.

- ▶ Incorporate the data generated in the UaModeler in the project of the client SDK.

# 8 Setting

## 8.1 Information model — mapping

The AutoID information model is structured in nodes which may also contain subnodes:

| Node class | Description |
|---|---|
| Folder | General collection |
| Object | Mapping of a technical object |
| Property | Description of an object |
| Variable | Process data or status information |
| Method | Functional scan with status feedback (e.g. RFID commands) |

In the information model, the devices are defined as objects and structured as follows:

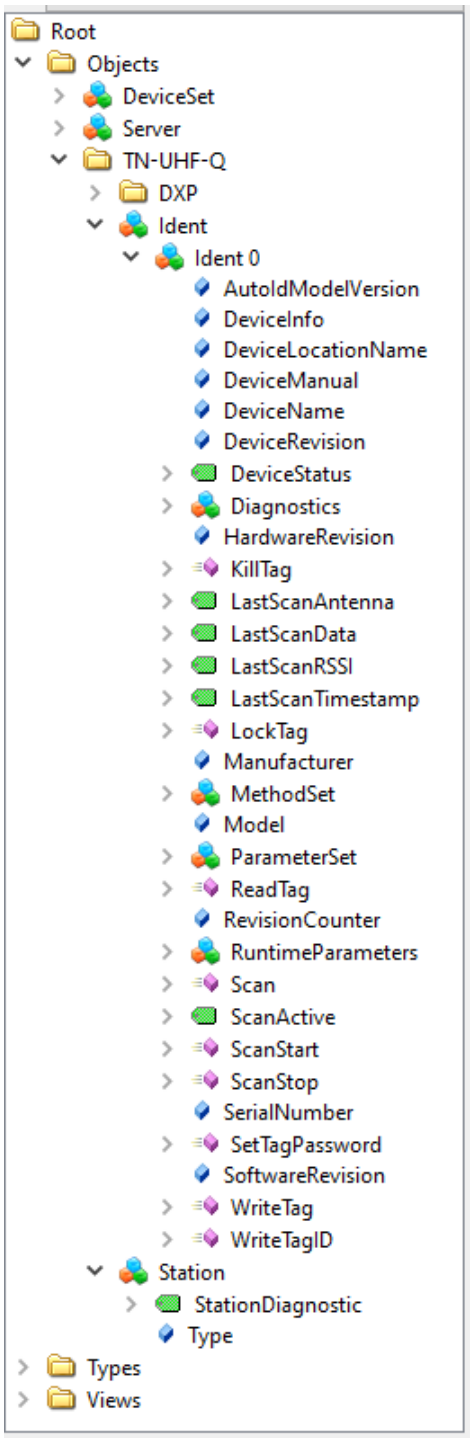



Fig. 46: Information model of the RFID channel Ident 0 — example: UA Expert

### 8.1.1 RFID channels — mapping in the information model

Each connected read/write device is assigned an Ident channel. The Ident 0 object contains properties, variables and methods.

#### Properties

| Property | Description | Example |
|---|---|---|
| AutoIdModelVersion | Version of the AutoID specification | 1.01 |
| DeviceInfo | RFID frequency range (HF/UHF) of the connected device | UHF |
| DeviceLocationName | — | — |
| DeviceManual | Link to operating instructions of the connected device | www.turck.de |
| DeviceName | Device name of the connected device | RFID read/write device |
| DeviceRevision | — | — |
| HardwareRevision | Hardware version of the connected device | V1.2 |
| Manufacturer | Manufacturer of the connected device | Turck |
| Model | Type designation of the connected device | 0x018F |
| RevisionCounter | Firmware version of the connected device | V1.69.82 |
| SerialNumber | Serial number of the connected device | 197601056 |
| SoftwareRevision | Firmware version of the connected device | V1.69.82 |

#### Variables — properties

**NOTE**
The variables in the **LastAccess (Diagnostics)** folder are not supported by the **ScanStart** method or the **ScanActive** variable.

| Variable | Description | Folder |
|---|---|---|
| DeviceStatus | Device status:<br>■ Idle: Device is in Idle mode, command execution possible<br>■ Error: Error<br>■ Scanning: Inventory command active (asynchronous)<br>■ Busy: Read or write operation active (synchronous) | |
| AntennaNames | Address of the read/write device | LastAccess (Diagnostics) |
| Client | Client executing the last command | LastAccess (Diagnostics) |
| Command | Last executed command | LastAccess (Diagnostics) |
| CurrentPowerLevel | Set output power of the UHF reader at the last command execution | LastAccess (Diagnostics) |
| Identifier | EPC of the last detected UHF tag | LastAccess (Diagnostics) |
| PC | PC of the last detected UHF tag | LastAccess (Diagnostics) |
| RWData | Read or write data of the last command execution | LastAccess (Diagnostics) |
| Strength | RSSI value of the last tag read | LastAccess (Diagnostics) |

| Variable | Description | Folder |
|---|---|---|
| Timestamp | Time stamp of the last UID or EPC read | LastAccess (Diagnostics) |
| LastLogEntry | Last log book entry for diagnostic messages | Logbook (Diagnostics) |
| LogColumns | Number of log book entries | Logbook (Diagnostics) |
| Presence | Indicates whether a tag was detected or not in front of the read/write device (true/false). | |
| LastScanAntenna | Address of the read/write device detecting the last read tag | |
| LastScanData | Last UID or EPC read | |
| LastScanTimestamp | Time stamp of the last UID or EPC read | |
| LastScanRSSI | RSSI value of the last tag read | |
| CodeTypes | Defines the EPC or UID format. | RuntimeParameters |
| CodeTypesRWData | Defines the format of the data to be read/written. | RuntimeParameters |
| MinRSSI | Minimum value of the RSSI to execute the action | RuntimeParameters |
| RfPower | Adaption of the output power of the UHF reader | RuntimeParameters |
| ScanSettings | Settings for the continuous scanning and reading of the UIDs or EPCs | RuntimeParameters |
| Cycles | Number of retries<br>If a total run time of cycles × duration > 6000 ms is exceeded, the device outputs the error message INVALID_CONFIGURATION. | ScanSettings (RuntimeParameters) |
| Duration | Duration in ms<br>If a total run time of cycles × duration > 6000 ms is exceeded, the device outputs the error message INVALID_CONFIGURATION. | ScanSettings (RuntimeParameters) |
| DataAvailable | Execute the action until a tag is in the detection range | ScanSettings (RuntimeParameters) |
| ScanActive | The read/write head searches for tags in the detection range and reads the UID or EPC continuously. The read UIDs or EPCs are presented as events in the **LastScanData** variable. The write permissions of the variable are restricted to one client or user. The variable cannot be used in Multitag mode. | |

## Methods — properties

The methods also contain arguments. The arguments enable the methods to be configured and status messages read out.

**NOTE**
The reading of USER data can be set via the web server parameters.

| Method | Argument (type) | Description |
|---|---|---|
| Scan | | The read/write device searches for tags in the detection range and reads the UID or EPC once. If the **Multitag** parameter is activated, several tags are read and output. |
| | Setting (ScanSettings) | Settings for reading the UIDs or EPCs |
| | Results (RfidScanResults) | UID or EPC of the read tags |
| | Status (AutoIdOperationStatusEnumeration) | Status of scan operation |

| Method | Argument (type) | Description |
|---|---|---|
| ScanStart | | The read/write device searches for tags in the detection range and reads the UID or EPC continuously. The reading of USER data of HF tags can also be set via the web server parameters. The read UIDs, EPCs or USER data are presented as events in the **LastScanData** variable. The method cannot be used in multitag mode. |
| | Setting (ScanSettings) | Settings for continuous reading of UIDs or EPCs |
| | Status (AutoIdOperationStatusEnumeration) | Status of the continuous scan operation |
| ScanStop | | Terminates the continuous reading of data initiated by **ScanStart**. |
| KillTag | | The memory of a UHF tag is made unusable. The tag can neither be read nor written after a KillTag command. A KillTag command cannot be reversed. |
| | AutoID identifier (ScanData) | EPC of the tag for which the Kill command is to be executed |
| | KillPassword (ByteString) | Kill password of the tag for which the Kill command is to be executed |
| | CodeType (String) | Defines the EPC or UID format. |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |
| LockTag | | Activates or deactivates the password protection for a tag or protects the selected memory area permanently and irrevocably. |
| | AutoID identifier (ScanData) | EPC of the tag to be locked |
| | CodeType (String) | Defines the EPC or UID format. |
| | Password (ByteString) | Access password of the tag (if required) |
| | Region (RfidLockRegionEnumeration) | Only in UHF applications: Defines the memory area of the UHF tag to be locked. The following memory areas can be locked:<br>■ 0: Reserved (kill and access password)<br>■ 1: EPC<br>■ 3: USER |
| | Lock (RfidLockOperationEnumeration) | Sets the type of lock:<br>■ 0: Lock (the entire memory area selected is write protected with a password.)<br>■ 1: Unlock (not supported)<br>■ 2: Permanent Lock (the entire memory area selected is permanently locked from write access. Kill password and access password are also locked irrevocably from read access.)<br>■ 3: Permanent Unlock (not supported)<br><br>Memory areas lock: EPC and PC, USER<br>Memory areas permanent lock: EPC and PC, USER, Access password, Kill password |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |

| Method | Argument (type) | Description |
|---|---|---|
| SetTagPassword | | Sets a password in the UHF tag. The method is only available for UHF applications. |
| | AutoID identifier (ScanData) | EPC of the UHF tag to be protected |
| | PasswordType (RfidPasswordTypeEnumeration) | Password type (e.g. Access password) |
| | AccessPassword (ByteString) | Access password of the tag (if required) |
| | NewPassword (ByteString) | New password to be written to the tag |
| | CodeType (String) | Defines the EPC or UID format. |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |
| ReadTag | | The read/write device reads the data of the tags in the detection range. |
| | AutoID identifier (ScanData) | UID or EPC of the tag that is to be read |
| | Offset (UInt32) | Start address of the memory area to be read on the tag |
| | Length (UInt32) | Number of bytes to be read |
| | Password (ByteString) | Access password of the tag (if required) |
| | Region (RfidLockRegionEnumeration) | Only in UHF applications: Defines the memory area of the UHF tag to be read. The following memory areas can be read:<br>■ 0: Reserved<br>■ 1: EPC<br>■ 2: TID<br>■ 3: User |
| | CodeType (String) | Defines the EPC or UID format. |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |
| | ResultData (ByteString) | Read data |
| WriteTag | | The read/write device writes the data to tags in the detection range. |
| | AutoID identifier (ScanData) | UID or EPC of the tag that is to be written to |
| | Offset (UInt32) | Start address of the memory area on the tag |
| | Password (ByteString) | Access password of the tag (if required) |
| | Region (RfidLockRegionEnumeration) | Only in UHF applications: Defines the memory area of the UHF tag to be written. The following memory areas can be written:<br>■ 0: Reserved<br>■ 1: EPC<br>■ 3: User |
| | CodeType (String) | Defines the EPC or UID format. |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |
| | Data (ByteString) | Write data |

| Method | Argument (type) | Description |
|---|---|---|
| WriteTagID | | Writing of a new UID or EPC (only for UHF applications) |
| | AutoID identifier (ScanData) | UID or EPC of the tag that is to be written to |
| | CodeType (String) | Defines the EPC or UID format. |
| | NewUid (ByteString) | UID or EPC to be written to the tag |
| | AFI (Byte) | (not supported) |
| | Toggle (Boolean) | (not supported) |
| | Password (ByteString) | Access password of the tag (if required) |
| | Status (AutoIdOperationStatusEnumeration) | Status of command execution |

### 8.1.2 Digital channels (DXP) — mapping in the information model

A DXP channel is assigned to every connected digital sensor or actuator.

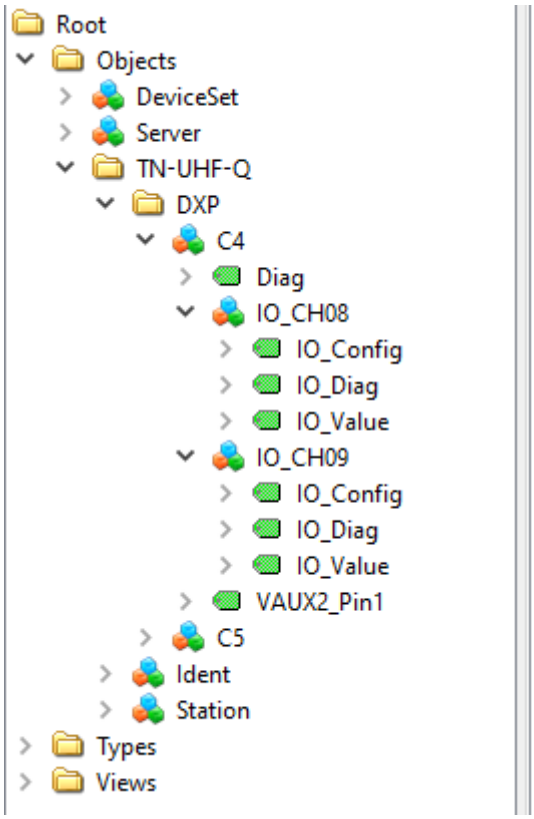



Fig. 47: Information model of DXP channels 8 and 9 — example: UAExpert

#### Variables — properties

| Name | Description |
|---|---|
| IO_Config | 0: Configure channel as a digital input<br>1: Configure channel as a digital output |
| IO_Diag | 0: No error present<br>1: Error present |
| IO_Value | 0: No signal present<br>1: Signal present |

## 8.2 Setting RFID interface parameters via the web server

The parameters for the RFID channels and the digital channels can also be set via the integrated web server in addition to the OPC UA configuration. The switchable VAUX power supply can also be set in the web server.

A login is required to edit settings via the web server. The default password is "password".

**NOTE**
TURCK recommends changing the password after the first login for security reasons.

- Open the device's web server.
- Enter **Username** and **Password**.
- Click **Login**

### 8.2.1 Setting digital channels (DXP) parameters via the web server

- Open the web server.
- Click **Local I/O** → **Parameter** in the navigation bar on the left of the screen.
- Select the DXP channel (here: **Digital In/Out 8**).
- Set the required parameters via the appropriate drop-down menu.

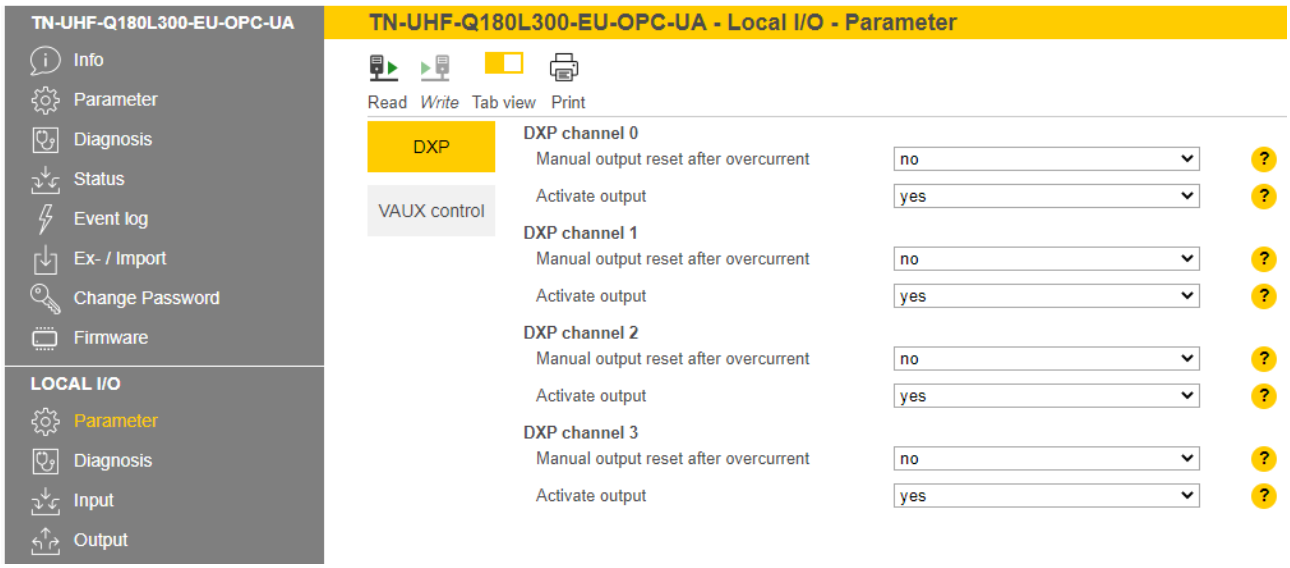



Fig. 48: Web server — DXP channel parameters

#### DXP channels — meaning of the parameters

Default values are shown in **bold**.

| Designation | Meaning |
|---|---|
| Activate output | **Yes: Output activated.**<br>No: Output deactivated. |
| Manual output reset after overcurrent | Yes: The output only switches back on after the overcurrent is removed and the switch signal is reset<br>**No: The output switches on automatically again after overcurrent.** |

### 8.2.2 Digital channels – setting switchable VAUX power supply

- Open the web server.
- Click **Local I/O** → **Parameter** in the navigation bar on the left of the screen.
- Select switchable **VAUX control** power supply.
- Set the required parameters via the appropriate drop-down menu.

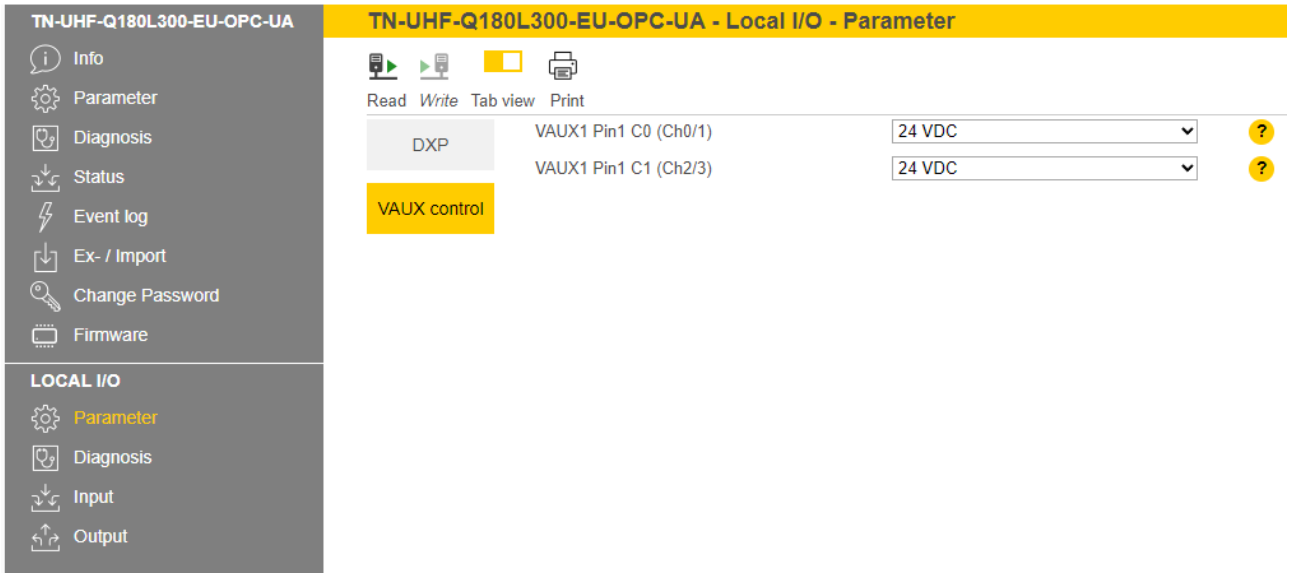



Fig. 49: Web server — VAUX control parameter

#### Switchable power supply — meaning of the parameters

| Designation | Meaning |
|---|---|
| VAUX2 Pin1 C4 (Ch0/1) | Activates or deactivates the VAUX2 24-VDC power supply at pin 1 of channel 0 and channel 1.<br>Default setting: **On** |
| VAUX2 Pin1 C5 (Ch2/3) | Activates or deactivates the VAUX2 24-VDC power supply at pin 1 of channel 2 and channel 3.<br>Default setting: **On** |

## 8.3 Testing the device with demo programs

Two demo programs can be downloaded free of charge for test purposes at www.turck.com:

| Program | Description |
|---|---|
| OPC UA Client Demo V1.2.0 – Complete RFID functionality | Testing RFID methods |
| OPC UA Client Demo V1.2.0 – Notifications about scan events | Testing the reading of UID or EPC |

**NOTE**
The demo programs can be used for one hour from the time when they were connected.

The source code of the demo programs is also available for download free of charge. The demo programs were created with the followings software:

- Visual Studio IDE V 17
- Unified Automation .NET-SDK V 2.5.8.410

### 8.3.1 Testing RFID methods

The program contains the following methods and functions:

- Scan
- ScanStart
- ScanStop
- ReadTag
- WriteTag
- Info (properties of the connected read/write device)

**NOTE**
With UHF, the user area is read or written automatically.

A description of the methods is provided in the chapter “RFID channels – mapping in the information model”

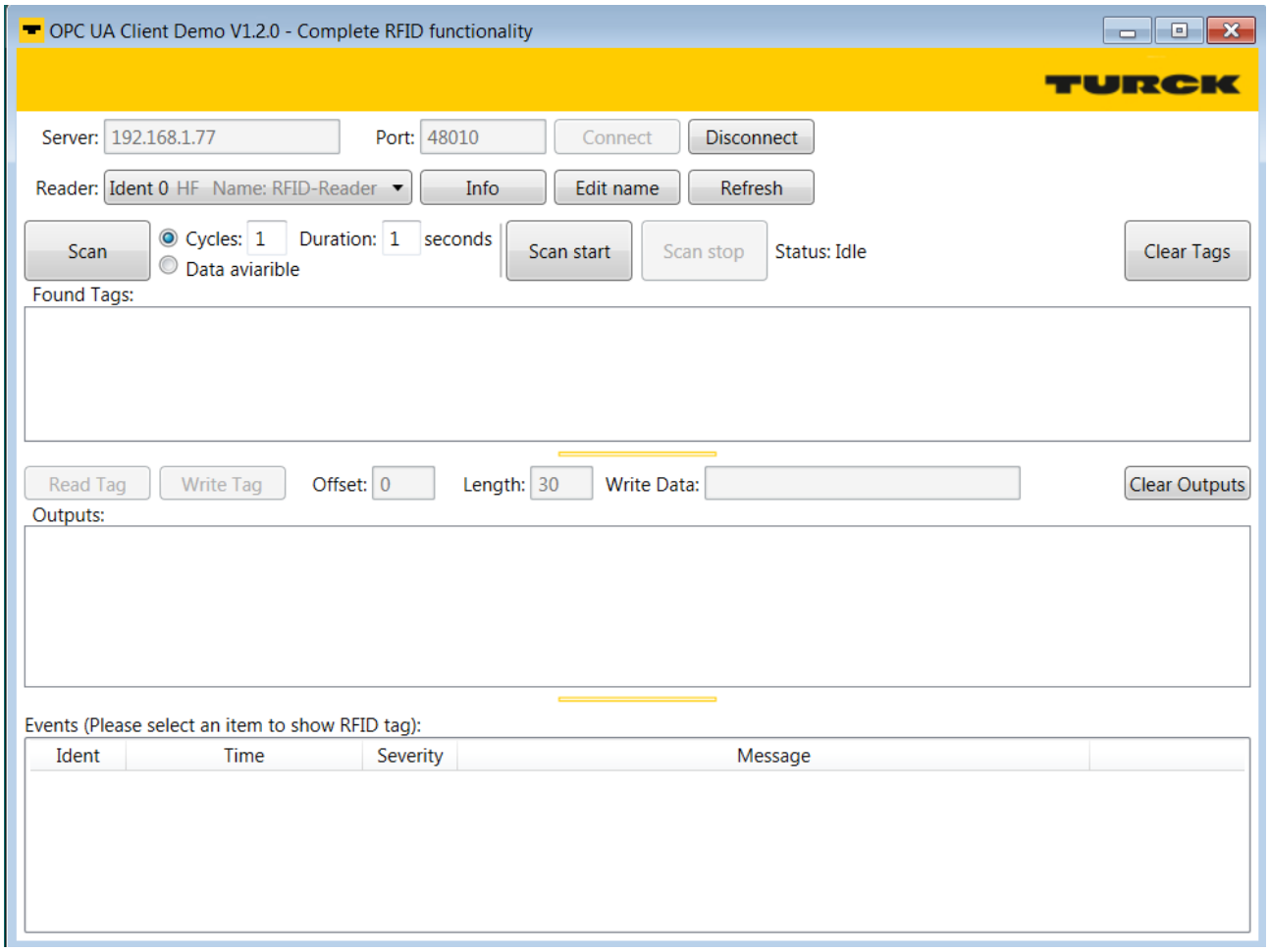



Fig. 50: OPC UA Client Demo V1.2.0 – complete RFID functionality

### Example: Running the scan method

✓ The device must be connected to a PC.

- ▶ Enter the IP address of the server and port.
- ▶ Establish a connection to the OPC UA server via **Connect**.
- ▶ Select the read/write device. The properties of the connected read/write device can be displayed via **Info**. The name of the selected read/write device can be changed via **Edit**.
- ▶ Set the number of cycles and duration of command execution in seconds or select **Data available**. With **Data available**, the command is executed until a tag is found.
- ▶ Search for tags via **Scan**.
- ⇨ The found tags are displayed in the **Result** area.
- ▶ Select tags for further processing.
- ▶ Adjust the offset and length if required.
- ▶ Read data from the tag: Click **Read Tag**.
- ▶ Writing data to the tag: Enter the required data and click **Write Tag**.

### 8.3.2 Testing reading of the EPC

The program contains the following methods and functions:

- ScanStart
- ScanStop

A description of the methods is provided in the chapter “RFID channels — mapping in the information model”

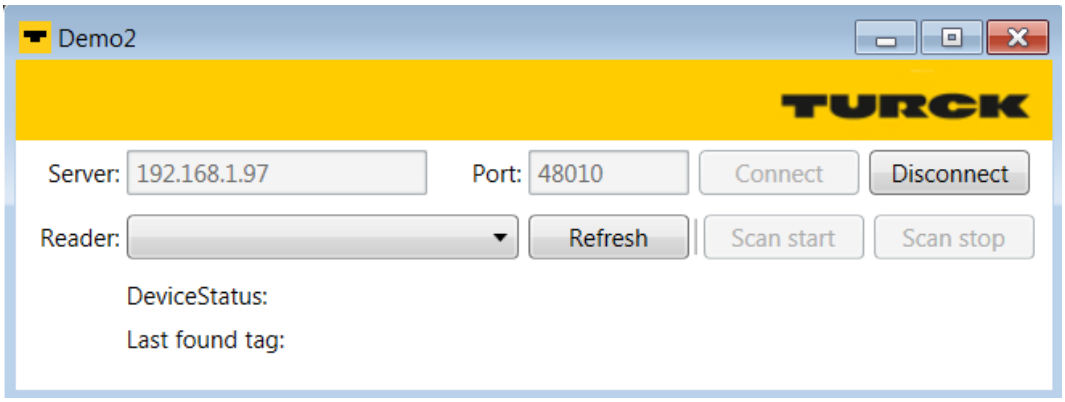



Fig. 51: OPC UA Client Demo V1.2.0 - Notifications about read events

#### Example: executing the ScanStart method

✓ The device must be connected to a PC.

▶ Enter the IP address of the server and port.

▶ Establish a connection to the OPC UA server via **Connect**.

▶ Select the reader. The properties of the connected reader can be displayed via **Info**. The name of the selected reader can be changed via **Edit**.

▶ Click **ScanStart**.

⇨ The last tag found tag and the device status of the interface are displayed.

# 9 Operation

**NOTE**
The read and write data stored in the device is reset after a power reset.

## 9.1 Executing a method and calling data

The data can either be called by the OPC UA client or forwarded as event messages to the higher-level system by the OPC UA server.

- ▶ Execute the **Scan** method.
- ⇨ The data is returned as a result and can be queried by the client.
- ⇨ The last tag read can be read in the **LastScanData** variable.
- ⇨ The **Status** variable shows if a method is active and if the reader is operational.

- ▶ Execute a command via the **ScanStart** method.
- ⇨ The readers are set to report mode. The read data is provided via event messages for all clients that have subscribed to this service. A separate scan by the OPC UA client is not required.
- ⇨ The last tag read can be read in the **LastScanData** variable.
- ⇨ The **Status** variable shows if a method is active and if the read/write device is operational.

### 9.1.1 Example: Reading or writing tags with a specific UID

- Call the **Scan** method in the OPC UA client (here: UAExpert).
- At **Input Arguments** → **Setting** click the **[…]** button.
  ⇨ The **Edit Value** window opens.
- Change the value in the **DataAvailable** line from **false** to **true** (double-click, tick checkbox).
- Confirm operation with **Write** and read the tag by clicking **Call**.

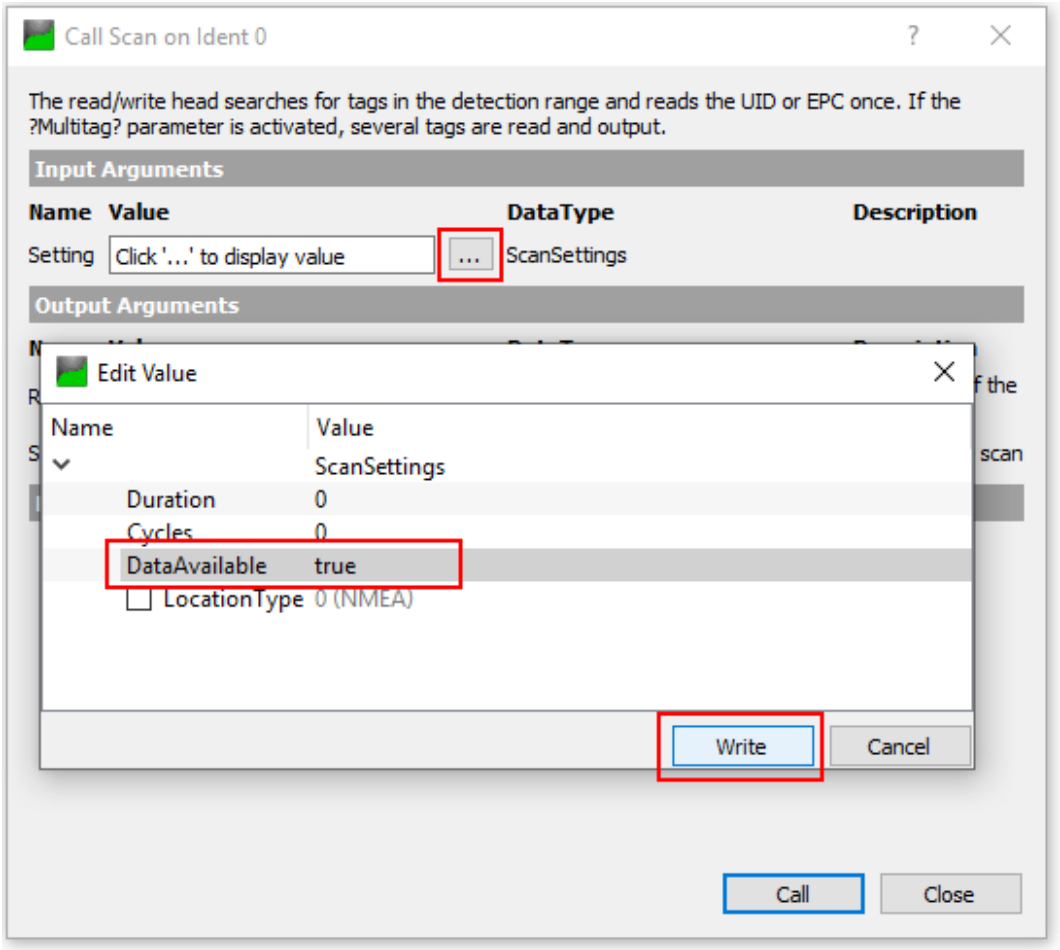



Fig. 52: Scan method – settings (example: UAExpert)

- At **Output Arguments** → **Results** click the **[…]** button.
- Copy the read UID by right-clicking in the **Value** window in the **ByteString** line (here: **E0040150588039B1**).

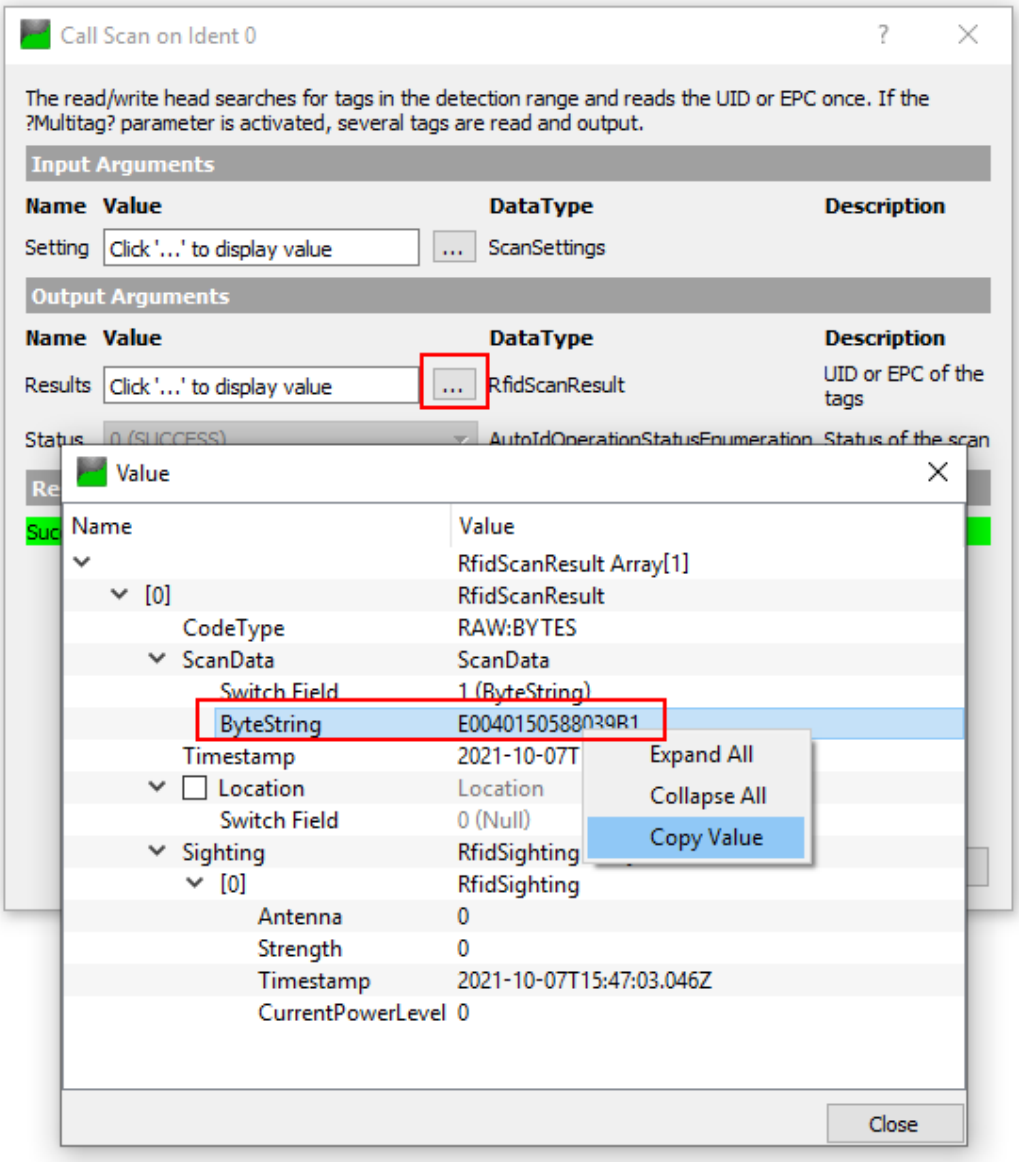



Fig. 53: Copying the read UID

- Call the **ReadTag** method.
- At **Input Arguments** → **Identifier** click the **[…]** button.
- In the **Edit Value** window in the **Switch Field** line select **1 (ByteString)** in the drop-down menu.

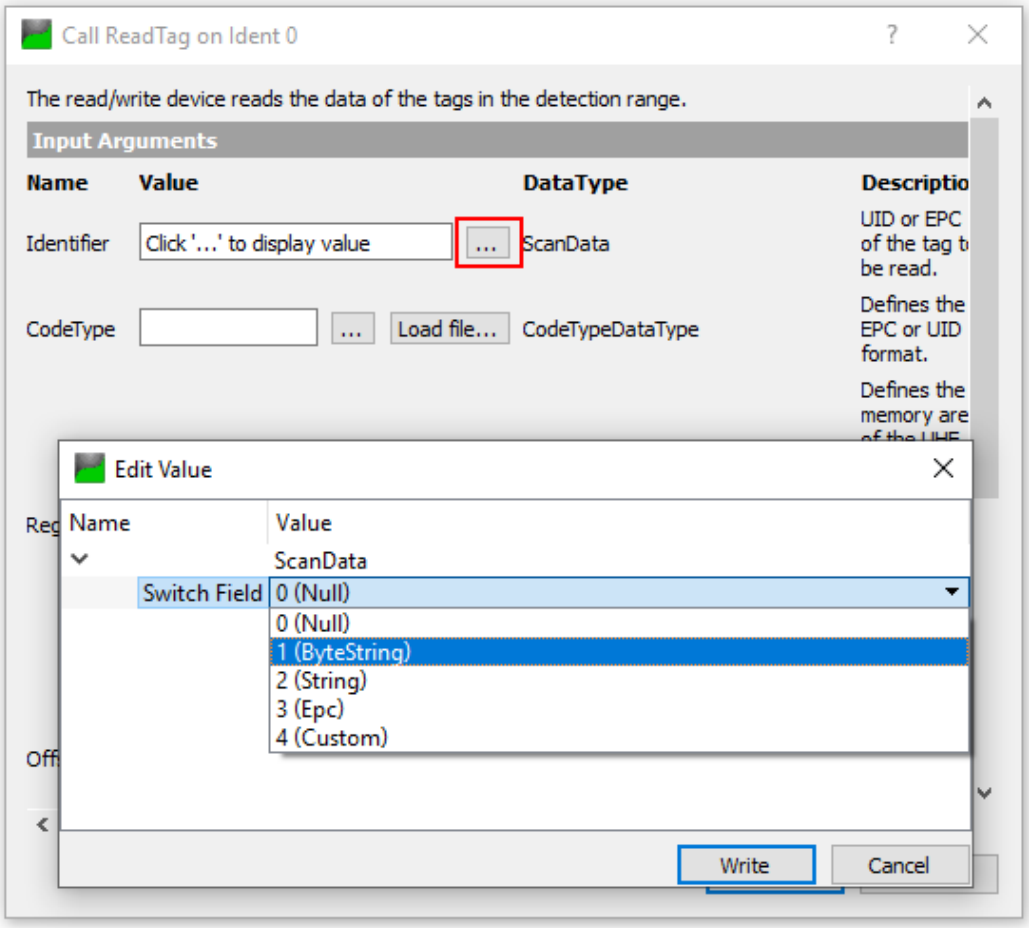



Fig. 54: ReadTag method – selecting ByteString

- Insert the copied UID in the **ByteString** line.
- Confirm the operation with **Write**.

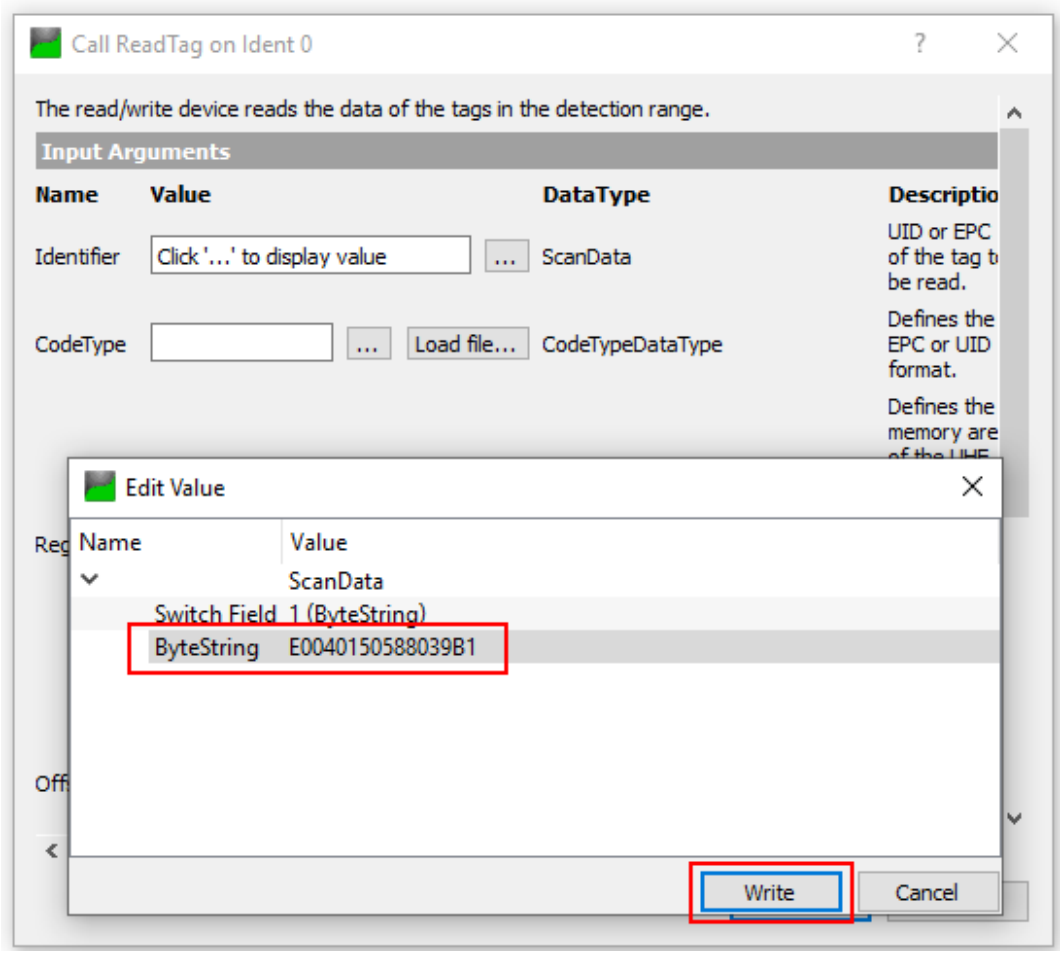



Fig. 55: Identifier – entering a copied UID

- ▶ Enter under **Input Arguments** → **Offset** the start address of the register to be read (here: **0**).
- ▶ Enter the number of bytes to be read in **Length** (here: **30**).
- ▶ At **CodeType** click the **[…]** button.
- ▶ In the **Edit Value** window enter the term **UID**.
- ▶ Confirm the operation with **Write** and click **Call**.
- ⇨ The tag is read.

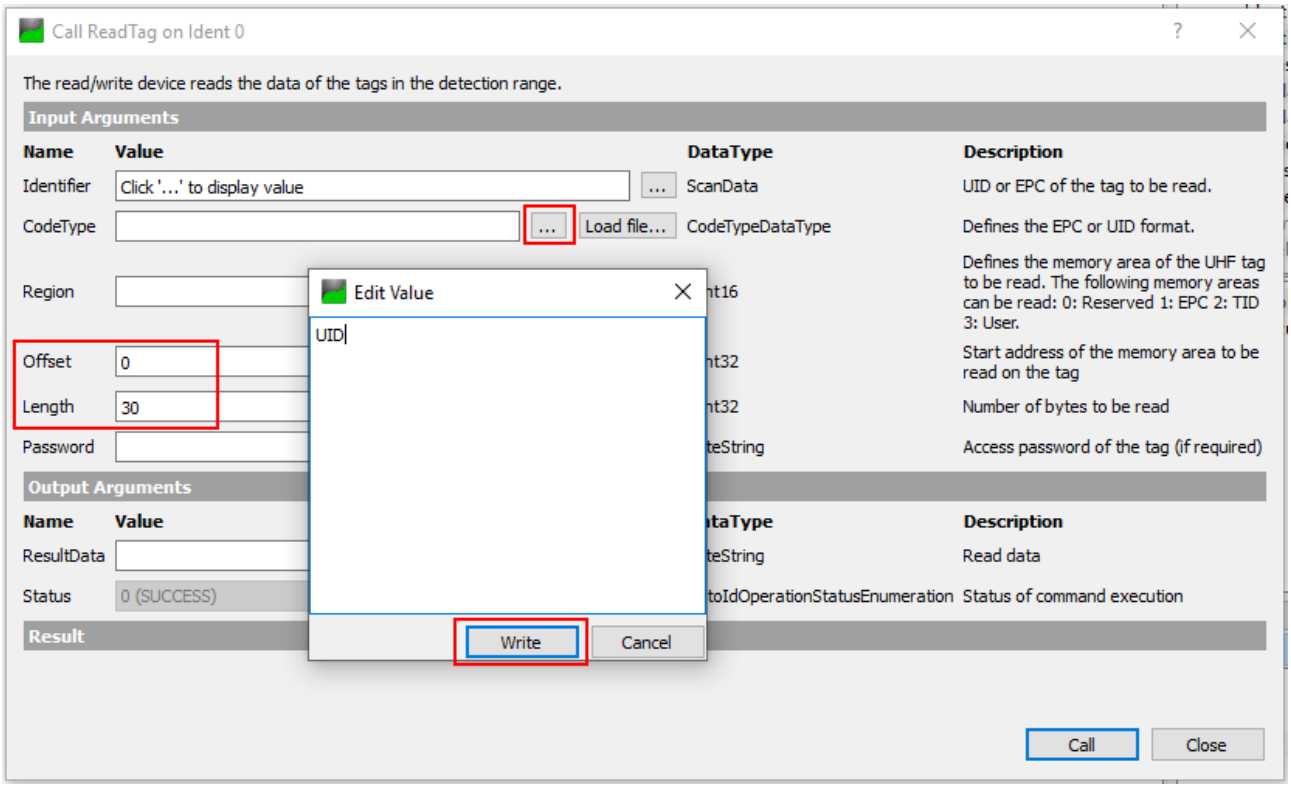


Fig. 56: ReadTag method settings

- ▶ At **Output Arguments** → **ResultsData** click the **[…]** button.
- ⇨ The information stored on the tag is displayed in the **Value** window.

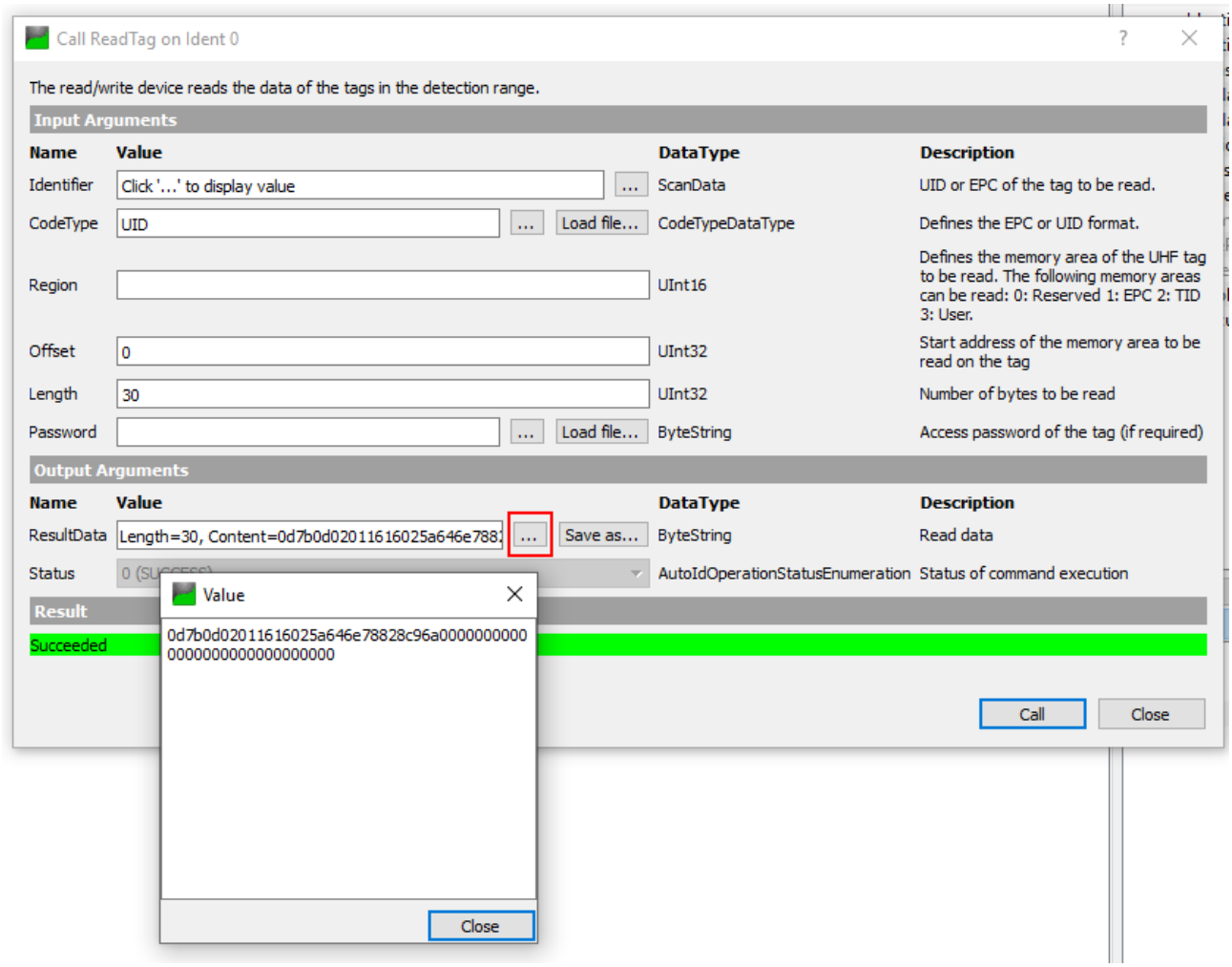



Fig. 57: Information stored on the tag

## 9.2 Linking sensor signals and RFID methods

Sensor signals can be linked with the execution of an RFID method by programming in the client application. Alternatively, the Report mode of the read/write head can be used (see ScanStart method). The read/write head is automatically triggered in Report mode as soon as a tag is located in the detection range.

## 9.3 LEDs

The device has the following LED indicators:

- Power supply
- Group and bus errors
- Status
- Diagnostics

| PWR LED | Meaning |
|---|---|
| Off | No voltage or undervoltage at V1 |
| Green | Voltage at V1 ok |
| Red | No voltage or undervoltage at V2 |

| ERR LED | Meaning |
|---|---|
| Off | No voltage present |
| Green | No diagnostics |
| Red | Diagnostics present |

| RUN LED | Meaning |
|---|---|
| Off | OPC UA server not active |
| Green | OPC UA server active |
| Red flashing (double, 1 Hz) | F_Reset active |

| ETH1 and ETH2 LEDs | Meaning |
|---|---|
| Off | No Ethernet connection |
| Green | Ethernet connection established, 100 Mbit/s |
| Green flashing | Data transfer, 100 Mbit/s |
| Yellow | Ethernet connection established, 10 Mbit/s |
| Yellow flashing | Data transfer, 10 Mbit/s |

## 9.4 Reading status and diagnostic messages

### 9.4.1 Read out OPC UA diagnostic messages

The OPC UA diagnostic messages are output via the Status argument when methods are executed.

**NOTE**
Additional specific fault signals relating to the readers are output in the web server.

| Message | Description | Possible causes |
|---|---|---|
| SUCCESS | No error, command successfully executed | — |
| MISC_ERROR_TOTAL | Command not fully executed | ■ Unknown error |
| PERMISSON_ERROR | Password required | ■ A valid password is expected before the command is accepted. |
| PASSWORD_ERROR | Password incorrect | |
| REGION_NOT_FOUND_ERROR | Addressed memory area not available for current tag | ■ Memory area of the tag outside of the permissible range |
| OUT_OF_RANGE_ERROR | Specified memory area not available for current tag | ■ Block size of the tag not supported<br>■ **Tag type** parameter outside of the permissible range<br>■ Address outside of the permissible range<br>■ Length and address outside of the permissible range<br>■ Length of the UID outside of the permissible range<br>■ Length outside of the tag specification<br>■ Address outside of the tag specification<br>■ Length and address outside of the tag specification |
| NO_IDENTIFIER | Command not fully executed — no tag in the detection range | ■ No tag found<br>■ Timeout<br>■ Air interface error: Timeout<br>■ Air interface error: UHF tag outside of the detection range before all commands could be executed<br>■ UHF reader: no tag in the field<br>■ Air interface error: Tag does not have the expected UID |
| MULTIPLE_IDENTIFIERS | Multiple tags were selected, command only usable for one tag. | |
| READ_ERROR | Tag could not be read. | ■ Error when reading from a tag<br>■ Read process not possible (e.g. invalid tag)<br>■ The UHF reader failed to execute an inventory command |
| WRITE_ERROR | Tag could not be written. | ■ Write process not possible (e.g. tag readable only)<br>■ Error when writing to a tag |

| Message | Description | Possible causes |
|---|---|---|
| NOT_SUPPORTED_BY DEVICE | Command or parameter are not supported by the device. | ■ Command not supported<br>■ Command for applications with automatic tag detection not supported<br>■ Command only supported for applications with automatic tag detection<br>■ Password function not supported by the UHF reader<br>■ Command not supported by the UHF reader version |
| NOT_SUPPORTED_BY_TAG | Command or parameter are not supported by the tag. | ■ Password function of the tag not supported<br>■ Command for multitag application with automatic tag detection not supported<br>■ Command not supported for multitag application |
| DEVICE_NOT_READY | Device is not operational | ■ UHF reader is encountering an issue |
| INVALID_CONFIGURATION | Device configuration invalid | ■ Parameter undefined<br>■ **Bypass time** parameter outside of the permissible range<br>■ Value for timeout outside of the permissible range<br>■ Error in parameterization of UHF reader |
| RF_COMMUNICATION_ERROR | Error during communication between the read/write device and tag | ■ Air interface error<br>■ Air interface error: CRC error<br>■ Air interface error: Timeout<br>■ Air interface error: UHF tag error |
| DEVICE_FAULT | Hardware error in the connected device | ■ UHF reader not connected |

### 9.4.2 Calling channel and module diagnostic messages in the web server

#### Diagnostic Messages — Module Status

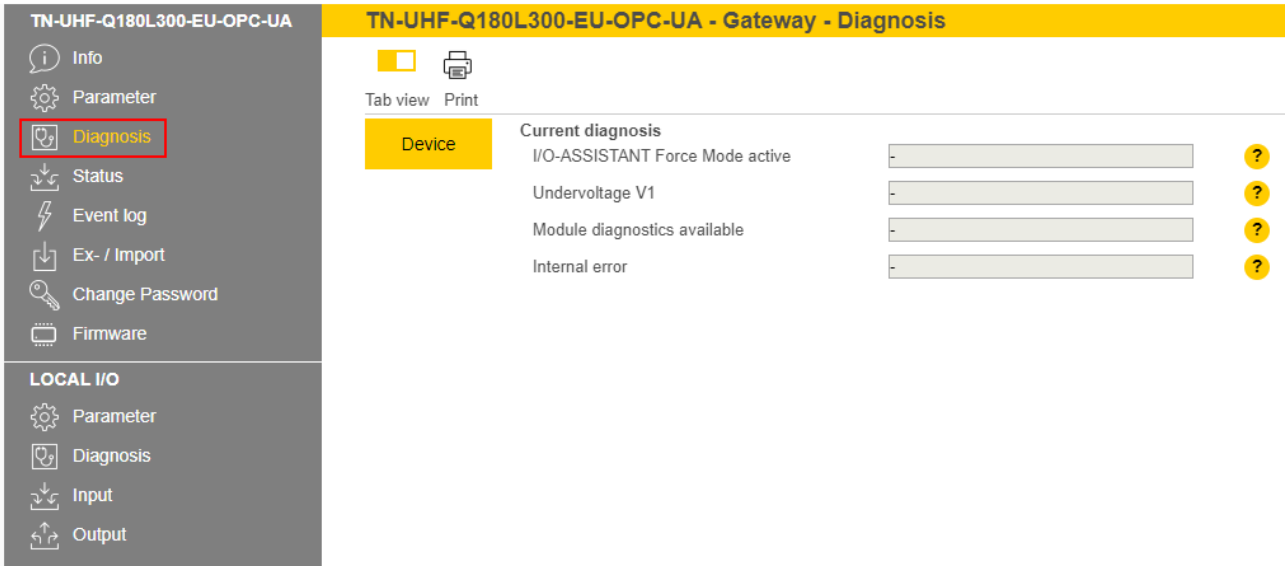



Fig. 58: Web server — module status diagnostics

| Status message | Description |
|---|---|
| I/O-ASSISTANT Force Mode active | DTM active in force mode |
| Undervoltage V1 | Undervoltage V1 |
| Module diagnostics available | Module diagnostics available |
| Internal error | Internal error |

## Diagnostic Messages — RFID Channels

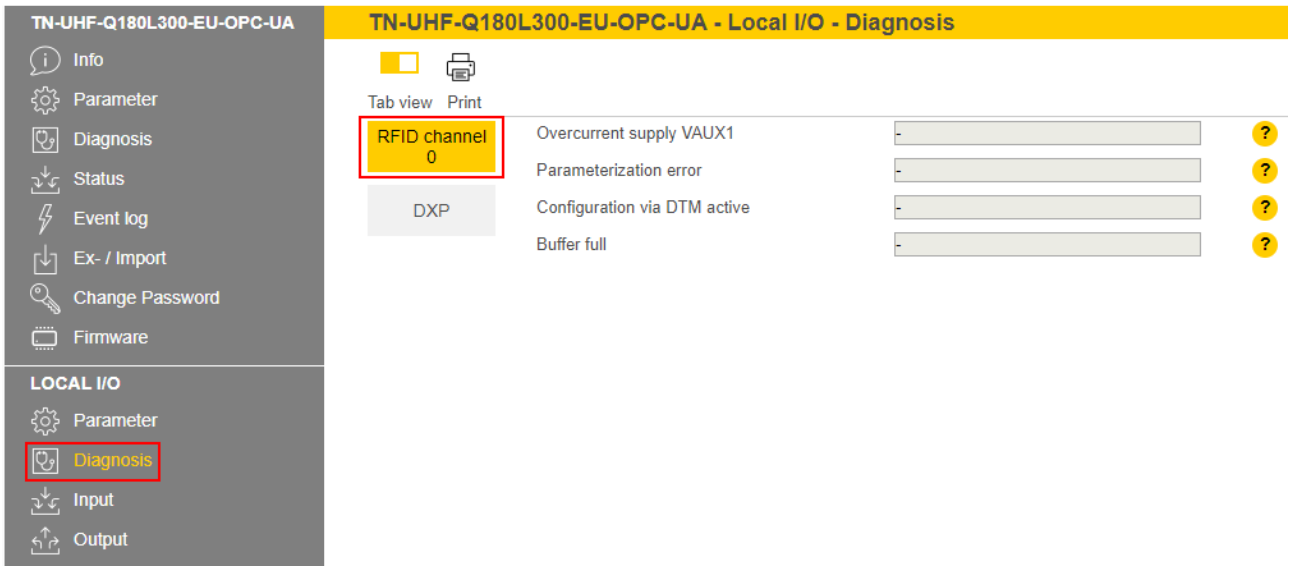



Fig. 59: Web server — RFID channel diagnostics

| Diagnostics | Description |
|---|---|
| Overcurrent supply VAUX1 | Overcurrent VAUX 1 |
| Parameterization error | Parameterization error |
| Configuration via DTM active | Configuration via DTM active |
| Buffer full | Buffer full |

## Diagnostic messages — DXP channels

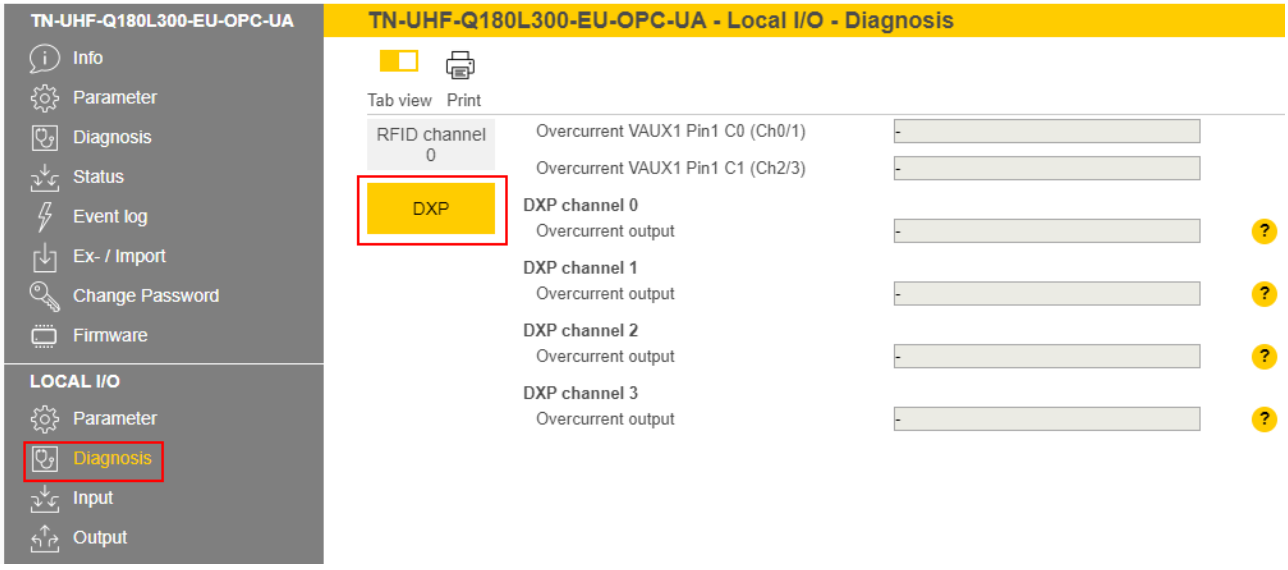



Fig. 60: Web server — DXP channel diagnostics

| Diagnostics | Description |
|---|---|
| Overcurrent output | Overcurrent at output |

## 9.5 Reset device (Reset)

**NOTE**
There are two ways to reset the device.

### Resetting the device without resetting the OPC UA server

✓ No preparation required.

▶ Perform a reset directly via the TAS or the web server.

### Restarting the device by performing a power reset, including resetting the OPS UA server

▶ Restart the device by performing a power reset.

⇨ This ensures that the user has physical access to the device.

▶ Perform a reset via the TAS or the web server within 60 seconds.

# 10 Troubleshooting

Proceed as follows if the device does not operate as expected:

- Exclude environmental interference.
- Check the terminals of the device for faults.
- Check the device for parameter errors.

A device fault is present if the malfunction continues. In this case, decommission the device and replace it with a new device of the same type.

## 10.1 Rectifying errors

Errors are displayed by an ERR LED lit red on the device.

### Calling fault signals in the web server and rectifying them

**NOTE**
Contact TURCK if the error persists after the device is reset.

- Log in to the web server (see page Editing settings in the web server).
- Click **Diagnostics** in the navigation bar on the left of the screen.

⇨ The fault signals are displayed in the device status.

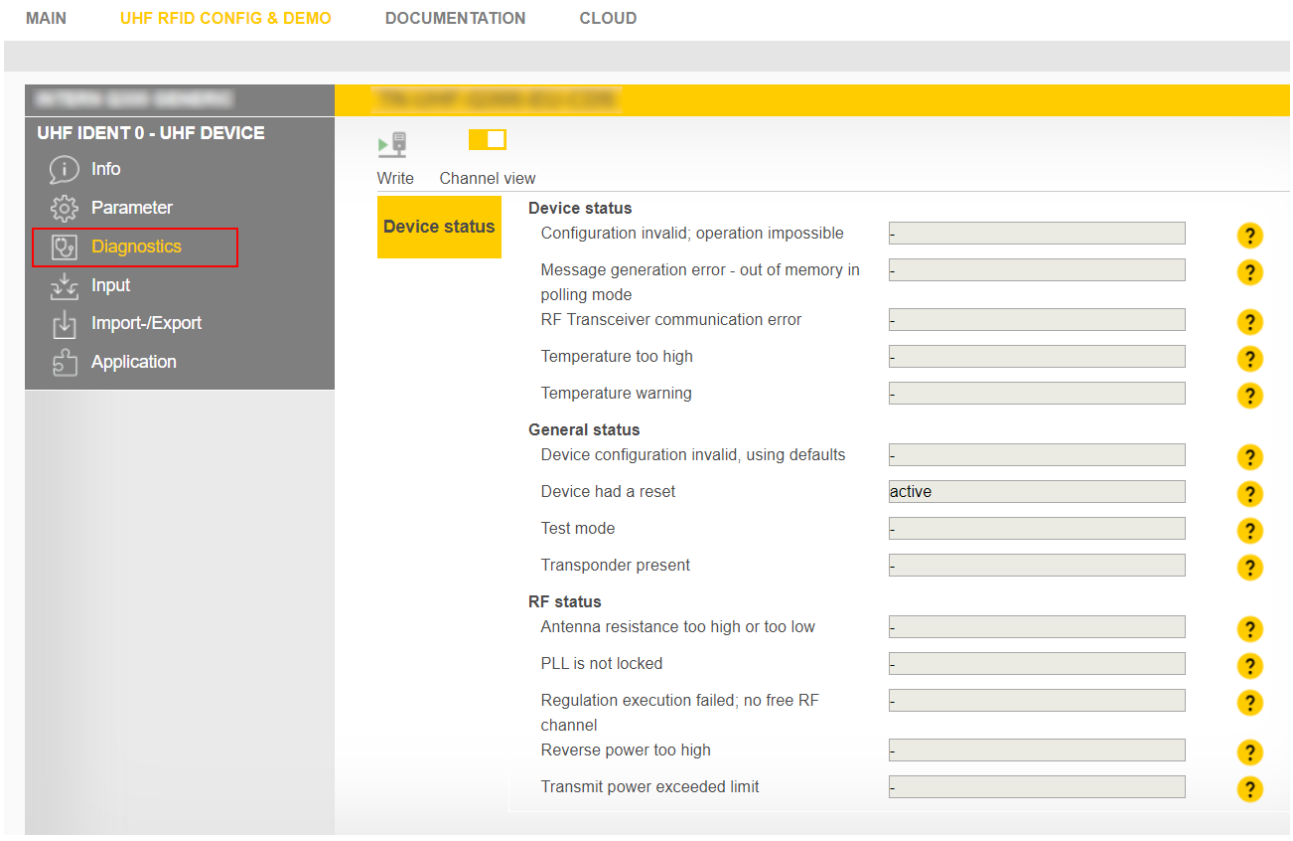



Fig. 61: Web server – Diagnostics

Rectifying fault signals:

- ▶ Click **Local I/O → Output** in the navigation bar on the left of the screen.
- ▶ Select **RFID control/status ch0**.
- ▶ Select the Reset command via the **Command code** drop-down menu: **0x8000 Reset**
- ⇨ The device is reset.

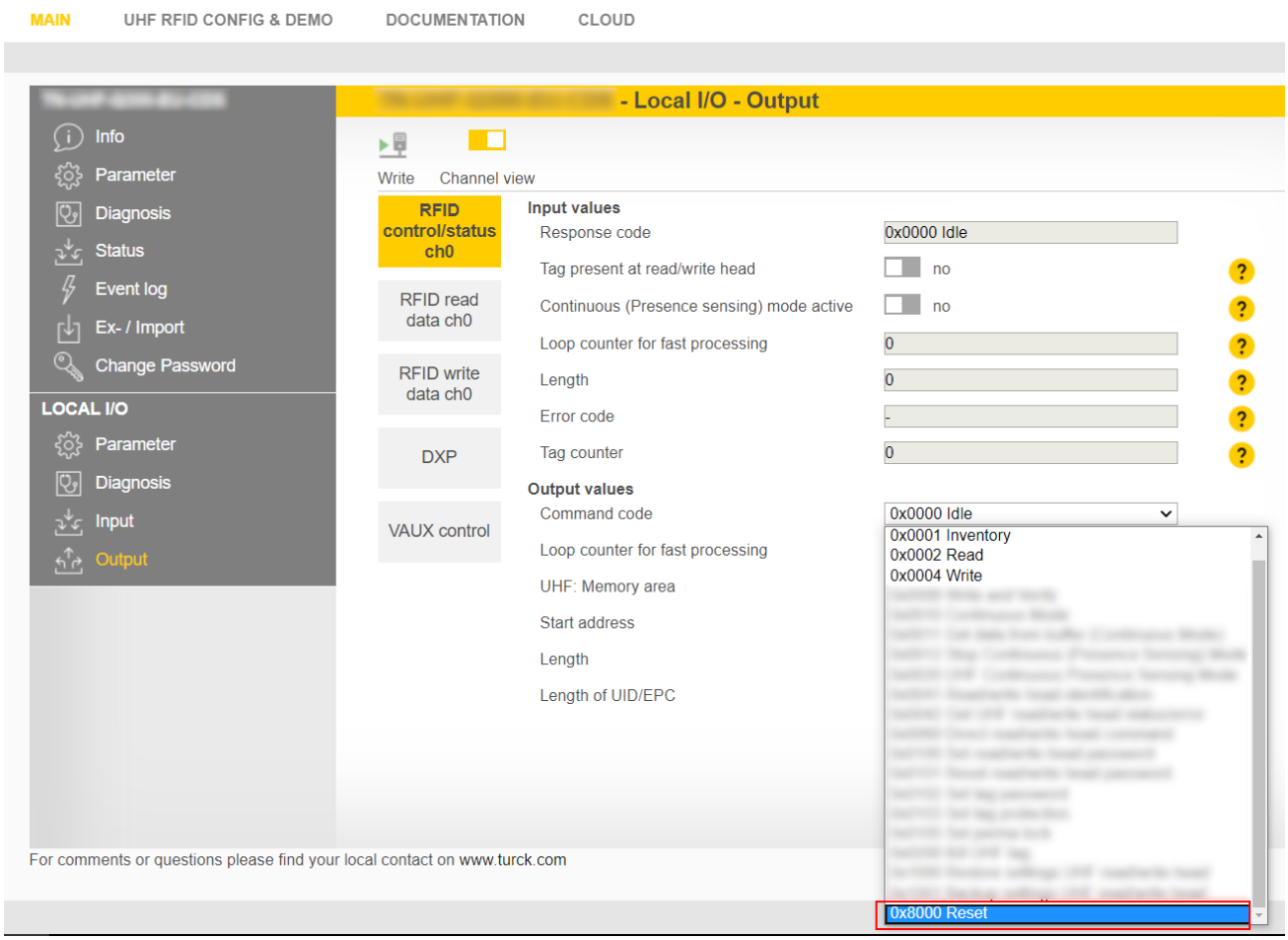



Fig. 62: Web server — reset the device

# 11 Maintenance

## 11.1 Updating the firmware via TAS

**NOTICE**
Interruption of the power supply during the firmware update
**Risk of device damage due to faulty firmware update**
- ▶ Do not interrupt the power supply during the firmware update.
- ▶ During the firmware update do not reset the power supply.
- ▶ Do not interrupt the Ethernet connection during the firmware update.

**NOTE**
The firmware update function in TAS is locked when the controller connection is active. The device must first be disconnected from the controller before performing the update.

### Starting a firmware update for a device

- ▶ Open TAS.
- ▶ Open the network view and scan the network.
- ▶ Select the device.
- ▶ Click **Firmware update**.
- ▶ In the following dialog: Click **Select file** and open the directory of the firmware file.
- ▶ Select the new firmware file and load it via **Open**.
- ▶ Click **Start** to start the firmware update.
- ▶ Enter the device password and click **Login**

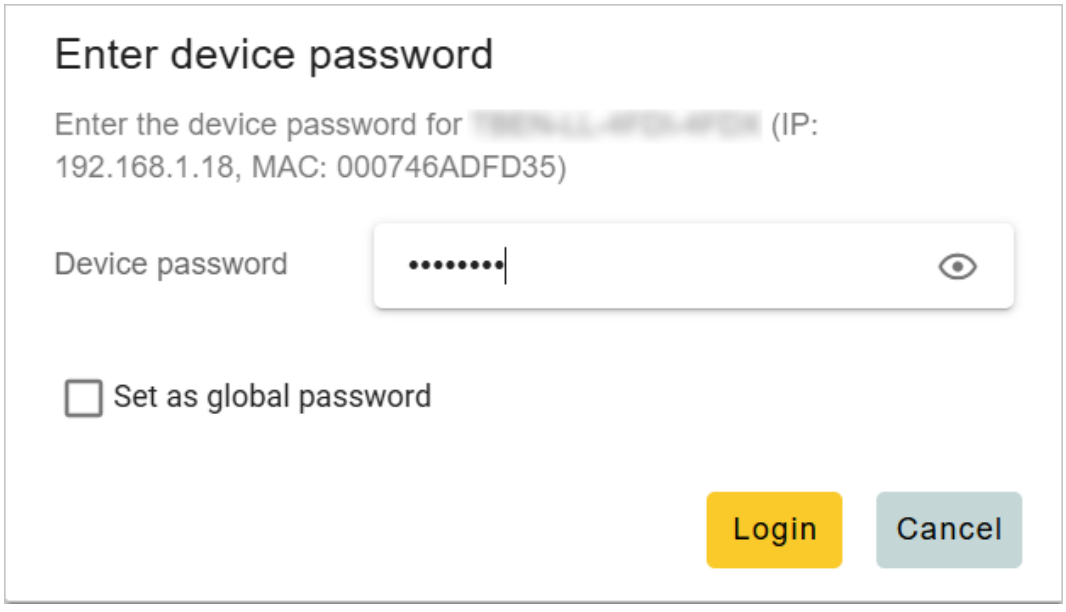



Fig. 63: Entering the device password

⇨ The progress of the firmware update is displayed.

**NOTE**
TAS makes it possible to set a global password with which all devices can be unlocked. This requires that all selected devices have the same device password and are in the same TCP network.

As an alternative to selecting a single device, it is also possible to select multiple devices. To do so, all devices to be updated must correspond to the same device type and be in the same TCP network.

This enables a firmware update to be performed for multiple devices at once.

### Starting a firmware update for multiple devices

- Select all desired devices in the network view using the checkbox.
- Click **FW Update** in the header.

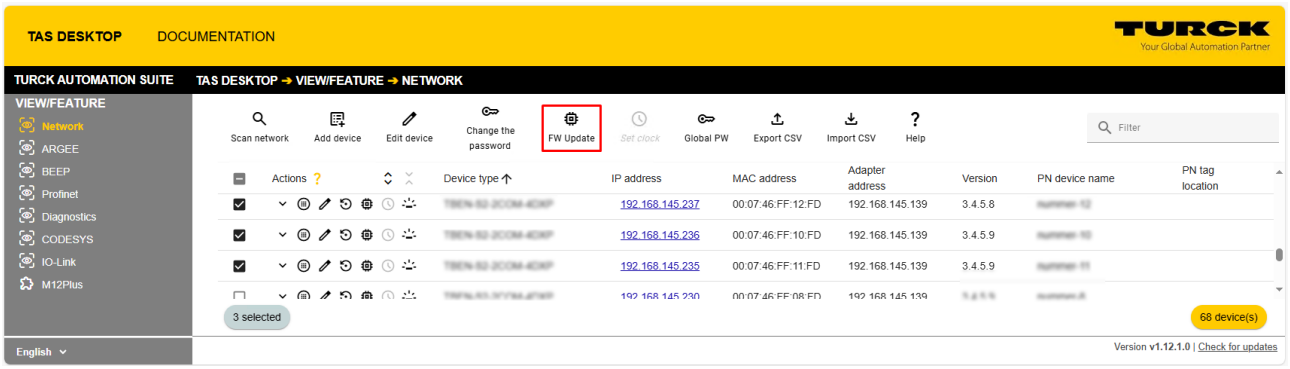


Fig. 64: Firmware update network view multiple devices

- In the following dialog: Click **Select file** and open the directory of the firmware file.
- Select the new firmware file and load it via **Open**.
- Click **Start** to start the firmware update.
- If a global password has not yet been defined: Enter the password and activate the **Set as global password** option.
  Note: If a global password has not yet been defined and the **Set as global password** option is not activated, the password is requested individually for each device.
- Click **Login**.

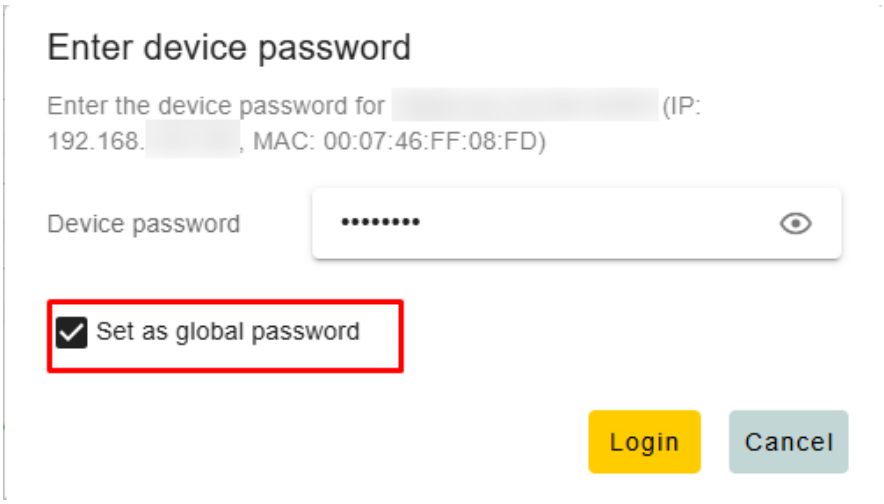


Fig. 65: Entering the device password and setting it as global password

⇨ The progress of the firmware update is displayed.

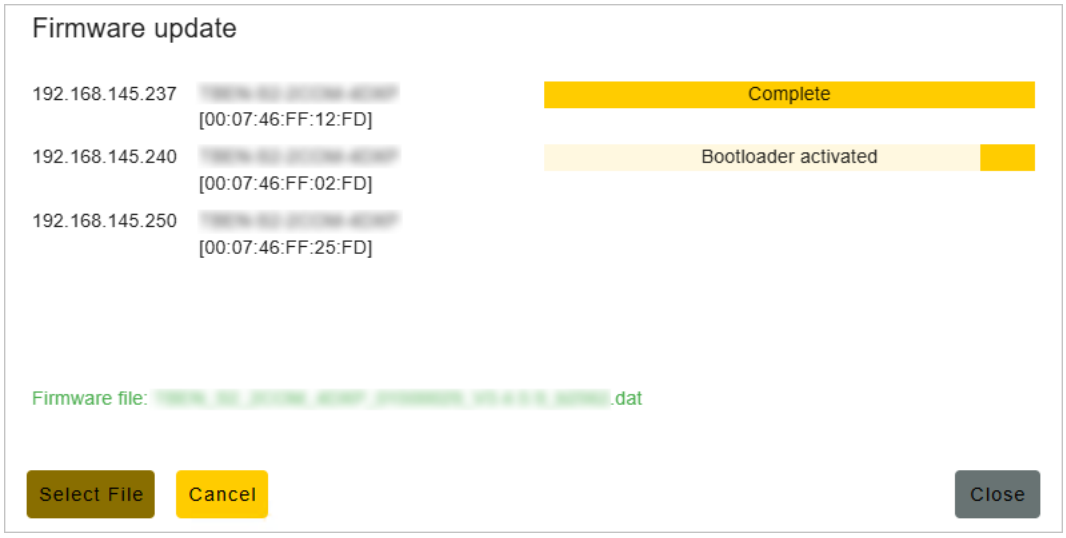



Fig. 66: Firmware update, progress

## 11.2 Updating the firmware via web server

**NOTICE**
Interruption of the power supply during the firmware update
**Risk of device damage due to faulty firmware update**

- ▶ Do not interrupt the power supply during the firmware update.
- ▶ During the firmware update do not reset the power supply.
- ▶ Do not interrupt the Ethernet connection during the firmware update.

- ▶ Open the web server.
- ▶ Log into the device as administrator. The default password for the web server is "password".
- ▶ Click **Firmware** → **SELECT FIRMWARE FILE**.
- ▶ Select a new firmware file and load it by clicking **Open**.

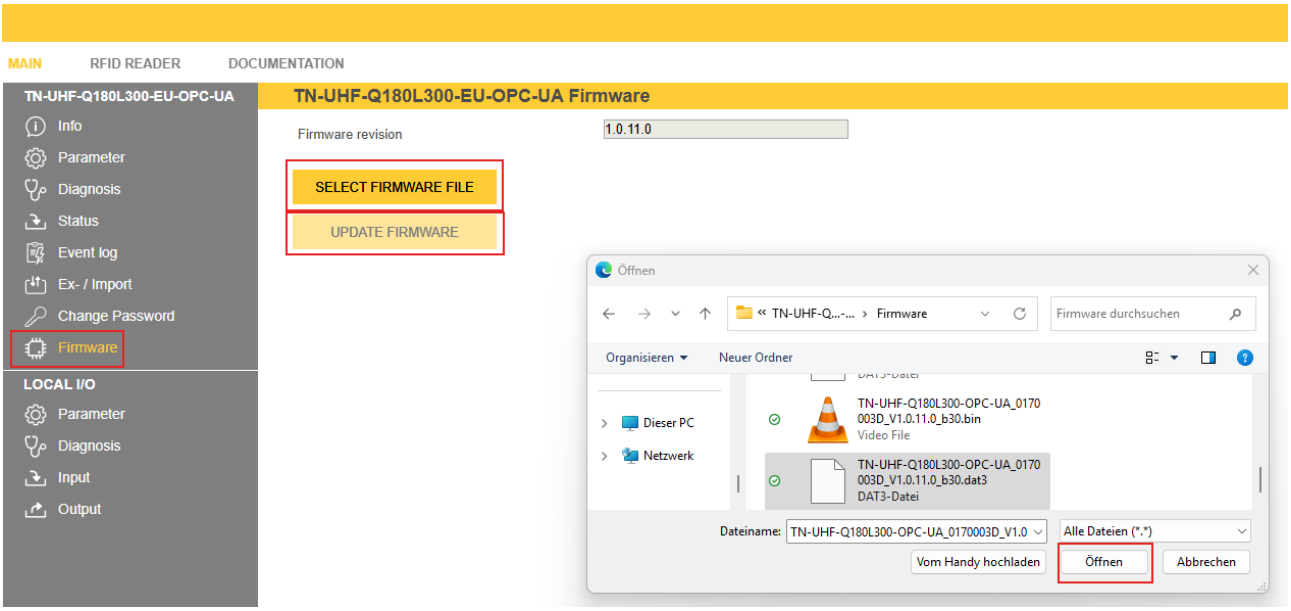



Fig. 67: Web server — firmware update

- ▶ Click **UPDATE FIRMWARE** and start the firmware update.
- ▶ Restart the device after the update process is complete by clicking **OK**.

# 12 Repair

The device is not intended for repair by the user. The device must be decommissioned if it is faulty. Observe our return acceptance conditions when returning the device to TURCK.

## 12.1 Returning devices

If a device has to be returned, bear in mind that only devices with a decontamination declaration will be accepted. This is available for download at
**https://www.turck.de/en/return-service-6079.php**
and must be completely filled in, and affixed securely and weather-proof to the outside of the packaging.

# 13 Disposal

The devices must be disposed of properly and do not belong in the domestic waste.

# 14 Technical data

| Technical data | |
|---|---|
| **Electrical data** | |
| Operating voltage | 18…30 VDC |
| DC rated operational current | ≤ 3500 mA |
| Data transfer | Electromagnetic AC field |
| Technology | UHF RFID |
| Radio communication and protocol standards | ISO 18000-63<br>EPCglobal Gen 2 |
| Antenna polarization | Circular/linear, adjustable |
| Antenna HPBW | 65° |
| Output function | Read/write |
| **Mechanical data** | |
| Mounting condition | Non-flush |
| Ambient temperature | -20…+50 °C |
| Design | Rectangular |
| Dimensions | 300 × 300 × 61.7 mm |
| Housing material | Aluminum, AL, silver |
| Material of active face | Fiber glass reinforced polyamide, PA6-GF30, black |
| Vibration resistance | 55 Hz (1 mm) |
| Shock resistance | 30 g (11 ms) |
| Protection class | IP67 |
| Electrical connection | RP-TNC |
| Input impedance | 50 ohm |
| MTTF | 49 years acc. to SN 29500 (Ed. 99) 20 °C |
| **System description** | |
| Processor | ARM Cortex A8, 32-bit, 800 MHz |
| Memory | MB Flash |
| RAM | 512 MB DDR3 |
| **System data** | |
| Ethernet transfer rate | 10/100 Mbps |
| Connection technology Ethernet | 1 × M12, 4-pin, D-coded |
| Web server | Default: 192.168.1.100 |
| **Digital inputs** | |
| Number of channels | 4 |
| Connection technology | M12, 5-pin |
| Input type | PNP |
| Switching threshold | EN 61131-2 Type 3, PNP |
| Low-level signal voltage | < 5 V |
| High-level signal voltage | >11 V |
| Low-level signal current | < 1.5 mA |
| High-level signal current | > 2 mA |

| Technical data | |
|---|---|
| Type of input diagnostics | Channel diagnostics |
| **Digital outputs** | |
| Number of channels | 4 |
| Connection technology | M12, 5-pin |
| Output type | PNP |
| Type of output diagnostics | Channel diagnostics |

# 15 TURCK branches — contact data

| | |
|---|---|
| **Germany** | TURCK GmbH<br>Witzlebenstraße 7, 45472 Mülheim an der Ruhr<br>www.turck.de |
| **Australia** | Turck Australia Pty Ltd<br>Building 4, 19-25 Duerdin Street, Notting Hill, 3168 Victoria<br>www.turck.com.au |
| **Austria** | Turck GmbH<br>Graumanngasse 7/A5-1, A-1150 Vienna<br>www.turck.at |
| **Belgium** | Turck Multiprox N. V.<br>Lion d'Orweg 12, B-9300 Aalst<br>www.multiprox.be |
| **Brazil** | Turck do Brasil Automação Ltda.<br>Rua Anjo Custódio Nr. 42, Jardim Anália Franco, CEP 03358-040 São Paulo<br>www.turck.com.br |
| **Canada** | Turck Canada Inc.<br>140 Duffield Drive, CDN-Markham, Ontario L6G 1B5<br>www.turck.ca |
| **China** | Turck (Tianjin) Sensor Co. Ltd.<br>18,4th Xinghuazhi Road, Xiqing Economic Development Area, 300381 Tianjin<br>www.turck.com.cn |
| **Czech Republic** | TURCK s.r.o.<br>Na Brne 2065, CZ-500 06 Hradec Králové<br>www.turck.cz |
| **France** | TURCK BANNER S.A.S.<br>11 rue de Courtalin Bat C, Magny Le Hongre, F-77703 MARNE LA VALLEE Cedex 4<br>www.turckbanner.fr |
| **Hungary** | TURCK Hungary kft.<br>Árpád fejedelem útja 26-28., Óbuda Gate, 2. em., H-1023 Budapest<br>www.turck.hu |
| **India** | TURCK India Automation Pvt. Ltd.<br>401-403 Aurum Avenue, Survey. No 109 /4, Near Cummins Complex, Baner-Balewadi Link Rd., 411045 Pune - Maharashtra<br>www.turck.co.in |
| **Italy** | TURCK BANNER S.R.L.<br>Via San Domenico 5, IT-20008 Bareggio (MI)<br>www.turckbanner.it |
| **Japan** | TURCK Japan Corporation<br>ISM Akihabara 1F, 1-24-2, Taito, Taito-ku, 110-0016 Tokyo<br>www.turck.jp |

| | |
|---|---|
| **Korea** | Turck Korea Co, Ltd.<br>A605, 43, Iljik-ro, Gwangmyeong-si<br>14353 Gyeonggi-do<br>www.turck.kr |
| **Malaysia** | Turck Banner Malaysia Sdn Bhd<br>Unit A-23A-08, Tower A, Pinnacle Petaling Jaya, Jalan Utara C,<br>46200 Petaling Jaya Selangor<br>www.turckbanner.my |
| **Mexico** | Turck Comercial, S. de RL de CV<br>Blvd. Campestre No. 100, Parque Industrial SERVER, C.P. 25350 Arteaga,<br>Coahuila<br>www.turck.com.mx |
| **Netherlands** | Turck B. V.<br>Ruiterlaan 7, NL-8019 BN Zwolle<br>www.turck.nl |
| **Poland** | TURCK sp.z.o.o.<br>Wroclawska 115, PL-45-836 Opole<br>www.turck.pl |
| **Romania** | Turck Automation Romania SRL<br>Str. Siriului nr. 6-8, Sector 1, RO-014354 Bucuresti<br>www.turck.ro |
| **Sweden** | Turck AB<br>Fabriksstråket 9, 433 76 Jonsered<br>www.turck.se |
| **Singapore** | TURCK BANNER Singapore Pte. Ltd.<br>25 International Business Park, #04-75/77 (West Wing) German Centre,<br>609916 Singapore<br>www.turckbanner.sg |
| **South Africa** | Turck Banner (Pty) Ltd<br>Boeing Road East, Bedfordview, ZA-2007 Johannesburg<br>www.turckbanner.co.za |
| **Turkey** | Turck Otomasyon Ticaret Limited Sirketi<br>Inönü mah. Kayisdagi c., Yesil Konak Evleri No: 178, A Blok D:4,<br>34755 Kadiköy/ Istanbul<br>www.turck.com.tr |
| **United Kingdom** | TURCK BANNER LIMITED<br>Blenheim House, Hurricane Way, GB-SS11 8YT Wickford, Essex<br>www.turckbanner.co.uk |
| **USA** | Turck Inc.<br>3000 Campus Drive, USA-MN 55441 Minneapolis<br>www.turck.us |

TURCK

Your Global Automation Partner

Over 30 subsidiaries and
60 representations worldwide!

100003070 | 2025/09

www.turck.com