Your Global Automation Partner

TURCK

TBEN-L5-4RFID-8DXP-OPC-UA

Compact RFID Interface

Instructions for Use

Contents

1 About these instructions

These instructions for use describe the structure, functions and the use of the product and will help you to operate the product as intended. Read these instructions carefully before using the product. This is to avoid possible damage to persons, property or the device. Retain the instructions for future use 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 personnel and must be carefully read by anyone mounting, commissioning, operating, maintaining, dismantling or disposing of the device.

When operating the device in a hazardous area, the user must have a working knowledge of explosion protection (EN 60079-14, etc.).

1.2 Explanation of symbols used

The following symbols are used in these instructions:

⚠	**DANGER** DANGER indicates a dangerous situation with high risk of death or severe injury if not avoided.
⚠	**WARNING** WARNING indicates a dangerous situation with medium risk of death or severe injury if not avoided.
⚠	**CAUTION** CAUTION indicates a dangerous situation of medium risk which may result in minor or moderate injury if not avoided.
❗	**NOTICE** NOTICE indicates a situation which may lead to property damage if not avoided.
ℹ	**NOTE** NOTE indicates tips, recommendations and useful information on specific actions and facts. The notes simplify your work and help you to avoid additional work.
▶	**CALL TO ACTION** This symbol denotes actions that the user must carry out.
⇨	**RESULTS OF ACTION** This symbol denotes relevant results of actions.

1.3 Other documents

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

- Data sheet
- Instructions for use
- Declarations of conformity (current versions)
- Approvals

1.4 Naming convention

Read/write devices are called “read/write heads” for the HF range and “readers” for the UHF range. Common synonyms for “data carriers” are “tags”, “transponders” and “mobile data memory”.

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 compact RFID interfaces:

- TBEN-L5-4RFID-8DXP-OPC-UA

2.2 Scope of delivery

The scope of delivery includes:

- Compact RFID interface
- Closure caps for M12 connectors
- Quick Start Guide

2.3 Legal requirements

The device falls under the following EU directives:

- 2014/30/EU (electromagnetic compatibility)
- 2011/65/EU (RoHS directive)
- 2014/34/EU (ATEX directive)

2.4 Turck service

Turck supports you with your projects, from initial analysis to the commissioning of your application. The Turck product database under www.turck.com contains software tools for programming, configuration or commissioning, data sheets and CAD files in numerous export formats.

The contact details of Turck subsidiaries worldwide can be found on p. [▸ 118].

2.5 Exclusion of liability

Only a functioning IT security concept can ensure the security of the data for the entire installation in which the device is used. Turck does not accept any liability in the event that third parties access data transferred with the device.

3 For your safety

The product is designed according to state-of-the-art technology. However, residual risks still exist. Observe the following warnings and safety notices to prevent damage to persons and property. Turck accepts no liability for damage caused by failure to observe these warning and safety notices.

3.1 Intended use

The TBEN-L5-4RFID-8DXP-OPC block module is an RFID interface for use in the Turck RFID system. The Turck RFID system is used for the contactless exchange of data between a tag and a read/write device in object identification applications. I/O data can also be processed via the digital channels.

The device supports the HF read/write heads from firmware version Vx.90 and UHF readers from firmware version FW 1.45.

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

Installation directly in the field is possible thanks to degree of protection IP67. The devices are suitable for operation in hazardous areas in Zone 2 and Zone 22.

The devices may 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 may only be assembled, installed, operated, parameterized and maintained by professionally-trained personnel.
- The device may only be used in accordance with applicable national and international regulations, standards and laws.
- The device meets the EMC requirements for industrial areas. When used in residential areas, take measures to avoid radio interference.
- Change the default password of the integrated web server after the first login. Turck recommends using a secure password.

3.3 Notes on Ex protection

- When operating the device in a hazardous area, the user must have a working knowledge of explosion protection (EN 60079-14, etc.).
- Observe national and international regulations for explosion protection.
- Use the device only within the permissible operating and ambient conditions (see approval data and Ex approval specifications).

3.4 Ex approval requirements for use in Ex area

- Only use the device in an area with no more than pollution degree 2.
- Only disconnect and connect circuits when no voltage is applied.
- Only operate the switches if no voltage is present.
- Connect the metal protective cover to the equipotential bonding in the Ex area.
- Ensure impact resistance in accordance with EN IEC 60079-0 – alternative measures:
  - Install the device in the TB-SG-L protective housing (available in the set with Ultem window: ID 100014865) and replace the service window with an Ultem window.
  - Install the device in an area offering impact protection (e.g. in robot arm) and attach a warning: "DANGER: Only connect and disconnect circuits when no voltage is present. Do not operate switches when energized."
- Do not install the device in areas critically exposed to UV light.
- Prevent risks caused by electrostatic charge.
- Protect unused connectors with dummy plugs to ensure protection class IP67.

3.5 Notes on UL approval

- Use UL certified PVVA or CYJV cables that are suitable for the current/voltage rating and have an insulation temperature of at least 90 °C.

4 Product description

The device is designed with a fully encapsulated housing with degree of protection IP67/IP69K. Four RFID channels are provided for connecting read/write devices. Sensors and actuators can also be connected via eight digital I/O channels. The digital I/O channels can be configured as inputs or outputs as required. The terminals for the read/write devices and for digital I/Os are M12 sockets. Two M12 female connectors are provided for connecting to the Ethernet ports.

4.1 Device overview

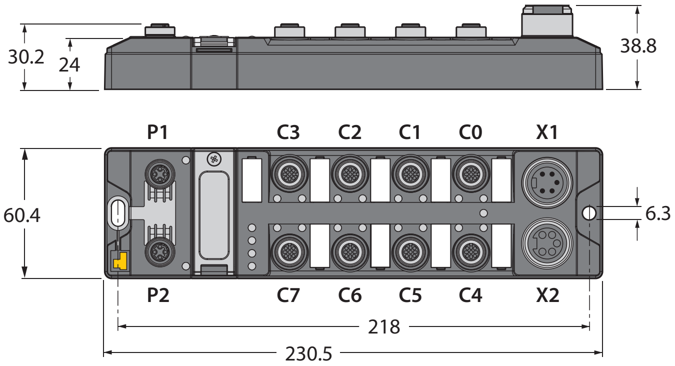


Fig. 1: Dimensions

4.1.1 Display elements

The device has the following LED indicators:

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

4.1.2 Operating elements

The device is provided with the following operating elements:

- Rotary coding switches and DIP switches for adjusting the network settings
- SET button and USB Host port (without function)

4.2 Properties and features

- Glass fiber reinforced housing
- Shock and vibration tested
- Fully encapsulated module electronics
- Degree of protection IP65/IP67/IP69K
- Integrated OPC UA server standardized according to the AutoID Companion Specification
- Calling of data via OPC UA clients
- Universal interface offers interoperability
- Supports security mechanisms and authentication
- Four channels with M12 connection for RFID
- Eight universal digital channels as 2 A PNP inputs and/or outputs
- Multiple LEDs for status display
- Integrated Ethernet switch enables line topology
- 10 Mbps/100 Mbps transfer rate

4.3 Operating principle

The RFID interfaces connect the RFID system with higher-level systems (e.g. ERP systems). The interfaces are provided with an OPC UA fieldbus interface and fieldbus-independent I/O electronics with an RFID interface. The interface signals of sensors and actuators can also be processed via eight universal digital channels.

The OPC UA interface connects the interface to the higher-level system via Ethernet. Up to four read/write devices can be connected via the RFID interfaces. During operation, the process data is exchanged between the higher-level system and RFID system. For this the integrated OPC UA server of the interface communicates with the OPC UA client of the higher-level system.

4.4 Functions and operating modes

Turck HF read/write heads and Turck UHF readers can be connected to the RFID channels. Parallel operation of HF read/write heads and UHF readers on the same device is also possible. The RFID functionality is defined in accordance with the AutoID Companion Specification and is available to the user regardless of the platform and manufacturer.

Sensors and actuators can be connected to the universal digital channels. In all, up to four 3-wire PNP sensors or four PNP DC actuators can be connected per input or output. The maximum output current per channel is 2 A. The read data is saved on the OPC UA server of the module and can be called via OPC UA clients.

4.4.1 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.

4.4.2 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.

4.4.3 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 chapter “Setting”.

The device can perform the following methods and functions:

- Scan
- ScanStart
- ScanStop
- ReadTag
- WriteTag
- KillTag (only UHF)
- LockTag
- SetTagPassword
- WriteTagID

Methods and functions in HF bus mode:

- ActivateBusHead
- DeactivateBusHead
- DeactivateAllBusHeads
- GetActivatedBusHeads
- GetConnectedBusHeadAddresses
- SetBusHeadAddress

4.4.4 HF bus mode

In HF bus mode up to 32 bus-capable read/write heads per RFID channel can be connected to the RFID module. An additional power supply may be required depending on the number and power consumption of connected read/write heads. A power consumption analysis of the connected read/write heads is required in order to determine the additional power supply required. A tool is provided at www.turck.com/hf-busmodus for calculating the power.

Every connected read/write head supplies a " **Tag present**" signal in HF bus mode. HF bus mode is suitable for static applications and very slow dynamic applications because a command can only be processed by one read/write head at a time.

The **ScanStart** method for continuous reading in HF bus mode allows a command to be performed simultaneously at all read/write heads in a bus topology. The logged data is stored in the ring memory of the module.

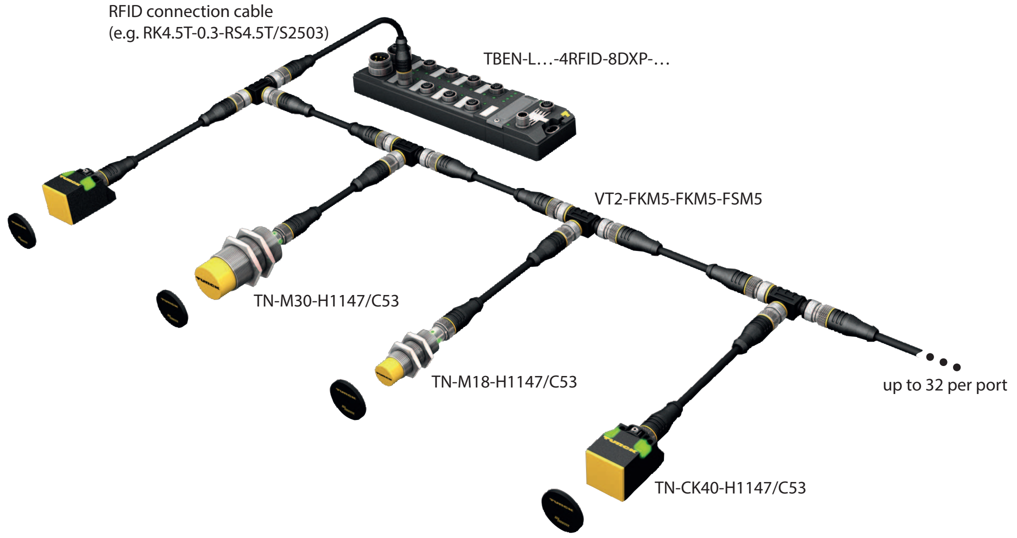


Fig. 2: HF bus mode setup

The following read/write heads can be used for HF bus mode:

- TN-M18-H1147/C53
- TB-M18-H1147/C53
- TN-M30-H1147/C53
- TB-M30-H1147/C53
- TN-CK40-H1147/C53
- TB-Q08-0.15-RS4.47T/C53
- TN-Q14-0.15-RS4.47T/C53
- TN-Q80-H1147/C53
- TN-R42TC-EX/C53
- TN-R42TC-EX/C65
- TNLR-Q80-H1147/C53
- TNSLR-Q42TWD-H1147/C53
- TNSLR-Q80WD-H1147/C53

HF bus mode supports the HF read/write heads from firmware version Vx.90.

The **ScanStart** method for continuous reading in HF bus mode supports the HF read/write heads from firmware version Vx.93.

4.4.5 Universal digital channels – functions

The device is provided with eight universal digital channels, which can be used as inputs or outputs according to the application requirements. In all, up to eight 3-wire PNP sensors or eight PNP DC actuators can be connected per input or output. The maximum output current per channel is 2 A.

4.5 Technical accessories

Accessories for mounting, connecting and parameterizing can be found in product database under **www.turck.com**. The accessories are not part of the scope of delivery.

5 Installing

5.1 Installing the device in Zone 2 and Zone 22

In Zone 2 and Zone 22, the devices can be used in conjunction with the protective housing set .

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition
For use in Zone 2 and Zone 22:

- ▶ Only install the device if there is no potentially explosive atmosphere present.
- ▶ Observe requirements for Ex approval.

- ▶ Unscrew the housing. Use Torx T8 screwdriver.
- ▶ Replace the service window with the enclosed Ultem window.
- ▶ Place the device on the base plate of the protective housing and fasten both together on the mounting plate, see [▸ 18].
- ▶ Connect the device, see [▸ 21].
- ▶ Mount and screw the housing cover according to the following figure. The tightening torque for the Torx T8 screw is 0.5 Nm.

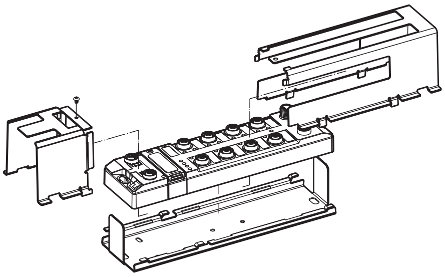


Fig. 3: Mounting the device in protection housing TB-SG-L

5.2 Mounting onto a mounting plate

NOTICE
Mounting on uneven surfaces
Device damage due to stresses in the housing
- ▶ Fix the device on a flat mounting surface.
- ▶ Use two M6 screws to mount the device.

The device can be screwed onto a flat mounting plate.

- ▶ Attach the module to the mounting surface with two M6 screws. The maximum tightening torque for the screws is 1.5 Nm.
- ▶ Avoid mechanical stresses.
- ▶ Optional: Ground the device.

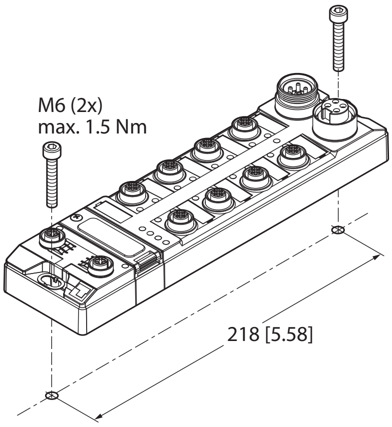


Fig. 4: Mounting the device onto a mounting plate

5.3 Mounting the device outdoors

The device is UV-resistant according to DIN EN ISO 4892-2. Direct sunlight can cause material abrasion and color changes. The mechanical and electrical properties of the device are not affected.

- ▶ To avoid material abrasion and color changes: Protect the device from direct sunlight, e.g. by using protective shields.

5.4 Grounding the device

5.4.1 Equivalent wiring diagram and shielding concept

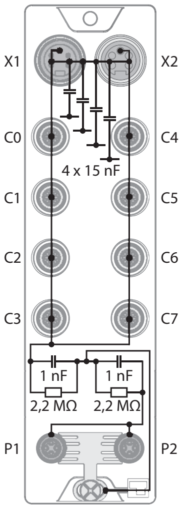


Fig. 5: TBEN-L5-4RFID-8DXP-OPC-UA – equivalent wiring diagram and shielding concept

5.4.2 Shielding of the fieldbus and I/O level

The fieldbus and the I/O level of the modules can be grounded separately.

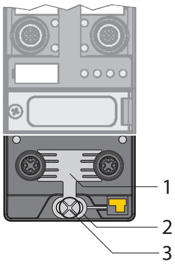


Fig. 6: Grounding clip (1), grounding ring (2) and metal screw (3)

The grounding ring (2) is the module grounding. The shielding of the I/O level is permanently connected to the module grounding. The module grounding is only connected to the reference potential of the installation when the module is mounted.

I/O level shielding

In the case of direct mounting on a mounting plate, the module grounding is connected to the reference potential of the system via the metal screw in the lower mounting hole (3). If module grounding is not desired, the electrical connection to the reference potential must be interrupted, e.g. by using a plastic screw.

Fieldbus level shielding

The grounding of the fieldbus level can either be connected directly via the grounding clip (1) or connected and routed indirectly via an RC element to the module grounding. If the grounding is to be routed via an RC element, the grounding clip must be removed.

In the delivery state, the grounding clip is mounted.

5.4.3 Disconnecting the direct grounding of the fieldbus level: removing the grounding clip

- ▶ Use a flat screwdriver to slide the grounding clip forward and remove it.

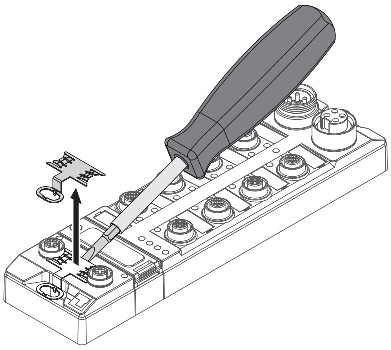


Fig. 7: Use a flat slotted screwdriver to push the grounding clip forwards and remove it.

5.4.4 Grounding the fieldbus level directly: inserting the grounding clip

- ▶ Place the grounding clip between the fieldbus connectors by using a screwdriver in such way that the clip contacts the metal housing of the connectors.
- ▶ The shielding of the fieldbus cables is connected to the grounding clip.

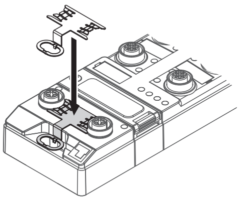


Fig. 8: Mounting the grounding clip

5.4.5 Grounding the device – mounting on a mounting plate

- ▶ For mounting onto a mounting plate: Fix the device with a metal screw through the lower mounting hole.
- ➪ The module grounding is connected to the reference potential of the installation via the metal screw.
- ➪ With mounted grounding clip: The shielding of the fieldbus and the module grounding are connected to the reference potential of the installation.

6 Connection

NOTICE
Intrusion of liquids or foreign bodies through leaking connections
Loss of protection class IP65/IP67/IP69K, device damage possible

- Tighten M12 connectors with a tightening torque of 0.6 Nm.
- Tighten 7/8″ connectors with a tightening torque of 0.8 Nm.
- Only use accessories that guarantee the protection class.
- Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

6.1 Connecting the device in Zone 2 and Zone 22

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition
When used in Zone 2 and Zone 22:

- Only disconnect and connect circuits when no voltage is applied.
- Only use connecting cables that are approved for use in potentially explosive atmospheres.
- Use all connectors or seal them with blind plugs.
- Observe requirements for Ex approval.

6.2 Connecting the modules to Ethernet

The device is provided with an integrated autocrossing switch with two 4-pin M12 Ethernet male connectors for connecting to an Ethernet system. The maximum tightening torque is 0.6 Nm.

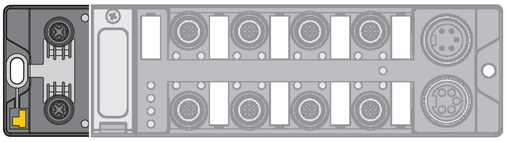


Fig. 9: M12 Ethernet male connectors for connecting the fieldbus

- Connect the device to the fieldbus according to the pin assignment below.
- Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

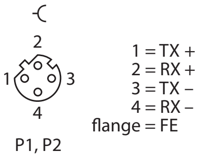


Fig. 10: Pin assignment of the Ethernet connections

6.3 Connecting the power supply

The device is provided with two 7/8" male connectors for connecting the power supply. These are 5-pin connectors. V1 and V2 are electrically isolated from each other. The maximum tightening torque is 0.8 Nm.

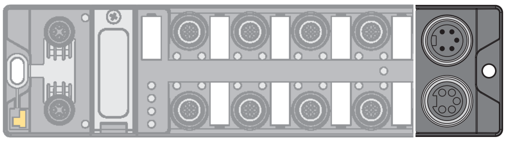


Fig. 11: TBEN-L5... – 7/8" male connector for connecting the power supply

- Connect the device to the power supply according to the pin assignment below.
- Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

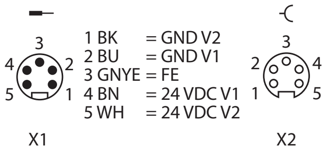


Fig. 12: TBEN-L5… – pin assignment of the power supply connections

Connector	Function
X1	Power feed
X2	Continuation of the power to the next node

Voltage	Function
V1	System voltage: power supply 1 (incl. supply of electronics)
V2	Load voltage: power supply 2

NOTE

The system voltage (V1) and the load voltage (V2) are supplied and monitored separately. If the voltage goes below the permissible lower limit, the sockets are disconnected according to the supply concept of the module type. If V2 goes below the permissible minimum voltage, PWR LED changes from green to red. If V1 goes below the permissible minimum, the PWR LED goes out.

6.4 Connecting RFID read/write devices

The device has four 5-pin M12 male connectors for connecting RFID read/write devices. The maximum tightening torque is 0.6 Nm.

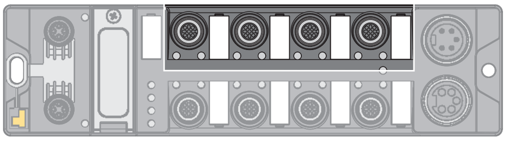
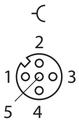


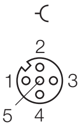
Fig. 13: M12 male connectors for connecting RFID read/write devices

- ▶ Connect the read/write devices to the device as per the pin assignment shown below.
- ▶ Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.



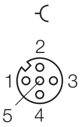
1 = $V_{aux}1$
2 = Data B
3 = GND V1
4 = Data A
5 = FE/Shield

Fig. 14: RS485 – pin assignment of the read/write device connections



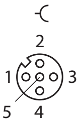
1 = BN (+)
2 = BK (Data)
3 = BU (GND)
4 = WH (Data)
5 = shield

Fig. 15: …/S2500 connection cables – pin assignment of the read/write device connections



1 = BN (+)
2 = WH (Data)
3 = BU (GND)
4 = BK (Data)
5 = shield

Fig. 16: …/S2501 connection cables – pin assignment of the read/write device connections



1 = RD (+)
2 = BU (Data)
3 = BK (GND)
4 = WH (Data)
5 = shield

Fig. 17: …/S2503 connection cables – pin assignment of the read/write device connections

6.4.1 Connecting read/write heads for the HF bus mode

In HF bus mode up to 32 bus-capable read/write heads per RFID channel can be connected to the device. The user must determine by means of a power consumption analysis whether an additional power supply is required for the connected read/write heads (see information in the data sheet or tool at www.turck.com/hf-busmodus).

The maximum permissible length of the bus is 50 m.

Connecting read/write heads for HF bus mode in the non-Ex area

The following accessories are required for the bus mode in the non-Ex area:

- The VT2-FKM5-FKM5-FSM5 (ID 6930573) junction box for connecting several read/write heads to an RFID channel
- RSE57-TR2/RFID bus terminating resistor (ID 6934908)
- Optional: VB2-FKM5-FSM5.205-FSM5.305/S2550 junction box (ID 6936821) for feeding in an additional power supply
- RFID connection cables (e.g. RK4.5T-0.3-RS4.5T/S2503)

▶ Connect the read/write head as per the figure below. The maximum length of the spur line is 2 m.

▶ Take the power supply into account, particularly at switch-on (see data sheet), as well as the maximum current carrying capacity of the lines (4 A).

▶ Take the voltage drop on the line into account. If necessary, provide an additional power supply between the read/write heads using junction box VB2-FKM5-FSM5.205-FSM5.305/S2550.

▶ Connect a terminating resistor (e.g. RSE57-TR2/RFID) behind the last read/write head.

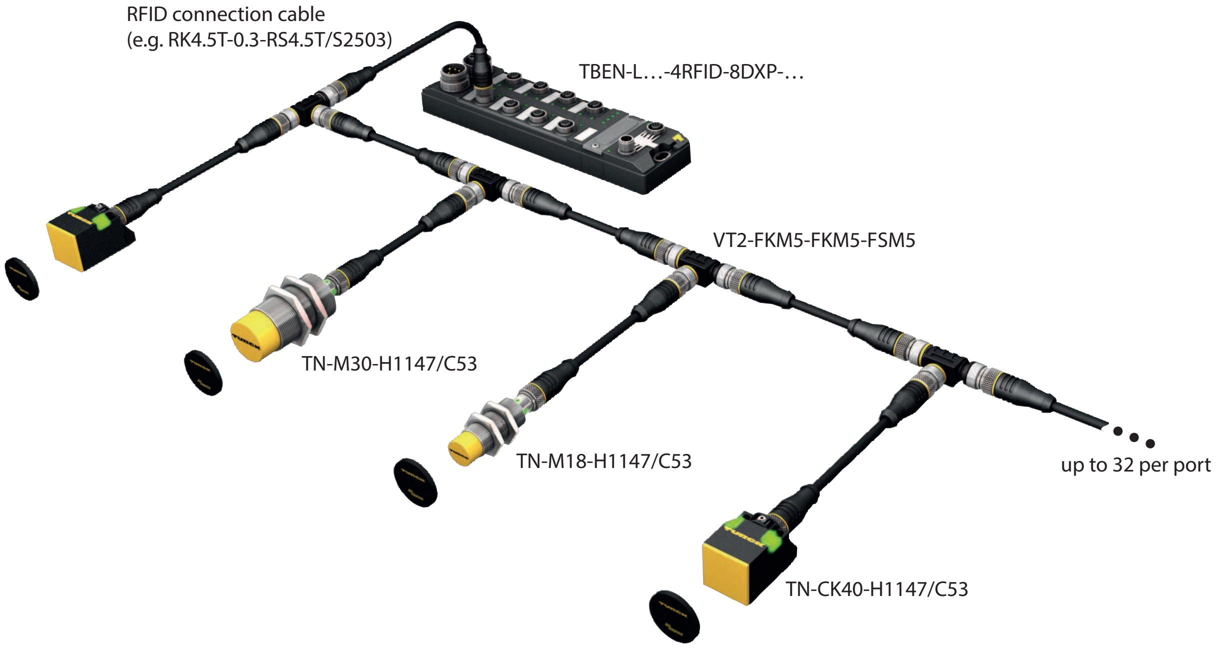


Fig. 18: HF bus mode setup

Connecting read/write heads for HF bus mode in the Ex area

NOTE
Information on the maximum cable lengths in the Ex area is provided in the data sheets of the connected read/write heads.

The following accessories are required for bus mode in the Ex area:

- TN-R42TC-EX/C53 read/write heads (ID 100020167)
- TN-R42TC-EX/C65 read/write head (ID 100028462) with integrated bus terminating resistor
- …/S2500 RFID connection cables
- Operation in Zone 2/22:
  - VT2-FKM5-FKM5-FSM5 (ID 6930573) junction box for connecting several read/write heads to an RFID port
  - SC-M12/3GD captive safety clip (ID 6900390)
  - Optional: VB2-FKM5-FSM5.205-FSM5.305/S2550 junction box (ID 6936821) for feeding in an additional power supply
- Operation in Zone 1/21:
  - Ex-e terminal boxes

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition
Operation in Zone 2/22:

- ▶ Only connect the read/write heads if there is no potentially explosive atmosphere present or if the device is in a de-energized state.
- ▶ Protect the M12 male connector from accidental removal during operation using safety clip SC-PM12/3GD.
- ▶ Protect the M12 male connector from mechanical damage.

DANGER
Potentially explosive atmosphere
Risk of explosion through spark ignition

- ▶ When used in Zone 1/21 observe the instructions for use of the connected devices.

- ▶ Operation in Zone 2/22: connect the read/write heads via VT2-FKM5-FKM5-FSM5 junction boxes as per the figure below (max. tightening torque see data sheet of the cable used). The maximum length of the spur line is 2 m.
- ▶ Operation in Zone 1/21: connect the read/write heads via terminal boxes as per the figure below. The maximum length of the spur line is 2 m.
- ▶ Take the power supply into account, particularly at switch-on (see data sheet), as well as the maximum current carrying capacity of the lines (4 A).
- ▶ Take the voltage drop on the line into account. When used in Zone 2/22 provide an additional power supply between the read/write heads using junction box VB2-FKM5-FSM5.205-FSM5.305/S2550. Up to 20 read/write heads can be connected without an additional power supply.
- ▶ Use the TN-R42TC-EX/C65 read/write head with an integrated bus terminating resistor as the last device. Do not connect a separate bus terminating resistor.

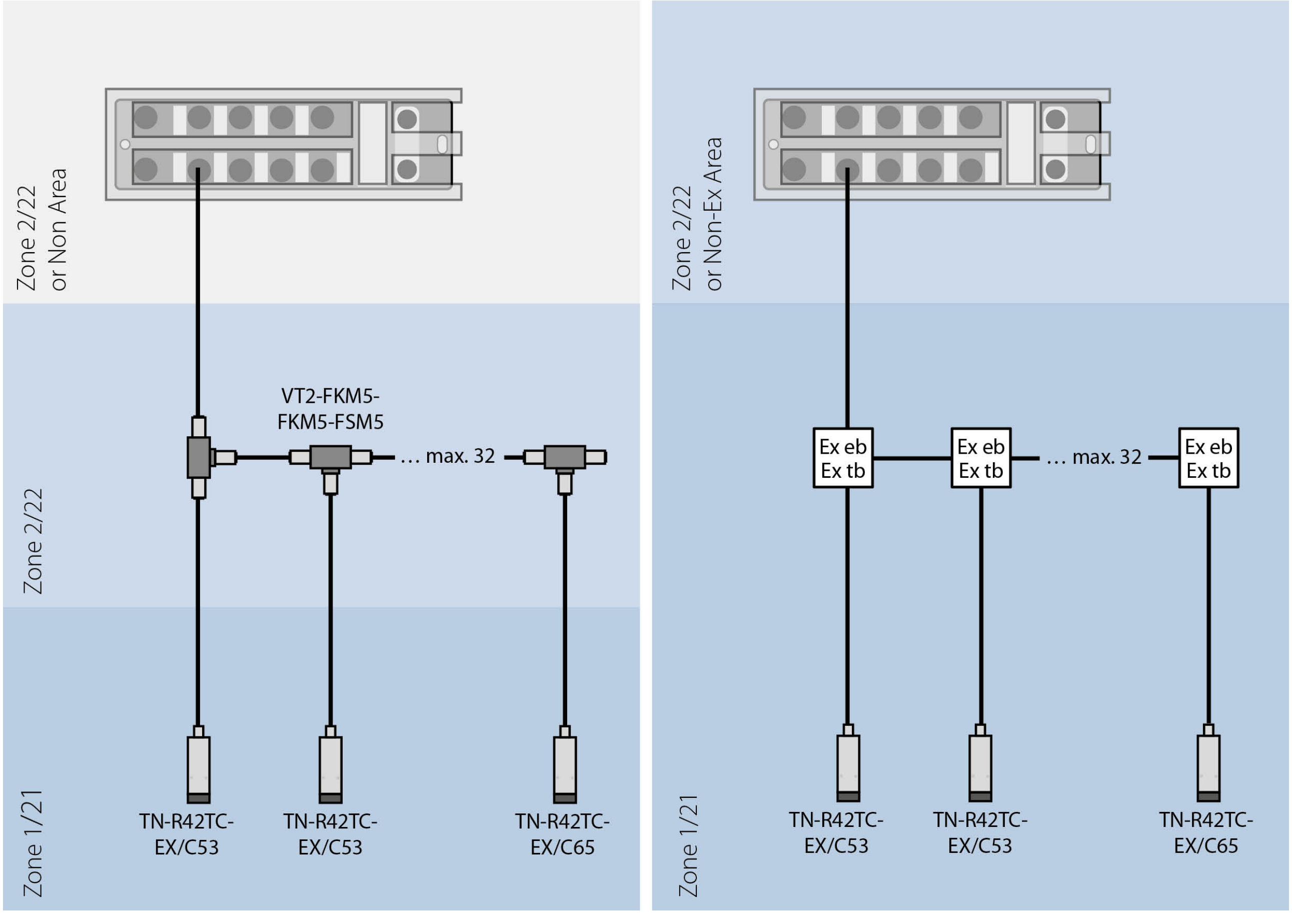


Fig. 19: System setup

6.5 Connecting digital sensors and actuators

The device has four 5-pin M12 male connectors for connecting digital sensors and actuators. The maximum tightening torque is 0.6 Nm.

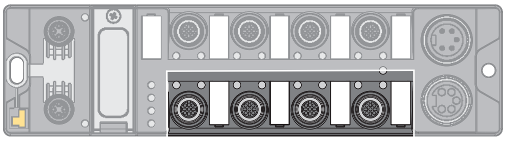


Fig. 20: M12 male connectors for connecting digital sensors and actuators

- ▶ Connect the sensors and actuators to the device as per the pin assignment below.
- ▶ Always seal unused connectors with suitable screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.

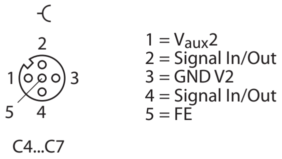


Fig. 21: Connections for digital sensors and actuators – pin assignment

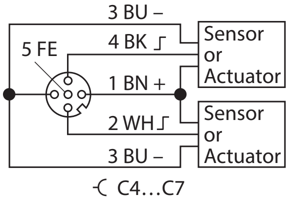


Fig. 22: Connections for digital sensors and actuators – wiring diagram

The channels are assigned to the connectors as follows:

Channel	Connector	Pin
DXP8 (Ch8)	C4	4
DXP9 (Ch9)	C4	2
DXP10 (Ch10)	C5	4
DXP11 (Ch11)	C5	2
DXP12 (Ch12)	C6	4
DXP13 (Ch13)	C6	2
DXP14 (Ch14)	C7	4
DXP15 (Ch15)	C7	2

7 Commissioning

7.1 Adjusting network settings

The network settings can be adjusted via two decimal rotary coding switches and DIP switches on the device, via the web server or via the Turck Service Tool.

7.1.1 Adjusting network settings using switches on the device

The switches, together with the USB ports and the SET button, are located under a service window.

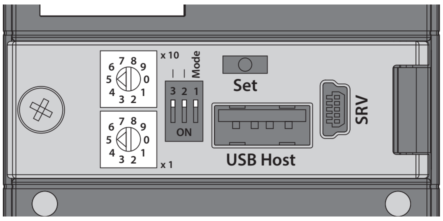


Fig. 23: Service window

- ▶ Open the service window above the switches.
- ▶ Set the required rotary coding switches to the required mode according to the table below.
- ▶ Set the DIP switch [Mode] to the required mode according to the table below.
- ▶ Carry out a voltage reset.
- ▶ NOTICE! IP67 or IP69K protection is not guaranteed when the service window over the rotary coding switches is opened. Device damage through penetrating foreign objects or liquids is possible. Close the service window over the switches securely.

Switch positions

The network settings of the device depend on the selected mode. Changes to the settings are active after a voltage reset.

The switch positions 00 and 90 are not operating modes. The setting of an operating mode is required each time the device is reset to the default values.

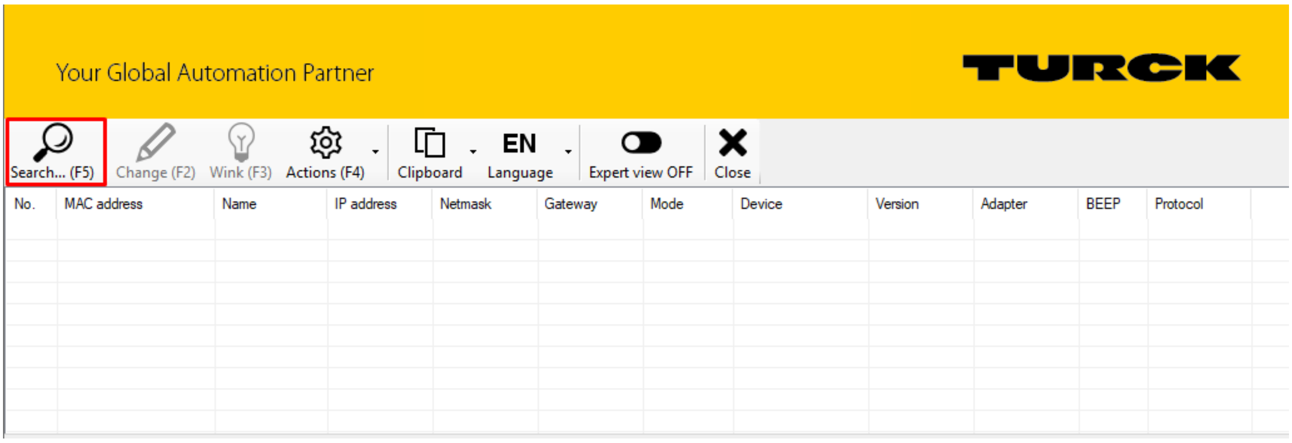
Switch position		**Mode**	**Description**
DIP switch [Mode]	**Rotary coding switch**		
0	00	Network reset	The network resets the following network settings to the default values: IP address: 192.168.1.100 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1
0	1…99	Rotary	In Rotary mode (static rotary), the last byte of the IP address is set manually on the gateway. The other network settings are stored retentively in the device memory and cannot be changed in Rotary mode. Addresses 1…99 can be set.
1	50	PGM	In PGM mode, the network settings can be assigned manually via the Turck Service Tool, FDT/DTM or via a web server. The settings are saved in the non-volatile memory of the device.

Switch position		Mode	Description
DIP switch [Mode]	Rotary coding switch		
1	60	PGM-DHCP	In PGM-DHCP mode, the device is first of all a DHCP client and sends DHCP requests until it is assigned a fixed IP address. The DHCP client is automatically deactivated as soon as an IP address is assigned to the device via the DTM, the Turck Service Tool or a web server.
1	90	Factory reset	The factory reset resets all settings to the default values: ■ Network settings (IP address, subnet mask, gateway) ■ Device parameters The OPC UA server does not start up when a restart is performed with this switch position. The Run and OPC LEDs flash green simultaneously. After a factory reset a reboot is necessary with a switch position permissible for operation.

7.1.2 Adjusting the network settings via the Turck Service Tool

The device is factory set to IP address 192.168.1.100. The IP address can be set via the Turck Service Tool. The Turck Service Tool is available free of charge from **www.turck.com**.

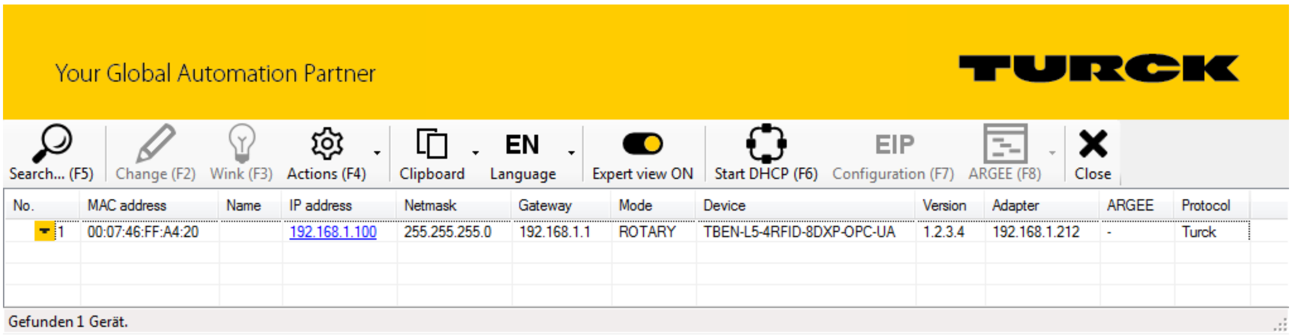
- ▶ Connect the device to a PC via the Ethernet interface.
- ▶ Launch the Turck Service Tool.
- ▶ Click **Search** or press [F5].



No.	MAC address	Name	IP address	Netmask	Gateway	Mode	Device	Version	Adapter	BEEP	Protocol

Fig. 24: Turck Service Tool – start screen

The Turck Service Tool displays the connected devices.



No.	MAC address	Name	IP address	Netmask	Gateway	Mode	Device	Version	Adapter	ARGEE	Protocol
1	00:07:46:FF:A4:20		192.168.1.100	255.255.255.0	192.168.1.1	ROTARY	TBEN-L5-4RFID-8DXP-OPC-UA	1.2.3.4	192.168.1.212	-	Turck

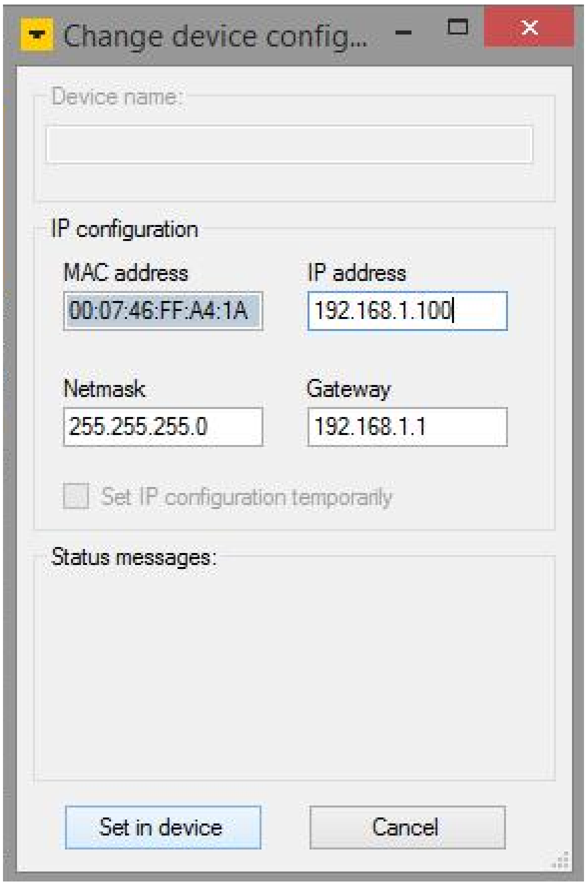
Gefunden 1 Gerät.

Fig. 25: Turck Service Tool – found devices

- ▶ Click the required device.
- ▶ Click **Change** or press [F2].

NOTE
Clicking the IP address of the device opens the web server.

- Change the IP address and if necessary the network mask and gateway.
- Accept the changes by clicking **Set in device**.



Change device config...

Device name:

IP configuration

MAC address: 00:07:46:FF:A4:1A

IP address: 192.168.1.100

Netmask: 255.255.255.0

Gateway: 192.168.1.1

□ Set IP configuration temporarily

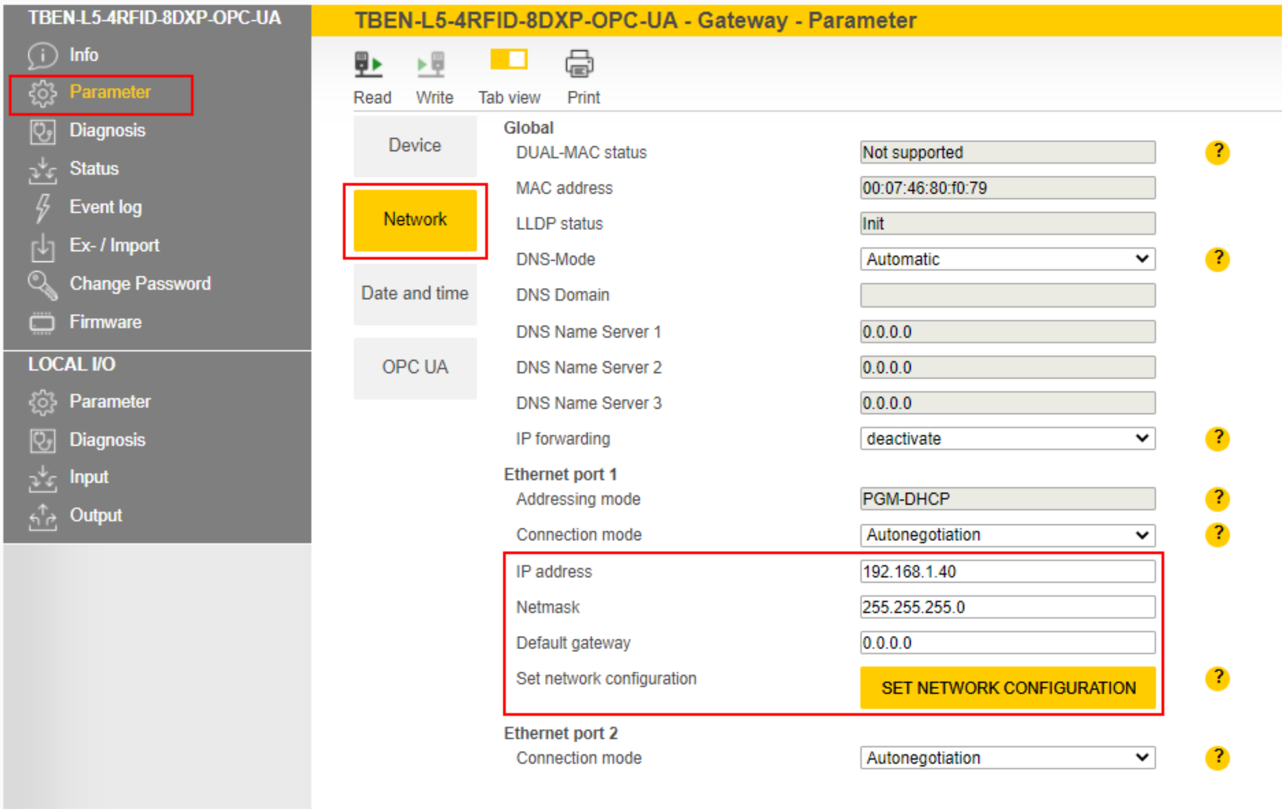
Status messages:

Fig. 26: Turck Service Tool – changing the device configuration

7.1.3 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.



Global	
DUAL-MAC status	Not supported
MAC address	00:07:46:80:f0:79
LLDP status	Init
DNS-Mode	Automatic
DNS Domain	
DNS Name Server 1	0.0.0.0
DNS Name Server 2	0.0.0.0
DNS Name Server 3	0.0.0.0
IP forwarding	deactivate
Ethernet port 1	
Addressing mode	PGM-DHCP
Connection mode	Autonegotiation
IP address	192.168.1.40
Netmask	255.255.255.0
Default gateway	0.0.0.0
Set network configuration	SET NETWORK CONFIGURATION
Ethernet port 2	
Connection mode	Autonegotiation

Fig. 27: Adjusting network settings via the web server

7.2 Preparing the device for commissioning via the web server

NOTE
The web server always displays all setting options. All values are displayed as decimal numbers.

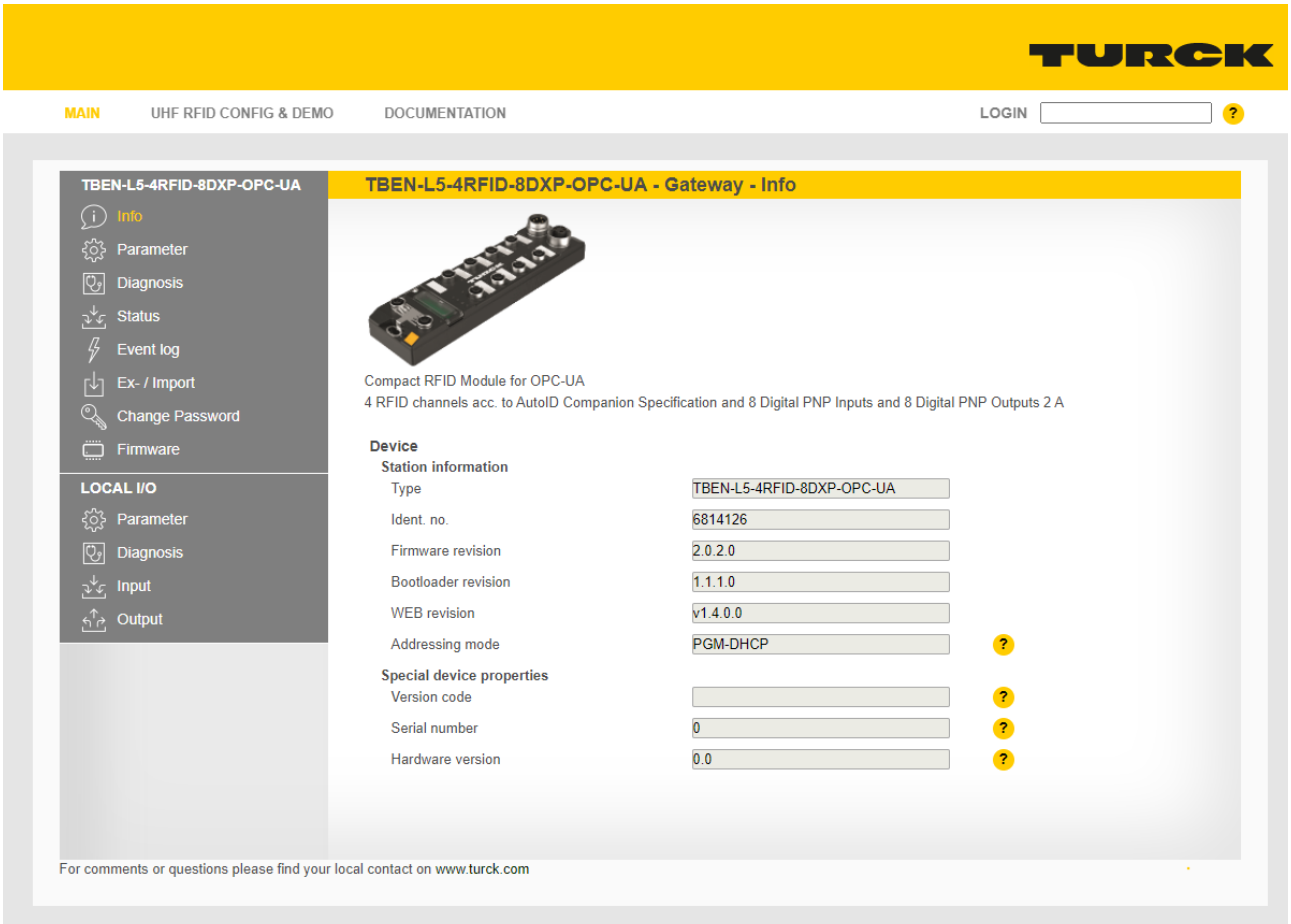
The devices can be set and commands can be sent to the devices via the integrated web server. To be able to open the web server with a PC, the device and the PC must be in the same IP network.

7.2.1 Opening the web server and editing the settings

The web server can be opened via a web browser or via the Turck Service Tool. Calling the web server via the Turck Service Tool is described in the section ”Setting the Network address”.

The device is factory set to IP address 192.168.1.100. To open the web server via a web browser, enter http://192.168.1.100 in the address bar of the web browser.

The start page shows status information and network settings.



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Info

Compact RFID Module for OPC-UA
4 RFID channels acc. to AutoID Companion Specification and 8 Digital PNP Inputs and 8 Digital PNP Outputs 2 A

Device

Station information

Type	TBEN-L5-4RFID-8DXP-OPC-UA
Ident. no.	6814126
Firmware revision	2.0.2.0
Bootloader revision	1.1.1.0
WEB revision	v1.4.0.0
Addressing mode	PGM-DHCP

Special device properties

Version code	
Serial number	0
Hardware version	0.0

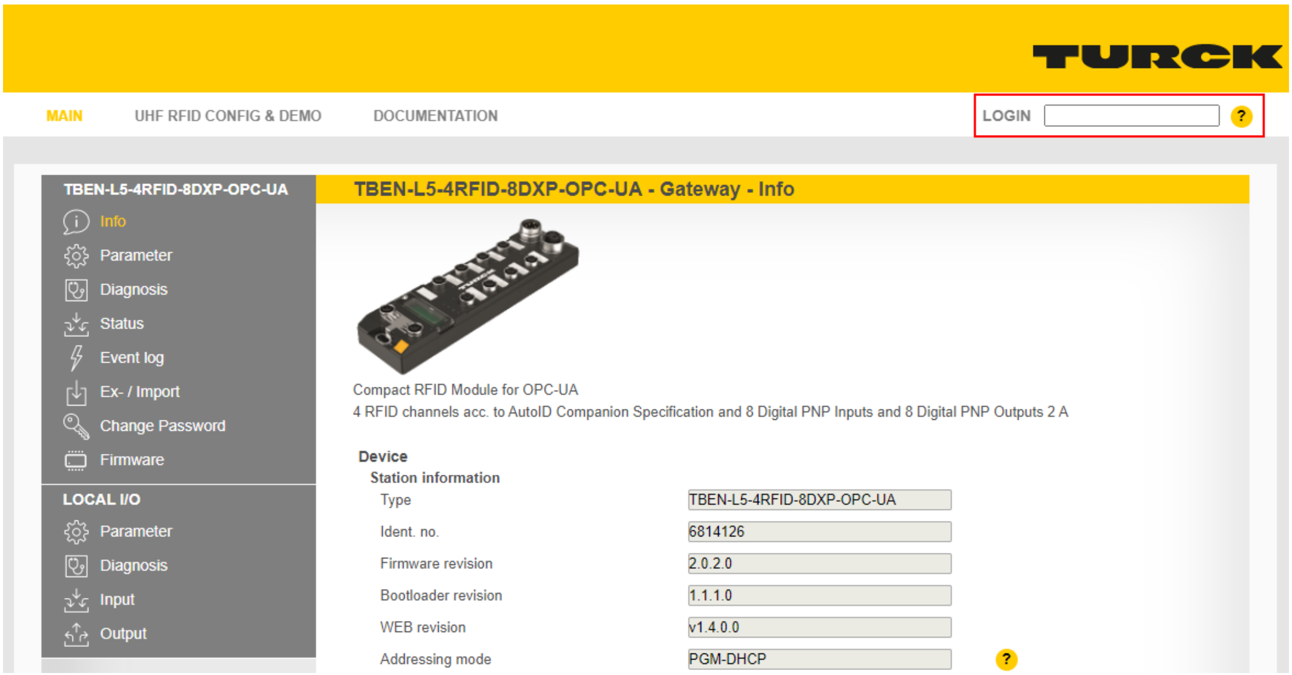
For comments or questions please find your local contact on www.turck.com

Fig. 28: Web server – start page

A login is required in order to edit settings via the web server. The default password is “password”.

NOTE
To ensure greater security, Turck recommends changing the password after the first login.

- ▶ Enter the password in the Login field on the start page of the web server.
- ▶ Click **Login**.



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Info

Compact RFID Module for OPC-UA
4 RFID channels acc. to AutoID Companion Specification and 8 Digital PNP Inputs and 8 Digital PNP Outputs 2 A

Device
Station information

Type	TBEN-L5-4RFID-8DXP-OPC-UA
Ident. no.	6814126
Firmware revision	2.0.2.0
Bootloader revision	1.1.1.0
WEB revision	v1.4.0.0
Addressing mode	PGM-DHCP

Fig. 29: Login field on the start page of the web server (marked in red)

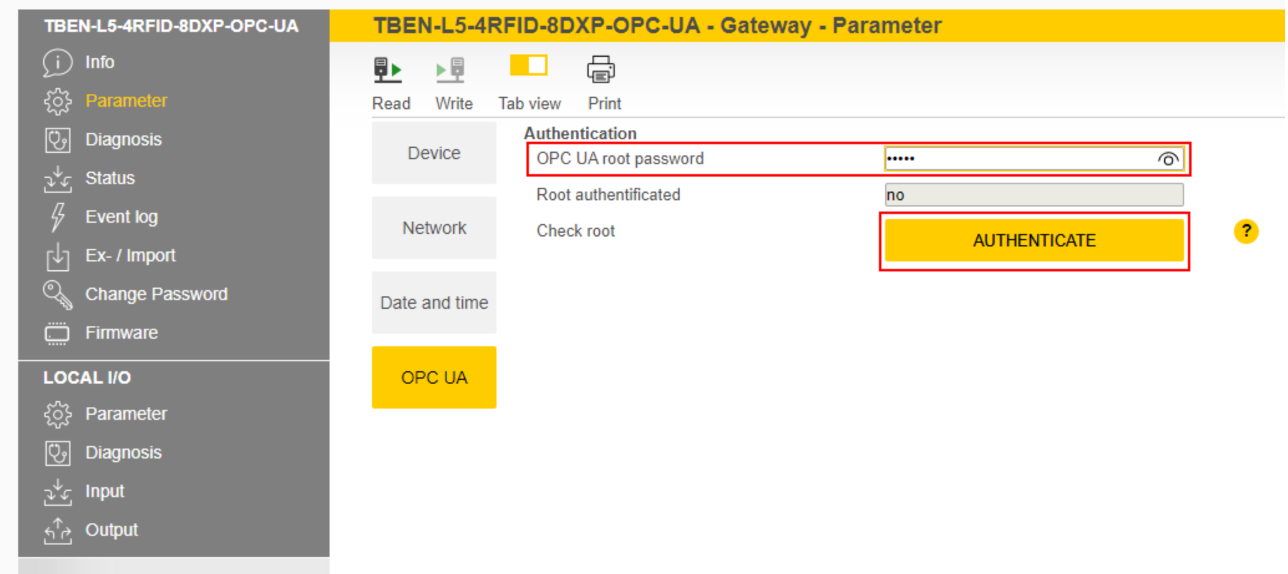
Write access to the parameter data of the module is possible after the login.

To access OPC UA 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**.



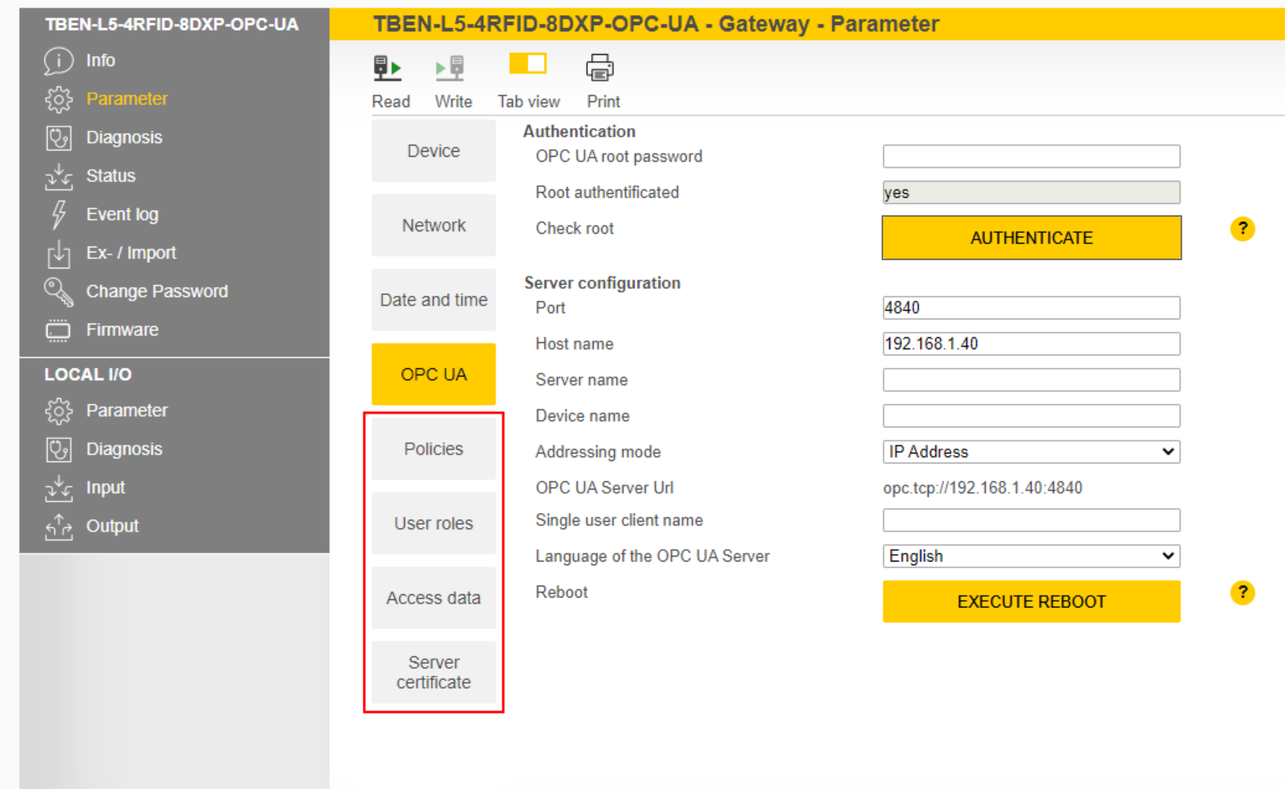
TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Parameter

Authentication

OPC UA root password	•••••
Root authentificated	no
Check root	AUTHENTICATE

Fig. 30: Entering the OPC UA root password

➩ The parameters for the OPC UA configuration are shown.



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Parameter

Authentication

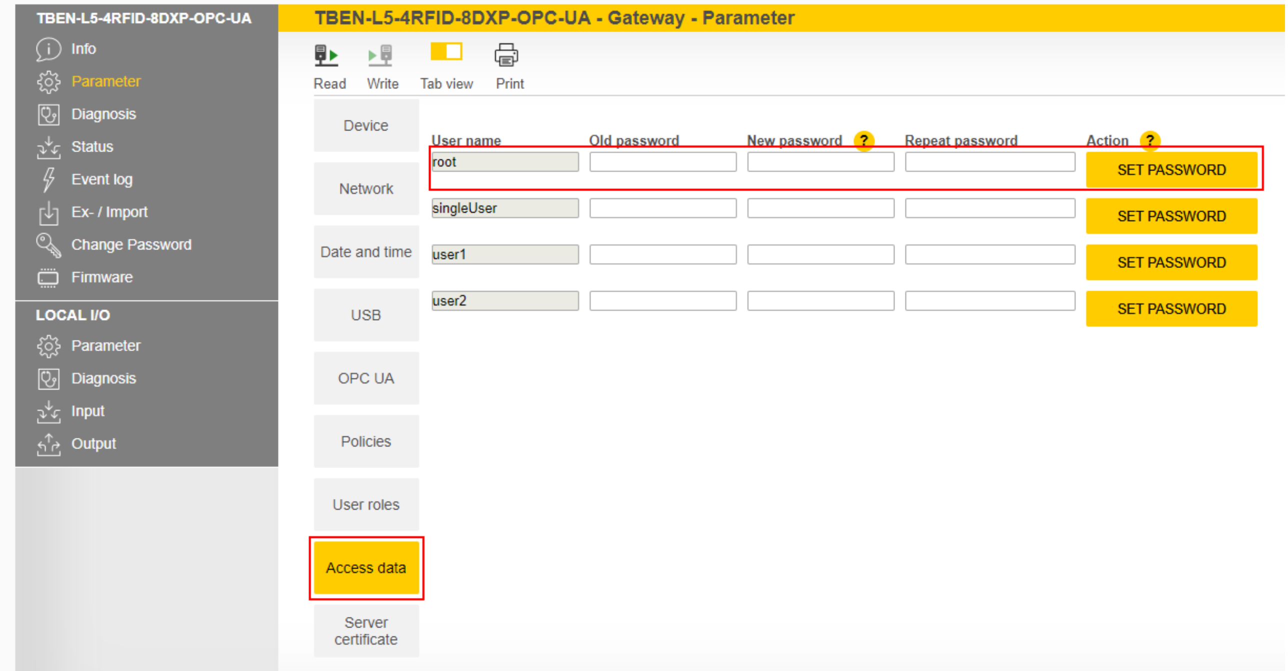
OPC UA root password	
Root authentificated	yes
Check root	AUTHENTICATE

Server configuration

Port	4840
Host name	192.168.1.40
Server name	
Device name	
Addressing mode	IP Address
OPC UA Server Url	opc.tcp://192.168.1.40:4840
Single user client name	
Language of the OPC UA Server	English
Reboot	EXECUTE REBOOT

Fig. 31: Parameters for the OPC UA configuration

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



User name	Old password	New password ?	Repeat password	Action ?
root				SET PASSWORD
singleUser				SET PASSWORD
user1				SET PASSWORD
user2				SET PASSWORD

Fig. 32: Changing the root password

7.2.2 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.

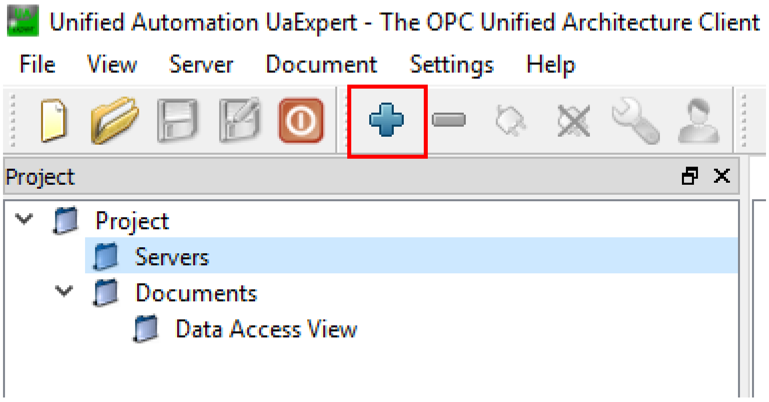
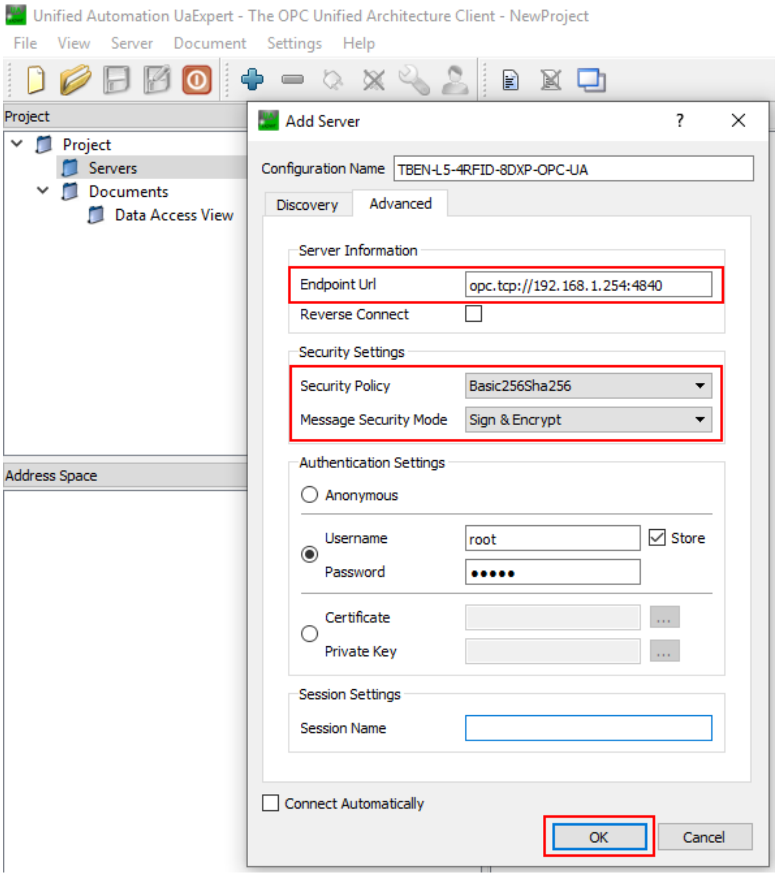

Unified Automation UaExpert - The OPC Unified Architecture Client
File View Server Document Settings Help
Project
Project
Servers
Documents
Data Access View

Fig. 33: Adding OPC UA server in the OPC UA client (example: UAExpert)

- ▶ Enter in the following window the OPC UA server URL and the required **Security Settings**.
- ▶ Confirm entries with **OK**.
- ➪ The OPC UA server is added to the project tree.


Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject
File View Server Document Settings Help
Project
Project
Servers
Documents
Data Access View
Address Space
Add Server
?
Discovery
Advanced
OK
Cancel

Configuration Name: TBEN-L5-4RFID-8DXP-OPC-UA

Server Information
Endpoint Url: opc.tcp://192.168.1.254:4840
Reverse Connect: □

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

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

Session Settings
Session Name:

□ Connect Automatically

Fig. 34: Enter the OPC UA server URL and choose the Security Settings

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

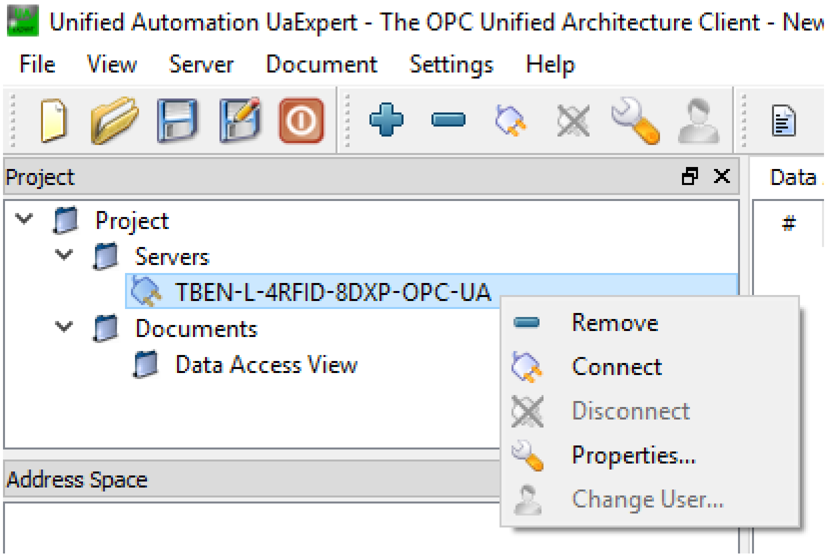
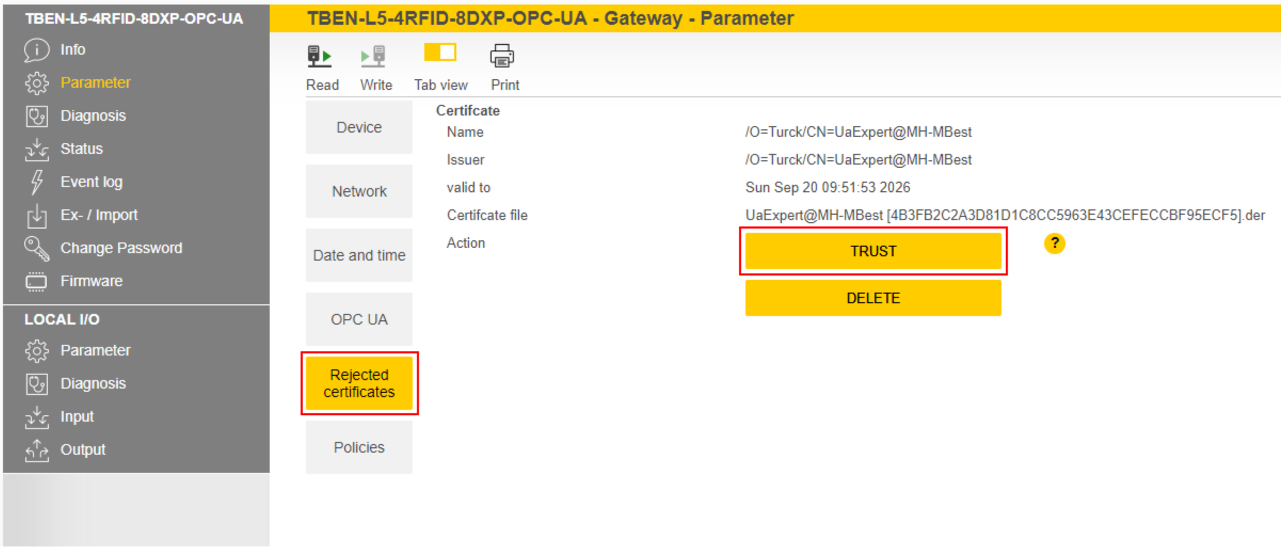


Fig. 35: Connecting the OPC UA server

➪ 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**.



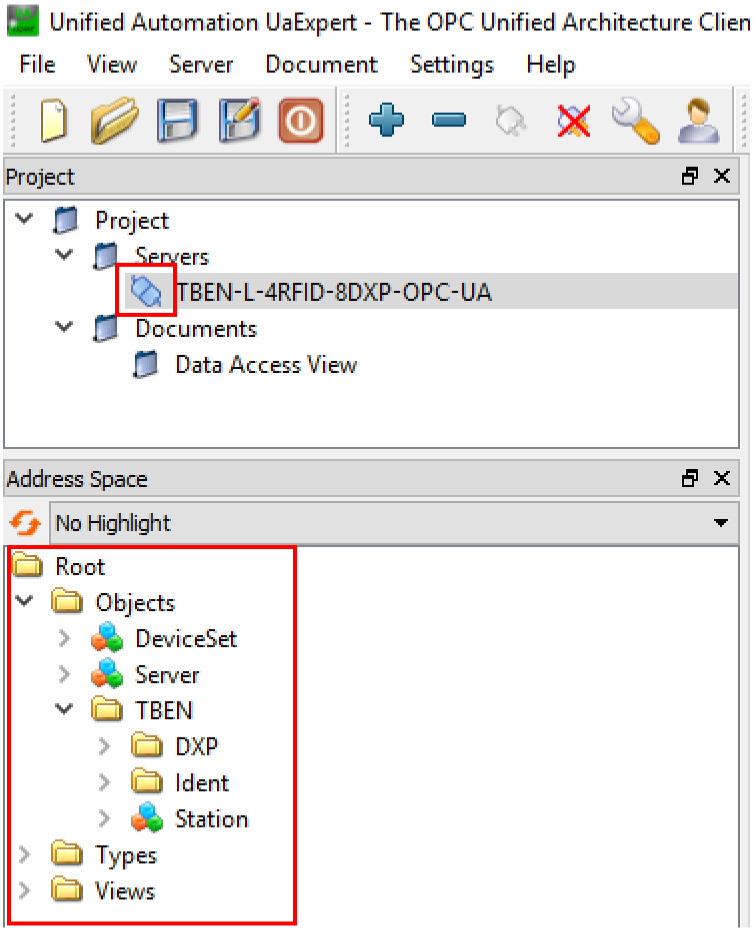
Certifcate

Name	/O=Turck/CN=UaExpert@MH-MBest
Issuer	/O=Turck/CN=UaExpert@MH-MBest
valid to	Sun Sep 20 09:51:53 2026
Certifcate file	UaExpert@MH-MBest [4B3FB2C2A3D81D1C8CC5963E43CEFECCBF95ECF5].der
Action	TRUST DELETE

Fig. 36: Trusting security certificates

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



Unified Automation UaExpert - The OPC Unified Architecture Clien

Fig. 37: Connection established, address space created

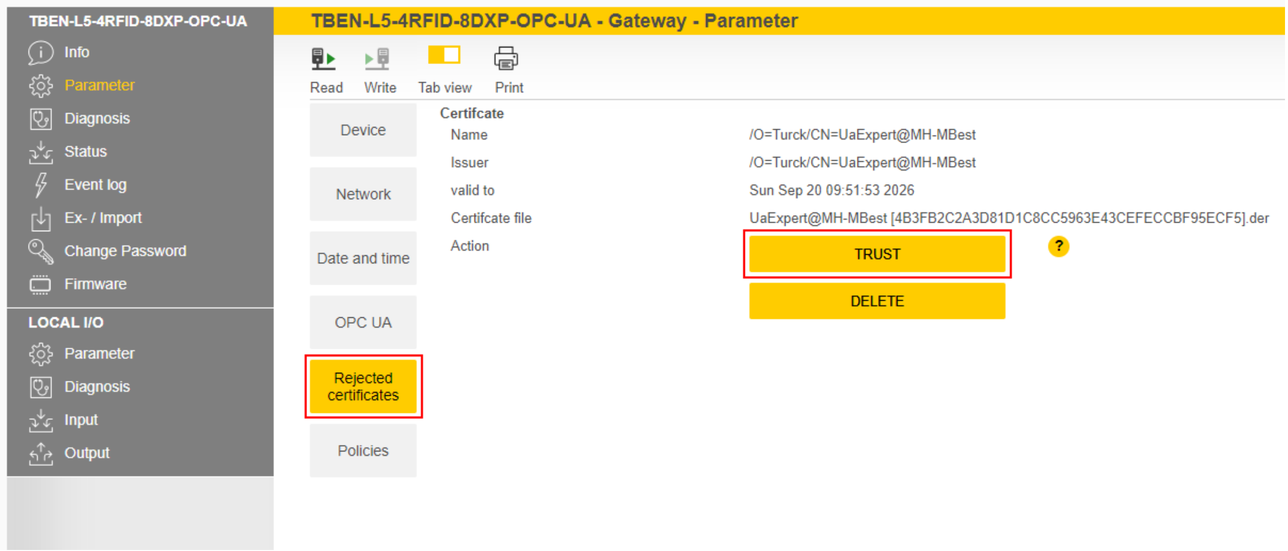
7.2.3 Validating security certificates

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**.

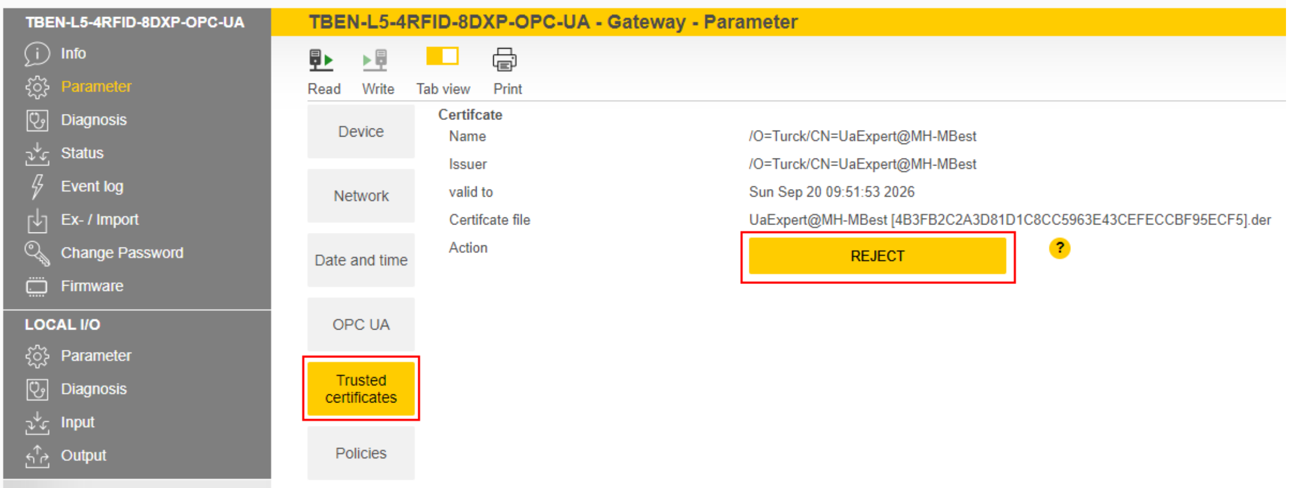
➪ The security certificate is added to the list of trusted certificates.



Certifcate
Name /O=Turck/CN=UaExpert@MH-MBest
Issuer /O=Turck/CN=UaExpert@MH-MBest
valid to Sun Sep 20 09:51:53 2026
Certifcate file UaExpert@MH-MBest [4B3FB2C2A3D81D1C8CC5963E43CEFECCBF95ECF5].der
Action

Fig. 38: Trusting security certificates

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



Certifcate
Name /O=Turck/CN=UaExpert@MH-MBest
Issuer /O=Turck/CN=UaExpert@MH-MBest
valid to Sun Sep 20 09:51:53 2026
Certifcate file UaExpert@MH-MBest [4B3FB2C2A3D81D1C8CC5963E43CEFECCBF95ECF5].der
Action

Fig. 39: 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**.

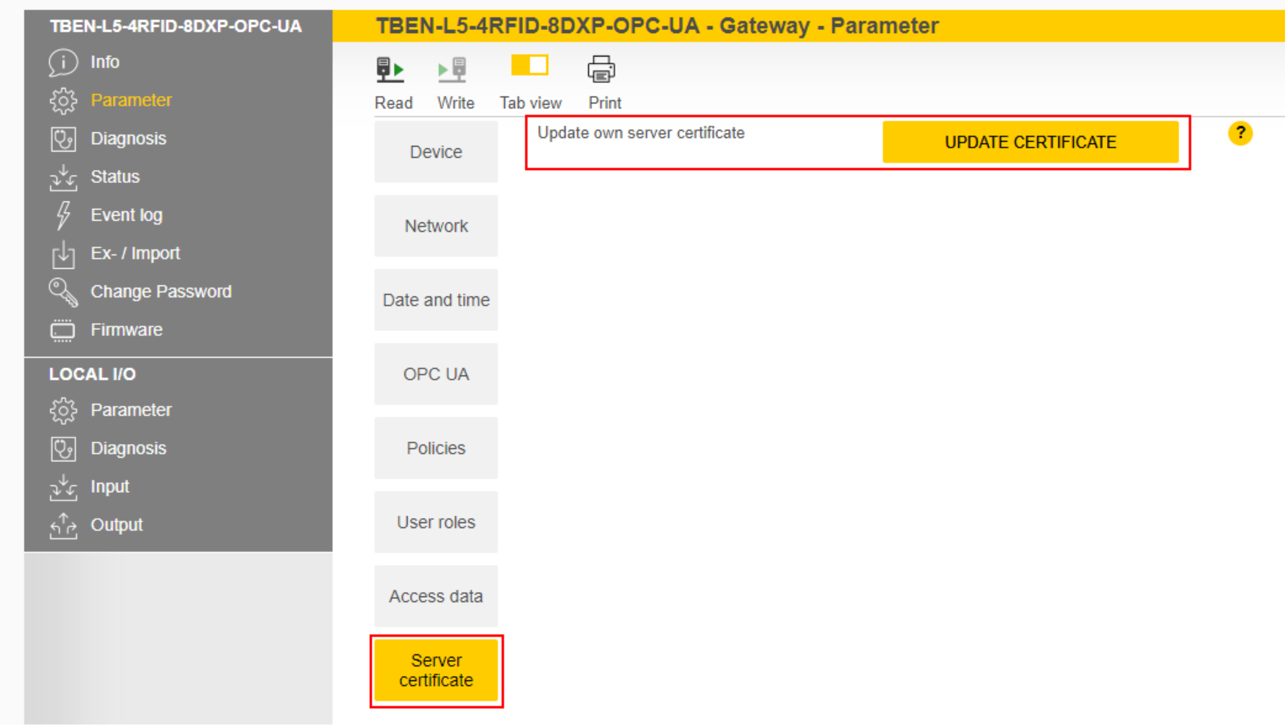


Fig. 40: Creating a specific security certificate

7.2.4 Adapting settings for OPC UA communication – set endpoints

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

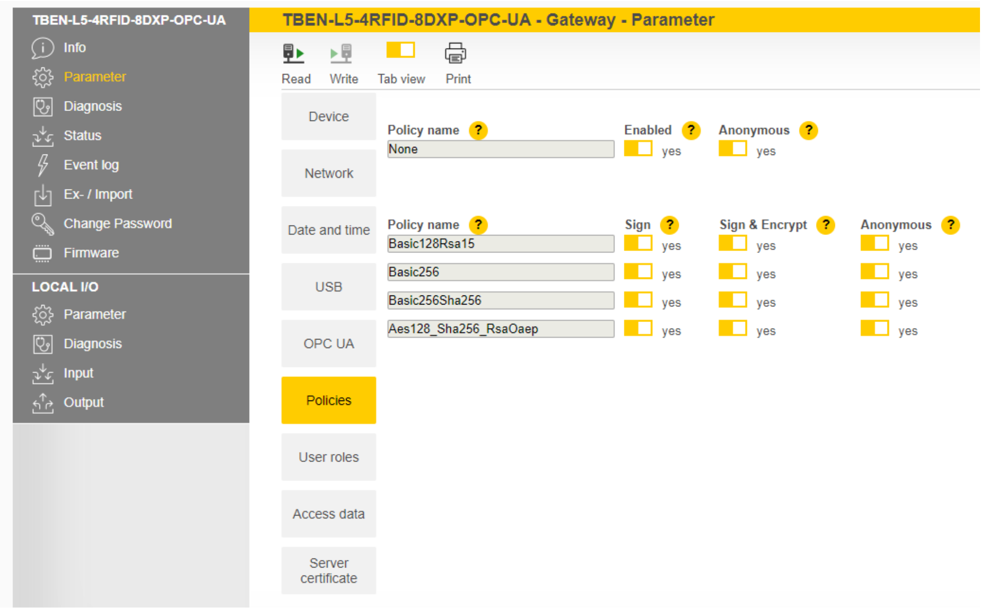
Changing the security settings

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.



Policy name ?	Enabled ?	Anonymous ?
None	yes	yes

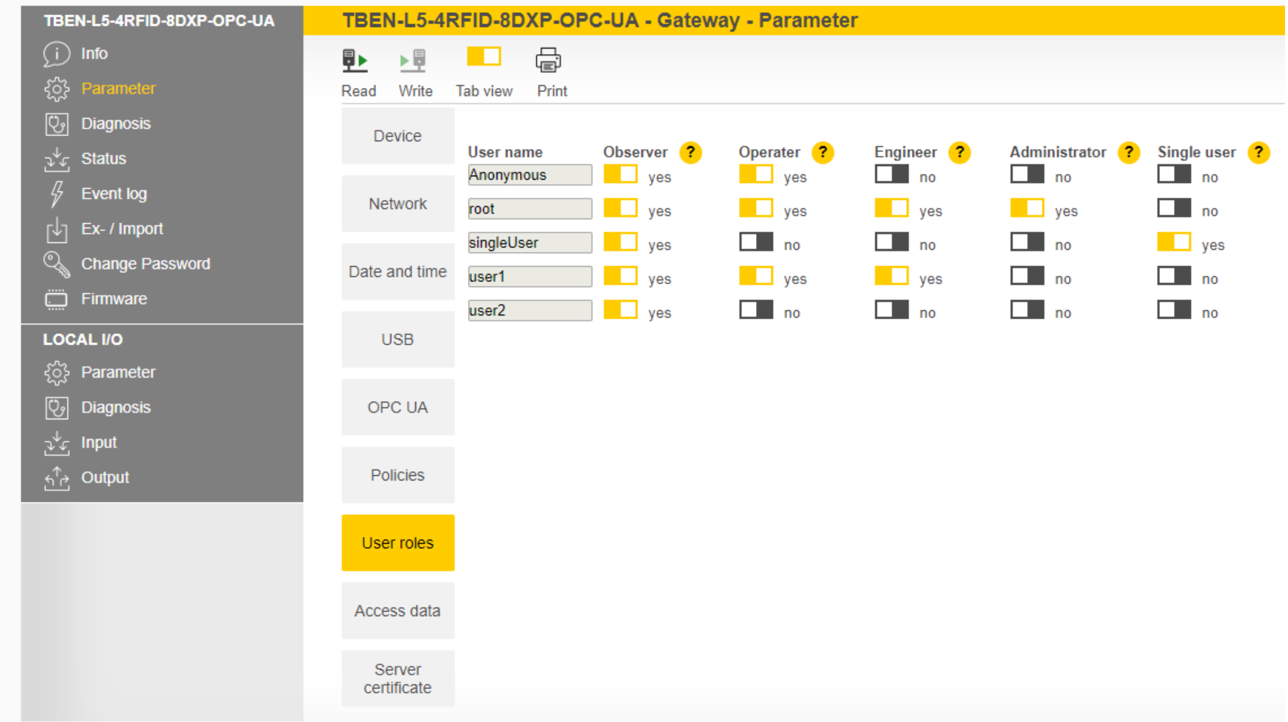
Policy name ?	Sign ?	Sign & Encrypt ?	Anonymous ?
Basic128Rsa15	yes	yes	yes
Basic256	yes	yes	yes
Basic256Sha256	yes	yes	yes
Aes128_Sha256_RsaOaep	yes	yes	yes

Fig. 41: 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)



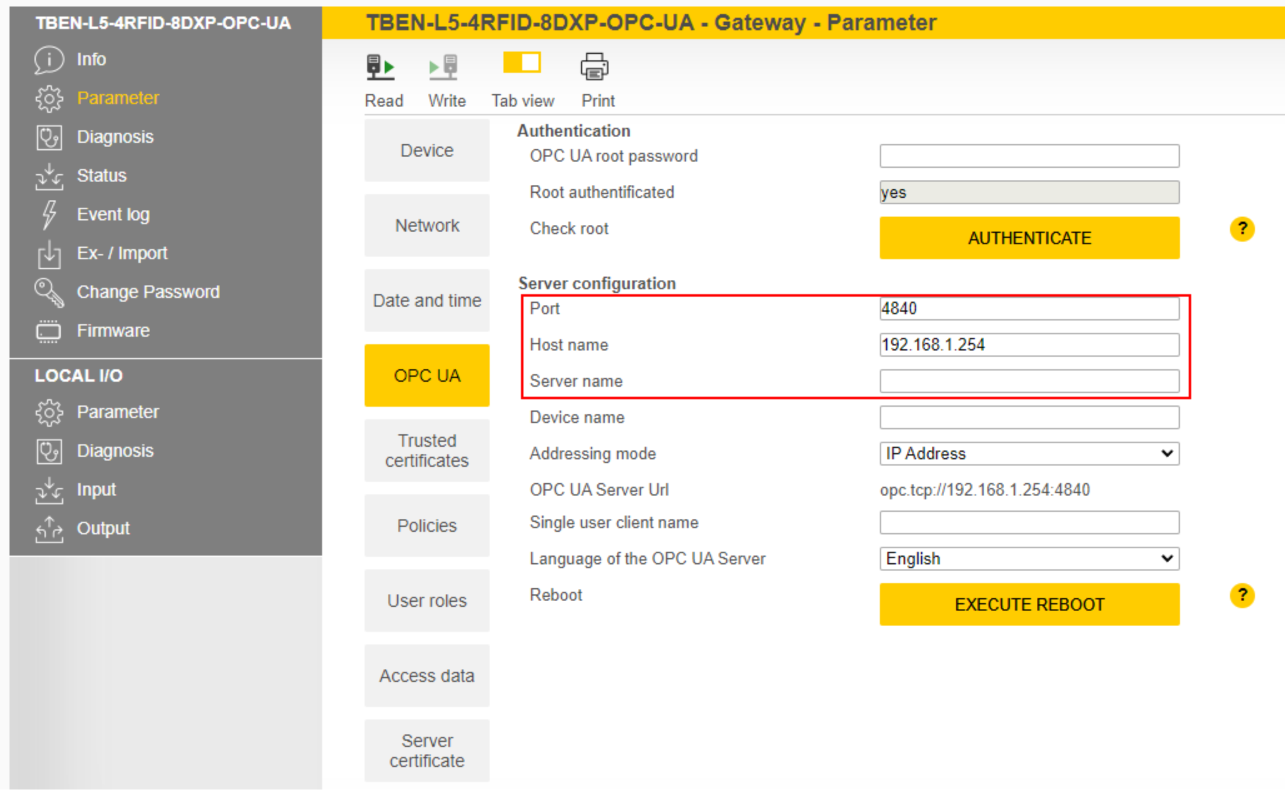
User name	Observer ?	Operater ?	Engineer ?	Administrator ?	Single user ?
Anonymous	yes	yes	no	no	no
root	yes	yes	yes	yes	no
singleUser	yes	no	no	no	yes
user1	yes	yes	yes	no	no
user2	yes	no	no	no	no

Fig. 42: User roles

Configuring endpoints – server configuration

The following settings can be changed in the **Parameter** → **OPC UA** → **Server configuration** area:

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



Authentication

OPC UA root password	
Root authentificated	yes
Check root	AUTHENTICATE

Server configuration

Port	4840
Host name	192.168.1.254
Server name	
Device name	
Addressing mode	IP Address
OPC UA Server Url	opc.tcp://192.168.1.254:4840
Single user client name	
Language of the OPC UA Server	English
Reboot	EXECUTE REBOOT

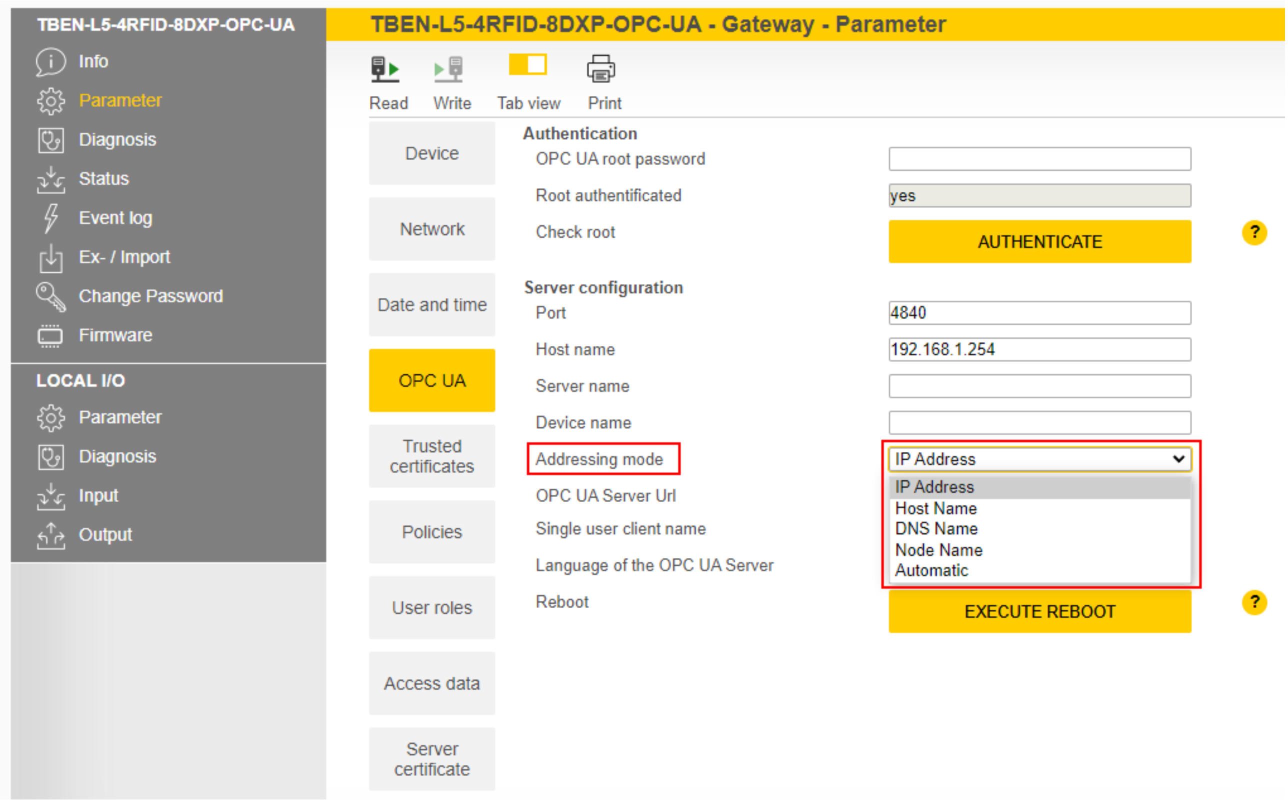
Fig. 43: Server configuration

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.



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Parameter

Authentication

OPC UA root password	
Root authentificated	yes
Check root	AUTHENTICATE

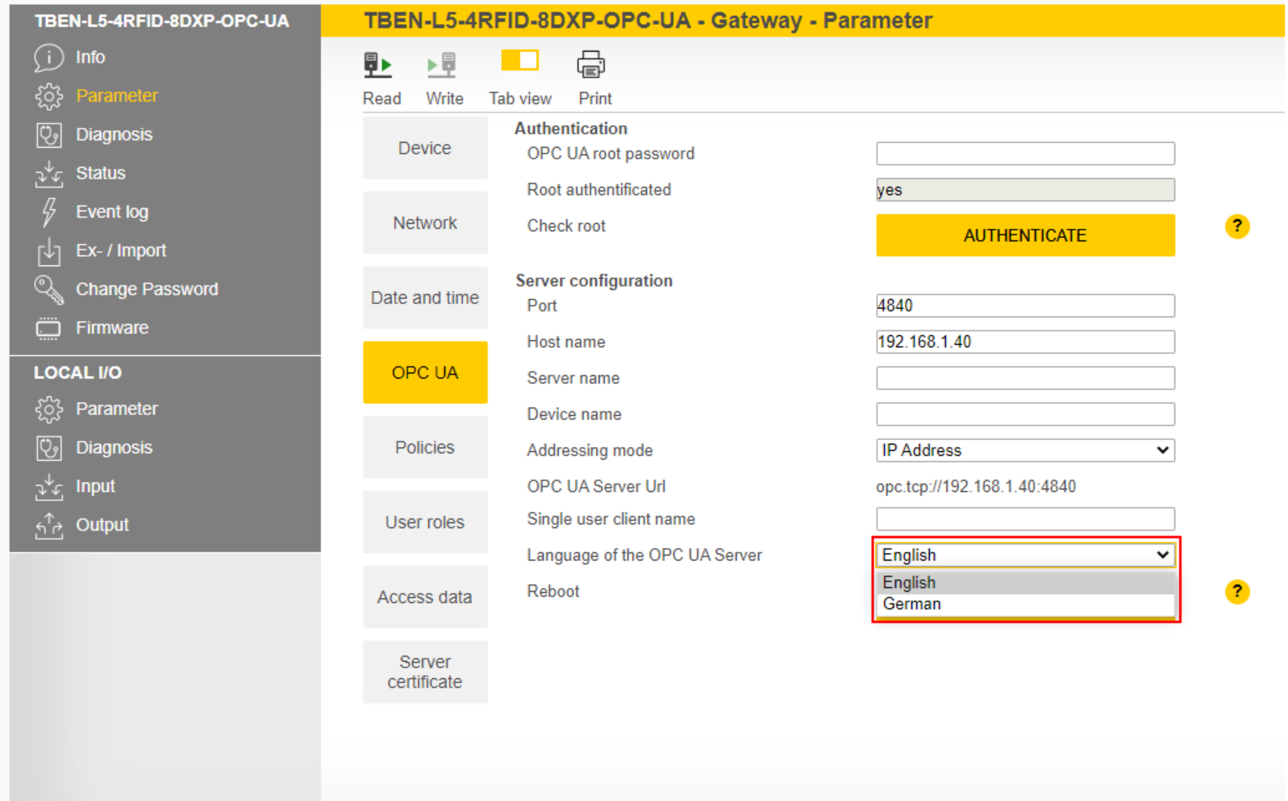
Server configuration

Port	4840
Host name	192.168.1.254
Server name	
Device name	
Addressing mode	IP Address IP Address Host Name DNS Name Node Name Automatic
OPC UA Server Url	
Single user client name	
Language of the OPC UA Server	
Reboot	EXECUTE REBOOT

Fig. 44: 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.



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Parameter

Authentication
OPC UA root password:
Root authentificated: yes
Check root: AUTHENTICATE

Server configuration
Port: 4840
Host name: 192.168.1.40
Server name:
Device name:
Addressing mode: IP Address
OPC UA Server Url: opc.tcp://192.168.1.40:4840
Single user client name:
Language of the OPC UA Server: English
Reboot

Fig. 45: Changing language settings of the OPC UA server

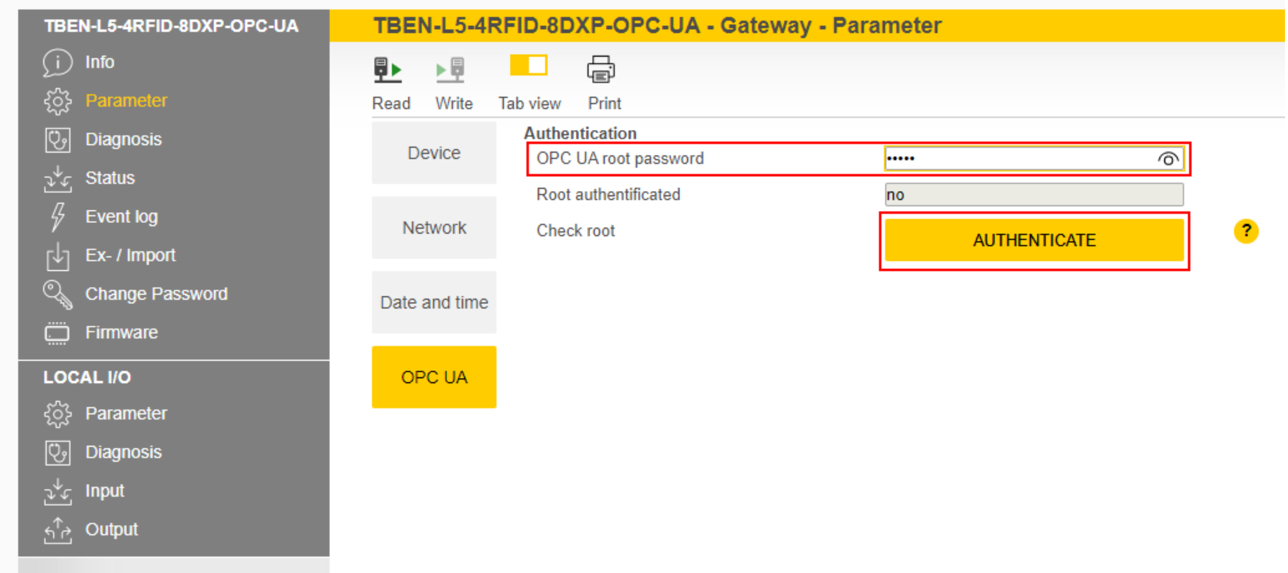
7.2.5 Setting the OPC UA password

To access OPC UA 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**.


TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Parameter

Authentication

OPC UA root password: •••••

Root authentificated: no

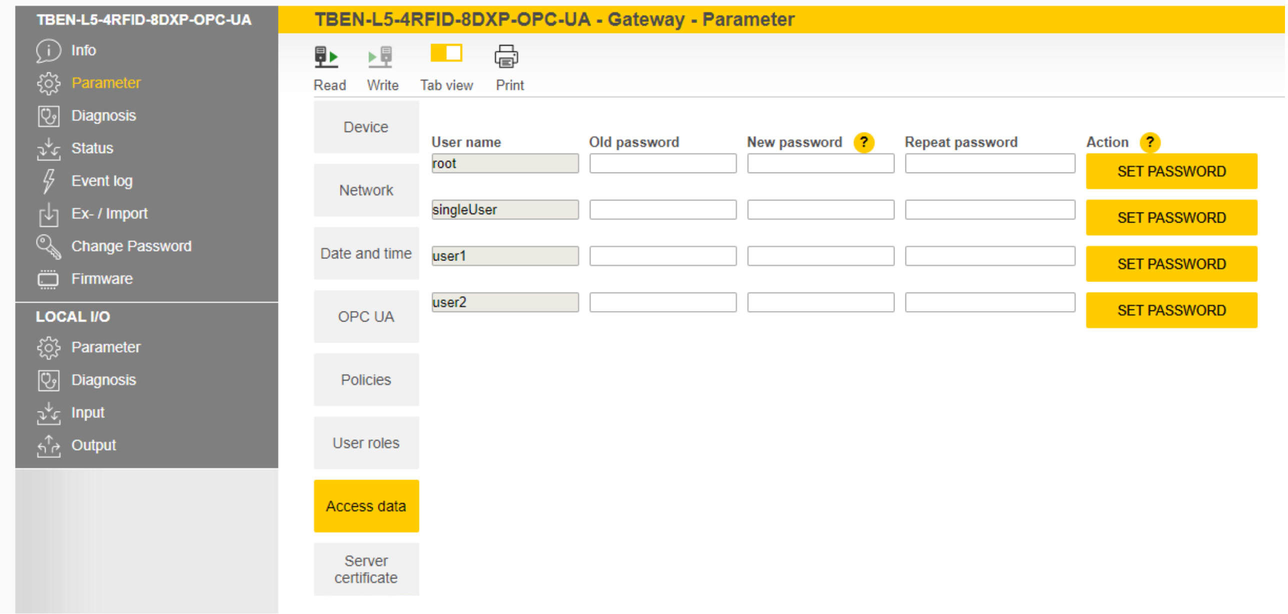
Check root: AUTHENTICATE

Fig. 46: 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**.



User name	Old password	New password ?	Repeat password	Action ?
root				SET PASSWORD
singleUser				SET PASSWORD
user1				SET PASSWORD
user2				SET PASSWORD

Fig. 47: 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.

7.2.6 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.

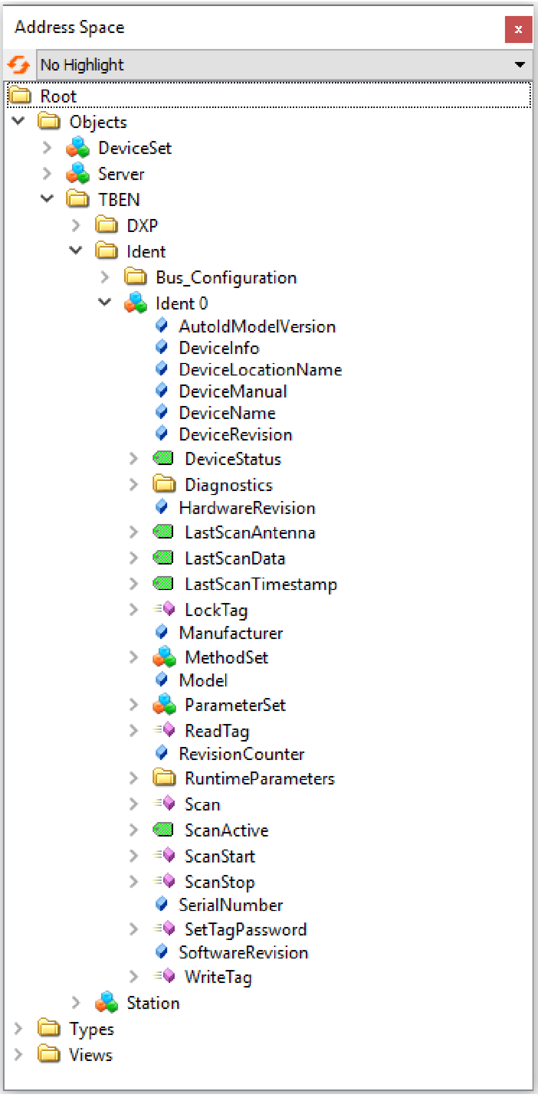
8 Setting

8.1 Information model – mapping

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

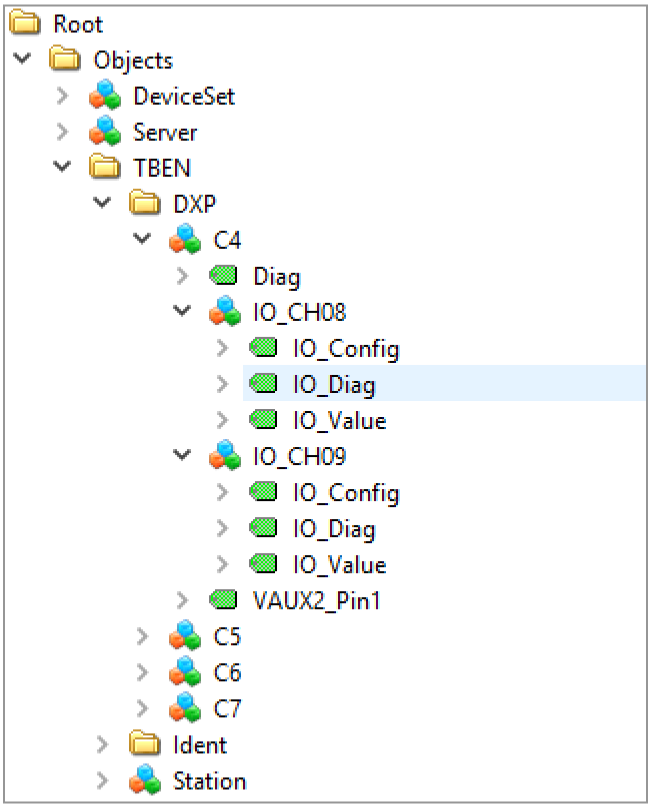
Node class	Description
Folder	General collection
Object	Mapping of a technical object
Property	Description of an object
Variable	Process data or status information
Method	Functional scan with status feedback (e.g. RFID commands)

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



```
Address Space
No Highlight
Root
  Objects
    DeviceSet
    Server
    TBEN
      DXP
      Ident
        Bus_Configuration
        Ident 0
          AutoIdModelVersion
          DeviceInfo
          DeviceLocationName
          DeviceManual
          DeviceName
          DeviceRevision
          DeviceStatus
          Diagnostics
          HardwareRevision
          LastScanAntenna
          LastScanData
          LastScanTimestamp
          LockTag
          Manufacturer
          MethodSet
          Model
          ParameterSet
          ReadTag
          RevisionCounter
          RuntimeParameters
          Scan
          ScanActive
          ScanStart
          ScanStop
          SerialNumber
          SetTagPassword
          SoftwareRevision
          WriteTag
      Station
  Types
  Views
```

Fig. 48: Information model of the RFID channel Ident 0 – example: UA Expert



```
Root
  Objects
    DeviceSet
    Server
    TBEN
      DXP
        C4
          Diag
          IO_CH08
            IO_Config
            IO_Diag
            IO_Value
          IO_CH09
            IO_Config
            IO_Diag
            IO_Value
          VAUX2_Pin1
        C5
        C6
        C7
      Ident
      Station
```

Fig. 49: Information model of DXP channels 8 and 9 – example: UA Expert

8.1.1 RFID channels – mapping in the information model

Each connected read/write device is assigned with an Ident channel. The objects Ident 0… Ident 3 contain 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 and the **ScanActive** variable.

Variable	Description	Ordner
BusMode (Ident…)	Indicates whether the HF bus mode is activated on the RFID channel Ident... .	Bus_Configuration
DeviceStatus	Device status: ■ Idle: Device is in Idle mode, command execution possible ■ Error: Error ■ Scanning: Inventory command active (asynchronous) ■ 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)

Variable	Description	Ordner
Strength	RSSI value of the last tag read	LastAccess (Diagnostics)
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 device (true/false).	
PresenceOnAntenna	Indicates in HF bus mode which of the connected HF read/write heads detected a tag in front of it or not (true/false).	PresencePerAntenna (Diagnostics)
EnableAntennas	HF bus mode: Address of the activated read/write head. The address must be activated beforehand via ActivateBusHead.	RuntimeParameters
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 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 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
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: ■ 0: Reserved (kill and access password) ■ 1: EPC ■ 3: USER

Method	Argument (type)	Description
	Lock (RfidLockOperationEnumeration)	Sets the type of lock: ▪ 0: Lock (the entire memory area selected is write protected with a password.) ▪ 1: Unlock (not supported) ▪ 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.) ▪ 3: Permanent Unlock (not supported) Memory areas lock: EPC and PC, USER Memory areas permanent lock: EPC and PC, USER, Access password, Kill password
	Offset (UInt32)	Only in HF applications: Start address of the memory area to be locked on the HF tag
	Length (UInt32)	Only in HF applications: Number of bytes to be locked on the HF tag
	Status (AutoIdOperationStatusEnumeration)	Status of command execution
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 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: ▪ 0: Reserved ▪ 1: EPC ▪ 2: TID ▪ 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 to be written

Method	Argument (type)	Description
	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: ■ 0: Reserved ■ 1: EPC ■ 3: User
	CodeType (String)	Defines the EPC or UID format.
	Status (AutoIdOperationStatusEnumeration)	Status of command execution
	Data (ByteString)	Write data
WriteTagID		Writing of a new UID or EPC (only for UHF applications)
	AutoID identifier (ScanData)	UID or EPC of the tag to be written
	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

Methods in UHF bus mode for OPC UA

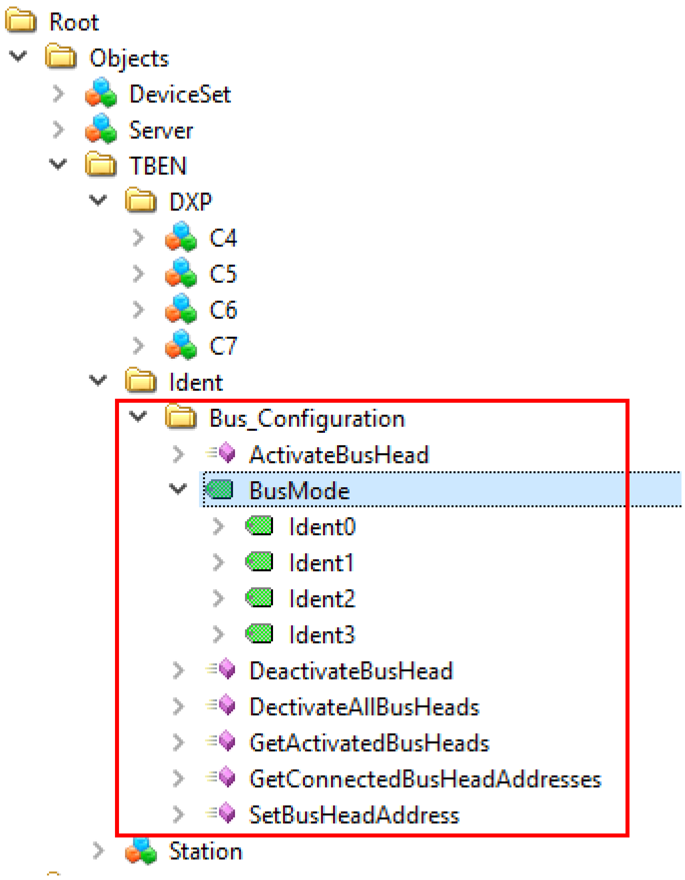


Fig. 50: Information model of HF bus mode – example: UAExpert

Method	Argument (type)	Description
ActivateBusHead		Sets the parameter to activate the HF read/write head and starts automatic addressing if no address has been assigned. If no HF read/write head is activated yet, the **ActivateBusHead** method switches the channel to HF bus mode for OPC UA.
	IdentChannel (UInt16)	RFID channel (Ident)
	BusAddress (UInt16)	Address of the HF read/write head that is activated
	EnableDirectly (Boolean)	Sets the address of the HF read/write head that is executing the method to EnableAntennas.
Deactivate-BusHead		Deactivates a specific HF read/write head.
	IdentChannel (UInt16)	RFID channel (Ident)
	BusAddress (UInt16)	Address of the read/write head to be deactivated
DeactivateAll-BusHeads		Deactivates the HF bus mode OPC UA and resets the settings to HF bus mode. Information about the read/write head addresses that were activated is lost.
	IdentChannel (UInt16)	RFID channel (Ident)
GetActivated-BusHeads		Shows the number and addresses of the activated read/write heads in an array.
	IdentChannel (UInt16)	RFID channel (Ident)

Method	Argument (type)	Description
	ActiveBusHeads (UInt32)	Addresses of the activated HF read/write heads
	NumberOfActiveBusHeads (UInt16)	Number of activated HF read/write heads
GetConnectedBusHeadAddresses		Reading of all addresses of the connected HF read/write heads irrespective of whether the HF read/write head is activated
	IdentChannel (UInt16)	RFID channel (Ident)
	ConnectedBusHeads (UInt32)	Addresses of the connected read/write heads
	NumberOfConnectedBusHeads (UInt16)	Number of connected HF read/write heads
SetBusHeadAddress		Sets a specific read/write head address (only one HF read/write head can be connected)
	IdentChannel (UInt16)	RFID channel (Ident)
	Bus Head Address (UInt16)	Address to be set in the connected HF read/write head

8.1.2 Variable Presence – tag present at read/write head

The **Presence** variable is set automatically if a read/write device detects a tag.

The variable is set by default in HF applications apart from with the **ScanStart** method. In HF bus mode, the **PresenceOnAntenna** variable indicates which of the connected HF read/write heads detected a tag in front of it or not.

All methods can be executed irrespective of whether the **Presence** variable is set. If no tag is present in the detection range at the time the method is sent, the method is executed as soon as there is a tag in the field of the read/write device. A method is executed immediately if there is a tag in the detection range at the time of sending.

8.1.3 Setting HF bus mode for OPC UA

HF bus mode for OPC UA supports the HF read/write heads from firmware version Vx.90. The **ScanStart** method for continuous reading in HF bus mode supports the HF read/write heads from firmware version Vx.93.

NOTE
The use of an HF read/write head with a firmware < Vx.90 in HF bus mode or < Vx.93 with the ScanStart method in HF bus mode can trigger the diagnostic message NOT_SUPPORTED_BY_DEVICE in the status or logbook.

The read/write heads can be addressed both automatically or via the **SetBusHeadAddress** method. The addresses must be assigned per channel from 1 to 32.

Addressing read/write heads automatically

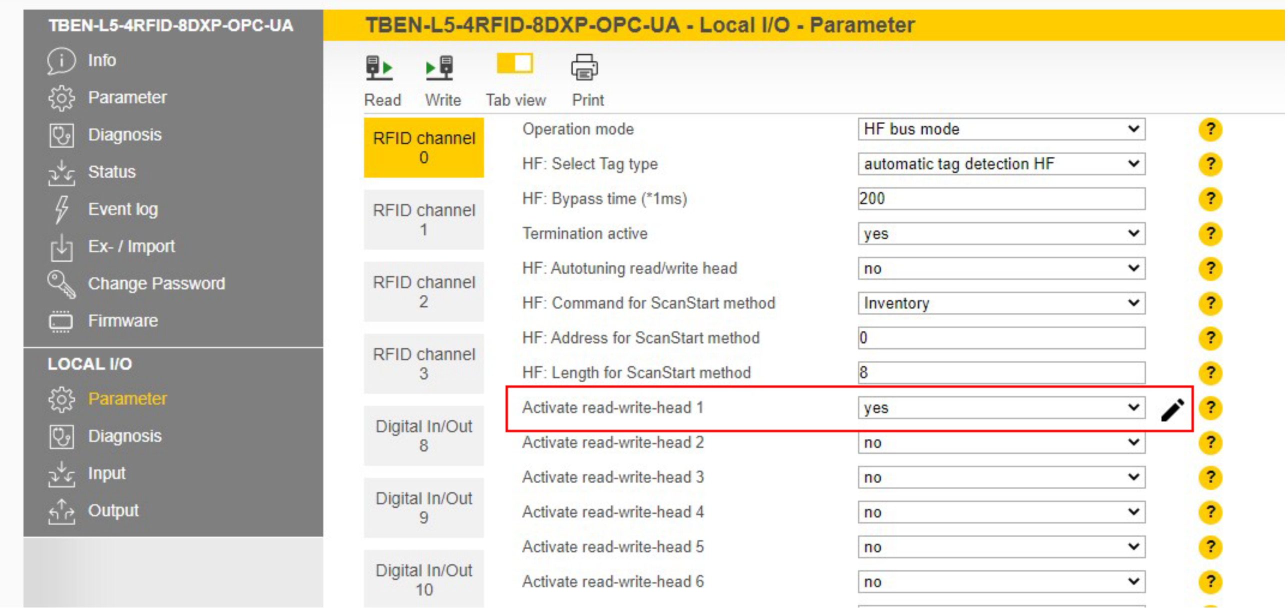
NOTE
Turck recommends making the bus address of the read/write head visible on the device. The label on the cable can be used to mark the address on the read/write head. The appropriate labels can be ordered with ID 6936206.

Read/write heads with the default bus address 68 can be automatically addressed. For this, either the **ActivateBusHead** method must be executed in the OPC UA client or the read/write heads must be activated in the web server.

- ▶ Switch on the RFID interface power supply.
- ▶ Activate the required read/write heads in the OPC UA client with the **ActivateBusHead** method.

or

- ▶ Activate the required read/write heads in the web server with **Activate read-write-head …**.



TBEN-L5-4RFID-8DXP-OPC-UA - Local I/O - Parameter

Operation mode	HF bus mode
HF: Select Tag type	automatic tag detection HF
HF: Bypass time (*1ms)	200
Termination active	yes
HF: Autotuning read/write head	no
HF: Command for ScanStart method	Inventory
HF: Address for ScanStart method	0
HF: Length for ScanStart method	8
Activate read-write-head 1	yes
Activate read-write-head 2	no
Activate read-write-head 3	no
Activate read-write-head 4	no
Activate read-write-head 5	no
Activate read-write-head 6	no

Fig. 51: Web server – example: Activate read/write head 1

- ▶ Connect the read/write heads to the interface in a line one by one.
- ➪ The read/write heads are automatically assigned addresses in ascending order in the order of connection. The lowest address is automatically assigned to the next connected read/write head with the default address 68.
- ➪ The addressing is successful if the LED of the read/write head is permanently lit.

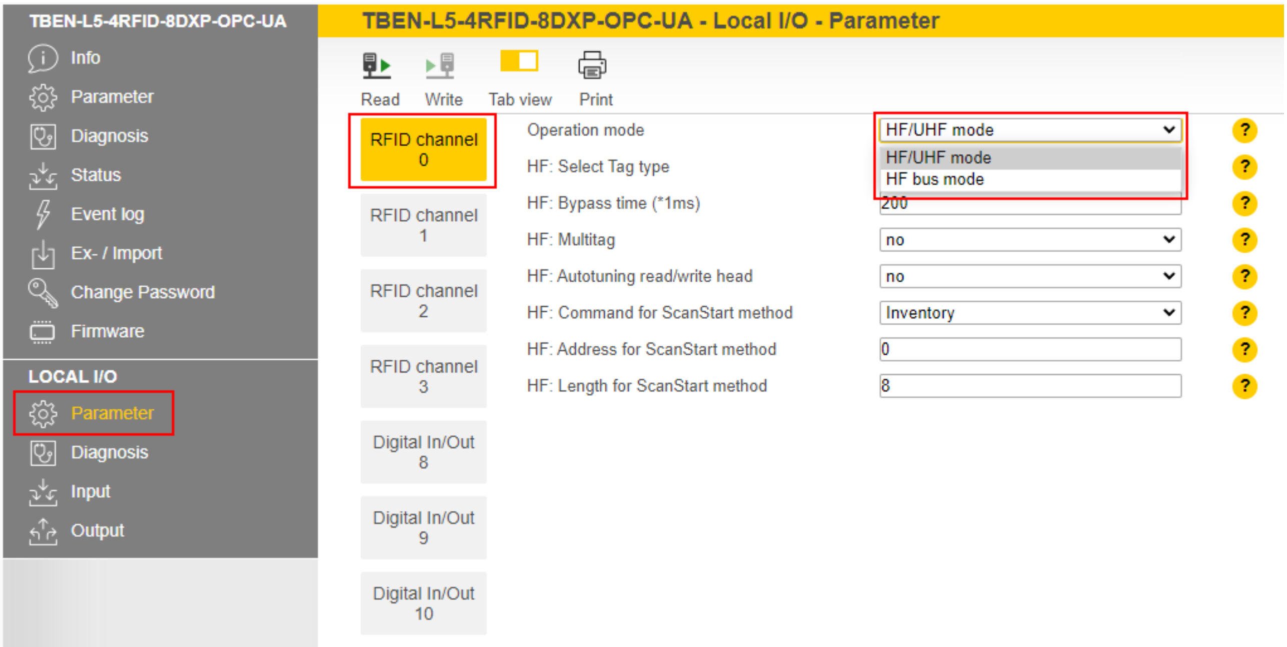
Activating or deactivating HF bus mode for OPC UA with methods

- ▶ Execute the **ActivateBusHead** method.
- ➪ The HF bus mode for OPC UA is activated as soon as at least one bus-capable read/write head with the specified address is connected. Only HF read/write heads with a valid bus address are detected.
- ➪ If at least one bus-capable HF read/write head with address 1…32 is connected, the corresponding channel (Ident …) is indicated as available.

In order for the OPC UA server on the Ident channel to detect UHF readers and HF read/write heads again without a bus function, HF bus mode for OPC UA must be reset.

- ▶ Reset HF bus mode: execute the **DeactivateAllBusHead** method.
- ➪ The OPC UA server detects on this Ident channel UHF readers and HF read/write heads again without a bus function.

The HF bus mode for OPC UA can also be activated and deactivated via the web server.



TBEN-L5-4RFID-8DXP-OPC-UA - Local I/O - Parameter

Operation mode	HF/UHF mode
HF: Select Tag type	
HF: Bypass time (*1ms)	200
HF: Multitag	no
HF: Autotuning read/write head	no
HF: Command for ScanStart method	Inventory
HF: Address for ScanStart method	0
HF: Length for ScanStart method	8

Fig. 52: Activating HF bus mode in the web server

If at least one HF read/write head is activated and connected in HF bus mode for OPC UA, the optional **EnableAntennas** and **PresenceOnAntenna** variables are available in the information model.

The **EnableAntennas** variable defines the read/write head with a specific address that can be used for executing the method. The variable can only activate a maximum of one read/write head and returns the address of the activated read/write head in a 32-bit structure. This does not take into consideration whether the read/write heads are connected or not.

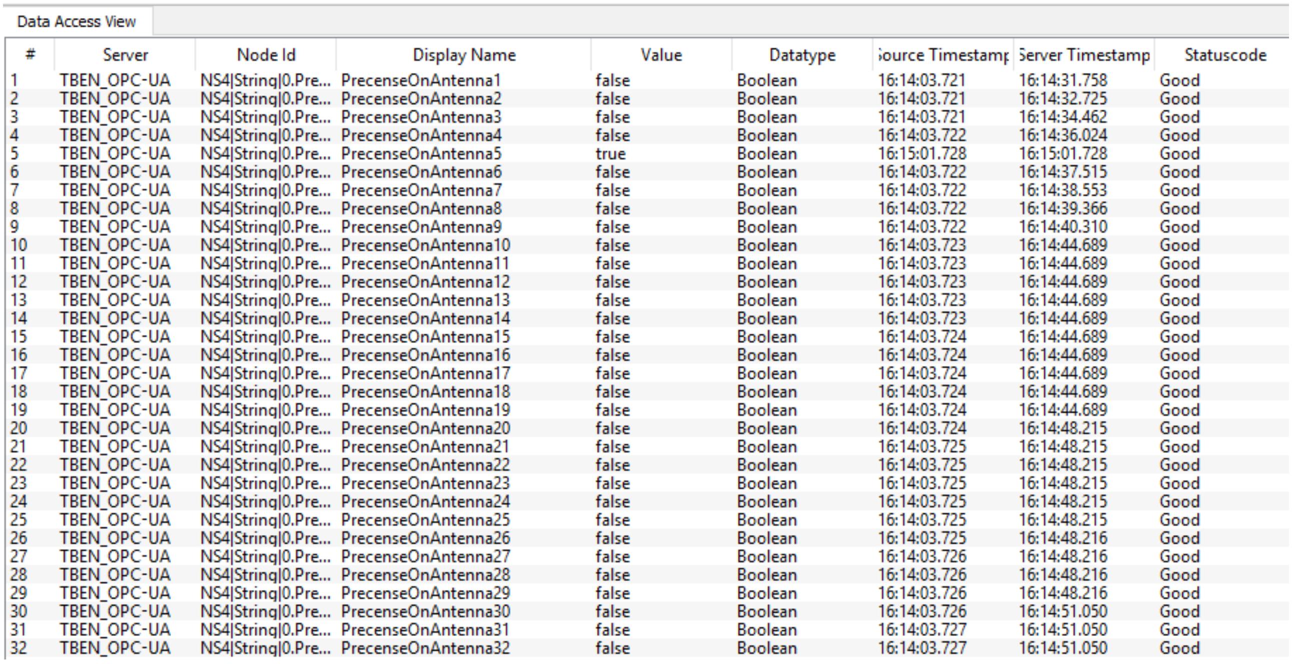
The appropriate read/write head address is selected with a bit code. Only addresses of active read/write heads can be selected and only one address can be active in order to execute methods such as Scan, ReadTag or WriteTag. Exception: the **ScanStart** method (also activated with the **ScanActive** variable) searches all activated addresses for tags and returns the corresponding read/write head address.

Read/write head address	**EnableAntennas value**	**Read/write head address**	**EnableAntennas value**
1	1	17	65536
2	2	18	131072
3	4	19	262144
4	8	20	524288
5	16	21	1048576
6	32	22	2097152
7	64	23	4194304
8	128	24	8388608
9	256	25	16777216
10	512	26	33554432
11	1024	27	67108864
12	2048	28	134217728
13	4096	29	268435456
14	8192	30	536870912
15	16384	31	1073741824
16	32768	32	2147483648

The value of EnableAntennas is calculated as follows: $2^{\text{Read/write head address – 1}}$

Bit position																																**Read/write head address**	**EnableAntennas value**
32	**31**	**30**	**29**	**28**	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**	**19**	**18**	**17**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	3	4
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	14	8192

The **PresenceOnAntenna** variable indicates which of the connected HF read/write heads detected a tag in front of it or not (true/false).



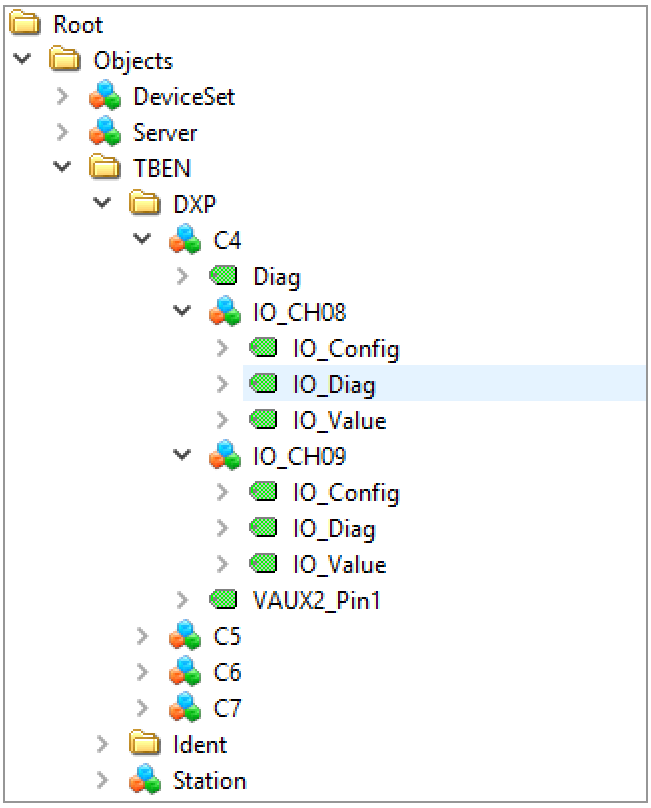
Data Access View

#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna1	false	Boolean	16:14:03.721	16:14:31.758	Good
2	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna2	false	Boolean	16:14:03.721	16:14:32.725	Good
3	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna3	false	Boolean	16:14:03.721	16:14:34.462	Good
4	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna4	false	Boolean	16:14:03.722	16:14:36.024	Good
5	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna5	true	Boolean	16:15:01.728	16:15:01.728	Good
6	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna6	false	Boolean	16:14:03.722	16:14:37.515	Good
7	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna7	false	Boolean	16:14:03.722	16:14:38.553	Good
8	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna8	false	Boolean	16:14:03.722	16:14:39.366	Good
9	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna9	false	Boolean	16:14:03.722	16:14:40.310	Good
10	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna10	false	Boolean	16:14:03.723	16:14:44.689	Good
11	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna11	false	Boolean	16:14:03.723	16:14:44.689	Good
12	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna12	false	Boolean	16:14:03.723	16:14:44.689	Good
13	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna13	false	Boolean	16:14:03.723	16:14:44.689	Good
14	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna14	false	Boolean	16:14:03.723	16:14:44.689	Good
15	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna15	false	Boolean	16:14:03.724	16:14:44.689	Good
16	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna16	false	Boolean	16:14:03.724	16:14:44.689	Good
17	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna17	false	Boolean	16:14:03.724	16:14:44.689	Good
18	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna18	false	Boolean	16:14:03.724	16:14:44.689	Good
19	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna19	false	Boolean	16:14:03.724	16:14:44.689	Good
20	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna20	false	Boolean	16:14:03.724	16:14:48.215	Good
21	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna21	false	Boolean	16:14:03.725	16:14:48.215	Good
22	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna22	false	Boolean	16:14:03.725	16:14:48.215	Good
23	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna23	false	Boolean	16:14:03.725	16:14:48.215	Good
24	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna24	false	Boolean	16:14:03.725	16:14:48.215	Good
25	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna25	false	Boolean	16:14:03.725	16:14:48.215	Good
26	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna26	false	Boolean	16:14:03.725	16:14:48.216	Good
27	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna27	false	Boolean	16:14:03.726	16:14:48.216	Good
28	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna28	false	Boolean	16:14:03.726	16:14:48.216	Good
29	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna29	false	Boolean	16:14:03.726	16:14:48.216	Good
30	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna30	false	Boolean	16:14:03.726	16:14:51.050	Good
31	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna31	false	Boolean	16:14:03.727	16:14:51.050	Good
32	TBEN_OPC-UA	NS4|String|0.Pre...	PrecenseOnAntenna32	false	Boolean	16:14:03.727	16:14:51.050	Good

Fig. 53: PresenceOnAntenna in HF bus mode variable (example: UAExpert)

8.1.4 Digital channels (DXP) – mapping in the information model

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



- Root
- Objects
  - DeviceSet
  - Server
  - TBEN
    - DXP
      - C4
        - Diag
        - IO_CH08
          - IO_Config
          - IO_Diag
          - IO_Value
        - IO_CH09
          - IO_Config
          - IO_Diag
          - IO_Value
        - VAUX2_Pin1
      - C5
      - C6
      - C7
    - Ident
    - Station

Fig. 54: Information model of DXP channels 8 and 9 – example: UAExpert

Variables – properties

Name	Description
IO_Config	0: Configure channel as a digital input 1: Configure channel as a digital output
IO_Diag	0: No error present 1: Error present
IO_Value	0: No signal present 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.

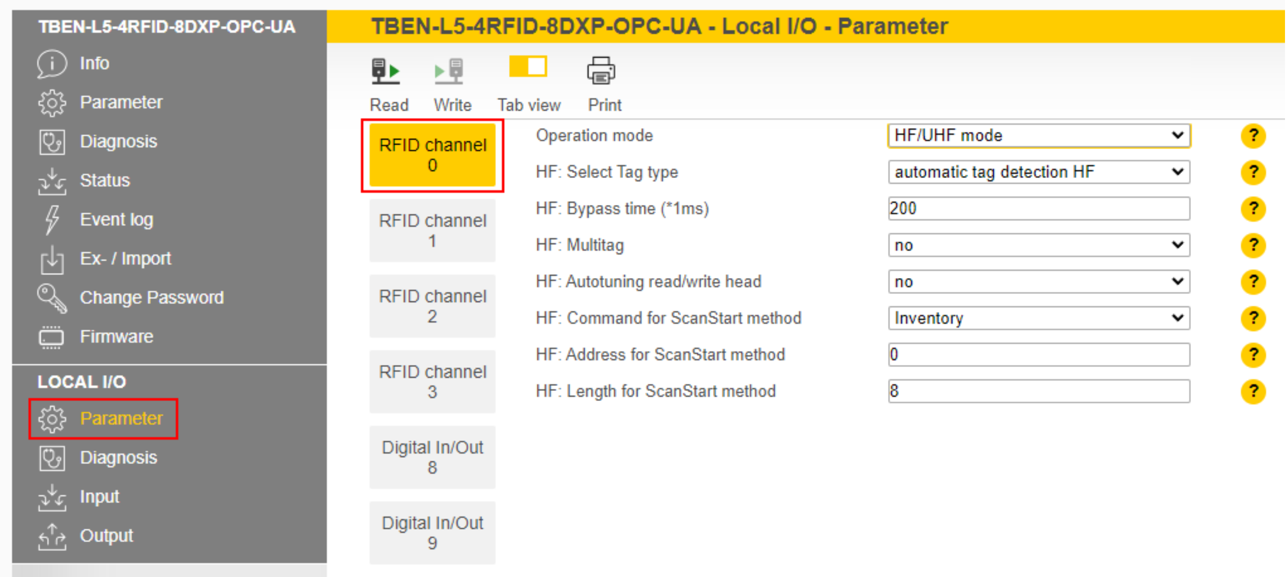
A login is required in order to edit settings via the web server. The default password is “password”.

NOTE
To ensure greater security, Turck recommends changing the password after the first login.

- Enter the password in the Login field on the start page of the web server.
- Click **Login**.

8.2.1 Setting RFID channel 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 RFID channel (here: **RFID channel 0**).
- Set the required RFID parameters.



Operation mode	HF/UHF mode
HF: Select Tag type	automatic tag detection HF
HF: Bypass time (*1ms)	200
HF: Multitag	no
HF: Autotuning read/write head	no
HF: Command for ScanStart method	Inventory
HF: Address for ScanStart method	0
HF: Length for ScanStart method	8

Fig. 55: Web server – RFID channel 0 parameters

RFID channels – meaning of the parameters

Default values are shown in **bold** type.

Designation	Meaning
Operation mode	▪ **HF/UHF mode** ▪ HF bus mode
HF: Select tag type	**0: Automatic HF tag detection** 1: NXP Icode SLIX 2: Fujitsu MB89R118 3: TI Tag-it HF-I Plus 4: Infineon SRF55V02P 5: NXP Icode SLIX-S 6: Fujitsu MB89R119 7: TI Tag-it HF-I 8: Infineon SRF55V10P 9: Reserved 10: Reserved 11: NXP Icode SLIX-L 12: Fujitsu MB89R112 13: EM4233SLIC Read/write heads with firmware from Vx.91 also support: 14: NXP SLIX2 15: TI Tag-it HFI Pro 16:Turck sensor tag 17: Infineon SRF55V02S 18: Infineon SRF55V10S 19: EM4233 20: EM4237 21: EM4237 SLIC 22: EM4237 SLIX 23: EM4033
HF: Bypass time (*ms)	Bridging time in ms, adjustable from 4…1020 ms, Default setting: **200 ms**
Termination active	Activates or deactivates the bus termination. Default setting: **On**
HF: Autotuning read/write head	Activates or deactivates the automatic tuning of the read/write heads. Default setting: **Off**
HF: Multitag	In HF applications several tags can be read or written in the detection range. Multitag mode is not possible in combination with the **ScanStart** method. A **Scan** operation outputs the UIDs of all tags in the detection range. The **LastScanData** variable always shows the last UID read. Default setting: **Off**
HF: Command for ScanStart method	▪ **Inventory**: The read/write device searches for tags in the detection range and reads the UID or EPC. ▪ Read: the read/write device reads the data (max. 64 bytes) of the tags in the detection range. If the **ScanStart** parameter is set to Read, a tag must be selected beforehand via the **HF: Select tag type** parameter. Automatic tag detection is not possible.

Designation	Meaning
HF: Address for ScanStart method	Start address of the UID or USER memory area on the tag to be read Default setting: **0**
HF: Length for ScanStart method	Number of bytes to be read with the **ScanStart** method Default setting: **8**
HF bus mode: Activate read/write head …	Activates or deactivates the read/write head with address ..... Default setting: **Off**

8.2.2 HF applications – selecting the tag type

- If the **ScanStart** parameter is set to Read, a tag must be selected beforehand. Automatic tag detection is not possible.
- In multitag applications select a tag type for the execution of the **read** and **write** methods. Automatic tag detection is not supported for the **read** and **write** commands in multitag mode.

The “RF communication error” is generated if the parameters of a tag located in the detection range of the read/write head do not match the selected tag type. In this case check the set tag type.

The tag type does not have to be selected in single tag applications and for the execution of inventory commands or scan methods in multitag applications if the read/write head detects the tags automatically.

Tag	Firmware version Read/write head	Selectable	Automatic detection possible	Displayed in web server
1: NXP Icode SLIX	≥ Vx.91	x	x	x
	≤ Vx.90	x	x	x
2: Fujitsu MB89R118	≥ Vx.91	x	x	x
	≤ Vx.90	x	x	x
3: TI Tag-it HF-I Plus	≥ Vx.91	x	x	x
	≤ Vx.90	x	x	x
4: Infineon SRF55V02P	≥ Vx.91	x	x	x
	≤ Vx.90	x	x	x
5: NXP Icode SLIX-S	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
6: Fujitsu MB89R119	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
7: TI Tag-it HF-I	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
8: Infineon SRF55V10P	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
11: NXP Icode SLIX-L	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
12: Fujitsu MB89R112	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x
13: EM4233SLIC	≥ Vx.91	x	x	x
	≤ Vx.90	x	–	x

Tag	Firmware version Read/write head	Selectable	Automatic detection possible	Displayed in web server
14: NXP SLIX2	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
15: TI Tag-it HFI Pro	≥ Vx.91	–	x	x
	≤ Vx.90	–	–	–
16: Turck sensor tag	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
17: Infineon SRF55V02S	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
18: Infineon SRF55V10S	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
19: EM4233	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
20: EM4237	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
21: EM4237 SLIC	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
22: EM4237 SLIX	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–
23: EM4033	≥ Vx.91	x	x	x
	≤ Vx.90	–	–	–

8.2.3 HF applications – setting the bridging time (bypass time)

Due to the expansion of the HF transmission zone the tag may drop out momentarily during a write or read operation and then later return again. The period between the drop out and the return to the transmission zone must be bridged so that the write or read operation is completed. The bridging time is the time between the dropout and the return to the detection range. The **Bypass time** parameter takes up one word in the parameter data image and is stated in ms.

The bridging time can be set between 4…1020 ms. The bridging time parameter depends on the components used, the write/read distances, the speed of the tag to the read/write head and other external factors.

The following figure shows the typical characteristics of the sensing range and the path covered by the read/write head. **A** shows the section to be bridged:

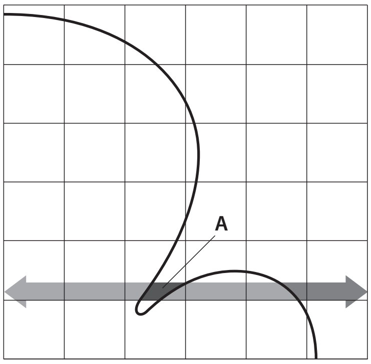


Fig. 56: Detection range of a read/write head

Retaining the default setting

- ▶ Retain the default setting: If the commissioning is successful, the parameter does not have to be adjusted to the application. If the commissioning is not successful, an error message will appear.
- ▶ If the error message appears, adjust the bridging time. If the bridging time cannot be adjusted, reduce the speed or the data volume.

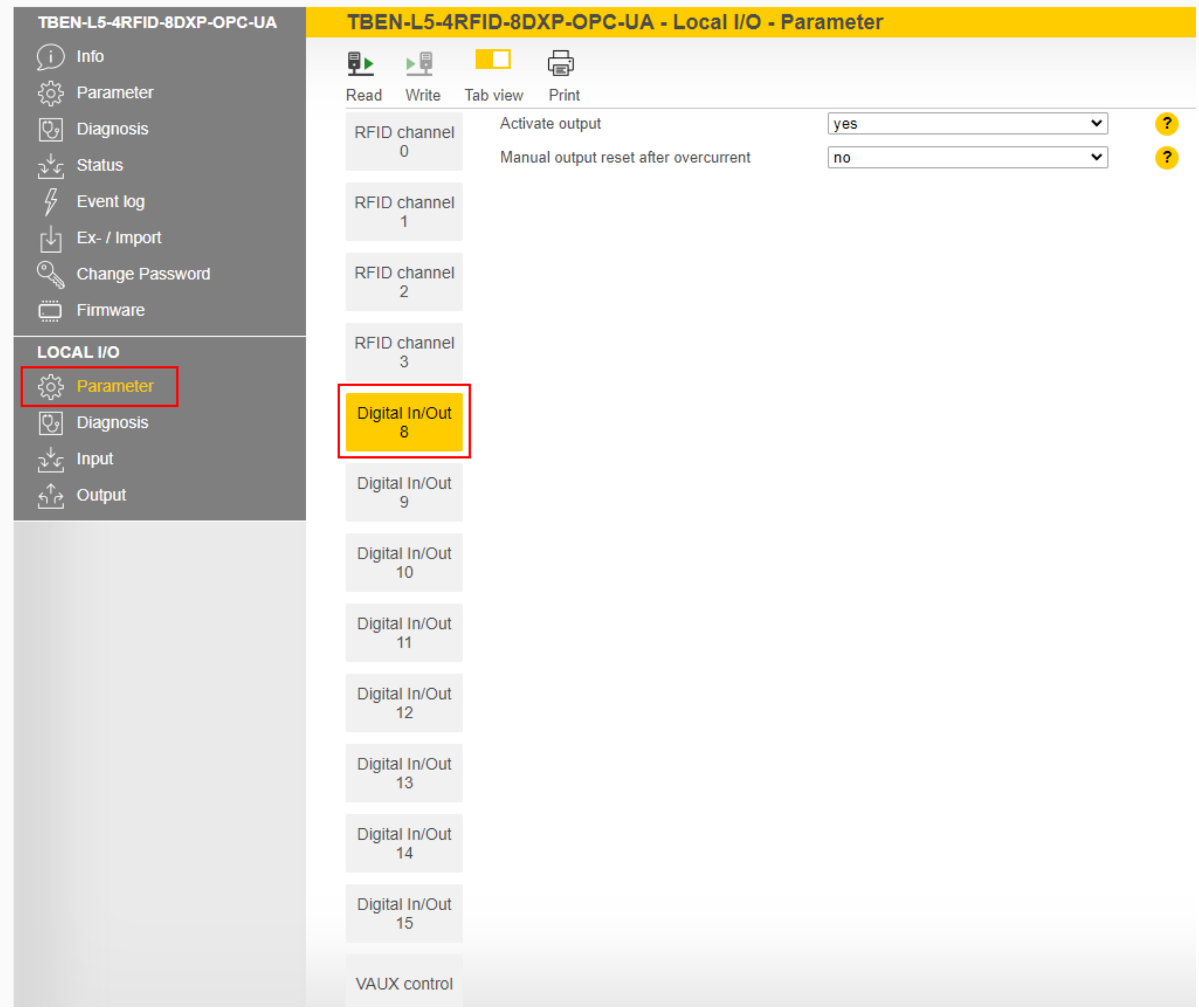
The “recommended” and “maximum distance” entries are shown in the product specific data sheet.

Adapting the bridging time to the application

- ▶ Measure the required bridging time directly on location. The LEDs of the read/write head and the TP status bit of process input data indicate whether the tag is in the sensing range or not.
- ▶ Enter the required bridging time.

8.2.4 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.



TBEN-L5-4RFID-8DXP-OPC-UA - Local I/O - Parameter

Activate output: yes

Manual output reset after overcurrent: no

Fig. 57: Web server – DXP channel 8 parameters

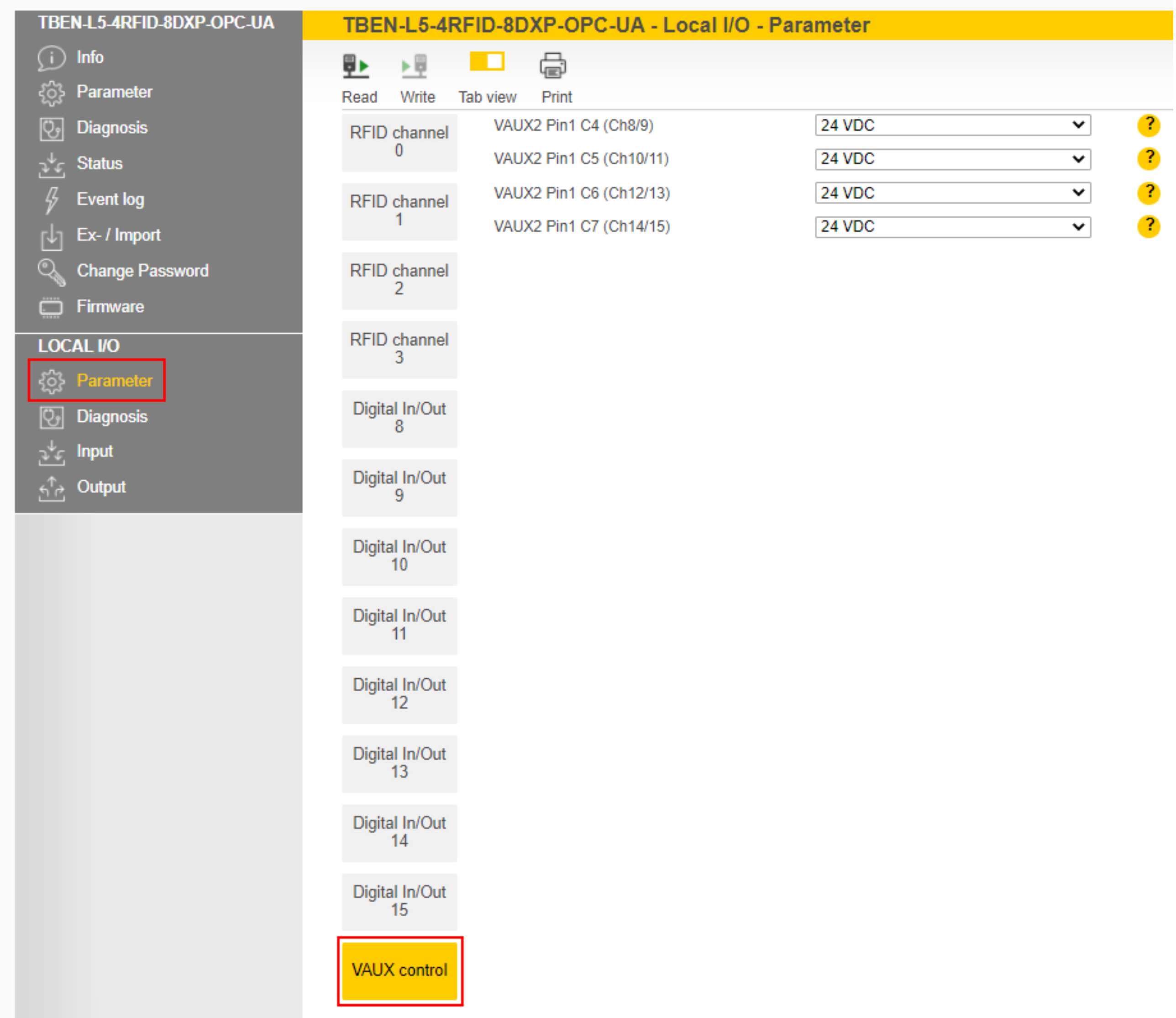
DXP channels – meaning of the parameters

Default values are shown in **bold** type.

Designation	Meaning
Activate output	**Yes: Output activated.** 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 **No: The output automatically switches back on after an overcurrent.**

8.2.5 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.



VAUX2 Pin1 C4 (Ch8/9)	24 VDC
VAUX2 Pin1 C5 (Ch10/11)	24 VDC
VAUX2 Pin1 C6 (Ch12/13)	24 VDC
VAUX2 Pin1 C7 (Ch14/15)	24 VDC

Fig. 58: Web server – VAUX control parameter

Switchable power supply – meaning of the parameters

Designation	Meaning
VAUX2 Pin1 C4 (Ch8/9)	Activates or deactivates the VAUX2 24 VDC power supply at pin 1 of channel 8 and channel 9. Default setting: **On**
VAUX2 Pin1 C5 (Ch10/11)	Activates or deactivates the VAUX2 24 VDC power supply at pin 1 of channel 10 and channel 11. Default setting: **On**
VAUX2 Pin1 C6 (Ch12/13)	Activates or deactivates the VAUX2 24 VDC power supply at pin 1 of channel 12 and channel 13. Default setting: **On**
VAUX2 Pin1 C7 (Ch14/15)	Activates or deactivates the VAUX2 24 VDC power supply at pin 1 of channel 14 and channel 15. Default setting: **On**

8.3 Setting RFID interface parameters via the DTM

The device can be assigned parameters with the DTM (Device Type Manager) via PACTware.

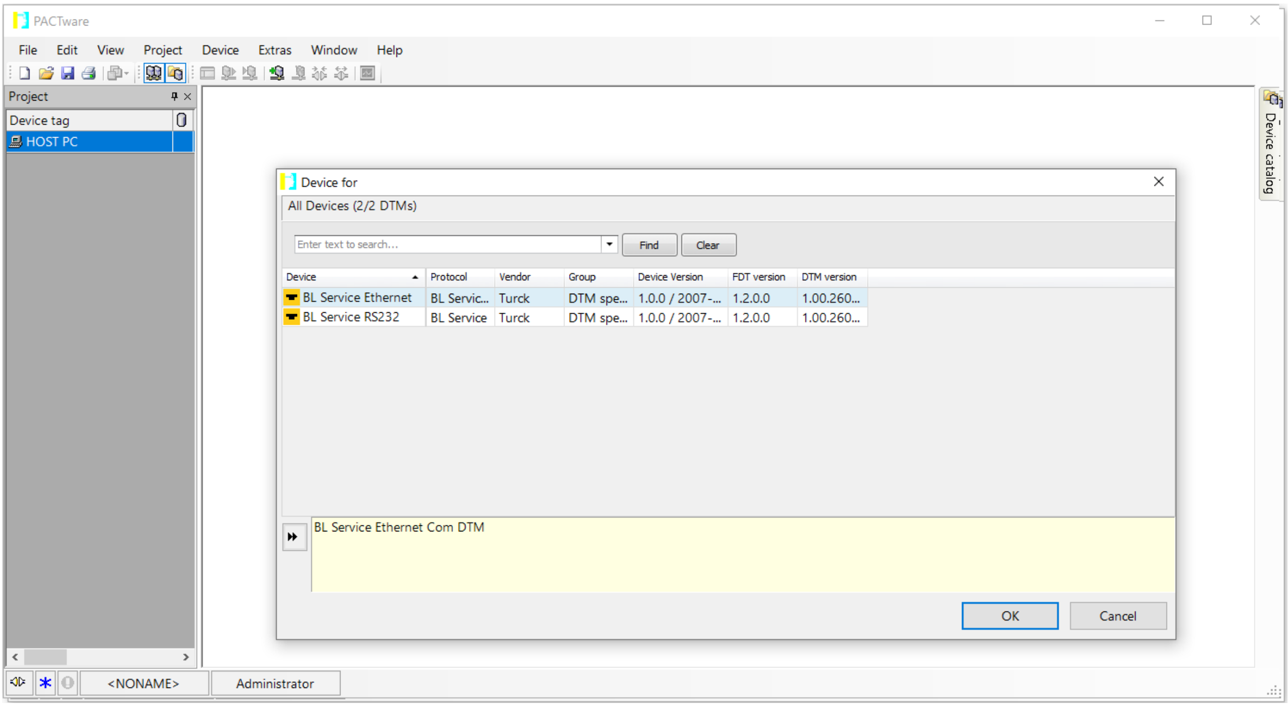
The different functions of the DTM are displayed by right-clicking the device in the project tree.

You can start the following functions:

- **Parameters**: Adapt parameters to the actual application
- **Diagnostics**: Display of the diagnostic messages of the device or the entire RFID system

8.3.1 Connecting the device with the PC

- ▶ Open PACTware.
- ▶ Right-click **Host PC** in the project tree.
- ▶ Click **Add device**.
- ▶ Select **BL Service Ethernet**.
- ▶ Confirm selection with **OK**.

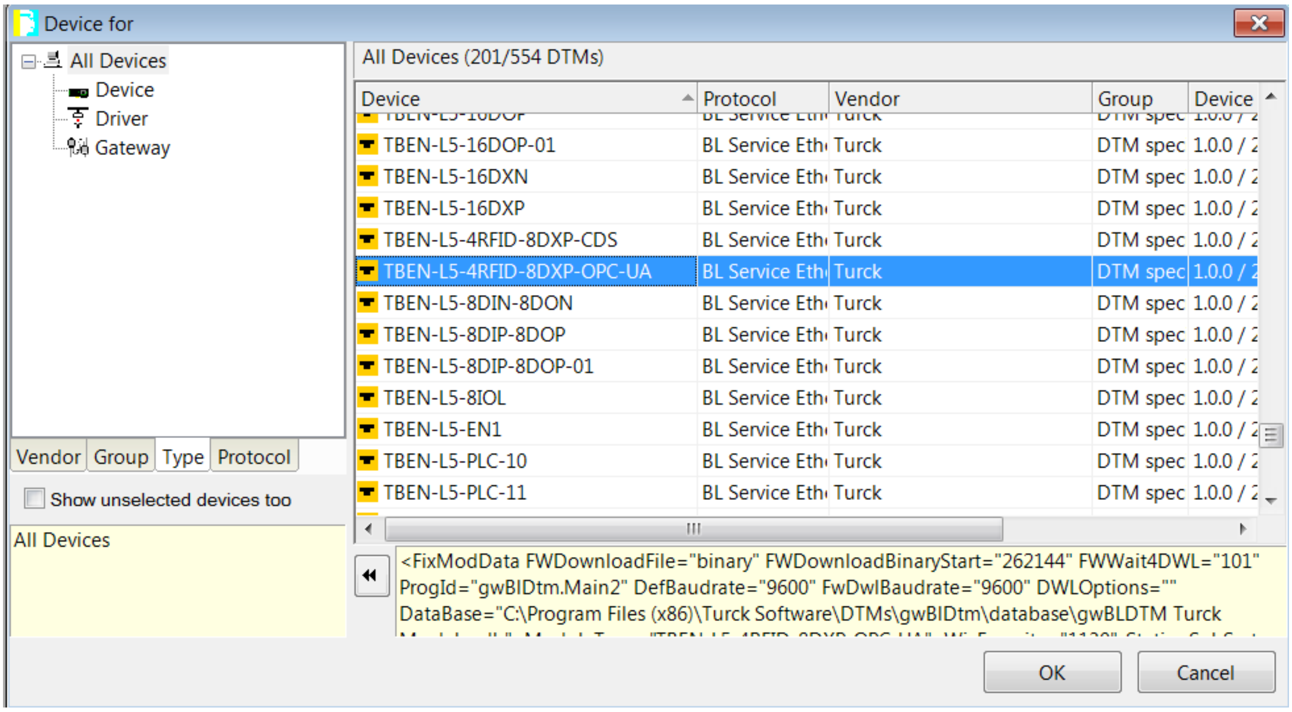


Device	Protocol	Vendor	Group	Device Version	FDT version	DTM version
BL Service Ethernet	BL Servic...	Turck	DTM spe...	1.0.0 / 2007-...	1.2.0.0	1.00.260...
BL Service RS232	BL Service	Turck	DTM spe...	1.0.0 / 2007-...	1.2.0.0	1.00.260...

BL Service Ethernet Com DTM

Fig. 59: Selecting an Ethernet adapter

- ▶ Right-click the Ethernet adapter in the project tree.
- ▶ Click **Add device**.
- ▶ Select TBEN-L…-4RFID-8DXP-OPC-UA.
- ▶ Confirm selection with **OK**.

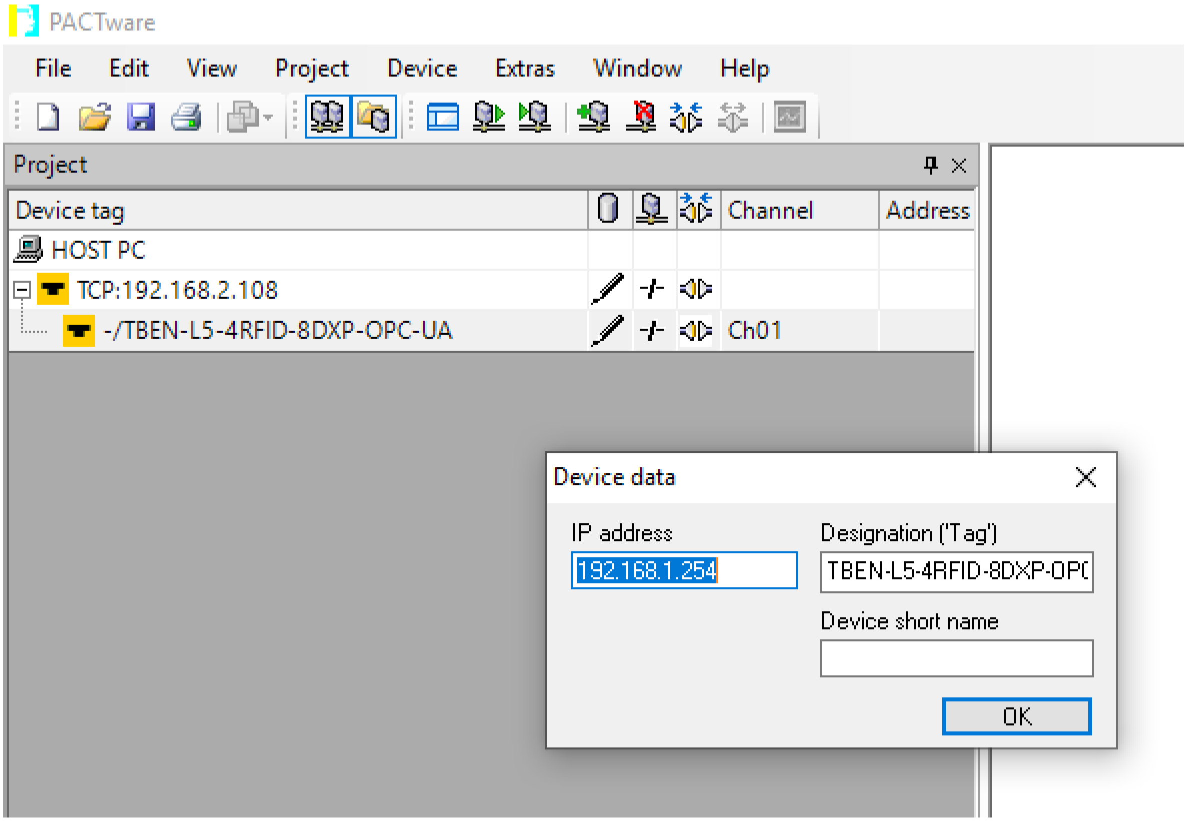


Device	Protocol	Vendor	Group	Device
TBEN-L5-16DOP	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-16DOP-01	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-16DXN	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-16DXP	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-4RFID-8DXP-CDS	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-4RFID-8DXP-OPC-UA	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-8DIN-8DON	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-8DIP-8DOP	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-8DIP-8DOP-01	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-8IOL	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-EN1	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-PLC-10	BL Service Eth	Turck	DTM spec	1.0.0 / 2
TBEN-L5-PLC-11	BL Service Eth	Turck	DTM spec	1.0.0 / 2

```
<FixModData FWDownloadFile="binary" FWDownloadBinaryStart="262144" FWWait4DWL="101"
ProgId="gwBIDtm.Main2" DefBaudrate="9600" FwDwlBaudrate="9600" DWLOptions=""
DataBase="C:\Program Files (x86)\Turck Software\DTMs\gwBIDtm\database\gwBLDTM Turck
```

Fig. 60: TBEN-L…-4RFID-8DXP-OPC-UA

- ▶ Enter the **IP address** of the device (example: 192.168.1.254)
- ▶ Optional: enter the **designation** and **device description**.
- ▶ Confirm entries with **OK**.



Device tag				Channel	Address
HOST PC					
TCP:192.168.2.108					
-/TBEN-L5-4RFID-8DXP-OPC-UA				Ch01	

Device data

IP address: 192.168.1.254

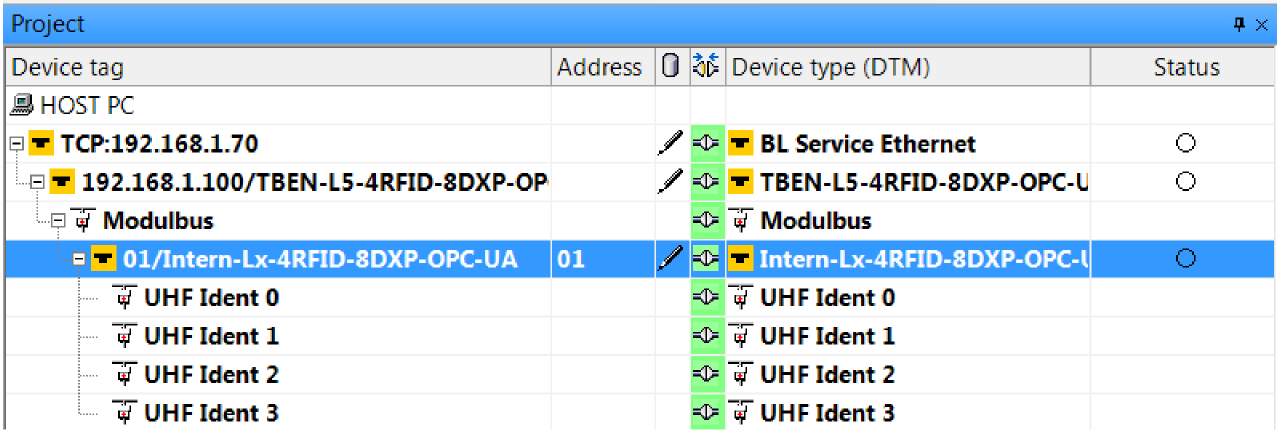
Designation ('Tag'): TBEN-L5-4RFID-8DXP-OP(

Device short name:

OK

Fig. 61: Entering the IP address

- ✓ The project tree is complete.
- ▶ Right-click the device in the project tree.
- ▶ Click **Connect**.
- ➪ After connecting, read and write access to input, output and parameter data is possible.



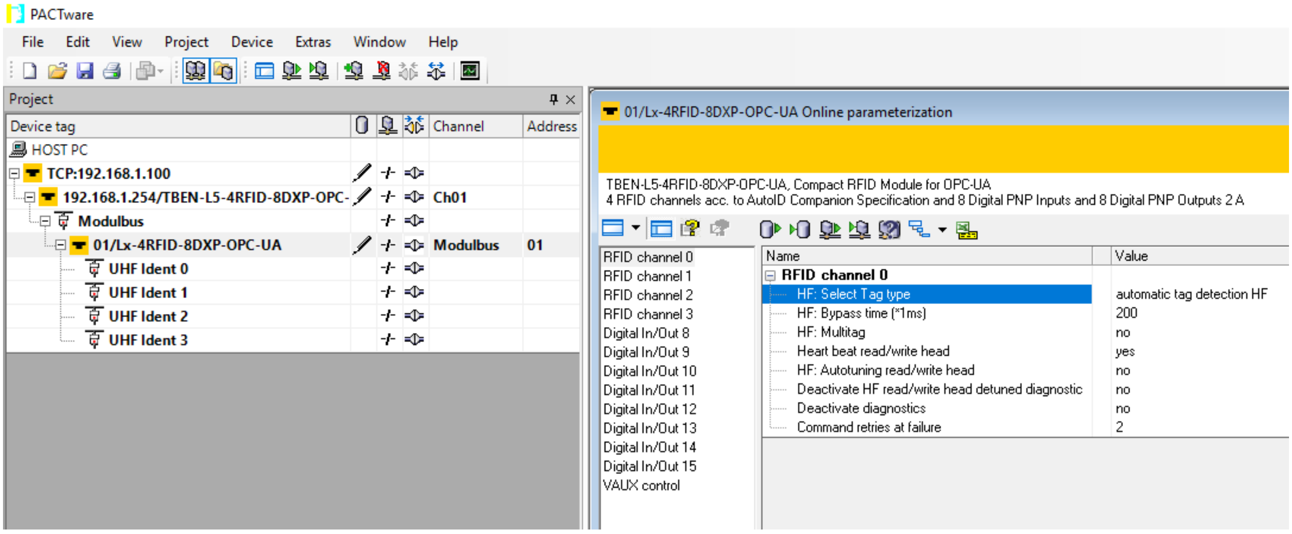
Device tag	Address			Device type (DTM)	Status
HOST PC					
TCP:192.168.1.70				**BL Service Ethernet**	○
192.168.1.100/TBEN-L5-4RFID-8DXP-OP				**TBEN-L5-4RFID-8DXP-OPC-U**	○
Modulbus				**Modulbus**	
01/Intern-Lx-4RFID-8DXP-OPC-UA	**01**			**Intern-Lx-4RFID-8DXP-OPC-U**	○
UHF Ident 0				**UHF Ident 0**	
UHF Ident 1				**UHF Ident 1**	
UHF Ident 2				**UHF Ident 2**	
UHF Ident 3				**UHF Ident 3**	

Fig. 62: Complete project tree

8.3.2 Editing parameter data with the DTM – online parameterization

The online parameterization function enables parameter data to be changed and written to the device.

- ▶ Right-click the device in the project tree.
- ▶ Click **Online parameterization**.



Device tag	Channel	Address
HOST PC		
TCP:192.168.1.100		
192.168.1.254/TBEN-L5-4RFID-8DXP-OPC-	Ch01	
Modulbus		
01/Lx-4RFID-8DXP-OPC-UA	Modulbus	01
UHF Ident 0		
UHF Ident 1		
UHF Ident 2		
UHF Ident 3		

01/Lx-4RFID-8DXP-OPC-UA Online parameterization

TBEN-L5-4RFID-8DXP-OPC-UA, Compact RFID Module for OPC-UA
4 RFID channels acc. to AutoID Companion Specification and 8 Digital PNP Inputs and 8 Digital PNP Outputs 2 A

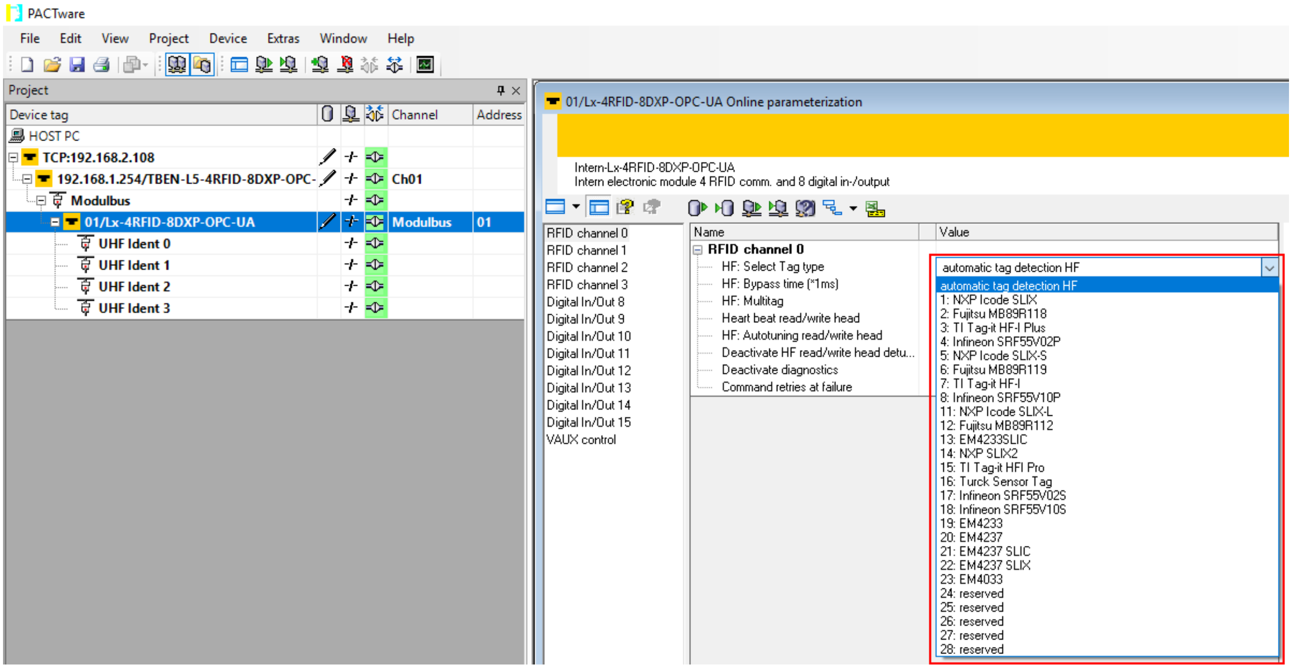
RFID channel 0
RFID channel 1
RFID channel 2
RFID channel 3
Digital In/Out 8
Digital In/Out 9
Digital In/Out 10
Digital In/Out 11
Digital In/Out 12
Digital In/Out 13
Digital In/Out 14
Digital In/Out 15
VAUX control

Name	Value
RFID channel 0	
HF: Select Tag type	automatic tag detection HF
HF: Bypass time (*1ms)	200
HF: Multitag	no
Heart beat read/write head	yes
HF: Autotuning read/write head	no
Deactivate HF read/write head detuned diagnostic	no
Deactivate diagnostics	no
Command retries at failure	2

Fig. 63: Parameterization

Example: selecting the tag type

- ▶ Click the tag type in the **Online Parameterization** window.
- ▶ Select the required tag from the drop-down menu.



Device tag	Channel	Address
HOST PC		
TCP:192.168.2.108		
192.168.1.254/TBEN-L5-4RFID-8DXP-OPC-	Ch01	
Modulbus		
01/Lx-4RFID-8DXP-OPC-UA	Modulbus	01
UHF Ident 0		
UHF Ident 1		
UHF Ident 2		
UHF Ident 3		

01/Lx-4RFID-8DXP-OPC-UA Online parameterization

Intern-Lx-4RFID-8DXP-OPC-UA
Intern electronic module 4 RFID comm. and 8 digital in-/output

RFID channel 0
RFID channel 1
RFID channel 2
RFID channel 3
Digital In/Out 8
Digital In/Out 9
Digital In/Out 10
Digital In/Out 11
Digital In/Out 12
Digital In/Out 13
Digital In/Out 14
Digital In/Out 15
VAUX control

Name	Value
RFID channel 0	
HF: Select Tag type	automatic tag detection HF
HF: Bypass time (*1ms)	
HF: Multitag	
Heart beat read/write head	
HF: Autotuning read/write head	
Deactivate HF read/write head detu...	
Deactivate diagnostics	
Command retries at failure	

automatic tag detection HF
1: NXP Icode SLIX
2: Fujitsu MB89R118
3: TI Tag-it HF-I Plus
4: Infineon SRF55V02P
5: NXP Icode SLIX-S
6: Fujitsu MB89R119
7: TI Tag-it HF-I
8: Infineon SRF55V10P
11: NXP Icode SLIX-L
12: Fujitsu MB89R112
13: EM4233SLIC
14: NXP SLIX2
15: TI Tag-it HFI Pro
16: Turck Sensor Tag
17: Infineon SRF55V02S
18: Infineon SRF55V10S
19: EM4233
20: EM4237
21: EM4237 SLIC
22: EM4237 SLIX
23: EM4033
24: reserved
25: reserved
26: reserved
27: reserved
28: reserved

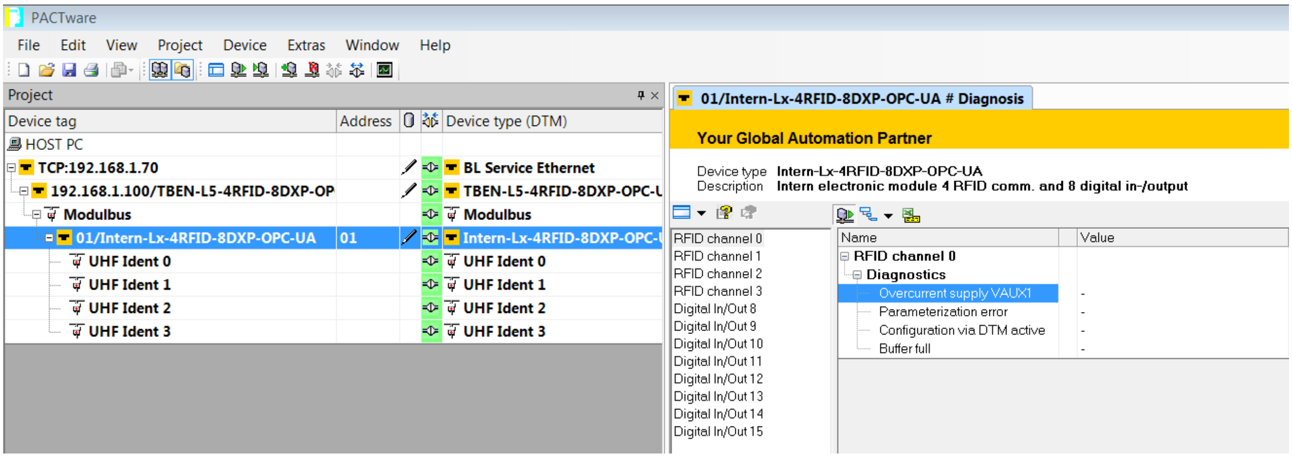
Fig. 64: Selecting the tag type

8.3.3 Evaluating diagnostics with the DTM

The diagnostics function of the DTM enables the diagnostics of all channels and general module diagnostics to be called.

Calling channel diagnostics

- ▶ Right-click the device **(01/Intern-Lx-4RFID-8DXP-OPC-UA)** in the project tree.
- ▶ Click **Diagnosis**.
- ▶ Select in the middle window the required channel.
- ➪ The diagnostic data is displayed in the window on the right-hand side (example: no diagnostic messages are present for RFID channel 0).



Device tag	Address	Device type (DTM)
HOST PC		
TCP:192.168.1.70		BL Service Ethernet
192.168.1.100/TBEN-L5-4RFID-8DXP-OP		TBEN-L5-4RFID-8DXP-OPC-U
Modulbus		Modulbus
01/Intern-Lx-4RFID-8DXP-OPC-UA	01	Intern-Lx-4RFID-8DXP-OPC-U
UHF Ident 0		UHF Ident 0
UHF Ident 1		UHF Ident 1
UHF Ident 2		UHF Ident 2
UHF Ident 3		UHF Ident 3

01/Intern-Lx-4RFID-8DXP-OPC-UA # Diagnosis

Your Global Automation Partner

Device type Intern-Lx-4RFID-8DXP-OPC-UA
Description Intern electronic module 4 RFID comm. and 8 digital in-/output

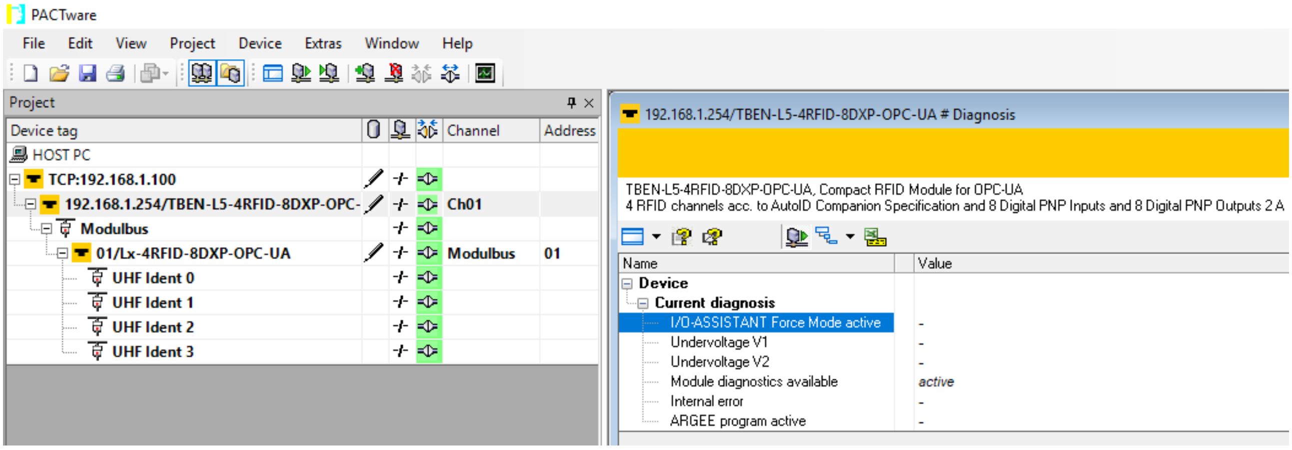
RFID channel 0
RFID channel 1
RFID channel 2
RFID channel 3
Digital In/Out 8
Digital In/Out 9
Digital In/Out 10
Digital In/Out 11
Digital In/Out 12
Digital In/Out 13
Digital In/Out 14
Digital In/Out 15

Name	Value
RFID channel 0	
Diagnostics	
Overcurrent supply VAUX1	-
Parameterization error	-
Configuration via DTM active	-
Buffer full	-

Fig. 65: DTM – channel diagnostics

Calling module diagnostics

- ▶ Right-click the device in the project tree
(here: **192.168.1.100/TBEN-L5-4RFID-8DXP-OPC-UA**).
- ▶ Click **Diagnosis**.
- ➪ The diagnostic data is displayed in the window on the right-hand side (example: no diagnostic messages are present for the module).



Device tag	Channel	Address
HOST PC		
TCP:192.168.1.100		
192.168.1.254/TBEN-L5-4RFID-8DXP-OPC-	Ch01	
Modulbus		
01/Lx-4RFID-8DXP-OPC-UA	Modulbus	01
UHF Ident 0		
UHF Ident 1		
UHF Ident 2		
UHF Ident 3		

192.168.1.254/TBEN-L5-4RFID-8DXP-OPC-UA # Diagnosis

TBEN-L5-4RFID-8DXP-OPC-UA, Compact RFID Module for OPC-UA
4 RFID channels acc. to AutoID Companion Specification and 8 Digital PNP Inputs and 8 Digital PNP Outputs 2 A

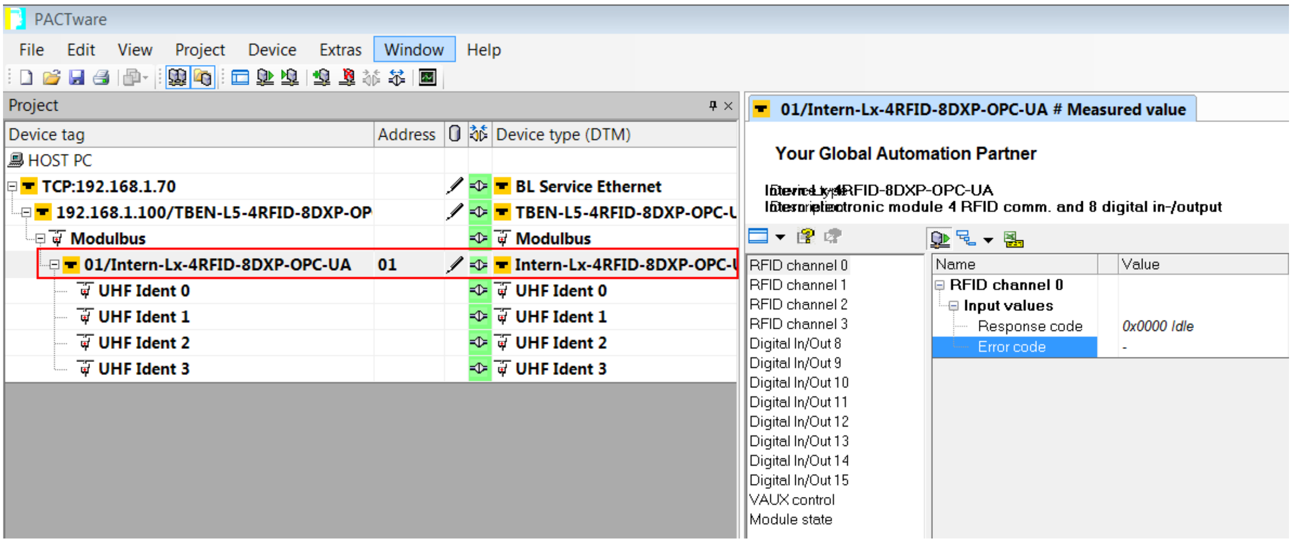
Name	Value
Device	
Current diagnosis	
I/O-ASSISTANT Force Mode active	-
Undervoltage V1	-
Undervoltage V2	-
Module diagnostics available	*active*
Internal error	-
ARGEE program active	-

Fig. 66: DTM – module diagnostics

8.3.4 Reading process input data with the DTM – measured value

The measured value function of the DTM enables the reading of the process input data.

- ▶ Right-click the device (**01/Intern-Lx-4RFID-8DXP-OPC-UA**) in the project tree.
- ▶ Click **Measured value**.
- ▶ Select in the middle window the required channel.
- ➩ The process input data is displayed in the window on the right-hand side. (example: the device is in Idle mode. Error messages are not present.)



PACTware
File Edit View Project Device Extras Window Help
Project
01/Intern-Lx-4RFID-8DXP-OPC-UA # Measured value
Your Global Automation Partner

Device tag	Address			Device type (DTM)
HOST PC				
TCP:192.168.1.70				BL Service Ethernet
192.168.1.100/TBEN-L5-4RFID-8DXP-OP				TBEN-L5-4RFID-8DXP-OPC-U
Modulbus				Modulbus
01/Intern-Lx-4RFID-8DXP-OPC-UA	01			Intern-Lx-4RFID-8DXP-OPC-U
UHF Ident 0				UHF Ident 0
UHF Ident 1				UHF Ident 1
UHF Ident 2				UHF Ident 2
UHF Ident 3				UHF Ident 3

Device type: Intern-Lx-4RFID-8DXP-OPC-UA
Description: Electronic module 4 RFID comm. and 8 digital in-/output

RFID channel 0
RFID channel 1
RFID channel 2
RFID channel 3
Digital In/Out 8
Digital In/Out 9
Digital In/Out 10
Digital In/Out 11
Digital In/Out 12
Digital In/Out 13
Digital In/Out 14
Digital In/Out 15
VAUX control
Module state

Name	Value
RFID channel 0	
Input values	
Response code	*0x0000 Idle*
Error code	-

Fig. 67: DTM – reading out measured values

8.4 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

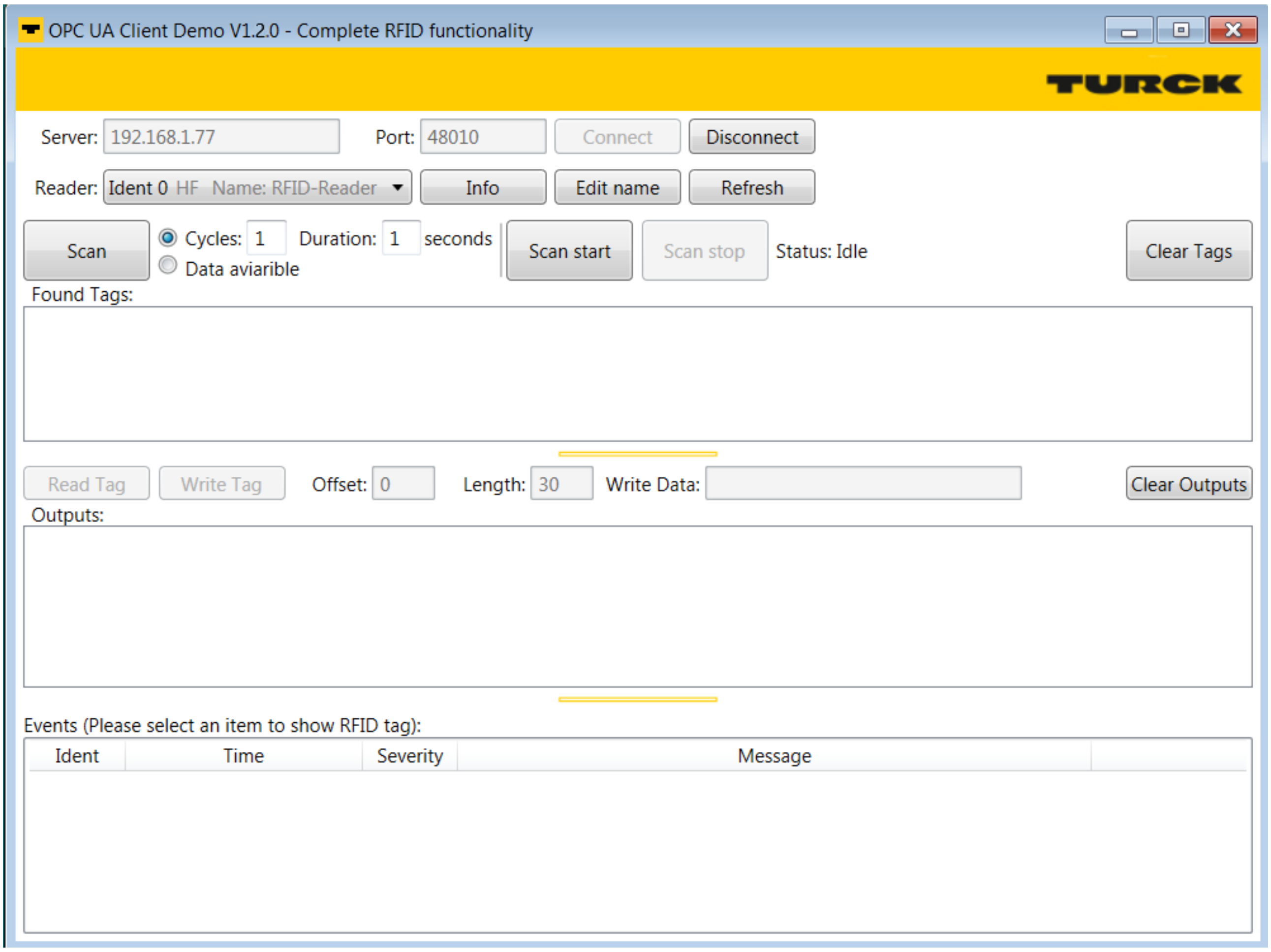
8.4.1 Testing RFID methods

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”



Server: 192.168.1.77 Port: 48010

Reader: Ident 0 HF Name: RFID-Reader

● Cycles: 1 Duration: 1 seconds

○ Data aviarible

Status: Idle

Offset: 0 Length: 30 Write Data:

Fig. 68: 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.

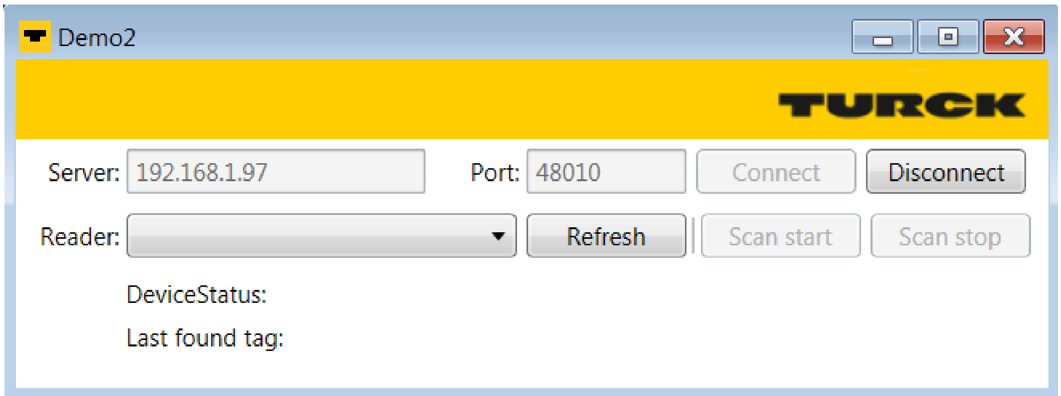
- ▶ Select tags for further processing.
- ▶ Adjust the offset and length if required.
- ▶ Read data from the tag: Click **Read Tag**.
- ▶ Writing data to the tag: Enter the required data and click **Write Tag**.

8.4.2 Testing the reading of UID or 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”



Server: 192.168.1.97

Port: 48010

Reader:

DeviceStatus:

Last found tag:

Fig. 69: 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 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**.
- ▶ Click **ScanStart**.

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

8.5 Setting UHF readers

8.5.1 Setting UHF readers via the DTM

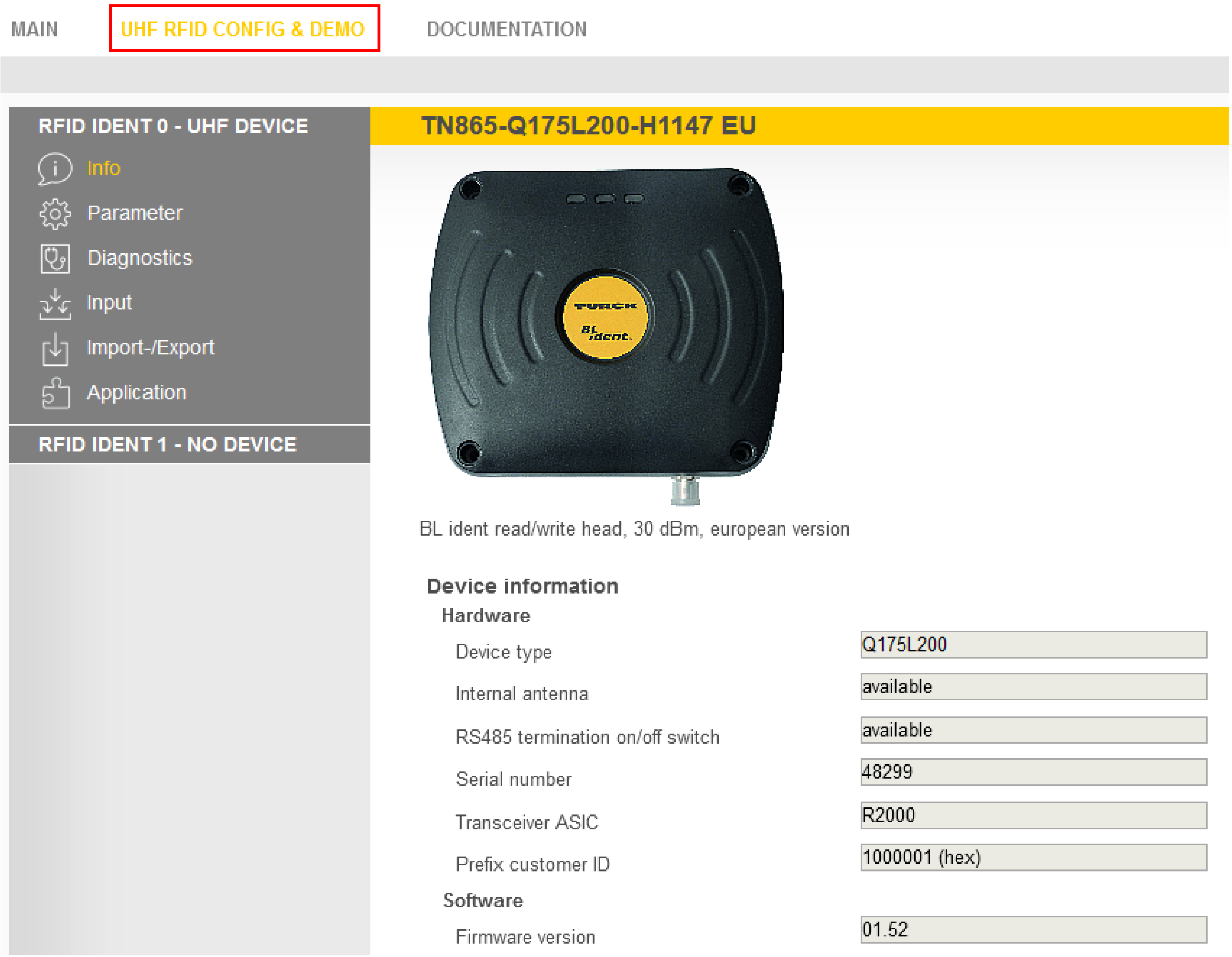
UHF readers can be assigned additional parameters via a DTM. No parameters can be set in UHF readers via the parameter data of the interface. The DTM for the specific device is available for download from www.turck.com.

A comprehensive description of the settings for UHF readers is provided in the instructions for use of the specific device.

8.5.2 Setting UHF readers via the web server

UHF readers can be set and commands sent to the readers via the web server.

- ▶ Open the web server and log in.
- ▶ Click **UHF RFID CONFIG & DEMO** to display and set the device parameters.



TN865-Q175L200-H1147 EU

BL ident read/write head, 30 dBm, european version

Device information

Hardware

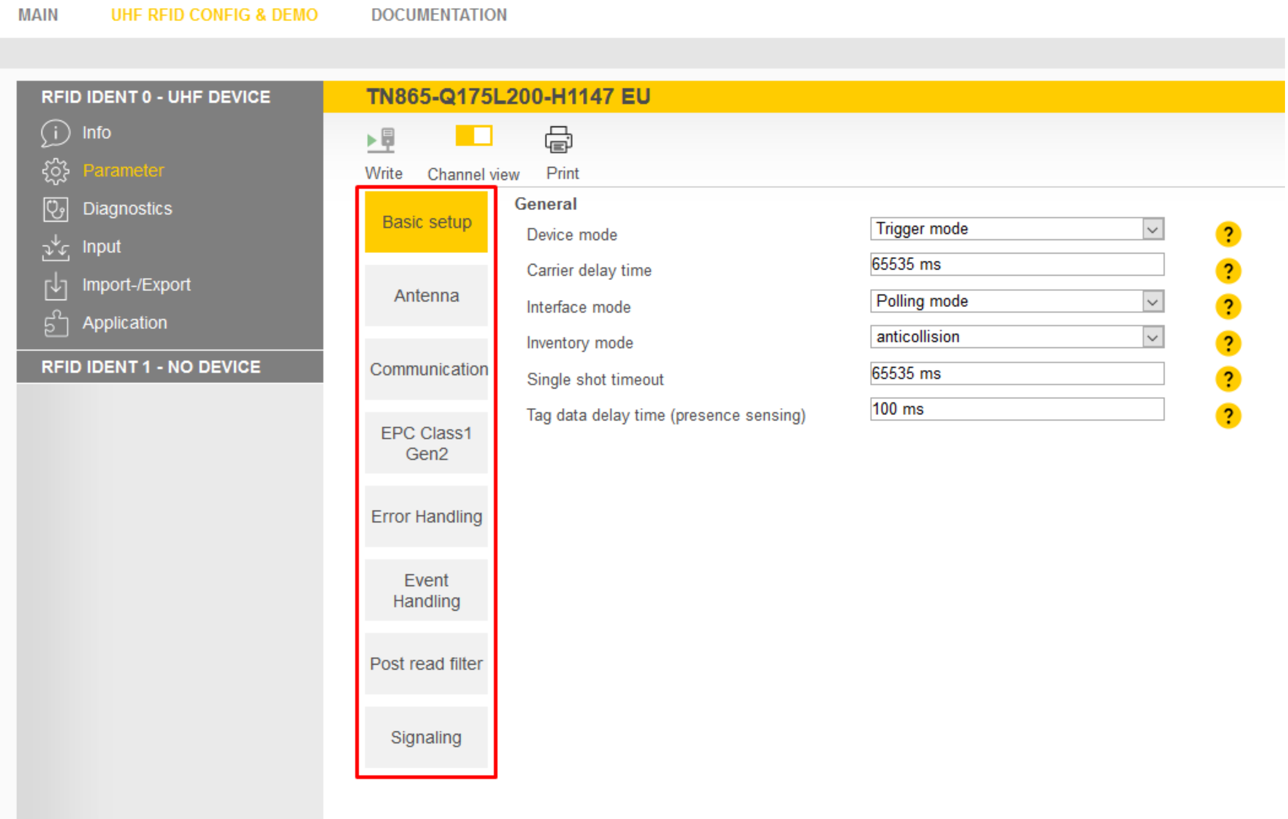
Device type	Q175L200
Internal antenna	available
RS485 termination on/off switch	available
Serial number	48299
Transceiver ASIC	R2000
Prefix customer ID	1000001 (hex)

Software

Firmware version	01.52

Fig. 70: Web server – start page UHF reader

- ▶ Click **Parameter** in the navigation bar on the left of the screen.
- ➪ All parameters of the device are displayed.



General

Device mode	Trigger mode
Carrier delay time	65535 ms
Interface mode	Polling mode
Inventory mode	anticollision
Single shot timeout	65535 ms
Tag data delay time (presence sensing)	100 ms

Fig. 71: Web server – UHF reader parameters

NOTE
The parameters are arranged in the web server in the same way as in the UHF DTM. The access level displayed in the web server corresponds to the Advanced level in the DTM.

8.5.3 Testing UHF readers via the web server

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

▶ Click **UHF RFID CONFIG & DEMO** → **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 Diagnostics**: The graphs show 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.

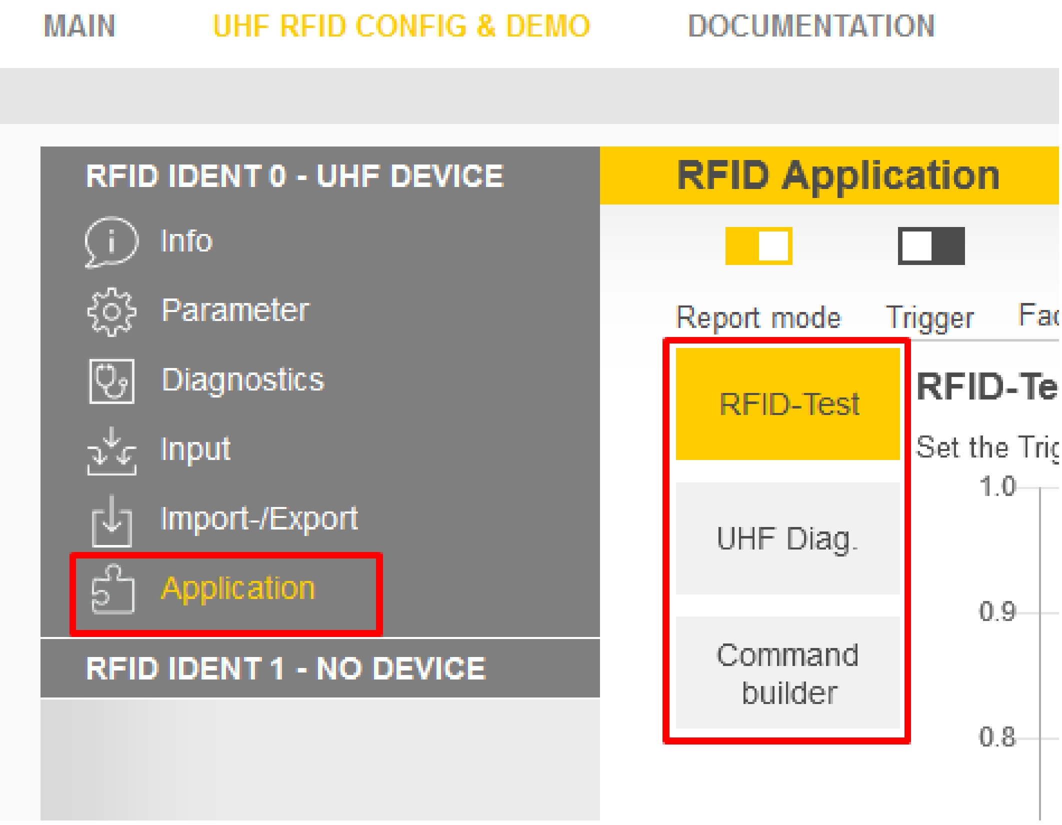
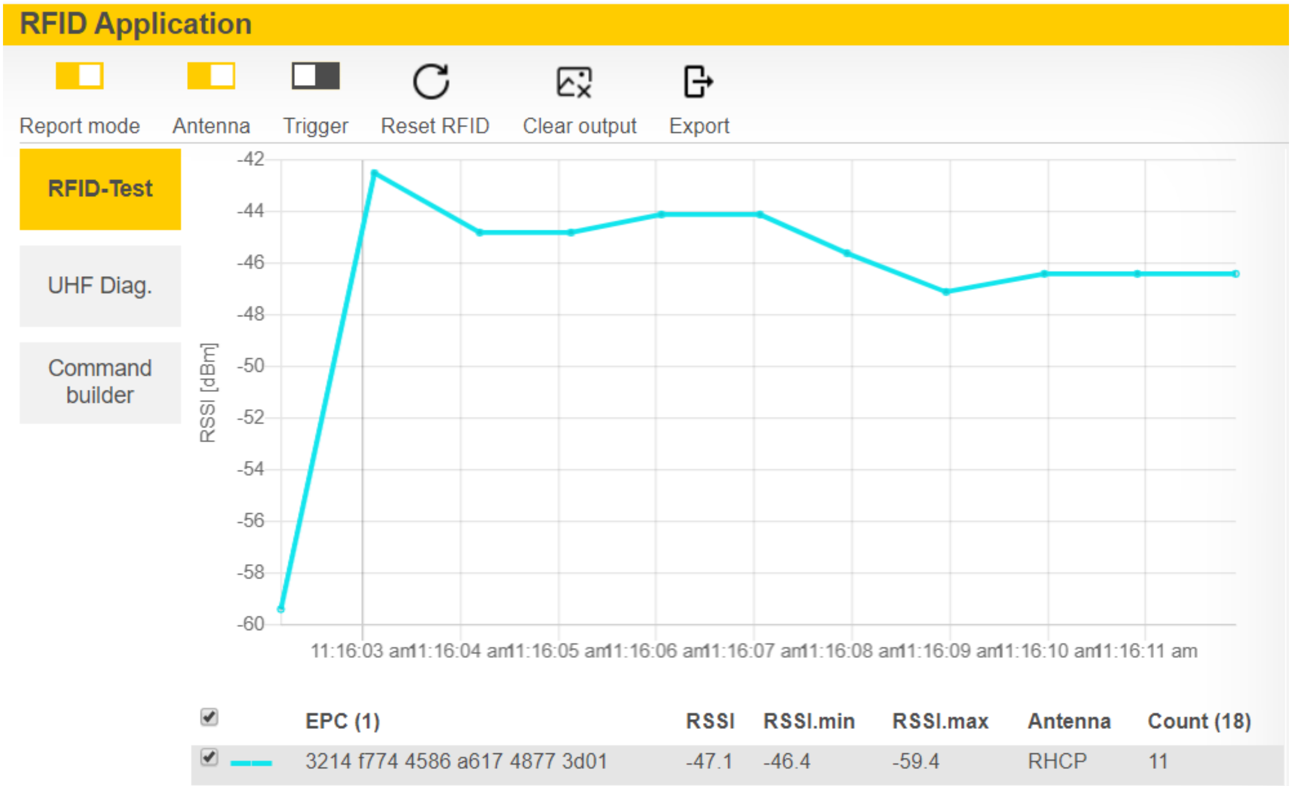


Fig. 72: Web server – RFID application

RFID Test enables EPC information on tags to be displayed and read out in single tag and multitag mode. The received RSSI values are displayed as a curve in relation to time.



☑	EPC (1)	RSSI	RSSI.min	RSSI.max	Antenna	Count (18)
☑	3214 f774 4586 a617 4877 3d01	-47.1	-46.4	-59.4	RHCP	11

Fig. 73: Example of RFID test: detection of a tag with received RSSI values over time and the number of read operations

The currently received power level for each channel of the reader is displayed in the **UHF Diagnostics** window.

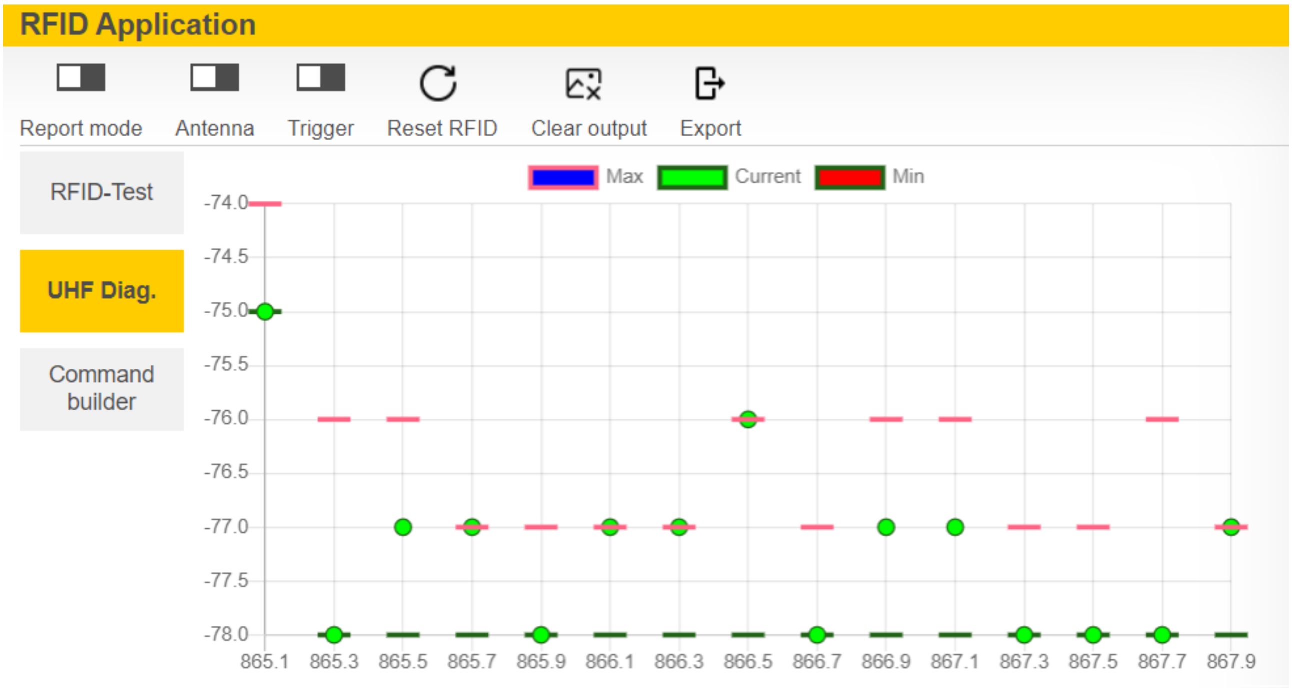


Fig. 74: Example of UHF diagnostics: received power level per channel

9 Operation

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

9.1 Executing a method and calling data

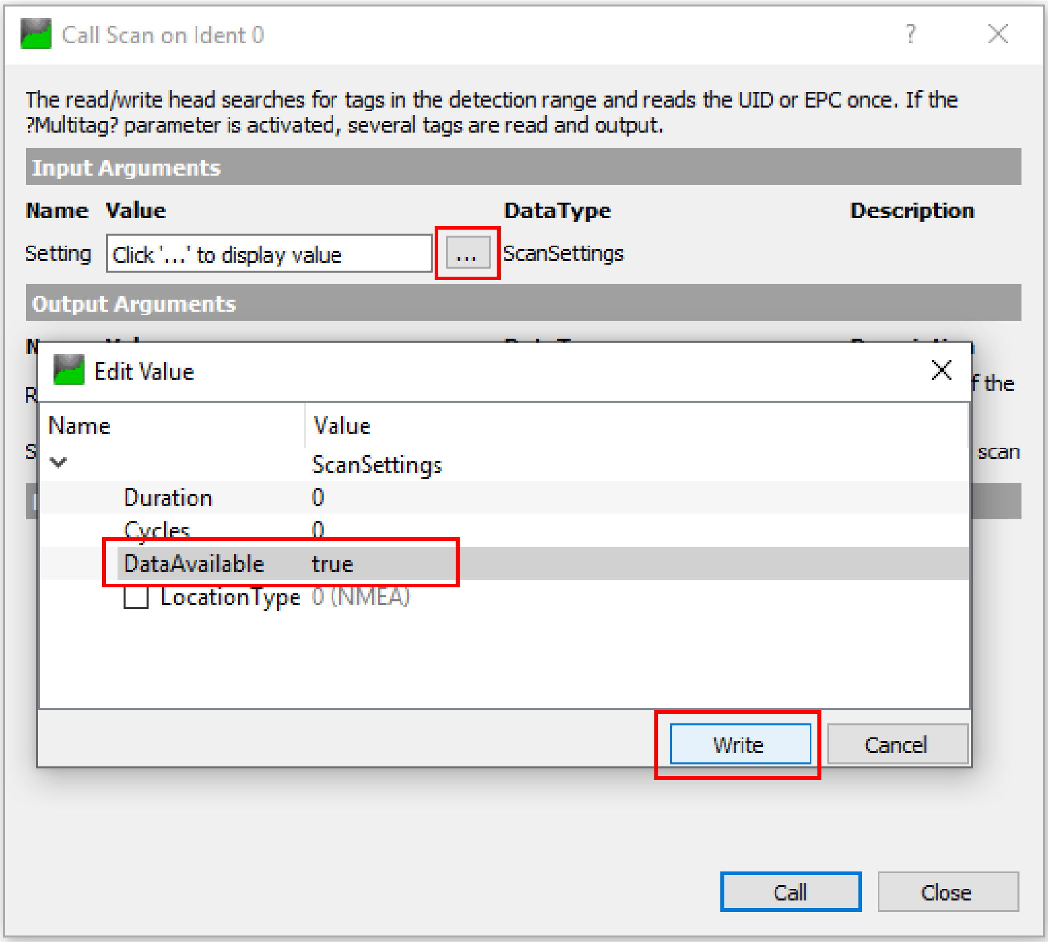
The data can either be called by the OPC UA client or forwarded as event messages to the higher-level system by the OPC UA server.

▶ 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 read/write device is operational.

▶ Execute a command via the **ScanStart** method.
➪ The read/write heads are switched 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**.



Call Scan on Ident 0

The read/write head 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.

Input Arguments

Name	Value	DataType	Description
Setting	Click '…' to display value	ScanSettings	

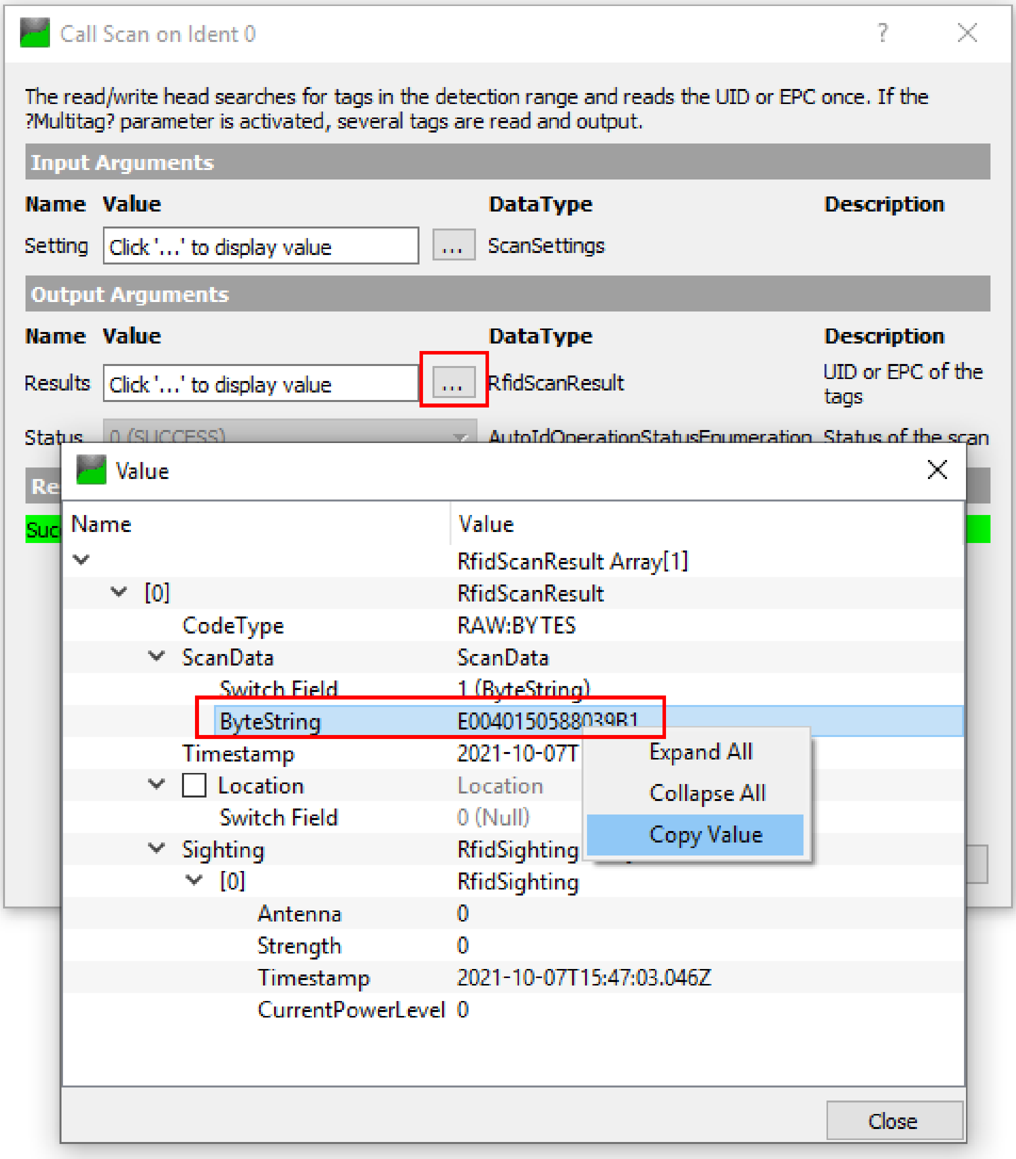
Output Arguments

Edit Value

Name	Value
⌄	ScanSettings
Duration	0
Cycles	0
DataAvailable	true
□ LocationType	0 (NMEA)

Fig. 75: 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**).



Call Scan on Ident 0

The read/write head 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.

Input Arguments

Name	Value	DataType	Description
Setting	Click '...' to display value	ScanSettings	

Output Arguments

Name	Value	DataType	Description
Results	Click '...' to display value	RfidScanResult	UID or EPC of the tags
Status	0 (SUCCESS)	AutoIdOperationStatusEnumeration	Status of the scan

Re

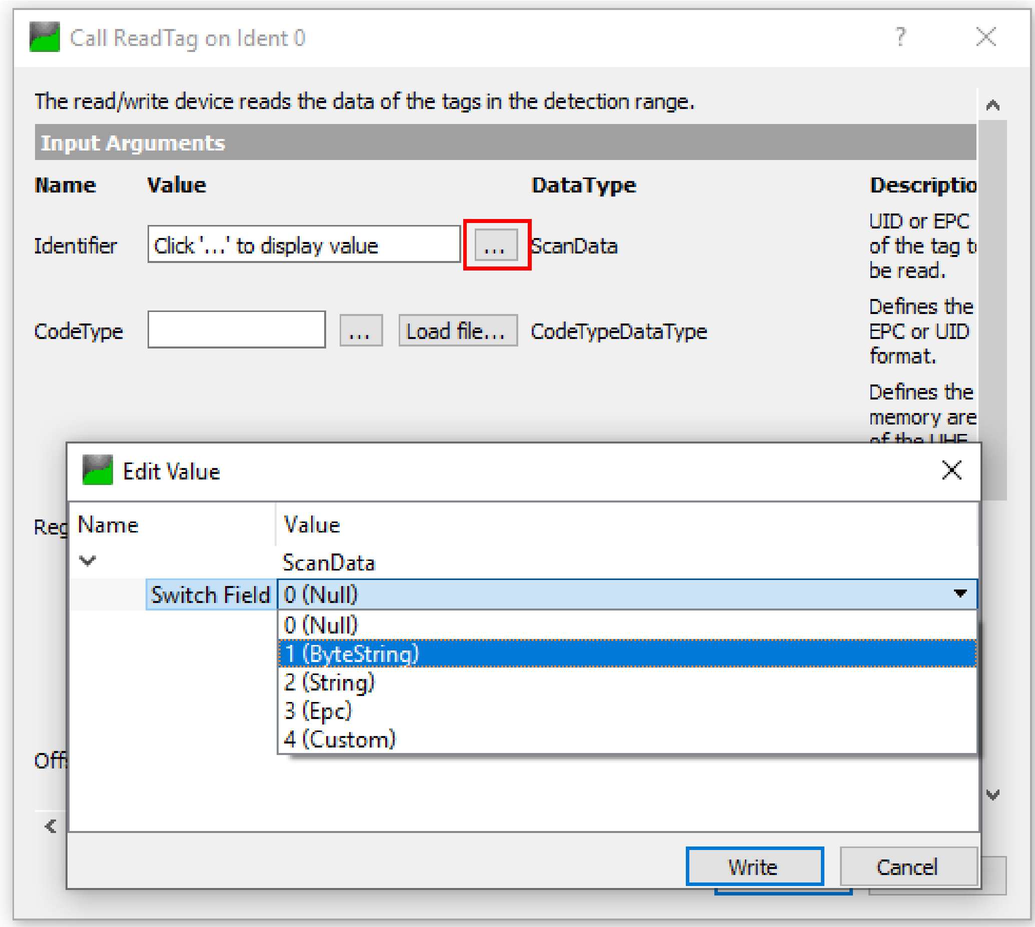
Suc

Value

Name	Value
	RfidScanResult Array[1]
[0]	RfidScanResult
CodeType	RAW:BYTES
ScanData	ScanData
Switch Field	1 (ByteString)
ByteString	E0040150588039B1
Timestamp	2021-10-07T
□ Location	Location
Switch Field	0 (Null)
Sighting	RfidSighting
[0]	RfidSighting
Antenna	0
Strength	0
Timestamp	2021-10-07T15:47:03.046Z
CurrentPowerLevel	0

Fig. 76: 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.



The read/write device reads the data of the tags in the detection range.

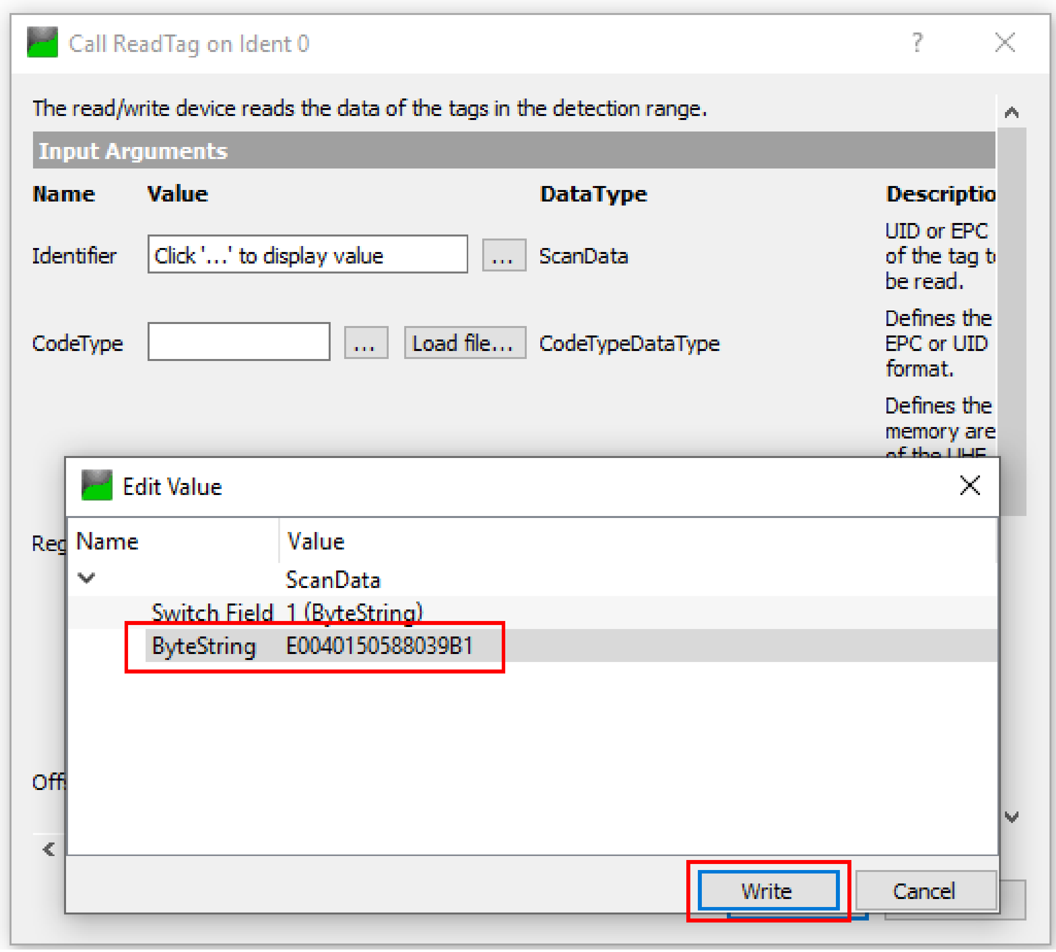
Name	Value	DataType	Descriptio
Identifier	Click '...' to display value	ScanData	UID or EPC of the tag t be read.
CodeType		CodeTypeDataType	Defines the EPC or UID format.
			Defines the memory are of the UHF

Name	Value
	ScanData
Switch Field	0 (Null)

0 (Null)
1 (ByteString)
2 (String)
3 (Epc)
4 (Custom)

Fig. 77: ReadTag method – selecting ByteString

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



Call ReadTag on Ident 0

The read/write device reads the data of the tags in the detection range.

Input Arguments

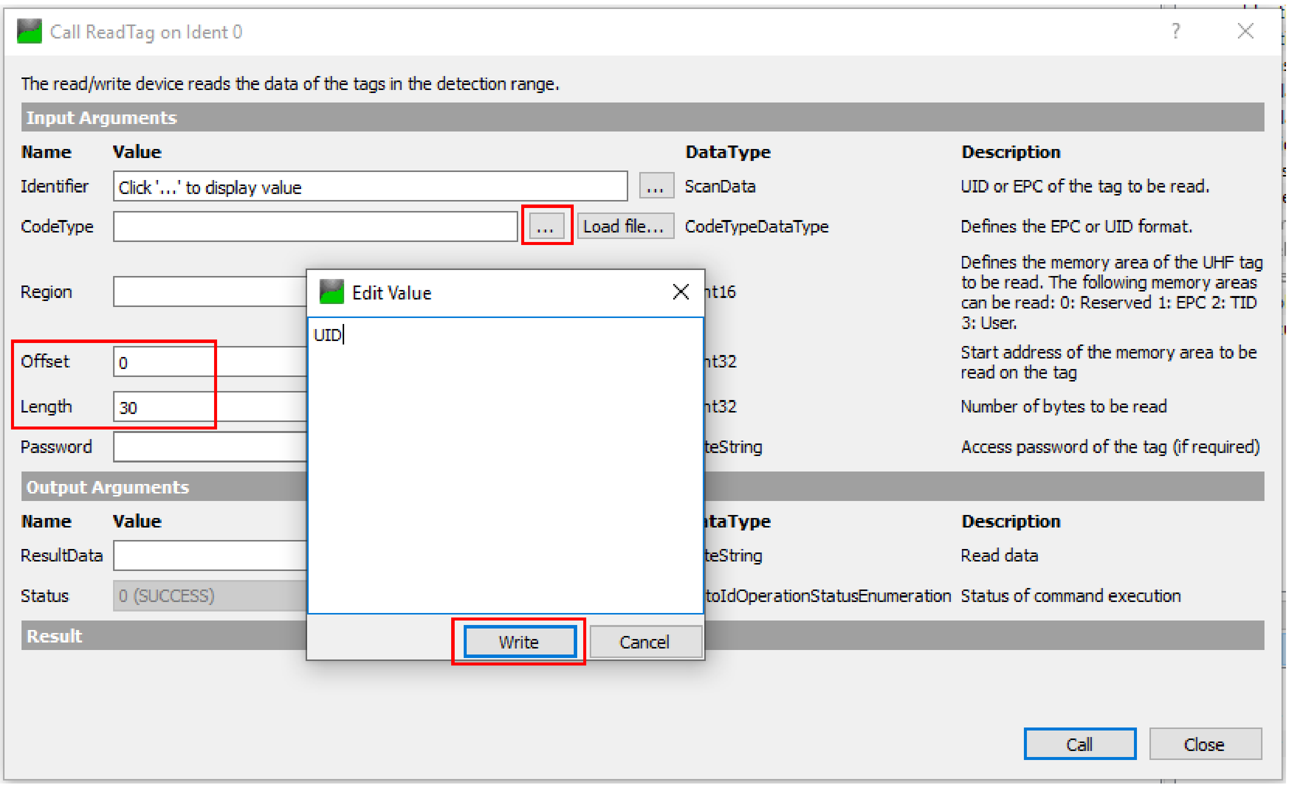
Name	Value	DataType	Descriptio
Identifier	Click '...' to display value	ScanData	UID or EPC of the tag t be read.
CodeType		CodeTypeDataType	Defines the EPC or UID format.
			Defines the memory are of the UHF

Edit Value

Name	Value
	ScanData
Switch Field	1 (ByteString)
ByteString	E0040150588039B1

Fig. 78: 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.



Call ReadTag on Ident 0

The read/write device reads the data of the tags in the detection range.

Input Arguments

Name	Value	DataType	Description
Identifier	Click '...' to display value	ScanData	UID or EPC of the tag to be read.
CodeType		CodeTypeDataType	Defines the EPC or UID format.
Region		nt16	Defines the memory area of the UHF tag to be read. The following memory areas can be read: 0: Reserved 1: EPC 2: TID 3: User.
Offset	0	nt32	Start address of the memory area to be read on the tag
Length	30	nt32	Number of bytes to be read
Password		teString	Access password of the tag (if required)

Output Arguments

Name	Value	taType	Description
ResultData		teString	Read data
Status	0 (SUCCESS)	toIdOperationStatusEnumeration	Status of command execution

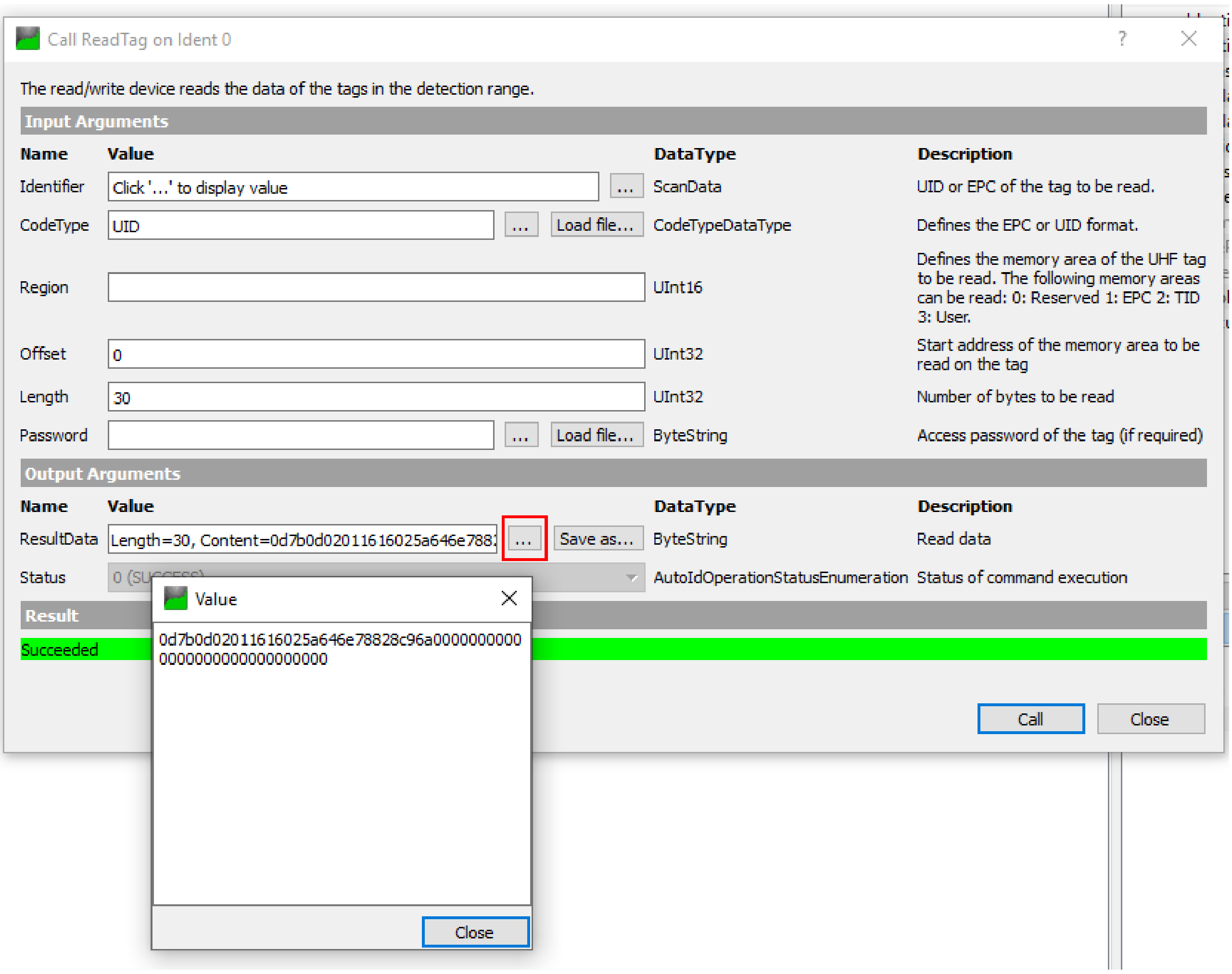
Result

Edit Value

UID

Fig. 79: ReadTag method settings

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



Call ReadTag on Ident 0

The read/write device reads the data of the tags in the detection range.

Input Arguments

Name	Value	DataType	Description
Identifier	Click '…' to display value	ScanData	UID or EPC of the tag to be read.
CodeType	UID	CodeTypeDataType	Defines the EPC or UID format.
Region		UInt16	Defines the memory area of the UHF tag to be read. The following memory areas can be read: 0: Reserved 1: EPC 2: TID 3: User.
Offset	0	UInt32	Start address of the memory area to be read on the tag
Length	30	UInt32	Number of bytes to be read
Password		ByteString	Access password of the tag (if required)

Output Arguments

Name	Value	DataType	Description
ResultData	Length=30, Content=0d7b0d02011616025a646e7882	ByteString	Read data
Status	0 (SUCCESS)	AutoIdOperationStatusEnumeration	Status of command execution

Result

Succeeded

Value

```
0d7b0d02011616025a646e78828c96a0000000000
0000000000000000000
```

Fig. 80: Information stored on the tag

9.2 HF applications – using the ScanStart method

The **ScanStart** method enables the read/write head to read up to 64 bytes (see the table User data areas of the HF tags [▸ 94].

The following parameters must be set in the web server for the **ScanStart** method:

- Tag type
- HF: Command for ScanStart method
- HF: Length for ScanStart method
- HF: Address for ScanStart method

▶ With read command: In the parameter **HF: Select tag type** specify the tag type. Automatic tag detection is not possible.

▶ In the parameter **HF: Command for ScanStart method** select the command. Inventory and read are possible.

▶ In the parameter **HF: Length for ScanStart method** enter the length of the data to be read in bytes. The length must be a multiple of the block size of the tag used according to the user data areas of the HF tags ([▸ 94]). The addressing of an odd byte number is not possible.

▶ In the parameter **HF: Address for ScanStart method** specify the start address for the command. The start address must be a multiple of the block size of the tag used according to the user data areas of the HF tags ([▸ 94]). The addressing of an odd byte number is not possible.

▶ Execute **ScanStart** via an OPC UA client.

⇨ The set command is preloaded and carried out in the connected read/write head as soon as a tag is in the field.

▶ The data received from the read/write head is polled cyclically by the RFID interface.

▶ To end **ScanStart** execute **ScanStop**.

NOTE
The tag is detected with an edge trigger. A tag is only detected when entering the RF field of read/write head. The Presence variable is not updated in this mode.

9.2.1 Executing the ScanStart method by setting the ScanActive variables

Setting the **ScanActive** variable causes **ScanStart** to be executed and the event notifications on the read data to be generated without the **ScanStart** method having to be called. If the **ScanActive** variable is restored to false, **ScanStart** is ended. The **ScanActive** variable stays set after a voltage reset and tags continue to be logged. Parameters are set in the same way as with the **ScanStart** method.

9.3 HF applications – using the ScanStart method in HF bus mode

The **ScanStart** method for continuous reading in HF bus mode enables the read/write head to read up to 64 bytes (see the table User data areas of the HF tags [▸ 94].

The following parameters must be set in the web server for the **ScanStart** method:

- Tag type
- HF: Command for ScanStart method
- HF: Length for ScanStart method
- HF: Address for ScanStart method

▶ With read command: In the parameter **HF: Select tag type** specify the tag type. Automatic tag detection is not possible.

▶ In the parameter **HF: Command for ScanStart method** select the command. Inventory and read are possible.

▶ In the parameter **HF: Length for ScanStart method** enter the length of the data to be read in bytes. The length must be a multiple of the block size of the tag used according to the user data areas of the HF tags ([▸ 94]). The addressing of an odd byte number is not possible.

▶ In the parameter **HF: Address for ScanStart method** specify the start address for the command. The start address must be a multiple of the block size of the tag used according to the user data areas of the HF tags ([▸ 94]). Refer to the table below for the block size of the tags. The addressing of an odd byte number is not possible.

▶ Execute **ScanStart** via an OPC UA client.

⇨ The set command is preloaded and carried out in the connected read/write head as soon as a tag is in the field.

▶ With the read command and when querying UIDs, the data received from the read/write head is polled cyclically by the RFID interface.

▶ To end the **ScanStart** method execute **ScanStop**.

NOTE
The tag is detected continuously and controlled by the bypass time. The same tag is read repeatedly. In this mode the **PresenceOnAntenna** variables are updated.

User data areas of HF tags

Chip type	User data area			Access	Bytes per block
	First block	Last block	Total memory in bytes		
NXP SLIX2	0x00	0x4E	320	Read/write	4
NXP Icode SLIX	0x00	0x1B	112	Read/write	4
NXP Icode SLIX-S	0x00	0x27	160	Read/write	4
NXP Icode SLIX-L	0x00	0x07	32	Read/write	4
Fujitsu MB89R118 Fujitsu MB89R118B	0x00	0xF9	2000	Read/write	8
Fujitsu MB89R112	0x00	0xFF	8192	Read/write	32
TI Tag-it HF-I Plus	0x00	0x3F	256	Read/write	4
TI Tag-it HF-I	0x00	0x07	32	Read/write	4
Infineon SRF55V02P	0x00	0x37	224	Read/write	4
Infineon SRF55V10P	0x00	0xF7	992	Read/write	4
EM4233	0x00	0x33	208	Read/write	4
EM4233 SLIC	0x00	0x1F	128	Read/write	4

9.4 Using HF bus mode

9.4.1 Executing methods in HF bus mode for OPC UA

Activate HF bus mode for read/write head:

- ▶ Call the **ActivateBusHead** method in the OPC UA client.
- ▶ At **InputArguments** set the **RFID channel** and the **read/write head address**.
- ▶ Execute the **ActivateBusHead** method with the defined arguments.
- ➪ The device is in HF bus mode.

Execute the method in HF bus mode:

- ▶ Execute the **EnableAntennas** variable.
- ▶ Call the required method and set the associated arguments.
- ▶ Execute the method.
- ➪ The set read/write head executes the method.

9.4.2 Replacing bus-capable read/write heads

- ▶ Remove the faulty read/write head.
- ▶ Connect the new read/write head with the default address 68 and 0 (factory setting …/ C53).
- ▶ If multiple read/write heads are exchanged: connect the read/write heads in the order of the connection, i.e. connect the read/write head with the lowest address first.
- ➪ The read/write heads are automatically assigned addresses in ascending order in the order of connection. The lowest address is automatically assigned to the next connected read/write head with the default address 68.
- ➪ The addressing is successfully completed if the LED of the read/write head is permanently lit.

9.4.3 ScanStart in HF bus mode – data query and speed

All activated read/write heads are triggered within a bypass time + wait time. The command is permanently stored once in the activated read/write heads. The set command (e.g. Inventory or Read) is processed in the **ScanStart** method within this time.

Only one read/write head sends data to the RFID interface during command execution of all activated read/write heads. The other read/write heads store the read data for a later query within the bus cycle of the **ScanStart** method.

When the same read/write head detects a new tag, the data in the buffer of a read/write head is overwritten if it was not yet sent to the RFID interface. The time must therefore be allowed until the data of all read/write heads has been fetched. The maximum time required for this is based on the formula **(bypass time + wait time)** × **number of activated read/write heads**.

Possibilities for optimizing the speed:

- Reduce the bypass time to suit the application
- Arrange the read/write heads over four channels or over several modules
- Reduce the data to the relevant part

NOTE
The repeated reading of the same tag is time-triggered.

The read/write heads do not detect any tags between two queries and when sending data to the RFID interface. The following table describes the required wait times:

Command	Wait time
Inventory	15 ms
Read	25 ms

The default bypass time of the **ScanStart** method in HF bus mode is 48 ms.

The following table shows when commands (CMD) are executed and data is exchanged (DATA).

- CMD: Command is executed.
- DATA: Data exchange
- DATA or CMD: If data is stored on the read/write head, the data is sent to the RFID module. If no data is stored on the read/write head, the command is executed.

Read/write head	Pass 1		Pass 2		Pass 3		Pass n	
Address 1	DATA or CMD	No action	CMD	No action	CMD	No action	CMD	No action
Address 2	CMD	No action	DATA or CMD	No action	CMD	No action	CMD	No action
Address 3	CMD	No action	CMD	No action	DATA or CMD	No action	CMD	No action
Address n	CMD	No action	CMD	No action	CMD	No action	DATA or CMD	No action
Time	Bypass time	Wait time	Bypass time	Wait time	Bypass time	Wait time	Bypass time	Wait time

9.5 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.

9.6 LEDs

The device has the following LED indicators:

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

OPC LED	**Meaning**
Off	No OPC UA client connected
Green	OPC UA client connected
White flashing	Wink command active

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

BUS LED	**Meaning**
Off	No voltage present
Green	Connection to a master active
Green flashing (1 Hz)	Device is operational (slave)
Red	IP address conflict, Restore mode active or F_Reset active
Red flashing	Wink command active
Red/green flashing (1 Hz)	Autonegotiation and/or wait for IP address allocation in DHCP or BootIP mode

ERR LED	**Meaning**
Off	No voltage connected
Green	No diagnostics
Red	Diagnostic message pending

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

LEDs ETH1 and ETH2	**Meaning**
Off	No Ethernet connection
Green	Ethernet connection established, 100 Mbps
Green flashing	Ethernet traffic, 100 Mbps
Yellow	Ethernet connection established, 10 Mbps
Yellow flashing	Ethernet traffic, 10 Mbps

TP0…TP3 LEDs	Meaning
Off	No tag within the detection range
Green	Tag present at read/write head
Green flashing	Tag present at read/write head, command is processed
Red/green flashing (1 Hz)	Connection with DTM. No connection to controller active.
Red	Diagnostics present

CMD0…CMD3 LEDs	Meaning
Off	Read/write head off
Green	Read/write head on
Green flashing	BUSY (command active)
Red flashing	Interface memory full
Red	Error in the data interface

RFID channel LEDs	Meaning
TP… and CMD… flash simultaneously	Overload of the auxiliary voltage
TP… and CMD… flash alternately	Parameter error

DXP channel LEDs	Meaning (input)	Meaning (output)
Off	No input signal	Output not active
Green	Input signal present	Output active (max. 2 A)
Red	–	Actuator overload
Red flashing (1 Hz)	Overload of sensor supply	

9.7 Reading status and diagnostic messages

9.7.1 Read out OPC UA diagnostic messages

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

NOTE
Other specific error messages of the read/write devices are output in the web server.

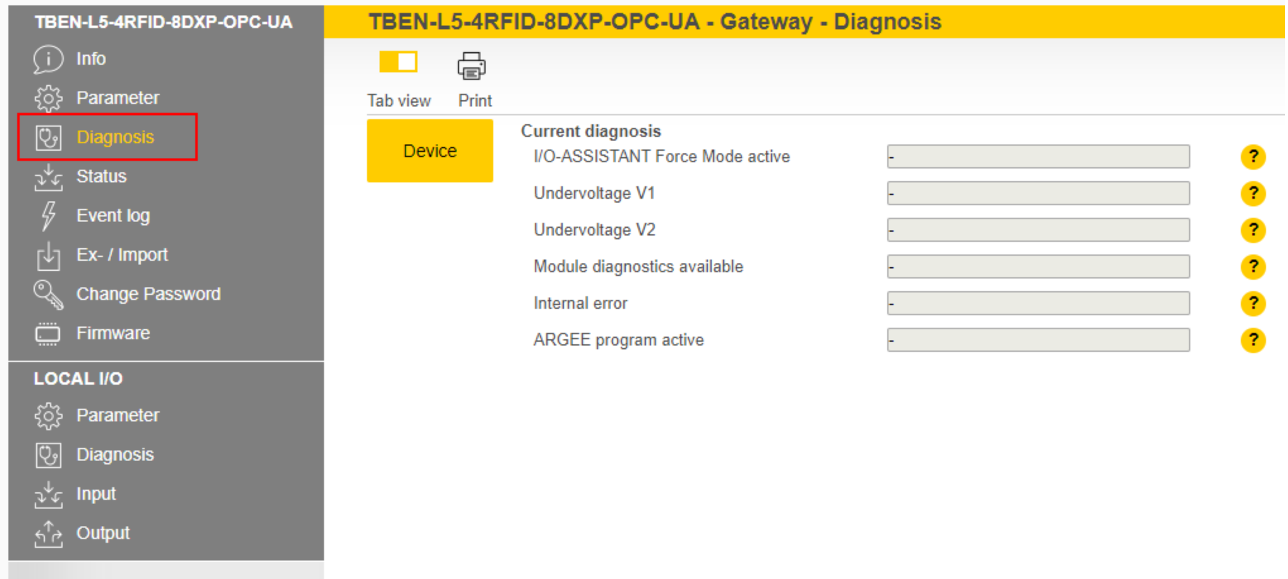
Message	Description	Possible causes
SUCCESS	No error, command successfully executed	–
MISC_ERROR_TOTAL	Command not fully executed	▪ Unknown error
PERMISSON_ERROR	Password required	▪ UHF reader: A valid password is expected before the command is accepted.
PASSWORD_ERROR	Password incorrect	
REGION_NOT_FOUND_ERROR	Addressed memory area not available for current tag	▪ Memory area of the tag outside of the permissible range
OP_NOT_POSSIBLE_ERROR	Command not available for current tag	▪ ISO 15693 error: command not supported ▪ ISO 15693 error: command not detected, e.g. incorrect input format ▪ ISO 15693 error: command option not supported ▪ ISO 15693 error: undefined error ▪ ISO 15693 error: addressed memory area not available ▪ ISO 15693 error: addressed memory area locked ▪ ISO 15693 error: addressed memory area locked and not writable ▪ ISO 15693 error: write operation not successful ▪ ISO 15693 error: addressed memory area could not be locked.
OUT_OF_RANGE_ERROR	Specified memory area not available for current tag	▪ Block size of the tag not supported ▪ **Tag type** parameter outside of the permissible range ▪ Address outside of the permissible range ▪ Length and address outside of the permissible range ▪ Length of the UID outside of the permissible range ▪ Length outside of the tag specification ▪ Address outside of the tag specification ▪ Length and address outside of the tag specification

Message	Description	Possible causes
NO_IDENTIFIER	Command not fully executed – no tag in the detection range	■ No tag found ■ Timeout ■ Air interface error: timeout ■ Air interface error: UHF tag outside of the detection range, before all commands could be executed ■ UHF reader: no tag in the field ■ 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 ■ UHF reader: read operation not possible (e.g. invalid tag) ■ Read/write device error when executing an Inventory command
WRITE_ERROR	Tag could not be written.	■ UHF reader: write operation not possible (e.g. tag can only be read) ■ Error when writing to a tag
NOT_SUPPORTED_BY DEVICE	Command or parameter are not supported by the device.	■ Command not supported ■ Command not supported in HF applications ■ Command not supported in UHF applications ■ Command for applications with automatic tag detection not supported ■ Command only supported for applications with automatic tag detection ■ UHF reader: command not supported ■ Password function not supported by read/write device ■ Command not supported by read/write device version
NOT_SUPPORTED_BY_TAG	Command or parameter are not supported by the tag.	■ Password function not supported by tag ■ Command for multitag application with automatic tag detection not supported ■ Command not supported for multitag application
DEVICE_NOT_READY	Device is not operational	■ Read/write device detuned
INVALID_CONFIGURATION	Device configuration invalid	■ Parameter undefined ■ **Bypass time** parameter outside of the permissible range ■ Value for timeout outside of the permissible range ■ Error with the parameter setting of the HF read/write head ■ Error with the extended parameter setting of the HF read/write head ■ Error in parameterization of UHF reader

Message	Description	Possible causes
RF_COMMUNICATION_ERROR	Error during communication between the read/write device and tag	■ Air interface error ■ Error when switching on the HF read/write head ■ Air interface error: CRC error ■ Air interface error: timeout ■ Air interface error: UHF tag error ■ HF tag does not match the tag type set in the parameters
DEVICE_FAULT	Hardware error in the connected device	■ Read/write device not connected ■ HF read/write head faulty

9.7.2 Calling channel and module diagnostic messages in the web server

Diagnostic messages – module status



TBEN-L5-4RFID-8DXP-OPC-UA - Gateway - Diagnosis

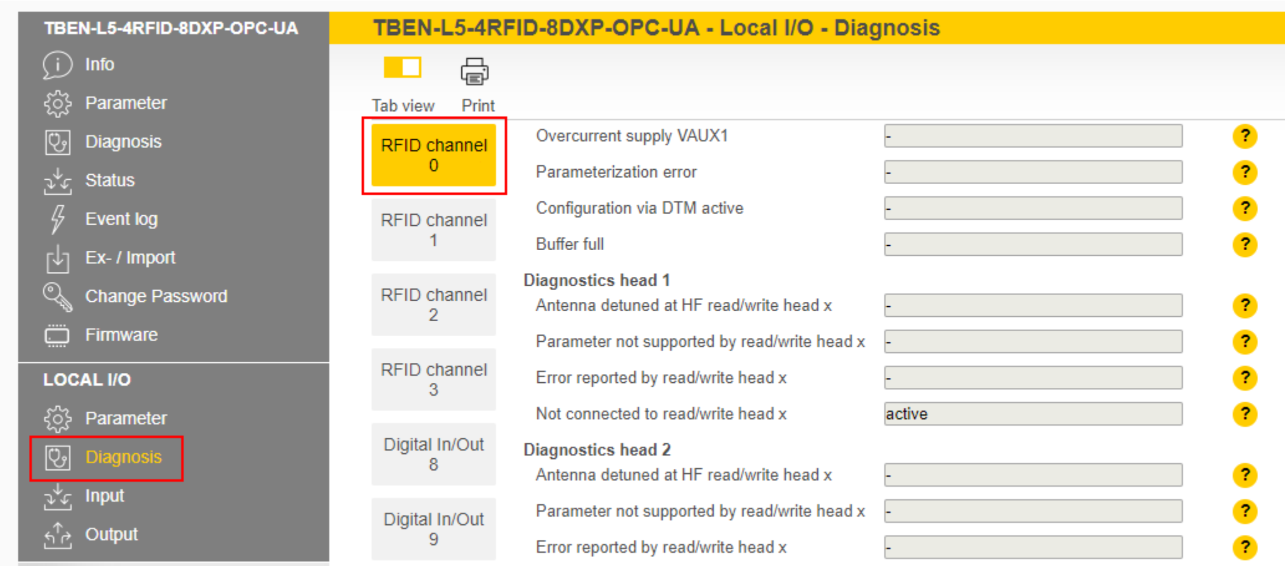
Current diagnosis

I/O-ASSISTANT Force Mode active	-
Undervoltage V1	-
Undervoltage V2	-
Module diagnostics available	-
Internal error	-
ARGEE program active	-

Fig. 81: Web server – module status diagnostics

Status message	Description
I/O-ASSISTANT Force Mode active	DTM active in Force mode
Undervoltage V2	Undervoltage V2
Undervoltage V1	Undervoltage V1
Module diagnostics available	Module diagnostics available
Internal error	Internal error

Diagnostic messages – RFID channels



TBEN-L5-4RFID-8DXP-OPC-UA - Local I/O - Diagnosis

Overcurrent supply VAUX1	-
Parameterization error	-
Configuration via DTM active	-
Buffer full	-
Diagnostics head 1	
Antenna detuned at HF read/write head x	-
Parameter not supported by read/write head x	-
Error reported by read/write head x	-
Not connected to read/write head x	active
Diagnostics head 2	
Antenna detuned at HF read/write head x	-
Parameter not supported by read/write head x	-
Error reported by read/write head x	-

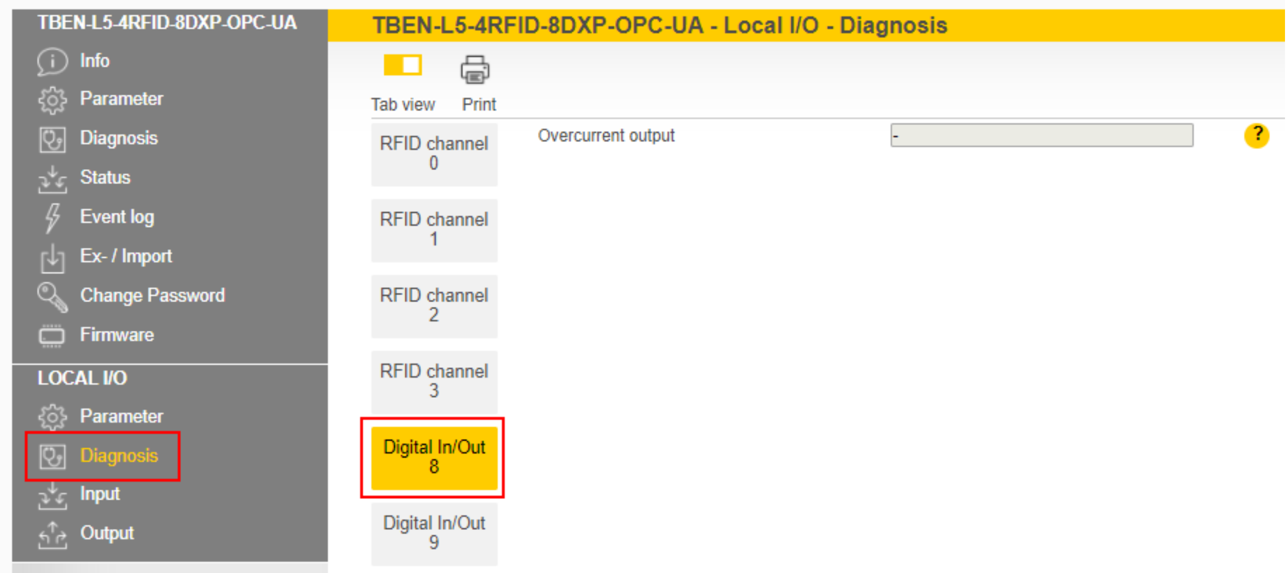
Fig. 82: Web server – RFID channel diagnostics

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

HF bus mode-specific error messages of the read/write heads:

Diagnostics	Description
Antenna detuned at HF read/write head x	HF read/write head … detuned
Parameter not supported by read/write head x	Parameter not supported by read/write head
Error reported by read/write head x	Read/write head ... reports error
Not connected to read/write head x	Expected read/write head ... not connected

Diagnostic messages – DXP channels

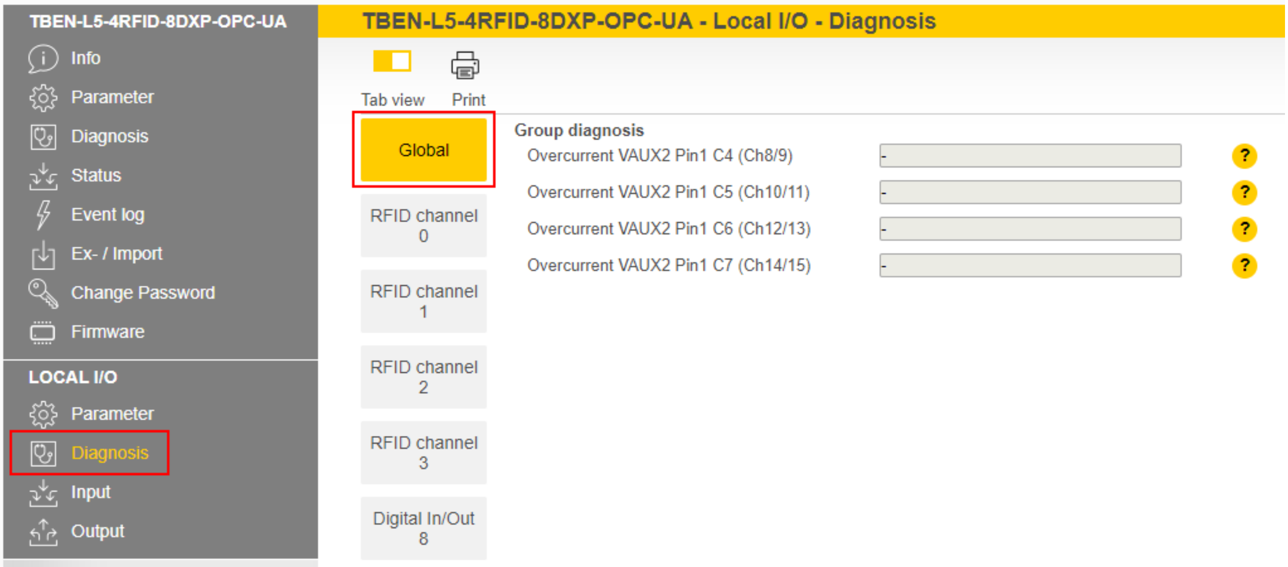


Overcurrent output -

Fig. 83: Web server – DXP channel diagnostics

Diagnostics	Description
Overcurrent output	Overcurrent at output

Diagnostic messages – additional power supply of digital channels



Group diagnosis
Overcurrent VAUX2 Pin1 C4 (Ch8/9) -
Overcurrent VAUX2 Pin1 C5 (Ch10/11) -
Overcurrent VAUX2 Pin1 C6 (Ch12/13) -
Overcurrent VAUX2 Pin1 C7 (Ch14/15) -

Fig. 84: Web server – diagnostics additional power supply of digital channels

Diagnostics	Description
Overcurrent VAUX2 Pin1 C… (Ch…/…)	Overcurrent VAUX2 at pin 1 of the socket C… (K…/…)

9.8 Reset device (Reset)

The device can be reset using different tools (rotary coding switch, Turck Service Tool, web server).

The device can be reset to the factory settings with the rotary coding switches via the F_Reset function as follows:

- Rotary switches at 90: a normal voltage reset (alternatively via the Turck Service Tool or the web server) fully resets the device including the OPC UA configurations (parameters, certificates, passwords etc.). The OPC UA server does not start up when a restart is performed with this switch position. The Run and OPC LEDs flash green simultaneously. After a factory reset a reboot is necessary with a switch position permissible for operation.
- Rotary switches not at 90: F_Reset via web server or Turck Service Tool resets everything except the OPC UA configurations (parameters, certificates, passwords etc.).

A reboot via the Turck Service Tool and the web server is possible. The device cannot be reset via the reboot in the event of an error.

10 Troubleshooting

If the device does not work as expected, proceed as follows:

- ▶ Exclude environmental disturbances.
- ▶ Check the connections of the device for errors.
- ▶ Check device for parameterization errors.

If the malfunction persists, the device is faulty. In this case, decommission the device and replace it with a new device of the same type.

10.1 Eliminating parameterization errors

DXP channels

Error	Possible causes:	Remedy
DXP output does not switch	The output is deactivated per default.	▶ Enable the output function via parameter **Activate output** (DXP_EN_DO =1).

11 Maintenance

11.1 Executing the firmware update via FDT/DTM

The firmware of the device can be updated using the FDT/DTM. The PACTware FDT frame application, the DTM for the device and the latest firmware can be downloaded free of charge from **www.turck.com**.

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.

Example: Updating the firmware with the PACTware FDT frame application

- ▶ Launch PACTware.
- ▶ Right-click **HOST PC** → **Add device**.

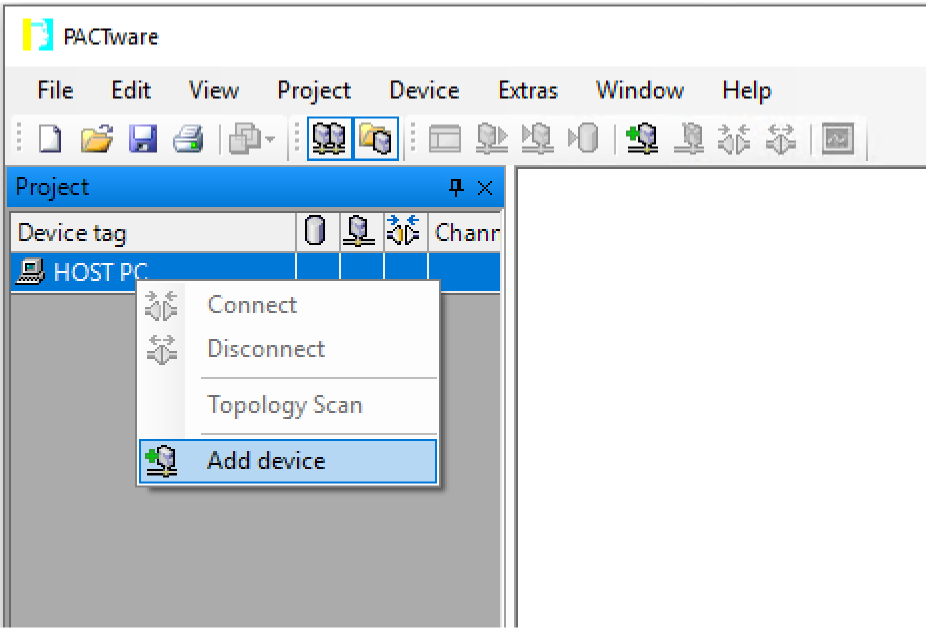
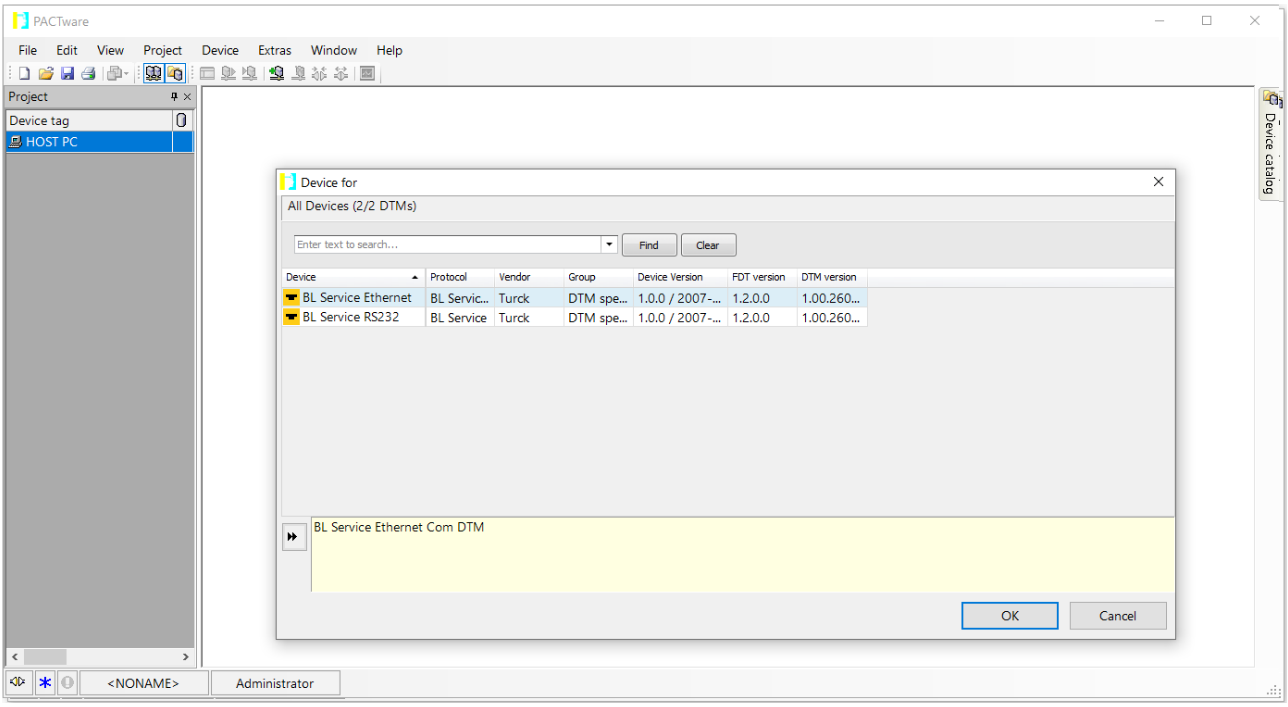


Fig. 85: Adding a device in PACTware

- Select **BL Service Ethernet** and confirm with **OK**.



All Devices (2/2 DTMs)

Enter text to search...

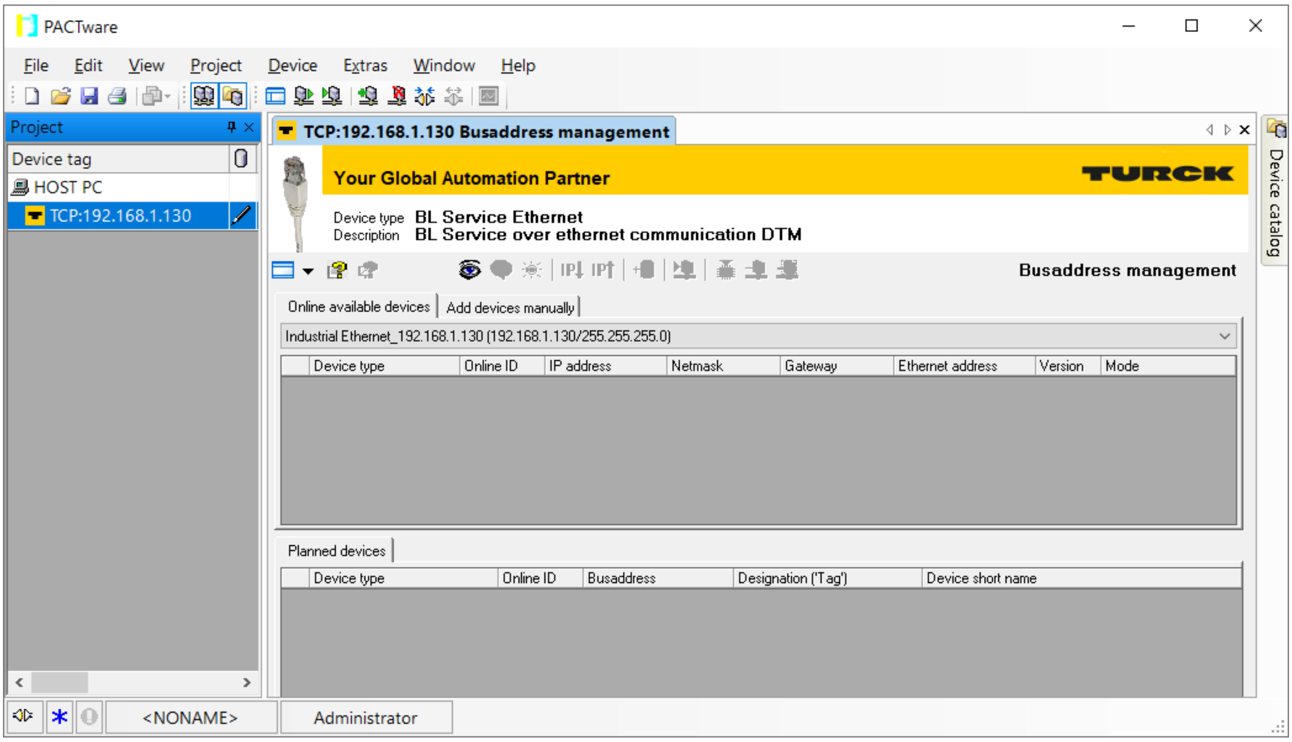
Device	Protocol	Vendor	Group	Device Version	FDT version	DTM version
BL Service Ethernet	BL Servic...	Turck	DTM spe...	1.0.0 / 2007-...	1.2.0.0	1.00.260...
BL Service RS232	BL Service	Turck	DTM spe...	1.0.0 / 2007-...	1.2.0.0	1.00.260...

BL Service Ethernet Com DTM

Fig. 86: Select the Ethernet interface

- Double-click the connected device.

➪ PACTware opens the Bus Address Management function.



Device type BL Service Ethernet
Description BL Service over ethernet communication DTM

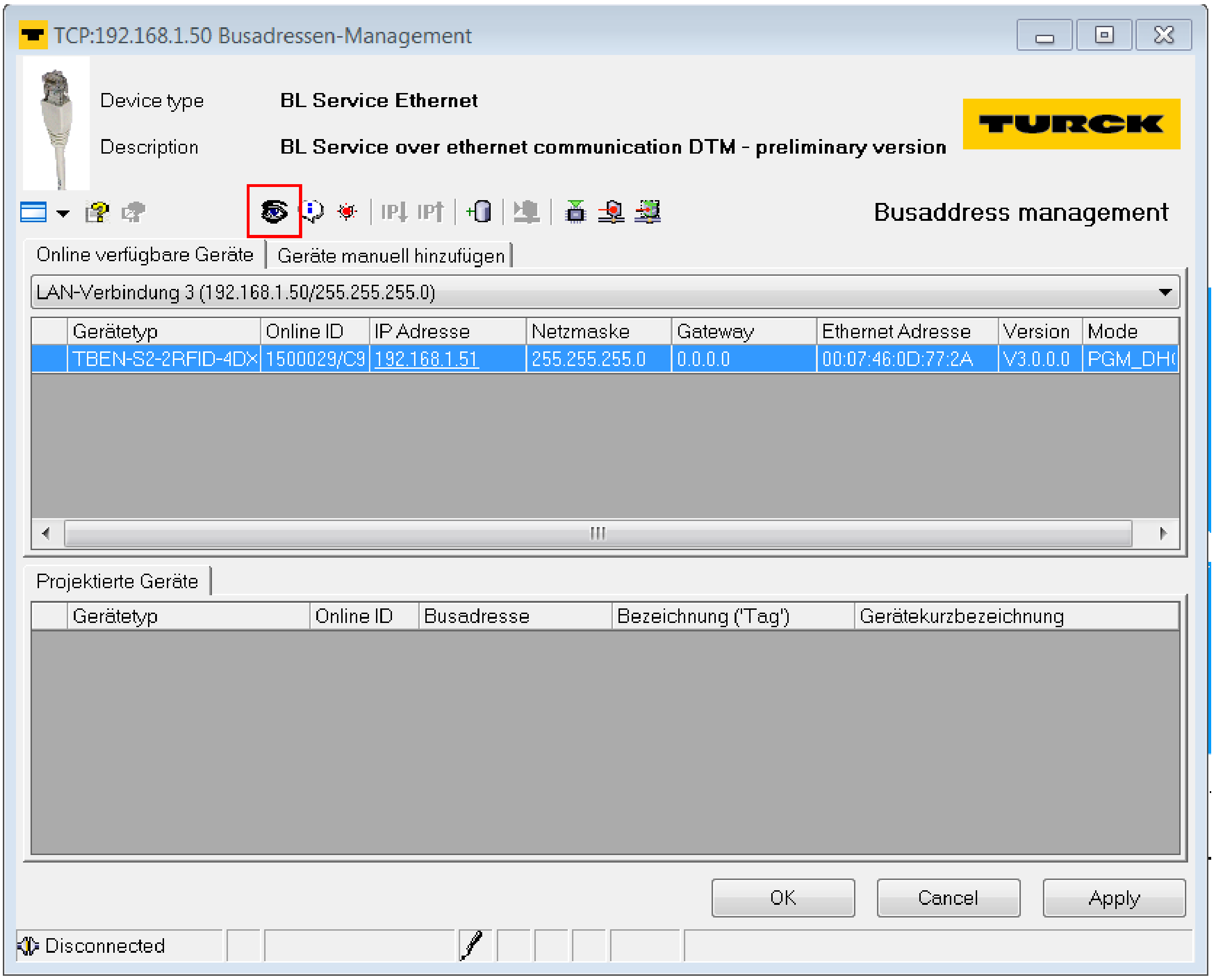
Industrial Ethernet_192.168.1.130 (192.168.1.130/255.255.255.0)

Device type	Online ID	IP address	Netmask	Gateway	Ethernet address	Version	Mode

Device type	Online ID	Busaddress	Designation ('Tag')	Device short name

Fig. 87: Opening Bus Address Management

- ▶ Searching for connected Ethernet devices: Click the **Search** icon.
- ▶ Select the required device.



Device type BL Service Ethernet

Description BL Service over ethernet communication DTM - preliminary version

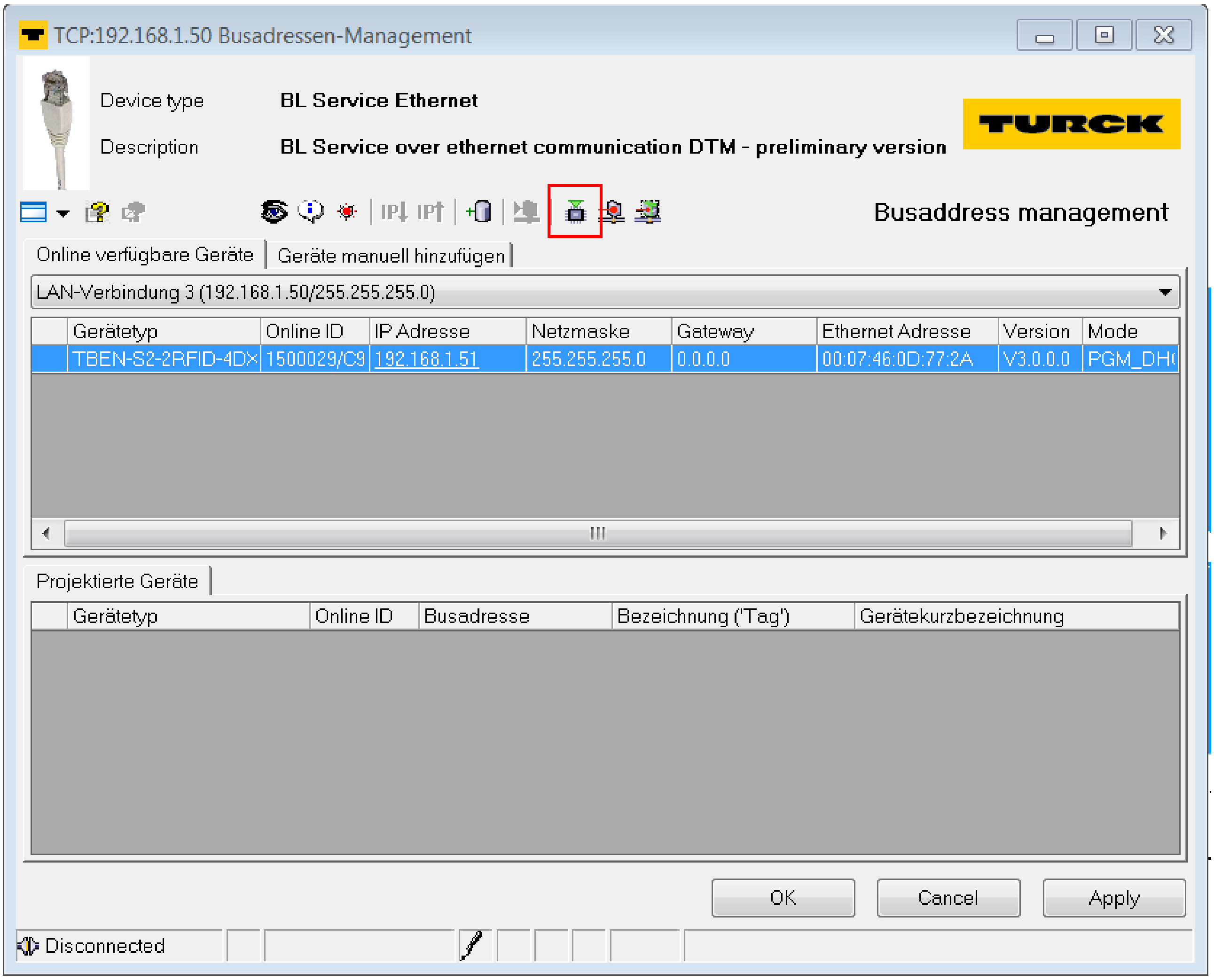
LAN-Verbindung 3 (192.168.1.50/255.255.255.0)

Gerätetyp	Online ID	IP Adresse	Netzmaske	Gateway	Ethernet Adresse	Version	Mode
TBEN-S2-2RFID-4DX	1500029/C9	192.168.1.51	255.255.255.0	0.0.0.0	00:07:46:0D:77:2A	V3.0.0.0	PGM_DH(

Gerätetyp	Online ID	Busadresse	Bezeichnung ('Tag')	Gerätekurzbezeichnung

Fig. 88: Selecting the device

- Click **Firmware Download** to start the firmware update.



TCP:192.168.1.50 Busadressen-Management

Device type: BL Service Ethernet

Description: BL Service over ethernet communication DTM - preliminary version

Busaddress management

LAN-Verbindung 3 (192.168.1.50/255.255.255.0)

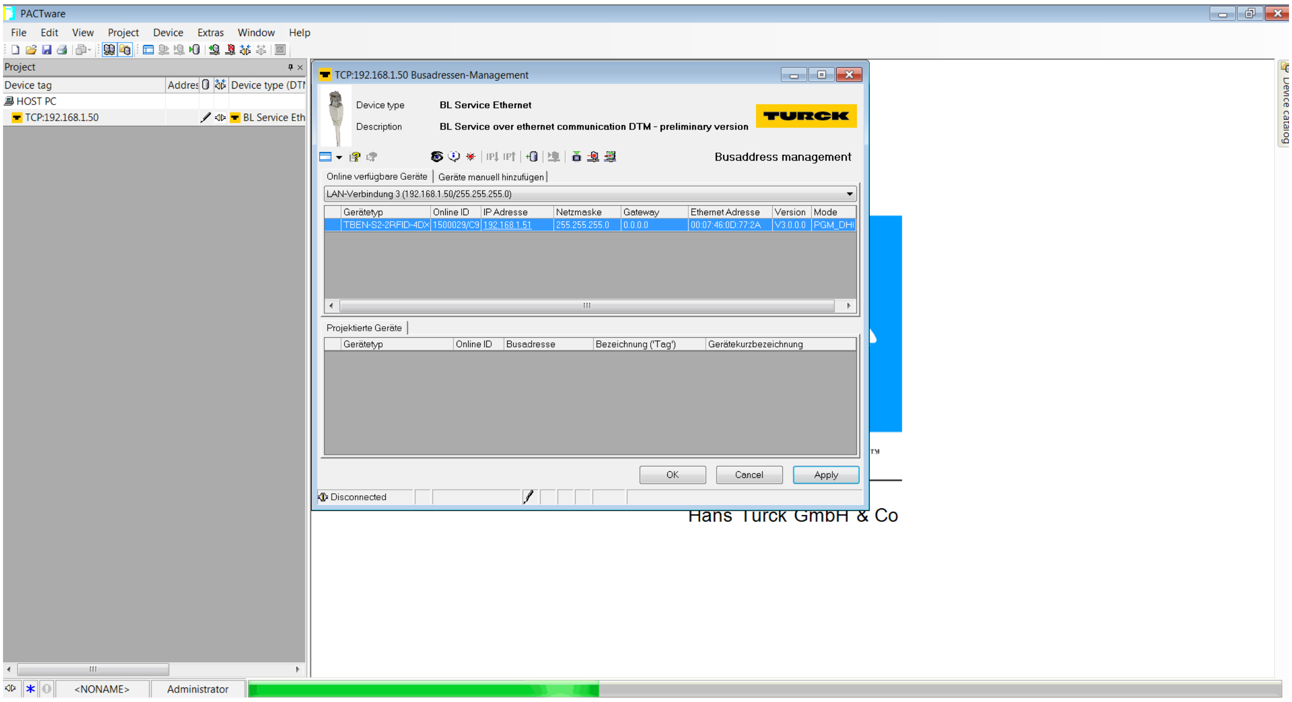
Gerätetyp	Online ID	IP Adresse	Netzmaske	Gateway	Ethernet Adresse	Version	Mode
TBEN-S2-2RFID-4DX	1500029/C9	192.168.1.51	255.255.255.0	0.0.0.0	00:07:46:0D:77:2A	V3.0.0.0	PGM_DH(

Gerätetyp	Online ID	Busadresse	Bezeichnung ('Tag')	Gerätekurzbezeichnung

Fig. 89: Starting the firmware update

- Select BL Service Ethernet and confirm with **OK**.

➪ PACTware displays a green bar at the bottom of the screen to indicate the progress of the bootloader update.



TCP:192.168.1.50 Busadressen-Management

Device type BL Service Ethernet

Description BL Service over ethernet communication DTM - preliminary version

Busaddress management

LAN-Verbindung 3 (192.168.1.50/255.255.255.0)

Gerätetyp	Online ID	IP Adresse	Netzmaske	Gateway	Ethernet Adresse	Version	Mode
TBEN-S2-2RFID-4DX	1500029/C9	192.168.1.51	255.255.255.0	0.0.0.0	00:07:46:0D:77:2A	V3.0.0.0	PGM_DH(

Projektierte Geräte

Gerätetyp	Online ID	Busadresse	Bezeichnung ('Tag')	Gerätekurzbezeichnung

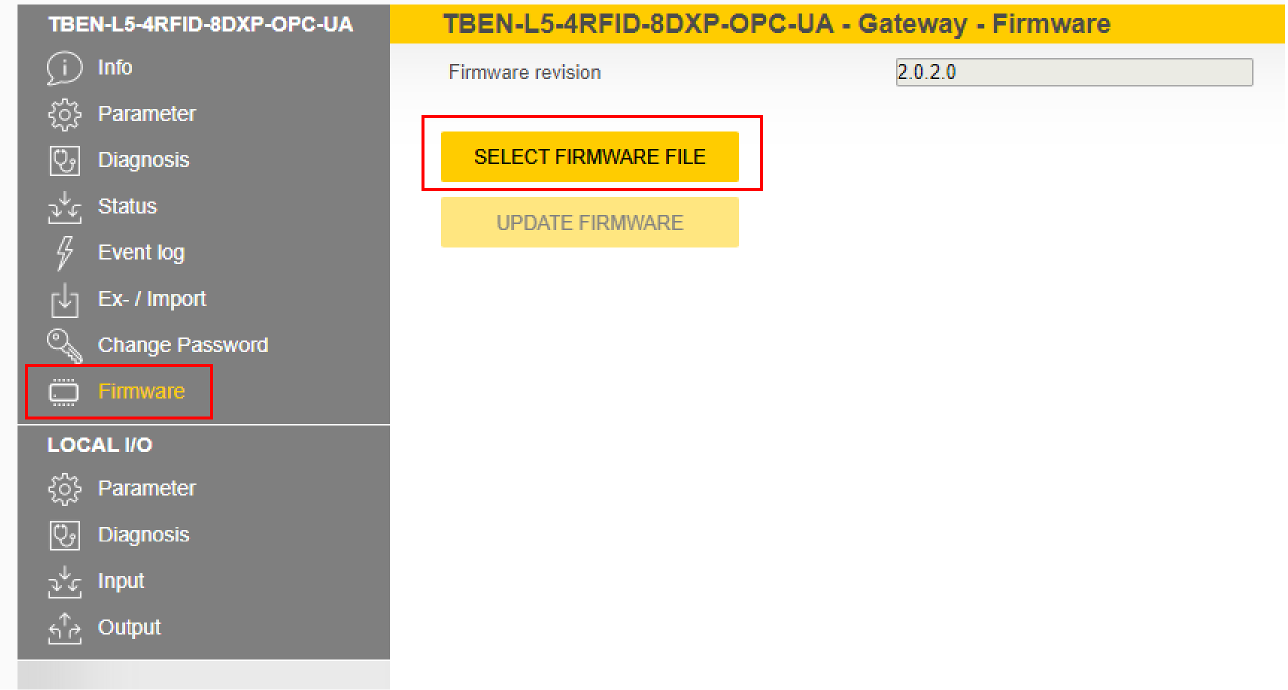
Fig. 90: Firmware update in progress

▶ When updating from Version 1.1.0.0 to a newer version after the firmware update, carry out a factory reset via the rotary switches ([▹ 104]).

➪ The firmware update has been successfully carried out.

11.2 Carry out a firmware update via the web server (from firmware version 2.0.11.0)

- Open the web server and log in on the device.
- Click **Firmware** → **SELECT FIRMWARE FILE**.

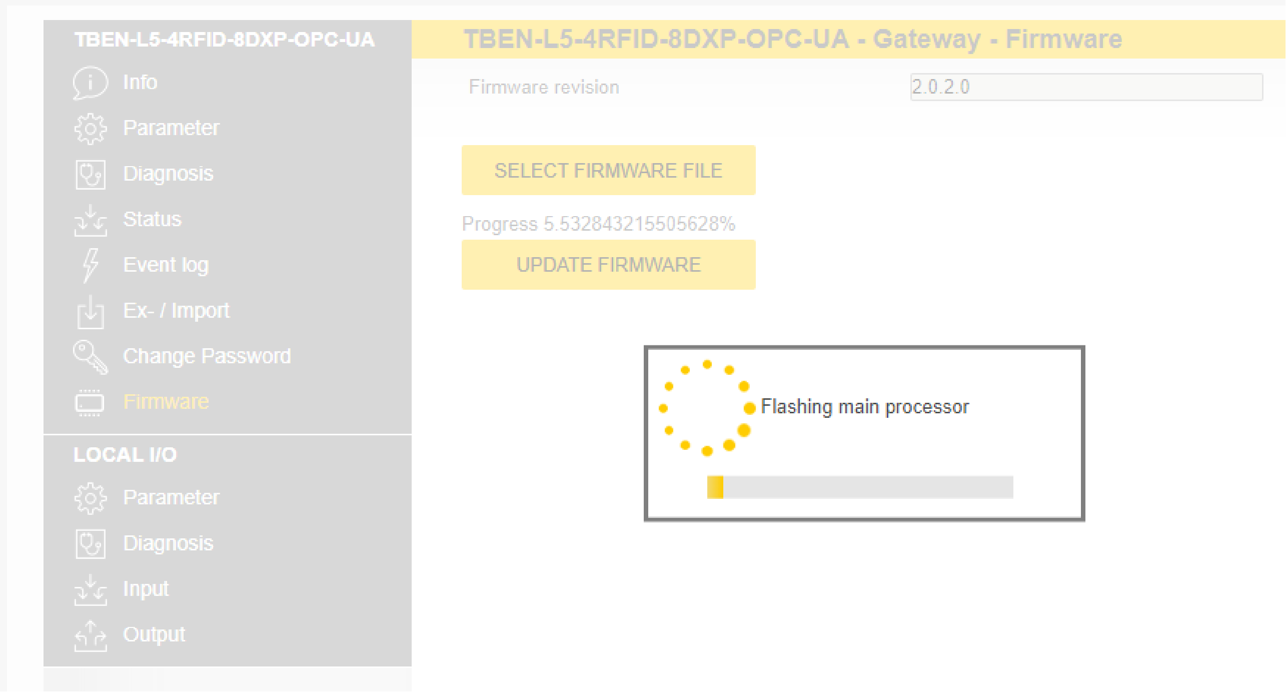


Firmware revision 2.0.2.0

Fig. 91: Selecting the new firmware file

- Select the storage location of the file and select the file.
- Start the firmware update via the **UPDATE FIRMWARE** button.

➪ The progress of the firmware update is displayed.



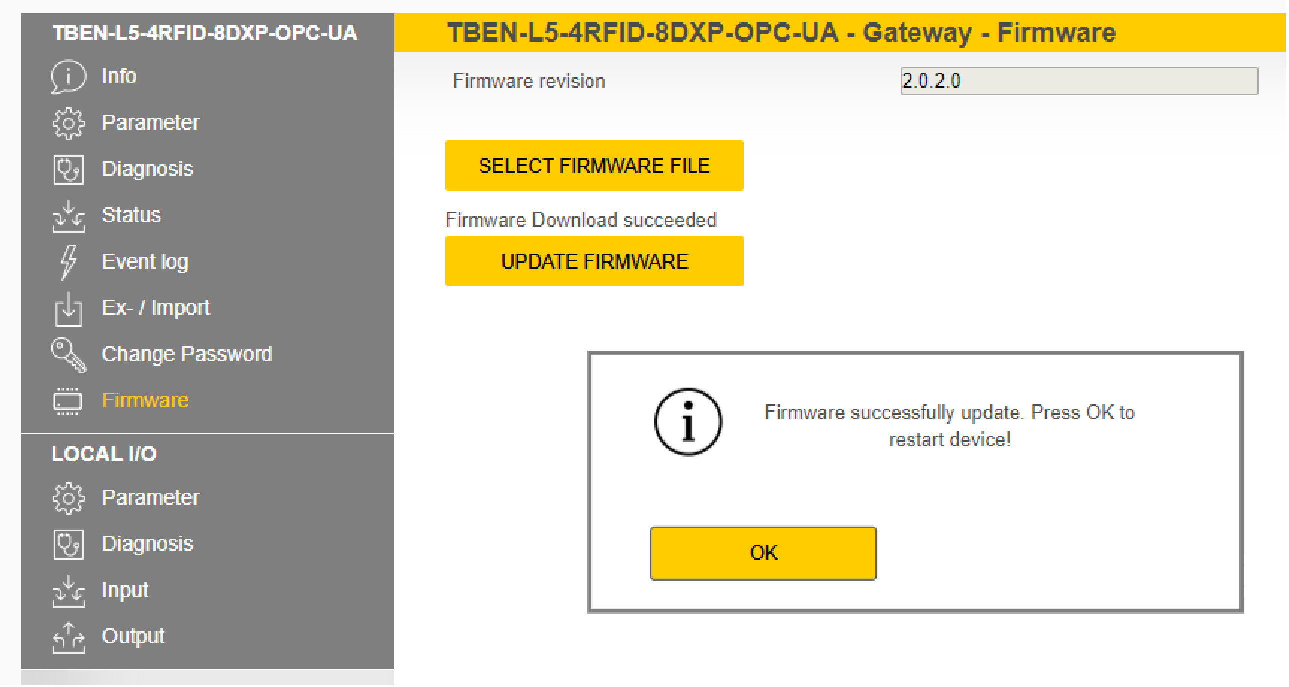
Firmware revision 2.0.2.0

Progress 5.532843215505628%

Flashing main processor

Fig. 92: Firmware update

- After a firmware update has been successfully completed, start the device by clicking **OK**.



Firmware revision: 2.0.2.0

Firmware Download succeeded

Firmware successfully update. Press OK to restart device!

Fig. 93: Firmware update successful

12 Repair

The device must not be repaired 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

Returns to Turck can only be accepted if the device has been equipped with a Decontamination declaration enclosed. The decontamination declaration can be downloaded from
https://www.turck.de/en/retoure-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 correctly and must not be included in general household garbage.

14 Technical data

Technical Data	
Type code	TBEN-L5-4RFID-8DXP-OPC-UA
ID	6814126
Power supply	
Power supply	24 VDC
Permissible range	18…30 VDC Total current V1 max. 8 A: (UL: 7 A), V2 max. 9 A at 70 °C (UL: 55 °C) per module
Voltage supply connection	5-pin male 7/8" connector X1
RFID power supply	Sockets C0..C3 from V1 Short-circuit-proof, 2 A per channel at 70 °C (UL: 1.74 A per channel at 55 °C)
Sensor/actuator supply	Sockets C4...C7 from V2 Power supply pin 1 switchable per socket Short-circuit-proof, 2 A per channel at 70 °C (UL: 55 °C)
Potential isolation	Potential isolation of V1 and V2 voltage group Voltage proof up to 500 VDC
Heat dissipation, typical	≤ 6.5 W
System description	
Processor	ARM Cortex A8, 32-bit, 800 MHz
ROM memory	256 MB Flash
RAM memory	512 MB DDR3
Real-time clock	Yes
System data	
Ethernet transfer rate	10 Mbit/s / 100 Mbit/s
Ethernet connection technology	2 × M12, 4-pin, D-coded
Web server	Default: 192.168.1.100
RFID	
No. of channels	4
Connection technology	M12
Power supply	2 A per channel at 70° C (UL: 1.74 A per channel at 55 °C), short-circuit-proof
Operation per channel	1x HF read/write or UHF reader
Mixed operation of	HF read/write heads and UHF readers
Cable length	Max. 50 m
Digital inputs	
No. of channels	8
Connection technology	M12, 5-pin
Input type	PNP
Type of input diagnostics	Channel diagnostics
Switch threshold	EN 61131-2 type 3, PNP
Signal voltage Low signal	< 5 V
Signal voltage High signal	> 11 V

Technical Data	
Signal current Low signal	<1.5 mA
Signal current High signal	> 2 mA
Potential isolation	Galvanic isolation at P1/P2 Voltage proof up to 500 VDC
Digital outputs	
No. of channels	8
Connection technology of outputs	M12, 5-pin
Output type	PNP
Type of output diagnostics	Channel diagnostics
Output voltage	24 VDC from potential group
Output current per channel	2.0 A, short-circuit proof, max. 4.0 A per socket
Utilization factor	0.56
Load type	EN 60947-5-1: DC-13
Short-circuit protection	Yes
Potential isolation	Galvanic isolation at P1/P2 Voltage proof up to 500 VDC
Conformity with standard/directive	
Vibration test	Acc. to EN 60068-2-6 Acceleration up to 20 g
Shock testing	Acc. to EN 60068-2-27
Drop and topple	Acc. to IEC 60068-2-31/IEC 60068-2-32
EMC (electromagnetic compatibility)	Acc. to EN 61131-2
Approvals and certificates	CE UKCA FCC FM Class I, Zone 2; Class I, Division 2 UV resistant acc. to DIN EN ISO 4892-2A (2013)
UL certificate	cULus LISTED 21 W2, Encl.type 1 IND.CONT.EQ.
UL cond.	
Pollution degree	2
Load type	Resistive load, inductive load
Intended use	Indoor use
General information	
Dimensions (W × L × H)	60.4 × 230.4 × 39 mm
Operating temperature	-40…+70 °C (UL: 55 °C)
Storage temperature	-40…+85 °C
Operating height	Max. 5000 m
Type of protection	IP65/IP67/IP69K
MTTF	75 years acc. to SN 29500 (Ed. 99) 20 °C
Housing material	PA6-GF30
Housing color	Black
Material of window	Lexan
Material of screw	303 stainless steel
Material of label	Polycarbonate

Technical Data	
Halogen-free	Yes
Installing	2 fixing holes, Ø 6.3 mm

15 Appendix: approvals and markings

Approvals	**Marking according to ATEX directive UKSI (SI 2016/1107)**	**EN 60079-0/-7/-31**
ATEX approval no.: TÜV 20 ATEX 264795 X UKEX approval no.: TURCK Ex-20002HX	⟨Ex⟩II 3 G ⟨Ex⟩II 3 D	Ex ec IIC T4 Gc Ex tc IIIC T115 °C Dc
IECEx approval no.: IECEx TUN 20.0010X		Ex ec IIC T4 Gc Ex tc IIIC T115 °C Dc

Ambient temperature $T_{amb.}$: -25 °C…+60 °C

Type code	**TBEN-L…-4RFID-8DXP-…**
Power supply	24 VDC ±10 %
Input current I_{max}	9 A (total current per module)
Output current I_{max}	1.5 A (per output)

16 Turck subsidiaries – contact information

Germany
Hans Turck GmbH & Co. KG
Witzlebenstraße 7, 45472 Mülheim an der Ruhr
www.turck.de

Australia
Turck Australia Pty Ltd
Building 4, 19-25 Duerdin Street, Notting Hill, 3168 Victoria
www.turck.com.au

Belgium
TURCK MULTIPROX
Lion d'Orweg 12, B-9300 Aalst
www.multiprox.be

Brazil
Turck do Brasil Automação Ltda.
Rua Anjo Custódio Nr. 42, Jardim Anália Franco, CEP 03358-040 São Paulo
www.turck.com.br

China
Turck (Tianjin) Sensor Co. Ltd.
18,4th Xinghuazhi Road, Xiqing Economic Development Area, 300381 Tianjin
www.turck.com.cn

France
TURCK BANNER S.A.S.
11 rue de Courtalin Bat C, Magny Le Hongre, F-77703 MARNE LA VALLEE Cedex 4
www.turckbanner.fr

Great Britain
TURCK BANNER LIMITED
Blenheim House, Hurricane Way, GB-SS11 8YT Wickford, Essex
www.turckbanner.co.uk

India
TURCK India Automation Pvt. Ltd.
401-403 Aurum Avenue, Survey. No 109 /4, Near Cummins Complex,
Baner-Balewadi Link Rd., 411045 Pune - Maharashtra
www.turck.co.in

Italy
TURCK BANNER S.R.L.
Via San Domenico 5, IT-20008 Bareggio (MI)
www.turckbanner.it

Japan
TURCK Japan Corporation
Syuuhou Bldg. 6F, 2-13-12, Kanda-Sudacho, Chiyoda-ku, 101-0041 Tokyo
www.turck.jp

Canada
Turck Canada Inc.
140 Duffield Drive, CDN-Markham, Ontario L6G 1B5
www.turck.ca

Korea
Turck Korea Co, Ltd.
B-509 Gwangmyeong Technopark, 60 Haan-ro, Gwangmyeong-si,
14322 Gyeonggi-Do
www.turck.kr

Malaysia
Turck Banner Malaysia Sdn Bhd
Unit A-23A-08, Tower A, Pinnacle Petaling Jaya, Jalan Utara C,
46200 Petaling Jaya Selangor
www.turckbanner.my

Mexico
Turck Comercial, S. de RL de CV
Blvd. Campestre No. 100, Parque Industrial SERVER, C.P. 25350 Arteaga, Coahuila
www.turck.com.mx

Netherlands
Turck B. V.
Ruiterlaan 7, NL-8019 BN Zwolle
www.turck.nl

Austria
Turck GmbH
Graumanngasse 7/A5-1, A-1150 Wien
www.turck.at

Poland
TURCK sp.z.o.o.
Wroclawska 115, PL-45-836 Opole
www.turck.pl

Romania
Turck Automation Romania SRL
Str. Siriului nr. 6-8, Sector 1, RO-014354 Bucuresti
www.turck.ro

Russian Federation
TURCK RUS OOO
2-nd Pryadilnaya Street, 1, 105037 Moscow
www.turck.ru

Sweden
Turck Sweden Office
Fabriksstråket 9, 433 76 Jonsered
www.turck.se

Singapore
TURCK BANNER Singapore Pte. Ltd.
25 International Business Park, #04-75/77 (West Wing) German Centre, 609916 Singapore
www.turckbanner.sg

South Africa
Turck Banner (Pty) Ltd
Boeing Road East, Bedfordview, ZA-2007 Johannesburg
www.turckbanner.co.za

Czech Republic
TURCK s.r.o.
Na Brne 2065, CZ-500 06 Hradec Králové
www.turck.cz

Turkey
Turck Otomasyon Ticaret Limited Sirketi
Inönü mah. Kayisdagi c., Yesil Konak Evleri No: 178, A Blok D:4,
34755 Kadiköy/ Istanbul
www.turck.com.tr

Hungary
TURCK Hungary kft.
Árpád fejedelem útja 26-28., Óbuda Gate, 2. em., H-1023 Budapest
www.turck.hu

USA
Turck Inc.
3000 Campus Drive, USA-MN 55441 Minneapolis
www.turck.us

TURCK

Over 30 subsidiaries and over
60 representations worldwide!

100002297 | 2021/11

www.turck.com