TigoMaster 2TH (EtherNet/IP)

USER MANUAL

Table of Contents

List of Figures

List of Tables

Revision Control

Author Name	Description	Revision	Date
Shoval Ben Shanan	Original Document	01	February 2022
Robert Collins	Editing	01	March 2022
Gali Ben Natan	Updating Tigo Engine Screenshots	03	June 2022
Mike Carmel	Edits, Reformats, Updates (MC002)	04	January 2023
Mike Carmel	Edits, Reformats, Updates (MC003)	05	February 2023
Mike Carmel	Edits, Reformats, Updates (MC004)	05	February 2023
Shoval Ben Shanan	Updated device port validation and backup values	06	September 2023

Acronyms and Abbreviations

Acronyms and abbreviations used in this document are listed in this table:

Term	Meaning
DSlot	Double Slot
FAT	File Allocation Table
FOTA	Firmware Upgrade Over the Air
FW	Firmware
HW	Hardware
IF	Interface
IOLW	IO-Link Wireless
ISDU	Indexed Service Data Unit
LQI	Link Quality Indicators
PDin	Process Data Input
PDout	Process Data Output
PER	Packet Error Rate
RSSI	Received Signal Strength Indication
SSlot	Single Slot
SW	Software
W-Device	Wireless Device (e.g., TigoBridge)
W-Master	Wireless Master (e.g., TigoMaster 2TH)

1. Introduction

1.1. About this User Manual

This User Manual describes the TigoMaster 2TH IO-Link Wireless Master (TigoMaster 2TH). TigoMaster 2TH is a wireless, decentralized input and output device which operates within a given computer network, such as those based on the PROFINET, EtherNet/IP, or EtherCAT protocols.
This User Manual focuses only on use with the EtherNet/IP protocol.

Note:
The TigoMaster 2TH IO-Link Wireless Master can be used with the PROFINET protocol (Part Number: CT241-0003t2-02) or EtherCAT protocol (Part Number: CT241-0008t2-01). This User Manual only focuses on use with the EtherNet/IP protocol.

The product and its firmware are under development and, therefore, functionality may change. As such, all information provided in this User Manual is preliminary and may not be complete or error free.

1.2. Manual Structure

The sections of this User Manual build on one another from section numbers 1 to 10.

1.3. Typographical Conventions

Enumerations are shown in list form with bullet points:

- Entry 1
- Entry 2
- Entry 3

Instructional steps are shown in list form with numbering:

1. Step 1
2. Step 2
3. Step 3

Decimal numbers are shown without additional indicators and are not spelled out (for example, 123).

1.4. Symbols

The following symbols are used in this User Manual:

Symbol	Meaning
	Note: This symbol indicates a general note.
	Warning: This symbol indicates a security notice which must be observed.
REF	**Reference**: This symbol indicates a cross-reference to other documentation

1.5. Deviating Views

The product views and illustrations in this User Manual may deviate from the actual product.

2. Safety and Requirements

2.1. General Note

Users of this manual must be qualified to use the device described. All safety messages, property damage messages, and valid legal regulations must be observed by users.

Note: CoreTigo Ltd. assumes that users have the required technical capabilities.

2.2. Intended Use

The TigoMaster 2TH IO-Link Wireless Master can be used to either acquire or output IO-Link field signals to sensors, actuators, and hubs, with such signals being sent and received to a higher-level control system. It is intended for use in operating temperatures of -25°C to 55°C. Its housing will protect it from damage caused by any buildup of moisture on surfaces which are in contact with the air. It is developed for any working environment requiring protection class IP67.

Note:
The TigoMaster 2TH is intended for indoor use. If mounted outside, it must be mounted in such a way that it is protected from weathering, especially from direct sunlight and the effects of UV light, salt water, or salt spray: for example, in a switch box.

For more details on Select the Mounting Location, see section 4.1.1.

Warning:
Product applications other than those described in this User Manual are not permitted.

2.3. Personnel Qualification

The product may only be mounted, configured, operated, or demounted by qualified personnel with skills in the following areas:

- Safety and health at work
- Mounting and connecting of electrical equipment
- Measurement and analysis of electrical functions and systems
- Evaluation of the safety of electrical systems and equipment.

Warning:
CoreTigo Ltd. does not assume any warranty or liability for damage caused to the product due to non-compliance with security measures or incorrect installation of the product.

2.4. Power Drop for Write/Delete Access in File System

The **File Allocation Table (FAT)** file system in the netX firmware is subject to certain operational limitations. Specifically, write and delete access in the file system (for the purpose of firmware update, configuration, download, and so forth) may destroy the FAT if access cannot be completed during power drops.

Without such a proper FAT, firmware might not be found nor started. Hence, it is important to verify that the power supply of the device does not drop during write and delete access in the file system.

2.5. Exceeding the Maximum Number of Permitted Write/Delete Access

TigoMaster 2TH uses a serial flash chip to store remaining data, such as firmware and configuration storage. It allows for a maximum of 100,000 write/delete accesses, which suffices for standard operation of the device. However, excessive writing/deleting on the chip (for example, by modifying the configuration or station name) will lead to the maximum number of permitted write/delete accesses being exceeded, thereby causing damage to TigoMaster 2TH.

For example:

- If the configuration is changed once an hour, then the maximum accesses will be reached after 11.5 years.
- If the configuration is changed once a minute, then the maximum accesses will be reached after ~69 days.

Therefore, it is highly recommended to avoid excessive writing/deleting on the chip.

2.6. Information and Data Security

Users are expected to follow all safety measures regarding information and data security relevant to devices used with EtherNet technology.

If a TigoMaster 2TH is connected to a public network, safeguard its data integrity by doing one of the following:

- Install it behind a firewall (recommended).
- Make the TigoMaster 2TH accessible only through a secure connection (for example, an encrypted VPN connection).

2.7. Regulatory Notices

2.7.1. Class A Warnings - Industrial Use

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

2.7.2. FCC Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment - **FCC ID:** 2ATSM-COR2TH.

2.7.3. ISED Warning

CoreTigo Ltd. does not endorse any changes made to the device by the user of any kind. Any change or modification may void the user's right to use the device.

CoreTigo Ltd. n'approuve aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

2.7.4. Interference Statement

This device complies with Part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. *L'appareil ne doit pas produire de brouillage, et*
2. *L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

2.7.5. Wireless Notice

This device complies with FCC/ISED radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines and RSS-102 of the ISED radio frequency (RF) Exposure rules. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Le présent appareil est conforme à l'exposition aux radiations FCC / ISED définies pour un environnement non contrôlé et répond aux directives d'exposition de la fréquence de la FCC radiofréquence (RF) et RSS-102 de la fréquence radio (RF) ISED règles d'exposition. L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur.

2.8. Requirements

2.8.1. Hardware and System Requirements

Installation of the product requires the following hardware:

- TigoMaster 2TH IO-Link Wireless Master
- 24 V DC SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage) Power Supply
- Power Supply Cable With L-Coded M12 Connector
- EtherNet Cable With D-Coded M12 Connector
- EtherNet/IP Supported PLC (not mandatory)
- IO-Link Wireless Device or IO-Link Wireless Bridge (at least one)
- Wired IO-Link Device
- EtherNet Network Switch
- PC or Notebook with a minimum of 1 additional EtherNet Port and Internet Access/PLC

All components listed above are supplied by CoreTigo Ltd. upon purchase.

2.8.2. Software

Configuration and commissioning of the product require the TigoEngine (provided by CoreTigo Ltd. upon purchase) and an internet browser.

3. Getting Started

3.1. Product Description

The TigoMaster 2TH is an IO-Link Wireless Master that you can use in an EtherNet/IP network and can operate up to 16 IO-Link sensors/actuators via wireless connectivity. It is supplied with a software tool, TigoEngine, which you can use to configure it over the EtherNet/IP network. You can also use TigoEngine to configure the parameters of any IO-Link Wireless sensors/actuators connected to the TigoMaster 2TH. Alternatively, you can use various other configuration tools, such as the CoreTigo Web Server.

The TigoMaster 2TH has an integral OPC UA server, providing identification, statuses, and configuration capabilities.

3.2. Product Overview

3.2.1. Functionality

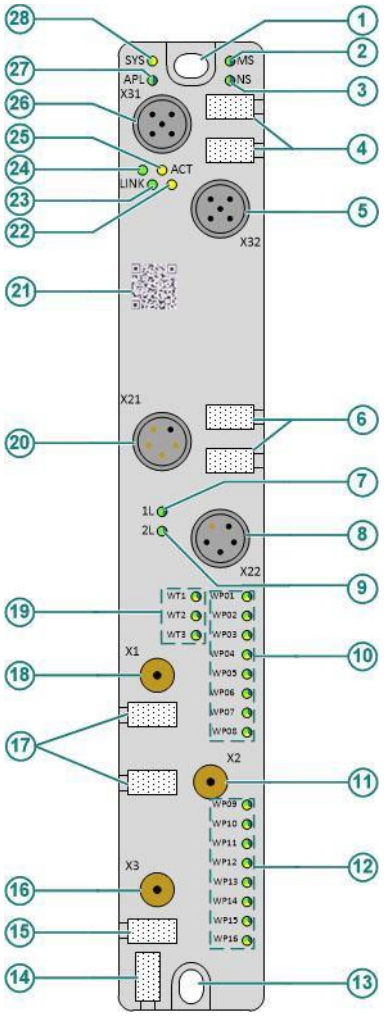


Figure 1: TigoMaster 2TH (EtherNet/IP Version)

The functionality illustrated by **Error! Reference source not found.** above is described in **Error! Reference source not found.**.

Table 1: TigoMaster 2TH Functionality (EtherNet/IP Version)

Function	Number	Name	Description
EtherNet	(26)	X31	EtherNet interface, M12, D-coded, EtherNet /IP port 1 (CH0)
	(5)	X32	EtherNet interface, M12, D-coded, EtherNet /IP port 2 (CH1)
	(24)	LINK (X31)	Link LED for connector X31
	(25)	ACT (X31)	Activity LED for connector X31
	(22)	ACT (X32)	Activity LED for connector X32
	(23)	LINK (X32)	Link LED for connector X32
	(24)	-	Labeling fields EtherNet interfaces X31 and X32
LEDs	(28)	SYS	System status LED
	(27)	APL	Application status LED
	(2)	MS	Module status LED
	(3)	NS	Network status LED
Power supply	(20)	X21	Power supply input (Power In), M12, L-coded
	(8)	X22	Power supply output (Power Out), M12, L-coded
	(7)	1L (X22)	1L supply voltage status LED (DC 24 V)
	(9)	2L (X22)	2L supply voltage status LED (DC 24 V)
	(6)	-	Labeling fields power supply input X21and output X22
Antenna connectors and LEDs for IO- Link wireless radio module	(18)	X1	Connector for SMA antenna for IO-Link wirelessconnection to the devices 1 to 8
	(11)	X2	Connector for SMA antenna for IO-Link wirelessconnection to the devices 9 to 16
	(16)	X3	Connector for auxiliary antenna
	(17), (15)	-	Labeling fields SMA antennas X1, X2, X3
	(19)	WT1 …WT3	IO-Link wireless track status LEDs
	(10)	WP01 …WP08	Port status LEDs for IO-Link wireless device ports P01 to P08
	(12)	WP09 …WP16	Port status LEDs for IO-Link wireless device ports P09 to P16
Device identification	(21)	-	Data matrix code
	(14)	-	Device labeling field for the TIGOMASTER 2TH device
Mounting	(1)	-	Mounting hole (up) and grounding
	(13)	-	Mounting hole (down)

3.2.2. Lasering

All technical data, such as the manufacturer's address, product name, part number, serial number, MAC address, certification signs (for example, CEL and UL), environmental signs (for example, disposal), and other data is provided in the form of lasering on the right- or left-hand side of the device's housing.

See section 10 of this User Manual for further details on Technical Data.

3.2.3. Revisions and Versions

The device's hardware revision listed in Table functionally belongs with the software and firmware versions listed in

Table and

Table below. With any hardware installation, firmware must be updated.

Table 2: TigoMaster 2TH Hardware

Product Name	Description	Part Number	Hardware Revision
TigoMaster 2TH-EtherNet/IP	IO-Link Wireless Master (EtherNet/IP Version)	CT241-0004t2-01	Rev03

Table 3: TigoMaster 2TH Software

Software	Name	Version
Engineering Tool	TigoEngine	3.1
Integrated Web Server	CoreTigo Web Server	1.2
PLC IDE	Studio5000	32.00.00

Table 4: TigoMaster 2TH Firmware

Protocol	File Name	Version
EtherNet/IP Adapter	UI197H001.nxi	2.x.x

3.2.4. Identification

A 2D data matrix code (DM code, 10x10 mm) is provided on the front side of the TigoMaster 2TH housing. This code includes a part number, hardware revision, and serial number for device identification.

Figure 2: TigoMaster 2TH Identification Code

Additional identification data is provided in plain text on the right-hand side of the device's housing.

Sample values:

- Product Name: 1234.567
- Part Number: 1912.122
- Serial Number: 2000
- MAC ID: 00-02-A2-2F-75-44

3.2.5. LED Indications

The tables below detail what is indicated by each state of each LED on the TigoMaster 2TH.

3.2.5.1. System LEDs

Table 5: System LEDs

LED Type	Color	State	Description
SYS		On	The firmware is running.
		Blinking	File system formatting is in progress.
		On	A system error has occurred.
		Blinking (3 x Yellow, 3 x Green)	Firmware crash, unrecoverable (an internal exception occurred that cannot be handled).
		Blinking (1 Hz, 4Hz)	1 Hz: The maintenance firmware is idle (waiting for update). 4 Hz: The maintenance firmware is in operation: a firmware update will be installed.
		Off	No supply voltage to the TigoMaster 2TH, or a hardware defect during a firmware reset.

Table 6: System LED States

LED State	Description
Blinking	The display turns on and off in phases.
Blinking (3 x **Yellow**, 3 x **Green**)	The indicator turns on and off with a frequency of approximately 1 Hz: • 3 x **Yellow** "On" for 500 ms and "Off" for 500 ms • 3 x **Green** "On" for 500 ms and "Off" for 500 ms
Blinking (1Hz, 4 Hz)	The indicator turns on in phases **Yellow** or **Green** with a frequency of approximately: • 1 Hz: 1 x **Yellow** "On" for 500 ms and 1 x **Green** "On" for 500 ms • 4 Hz: 1 x **Yellow** "On" for 125 ms and 1 x **Green** "On" for 125 ms

3.2.5.2. APL LEDs

Table 7: APL LEDs

LED Type	Color	State	Description
APL		On	IO-Link Wireless Master configured.
		Blinking	Communication established.
		On	Initialization of components done.
		Blinking	Communication error.
		Off	Components not initialized.

3.2.5.3. Supply Voltage LEDs

Table 8: Supply Voltage LEDs

LED	Color	State	Description
1L		On	1L supply voltage OK.
		Off	No 1L supply voltage.
2L		On	2L supply voltage OK.
		Off	No 2L supply voltage.

3.2.5.4. EtherNet/IP Adapter LEDs

Table 2: EtherNet/IP Adapter LEDs

LED	Color	State	Description
MS (Module Status))		On	**Device Operational:** The device is operating correctly.
		Flashing (1 Hz)	**Standby:** The device has not been configured.
		Flashing	**Self-Test:** The device is performing its power-up testing. The module status indicator test sequence occurs

LED	Color	State	Description
			before the network status indicator test sequence, according to the following sequence: • Network status LED off • Module status LED turns **Green** for approximately 250 ms, turns **Red** for approximately 250 ms, and again turns **Green** (and holds that state until the power-up test has completed) • Network status LED turns **Green** for approximately 250 ms, turns **Red** for approximately 250 ms, and then turns off (and holds that state until the power-up test has completed)
		Flashing (1 Hz)	**Major Recoverable Fault:** The device has detected a major recoverable fault. e.g. an incorrect or inconsistent configuration can be considered a major recoverable fault.
		On	**Major Unrecoverable Fault:** The device has detected a major unrecoverable fault.
		Off	**No Power:** The device is powered off.
NS (Network Status)		On	**Connected:** An IP address is configured, at least one CIP connection (any transport class) is established, and an Exclusive Owner connection has not timed out.
		Flashing (1 Hz)	**No Connections:** An IP address is configured, but no CIP connections are established, and an Exclusive Owner connection has not timed out.
		Flashing	**Self-Test:** The device is performing its power-up testing. Refer to description for module status LED self-test.
		Flashing (1 Hz)	**Connection Time-Out:** An IP address is configured, and an Exclusive Owner connection for which this device is the target has timed out.

LED	Color	State	Description
			The network status indicator returns tosteady **Green** only when all timed out Exclusive Owner connections are reestablished.
		On	**Duplicate IP:** The device has detected that its IP address is already in use.
		Off	**Not Powered / No IP Address:** The device does not have an IP address (or is powered off).

Table 10: EtherNet/IP Adapter LED States

LED Status	Definition
Flashing (1Hz)	The indicator turns on and off with a frequency of 1 Hz: **On** for 500 ms, followed by **Off** for 500 ms.
Flashing **Green/Red/Green**	The MS LED indicator turns on **Green** on for 250 ms, then **Red** on for 250 ms, then **Green** on (until the test is completed).
Flashing **Green/Red/Off**	The NS LED indicator turns on **Green** on for 250 ms, then **Red** on for 250 ms, then **Off** (until the test is completed).

3.2.5.5. EtherNet LEDs

The following table describes the LED states of the link and activity LED.

Table 3: EtherNet Status

LED	Color	State	Description
LINK		On	The device is linked to the EtherNet.
		Off	The device has no link to the EtherNet.
ACT		Flickering (load dependent)	The device sends/receives EtherNet frames.
		Off	The device does not send/receive EtherNet frames.

Table 4: EtherNet LED States

LED Status	Definition
Flickering (LoadDependent)	The indicator turns on and off with a frequency of approximately 10 Hz to indicate high EtherNet activity – On for approximately 50 ms, followed by off for 50 ms. The indicator turns on and off in irregular intervals to indicate low EtherNet activity.

3.2.5.6. Wireless Track LEDs

The wireless track status LEDs WT1 … WT3 indicate the states for the wireless tracks 1, 2, 3 as described in the table below.

Table 5: Wireless Track Status WT1 … WT3

LED	Color	State	Description
WT1–WT3		On	Track operational mode and track service mode
		On	Track inactive.
		Blinking	Track error.
		Off	Track off.

3.2.5.7. Wireless Port LEDs

The wireless port status LEDs WP01 … WP16 indicate the states for the wireless ports 1 … 16 as described in the table below.

Table 6: Wireless Track Status WP01 … WP16

LED	Color	State	Description
WP1 … WP16		On	Port operational.
		Blinking	Pairing success, communication ready.
		Blinking	Port ready.
		Blinking	Port communication lost.
		On	Port errors (pairing timeout, pairing wrong slot-type, revision fault, compatibility fault, serial number fault, process data fault, cycle time fault).
		Off	Port inactive.

3.2.6. Connection Points

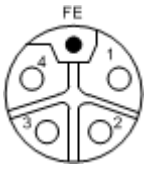
3.2.6.1. Power Supply

The device's power is supplied via connector X21 (PWR IN). Once connected, users can connect two supply lines to the connector which are both electrically isolated:

- **Supply Line 1**: 1L (U1L) and the reference potential 1L-
- **Supply Line 2**: 2L (U2L) and the reference potential 2L-

Each connector pin X21 (PWR IN) is connected to the same pin of socket X22 (PWR OUT) and is used to forward the power supply to the next device.

Table 7: Power Supply Connectors

PWR IN	PWR OUT	Pin	Signal	Description
 M12, L-coded, male 5-pin (4 + FE) (X21)	 M12, L-coded, female 5-pin (4 + FE) (X22)	1	1L+	+24 V DC power supply for system and sensor, U_{1L}
		2	2L-	Reference potential for 2L.
		3	1L-	Reference potential for 1L.
		4	2L+	+24 V DC power supply for auxiliary/switched power supply, U_{2L}
		FE	FE	Functional earth

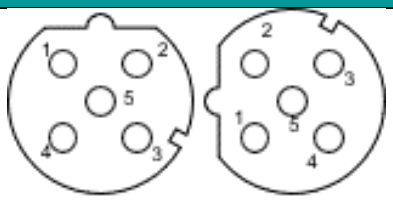
3.2.6.2. EtherNet

Users must use the following connectors to establish a connection with EtherNet interface ports of the TigoMaster 2TH (EtherNet/IP) device:

- Connector **X31** for EtherNet interface port 1 (CH0)
- Connector **X32** for EtherNet interface port 2 (CH1)

To identify the connectors see **Error! Reference source not found.**. Connector X31 is item (32), and connector X 32 is item (10).

Table 8: EtherNet Connectors

EtherNet	Pin	Signal	Description
 M12, D-coded, socket, 5-pin	1	TX+	Send data (positive).
	2	RX+	Receive data (positive).
	3	TX–	Send data (negative).
	4	RX–	Receive data (negative).
	5	FE	Functional earth.

3.2.6.3. SMA Antenna

The TigoMaster 2TH device is equipped with three SMA antenna tracks. Each track supports up to 8 IO-Link wireless devices (24 in total). The types of data transferred (e.g. length and data type) may vary depending on the connected IO-Link devices.

Table 9: SMA Antenna

SMA Antenna	Type	Manufacturer
	2.4GHz Antenna - 2.4GHz, 5GHz • **Bandwidth:** 1000 MHz • **Impedance:** 50 Ohms • **Power Rating:** 1 W	Silram Technologies Ltd., Kfar Saba, Israel Model: TLW2.5A-SMA-Male

It is not permitted to use an alternative SMA antenna from the one supplied by CoreTigo Ltd. Using an alternative SMA antenna may result in a loss of device approval. Additionally, all three SMA antennas (X1, X2, X3) must be mounted for proper device functioning

3.2.6.4. Derating

Note the derating when connecting a device to Power Out on the TigoMaster 2TH, and therefore a larger current passes through the TigoMaster 2TH. The amount of current, and also the ambient temperature, affect the heating of the TigoMaster 2TH. **Error! Reference source not found.** shows the maximum permissible current (I) that may flow into the TigoMaster 2TH as a function of the ambient temperature (T).

Note that the derating curve in **Error! Reference source not found.** below applies to operating conditions " without air flow or with air flow 0.5 m/s" and "mounting on poorly heat conducting wall". Other operating conditions (for example, higher air flow or a more heat conducting wall) might lead to better heat dissipation from the TigoMaster 2TH.

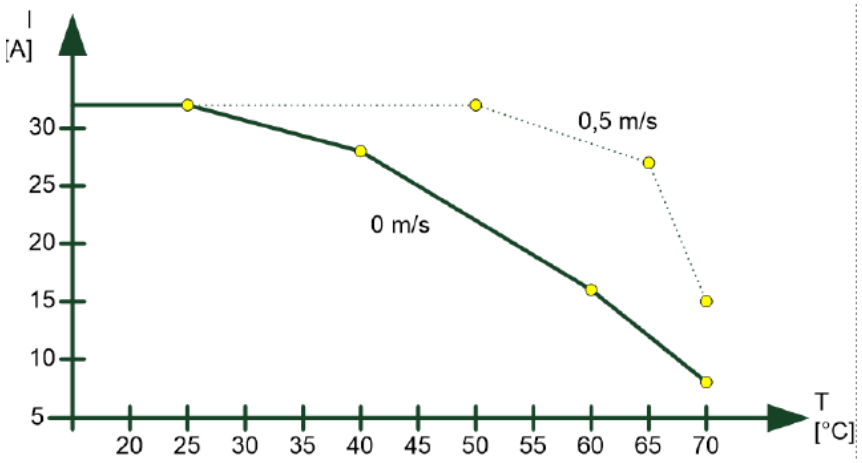


Figure 3: Derating TigoMaster 2TH IO-Link Wireless Master

4. Installation

Warning:

Comply with all safety instructions relevant to the TigoMaster 2TH (see section **Error! R eference source not found.**) and to the mounting tools.

The TigoMaster 2TH may only be installed and commissioned by qualified electricians in accordance with EN 50110-1/-2 and IEC 60364.

Make sure that the TigoMaster 2TH is not damaged. A damaged TigoMaster 2TH must not be put into operation.

Installation of the hardware, driver, and firmware for the TigoMaster 2TH has the following stages:

1. Installing Hardware – see section 4.1
2. Connection – see section 4.3

4.1. Installing Hardware

This section describes how to mount and ground the TigoMaster 2TH.

4.1.1. Select the Mounting Location

The TigoMaster 2TH can be mounted in the control cabinet or on any part of the system that meets the following requirements:

- If mounted outside, the TigoMaster 2TH must be mounted in such a way that it is protected from weathering, especially from direct sunlight and the effects of UV light, salt water or salt spray: for example, in a switch box.
- The TigoMaster 2TH must be screwed to a flat contact surfaces to protect it from mechanical tension.
- The TigoMaster 2TH must not be mounted in the shearing areas of moving system parts (otherwise it might be damaged).
- The cables for the TigoMaster 2TH must be laid in such a way that they cannot be caught in the shearing areas of moving system parts (otherwise they might be damaged).
- The mounting location must have sufficient space for easy replacement of the TigoMaster 2TH and connecting all required cables to it.
- The mounting location must meet the TigoMaster 2TH's vibration and shock resistance requirements.
- The diagnostic LEDs of the TigoMaster 2TH must be visible when it is mounted.
- The TigoMaster 2TH must not be mounted on or near highly inflammable materials.
- To prevent the TigoMaster 2TH from overheating:
  - It must not be mounted near strong heat sources
  - It must have an unobstructed air supply
  - Its cooling must not be impeded
- Do not bridge any gaps with the unit to protect it from any tensile forces that may occur.

4.1.2. Equipment Required

Mounting the TigoMaster 2TH requires the following equipment:

- M4 Allen key (for the TigoMaster 2TH mounting screws)
- Two M4 Allen screws, according to DIN 912 / ISO 4762, of suitable length

If the mounting location does not have suitable threaded holes for the M4 screws, the following equipment is also required:

- M4 thread tap (ready-made or a set of taps)
- Drilling machine (to pre-drill the holes for mounting the TigoMaster 2TH)

4.1.3. Mount the TigoMaster 2TH

Note:
Make sure not to soil the connectors on the TigoMaster 2TH during installation. Dirt will damage the contacts.

1. Disconnect the system from the power supply.
2. Ensure sufficient equipotential bonding in the system.
3. Make 2 M4 threaded screw holes as follows:
   - Hold the TigoMaster 2TH in the desired position.
   - Mark the 2 points where the threads are to be cut (at upper and lower ends of the TigoMaster 2TH).
   - If necessary, pre-drill holes with a drill.
   - Cut an M4 thread at each of the two marked points with the M4 thread cutter.
4. Secure the unit in the desired position using two M4 Allen screws of suitable length and the tightening torque detailed in section 10.
5. Mount the TigoMaster 2TH's three SMA antennas (X1, X2, X3).

   All SMA antennas (X1, X2, X3) must be mounted for proper TigoMaster 2TH operation

4.1.4. Ground the TigoMaster 2TH

Each of the TigoMaster 2TH's power supply connectors has an FE pin that is connected to the metal housing of the TigoMaster 2TH. The metal housing has a central grounding point for the FE.

Ground the TigoMaster 2TH as follows:

1. Connect each of the M4 mounting screws to FE (functional earth) in one or more of the following ways:
   - Via the metal housing
   - Via FE of the power supply connectors
   - Via a cable lug and the mounting hole, if the TigoMaster 2TH is mounted on a non-conductive base.
2. Make sure that the contacts are perfect and that the cable cross-section is sufficient.

4.2. Demount the TigoMaster 2TH

General Requirements:

- Allen key to loosen the M4 hexagon socket head screws according to DIN 912 or ISO 4762

Prerequisites**:**

- Disconnect the part of the plant to which you have mounted the TigoMaster 2TH from the power supply
- If the TigoMaster 2TH is dirty, clean it first. It is particularly important to clean dirty screw connections
- Before demounting, loosen all screw connections at the terminals and disconnect the cables

Instructions**:**

1. Verify that the plant on which the TigoMaster 2TH is mounted is de-energized.
2. Use the Allen key to loosen the two M4 cylinder head screws.
3. Remove the TigoMaster 2TH for replacement or reuse.

Warning:

During operation, high surface temperatures can occur on the housing and at the metal connections, especially at the M12 connector sleeve. After the TigoMaster 2TH is in operation, let it cool down before touching it or use gloves.

Warning:

If the demounted TigoMaster 2TH is defective, mark it as defective to prevent it from being used again.

Disposal of Waste Electronic Equipment

Important notes from the European Directive 2021/19/EU “Waste Electrical and Electronic Equipment (WEEE)”.

Warning:

- This product must not be treated as household waste. As a consumer, you are legally obliged to dispose of all waste electronic equipment according to national and local regulations.
- This product must be disposed of at a designated waste electronic equipment collecting point.

4.3. Connection

Warning:

- Danger of electrical shock.
- Operate the TigoMaster 2TH exclusively with 24 V DC SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage) power supply.
- Always use two separate supply lines/power supplies for 1L and 2L to supply the devices.
- Pay attention to a central grounding (FE) if two separate power supplies are used.

TigoMaster 2TH Destruction and Fuse Protection

The maximum supply current must not be exceeded and must be fused with an external fuse (16 A). Otherwise, the risk of TigoMaster 2TH destruction cannot be excluded, damage to the printed circuit board and the connecting plug.

Connection Example with TigoBridge

The connection example described hereafter shows a typical installation that uses a TigoBridge to connect a wired IO-Link device via a wireless connection to the IO-Link Wireless Master.

Requirements**:**

- L-Coded M12 power cable (+24 V DC SELV or PELV)
- D-Coded M12 EtherNet cable

Connect the EtherNet cable to the M12 connector EtherNet X31 of the TigoMaster 2TH and to the TigoEngine software and/or to PLC. Then connect the power cable (+24 V DC SELV or PELV) to the M12 connector PWR IN X21 of the TigoMaster 2TH.

TigoBridge**:**

Connect the wired IO-Link device with the cable to the W-Bridge. Then connect the power cable (+24 V DC SELV or PELV) to the power connector of the W-Bridge.

Switch on the power supply units of the TigoMaster and TigoBridge.

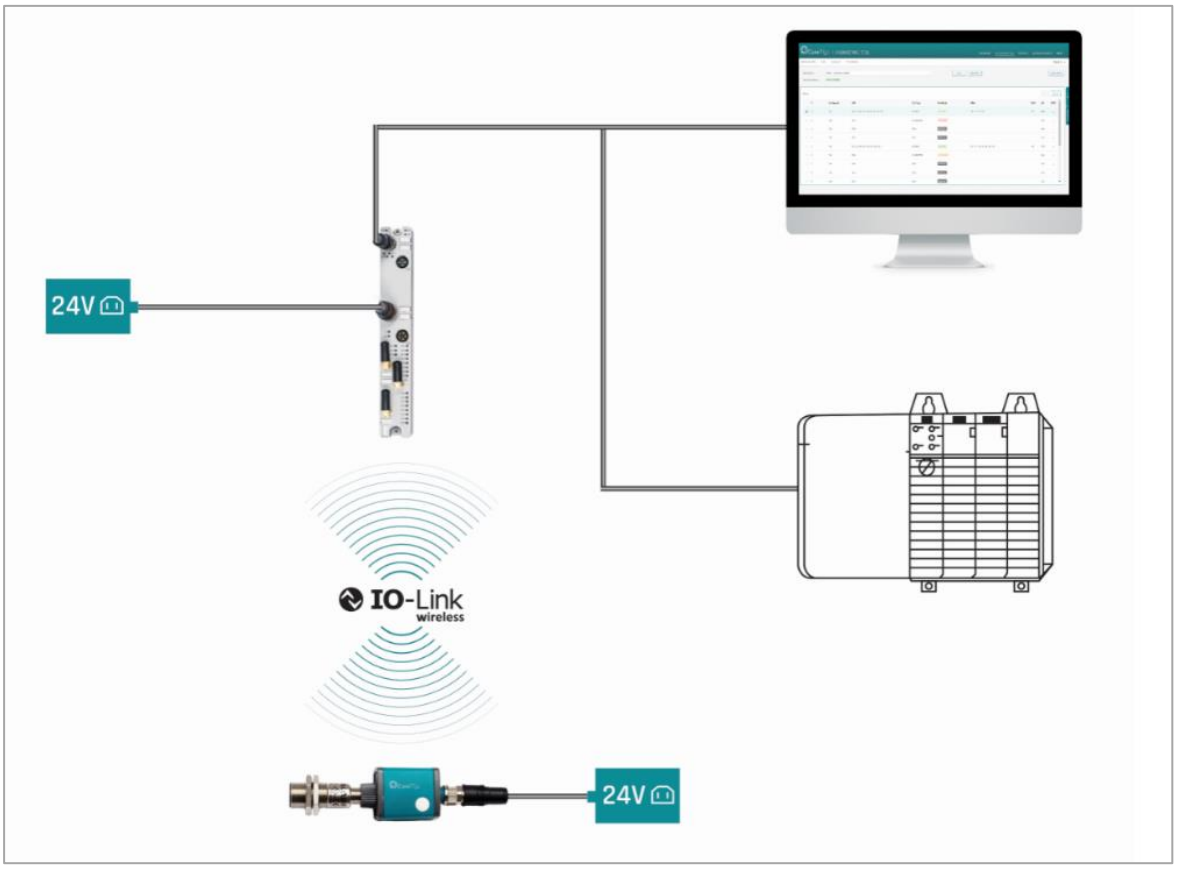


Figure 10: Connection Example with TigoBridge

5. Configuration

Before the TigoMaster 2TH can operate, it and its connected devices must be configured.

5.1. Introduction

In order for the TigoMaster 2TH to operate, it must be configured together with its connected devices, i.e. have their parameters set.

The parameters can be grouped in the following categories and sub-categories:

- TigoMaster 2TH:
  - EtherNet/IP connection.
  - Parameters for the IO-Link Wireless Master (e.g. track mode).
  - Parameters for the wireless ports (e.g. wireless slot number).
  - MQTT Client parameters – if the MQTT communication is to be used, then the MQTT Client in the TigoMaster 2TH requires MQTT Client parameters to be set.
- Connected IO-Link devices:
  - IO-Link device parameters.

To set parameters, use the following tools:

- **Configuration Software of the EtherNet/IP Scanner**
  - The EtherNet/IP Scanner must be configured to exchange process data with the TigoMaster 2TH device.
  - The configuration software of the EtherNet/IP Scanner requires an EDS file to configure the device.
  - The configuration software of the EtherNet/IP Scanner imports the EDS file, and the user can make the configuration settings and parameterizations for the device.
  - The user loads the configuration to the EtherNet/IP Scanner.
  - The EtherNet/IP Scanner performs the configuration and parameterization of the TigoMaster 2TH device.
- **CoreTigo Web Server**

  The CoreTigo Web Server can be displayed in a web browser, and enables you to set all the parameters for the TigoMaster 2TH, its connected IO-Link devices, and the MQTT Client in the TigoMaster 2TH.
- **TigoEngine**

  TigoEngine is software that enables you to do the following:
  - Set all parameters for the TigoMaster 2TH, its connected IO-Link devices, and the MQTT Client in the TigoMaster 2TH.
  - Monitor the TigoMaster 2TH and IO-Link devices in any system connected to TigoEngine.

Table 18 summarizes each tool and the parameters that it can set.

Table 18: Configuration Tools

Tool	IO-Link Wireless Master Parameters	Port Parameters	IO-Link Device Parameters	MQTT Client Parameters (if MQTT communication used)
EtherNet/IP Scanner	N/A	Applicable	N/A	N/A
TigoEngine Software Tool	Applicable	Applicable	Applicable	Applicable
CoreTigo Web Server	Applicable	Applicable	Applicable	Applicable (Not Secured)

Note:

When EtherNet/IP communication is initiated, the EtherNet/IP scanner transmits parameters to the TigoMaster 2TH device. Former port configuration parameters set by the TigoEngine software tool or OPC UA client are overwritten by the EtherNet/IP scanner.

To permanently modify port configuration parameters with the TigoEngine software tool or OPC UA client, parameters should be set using the EtherNet/IP scanner's configuration software.

To summarize, there are 3 levels of configuration, namely:

- IO-Link Configuration – Used for EtherNet/IP connection types
- IO-Link Wireless Configuration – Used for TigoMaster 2TH parameters
- Port Configuration – Used for IO-Link Wireless, the TigoBridge device, and SIO mode

Note:

Other IO-Link devices must also be configured.

5.2. EtherNet/IP Scanner

The EtherNet/IP scanner can be used to configure the TigoMaster 2TH IO-Link Wireless. While this manual describes how to configure TigoMaster 2TH with Studio5000, other available PLC IDEs may work as well.

Prerequisites

- Obtain an updated EDS file which may be provided separately or downloaded from the CoreTigo Ltd. website. The file should be named as follows: Coretigo_IOLW_TigoMaster_2TH-VX.X
- Components must be connected, and power plugged (as described in previous sections).
- The TigoMaster 2TH IO-Link Wireless Master must be connected to your PLC.

Instructions

Follow the steps below to configure the TigoMaster 2TH IO-Link Wireless Master using the EtherNet/IP scanner with Studio5000.

1. To import and install the EDS file, click the **TOOLS** tab in Studio5000.
2. Select the **EDS Hardware Installation Tool** option.

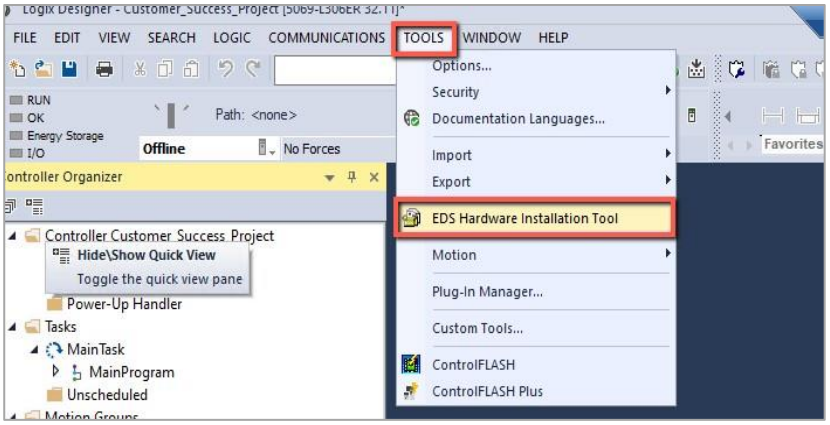


Figure 5: EDS File Installation (1)

3. Follow the steps described in the wizard.

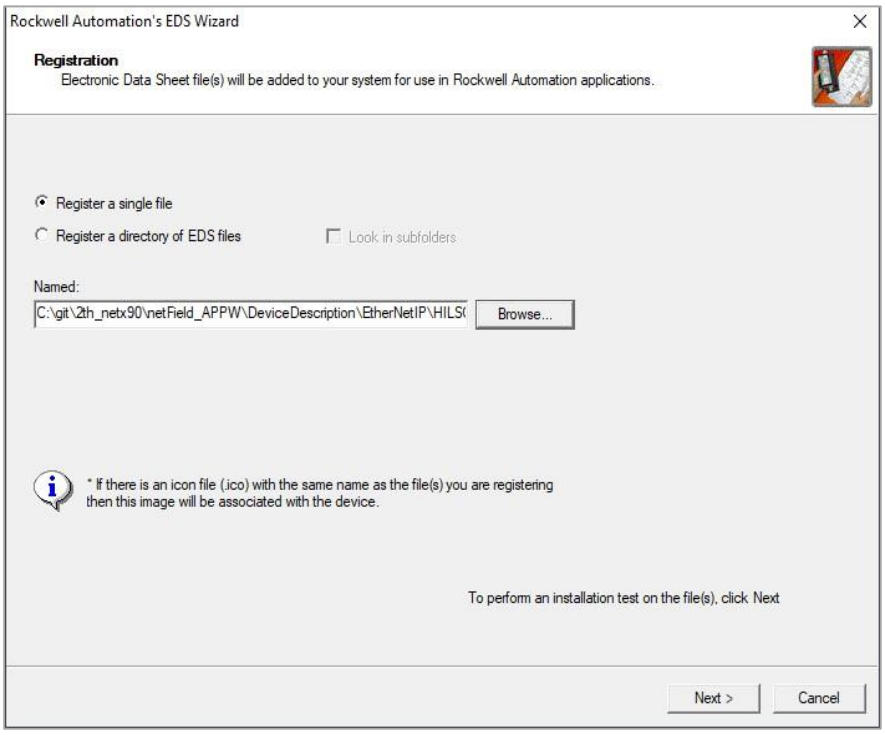


Figure 6: EDS File Installation (2)

4. To add a new module, click the **A1/A2 EtherNet** option in the navigation pane.

5. Click the **New Module** option.

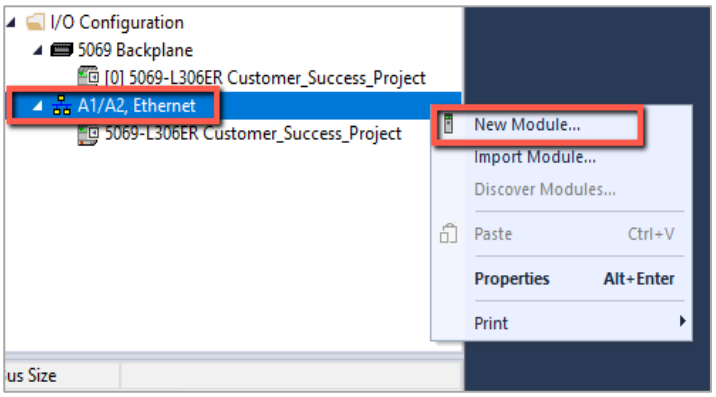


Figure 7: Add New Module (1)

6. Search for **Coretigo_IOLW_TigoMaster_2TH-V2.2** in the search field.
7. Click the relevant line found under **Catalog Number Press**.
8. Click the **Create** button.

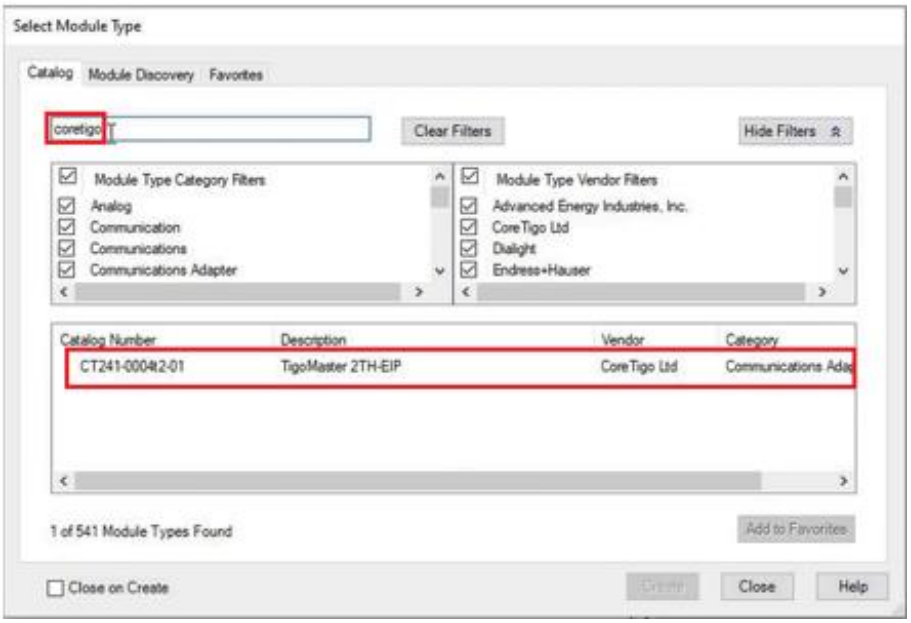


Figure 8: Add New Module (2)

Note:

Make sure you are using the same subnet for the TigoMaster 2TH IO-Link Wireless Masterand PLC. When set, TigoMaster 2TH data will also be visible on the PLC side.

9. To configure the module and connection types, enter a name for the new module.

10. Click the **Private Network** option.

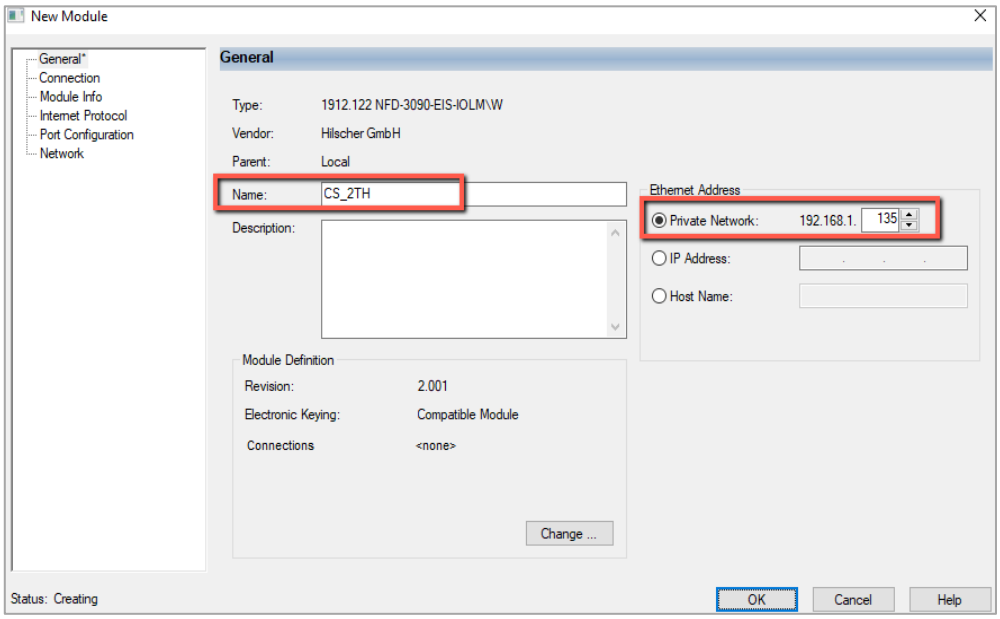


Figure 9: Configure Module (1)

11. Add the TigoMaster 2TH IP address.
12. Click the **Change…** button to change connection types.
13. In the **Module Definition** window, click the right arrow to expand the connection list.
14. Select the desired connection type.
15. Click the **OK** button.

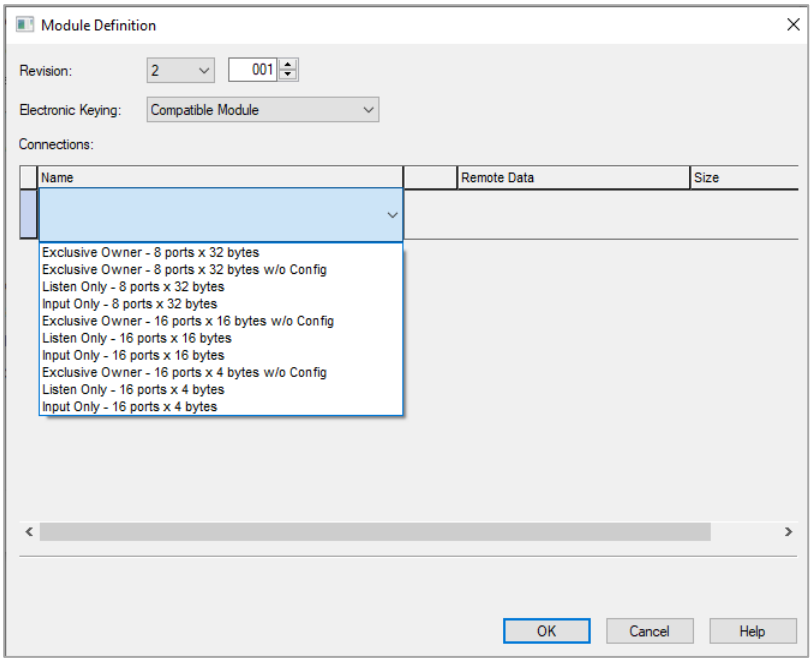


Figure 10: Configure Module (2)

16. In the **Logix Designer** window, click the **Yes** button to confirm the module definition changes.

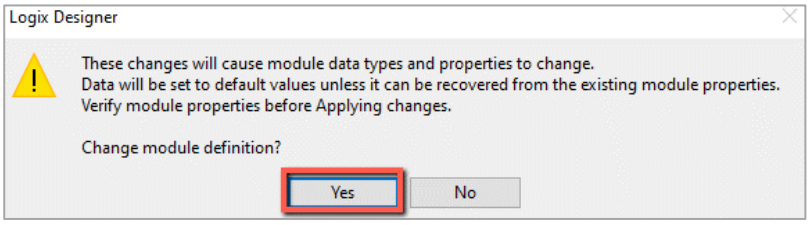


Figure 11: Configure Module (3)

17. In the **New Module** window, click the **Connection** option in the navigation pane to set the **Requested Packet Intervals (RPIs).**
18. Click the **OK** button.

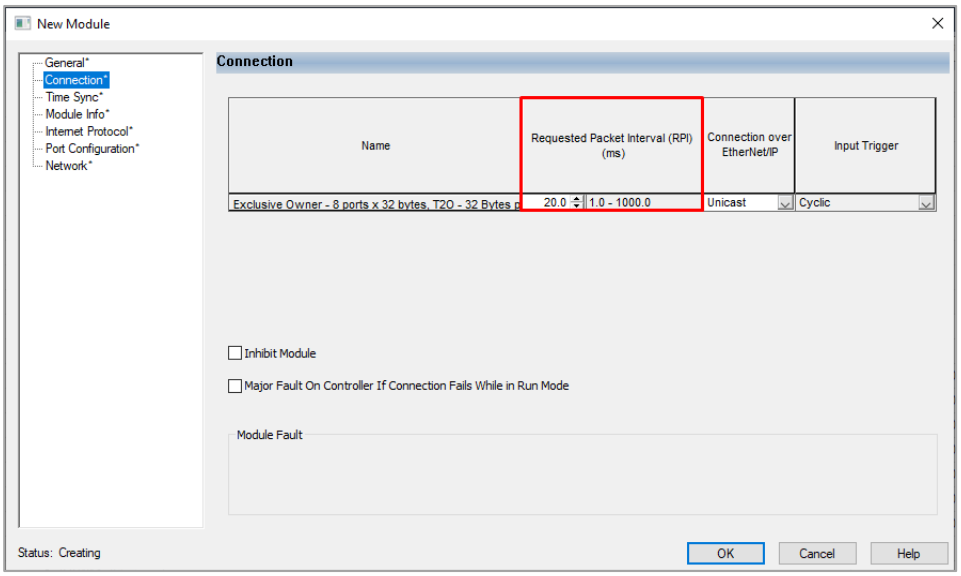


Figure 12: Set RPIs

19. To configure a wireless port using the EtherNet/IP scanner, click the **Exclusive Owner – 8Port X 32 Bytes** option which equates to connection type 1.
20. Under the **A1/A2, EtherNet** option, click the **Device Name: C** option.

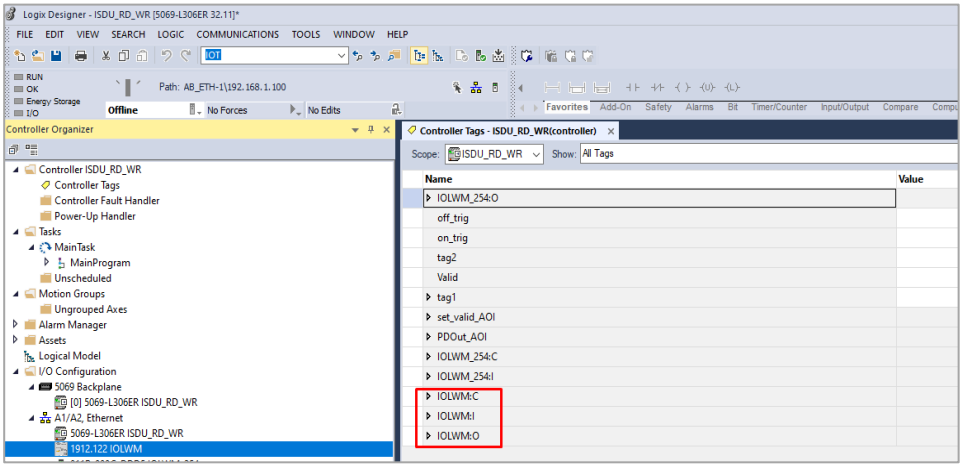


Figure 13: Wireless Port Configuration (1)

21. Click the relevant port name.

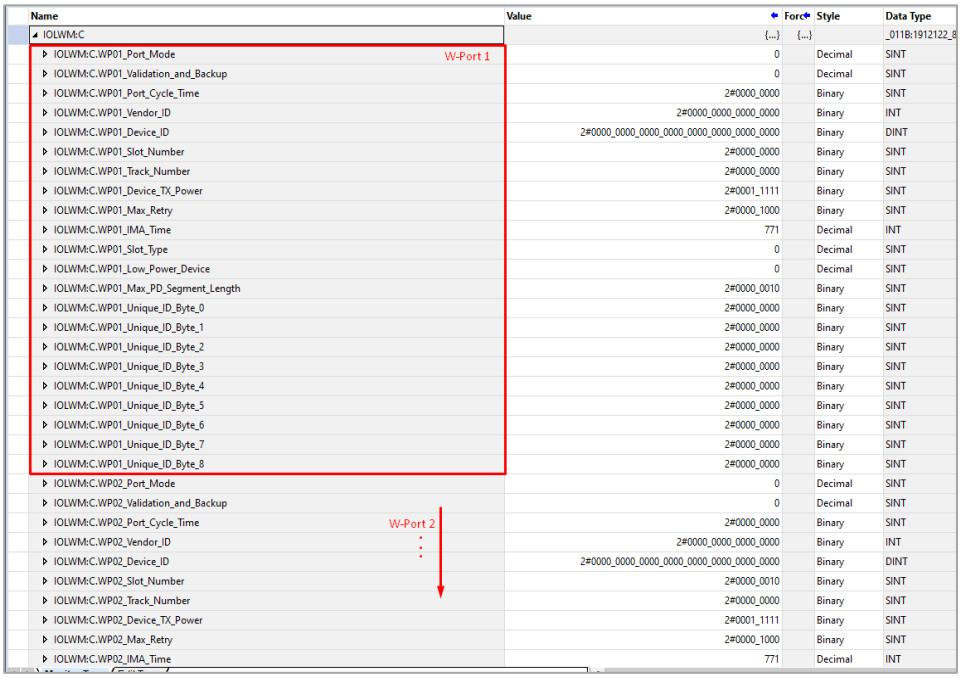


Figure 14: Wireless Port Configuration (2)

22. Change the required value according to the **Port Configuration** table below.

    Parameters can be configured only when using connection type 1.
    Default values are marked with an asterisk (*).

Table 19: Port Configuration

Name	Configuration	Mode	Description
Port Mode	Deactivated*	0*	The port is inactive. L+ is turned off, Input and Output Process Data is 0.
	Cyclic	1	Target mode based on user defined configuration including validation of Vendor ID, Device ID, and Revision.
	Roaming	2	Target mode without configuration. Validation: No Device Check.
Validation and Backup	No Device Check*	0*	There is no device check for validation or backup of connected IO-Link slave devices (default).
	Type Compare No Backup/Restore	5	A device check is performed for validation of connected IO-Linkslave devices to the specified device type, without backup/restore.
	Type Compare, Restore Only	7	A device check is performed for validation or restore of connected IO-Link slave devices to the specified device type, without backup.
	Type Compare, Backup and Restore	8	A device check is performed for validation or backup/restore ofconnected IO-Link slave devices to the specified device type.

Name	Configuration	Mode	Description
Port CycleTime	0*	N/A	Free running
	65 ... 127	N/A	Fixed Value
Vendor ID	0* … 65535	N/A	Vendor ID – See the documentation of the manufacturer of the sensor/actuator used.
Device ID	0* … 4294967295	N/A	Device ID – See the documentation of the manufacturer of the sensor/actuator used.
Slot Number	0 … 7	N/A	Wireless slot number to be used for the port.
Track Number	0 … 2	N/A	Wireless track number to be used for the port.
Device TX Power	0 … 31	N/A	This parameter contains the transmit power level of the W-Device.
Max. Retry	2 … 31	N/A	Maximum number of retries for a transmission in OPERATE mode.
IMA Time Base	1.664 msec	1	Requested IMA time for the OPERATE mode.
	5 msec	2	
	1 sec	3*	
	1 minute	4	
IMA Time Multi	1-255	N/A	Limited to 10 minutes maximum.
Slot Type	SSlot	0*	Slot type is “single slot”.
	DSlot	1	Slot type is “double slot”.
Low Power Device	No	0*	Connected W-Device is not low power.
	Yes	1	Connected W-Device is low power.
Max. PD Segment Length	0x00 … 0x20	0x00 … 0x20	This parameter contains the maximum segment length of the PDOut data to the Message handler to distribute PDOut Datawithin multiple W-cycles.
Unique ID – Byte 1	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 2	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 3	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 4	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 5	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 6	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 7	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 8	0 … 0xff	N/A	UniqueID of the W-Device.
Unique ID – Byte 9	0 … 0xff	N/A	UniqueID of the W-Device.

5.3. TigoEngine

The TigoEngine software tool must be installed prior to configuration and parameterization.

References:

- TigoEngine – User Manual
  (This User Manual refers to TigoEngine V1.3.1100.0.)

5.3.1. Masters View

TigoEngine supports multiple TigoMaster 2TH connections. TigoEngine's **Masters** view is used for connecting a new TigoMaster 2TH to TigoEngine and keeping a record of connected TigoMaster 2THs.

5.3.2. Connecting a New Master

Note:
Before connecting a new TigoMaster 2TH to TigoEngine, its IP address must be configured and known.

- The TigoMaster 2TH is provided with a default IP Address 192.168.1.100, and the subnet mask address is 255.255.255.0. See section 6.2.
- To define the IP address using CoreTigo Web Server see section 6.2.
- In case the TigoMaster 2TH is in BOOTP/DHCP mode please use the BOOTP tool to configure the IP address.

3. In TigoEngine's **Masters** view, click the **Connect New Master** button.

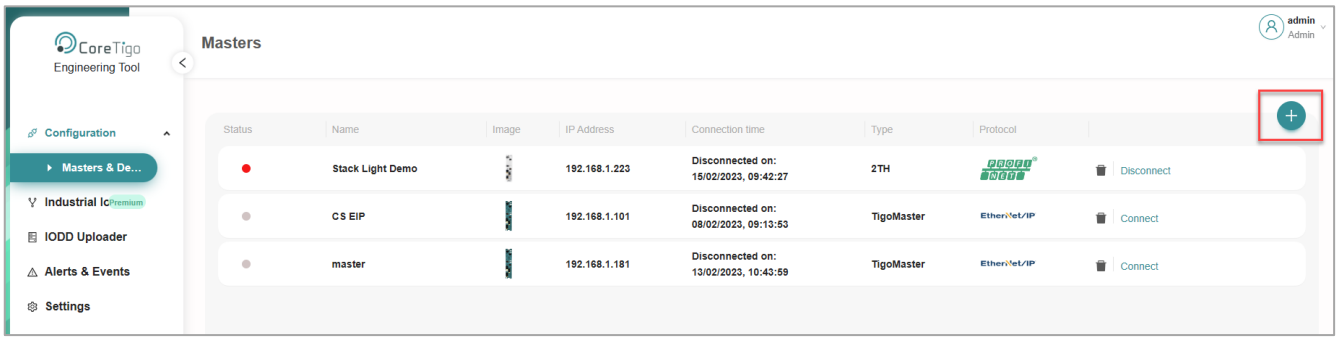


Figure 15: Connect New Master Button

4. In the **Connect New Master** window, set the following:
   - **Name** – type the desired name for this TigoMaster 2TH.
   - **IP** – type the IP address of the TigoMaster 2TH to connect to the TigoEngine.

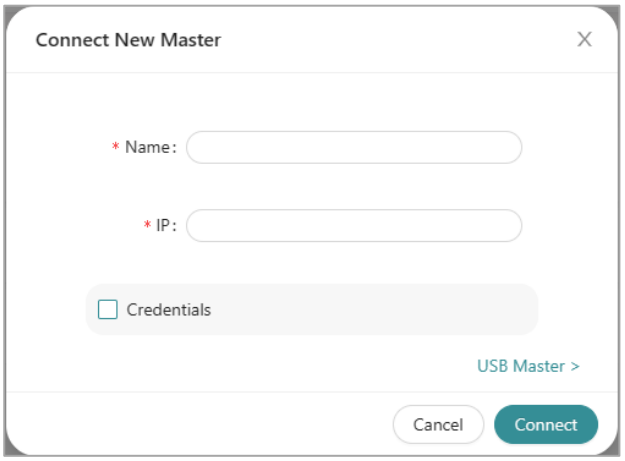


Figure 16: Connect New Master

5. Click **Connect**.

   When the TigoMaster 2TH is connected, its details appear in the table in the **Masters** window, together with a **Green** mark in the **Status** column.

   You can **Disconnect** the TigoMaster 2TH or **Edit/Delete** its details in TigoEngine by selecting it and then clicking the relevant button in the **Actions** column.

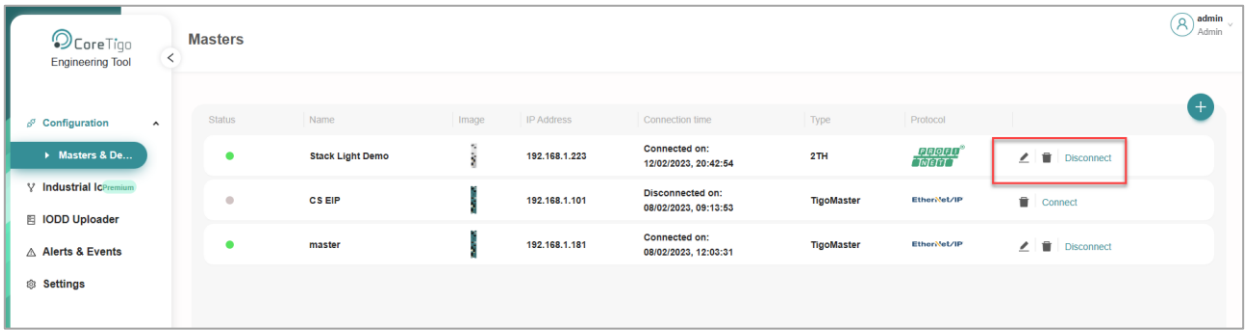


Figure 17: Masters View – Three TigoMasters 2TH Connected

5.4. CoreTigo Web Server

The CoreTigo Web Server enables the user to see information about the TigoMaster 2TH to which the web server is connected (via its IP address), configure the connected TigoMaster 2TH, and scan for unconnected IO-Link wireless devices.

This chapter describes the use of the integrated CoreTigo WirelessWeb Server to access detailed information about the current operating status of the IO-Link Wireless Master device and the connected IO-Link Devices. You also can make settings for device parameterization to influence the device behavior.

5.4.1. Prerequisites

To use the CoreTigo Web Server, the following is required:

- An Internet browser
- A login to the CoreTigo Web Server:
  - To configure TigoMaster 2TH, you need a login with administrator's privileges
  - To view information about TigoMaster 2TH on the web server dashboard, use the default login:

    Username = root
    Password = password
- IP address of the TigoMaster 2TH.

  If the IP address is not yet defined, you can define it using one of the following:
  - The TigoMaster 2TH is provided with a default IP Address 192.168.1.100, and the subnet mask address is 255.255.255.0. See section 6.1.
  - To define the IP address using CoreTigo Web Server see section 6.2.
  - In case the TigoMaster 2TH is in BOOTP/DHCP mode please use the BOOTP tool to configure the IP address.

5.4.2. Functional Overview

The following overview shows you which functions are provided by the CoreTigo Wireless Web Server integrated in the device and via which menu items or tabs of the UI these functions can be accessed.

Table 11: Functional Overview of the CoreTigo Wireless Web Server for IO-Link Devices

Menu	Tab	Description	Section
Dashboard	-	Display of device-specific information	Dashboard
Licenses	-	Display of the used software components	Licenses
IO-Link Wireless Master settings	Channel Selection	WLAN channel list	Channel Selection
	Configuration	Configure parameters of the IO-Link Wireless Master	Configuration
	Scan	Scan for unconnected IO-Link Devices	Scanning and Pairing

Menu	Tab	Description	Section
Wireless port WP01, WP02, WP03 …	(all)	Port-specific information and settings for the wireless IO-Link ports WP01, WP02, WP03 …	Device or port information
	Information	Displays device information on the connected IO-Link Device	Device information
	Status	Displays port status information	Port status
	Settings	Display (and setting) of port parameters.	Port settings
	ISDU	Display of device Index Service Data Units	Device ISDU
		Display of master Index Service Data Units	Master ISDU
Settings	(all)	Device settings	Process data
	Settings	Setting of port parameters (such as port mode, Unique ID, IMA Time, etc.)	Device settings
	Device configuration	Configure parameters for IP connection	Port settings
	Maintenance information	Store maintenance information	IP parameters
	Firmware update	Update the firmware of the device	Maintenance information
	Factory reset	Reset the device to factory settings	Firmware update
	MQTT	Client and connection configuration	Factory settings
User Administration	-	Set up and manage users	MQTT configuration
Sign In / Sign Out	-	User login and logout	

5.4.3. Open the CoreTigo Web Server

1. Make sure that the PC on which you want to access the website of the CoreTigo Wireless Web Server and the device you want to connect to are both on the same EtherNet subnet.
2. Enter the following in the address line of your web browser: http://<IP Address of TigoMaster 2TH>. The TigoMaster 2TH is provided with a default IP Address 192.168.1.100, and the subnet mask address is 255.255.255.0.

The dashboard of the CoreTigo Web Server appears. It displays information about the TigoMaster 2TH, as shown in Figure and Table .

3. Log in.

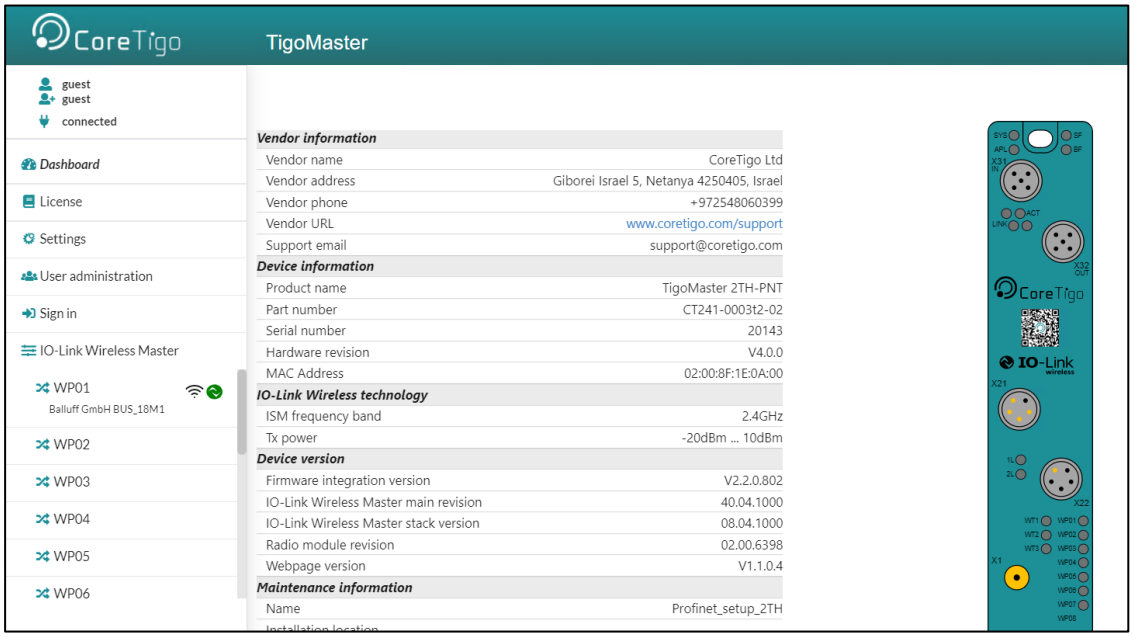


Figure 18: CoreTigo Web Server Dashboard

Table 21: Dashboard Information

Area	Information Displayed / Function
Top left corner	Current connection state and user role
Left column	Navigation area. Icons on errors or operating states may appear here.
Vendor information	Contact details of the device manufacturer
Device information	Identification details of the device
IO-Link Wireless technology	Radio connection specifications
Device version	Hardware and software version numbers
Maintenance information	Installation and service details - includes textual information that the user can specify, such as device name, installation location and date, contact information, description, date of last and next service of the device. These texts can be edited using the **Maintenance information** tab of the **Settings** menu.

5.4.4. Licenses

The Licenses menu item allows you to display the page of the same name.

This displays:

- a list of the licensed software components contained in the product.
- for each licensed software component, a link to the associated license conditions.

5.5. IO-Link Wireless Master Settings

The IO-Link Wireless Master Settings page is where you perform most procedures in the web server. It has the following tabs:

- **Channel selection** tab – here you can select the WLAN channels that you want to configure (for example, WLAN channels 01–04).
- **Configuration** tab – here you can do the following for the selected channels:
  - Configure TigoMaster 2TH parameters, including track transmission power
  - Activate/deactivate track 0, track 1, or track 2

  For further details, see section 5.5.3.
- **Scan** tab – here you can scan for unconnected IO-Link devices. A scan result then shows the found devices.

5.5.1. Channel Selection

1. Select **Master** in the left column of the CoreTigo Wireless Web Server.

   The **Channel Selection** tab appears.

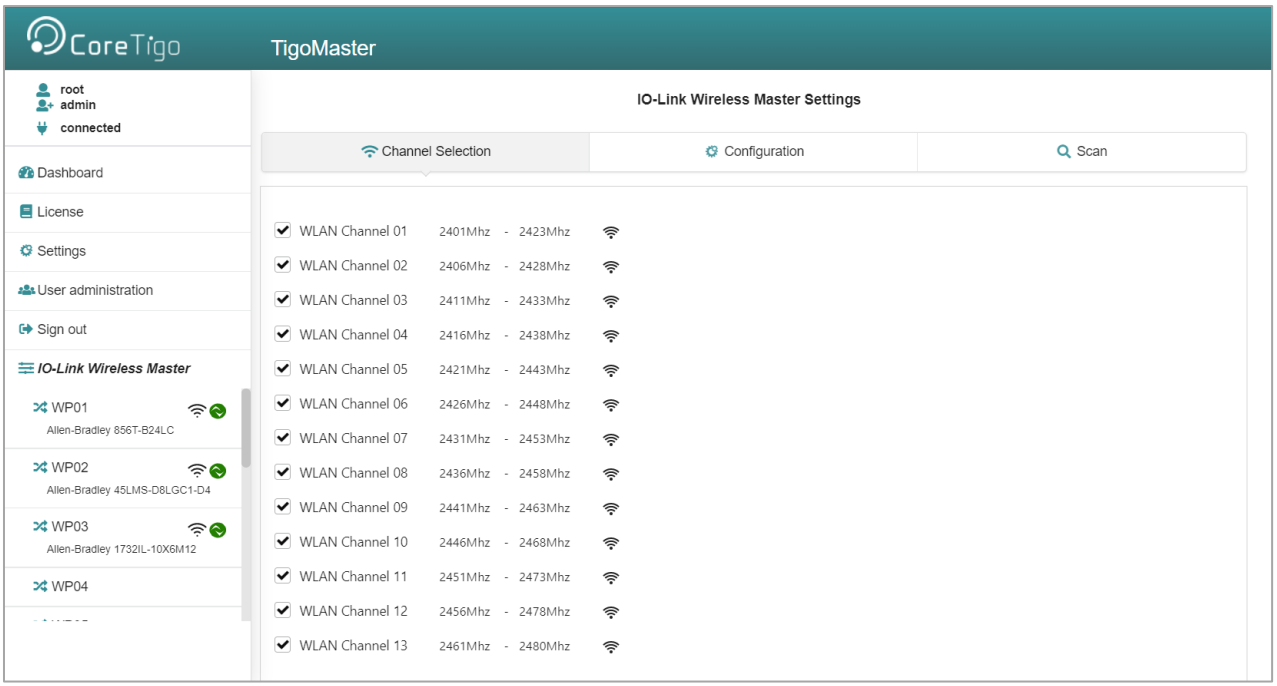


Figure 19: Channel Selection Tab

2. Use the **Channel Selection** tab to select the WLAN channels required for operation.
3. Click **Apply**.

   The selected WLAN channels are configured.

Table 22: WLAN Channels

Parameter	Description	Value/Value Range
WLAN Channel 01 … WLAN Channel 13	List of WLAN channels 01 to 13 on the 2.4 GHz frequency band. The radio symbols indicate whether a channel is activated fully or partially. Hover to indicate the help text. 	• checked • unchecked (default)

5.5.2. Expert Settings

The Expert mode allows a refinement of the transmission frequencies to be used. Here, each individual operating channel can be activated or deactivated. Since the list of operating channels is based on the WLAN channels, there are overlaps. When activating/deactivating the operating channels, these overlaps are automatically taken into consideration.

The complete range of wireless operating channels comprises 80 bitwise coded 1 MHz frequency channels.

- The wireless channels 1 (2401 MHz), 2 (2402 MHz), 79 (2479 MHz), 80 (2480 MHz) are used for network configurations and cannot be configured.
- The wireless channels 3-78 (2403 … 2478 MHz) can be configured to be used or not for IO-Link wireless communication within a Wireless Master. Frequency Hopping is used for transmission on different frequency channels on the 2.4 GHz Band frequency.

Note:
Ranges of wireless operating channels assigned to each of the WLAN channels 01 to 13 overlap each other. In consequence, if a 1 MHz frequency channel option is configured for one WLAN channel, this will have effect on the corresponding 1 MHz frequency channel that is also assigned to a WLAN channel in the neighborhood.

Check **Expert Settings** (at the bottom of the screen).
The following view appears with configuration options of each single MHz frequency.

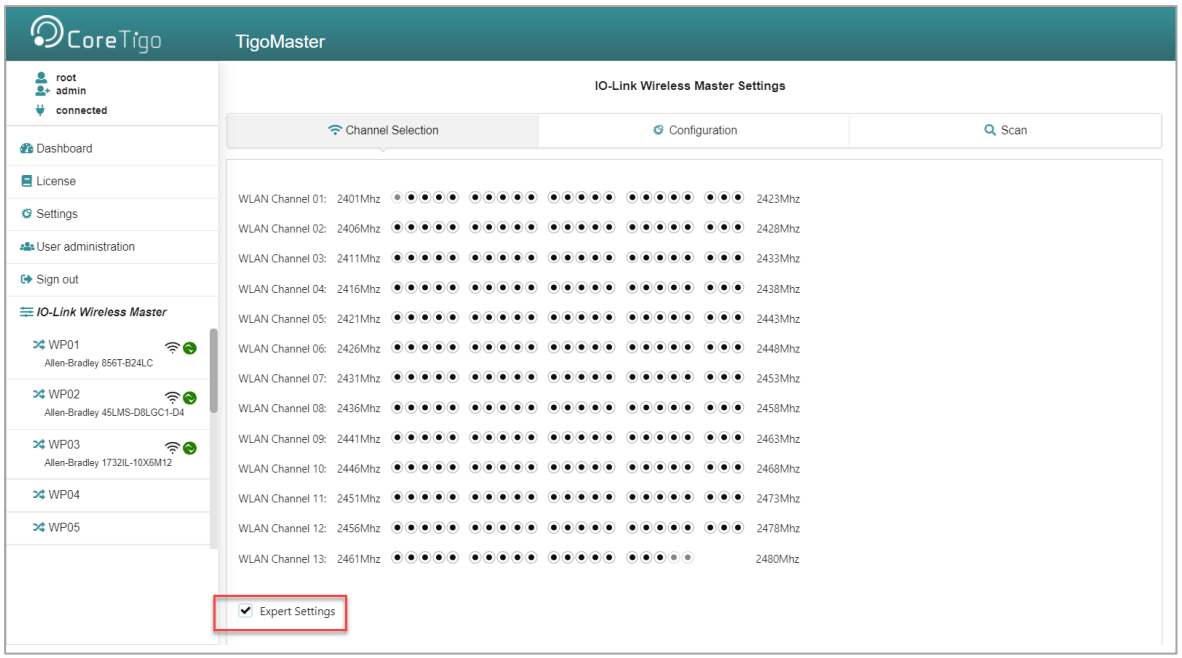


Figure 20: Expert Settings

5.5.3. W-Master Configuration

To open the IO-Link Wireless Master Settings page, click **W-Master** in the explorer bar on the left of the web server and select the **Configuration** tab.

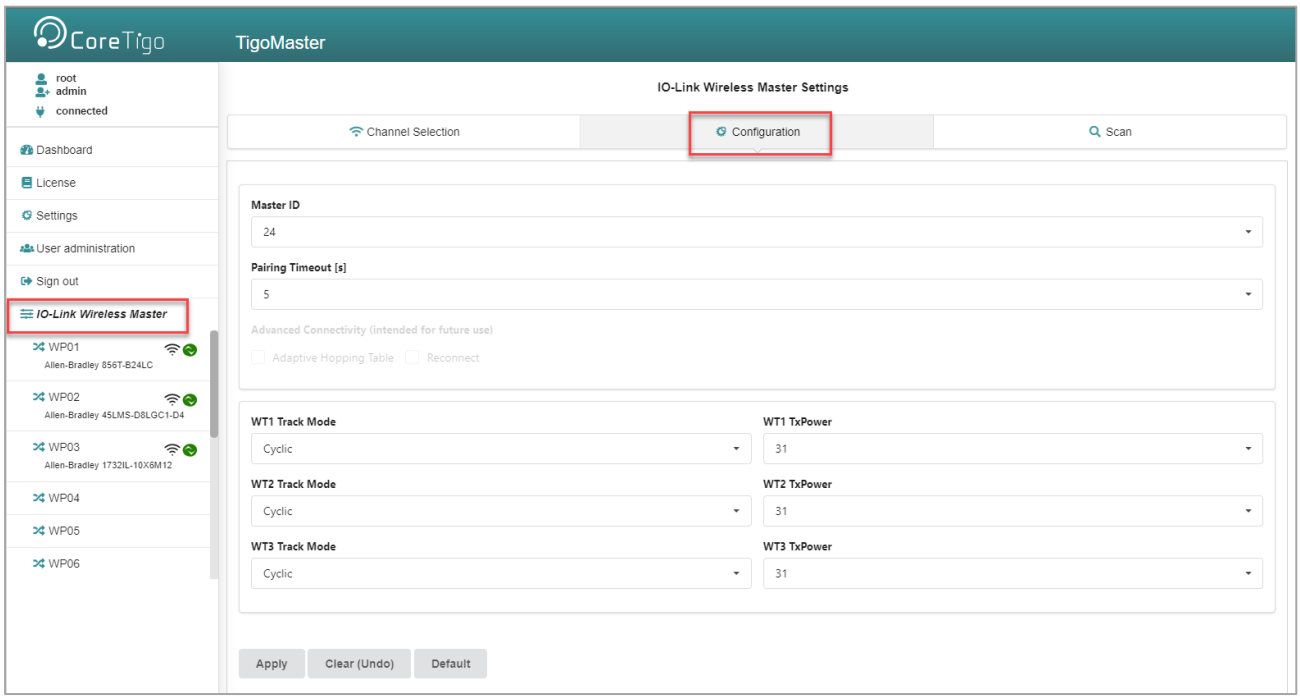


Figure 21: Configuration Tab

In the **Configuration** tab, you can set the parameters detailed in Table .

Table 23: W-Master Advanced Configuration View

Parameter		Description	Value/Value Range
Master ID		W-Master Identifier according to IOLW specification	• 1 … 29 • 0: when not yet configured
Advanced Connectivity	Adaptive Hopping Table	If checked, enhances Frequency Division Multiple Access (FDMA) technology	• checked • unchecked (default)
	Reconnect	If checked, reconnection trials will be performed when connection is lost	• checked (default) • unchecked
Pairing Timeout		Timeout for pairing by button/UID in seconds	• 5 … 60 • 0: when not yet configured
Track Mode		Operating mode of wireless track. Available modes are: • **Stop**: track is inactive • **Cyclic**: track is in cyclic only mode and can't perform service operations • **Service**: track is in service mode, meaning, cyclic mode that can perform service operations like scan/pair • **Roaming** • **Auto** NOTE: Only 1 track can be in Roaming or Service mode.	• Stop (default) • Cyclic • Service • Roaming • Auto
TX Power		Transmission strength. The maximum allowable value for the TX Power parameter is selected by the IO-Link Wireless Master.	1 … 31 (default 31)

1. Make settings for the parameters “Master ID”, “Pairing Timeout”, “Advanced Connectivity”, “WT1 Track Mode … WT3 Track Mode”, and“WT1 TXPower … WT3 TXPower”.
2. Click **Apply**.

   The request appears:
   Applying configuration will restart the device. Are you sure?
3. Click **Yes**.
4. Wait until reset operation is finished and the result is shown:

   The message **Master configured successfully** appears.

5.5.4. Error Handling

When the IO-Link Wireless Master assumes error status, an **Orange** triangle icon appears for the Master in the left column of the CoreTigo Wireless Web Server indicating that the message Master configuration has failed.

For troubleshooting:

- Delete the Master configuration.
- Perform a device reset.

5.5.5. Scan and Pair

5.5.5.1. Scan

1. Select **Master** in the left column of the CoreTigo Wireless Web Server.
2. Open the **Scan** tab.

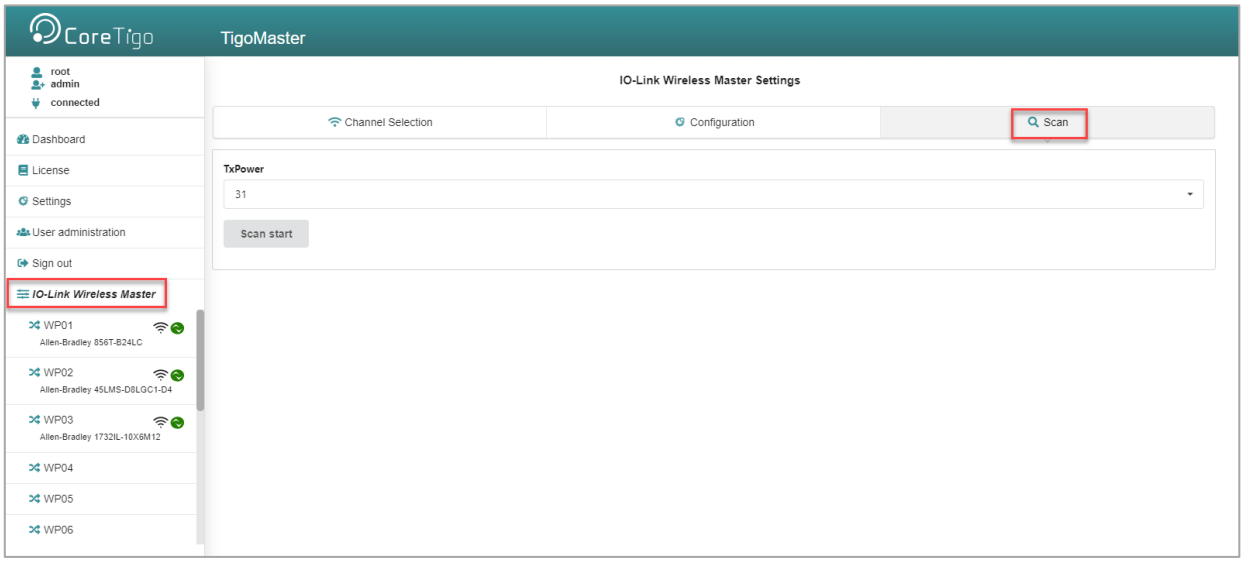


Figure 22: Scan Tab

5. Use the **Scan** tab, to scan for unconnected devices.
6. Select **TxPower**.

   The value range of “TxPower” (Transmission power) is “1 … 31” and the default value is “31”.
7. Click **Scan start**.

   The system searches for unconnected devices.

The scan result is displayed after a few moments.

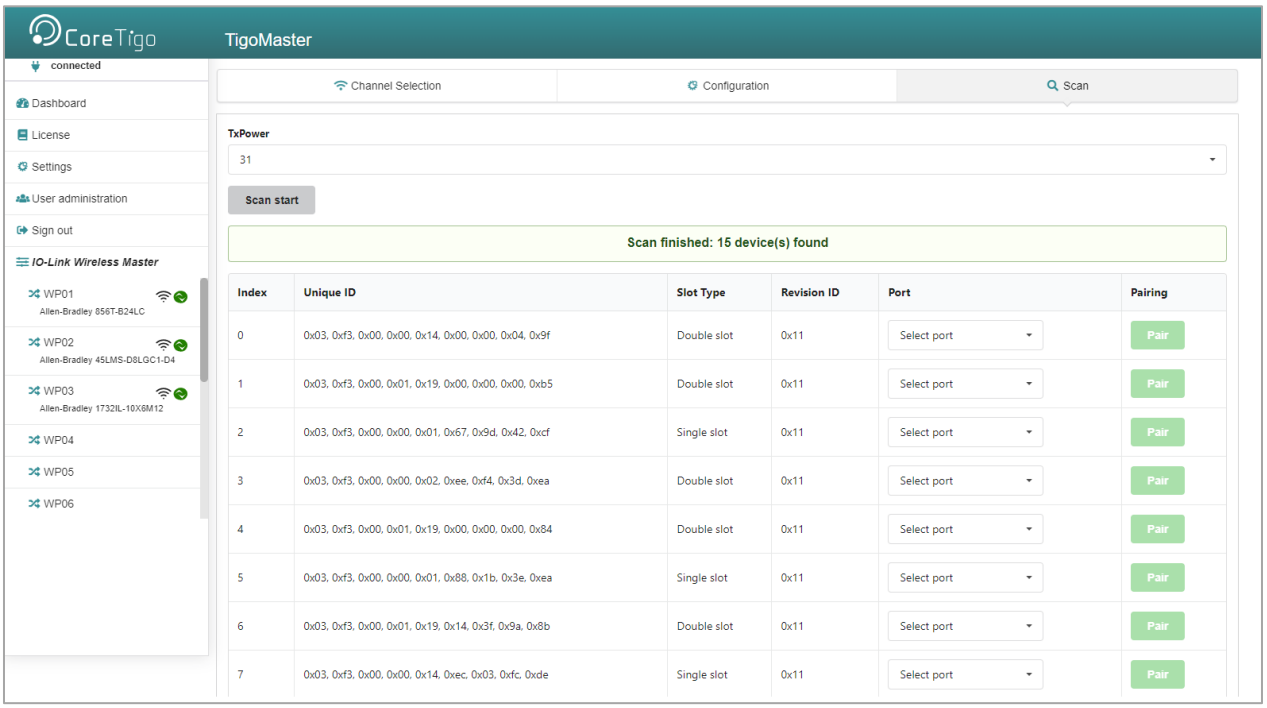


Figure 23: Scan Result

The scan result includes a textual description: **“Scan finished:** [*number of found devices*] **device(s) found**”.

For scan errors the following appears: **“Scan failed HTTP Error** [*error number*]: [*short description of error*]”plus a further message in the upper part of the **Scan** tab.

Table 24: Scan Result/Pairing

Parameter	Description	Value/Value Range
Index	Device index	• 0 … 20
Unique ID	Identification of the found IO-Link Device as unique ID(UUID, 9 Bytes). Copy/note the unique ID. This value is required for portconfiguration.	• 0 … 0xFF
Slot Type	Slot type of the found device	• Single slot (default) • Double slot
Revision ID	Revision ID of the found device This parameter is specified by the found device. It indicates software revision running on the found device.	• 0: No device connected • Others: Software revision running on the found device
Port	ID of wireless IO-Link port to which the IO-Link Device isto be paired. Note: For a device featuring “Double slot” an even portmust be assigned.	• WP01 … WP16

Parameter	Description	Value/Value Range
	Otherwise the error message appears: “Pairing failedHTTP Error 500:NetProxy returned with an error: C0000124”	
Pairing	A pairing service is provided to pair a found IO-Link Device to a wireless IO-Link port of the IO-Link WirelessMaster.	• Pair (**Green**) (default) • Remove (**Red**)

5.5.5.2. Pair / Unpair

For pairing an IO-Link Device to a wireless IO-Link port of the IO-Link Wireless Master device during device commissioning:

3. In the **Scan** tab in the scan result, select the **Port**.
4. Click 

.

   Pairing is performed and **Pair** (**Green**) switches to **Remove** (**Red**).

   The message **Pairing successful** appears.

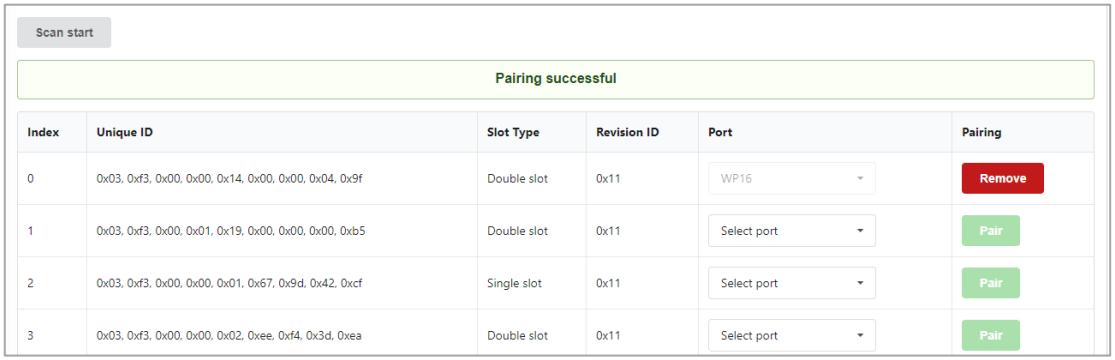
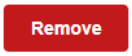


Figure 24: Pairing Successful

5. Change the pairing setting as follows:
   - To unpair an IO-Link Device and a paired wireless IO-Link port, click 

.
   - The message **Unpairing successful** appears.

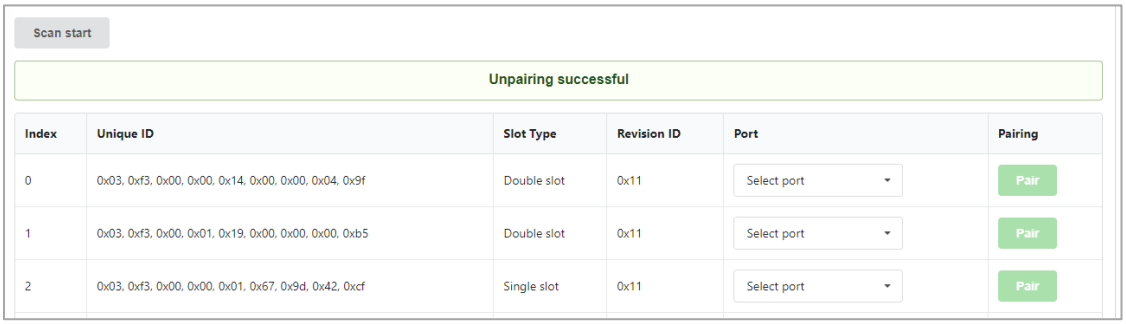


Figure 25: Unpairing Successful

5.6. Device or Port Information

In the port specific tabs **Information, Status, Settings, ISDU**, **Process Data**, device or port information is displayed individually for each of the wireless IO-Link ports of the IO-Link Wireless Master device.

In the **Settings** tab you can make port-specific settings.

Access the tabs as follows:

1. In the left-hand column, click on the wireless IO-Link port **WP01**, **WP02**, **WP03…..**

   The **Information** tab of the corresponding wireless IO-Link port appears.

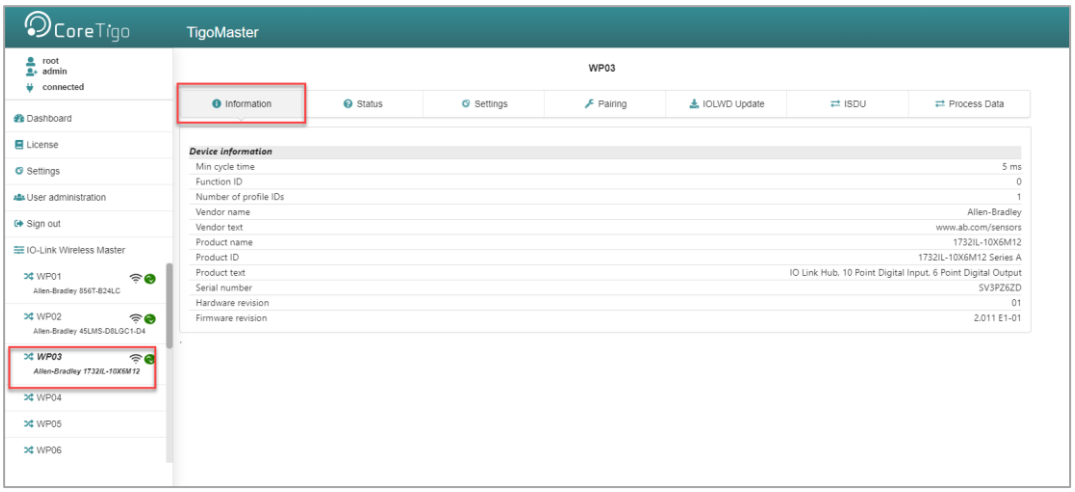


Figure 26: Information Tab

2. To open another tab, click **Status**, **Settings**, **ISDU**, or **Process Data**.

Table 25: Information, Status, Settings, ISDU, Process Data

Tab	Description
Information	Displays some “Device information” of the IO-Link Device (Mincycle time, Function ID, Number of profile IDs, Vendor name, Vendor text, Product name, Product ID, Product text, Serial number, Hardware revision, Firmware revision).
Status	Displays port status information (Port state, Port quality, RevisionID, Master cycle time, Input data length, Output data length, Vendor ID, Device ID, Signal quality). This tab shows current settings.
Settings	Display and setting of port parameters (Port mode, Port cycle time, Validation and backup, Vendor ID, Device ID, Low power device, Max PD segment length, Unique ID, Slot number, Tracknumber, Device TX power, Max retry, Slot type, IMA Time). This tab shows current settings.
ISDU	Display of the Index Service Data Units: • Read/write access to parameters of the connected IO-LinkDevice. • Read/write access to parameters of the IO-Link Wireless Master device.
Process Data	Display of the process data (input/output)

5.6.1. Device Information

The **Information** tab displays some “Device information” of the IO-Link Device connected to a wireless IO-Link port. The official IO-Link SMI layer does not provide this information.

1. In the left column of the CoreTigo Wireless Web Server, select the wireless IO-Link port with the connected IO-Link Device.

   The **Information** tab appears with the device information of the connected device.

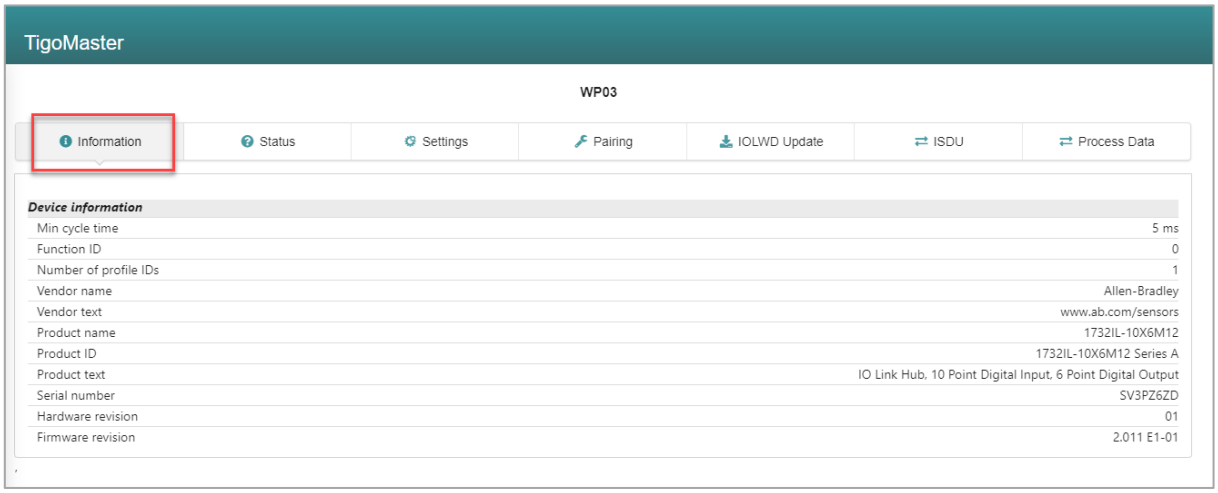


Figure 27: Information Tab – Device Information

Table 26: Information Tab Parameters

Parameter	Description	Value/Value Range
Min cycle time	Minimum cycle duration supported by a Device. This is aperformance feature of the Device and depends on its technology and implementation.	0 … ms
Function ID	Function ID of connected device.	
Number of profile IDs	Provides the number of ProfileIDs contained in the ProfileCharacteristic (index 0x000D) of the connected device. The complete list the ProfileIDs has to be read using common OnRequestData Read mechanism.	
Vendor name	Detailed name of vendor of connected device.	Character string (up to 64 characters)
Vendor text	Additional vendor information of the connected device.	Character string (up to 64 characters)
Product name	Detailed product or type name of the connected device.	Character string (up to 64 characters)
Product ID	Product or type identification of connected device.	Character string (up to 64 characters)
Product text	Description of function or characteristic of connected device.	Character string (up to 64 characters)

Parameter	Description	Value/Value Range
Serial number	Vendor specific serial number of connected device.	Character string (up to 16 characters)
Hardware revision	Revision of hardware of connected device in a vendor specificformat.	Character string (up to 64 characters)
Firmware revision	Revision of firmware in connected device in a vendor specificformat.	Character string (up to 64 characters)

5.6.2. Port Status

1. Select the wireless IO-Link port in the left column of the CoreTigo Wireless Web Server.
2. Open the **Status** tab.

   The current values for the status data of the selected wireless IO-Linkport appear.

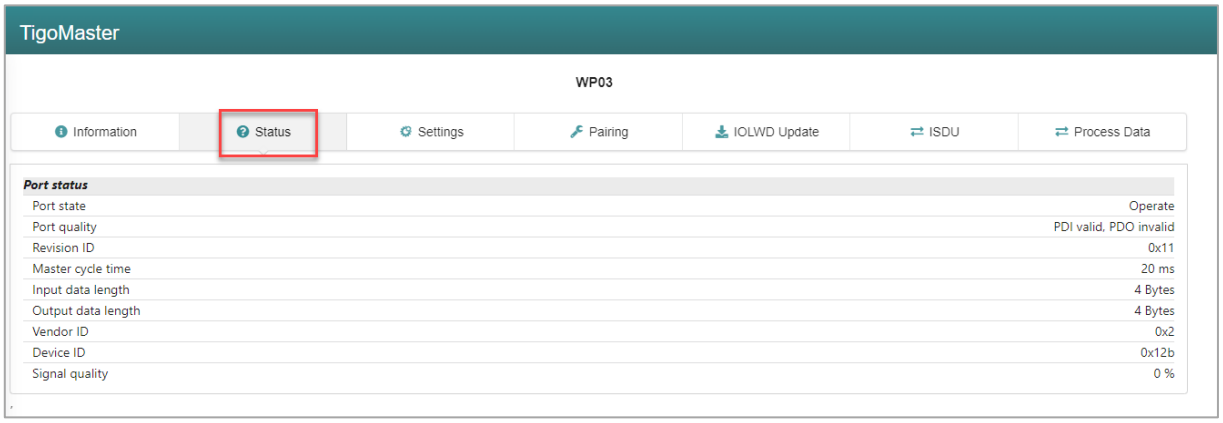


Figure 28: Port Status Tab

Table 27: Port Status Parameters

Parameter	Description	Value/Value Range
Port state	Current port state of wireless IO-Link port Descriptions of the possible values are listed in table.	Pairing success, Pairing timeout, Pairing wrong slot type, Inactive, Port ready, Communication ready, Operate, Communication lost, Revision fault, Compatibility fault, Serial number fault, Process data fault, Cycle time fault
Port quality	Status information of process data. Input process data is valid, Input process data is not valid. Output process data is valid, Output process data is not valid.	PDI valid, PDI invalid, PDO valid, PDO invalid.
Revision ID	Revision ID of the connected device.	0: No device connected Others: Revision ID of connected device

Parameter	Description	Value/Value Range
	This parameter is specified by the connected device.It indicates software revision running on the connected device.	
Master cycle time	Cycle time of communication in Operate mode. The Master cycle time is a Master parameter and sets up the actual cycle time of a particular wirelessIO-Link port. “Free running”: The Minimum Master cycle time is configured, based on the PD Segmentation length,Slot Type and Max Retry configurations.	“Free running”, 5 ms … 315 ms
Input data length	Real input data length of connected device in bytes.	0 … 32
Output data length	Real output data length of connected device in bytes.	0 … 32
Vendor ID	Vendor ID of the connected IO-Link Device	0 … 0xFFFF, Default: 0
Device ID	Device ID of the connected IO-Link Device	0 … 0xFFFFFF, Default: 0
Signal quality	Signal quality gives a relative indication on strength of radio connection between IO-Link Wireless Masterdevice and the connected IO-Link Device. The indicated value does not change during runtime.	0% … 100%

The **Status** tab with the port status data provides responses to the questions:

- What is the current port state of the wireless IO-Link port?
- Is the process data valid for input or output? Further port status values are displayed.

Table 28: Possible Values for the Port State

Value	Description
Pairing success	Device is connected to the port via radio and there is wireless communication with the connected device.
Pairing timeout	A timeout has occurred for the connection from this port to the device.
Pairing wrong slottype	A wrong slot type is used for the connection from this port to the device.
Inactive	The port is inactive.
Port ready	The port is ready.
Communication ready	The device is ready for communication.
Operate	The device is in communication.
Communication lost	The communication to the device is broken down.
Revision fault	An error was found during revision check.

Value	Description
Compatibility fault	An error was found during compatibility check.
Serial number fault	An error was found during serial number check.
Process data fault	An error was found during process data check.
Cycle time fault	The configured cycle time does not match the connected device.

5.6.3. Device ISDU

The **ISDU** tab allows read and write access to the IO-Link Device connected to a wireless IO-Link port by means of Index and Subindex. The ISDU message format is used for this.

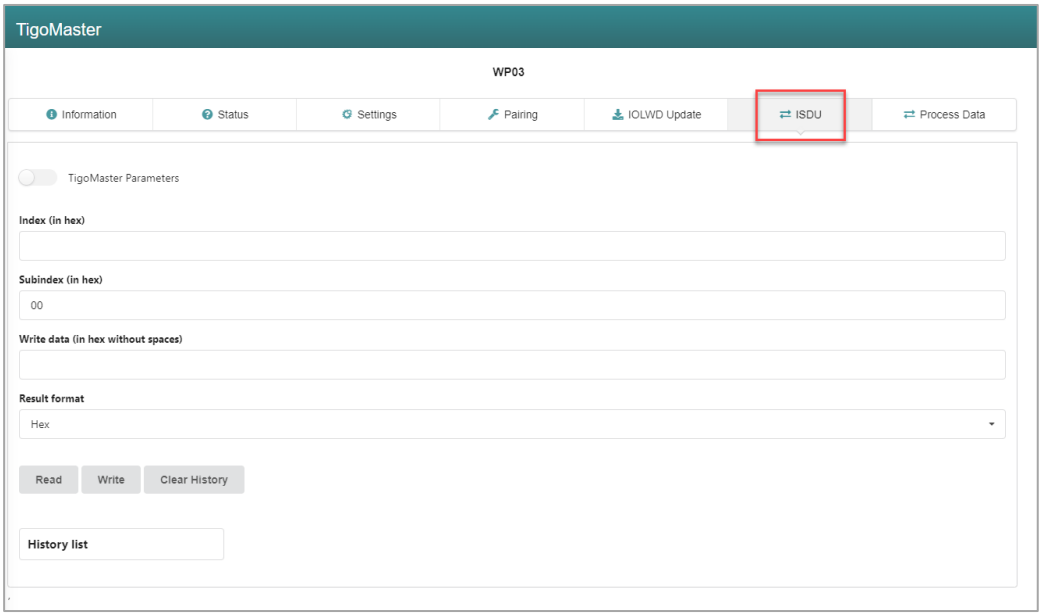


Figure 29: Display of On Request Data, Read/Write IO-Link Device Parameters

Note:
For the meaning of the Index and Subindex values, refer to the documentation of the connected IO-Link Device.
For a description of the ISDU message format, refer to the IO-Link specification.

5.6.3.1. Required Rights

Changes to settings require operator or admin rights. If these are not available, the **ISDU** tab is grayed out and the displayed values cannot be edited.

5.6.3.2. Access to IO-Link Device

To access the data of an IO-Link Device connected to the selected wireless IO-Link port via Index and Subindex (ISDU message format):

1. Select the wireless IO-Link port to which the IO-Link Device is connected in the menu on the left.
2. Open the **ISDU** tab.

   The **ISDU** tab is displayed.

5.6.3.3. Read Access to IO-Link Device

To read data from the connected IO-Link Device, proceed as follows:

1. Enter the **Index** for ISDU access as a hexadecimal value in the **Index** entry field.
2. Enter the **Subindex** for ISDU access as a hexadecimal value in the **Subindex** entry field.

   The default value here is `00`.

   In case of input errors, an error message appears.
3. Click on **Read**.

   The read access is executed.

   An entry with a time stamp is written tothe history at the bottom of the ISDU tab.

   If the execution was successful, the text **Read ok:** is displayed and the result is displayed in the history. The entries in the history then have the following structure:

   Time - Index:Subindex - Read ok: <Result>

Figure 30: History List

If the execution was not successful, an error message with error codes of the IO-Link Wireless Master and IO-Link Device is displayed in the history.

In this case, the entries in the history have the following structure:

Time - Index:Subindex - Read failed: IOLMErrorCode(<error code of the IO-Link master>): IOLDErrorCode(<error code of the IO-Link Device>)

Note:
Information on the meaning of the error codes of the IO-Link master (IOLMErrorCode) and device (IOLDErrorCode) can be found in the IO-Link specification.

The following applies in both cases:

- The **Time** is displayed in the format **HH:MM:SS**
- **Index** and **Subindex** are displayed in hexadecimal format.

5.6.3.4. Write Access to the IO-Link Device

To write data to the connected IO-Link Device, proceed as follows:

1. Enter the **Index** of the connected IO-Link Device that you want to access as a hexadecimal value in the **Index** entry field.
2. Enter the **Subindex** of the connected IO-Link Device that you want to access as a hexadecimal value in the **Subindex** entry field. The default value here is `00`.

   In case of input errors, an error message appears.
3. Enter the data to be written (in hexadecimal, without spaces, e.g.,0102030405) in the **Write data** entry field.
4. Click on **Write**.

   The write access is performed.

   If the execution was successful, the text **Write ok:** is displayed and the result is displayed in the history. The entries in the history then have the followingstructure:

   Time - Index:Subindex - Write ok: <Result>

   If the execution was not successful, an error message with error codes of the IO-Link Wireless Master and IO-Link Device is displayed in the history.

   The entries in the history then have the following structure:

   Time - Index:Subindex - Write failed: IOLMErrorCode(<error code of the IO-Link master>): IOLDErrorCode(<error code of the IO-Link Device>)

5.6.3.5. Delete the History of Read and Write Accesses

To clear the logged history of read and write accesses: Click **Clear history**.

The history of read and write accesses is deleted.

5.6.4. Master ISDU

The **ISDU** tab with the option **Tigo Master Parameters** allows read and write access to the IO-Link Wireless Master device, by means of PortId and ArgBlockId. The ISDU message format is used for this.

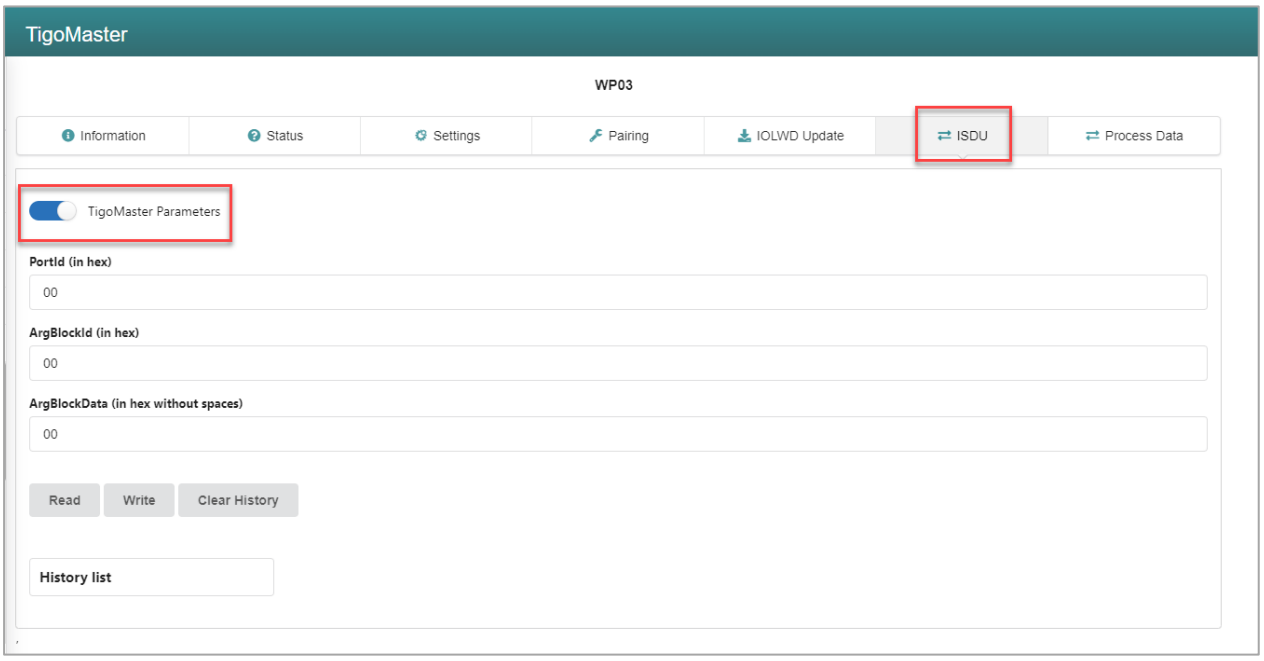


Figure 31: Display of the ISDU, Read/Write IO-Link Wireless Master Parameters

5.6.4.1. Required Rights

Changes to settings require operator or admin rights. If these are not available, the ISDU tab is grayed out and the displayed values cannot be edited.

5.6.4.2. Access to IO-Link Wireless Master

To access the data of the IO-Link Wireless Master via PortId andArgBlockId (ISDU message format):

1. In the menu on the left, select the wireless IO-Link port of the IO-LinkWireless Master to which an IO-Link Device is connected.
2. Open the **ISDU** tab.

   The ISDU tab is displayed.
3. Enable **Tigo Master Parameters**.

   The **Tigo Master Parameters** tab variant is displayed.

5.6.4.3. Read Access to IO-Link Wireless Master

To read data from the IO-Link Wireless Master, proceed as follows:

1. Enter the **PortId** of the IO-Link Wireless Master that you want to access as a hexadecimal value in the **PortId** entry field.
2. Enter the **ArgBlockId** of the IO-Link Wireless Master that you want to access as a hexadecimal value in the **ArgBlockId** entry field. The default value here is `00`.

   In case of input errors, an error message appears.
3. Click on **Read**.

   The read access is executed. An entry with a time stamp is written to the history at the bottom of the **ISDU** tab.

If the execution was successful, the text **Read ok:** is displayed and the result is displayed in the history. The entries in the history then have the following structure:

Time - PortId:ArgBlockId - Read ok: <Result>

If the execution was not successful, an error message with error codes of the IO-Link Wireless Master and IO-Link Device is displayed in the history.

In this case, the entries in the history have the following structure:

Time - PortId:ArgBlockId - Read failed: IOLMErrorCode(<error code of the IO-Link master>): IOLDErrorCode(<error code of the IO-Link Device>)

Note:
Information on the meaning of the error codes of the IO-Link master (IOLMErrorCode) and device (IOLDErrorCode) can be found in the IO-Link specification.

The following applies in both cases:

- The **Time** is displayed in the format **HH:MM:SS**
- **PortId** and **ArgBlockId** are displayed in hexadecimal format.

5.6.4.4. Write Access to IO-Link Wireless Master

To write data to the IO-Link Wireless Master, proceed as follows:

1. Enter the **PortId** of the IO-Link Wireless Master that you want to access as a hexadecimal value in the **PortId** entry field.
2. Enter the **ArgBlockId** of the connected IO-Link Device that you want to access as a hexadecimal value in the **ArgBlockId** entry field. The default value here is `00`.

   In case of input errors, an error message appears.
3. Enter the data to be written (in hexadecimal, without spaces, e.g.,0102030405) in the **ArgBlockData** entry field.

   Write example: PortId = 01, ArgBlockId = B090, ArgBlockData = 01020304
4. Click on **Write**.

   The write access is performed.

   If the execution was successful, the text **Write ok:** is displayed and the result is displayed in the history. The entries in the history then have the followingstructure:

   Time - PortId:ArgBlockId - Write ok: <Result>

   If the execution was not successful, an error message with error codes of the IO-Link Wireless Master and IO-Link Device is displayed in the history.

   The entries in the history then have the following structure:

   Time - PortId:ArgBlockId:Data - Write failed: IOLMErrorCode(<error code of the IO-Link master>): IOLDErrorCode(<error code of the IO-Link Device>)

5.6.4.5. Delete the History of Read and Write Accesses

To clear the logged history of read and write accesses: Click **Clear history**.

The history of read and write accesses is deleted.

5.6.5. Process Data

You can display the process data belonging to a specific wireless IO-Link port using the **Process Data** tab.

To display the process data for a port:

1. Select the wireless IO-Link port in the left column of the CoreTigo Wireless Web Server.
2. Open the **Process Data** tab.

   The current values of process data configured for input or output aredisplayed in hexadecimal format under input or output.

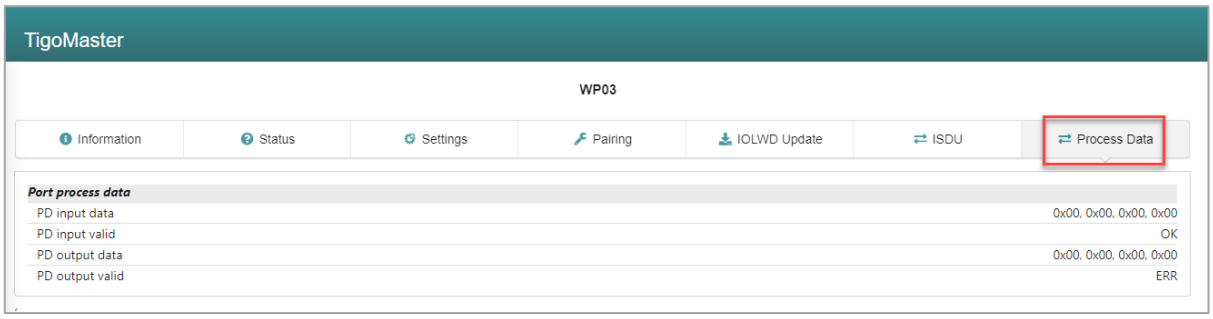


Figure 32: Display of the Process Data

The **Process Data** tab shows the process data input and output values from and to a connected IO-Link Device.

Table 29: Process Data Parameters

Parameter	Description
PD input data	“Process Data” input data to the connected IO-Link Devices.
PD input valid	Binary coded Port Qualifier for Input.
PD output data	“Process Data” output data from the connected IO-Link Devices.
PD output valid	Validation information for process data output. If **Output Enable** flag is set, data will be valid.

If no process data has been configured for a data direction (input or output), the corresponding field remains empty.

5.7. Device Settings

Using the CoreTigo Wireless Web Server, you can make the several settings on the device. Open the panes via the left column of the CoreTigo Wireless Web Server.

1. Select the wireless IO-Link port (**WP01**, **WP02**, **WP03** ...) and open the **Settings** tab to make the port settings.

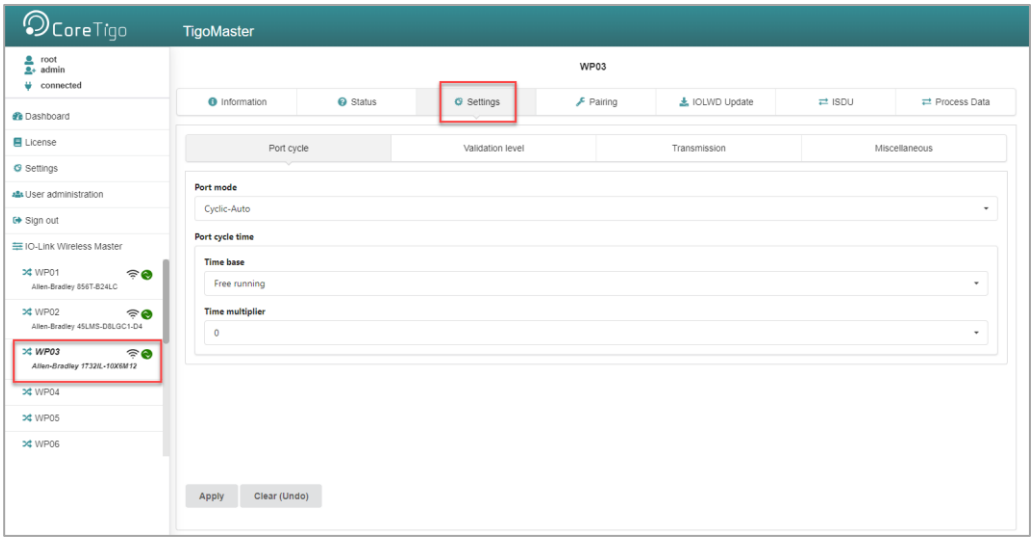


Figure 33: Settings Tab

2. Select **Settings** in the left column and open the corresponding tab:
   - Device information (with menu on the Configure IP parameters)
   - Maintenance information
   - Firmware update
   - Resetting the device to factory settings
   - MQTT

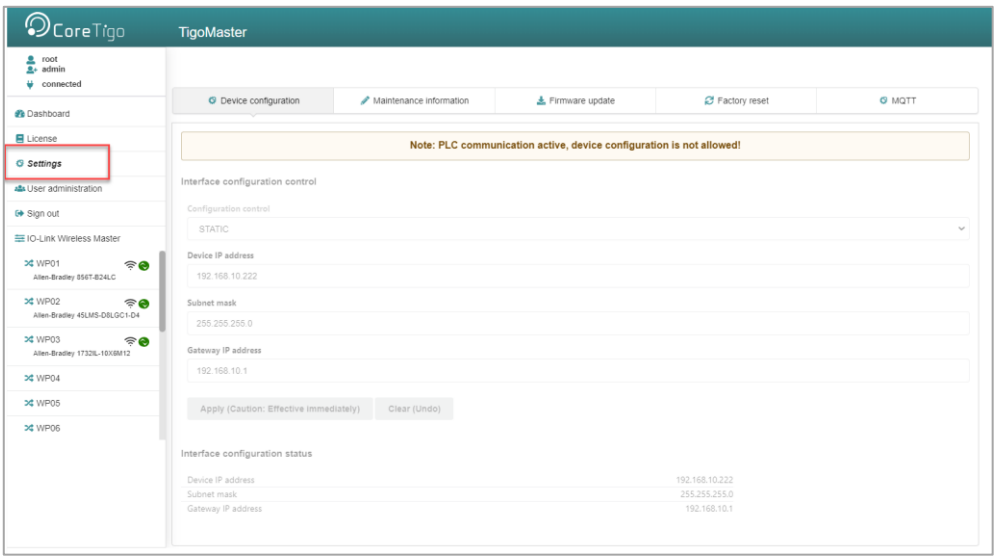


Figure 34: Device Configuration Subtab

3. Select **Sign In/Sign Out** or **User Administration** to access the Register, log off and manage users.

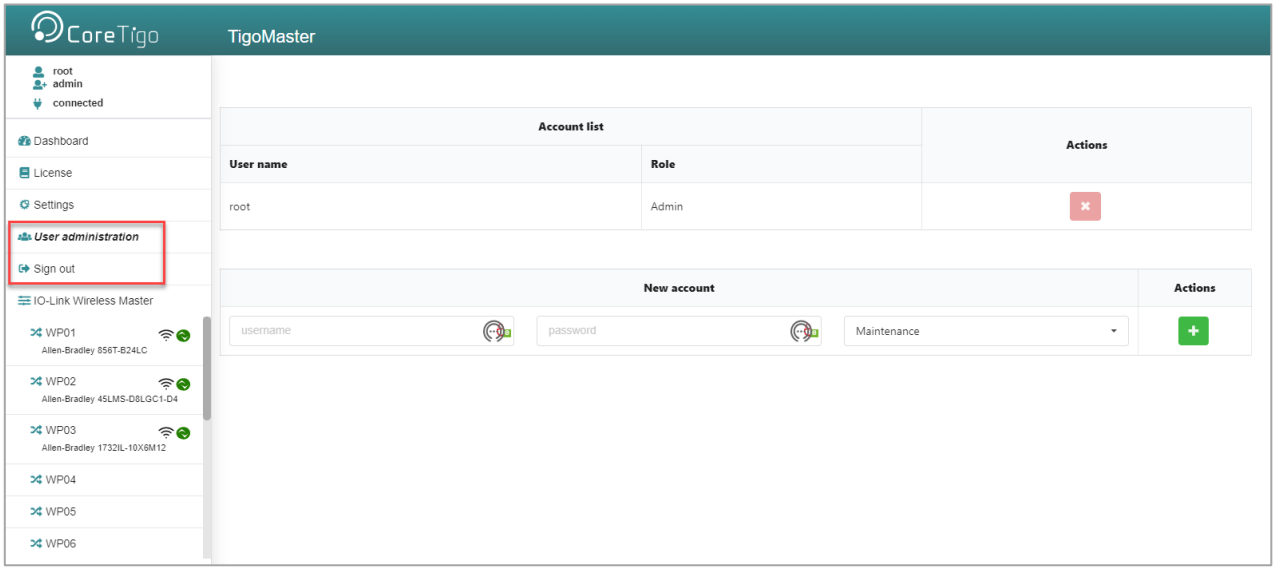


Figure 35: User Administration

5.7.1. Port Settings

Use the **Settings** tab to view and change the port settings individually.

1. Select the desired wireless port (WP01, WP02, WP03, ...) in the left column of the CoreTigo Wireless Web Server.
2. Open the **Settings** tab with its subtabs.

   The **Port Cycle** subtab appears by default.

5.7.1.1. Settings > Port Cycle

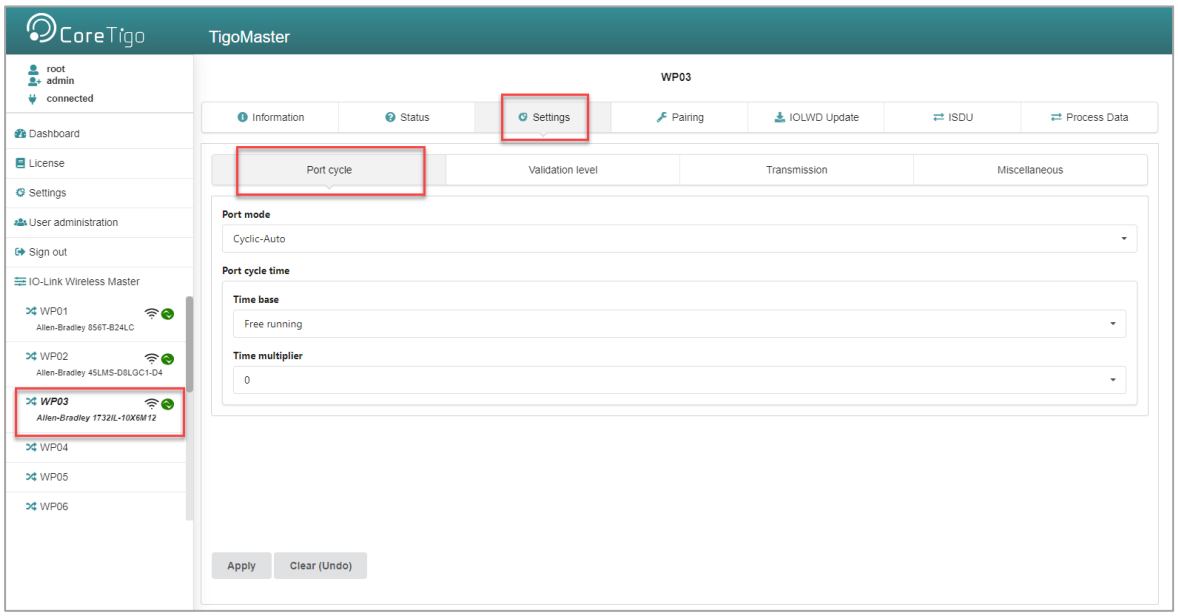


Figure 36: Settings Tab, Port Cycle Subtab

Table 30: Settings in Port Configuration for IO-Link Device, Port Cycle Subtab

Parameter	Description	Value/Value Range
Port mode	Operating mode of IO-Link port • Deactivated: The port is inactive, Input and Output Process Datais 0. • Cyclic • Roaming	• Deactivated (default) • Cyclic • Roaming
	Port cycle time expected by the SMI client The expected cycle time of the port is set depending on theselected operating parameters.	
Port cycle time	Time base: Used time base for the calculation of the port cycletime.	Free running, 5 ms
	Time multiplier: Used factor for the calculation of the port cycletime.	0 … 63

* Values are in hexadecimal

3. Configure port operating mode **Port mode** by selecting the corresponding option.
4. Configure the “Port cycle time”.

The parameter “Port cycle time” sets up the cycle time of a W-Port of theW-Master.
The cycle time is encoded using "Time base" (bits 6+7) and "Multiplier" (bits 0-5) values, as shown in the following table.

Table 31: Calculation of the Port Cycle Time of the IO-Link Wireless Master

Range of Values	Time Base (Bits 7+6)	Multiplier (Bits 5-0)	Resulting Cycle Time
0	00	0	Free-running mode Note: If the free-running mode is chosen with a time base of 0, the W- Master stack will automatically configure the Master cycle time to be theMinimum Master cycle time based on the PD Segmentation length, SlotType, and Max Retry configurations.
1 … 64	00	1 … 63	
65 … 127	01: 5ms	1 … 63 as multiplier	5 ... 315 ms (Time Base * Multiplier) Note: For W-Devices and W-Bridges the minimum possible transmissiontime is 5 ms.
128 … 255	10 ...11: reserved	1 … 63	Reserved, do not use

5. Select the **Time base** and the **Time multiplier** for the “Port cycle time”calculation.

   The result is indicated as value or text in brackets, e. g. **Port cycle time (Free running).**

5.7.1.2. Settings > Validation level

1. Open the **Validation level** subtab.

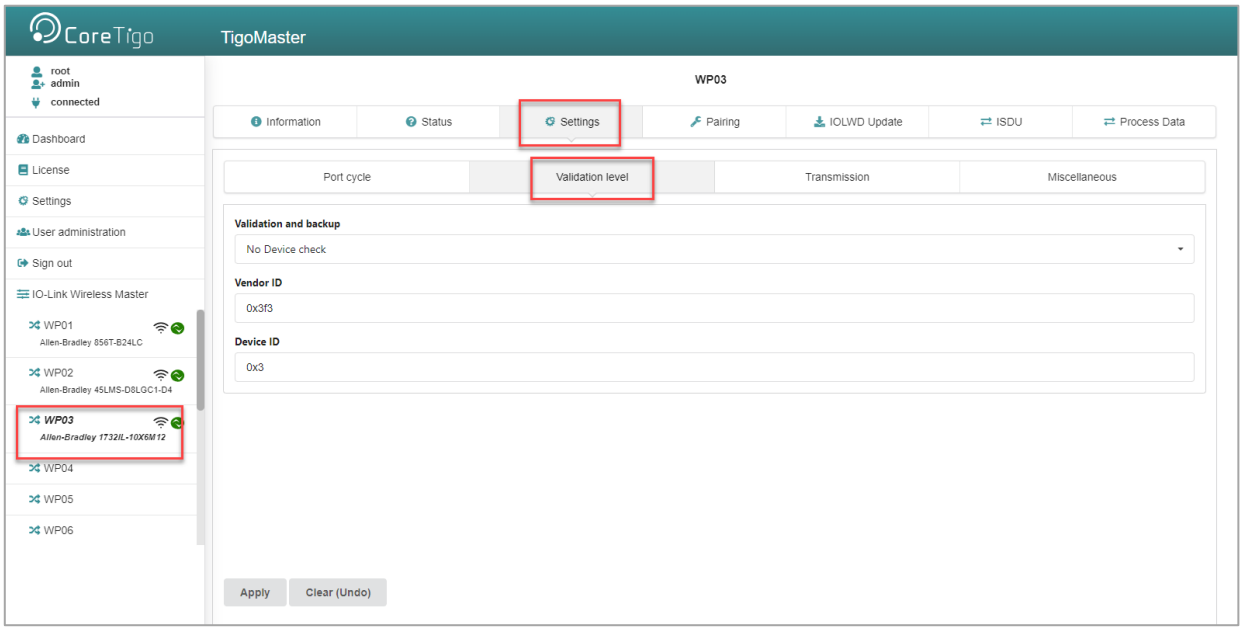


Figure 37: Settings Tab, Validation Level Subtab

2. Under **Validation and backup**, configure possible values for the inspection level to be performed by the device and the Backup/Restore behavior.
3. If necessary, set the expected port parameters VendorID and DeviceID.

Table 32: Settings in Port Configuration for IO-Link Device, Validation Level Subtab

Parameter	Description	Value/Value Range
Validation and backup	The table below contains descriptions for the possible values for the inspection level to be performed by the device and the Backup/Restore behavior:	Default: No device check
Vendor ID*	Expected Vendor ID of connected device. This information is required to check the device for type compatibility.	0 … 0xFFFF, Default: 0
Device ID*	Expected Device ID of connected device. This information is required to check the device for type compatibility.	1 … 0xFFFFFF, Default: 0xFFFFF

* Values are in hexadecimal

Table 33: Validation and Backup, Possible Values

Value	Description
No device check	There is no device check for validation or backup of connected IO-Link Devices
Type compare* No Backup/Restore	A device check is performed for validation of connected IO-Link Devices to the specifieddevice type, without backup/restore.
Type compare* Restore only	A device check is performed for validation or restore of connected IO-Link Devices to thespecified device type, without backup.

Value	Description
Type compare* Backup and Restore	A device check is performed for validation or backup/restore of connected IO-Link Devices tothe specified device type.
*Type compare means compare DeviceID and VendorID from the configuration object with the real device values.	

5.7.1.3. Settings > Transmission

1. Open the **Transmission** subtab.

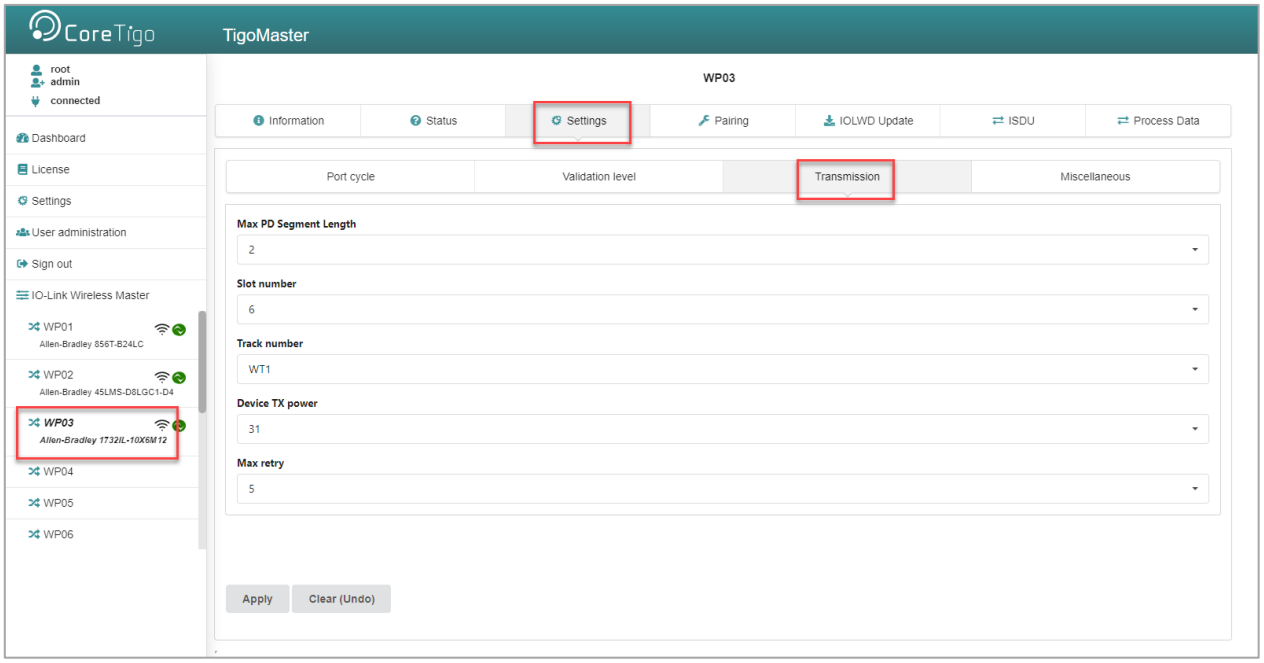


Figure 38: Settings Tab, Transmission Subtab

2. If necessary, set the expected port parameters Max PD Segment Length, Slot number, Track number, Device TX power or Max retry.

Table 34: Settings in Port Configuration for IO-Link Device, Transmission Subtab

Parameter	Description	Value/Value Range
Max PD Segment Length	This parameter contains the maximum segment length of the PDOut data to the message handler to distribute PDOut datawithin multiple wireless cycles. The maximum value depends by the actual transmission capacityof the used IO-Link Device.	1 … 32 Byte, Default: 2
Slot number	Wireless slot number to be used for the port	0 … 7, Default: 0
Track number	Wireless track number to be used for the port	0, 1, 2, Default: 0
Device TX power	This parameter contains the transmit power level of the W-Device	1 ... 31, Default: 31

Parameter	Description	Value/Value Range
Max retry	Maximum number of retries for a transmission in OPERATE mode“Unknown” is indicated if there is no value available.	2 … 31, Default: 8

* Values are in hexadecimal

5.7.1.4. Settings > Miscellaneous

1. Open the **Miscellaneous** subtab.

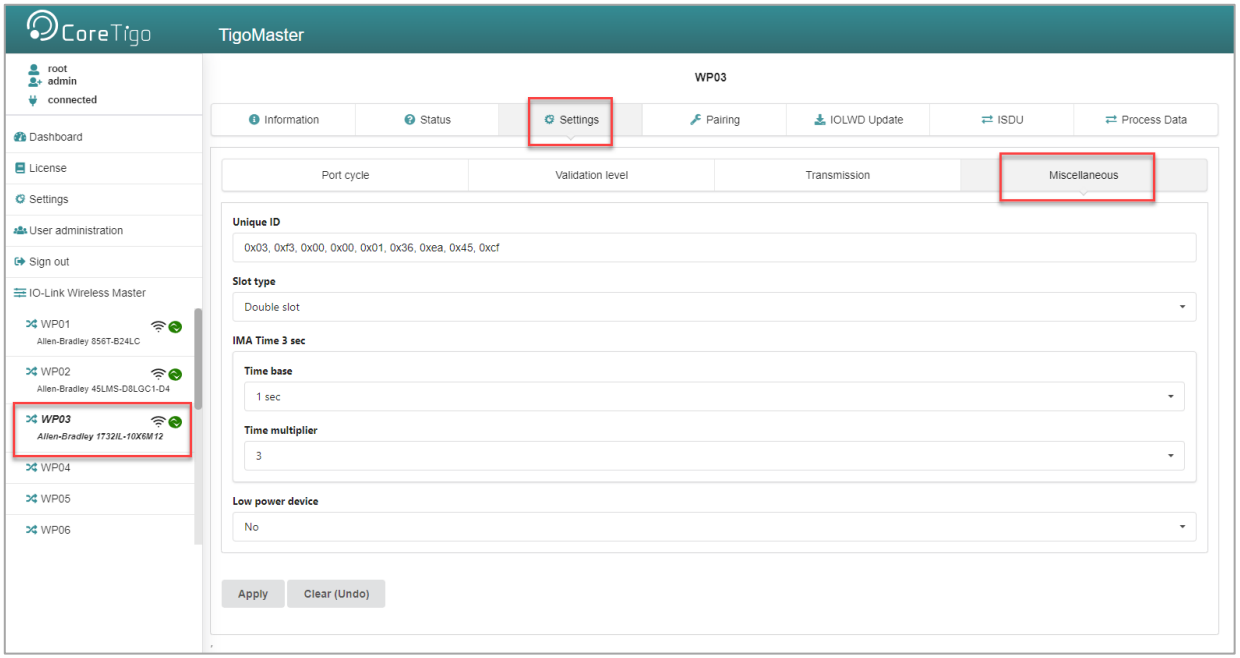


Figure 39: Settings Tab, Miscellaneous Subtab

2. To configure the Unique ID, use the Unique ID (UUID) from the scan result.
3. If necessary, set the expected port parameters Slot type or Low power device.
4. Configure the “IMA Time” (I-Am-Alive time).

Table 35: Settings in Port Configuration for IO-Link Device, Miscellaneous Subtab

Parameter	Description	Value/Value Range
Unique ID*	Unique ID of the IO-Link Device (9 Bytes. Use the Unique ID (UUID) from the scan result.	0 … 0xFF, Default: 0
Slot type	Slot type of the found device. Use the slot type from the scan result. Note: For a device featuring “Double slot” an even number must beassigned as value for the slot.	Single slot, Double slot, Default: Single slot
IMA Time 3 sec (*calculated time*)	Requested I-Am-Alive time for the OPERATE mode The I-Am-Alive time is calculated by multiplying the “time base”with the “time multiplier”.	1.664 ... 10 min (for highervalues an error message appears), Default: 3 sec
	Time base: Used time base for the calculation of the I-Am-Alivetime.	1.664 ms, 5 ms, 1 sec, 1 min

Parameter	Description	Value/Value Range
	Time multiplier: Used factor for the calculation of the I-Am-Alivetime.	1 … 255
Low power device	Is the connected IO-Link Device a low power device or not.	No, Yes, Default: No

* Values are in hexadecimal

The parameter “I-Am-Alive time” serves for W-Master and W-Device communication control if no other messages are transmitted. The W-Device has to send an “I-Am-Alive” messages to the W-Master before timeout, otherwise an error is reported, e.g. to start failsafe functionalities in the application.

The “I-Am-Alive time” is calculated by multiplying the "Time base" with the "Multiplier".

The Wireless Master verifies the calculated “I-Am-Alive time” with the following limits:

- “Minimum I-Am-Alive time” = W-Sub-cycle duration [ms] * (MaxRetry +1)

  If the calculated “I-Am-Alive time” is less than the “Minimum I-Am-Alivetime”, the Wireless Master uses the “Minimum I-Am-Alive time” as resulting “I-Am-Alive time”.
- Maximum I-Am-Alive time = 10 minutes

  If the calculated “I-Am-Alive time” is greater than the “Maximum I-Am- Alive time”, the error message **Port configuration failed HTTP Error 500: NetProxy returned with an error: C0000124** appears.

5. Select the **Time base** and the **Time multiplier** for the “IMA Time” calculation in order to avoid exceeding the maximum allowed value.

   The result is indicated as value in brackets.
6. Click **Apply**.

   Your changes now take effect.
   The message **Port configured successfully** appears and a **Green** tick appears for the selected port in the left column of the CoreTigo Wireless Web Server, indicating that a connection from an IO-Link Device to this wireless IO-Link port has been established, and that the IO-Link Device is in “operate” state.

Note:
The **Green** tick icon disappears if the IO-Link Wireless Master changes to an error state but the device connection is still established and in "connected" state (shown on top left corner of the CoreTigo Wireless Web Server).

If the device connection drops and "disconnected" state is shown, the **Green** tick icon is still visible and reflects the latest status obtained from the device.

5.7.2. IP Parameters

1. Select **Settings** in the left column of the CoreTigo Wireless WebServer.

   The **Device configuration** tab is displayed.

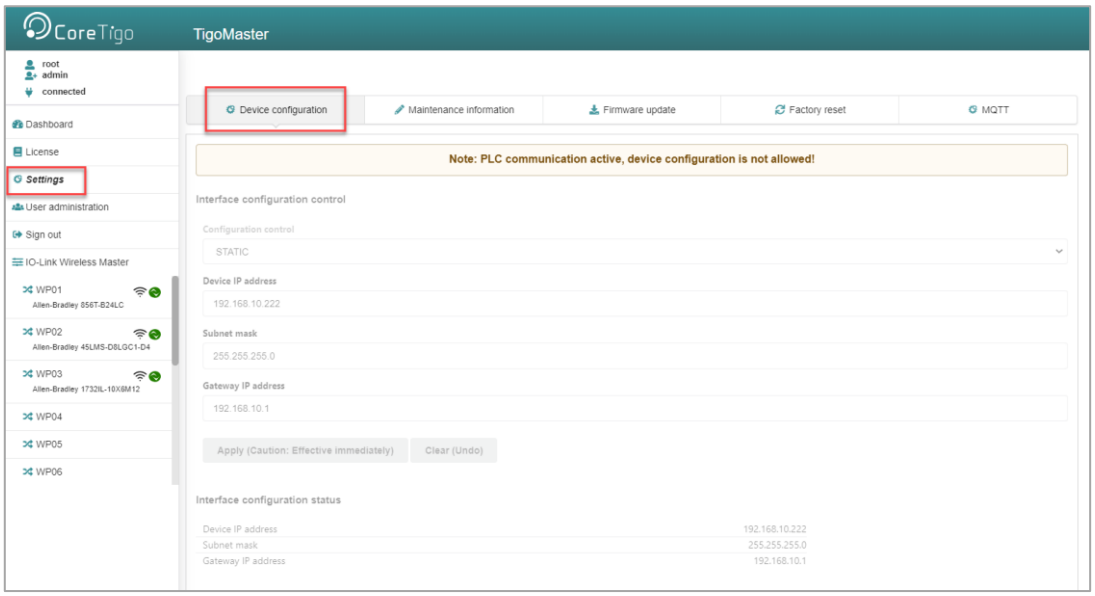


Figure 40: Device Configuration Tab

The EtherNet/IP Master configures the IP address of the device. Therefore, no manual configuration of the IP address is required for EtherNet/IP devices.

5.7.3. Maintenance Information

The **Maintenance information** tab is used to store maintenance information such as device name, installation location and date, contact information, a description text, or the date of the last and next service on the device.

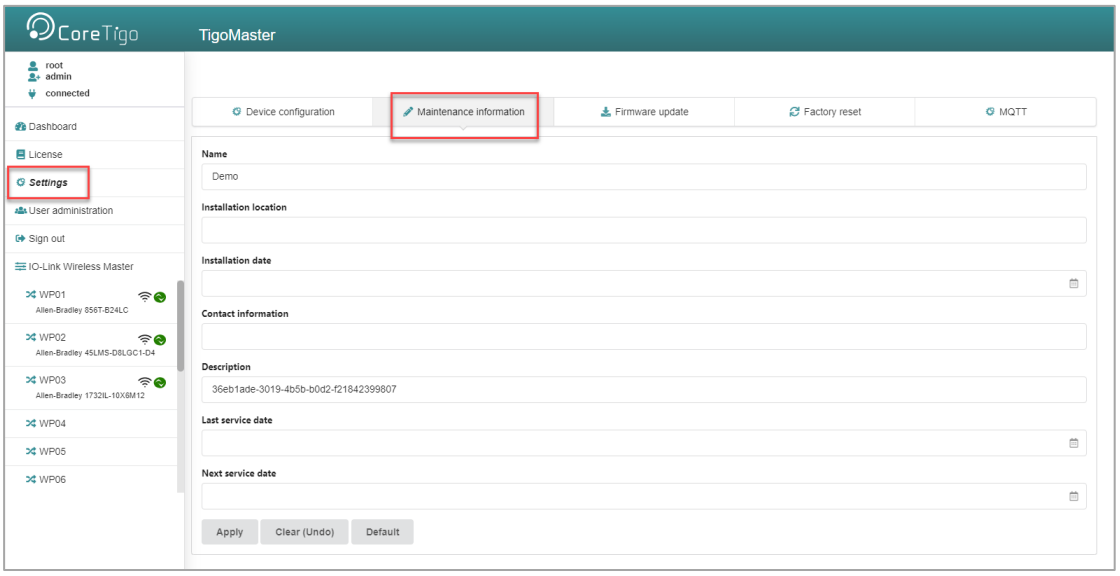


Figure 41: Maintenance Information Tab

Changes to settings require operator or admin rights. If these are not available, the tab is grayed out and cannot be edited.

Table 36: Maintenance Information Tab Parameters

Parameter	Data Format and Length	Description
Name	Printable ASCII string, max.64 characters	Uniform label (string) in the installation for the function of thisdevice
Installation location	Printable ASCII string, max.32 characters	Uniform label (string) in the system for the location where thedevice is mounted.
Installation date	ASCII time specification,max. 32 characters	Date of installation or commissioning of this device, the formatmay be defined by the fieldbus organization.
Contact information	Printable ASCII string, max.32 characters	Textual identification of a contact person for this managed node ofthe installation, together with information on how to contact this person.
Description	Printable ASCII string, max.64 characters	Readable comment field (in plain text) to store any individualstatus information and remarks.
Last service date	ASCII time specification,max. 32 characters	Date/time of the last service, e.g. firmware update
Next service date	ASCII time specification,max. 32 characters	Date/time of the next service, e.g. firmware

To make changes to the maintenance information:

1. Click on the **Settings** in the left column of the CoreTigo Wireless WebServer.

   The **Device configuration** tab appears.
2. Select the **Maintenance information** tab.
3. Change the relevant fields there.
4. Click **Apply**.

   Your changes take effect.

5.7.4. Firmware Update

The CoreTigo Wireless Web Server provides a way to update all firmware required for the IO-Link Wireless Master TigoMaster device via the **Firmware update** tab.

1. Select **Settings** in the left column of the CoreTigo Wireless WebServer.
2. Open the **Firmware update** tab.

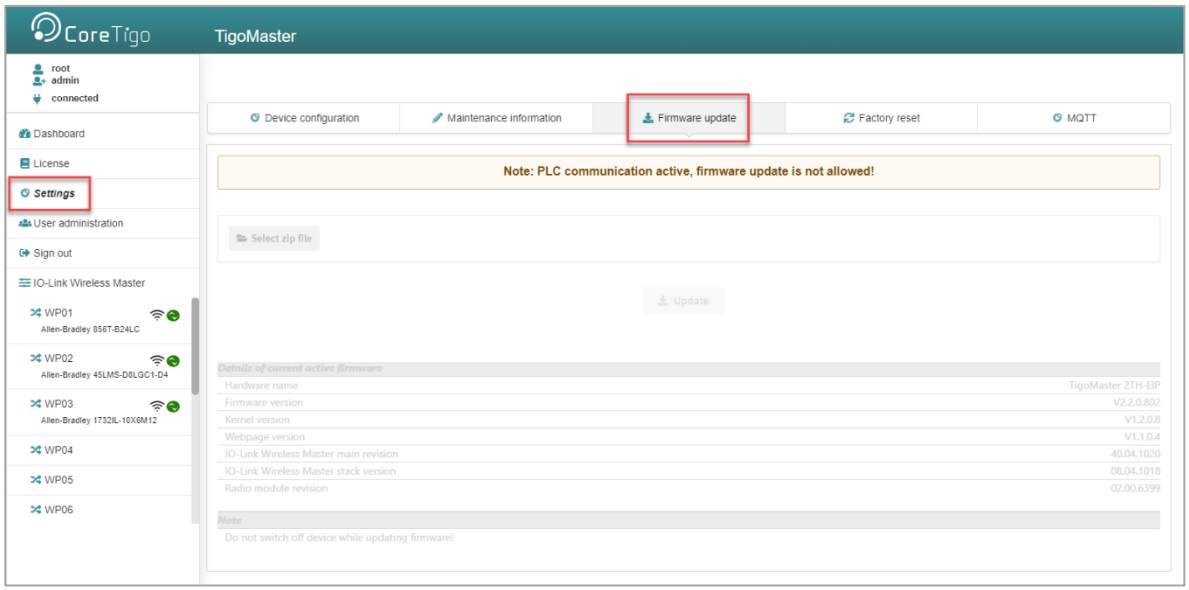


Figure 42: Firmware Update Tab

5.7.4.1. Bring the System into Safe Operating Condition

Never carry out a firmware update during operation of the system in which the TigoMaster device is installed. Before each firmware update, the system must first be shut down properly, or must be brought into a safe operating state.

5.7.4.2. Invalid Firmware

Loading invalid firmware files could render your device unusable. Only load firmware files to the device that are valid for this device. Otherwise, it may be necessary to send your device for repair.

Warning:
If you update the firmware of the TigoMaster device without making a backup of the firmware and configuration data, you cannot restore the state of your device prior to the update, including the previously used firmware.

Changes to settings require operator or admin rights. If these are not available, the **Firmware update** tab is grayed out and cannot be edited.

To update the firmware, you need the file *NFDW_Update_[protocol name]_V[version].zip* containing all firmware required for the TigoMaster device. You can download this from the website of the device manufacturer or provider.

1. In the **Firmware update** tab, click on **Choose File**.

   A file selection dialog appears.

2. Select the file **NFDW_Update_[protocol name]_V[version].zip** in this dialog.
3. Click **Update**.

   The firmware update is performed. This takes a short while.

   A message appears indicating that the firmware update has finished,and the device will be restarted after pressing **OK.** It will have a new IP address.

4. Click **OK**.
5. Perform the port configuration again.

5.7.5. Master Reset

Warnings:

- Never carry out a firmware update during operation of the system on which the TigoMaster device is installed.
- Before each firmware update, the system must first be shut down properly, or must be brought into a safe operating state.
- Loading invalid firmware files could render your device unusable. Load only firmware files to the device that are valid for this device, lest the device may require repair.
- If you update the firmware of the TigoMaster device and you did not make a backup of the firmware and configuration data, you cannot restore the state of your device prior to the update, including the previously used firmware.

To perform a reset of the IO-Link Wireless Master device, proceed as follows.

1. Verify that the system is in a safe operating condition.
2. Select **Settings** in the left column of the CoreTigo Wireless Web Server.
3. Open the **Firmware Update** tab.
4. Click **Delete all settings**.
5. Click **Reset**.

   The device reset is complete.

   The message **Device reset successfully** appears.

5.7.6. Factory Settings

In some cases, it is helpful to reset the device to the factory settings. This is possible for various selectable classes of settings via the **Factory reset** tab in the **Settings** menu.

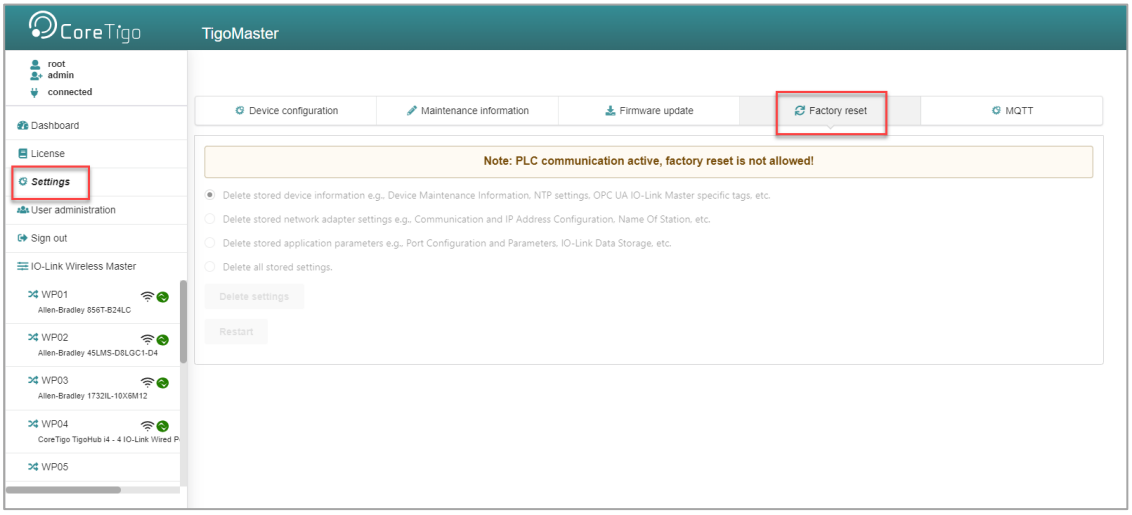


Figure 43: Factory Reset Tab

Changes to settings require operator or admin rights. If these are not available, the tab is grayed out and cannot be edited. Various settings made can be deleted depending on your selection.

Table 37: Options to Delete Settings

Option	Delete Stored Configuration
Delete stored device information	Device information (e.g. maintenance information, system time settings,and IO-Link master settings within OPC UA)
Delete stored network adaptersettings	Network adapter settings (communication settings, IP address configuration, Name of Station)
Delete stored application parameters	Application-specific data (port configuration and parameters, permanent parameters)
Delete all stored settings	All settings

To reset the device to the factory settings, proceed as follows:

1. Click on the **Settings** in the left column of the CoreTigo Wireless WebServer.

   The **Device configuration** tab appears.
2. Select the **Factory reset** tab.
3. Select which settings should be reset to the factory defaults.
4. Click on **Delete settings**.

   The selected settings are deleted.
5. Click on **Restart**.

   The device is restarted with the factory settings.

5.7.7. MQTT Configuration

Use the **MQTT** tab to view and change the MQTT client and connection configuration.

1. Select **Settings** in the left column of the CoreTigo Wireless WebServer.
2. Open the **MQTT** tab with its subtabs.

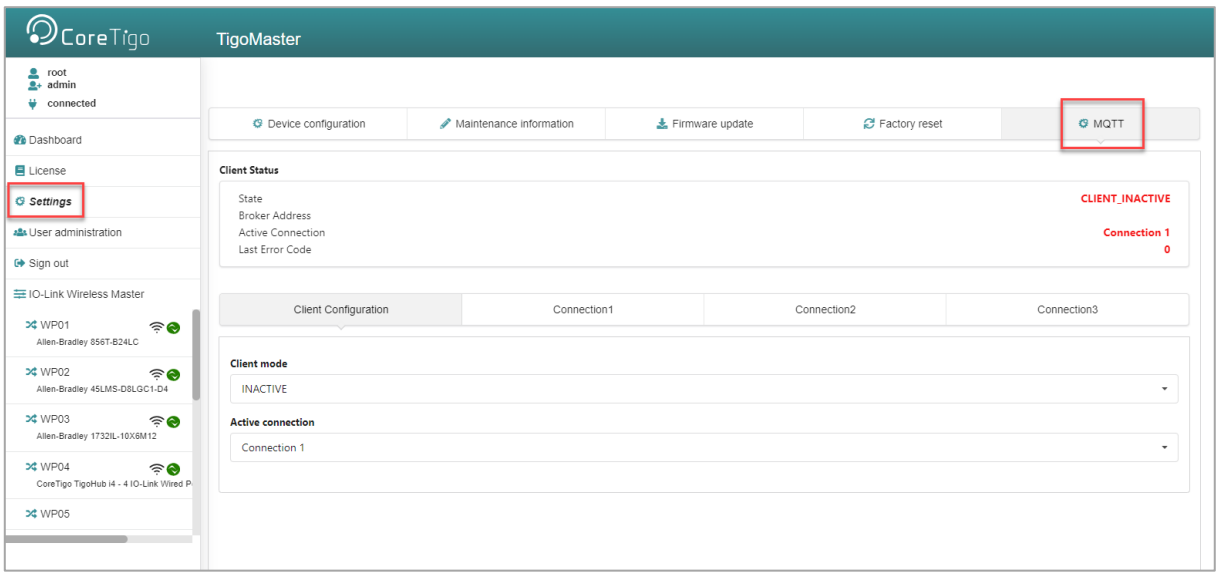


Figure 44: MQTT Tab

The **Client Status** appears, and by default the **Client Configuration** subtab.

5.7.7.1. MQTT > Client Status and Client Configuration

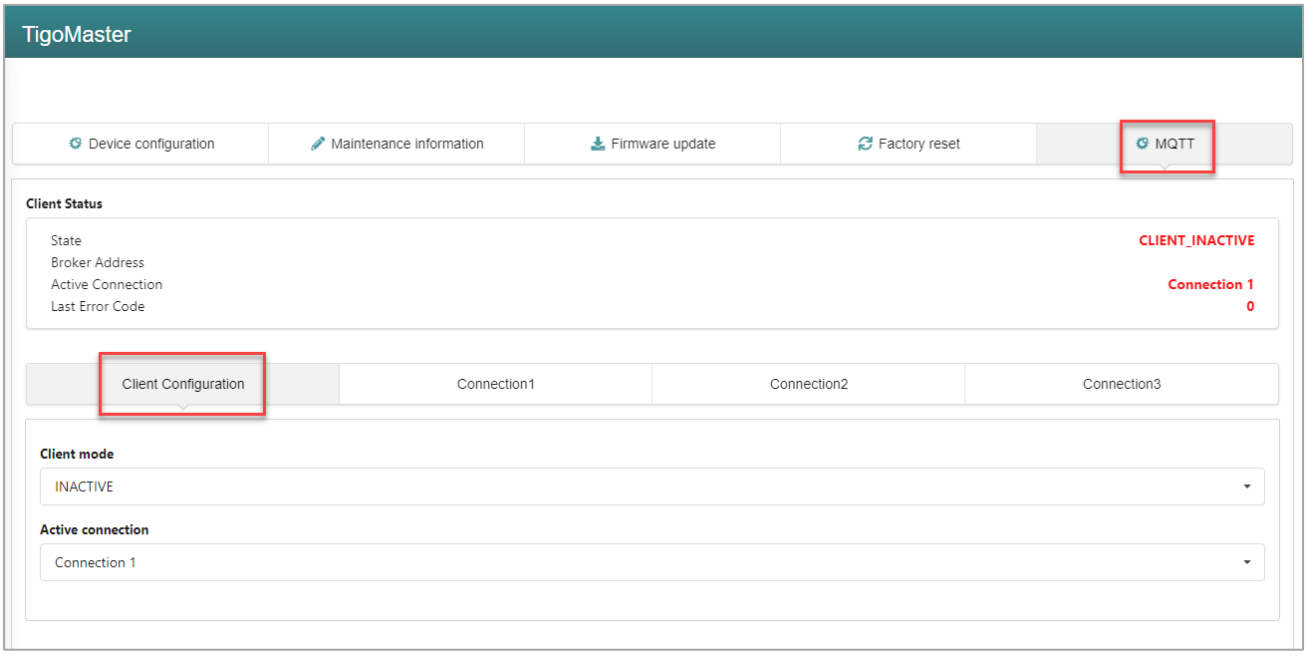


Figure 45: MQTT Tab, Client Status, Client Configuration Subtab

Table 38: MQTT in Port Configuration for IO-Link Device, Client Status

Parameter	Description	Value/Value Range
State	States 1, 2: "CONNECTING" State 3: "CONNECTION_ACCEPTED" States 0,4,5,6: "CLIENT_INACTIVE" Connection state code 0: Ready: initialization value, connection not established. 1: Connecting: TCP connection establishment in progress. 2: TCP Connected: TCP connection established. MQTT connection in progress. 3: MQTT Connected: MQTT connection established. 4: Disconnecting: MQTT connection shutdown in progress. 5: Disconnected: TCP connection terminated. 6: Wait Reconnect: Waiting for reconnection to be allowed again. See "Connect Timeout" parameter.	CONNECTING (**Red**), CONNECTION_ACCEPTED (**Green**), CLIENT_INACTIVE (**Red**)
Broker Address	Current value for “Broker Address”	Example: 192.168.10.5
Active connection	Current value for “Active connection”, respectively active connection configured.	Example: Connection 1
Last Error Code	Last error code, related to this connection.	Example: 0

Table 39: MQTT in Port Configuration for IO-Link Device, Client Configuration

Parameter	Description	Value/Value Range
Client mode	"ACTIVE" means MQTT client application is enabled and "INACTIVE" means disabled.	INACTIVE (default) ACTIVE
Active connection	Active connection configured.	Connection 1 (default) Connection 2 Connection 3

3. For **MQTT Client Configuration** make the following settings and configuration steps:
   - Client mode
   - Active connection

5.7.7.2. MQTT > Connection1 > IP Settings

1. Open the **Connection1** subtab.

   The **IP settings** subtab appears by default.

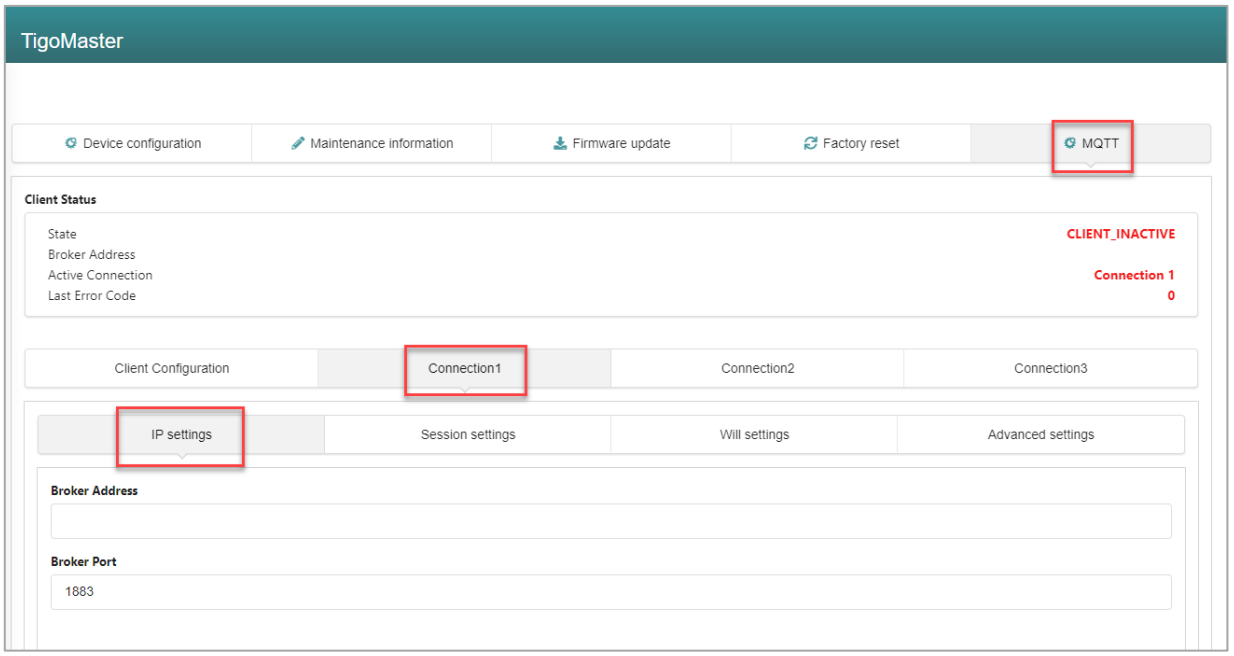


Figure 46: MQTT Tab, Connection 1 > IP Settings Subtab

Table 40: MQTT in Port Configuration for IO-Link Device, Connection1 > IP Settings

Parameter	Description	Value/Value Range
Broker Address	IP address of the broker.	Valid IP address Default: [BrokerAddress],
Broker Port	MQTT broker IP port number.	Typically: 1883

2. For **MQTT Connection Configuration** make the following settings and configuration steps:
   - Broker Address
   - Broker Port

5.7.7.3. MQTT > Connection1 > Session Settings

1. Open the **Session settings** subtab.

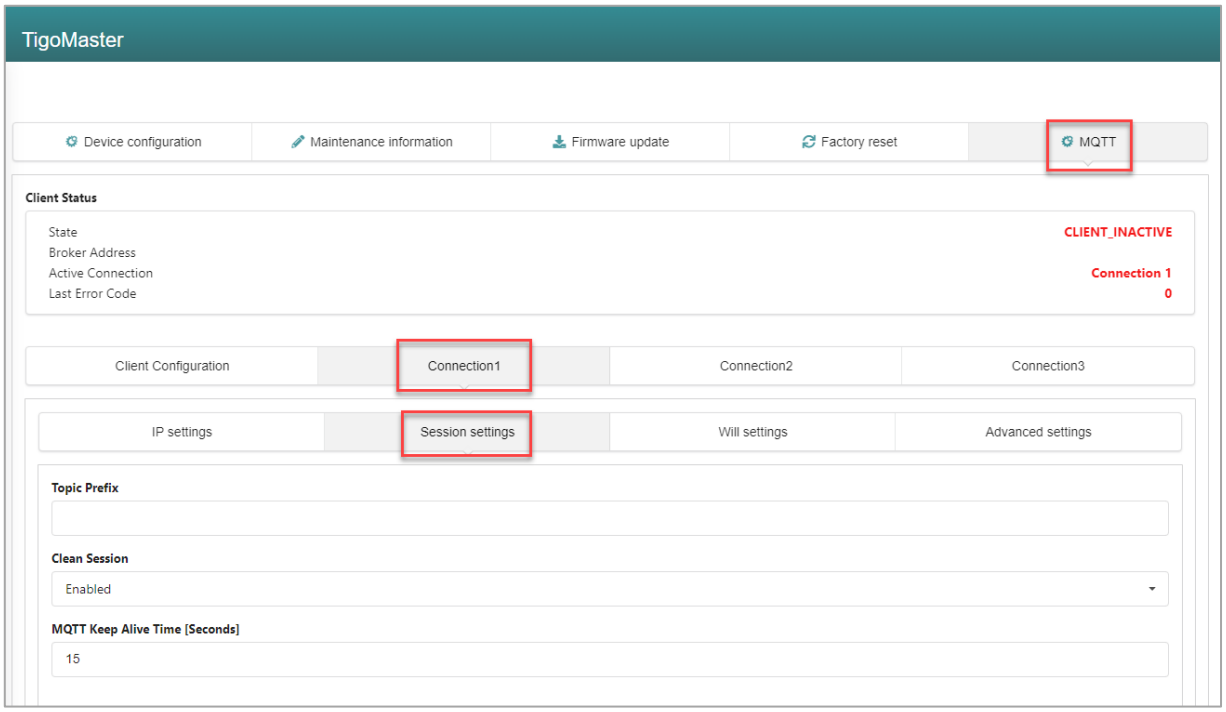


Figure 47: MQTT Tab, Connection1 > Session Settings Subtab

Table 41: MQTT in Port Configuration for IO-Link Device, Connection1 > Session Settings

Parameter	Description	Value/Value Range
Topic Prefix	Text that is prefixed to each topic, e. g. 'StationA'. For each single topic can be configured if this prefix is to be preceded or not. If left empty the firmware will try to use the MAC address.	Text of uppercase and lowercase letters and underscore, Default: [not specified]
Clean Session	Setting whether all topics are to be transferred to the broker after establishing a connection or not. Enabled (default): After a connection to the broker has been established, all topics of the type 'publish' are transmitted from the MQTT client to the broker. Disabled: Only those topics are transmitted to the broker, which have changed since the last connection. Note that if you use this setting, the broker must support the 'preserve context' function.	Enabled (default), Disabled
MQTT KeepAlive Time [Seconds]	Interval in which the MQTT client sends a sign of life to the broker. The set value for the MQTT client must be less than the monitoring time set in the broker.	Specified in s. 0 = send no sign of life to the broker. Default: 0

Parameter	Description	Value/Value Range
	Enabling this timeout is suitable if the connection is used for at least one subscription so a permanent connection to the broker is required. Not allowed to be enabled together with the Connection Idle Timeout.	

2. For **MQTT Connection Configuration** make the following settings and configuration steps:
   - Topic Prefix
   - Clean Session
   - MQTT Keep Alive Time

5.7.7.4. MQTT > Connection1 > Will Settings

1. Open the **Will Settings** subtab.

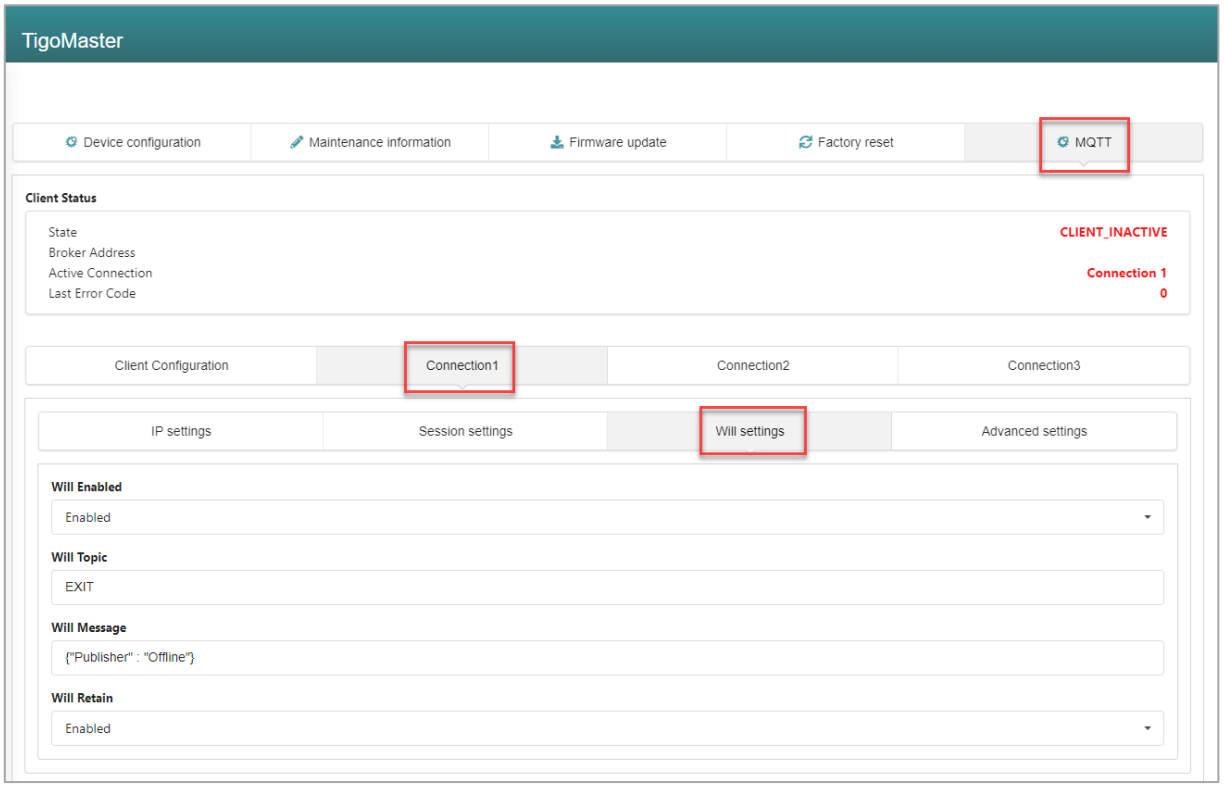


Figure 48: MQTT Tab, Connection1 > Will Settings Subtab

Table 42: MQTT in Port Configuration for IO-Link Device, Connection1 > Will Settings

Parameter	Description	Value/Value Range
Will Enabled	Enable this option if you want to use the “will” feature of MQTT.	Enabled (default), Disabled
Will topic	Unique name for the topic, editable. If left empty the firmware will use the string constant "will" prefixedby the Prefix Will if enabled.	Max. 128 characters of text from uppercase and lowercase letters and underscore. Default: [not specified]
Will Message	Payload forwarded by the broker to other clients subscribed to thewill topic in case of abnormal disconnection (when an MQTT Disconnect packet was not sent to the broker). If left empty, the string "Disconnected" is sent.	Text of uppercase and lowercase letters and underscore Default: [not specified]
Will QoS	Quality of Service Level for the Will Message. 0: "Only once": fire and forget 1: "At least once": acknowledged delivery2: "Exactly once": assured delivery	Only once (default) At least once Exactly once
Will Retain	Setting whether the broker shall store the history of a data value ornot.	Enabled (default), Disabled

2. For **MQTT Connection Configuration** make the following settings and configuration steps:
   - Will Enabled
   - Will Topic
   - Will Message
   - Will Retain

5.7.7.5. MQTT > Connection1 > Advanced Settings

1. Open the **Advanced settings** subtab.

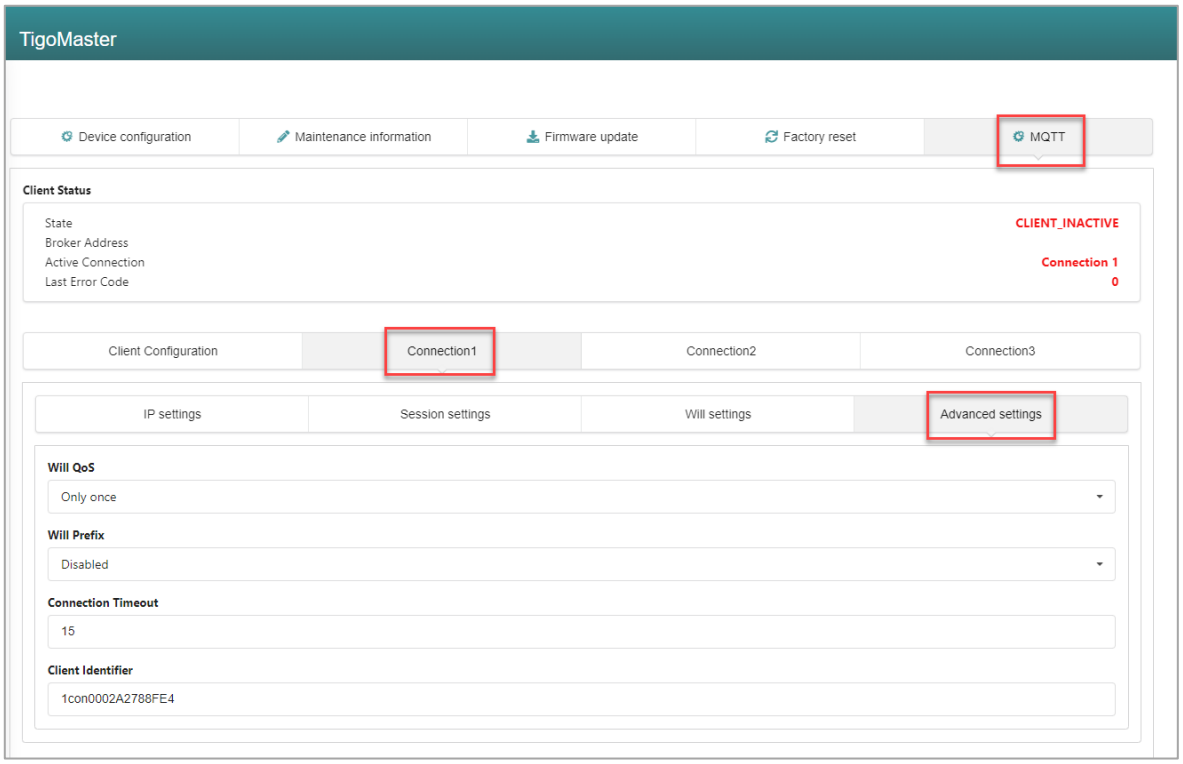


Figure 49: MQTT Tab, Connection1 > Advanced Settings Subtab

Table 43: MQTT in Port Configuration for IO-Link Device, Connection1 > Advanced Settings

Parameter	Description	Value/Value Range
Will QoS	Quality of Service Level for the Will Message. 0: "Only once": fire and forget 1: "At least once": acknowledged delivery 2: "Exactly once": assured delivery	Only once (default) At least once Exactly once
Will Prefix	Text that is prefixed to each Will topic. For each single topic can beconfigured if this prefix is to be preceded or not.	Text of uppercase and lowercase letters and underscore. Default: [not specified]
Connection Timeout	Time for trying to establish a connection (MQTT Connect) to the broker. If the connection could not be established, then the MQTTclient waits for the duration of 'Connection Timeout' until a new connection is established to the broker.	Specified in s. = 0 MQTT clientconstantly tries to establish a connection to the broker. Default: 0
Client Identifier	Unique name of the MQTT client in UTF-8 format used at connection establishment time. All devices that are connected to a broker, must have a unique name. The name may only consist of lowercase letters, uppercase letters and numbers. If the field is empty, the broker assigns a name.	Max. 23 bytes for Max. 23 characters. Default: [Client ID] Example: “ClientId1”

2. For **MQTT Connection Configuration** make the following settings and configuration steps:
   - Will QoS

- Will Prefix
- Connection Timeout
- Client Identifier

5.7.8. Log In and User Administration

5.7.8.1. Log In User

Note:
Log In is only possible when device connection state is “connected” (top left corner of the CoreTigo Wireless Web Server).

To log in as a user:

1. Select **Sign in** in the left column of the CoreTigo Wireless Web Server.

   The input mask for username and password appears:

Figure 50: Menu Item Sign In - Input Mask for Username and Password

2. Enter your username and password correctly in the corresponding input fields of the screen mask.
3. Click **Sign in**.

   If you have entered a known username correctly, you can work with the CoreTigo Wireless Web Server with the defined rights of this user.

   The user role (**Operator, Maintenance, Admin**) used for sign in is displayed in the upper left corner.

   The previous menu entry **Sign in** changes and is now called **Sign out**.

5.7.8.2. Log Out Users

To log out a user:

1. Click on the **Sign out** menu item in the main menu of the CoreTigo Wireless Web Server (left side panel).

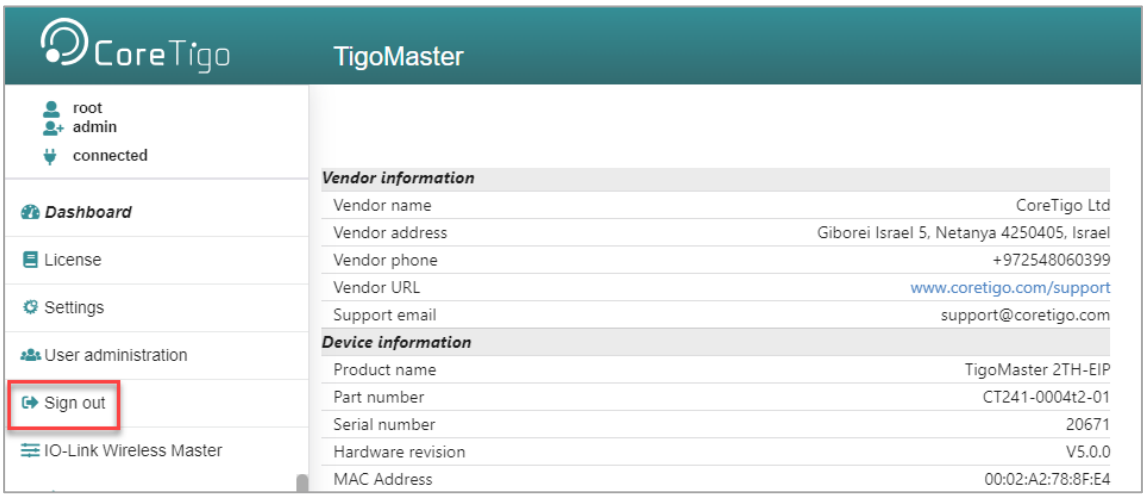


Figure 51: Menu Item Sign Out

From now on, you can no longer work with the CoreTigo Wireless WebServer with the previous rights.

The user role **guest** appears in the upper left corner.

The previous menu entry **Sign out** changes and is now called **Sign in** again.

5.7.8.3. Guest User Access

By default, the CoreTigo Wireless Web Server identifies a user guest without password, which has been set up to realize a first-time or guest access.

5.7.8.4. First-Time Login as Administrator

In the delivery state or after resetting to the factory settings, the CoreTigo Wireless Web Server can be accessed via the username “root” and the password “password”.

This combination also has administrator rights.

Warning:
Change the administrator password immediately after commissioning. The factory default setting is generally known and does not provide sufficient protection.

5.7.8.5. User Administration

1. Select **User Administration** in the left column of the CoreTigo Wireless Web Server.

   The Administration pane provides a role-based user administration. You can use it to create and delete users and assign roles to them on which their rights depend.

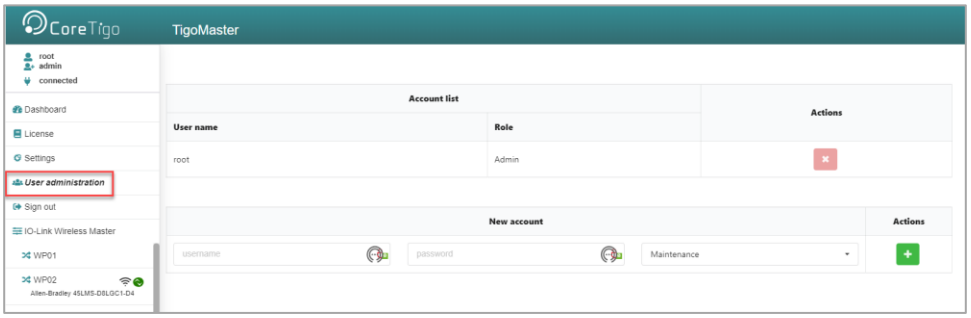


Figure 52: User Administration Screen

Users can be divided into three roles:

- Maintenance
- Operator
- Administrator

5.7.8.6. Create a New User

Proceed as follows:

1. In the **Username input** field (left side), enter the username for the user. Usernames that have already been used are not permitted here.
2. In the **Password input** field (middle), enter the password for this username.
3. Use the combo box on the right to select the role for the new user to be created (the roles **Maintenance**, **Operator** or **Administrator** are available).
4. Click on the **Green** field.

   The new user is created and assigned to the selected role, appearing in the **Account List**.

5.7.8.7. Remove User

To remove an existing user from the device user management, proceed as follows:

Click the **Red** square with a white cross to the right of the user to be removed.

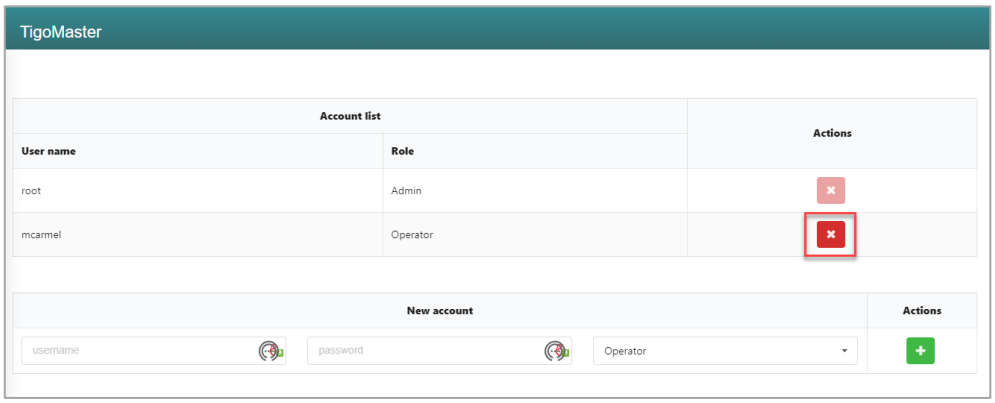


Figure 53: Remove a User

The user will be deleted.

The “root” user cannot be deleted, so the **Red** delete button is grayed out.

6. Commissioning

The TigoMaster 2TH is provided with a default IP Address 192.168.1.100, and the subnet mask address is 255.255.255.0.

There are 2 ways to set the IP address of the TigoMaster 2TH EtherNet/IP:

- Via the CoreTigo Web Server.
- In case the TigoMaster 2TH is in BOOTP/DHCP mode please use the BOOTP tool to configure the IP address.

6.1. Set the IP Address via the CoreTigo Web Server

To set the IP address via the CoreTigo Web Server:

1. Connect the TigoMaster 2TH directly to the PC.
2. Set the PC EtherNet interface to IP address in the same subnet. (ex 192.168.1.200).
3. Open the internet browser and navigate to https://192.168.1.100

   The CoreTigo Web Server will appear:

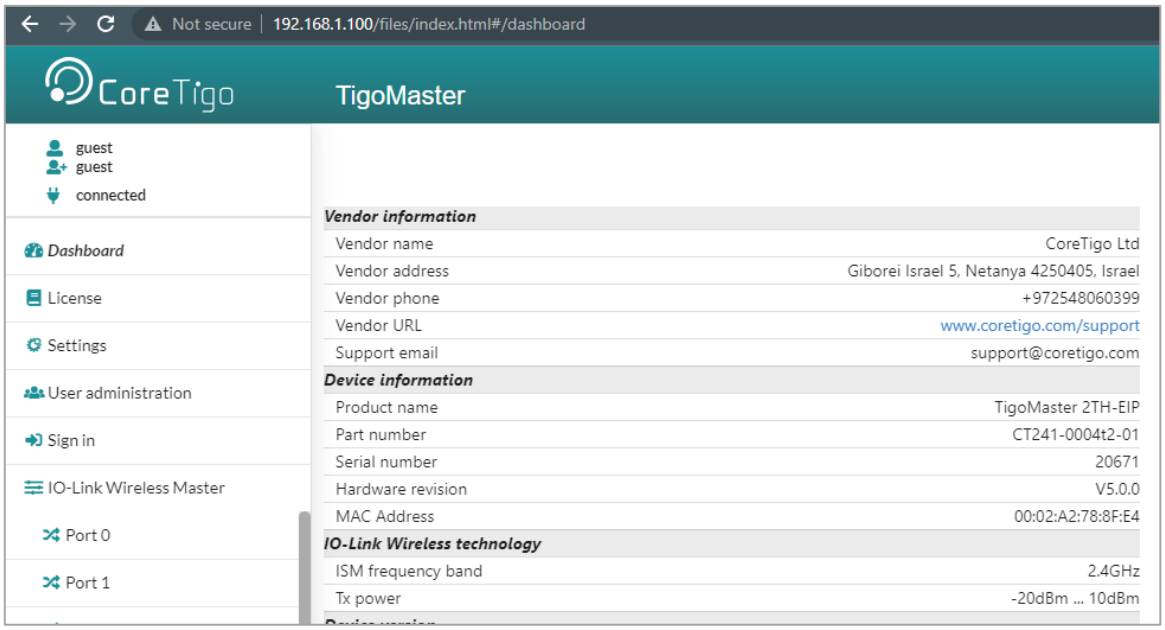


Figure 54: TigoMaster 2TH Web Server

4. Select **Sign in** from the menu in the left side panel.

5. Enter the credentials as follows and click **Sign in**:
    - Username: root
    - Password: password

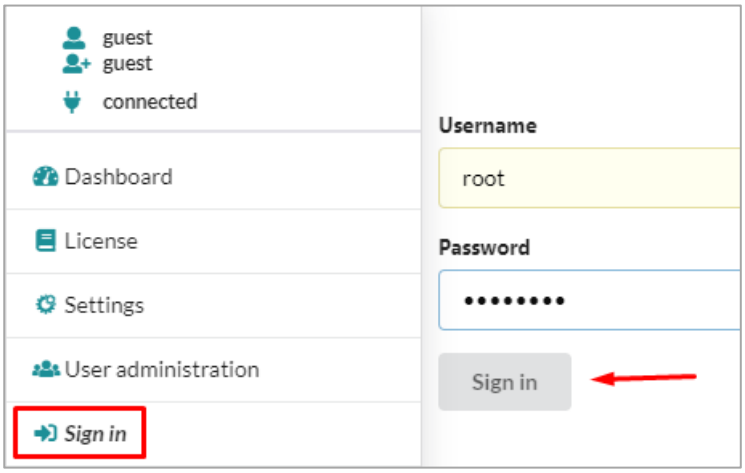


Figure 55: Sign In

6. Select **Settings** and in the **Device Configuration** tab enter the desired IP address, subnet mask, and default gateway.
7. Click **Apply**.

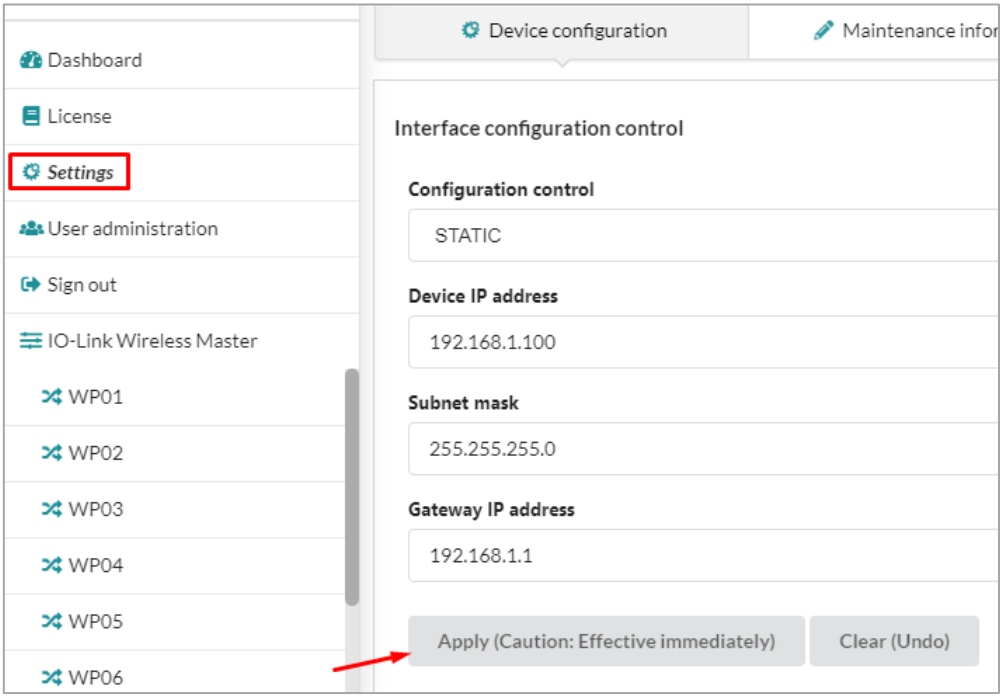


Figure 56: Device Configuration Tab

8. Enter the new IP address,Subnet mask and Gateway in the PC web browser. (All addresses must be entered for the changes to be accepted). If required change also the PC IP address to match the new network settings.

Where the TigoMaster 2TH is in BOOTP/DHCP mode, follow the below procedure to set the IP address:

1. Confirm that the device is connected to the network.
2. Start the BOOTP/DHCP.

   The MAC IP of the device appears in the **Request History** window.
3. Select the appropriate device and click **Add to Relation**.

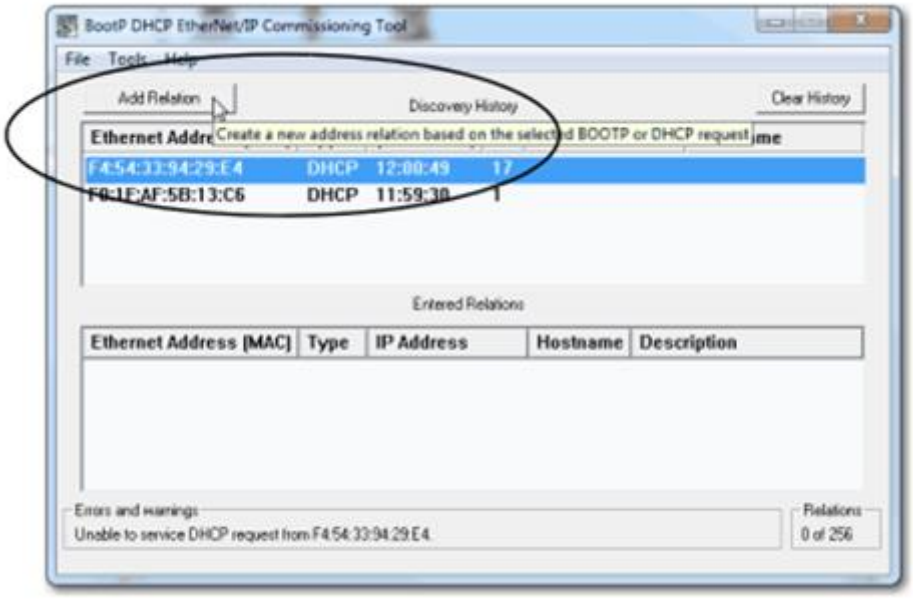


Figure 57: Add Relation

The **New Entry** dialog box appears.

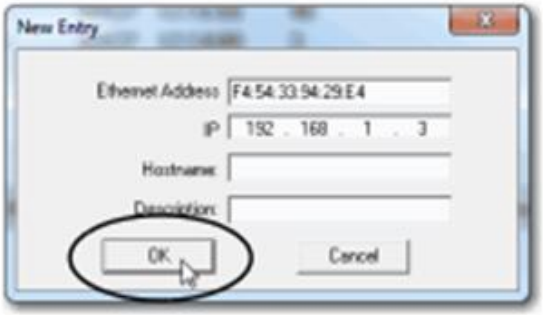


Figure 58: New Entry Dialog Box

4. Type an IP Address, Hostname, and Description for the device. (Hostname and Description are optional).
5. To assign this configuration on the device, wait for the device to appear in the **Relation List** panel and select it.
6. Click **Disable BOOTP/DHCP**.

The device now uses the assigned configuration and does not issue BOOTP or DHCP requests after power up.

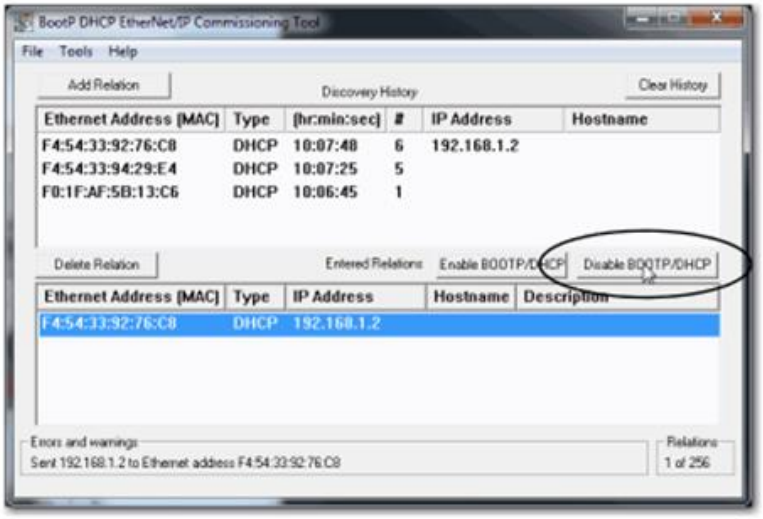


Figure 59: Disable BOOTP/DHCP

IMPORTANT

- If you do not click **Disable BOOTP/DHCP**, on future power cycles, the current IP configuration is cleared, and the controller sends DHCP requests again.
- If you click **Disable BOOTP/DHCP** and it does not disable BOOTP/DHCP, you can use **RSLinx® Classic** software to disable BOOTP/DHCP.

6.2. Configuration with the CoreTigo Web Server

Note:
Configuration can be performed also with the TigoEngine.
For further information refer to the *TigoEngine User Manual*.

6.2.1. Requirements

To allow the commissioning or configuration using the CoreTigo Web Server, the following requirements must be fulfilled:

- The device must be mounted, wired, and supplied with power.
- A browser is required, to connect to the CoreTigo Web Server.
- A login as admin.

6.2.2. Configure the IO-Link Wireless Master

1. Select **Master** in the left column of the CoreTigo Web Server.
2. On the **Channel Selection** tab select the WLAN channels required (e.g. WLAN channels 01 to 04).

3. Open the **Configuration** tab.

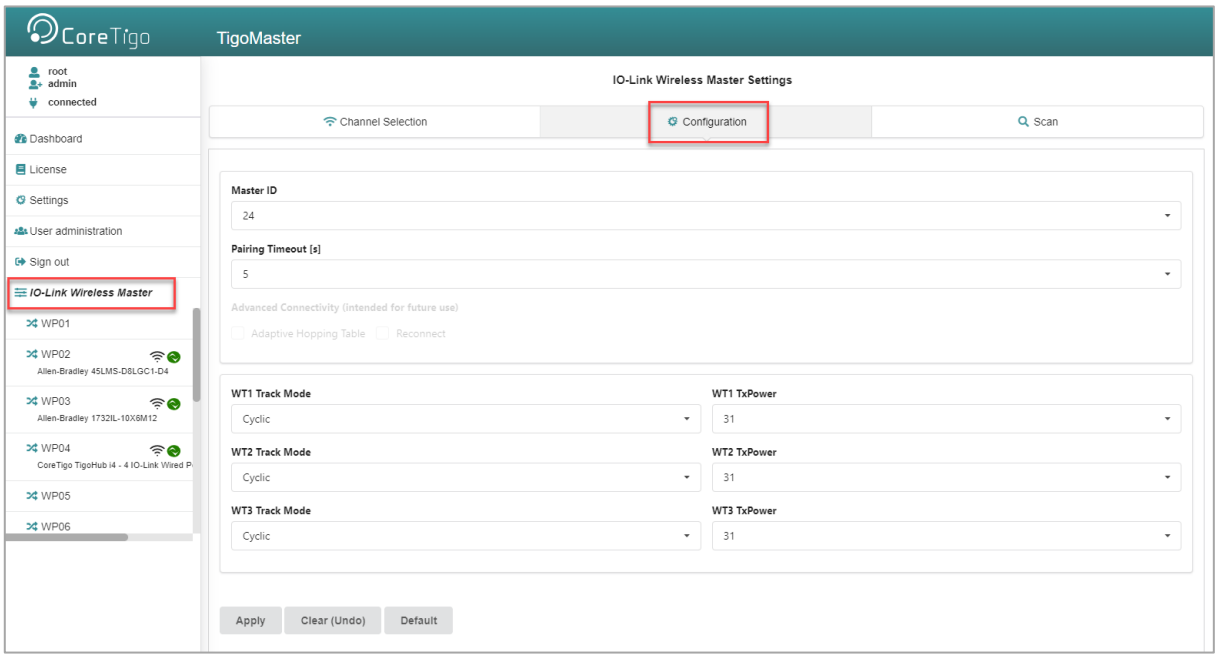


Figure 60: Master > Configuration Tab

4. Use the IO-Link Wireless Master settings in the table below as possible values for commissioning.
5. Click **Apply**.

   The request appears **Applying configuration will restart the device. Are you sure?**
6. Click **Yes**.
7. Wait until reset operation is finished and result is shown.
   - The message **Master configured successfully** appears.
   - The set IO-Link Wireless Master settings are used now.

Table 44: Configuration, Possible Values for IO-Link Wireless Master

Parameter	Possible Value for Commissioning	Note
Master ID	1	Enter the Master ID this way: “1”
Pairing Timeout	5	Seconds
Advanced Connectivity	Adaptive Hopping Table: unchecked Reconnect: checked	
WT1 Track Mode	Cyclic	
WT2 Track Mode	Cyclic	
WT3 Track Mode	Cyclic	
WT1 TXPower	31	“31” = max. transmission power
WT2 TXPower	31	
WT3 TXPower	31	

Warning:
For proper device operation all three tracks must be activated.

6.2.3. Scan

1. Select **Master** in the left column of the CoreTigo Wireless Web Server.
2. Open the **Scan** tab.

Figure 61: Scan Tab

3. Enter **TXPower** as decimal value: 31 (= maximum transmission power of the device)
4. Click **Scan start**.
   - The scan result is displayed. The connected device is found.
   - The scan result values in the table below are displayed.

Table 45: Scan Results

Parameter	Scan Result	Note
Index	0	
Unique ID	• 0x03 • 0xf3 • 0x00 • 0x00 • 0x01 • 0x72 • 0xc0, • 0x45 • 0xcf	Copy/note the unique ID. This value is required for port configuration.
Slot Type	Double slot	
Revision ID	0x11	
Port	Select port	Note: For a device featuring “Double slot” an even port must be assigned.
Pairing	Pair (**Green**)	

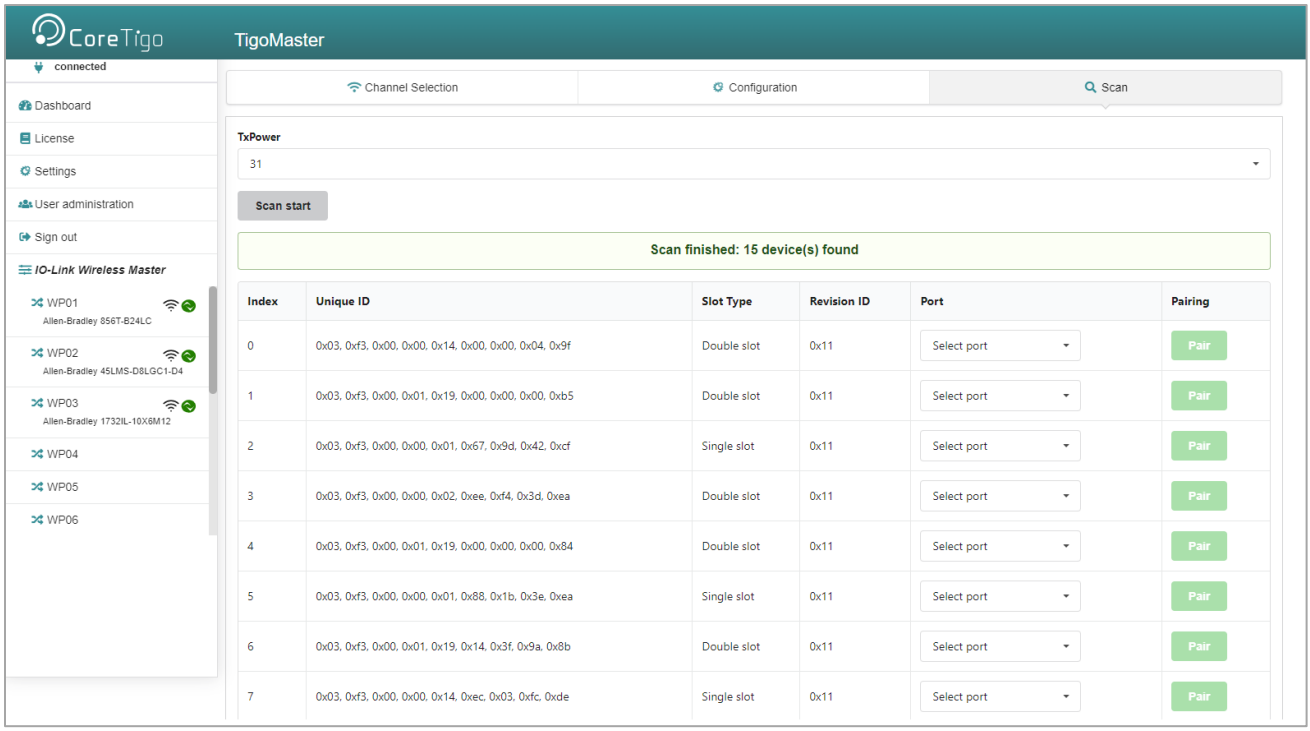


Figure 62: Scan Tab with Result

6.3. Use an OPC UA Client

TigoMaster 2TH has an integrated OPC UA server, enabling you to communicate with it using an OPC UA client. Communication has 2 levels:

- Read only—anonymous authentication permits read access only.
- Read and write—authentication with a username and password enables read and write access to users who have write permission.

  Usernames and passwords are set by means of TigoEngine and the CoreTigo Web Server.

The OPC UA client establishes a connection via the following URL: opc.tcp://IP address:4840

For test purposes, you can use such a client as the UaExpert from Unified Automation GmbH (http://www.unifiedautomation.com).

6.3.1. Requirements

- OPC UA client application installed on your local PC
- A username and password that have write permission
- Device IP address

6.3.2. Instructions

1. Start UaExpert (or your chosen OPC UA client).
2. Select **File > New**, and then select **Server > Add**.
3. In the **Add Server** dialog box, type the desired **Configuration Name**.

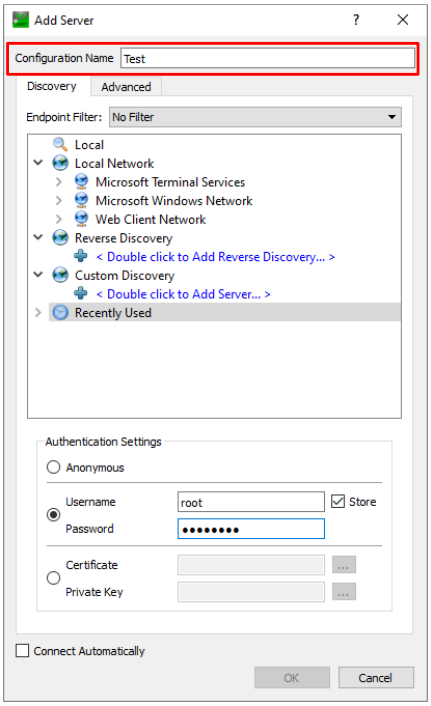


Figure 63: Add Server Dialog Box (Discovery Tab)

4. In the **Advanced** tab, set **Endpoint Url** = **opc.tcp://<IP address>:4840.**

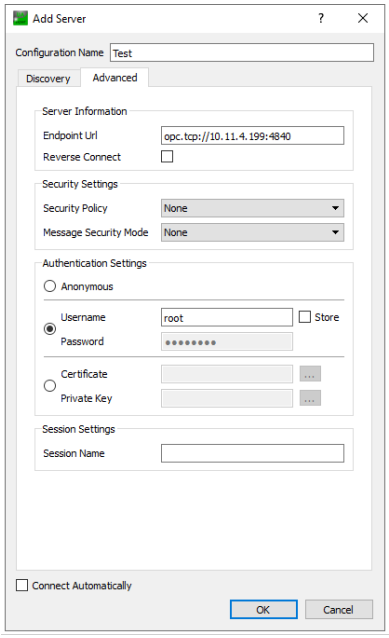


Figure 64: Add Server Dialog Box > Advanced Tab)

5. Under **Authentication Settings**, do the following:
   - If you need write access, select the **Username/Password** option, and enter the relevant **Username** and **Password**.
   - If read access only is sufficient, select the **Anonymous** option.
6. Click **OK**.

   In the project window, under **Project > Servers**, the UaExpert enters the server, for example, Test.
7. Open the **Context** menu of the server (Test) and select **Connect**.

   The connection starts.

6.3.3. Set the Device Date and Time Using OPC UA

6.3.3.1. Requirements

- OPC UA client.
- A username and password that have write permission
- NTP Server IP address: see section 0
- Converted IP address (from NTP server to a decimal number): see section 6.3.3.3
- Device is connected

6.3.3.2. Examples of an NTP Server

The German Federal Institute of the Physikalisch-Technische Bundesanstalt in Braunschweig has the following NTP servers:

- ptbtime1.ptb.de—IP address 192.53.103.108
- ptbtime2.ptb.de—IP address 192.53.103.104

6.3.3.3. Convert an IP Address to a Decimal Number

This section uses one of the above IP Addresses as its example: namely, 192.53.103.108 (belonging to NTP server ptbtime1.ptb.de).

Like most IP addresses, our example is composed of 4 segments, which are separated from each other by a period. To convert an IP address to a decimal number, each segment is inserted into a specific place in the conversion formula below, where the letters A, B, C, D are the placeholders for the 4 segments (in our example, A is the placeholder for 192, B is the placeholder for 53, C is the placeholder for 103, and D is the placeholder for 108).

The conversion formula is:
((A * 256 + B) * 256 + C) * 256 + D = IP address as a decimal number

Inserting an example IP address into the formula gives the following:
((192 * 256 + 53) * 256 + 103) * 256 + 108 = 3224725356

The decimal number in this example IP address is 3224725356.

6.3.3.4. Instructions

1. In the **Address Space** window, go to **Root > Objects > DeviceSet > [Device name] > Configuration > NtpClient > NtpClientUpdateConfiguration**.

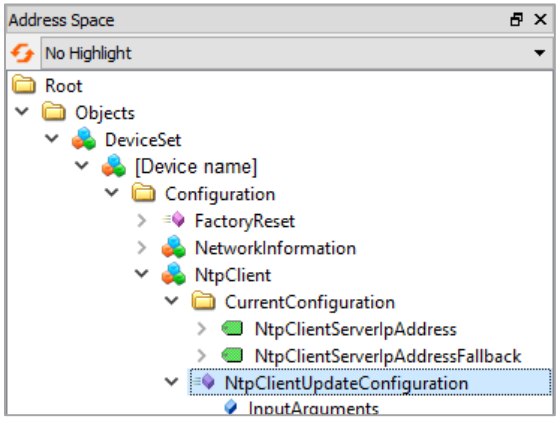


Figure 65: Path to NtpClientUpdateConfiguration

2. Right-click **NtpClientUpdateConfiguration,** and then click **Call**.

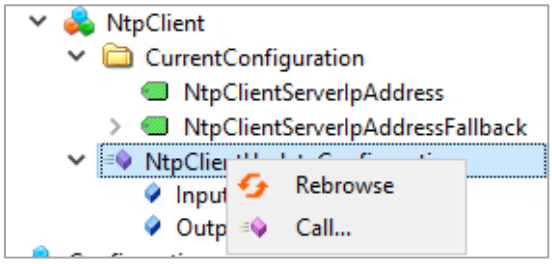


Figure 66: Right-Clicking NtpClientUpdateConfiguration

3. In the **Call NtpClientUpdateConfiguration** dialog box, set the following:
   - **ServerIpAddress** = **3224725356**
   - **ServerIpAddressFallback** = **3224725352**

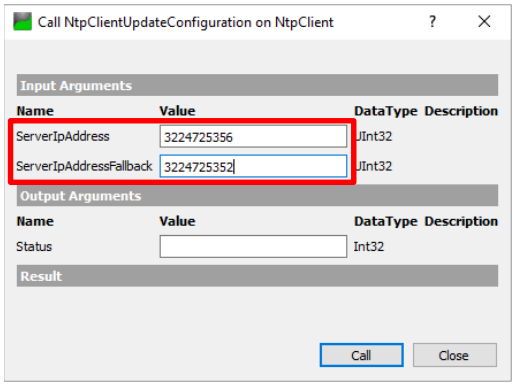


Figure 67: Call NtpClientUpdateConfiguration Dialog Box—Before Call

4. Click **Call**.
5. Verify that the Status = **0** and the **Result** = **Succeeded**.

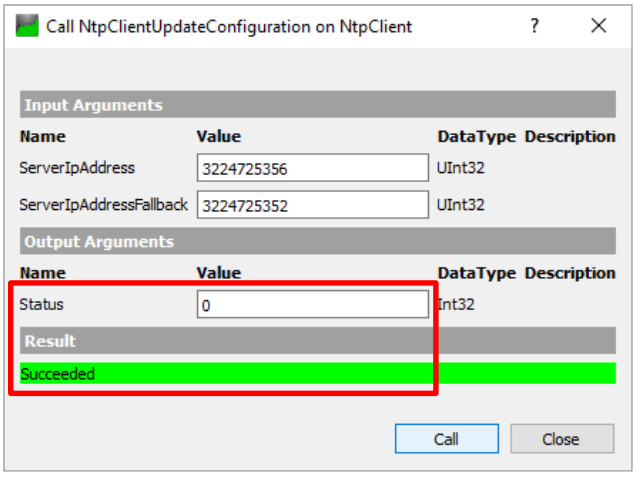


Figure 68: Call NtpClientUpdateConfiguration Dialog Box—After Call

7. Process Data Mapping

This section describes all process data for the TigoMaster 2TH IO-Link Wireless Master EtherNet/IP adapter for connections 1-10 which can be categorized as the following connection types:

- **Exclusive Owner:** The scanner can read input process data and write output process data.
- **Input Only:** The scanner can read input process data only.
- **Listen Only:** The scanner can read input process data only.

Note:
The “Listen Only” connection type requires that another scanner establishes an “ExclusiveOwner” or “Input Only” connection type with the TigoMaster 2TH device.

The allowed number of usable sensors/actuators depends on the number of IO- Link bytes which the used sensor/actuator must transfer:

- In case one or more sensors/actuators must transfer 17 or more IO-Link bytes, then a maximum number of 8 sensors/actuators (and one track) can be used.
- If all sensors/actuators require 16 IO-Link bytes or less, then up to 16 sensors/actuators (and two tracks) can be used.

Table 46: Connections 1-10 Overview

Connection No.	Name	Description
Connection 1	Exclusive Owner –8 ports x 32 bytes	Up to 8 sensors/actuators with up to 32 IO-Link bytes and one track can be used. The EtherNet/ IP scanner sends the port parameters to the TigoEngine software tool.
Connection 2	Exclusive Owner – 8 ports x 32 bytesw/o Config	Up to 8 sensors/actuators with up to 32 IO-Link bytes and one track can be used. The port parameters must be set using the Integrated Web Server.
Connection 3	Listen Only - 8 ports x 32 bytes	Up to 8 sensors/actuators with up to 32 IO-Link bytes andone track can be used.
Connection 4	Input Only – 8 ports x 32 bytes	Up to 8 sensors/actuators with up to 32 IO-Link bytes and one track can be used.
Connection 5	Exclusive Owner – 16 ports x 16 bytes w/o Config	Up to 16 sensors/actuators with up to 16 IO-Link bytes and two tracks can be used. The port parameters must be set using the Integrated Web Server.
Connection 6	Listen Only – 16 ports x 16 bytes	Up to 16 sensors/actors with up to 16 IO-Link bytes and twotracks can be used.
Connection 7	Input Only – 16 ports x 16 bytes	Up to 16 sensors/actors with up to 16 IO-Link bytes and two tracks can be used.
Connection 8	Exclusive Owner - 16 ports x 4 bytes w/o Config	Up to 16 sensors/actors with up to 4 IO-Link bytes and two tracks can be used. The port parameters must be set using theIntegrated Web Server.a

Connection No.	Name	Description
Connection 9	Listen Only – 16 ports x 4 bytes	Up to 16 sensors/actors with up to 4 IO-Link bytes and two tracks can be used.
Connection 10	Input Only – 16 ports x 4 bytes	Up to 16 sensors/actors with up to 4 IO-Link bytes and two tracks can be used.

Note:
The process data of the digital inputs and outputs for:

- Connections 1-4 have a fixed size of 276 Bytes.
- Connections 5-7 have a fixed size of 292 Bytes.
- Connections 8-10 have a fixed size of 100 Bytes.

7.1. Connections 1 – 4

The following table describes the structure of the input and output process data and is valid for connection 1, connection 2, connection 3, connection 4.

Table 47: Connections 1-4 Detail

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
0	1 byte	DI status	Reserved	DO status	Reserved
1	1 byte	Padding byte	Do not use	Padding byte	Do not use
2 … 3	2 bytes	DI data	Reserved	DO data	Reserved
4	1 byte	IO-Link Port 1 data status	0: IO-Link Port 1 input data notvalid. 1-255: IO-Link Port 1 input data valid.	IO-Link Port 1 Output enable	0: IO-Link Port 1 output data not valid. 1-255: IO-Link Port 1 output data valid.
5	1 byte	Padding byte	Do not use	Padding byte	Do not use
6 … 37	32 bytes	IO-Link port 1 process input data	IO-Link input data of the sensor/actor connected to Port 1. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 1 process output data	IO-Link output data of the sensor/actor connected to Port 1. For a description of the data,see manual of the manufacturer of the used sensor/actor.
38	1 byte	IO-Link Port 2 data status	0: IO-Link Port 2 input data notvalid. 1-255: IO-Link Port 2 input data valid.	IO-Link Port 2 Output enable	0: IO-Link Port 2 output data not valid. 1-255: IO-Link Port 2 output data valid.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
39	1 byte	Padding byte	Do not use	Padding byte	Do not use
40 … 71	32 bytes	IO-Link port 2 process input data	IO-Link input data of the sensor/actor connected to Port 2. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 2 process output data	IO-Link output data of the sensor/actor connected to Port 2. For a description of the data,see manual of the manufacturer of the used sensor/actor.
72	1 byte	IO-Link Port 3 data status	0: IO-Link Port 3 input data not valid. 1-255: IO-Link Port 3 input data valid.	IO-Link Port 3 Output enable	0: IO-Link Port 3 output data not valid. 1-255: IO-Link Port 3 outputdata valid.
73	1 byte	Padding byte	Do not use	Padding byte	Do not use
74 … 105	32 bytes	IO-Link port 3 process input data	IO-Link input data of the sensor/actor connected to Port 3. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 3 process output data	IO-Link output data of the sensor/actor connected to Port 3. For a description of the data,see manual of the manufacturer of the used sensor/actor.
106	1 byte	IO-Link Port 4 data status	0: IO-Link Port 4 input data notvalid. 1-255: IO-Link Port 4 input data valid.	IO-Link Port 4 Output enable	0: IO-Link Port 4 output data not valid. 1-255: IO-Link Port 4 output data valid.
107	1 byte	Padding byte	Do not use	Padding byte	Do not use
108 …139	32 bytes	IO-Link port 4 process input data	IO-Link input data of the sensor/actor connected to Port 4. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 4 process output data	IO-Link output data of the sensor/actor connected to Port 4. For a description of the data,see manual of the manufacturer of the used sensor/actor.
140	1 byte	IO-Link Port 5 data status	0: IO-Link Port 5 input data notvalid. 1-255: IO-Link Port 5 input data valid.	IO-Link Port 5 Output enable	0: IO-Link Port 5 output data not valid. 1-255: IO-Link Port 5 output data valid.
141	1 byte	Padding byte	Do not use.	Padding byte	Do not use.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
142 …173	32 bytes	IO-Link port 5 process input data	IO-Link input data of the sensor/actor connected to Port 5. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 5 process output data	IO-Link output data of the sensor/actor connected to Port 5. For a description of the data,see manual of the manufacturer of the used sensor/actor.
174	1 byte	IO-Link Port 6 data status	0: IO-Link Port 6 input data not valid. 1-255: IO-Link Port 6 input data valid.	IO-Link Port 6 Output enable	0: IO-Link Port 6 output data not valid. 1-255: IO-Link Port 6 output data valid.
175	1 byte	Padding byte	Do not use	Padding byte	Do not use
176 …207	32 bytes	IO-Link port 6 process input data	IO-Link input data of the sensor/actor connected to Port 6. For a description of the data see manual of the manufacturer of the used sensor/actor.	IO-Link port 6 process output data	IO-Link output data of the sensor/actor connected to Port 6. For a description of the data see manual of the manufacturer of the used sensor/actor.
208	1 byte	IO-Link Port 7 data status	0: IO-Link Port 7 input data not valid. 1-255: IO-Link Port 7 input data valid.	IO-Link Port 7 Output enable	0: IO-Link Port 7 output data not valid. 1-255: IO-Link Port 7 output data valid.
209	1 byte	Padding byte	Do not use	Padding byte	Do not use
210 …241	32 bytes	IO-Link port 7 process input data	IO-Link input data of the sensor/actor connected to Port 7. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 7 process output data	IO-Link output data of the sensor/actor connected to Port 7. For a description of the data,see manual of the manufacturer of the used sensor/actor.
242	1 byte	IO-Link Port 8 data status	0: IO-Link Port 8 input data not valid. 1-255: IO-Link Port 8 input data valid.	IO-Link Port 8 Output enable	0: IO-Link Port 8 output data not valid. 1-255: IO-Link Port 8 output data valid.
243	1 byte	Padding byte	Do not use	Padding byte	Do not use
244 …275	32 bytes	IO-Link port 8 process input data	IO-Link input data of the sensor/actor connected to Port 8. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 8 process output data	IO-Link output data of the sensor/actor connected to Port 8. For a description of the data,see manual of the manufacturer of the used sensor/actor.

7.2. Connections 5 – 7

The following table describes the structure of the input and output process data and is valid for connection 5, connection 6, connection 7.

Table 48: Connections 5-7 Detail

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
0	1 byte	DI status	Reserved	DO status	Reserved
1	1 byte	Padding byte	Do not use	Padding byte	Do not use
2 … 3	2 bytes	DI data	Reserved	DO data	Reserved
4	1 byte	IO-Link Port 1 data status	0: IO-Link Port 1 input data notvalid. 1-255: IO-Link Port 1 input data valid.	IO-Link Port 1 Output enable	0: IO-Link Port 1 output data not valid. 1-255: IO-Link Port 1 output data valid.
5	1 byte	Padding byte	Do not use	Padding byte	Do not use
6 … 21	16 bytes	IO-Link port 1 process input data	IO-Link input data of the sensor/actor connected to Port 1. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 1 process output data	IO-Link output data of the sensor/actor connected to Port 1. For a description of the data,see manual of the manufacturer of the used sensor/actor.
22	1 byte	IO-Link Port 2 data status	0: IO-Link Port 2 input data not valid. 1-255: IO-Link Port 2 input data valid.	IO-Link Port 2 Output enable	0: IO-Link Port 2 output data not valid. 1-255: IO-Link Port 2 output data valid.
23	1 byte	Padding byte	Do not use	Padding byte	Do not use
24 … 39	16 bytes	IO-Link port 2 process input data	IO-Link input data of the sensor/actor connected to Port 2. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 2 process output data	IO-Link output data of the sensor/actor connected to Port 2. For a description of the data,see manual of the manufacturer of the used sensor/actor.
40	1 byte	IO-Link Port 3 data status	0: IO-Link Port 3 input data not valid. 1-255: IO-Link Port 3 input data valid.	IO-Link Port 3 Output enable	0: IO-Link Port 3 output data not valid. 1-255: IO-Link Port 3 output data valid.
41	1 byte	Padding byte	Do not use	Padding byte	Do not use

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
42 … 57	16 bytes	IO-Link port 3 process input data	IO-Link input data of the sensor/actor connected to Port 3. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 3 process output data	IO-Link output data of the sensor/actor connected to Port 3. For a description of the data,see manual of the manufacturer of the used sensor/actor.
58	1 byte	IO-Link Port 4 data status	0: IO-Link Port 4 input data notvalid. 1-255: IO-Link Port 4 input data valid.	IO-Link Port 4 Output enable	0: IO-Link Port 4 output data not valid. 1-255: IO-Link Port 4 output data valid.
59	1 byte	Padding byte	Do not use	Padding byte	Do not use
60 … 75	16 bytes	IO-Link port 4 process input data	IO-Link input data of the sensor/actor connected to Port 4. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 4 process output data	IO-Link output data of the sensor/actor connected to Port 4. For a description of the data,see manual of the manufacturer of theused sensor/actor.
76	1 byte	IO-Link Port 5 data status	0: IO-Link Port 5 input data not valid. 1-255: IO-Link Port 5 input data valid.	IO-Link Port 5 Output enable	0: IO-Link Port 5 output data not valid. 1-255: IO-Link Port 5 output data valid.
77	1 byte	Padding byte	Do not use	Padding byte	Do not use
78 … 93	16 bytes	IO-Link port 5 process input data	IO-Link input data of the sensor/actor connected to Port 5. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 5 process output data	IO-Link output data of the sensor/actor connected to Port 5. For a description of the data,see manual of the manufacturer of the used sensor/actor.
94	1 byte	IO-Link Port 6 data status	0: IO-Link Port 6 input data notvalid. 1-255: IO-Link Port 6 input data valid.	IO-Link Port 6 Output enable	0: IO-Link Port 6 output data not valid. 1-255: IO-Link Port 6 output data valid.
95	1 byte	Padding byte	Do not use	Padding byte	Do not use
96 … 111	16 bytes	IO-Link port 6 process inputdata	IO-Link input data of the sensor/actor connected to Port 6. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 6 process output data	IO-Link output data of the sensor/actor connected to Port 6. For a description of the data,see manual of the manufacturer of the used sensor/actor.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
112	1 byte	IO-Link Port 7 data status	0: IO-Link Port 7 input data notvalid. 1-255: IO-Link Port 7 input data valid.	IO-Link Port 7 Output enable	0: IO-Link Port 7 output data not valid. 1-255: IO-Link Port 7 output data valid.
113	1 byte	Padding byte	Do not use	Padding byte	Do not use
114 …129	16 bytes	IO-Link port 7 process input data	IO-Link input data of the sensor/actor connected to Port 7. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 7 process output data	IO-Link output data of the sensor/actor connected to Port 7. For a description of the data,see manual of the manufacturer of the used sensor/actor.
130	1 byte	IO-Link Port 8 data status	0: IO-Link Port 8 input data notvalid. 1-255: IO-Link Port 8 input data valid.	IO-Link Port 8 Output enable	0: IO-Link Port 8 output data not valid. 1-255: IO-Link Port 8 output data valid.
131	1 byte	Padding byte	Do not use	Padding byte	Do not use
132 …147	16 bytes	IO-Link port 8 process input data	IO-Link input data of the sensor/actor connected to Port 8. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 8 process output data	IO-Link output data of the sensor/actor connected to Port 8. For a description of the data,see manual of the manufacturer of the used sensor/actor.
148	1 byte	IO-Link Port 9 data status	0: IO-Link Port 9 input data notvalid. 1-255: IO-Link Port 9 input data valid.	IO-Link Port 9 Output enable	0: IO-Link Port 9 output data not valid. 1-255: IO-Link Port 9 output data valid.
149	1 byte	Padding byte	Do not use	Padding byte	Do not use
150 …165	16 bytes	IO-Link port 9 process input data	IO-Link input data of the sensor/actor connected to Port 9. For a description of the data, see manual of the manufacturerof the used sensor/actor.	IO-Link port 9 process output data	IO-Link output data of the sensor/actor connected to Port 9. For a description of the data, see manual of the manufacturer of the used sensor/actor.
166	1 byte	IO-Link Port 10 data status	0: IO-Link Port 10 input data not valid. 1-255: IO-Link Port 10 input data valid.	IO-Link Port 10 Output enable	0: IO-Link Port 10 output data not valid. 1-255: IO-Link Port 10 outputdata valid.
167	1 byte	Padding byte	Do not use	Padding byte	Do not use

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
168 …183	16 bytes	IO-Link port 10 process input data	IO-Link input data of the sensor/actor connected to Port 10. For a description of thedata, see manual of the manufacturer of the used sensor/actor.	IO-Link port 10 process output data	IO-Link output data of the sensor/actor connected to Port 10. For a description of thedata, see manual of themanufacturer of the used sensor/actor.
184	1 byte	IO-Link Port 11 data status	0: IO-Link Port 11 input data not valid. 1-255: IO-Link Port 11 input data valid.	IO-Link Port 11 Output enable	0: IO-Link Port 11 output data not valid. 1-255:IO-Link Port 11 outputdata valid.
185	1 byte	Padding byte	Do not use	Padding byte	Do not use
186 …201	16 bytes	IO-Link port 11 process input data	IO-Link input data of the sensor/actor connected to Port 11. For a description of thedata, see manual of the manufacturer of the used sensor/actor.	IO-Link port 11 process output data	IO-Link output data of the sensor/actor connected to Port 11. For a description of thedata, see manual of the manufacturer of the used sensor/actor.
202	1 byte	IO-Link Port 12 data status	0: IO-Link Port 12 input data not valid. 1-255: IO-Link Port 12 input data valid.	IO-Link Port 12 Output enable	0: IO-Link Port 12 output data not valid. 1-255: IO-Link Port 12 outputdata valid.
203	1 byte	Padding byte	Do not use	Padding byte	Do not use
204 …219	16 bytes	IO-Link port 12 process input data	IO-Link input data of the sensor/actor connected to Port 12. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 12 process output data	IO-Link output data of the sensor/actor connected to Port 12. For a description of the data, see manual of themanufacturer of the used sensor/actor.
220	1 byte	IO-Link Port 13 data status	0: IO-Link Port 13 input data not valid. 1-255: IO-Link Port 13 input data valid.	IO-Link Port 13 Output enable	0: IO-Link Port 13 output data not valid. 1-255: IO-Link Port 13 outputdata valid.
221	1 byte	Padding byte	Do not use	Padding byte	Do not use
222 …237	16 bytes	IO-Link port 13 process input data	IO-Link input data of the sensor/actor connected to Port 13. For a description of thedata, see manual of the manufacturer of the used sensor/actor.	IO-Link port 13 process output data	IO-Link output data of the sensor/actor connected to Port 13. For a description of thedata, see manual of the manufacturer of the used sensor/actor.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
238	1 byte	IO-Link Port 14 data status	0: IO-Link Port 14 input data not valid. 1-255: IO-Link Port 14 input data valid.	IO-Link Port 14 Output enable	0: IO-Link Port 14 output data not valid. 1-255: IO-Link Port 14 outputdata valid.
239	1 byte	Padding byte	Do not use	Padding byte	Do not use
240 …255	16 bytes	IO-Link port 14 process input data	IO-Link input data of the sensor/actor connected to Port 14. For a description of thedata, see manual of the manufacturer of the used sensor/actor.	IO-Link port 14 process output data	IO-Link output data of the sensor/actor connected to Port 14. For a description of thedata, see manual of themanufacturer of the used sensor/actor.
256	1 byte	IO-Link Port 15 data status	0: IO-Link Port 15 input data not valid. 1-255: IO-Link Port 15 input data valid.	IO-Link Port 15 Output enable	0: IO-Link Port 15 output data not valid. 1-255: IO-Link Port 15 outputdata valid.
257	1 byte	Padding byte	Do not use	Padding byte	Do not use
258 …273	16 bytes	IO-Link port 15 process input data	IO-Link input data of the sensor/actor connected to Port 15. For a description of thedata, see manual of the manufacturer of the used sensor/actor.	IO-Link port 15 process output data	IO-Link output data of the sensor/actor connected to Port 15. For a description of thedata, see manual of themanufacturer of the used sensor/actor.
274	1 byte	IO-Link Port 16 data status	0: IO-Link Port 16 input data not valid. 1-255: IO-Link Port 16 input data valid.	IO-Link Port 16 Output enable	0: IO-Link Port 16 output data not valid. 1-255: IO-Link Port 16 outputdata valid.
275	1 byte	Padding byte	Do not use	Padding byte	Do not use
276 …291	16 bytes	IO-Link port 16 process input data	IO-Link input data of the sensor/actor connected to Port 16. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 16 process output data	IO-Link output data of the sensor/actor connected to Port 16. For a description of thedata, see manual of the manufacturer of the used sensor/actor.

7.3. Connections 8 - 10

The following table describes the structure of the input and output process data and is valid for connection 8, connection 9, connection 10.

Table 49: Connections 8-10 Detail

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
0	1 byte	DI status	Reserved	DO status	Reserved
1	1 byte	Padding byte	Do not use	Padding byte	Do not use
2 … 3	2 bytes	DI data	Reserved	DO data	Reserved
4	1 byte	IO-Link Port 1 data status	0: IO-Link Port 1 input data not valid. 1-255: IO-Link Port 1 input data valid.	IO-Link Port 1 Output enable	0: IO-Link Port 1 output data not valid. 1-255: IO-Link Port 1 output data valid.
5	1 byte	Padding byte	Do not use	Padding byte	Do not use
6 … 9	4 bytes	IO-Link port 1 process input data	IO-Link input data of the sensor/actor connected to Port 1. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 1 process output data	IO-Link output data of the sensor/actor connected to Port 1. For a description of the data, see manual of the manufacturer of the used sensor/actor.
10	1 byte	IO-Link Port 2 data status	0: IO-Link Port 2 input data not valid. 1-255: IO-Link Port 2 input data valid.	IO-Link Port 2 Output enable	0: IO-Link Port 2 output data not valid. 1-255: IO-Link Port 2 output data valid.
11	1 byte	Padding byte	Do not use	Padding byte	Do not use
12 … 14	4 bytes	IO-Link port 2 process input data	IO-Link input data of the sensor/actor connected to Port 2. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 2 process output data	IO-Link output data of the sensor/actor connected to Port 2. For a description of the data, see manual of the manufacturer of the used sensor/actor.
15	1 byte	IO-Link Port 3 data status	0: IO-Link Port 3 input data not valid. 1-255: IO-Link Port 3 input data valid.	IO-Link Port 3 Output enable	0: IO-Link Port 3 output data not valid. 1-255: IO-Link Port 3 output data valid.
16	1 byte	Padding byte	Do not use	Padding byte	Do not use

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
17 … 22	4 bytes	IO-Link port 3 process input data	IO-Link input data of the sensor/actor connected to Port 3. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 3 process output data	IO-Link output data of the sensor/actor connected to Port 3. For a description of the data, see manual of the manufacturer of the used sensor/actor.
18	1 byte	IO-Link Port 4 data status	0: IO-Link Port 4 input data not valid. 1-255: IO-Link Port 4 input data valid.	IO-Link Port 4 Output enable	0: IO-Link Port 4 output data not valid. 1-255: IO-Link Port 4 output data valid.
19	1 byte	Padding byte	Do not use	Padding byte	Do not use
20 … 28	4 bytes	IO-Link port 4 process input data	IO-Link input data of the sensor/actor connected to Port 4. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 4 process output data	IO-Link output data of the sensor/actor connected to Port 4. For a description of the data, see manual of the manufacturer of the used sensor/actor.
29	1 byte	IO-Link Port 5 data status	0: IO-Link Port 5 input data not valid. 1-255: IO-Link Port 5 input data valid.	IO-Link Port 5 Output enable	0: IO-Link Port 5 output data not valid. 1-255: IO-Link Port 5 output data valid.
30	1 byte	Padding byte	Do not use	Padding byte	Do not use
31 … 34	4 bytes	IO-Link port 5 process input data	IO-Link input data of the sensor/actor connected to Port 5. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 5 process output data	IO-Link output data of the sensor/actor connected to Port 5. For a description of the data, see manual of the manufacturer of the used sensor/actor.
35	1 byte	IO-Link Port 6 data status	0: IO-Link Port 6 input data not valid. 1-255: IO-Link Port 6 input data valid.	IO-Link Port 6 Output enable	0: IO-Link Port 6 output data not valid. 1-255: IO-Link Port 6 output data valid.
36	1 byte	Padding byte	Do not use	Padding byte	Do not use
37… 40	4 bytes	IO-Link port 6 process input data	IO-Link input data of the sensor/actor connected to Port 6. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 6 process output data	IO-Link output data of the sensor/actor connected to Port 6. For a description of the data, see manual of the manufacturer of the used sensor/actor.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
38	1 byte	IO-Link Port 7 data status	0: IO-Link Port 7 input data not valid. 1-255: IO-Link Port 7 input data valid.	IO-Link Port 7 Output enable	0: IO-Link Port 7 output data not valid. 1-255: IO-Link Port 7 output data valid.
39	1 byte	Padding byte	Do not use	Padding byte	Do not use
40 … 46	4 bytes	IO-Link port 7 process input data	IO-Link input data of the sensor/actor connected to Port 7. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 7 process output data	IO-Link output data of the sensor/actor connected to Port 7. For a description of the data, see manual of the manufacturer of the used sensor/actor.
47	1 byte	IO-Link Port 8 data status	0: IO-Link Port 8 input data not valid. 1-255: IO-Link Port 8 input data valid.	IO-Link Port 8 Output enable	0: IO-Link Port 8 output data not valid. 1-255: IO-Link Port 8 output data valid.
48	1 byte	Padding byte	Do not use	Padding byte	Do not use
49 … 52	4 bytes	IO-Link port 8 process input data	IO-Link input data of the sensor/actor connected to Port 8. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 8 process output data	IO-Link output data of the sensor/actor connected to Port 8. For a description of the data, see manual of the manufacturer of the used sensor/actor.
53	1 byte	IO-Link Port 9 data status	0: IO-Link Port 9 input data not valid. 1-255: IO-Link Port 9 input data valid.	IO-Link Port 9 Output enable	0: IO-Link Port 9 output data not valid. 1-255: IO-Link Port 9 output data valid.
54	1 byte	Padding byte	Do not use	Padding byte	Do not use
55 … 58	4 bytes	IO-Link port 9 process input data	IO-Link input data of the sensor/actor connected to Port 9. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 9 process output data	IO-Link output data of the sensor/actor connected to Port 9. For a description of the data, see manual of the manufacturer of the used sensor/actor.
59	1 byte	IO-Link Port 10 data status	0: IO-Link Port 10 input data not valid. 1-255: IO-Link Port 10 input data valid.	IO-Link Port 10 Output enable	0: IO-Link Port 10 output data not valid. 1-255: IO-Link Port 10 output data valid.
60	1 byte	Padding byte	Do not use	Padding byte	Do not use

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
61 … 64	4 bytes	IO-Link port 10 process input data	IO-Link input data of the sensor/actor connected to Port 10. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 10 process output data	IO-Link output data of the sensor/actor connected to Port 10. For a description of the data, see manual of the manufacturer of the used sensor/actor.
65	1 byte	IO-Link Port 11 data status	0: IO-Link Port 11 input data not valid. 1-255: IO-Link Port 11 input data valid.	IO-Link Port 11 Output enable	0: IO-Link Port 11 output data not valid. 1-255: IO-Link Port 11 output data valid.
66	1 byte	Padding byte	Do not use	Padding byte	Do not use
67 … 70	4 bytes	IO-Link port 11 process input data	IO-Link input data of the sensor/actor connected to Port 11. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 11 process output data	IO-Link output data of the sensor/actor connected to Port 11. For a description of the data, see manual of the manufacturer of the used sensor/actor.
71	1 byte	IO-Link Port 12 data status	0: IO-Link Port 12 input data not valid. 1-255: IO-Link Port 12 input data valid.	IO-Link Port 12 Output enable	0: IO-Link Port 12 output data not valid. 1-255: IO-Link Port 12 output data valid.
72	1 byte	Padding byte	Do not use	Padding byte	Do not use
73 … 76	4 bytes	IO-Link port 12 process input data	IO-Link input data of the sensor/actor connected to Port 12. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 12 process output data	IO-Link output data of the sensor/actor connected to Port 12. For a description of the data, see manual of the manufacturer of the used sensor/actor.
77	1 byte	IO-Link Port 13 data status	0: IO-Link Port 13 input data not valid. 1-255: IO-Link Port 13 input data valid.	IO-Link Port 13 Output enable	0: IO-Link Port 13 output data not valid. 1-255: IO-Link Port 13 output data valid.
78	1 byte	Padding byte	Do not use	Padding byte	Do not use
79 … 82	4 bytes	IO-Link port 13 process input data	IO-Link input data of the sensor/actor connected to Port 13. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 13 process output data	IO-Link output data of the sensor/actor connected to Port 13. For a description of the data, see manual of the manufacturer of the used sensor/actor.

Byte	No of Bytes	Input Process Data	Input Process Data Description	Output Process Data	Output Process Data Description
83	1 byte	IO-Link Port 14 data status	0: IO-Link Port 14 input data not valid. 1-255: IO-Link Port 14 input data valid.	IO-Link Port 14 Output enable	0: IO-Link Port 14 output data not valid. 1-255: IO-Link Port 14 output data valid.
84	1 byte	Padding byte	Do not use	Padding byte	Do not use
85 … 88	4 bytes	IO-Link port 14 process input data	IO-Link input data of the sensor/actor connected to Port 14. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 14 process output data	IO-Link output data of the sensor/actor connected to Port 14. For a description of the data, see manual of the manufacturer of the used sensor/actor.
89	1 byte	IO-Link Port 15 data status	0: IO-Link Port 15 input data not valid. 1-255: IO-Link Port 15 input data valid.	IO-Link Port 15 Output enable	0: IO-Link Port 15 output data not valid. 1-255: IO-Link Port 15 output data valid.
90	1 byte	Padding byte	Do not use	Padding byte	Do not use
91 … 94	4 bytes	IO-Link port 15 process input data	IO-Link input data of the sensor/actor connected to Port 15. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 15 process output data	IO-Link output data of the sensor/actor connected to Port 15. For a description of the data, see manual of the manufacturer of the used sensor/actor.
95	1 byte	IO-Link Port 16 data status	0: IO-Link Port 16 input data not valid. 1-255: IO-Link Port 16 input data valid.	IO-Link Port 16 Output enable	0: IO-Link Port 16 output data not valid. 1-255: IO-Link Port 16 output data valid.
96	1 byte	Padding byte	Do not use	Padding byte	Do not use
97 … 100	4 bytes	IO-Link port 16 process input data	IO-Link input data of the sensor/actor connected to Port 16. For a description of the data, see manual of the manufacturer of the used sensor/actor.	IO-Link port 16 process output data	IO-Link output data of the sensor/actor connected to Port 16. For a description of the data, see manual of the manufacturer of the used sensor/actor.

8. OPC UA Server Connection

The TigoMaster 2TH contains an OPC UA server, to which an OPC UA client can connect. The client can then access the following parameters:

- TigoMaster 2TH identification parameters
- Sensor/Actuator identification parameters

The OPC UA client connects via the following URL: **opc.tcp://IP address:4840**, wherein **IP address** is the IP address of the TigoMaster 2TH.

The OPC UA client can access parameters anonymously (read only) or with a username and password (read and write). The username and password are set by means of TigoEngine or the Integrated Web Server.

8.1. TigoMaster 2TH Identification

The TigoMaster 2TH includes nodes for its identification: for example, the OPC UA client can read the version of the TigoMaster 2TH firmware in the SoftwareRevision node (node path: **Root** > **Objects** > **DeviceSet** > **[Device Name]** > **ParameterSet** > **SoftwareRevision**).

Error! Reference source not found. shows the path to the nodes, and Table details the nodes.

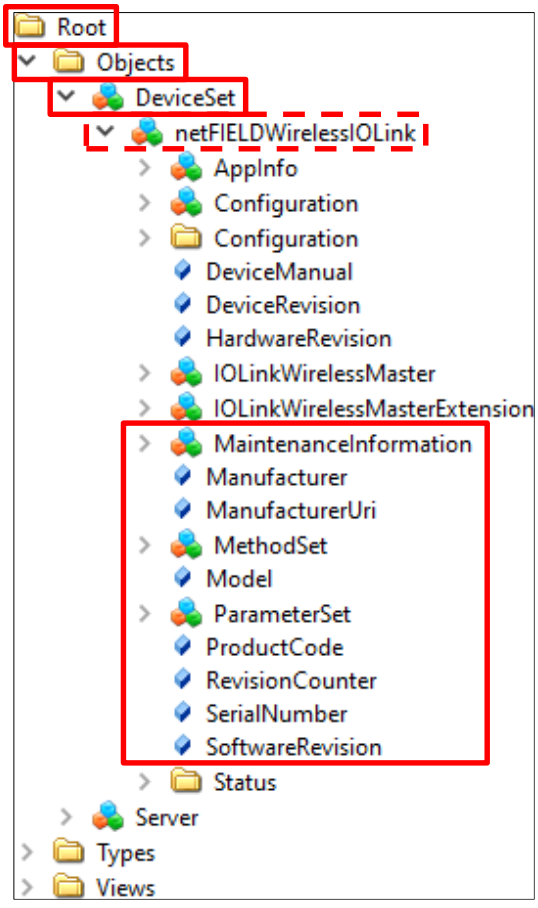


Figure 69: Path to TigoMaster 2TH Identification Nodes

Table 50: Device Identification Nodes

Node Name	Node Class	Access	Description
Manufacturer	Variable	Read	Device manufacturer
ManufacturerUri	Variable	Read	URL of the device manufacturer
Model	Variable	Read	Model name of the device
ProductCode	Variable	Read	Product code of the device
RevisionCounter	Variable	Read	Hardware revision of the device
SerialNumber	Variable	Read	Serial number of the device
SoftwareRevision	Variable	Read	Revision/version of the device firmware

8.2. Sensor/Actuator Identification

The TigoMaster 2TH includes nodes for the identification of connected sensors/actuators: for example, the OPC UA client can read the version of a sensor/actuator's firmware in the SoftwareRevision node (node path: **Root** > **Object** > **DeviceSet** > **[Device Name]** > **IOLinkWirelessMaster** > **PortXX** > **Device**).

Table 51: Sensor/Actuator Identification Nodes

Node Name	Node Class	Access	Description
Manufacturer	Variable	Read	Device manufacturer
MinCycleTime	Variable	Read	Minimum cycle time
Model	Variable	Read	Model name
RevisionID	Variable	Read	Hardware revision
SerialNumber	Variable	Read	Serial number
SoftwareRevision	Variable	Read	Revision/version of the firmware
VendorID	Variable	Read	Vendor identification

8.3. NTP Client Configuration

The OPC UA server provides nodes for configuring the NTP client. Each node is detailed in

Table 12, and the path to the nodes is: **Root > Object > DeviceSet > [Device Name] > Configuration > NtpClient > Configuration > CurrentConfiguration**.

Table 12: OPC UA Server Nodes for Configuring NTP Client

Node name	Node Class	Access	Default	Description
NtpClientServerIpAddress	Variable	Read/Write	0	IP address of the NTP server. The NTP client uses the set IP address to get the date and time from an NTP server. The IP address must be converted into a decimal number. The value 0 disables the function.
NtpClientServerIpAddressFallback	Variable	Read/Write	0	Fallback IP address of the NTP server. This is an optional additional IP address that will be used to reach the NTP server if it cannot be reached via the IP address in the NtpClientServerIpAddress node The IP address must be converted into a decimal number. The value 0 disables the function.
NtpClientUpdateConfiguration	Method	Write	-	Method for writing the nodes NtpClientServerIpAddress and NtpClientServerIpAddressFallback.

8.4. Convert an IP Address to a Decimal Number

A typical IP address (for example, 192.53.103.108) is composed of 4 segments, which are separated from each other by a period. To convert an IP address to a decimal number, each segment is inserted into a specific place in the conversion formula below, where the letters A, B, C, D are the placeholders for the 4 segments (in our example, A is the placeholder for 192, B is the placeholder for 53, C is the placeholder for 103, and D is the placeholder for 108).

The conversion formula is:
((A * 256 + B) * 256 + C) * 256 + D = IP address as a decimal number

Inserting our example IP address into the formula gives the following:
((192 * 256 + 53) * 256 + 103) * 256 + 108 = 3224725356

The decimal number for our example IP address is 3224725356.

8.5. Wireless Connection

Wireless connection is determined by frequency and time. Each wireless track supports 8 time slots.

Each connected W-Device (sensor/actuator) can occupy a single slot (SSlot) or a double slot (DSlot).

- SSlot supports 1 byte of PDIn per cycle time.
- DSlot supports up to 14 bytes of PDIn per cycle time.

If the PDIn size exceeds the slot type maximum size, then PDIn will be transmitted in segments, thereby resulting in longer latency.

Table shows an example of track and **double** slot configuration for an IO-Link wireless device, and Table shows an example of track and **single** slot configuration.

If the slot type is DSlot, then the slot value must be an even number.
If the slot type is SSlot, then the slot value must be an odd number.

Table 53: Track and Slot (Double-Slot)

Track	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7
0	W-Device with DSlot	Free	Free	Free	Free	Free	Free	Free
1	Free	Free	Free	Free	Free	Free	Free	Free

Table 54: Track and Slot (Single-Slot)

Track	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7
0	W-Device with SSlot	Free	Free	Free	Free	Free	Free	Free
1	Free	Free	Free	Free	Free	Free	Free	Free

9. Status and Diagnosis

9.1. TigoMaster 2TH

See section 3.2.5 of this User Manual for details of LED indications.

9.2. EtherNet/IP

TigoMaster 2TH contains the Event Log object with information about IO-Link events. The PLC can read attributes of the object to get the “Event Qualifier” and “Event Code” of an IO-Link Event.

Each IO-Link port has an assigned CIP instance. The Event Log Object contains information on IO-Link events.

Instance 0 (Class Attributes)

Table 55: Class Attributes Event Log Object 65 (0x41)

Attribute	Name	NV	Access	Data Type	Description	Default
1	Revision	NV	Get	UINT	Revision of this object	1
2	Max. Instance	NV	Get	UINT	Number of IO-Link ports	1 – 8
32	Time Format	NV	Get	USINT	Data type code of time format. Only data type STIME is supported.	204 (0xCC) = STIME
33	Present Time	NV	Get	STIME	Default for time value. Applies to all instances.	0

Instances 100, 101 … (Instance Attributes)

The following table shows the mapping of CIP instances to the IO-Link ports.

Table 56: Mapping CIP Instances to IO-Link Ports

IO Link Port	CIP Instance
1	100
2	101
3	102

The following table describes the attributes of the instances 100, 101.

Table 57: Instance Attributes Event Log Object 65 (0x41)

Attribute	Name	NV	Access	Data Type	Description	Default
2	State	V	Get	USINT	Status of this instance: • 0: Nonexistent • 1: Stopped • 2: Empty • 3: Available • 4: Full/Overwrite • 5: Full/Halted • 6–255: Reserved	-
9	Logged Data Config	NV	Get, Set	BYTE	Configures which data is stored in the eventlog. • Bit 0 = 0: Enter event without time value • Bit 0 = 1: Enter event with time value • Bit 1 – 7: Reserved (always 0).	0
10	Log Full Action	NV	Get, Set	USINT	Configures the action to take when a new event is detected and the log is full. • 0: Halt • 1: Scroll • 2 – 255: Reserved	1
11	Duplicate Event Action	NV	Get, Set	USINT	Configures the action to take when aDuplicate Event is detected. • 0: Ignore • 1: Add • 2 – 255: Reserved	1
12	Event/Data Log Maximum Size	V	Get	UDINT	Max. number of allowable entries in the Event/ Data Log.	8

Attribute	Name	NV	Access	Data Type	Description	Default
13	Event/Data Log Size	V	Get	UDINT	The present number of entries in the Event/Data Log. Values: 0 to max. (= value of attribute 12).	0
14	Event/Data Log	V	Get Get Member Remove Member	ARRAY of STRUCT	List of all events that have been logged. A log entry contains the IO-Link Event Qualifier (USINT) and the IO-Link EventCode (UINT). Attribute 9 determines whether the log entry also gets a time stamp (STIME). The structure of a log entry is described below.	0
19	Log Full	V	Get	BOOL	Log full? • False: Log not full • True: Log full	False
20	Log Contains Entries	V	Get	BOOL	Log contains entries? • False: Log is empty. • True: Log contains events.	False
21	Log Overrun	V	Get	BOOL	Log overrun? • False: No Log Overrun • True: LogOverrun	False
22	Sequential Event/Data Access	V	Get	STRUCT	Simple read access to Event/Data entries. • If one or several entries are available in thelog, Get_Attribute_Single will read the first entry which will then be removed from the Event Log. • If there is no entry in the Event Log, Get_Attribute_Single will not deliver any data.	-

Attribute	Name	NV	Access	Data Type	Description	Default
24	Event Identifier Format	NV	Get, Set	USINT	Format of a log entry • 0 – 3: Reserved. • 4: 24 Bit in the format USINT + UINT • 5 – 255: Reserved.	4

Log Entry Structure

The value of attribute 9 determines the structure of a log entry.

Table 58: Log Entry Structure

Structure of a Log Entry	Description
USINT	IO-Link Event Qualifier, always available.
UINT	IO-Link Event Code, always available.
STIME	System time. The system time is available only if attribute 9 bit 0 = 1.

Services

Table 59: Services Event Log Object 65 (0x41)

Service Code	Service Name	Class Level	Instance Level	Description
0x05	Reset	-	Yes	Reset
0x0E	Get Attribute Single	Yes	Yes	Read an attribute
0x10	Set Attribute Single	-	Yes	Write an attribute
0x18	Get Member	-	Yes	Read a log entry
0x1B	Remove Member	-	Yes	Remove a log entry

9.3. IO-Link Diagnosis

9.3.1. Event Qualifier

The event qualifier is bit-coded information about the event.

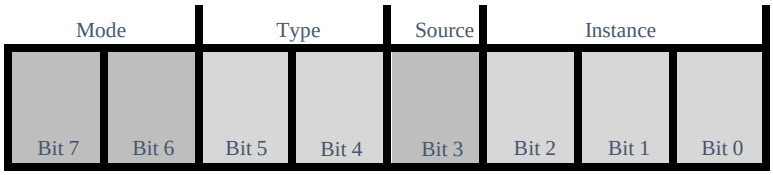


Figure 70: Event Qualifier

Table 60: Event Qualifier

Bit	Name	Description
Bit 6–7	Mode	0: Reserved 1: Event single shot 2: Event disappears 3: Event appears
Bit 4–5	Type	0: Reserved 1: Notification 2: Warning 3: Error
Bit 3	Source	0: Device (remote) 1: Master/Port
Bit 0–2	Instance	0: Unknown 1–3: Reserved 4: Application 5–7: Reserved

9.3.2. IO-Link Wireless Master Event Codes

Table 61: Master Event Codes

Event Code	Description	Type	Remedy
0x0000	No malfunction	Notification	No action required
0xFF21	Communication to Wireless Device (IO-Link Device is connected to Bridge)	Event	No action required
0xFF22	Communication loss to IO-Link Device (IO-Link Device is disconnected from TigoBridge)	Error	Check connection from IO-Link Device to the TigoBridge
0xFFB1	Max Retry error, indicating a packet loss The W-Master cannot create a message to the W-Device after MaxRetry attempts. This error indicates that one packet failed to be transmitted successfully. This can be, for example, the result of a noisy environment (RF-wise). It affects the PER of the system.	Error	If the PER is too high, check the system configuration (ranges, operating channels, etc.).
0xFFB2	IMA timeout The W-Master did not receive a message from the connected W-Device within the IMA timeout. This error indicates that the IOLW connection failed. Possibly this leads to Communication Loss 0xFF22.	Error	Check connection from IO-Link Device to TigoBridge

9.3.3. IO-Link Device Event Codes (Common)

The following table lists standard IO-Link Device Event Codes. For device-specific Event Codes or remedies, use the manual of the relevant IO-Link Device.

Table 62: IO-Link Device Event Codes

Event Code	Description	Type	Remedy (Common)
0x0000	No malfunction	Notification	No action required
0x1000	General malfunction (unknown error)	Error	See manual of the relevant IO-LinkDevice
0x1800 – 0x18FF	Vendor-specific	-	See manual of the relevant IO-LinkDevice
0x4000	Temperature fault – overload	Error	Check temperature, find source of overload
0x4210	Device temperature overrun	Warning	Clear source of heat

Event Code	Description	Type	Remedy (Common)
0x4220	Device temperature underrun	Warning	Insulate IO-Link Device
0x5000	Device hardware fault	Error	Exchange IO-Link Device
0x5010	Component malfunction	Error	Repair or exchange
0x5011	Non-volatile memory loss	Error	Check batteries
0x5012	Batteries low	Warning	Exchange batteries
0x5013	HMI button pressed	Notification	No action required
0x5100	General power supply fault	Error	Check availability of power supply
0x5101	Fuse blown/open	Error	Exchange fuse
0x5110	Primary supply voltage overrun	Warning	Check tolerance of 1L+ voltage
0x5111	Primary supply voltage underrun	Warning	Check tolerance of 1L+ voltage
0x5112	Secondary supply voltage fault (Port Class B)	Warning	Check tolerance of 1L+ voltage
0x6000	Device software fault	Error	Check firmware revision
0x6320	Parameter error	Error	Check data sheet and values
0x6321	Parameter missing	Error	Check data sheet
0x6350	Parameter changed	Error	Check configuration
0x7700	Wire break of a subordinate device	Error	Check installation
0x7701 – 0x770F	Wire break of subordinate device 1–device 15	Error	Check installation
0x7710	Short circuit	Error	Check installation
0x7711	Ground fault	Error	Check installation
0x8C00	Technology-specific application fault	Error	Reset Device
0x8C01	Simulation active	Warning	Check operational mode
0x8C10	Process variable range overrun – Process Data uncertain	Warning	Check configuration of device
0x8C20	Measurement range exceeded	Error	Check application
0x8C30	Process variable range underrun – Process Data uncertain	Warning	Check configuration of device
0x8C40	Maintenance required	Warning	Clean

Event Code	Description	Type	Remedy (Common)
0x8C41	Maintenance required	Warning	Refill
0x8C42	Maintenance required	Warning	Exchange wear and tear parts
0x8CA0 – 0x8DFF	Vendor-specific	-	See manual of the relevant IO-LinkDevice
0xB000 – 0xB0FF	Safety extensions	-	See manual of the relevant IO-LinkDevice
0xB100 – 0xBFFF	Profile-specific	-	See manual of the relevant IO-LinkDevice
0xFF91	Internal Data Storage upload request	Notification (single shot)	See manual of the relevant IO-LinkDevice
0xFFB9	Retry error	Error	See manual of the relevant IO-LinkDevice
Any other code	Reserved	-	See manual of the relevant IO-LinkDevice

10. Technical Data

10.1. Product Specifications

Table 63: Product Specifications

Category	Parameter	Value		
Product	Part number	1912.122		
	Product name	TigoMaster 2TH		
	Description	TigoMaster 2TH EtherNet/IP IO-Link Wireless Master		
	Function	• IO-Link Master Wireless for EtherNet/IP • 2 tracks, 16 channels • Connector/housing: 30 mm		
Communication controller	Type	netX 90		
Integrated memory	RAM	16 MB SDRAM		
	FLASH	8 MB		
EtherNet communication	Real-Time EtherNet	EtherNet/IP Adapter		
EtherNet interface	Interface type	100BASE-TX, 10BASE-T, isolated		
	Auto-negotiation, Auto-crossover	Yes		
	Connectors	• X31: EtherNet interface, M12, D-coded, EtherNet /IP port 1 • X32: EtherNet interface, M12, D-coded, EtherNet /IP port 2		
IO-Link	Radio	2 track = 16 IO-Link wireless salves, 3 antennas, 16 LEDs		
LEDs	System and application	SYS	System status	**Green**/**Yellow**
		APL	Application status	**Red**/**Green**
	Power supply	1L (X22)	1L power supply (DC 24 V)	**Red**/**Green**
		2L (X22)	2L power supply (DC 24 V)	**Red**/**Green**
	EtherNet/IP communication	MS	Module status	**Red**/**Green**
		NS	Network status	**Red**/**Green**

Category	Parameter	Value		
(LEDS continued)	EtherNet	LINK (X31)	Link status, connector X31	**Green**
		ACT (X31)	Activity status, connector X31	**Yellow**
		LINK (X32)	Link status, connector X32	**Green**
		ACT (X32)	Activity status, connector X32	**Yellow**
	Wireless tracks	WT01–WT03	IO-Link wireless track status antenna X1–X3	**Red**/**Yellow**/**Green**
	Wireless ports	WP01–WP08	Port status, IO-Link wireless device ports P01–P08	**Red**/**Yellow**/**Green**
		WP09–WP16	Port status, IO-Link wireless device ports P09–P16	**Red**/**Yellow**/**Green**
Power supply 1L, 2L	Voltage supply	24V DC, –25%/+30% (18 V DC … 31,2 V DC)		
	Under voltage warning	• 17.0 V (17.5 V -3%): ON • 18 V (17.5 V +3%): OFF		
	Over voltage warning	• 32.1 V (31.2 V +3%): ON • 30.3 V (31.2 V -3%): OFF		
	Power consumption (w/o DI/DO)	• 1L: 0.2 A (at 24 V DC) • 2L: 0.1 A (at 24 V DC)		
	Connectors	• X21: Power supply input (Power In), M12, L-Coded • X22: Power supply output (Power Out), M12, L-coded		
	Power consumption (power connectors)	Max. 16 A Max. current of the device including pass through must not exceed 16 A for 1L and 2L. Observe derating for the maximum current depending on the ambient temperature.		
	Reverse polarity protection	Yes		

Category	Parameter	Value
Ambient conditions	Operating temperature range	-25 °C to +70 °C
	Storage temperature range	-40 °C to +85 °C
	Max. temperature change	3 K / min
	Humidity	10–95% relative humidity, no condensation permitted
	Operating height	0–2000 m
	Over Voltage category	II (EN 60664-1)
Device	Dimensions (L x W x H)	200 x 30 x 20 mm
	Housing	Plastics
	Weight	212 g, with 3 antennas: 227 g
	Mounting/installation	Screw mounting with 2x M4 screws to the 2 mounting holes (1 x up and 1 x down). These screws make contact to FE (functional earth).
	Tightening torque	1.2 Nm
Conformance with EMC directives (preliminary)	CE sign	Yes
	Emission	EN 61000-6-4
	Radiated Emission	EN 55016-2-3
	Conducted emission	EN 55022
	Electromagnetic compatibility of multimedia equipment	EN 55032:2015
	Electromagnetic Compatibility (EMC) standard for radio equipment and services	EN 301489-1 V2.2.3
	Part 17: Specific conditions for Broadband DataTransmission Systems	EN 301489-17 V3.1.1 EN 301489-17 V3.2.4
	IMMUNITY	EN 61000-6-2:2019-11
	Electrostatic discharge (ESD) (air and contact discharge method)	EN 61000-4-2
	Radiated immunity	EN 61000-4-3

Category	Parameter	Value
	Fast transient interferences (Burst)	EN 61000-4-4
	Surge immunity	EN 61000-4-5
	Conducted immunity	EN 61000-4-6
	Wideband transmission systems	EN 300328 V2.2.2
	Audio/video, information and communication technology equipment - Part 1: Safety requirements	EN 62368-1:2014 + AC:2015
	RoHS	Compiled
Firmware download	Software to download and update the firmware	TigoEngine and CoreTigo Web Server
Configuration	Configuration software	TigoEngine, CoreTigo Web Server, PLC IDE
	Frequency Range	2400-2500 MHz
Electrical specifications	Max Gain	1.6 dBi
	Impedance	50Ω
	Polarization	Vertical
	Radiation	Omni
Mechanical specifications	Connector	Regular SMA-Male

Table 64: SMA Antenna Specifications

Category	Parameter	Value
Product data	Name	Wifi Antenna 2.4G rubber antenna
	Model	TLW2.5A-SMA-Male
	Type	Monopole whip antenna
	Manufacturer	Silram Technologies Ltd., Kfar Saba, Israel
Radio	Frequency Range	2400-2500 MHz
Electrical specifications	Max Gain	1.6 dBi
	Impedance	50Ω
	Polarization	Vertical
	Radiation	Omni

Category	Parameter	Value
Mechanical specifications	Connector	Regular SMA-Male
	Height	25.6 mm

10.2. EtherNet/IP Specifications

Table 65: Protocol Specifications

Parameter	Value
Connection 1 “Exclusive Owner - 32 bytes per IO-LinkPort with Config”	Input data: 276 bytes Output data: 276 bytes
Connection 2 “Exclusive Owner - 32 bytes per IO-LinkPort without Config”	
Connection 3 “Listen Only - 32 bytes per IO-Link”	Input data: 276 bytes Output data: 0 bytes
Connection 4 “Input Only - 32 bytes per IO-Link”	
Connection 5 “Exclusive Owner - 16 bytes per IO-LinkPort without Config”	Input data: 292 bytes Output data: 292 bytes
Connection 6 “Listen Only - 16 bytes per IO-Link”	Input data: 292 bytes Output data: 0 bytes
Connection 7 “Input Only - 16 bytes per IO-Link”	
Connection 8 “Exclusive Owner - 4 bytes per IO-LinkPort without Config”	Input data: 100 bytes Output data: 100 bytes
Connection 9 “Listen Only - 4 bytes per IO-Link”	Input data: 100 bytes Output data: 0 bytes
Connection 10 “Input Only - 4 bytes per IO-Link”	
I/O connection types (implicit)	• Exclusive Owner • Owner Input Only • Listen Only
I/O connection trigger type	Cyclic
Maximum number of I/O connections (class 1)	3
Maximum number of message connections (class 3)	6

Parameter	Value
Predefined standard objects	• Identity Object (0x01) • Message Router Object(0x02) • Assembly Object (0x04) • Connection Manager (0x06) • Event Log Object (0x41) • DLR Object (0x47) • QoS Object (0x48) • TCP/IP Interface Object (0xF5) • EtherNet Link Object (0xF6)
DHCP	Supported
BOOTP	Supported
Fixed IP address	Supported
Duplex mode	• Half duplex • Full duplex • Auto-negotiation
MDI mode	• MDI • MDI-X • Auto-MDIX
ACD (Address Conflict Detection)	Supported
Integrated switch	Supported
Reset services	CIP Reset services: • Identity Object • Reset ServicesType 0 and 1
Data transport layer	• EtherNet II • IEEE 802.3
Interface type	• 10BASE-T • 100BASE-TX • Isolated

10.3. OPC UA Server

Table 66: OPC UA Server Technical Data

Parameter	Description
OPC UA Server	According to IO-Link Companion Specification: http://opcfoundation.org/UA/IOLink/ Vendor-specific information model: http://www.hilscher.com/UA/IOLink/Wireless
Server profile	Micro Embedded Device
Protocol	OPC UA TCP
User access	Anonymous (read access only) Username / password (read and write access)
Number of sessions	2
Number subscriptions per session	2
Number of “Monitored Items” per session	20
Data coding	UA binary

10.4. Dimensions

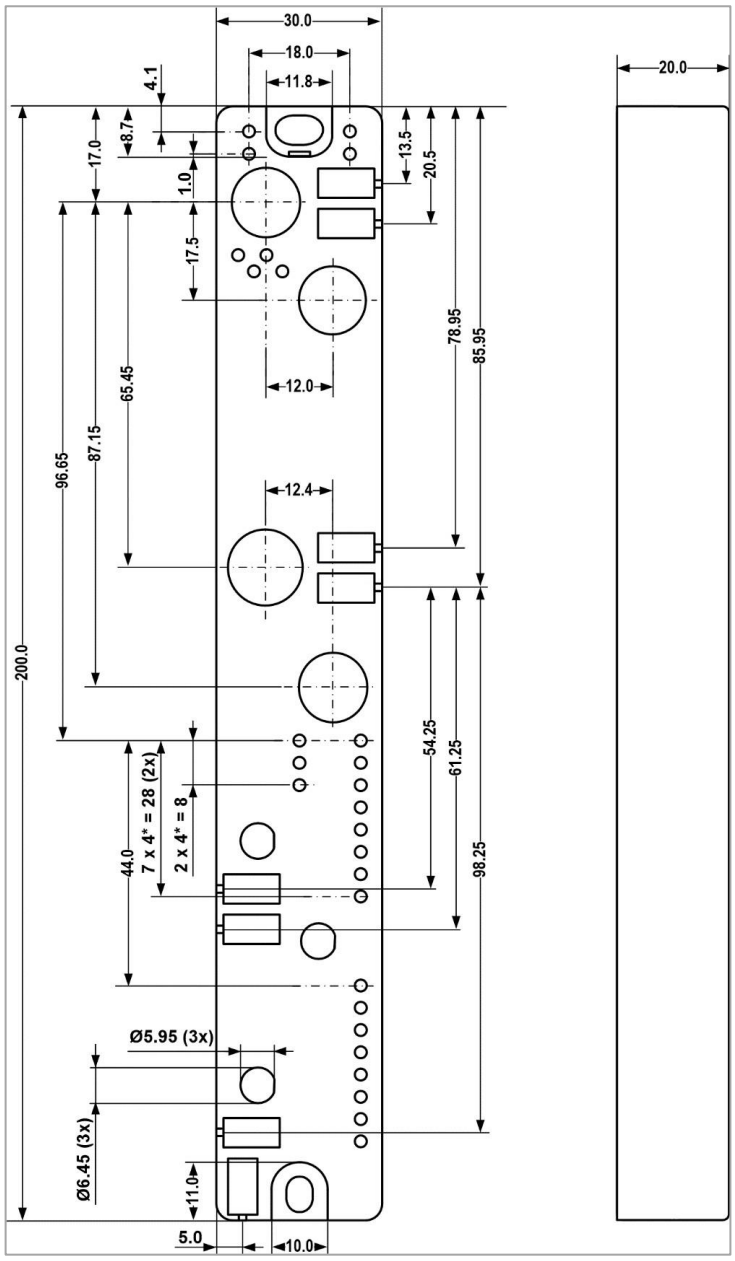


Figure 71: Dimensions

Appendix A – Part Number

Part number: CT241-0004t2-01 (EtherNet/IP Version)

Generation: 2

Product Identifier: 4

Product Type: 1

Protocol: 0004

Character Identifier of Features: t2

Version: 01

Table 67: EtherNet/IP Version

CTGXY-ZZZZii-vv					
G	**X**	**Y**	**ZZZZ**	**ii**	**vv**
Generation	Product Identifier	Product Type	Protocol	Character Identifier of Features	Version

Appendix B – Evaluation Agreement

IMPORTANT – PLEASE READ CAREFULLY THE TERMS OF THIS EVALUATION AGREEMENT ("AGREEMENT"). BY CLICKING "I ACCEPT" OR OTHER SIMILAR BUTTON OR BY DOWNLOADING, INSTALLING, ACCESSING AND/OR USING THE PRODUCT (AS DEFINED BELOW), YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU, OR THE COMPANY YOU REPRESENT, ("YOU" OR "COMPANY") ARE ENTERING INTO A LEGAL AGREEMENT WITH CORETIGO LTD. ("CORETIGO"), AND HAVE UNDERSTOOD AND AGREE TO COMPLY WITH, AND BE LEGALLY BOUND BY, THE TERMS AND CONDITIONS OF THIS AGREEMENT, AS OF THIS DATE ("EFFECTIVE DATE"). FURTHERMORE, YOU HEREBY WAIVE ANY RIGHTS OR REQUIREMENTS UNDER ANY LAWS OR REGULATIONS IN ANY JURISDICTION WHICH REQUIRE AN ORIGINAL (NON-ELECTRONIC) SIGNATURE OR DELIVERY OR RETENTION OF NON-ELECTRONIC RECORDS, TO THE EXTENT PERMITTED UNDER APPLICABLE LAW. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT PLEASE DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

THE PRODUCT MAY BE USED SOLELY FOR YOUR PERSONAL, NON-COMMERCIAL PURPOSES. FOR COMMERCIAL PURPOSES PLEASE CONTACT CORETIGO'S SUPPORT TEAM AT

https://www.CoreTigo.com/support.

1. **Purpose**. The purpose of this Agreement is to enable Company to internally evaluate CoreTigo's Product (as defined hereunder), pursuant to which Company may determine whether it has further interest in signing and executing a definitive license agreement with CoreTigo, with respect thereto. In accordance herewith, CoreTigo and Company have agreed to the terms and conditions set forth hereunder:

2. **Product**. As used herein "Product" shall mean CoreTigo's proprietary product, as set forth in CoreTigo's quotation attached hereto and/or associated and referencing this Agreement, including without limitation, any software or hardware components thereof, any user's guides and/or technical manuals or other documentation delivered by CoreTigo to Company along with the Product ("Documentation"), and any revisions, improvements, updates and upgrade thereof, to the extent delivered. The Product shall be licensed to Company under and subject to the terms of this Agreement and shall be installed by Company on Company's computers at its premises.

3. **License Grant**. CoreTigo hereby grants Company a limited, personal, non-exclusive, non-transferable, non-sublicensable, fully revocable right to use the Product internally for the sole purpose of evaluating the Product's capabilities and evaluating whether to enter into a commercial agreement for the licensing of the Product ("Evaluation"). The Evaluation shall be limited to Company's use of the Product for non- commercial use only. The Evaluation period is limited to 90 days ("Evaluation Period"). The results of the Evaluation and the outcome of the Evaluation shall not be used for any commercial purpose by Company and shall be destroyed by Company at the end of the Evaluation Period. Company shall be solely responsible to ensure that the Product is securely installed and used.

4. **Prohibited Uses**. Except as specifically permitted in Section 3 above, Company agrees not to: (i) copy, modify, merge or sub-license the Product; and (ii) use the Product for any commercial purpose; and (iii) sell, license (or sublicense), lease, assign, transfer, pledge, or share its rights under this Agreement with/to anyone else; and (iv) modify, disassemble, decompile, reverse engineer, revise or enhance the Product or attempt to discover the Product's source code; and (v) changing any proprietary rights notices which appear in the Product.

Company shall comply with all laws and regulations applicable to its business and use of Product and with any terms and conditions imposed by cloud services providers, to the extent applicable.

5. Price and Payment Terms. Company agrees to compensate CoreTigo for the Evaluation in the amount as set forth in the quotation attached hereto and/or associated and referencing this Agreement, which shall be paid prior to and as a contingent of the delivery of the Product. The foregoing payment shall be made free and clear of, and without reduction for sales, use, value added, excise, withholding or similar tax, which shall be at the sole responsibility of Company.

6. Title and Ownership. The Product is a valuable trade secret of CoreTigo and any disclosure or unauthorized use thereof will cause irreparable harm and loss to CoreTigo. All right, title and interest in and to the Product, any derivatives thereof and modifications thereto, including associated intellectual property rights (including, without limitation, patents, copyrights, trade secrets, trademarks, etc.), evidenced by or embodied in and/or attached/connected/related to the Product, are and will remain with CoreTigo. To dispel any doubt, the results of the Evaluation shall be considered CoreTigo's Confidential Information (as defined hereunder). This Agreement does not convey to Company an interest in or to the Product, but only a limited revocable right of use in accordance with the terms herein. Nothing in this Agreement constitutes a waiver of CoreTigo's intellectual property rights under any law.

7. Suggestions and Feedback. It is understood that Company may, at its sole discretion, provide CoreTigo with suggestions and/or comments with respect to the Product ("Feedback"). Company represents that it is free to do so and that it shall not provide CoreTigo with Feedback that infringes upon third parties' intellectual property rights. Company further acknowledges that notwithstanding anything herein to the contrary, any and all rights, including intellectual property rights in such Feedback shall belong exclusively to CoreTigo and that such shall be considered CoreTigo's Confidential Information. It is further understood that use of Feedback, if any, may be made by CoreTigo at its sole discretion, and that CoreTigo in no way shall be obliged to make use of any kind of the Feedback or part thereof.

8. Content. Company shall be solely responsible for any content and data used or optimized by Company by means of the Product.

UNDER NO CIRCUMSTANCES WHATSOEVER WILL CORETIGO BE LIABLE IN ANY WAY FOR ANY CONTENT AND/OR DATA INCLUDING, WITHOUT LIMITATION, FOR ANY ERRORS OR OMISSIONS IN ANY CONTENT AND/OR DATA, OR FOR ANY INFRINGEMENT OF THIRD PARTY'S RIGHT, LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF THE CONTENT, DATA AND/OR THE PRODUCT.

9. Support. During the Evaluation Period, CoreTigo shall make reasonable efforts to provide Company assistance via telephone, facsimile or email to answer any questions or concerns relating to the Product. Such assistance shall be provided at no charge to Company.

10. Warranty Disclaimer.

COMPANY ACKNOWLEDGES THAT THE PRODUCT IS PROVIDED "AS IS", AND CORETIGO DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT OF THIRD PARTIES' RIGHTS, INCLUDING INTELLECTUAL PROPERTY RIGHTS.

11. High Risk Activities. Company hereby acknowledges that the Product is not fault tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous or high risk environments and activities requiring fail-safe performance (such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines.

and/or devices, or weapons systems), in which the failure of the Product could lead directly to death, personal injury or severe physical or environmental damage, and Company hereby agrees not to use or allow the use of the Product or any portion thereof for, or in connection with, any such environment or activity.

12. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CORETIGO, ITS OFFICERS, DIRECTORS AND/OR EMPLOYEES, SHALL NOT BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY PERFORMANCE OF THIS AGREEMENT OR IN FURTHERANCE OF THE PROVISIONS OR OBJECTIVES OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO FOR ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL, LOST OR DAMAGED DATA OR DOCUMENTATION, AND COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES SUFFERED BY COMPANY AND/OR ANY ENTITY AND/OR PERSON ARISING FROM AND/OR RELATED/CONNECTED TO ANY USE OF THE PRODUCT, EVEN IF CORETIGO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. COMPANY'S SOLE RECOURSE IN THE EVENT OF ANY DISSATISFACTION WITH THE PRODUCT IS TO STOP USING IT AND RETURN IT TO CORETIGO. IN ANY EVENT, CORETIGO'S LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE AMOUNTS ACTUALLY RECEIVED BY CORETIGO HEREUNDER.

13. Indemnification. Company hereby agrees that CoreTigo shall have no liability whatsoever for any use made of the Product by Company or any third party. Company hereby agrees to defend, indemnify and hold harmless CoreTigo and its affiliates and their respective officers, directors and employees, from any and all claims, damages, liabilities, costs and expenses (including reasonable attorney's fees) arising from claims related to Company's use of the Product, as well as from Company's failure to comply with the terms of this Agreement.

14. Third Party and Open Source Software. The Product contains software provided by third parties, and such third parties' software is provided "AS IS" without any warranty of any kind, and subject to the license terms attached to such third party software, the provisions of this Agreement shall apply to all such third party software providers and third party software as if they were CoreTigo and the Product respectively. In addition, this Product contains open source components. Such open source components are protected under copyright law and are licensed to under specific license terms. Please see the license.txt file included in the Product and available for Company upon request for the applicable license terms of the open source components.

15. Confidentiality. All information disclosed by either party ("Disclosing Party") to the other party ("Receiving Party"), prior to or during the Evaluation Period, whether in writing, orally or in any other form which is not in the public domain ("Confidential Information"), shall be held in absolute confidence, and Receiving Party shall take all reasonable and necessary safeguards (affording the Confidential

Information at least the same level of protection that it affords its own information of similar importance) to prevent the disclosure of such Confidential Information to third parties. In addition, Receiving Party will limit its disclosure of the Confidential Information to employees and consultants with a "need to know" and only in the context of such employees' and consultants' fulfillment of their duties under this Agreement, and further provided that such employees and consultants are engaged in a confidentiality agreement with the Receiving Party with terms and conditions similar to the confidentiality terms under this Agreement and that Receiving Party shall remain liable for any breach of the terms herein by any of its employees and consultants. The provisions of this paragraph shall survive termination or expiration of this Agreement, for any reason whatsoever.

It is agreed that the following shall not be considered Confidential Information: (i) information that is already known to the Receiving Party at the time of disclosure, as such may be evidenced in the

Receiving Party's written records; (ii) information that is or becomes known to the general public through no act or omission of the Receiving Party in breach of this Agreement; (iii) information that is disclosed to the Receiving Party by a third party who is not in breach of an obligation of confidentiality; or (iv) information that was or is independently developed by the Receiving Party without use of any of the Confidential Information, as such may be evidenced in the Receiving Party's written records.

It is further agreed that the Receiving Party may disclose any information pursuant to a court order, provided the Receiving Party notifies the Disclosing Party of such order and uses reasonable efforts to limit such disclosure only to the extent required. For avoidance of doubt, the source code of the Product constitutes Confidential Information of CoreTigo.

16. Injunctive Relief. Each party agrees that the wrongful disclosure of Confidential Information may cause irreparable injury that is inadequately compensable in monetary damages. Accordingly, and notwithstanding Section 18 below, either party may seek injunctive relief in any court of competent jurisdiction for the breach or threatened breach of this Section in addition to any other remedies in law or equity.

17. Term and Termination.

17.1. This Agreement shall become valid on the Effective Date and shall remain in effect until completion of the Evaluation Period, unless earlier terminated as provided below.

17.2. Either party shall have the right to terminate this Agreement upon 7 days' prior written notice to the other party.

17.3. The license granted for the Evaluation shall terminate immediately upon written notice from CoreTigo in the event of Company's use of the Product for purposes other than the Evaluation and/or any other failure of Company to comply with any provision of this Agreement.

17.4. Upon the earlier of expiration or termination of this Agreement: (i) the license granted hereunder shall immediately terminate; (ii) Company shall return or, at Company's request, the Product and all of CoreTigo's Confidential Information to CoreTigo and shall destroy all copies of the Product contained in any of its systems, and (iii) CoreTigo shall erase or otherwise destroy all copies of the Company's Confidential Information, which was disclosed to CoreTigo under this Agreement. Upon request of either party, the other party shall certify in writing to the other its compliance with the terms of this Section 17.4.

17.5. Without derogating from any of the terms set forth above, Company further agrees that following the expiration or termination of this Agreement it shall not make any commercial use whatsoever of the content optimized by using the Product.

18. General. If any provision, or part thereof, of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable and such reform shall not affect the enforceability of such provision under other circumstances, or of the remaining provisions hereof under all circumstances. This Agreement shall be governed by and construed in accordance with the laws of the State of Israel and only the competent courts of Tel Aviv-Jaffa shall have jurisdiction over any dispute arising from this Agreement.

The following Sections shall survive termination of this Agreement: 4, 6, 7, 8, 10, 11, 13, 15, 16, 17.3, 17.4,17.5,18.

Company shall not assign and/or subcontract any of its rights and obligations under this Agreement, except with CoreTigo's prior written consent. CoreTigo may assign any of its rights and/or obligations hereunder at its sole discretion.

The parties have read this Agreement, and agree to be bound by its terms, and further agree that it constitutes the complete and entire agreement of the parties and supersedes all previous communications between them, oral or written, relating to the subject matter hereof. No representations or statements of any kind made by either party that are not expressly stated herein shall be binding on such party. Either party may use its standard business forms (such as purchase orders) or other communications to administer transactions under this Agreement but use of such forms is for the parties' convenience only and does not alter the provisions of this Agreement. Any terms or conditions that are preprinted in such forms or that are included in a quotation and/or order acknowledgement are null, void, and of no effect. A waiver of any provision will not constitute a continuing waiver of such provision or a waiver of any other provision. Failure by either party to demand performance or claim a breach of this Agreement will not constitute a waiver or otherwise affect the rights of such party.

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one in the same instrument.