CoreTigo

TigoMaster 2TH (EtherCAT)

USER MANUAL

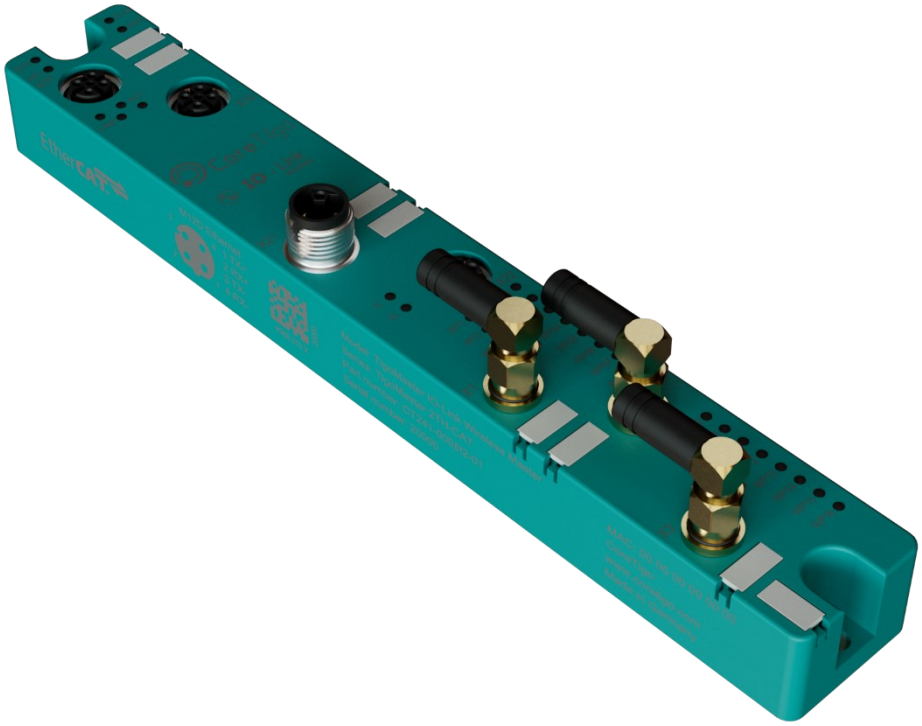


Table of Contents

List of Figures

List of Tables

Revision Control

Author Name	Description	Rev.	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	Retemplate, Edits, Reformats, Updates	04	September 2022
Mike Carmel	Edits, Reformats, Updates (MC0017)	05	November 2022
Mike Carmel	Edits, Reformats, Updates (MC0020)	05	January 2023
Mike Carmel	Edits, Reformats, Updates (MC0022)	05	February 2023

Acronyms and Abbreviations

Term	Meaning
AL	Application Layer
API	Application Programming Interface
CM	Configuration Manager
DS	Data Storage
DSlot	Double Slot
DU	Diagnosis Unit
ESI file	EtherCAT Slave Information file
FAT	File Allocation Table
FOTA	Firmware Upgrade Over the Air
FW	Firmware
HCI	Human-Computer Interaction
HW	Hardware
IF	Interface
IOLW	IO Link Wireless
ISDU	Indexed Service Data Unit
LQI	Link Quality Indicators
ODE	On-request Data Exchange
OPC UA	Open Platform Communication Unified Architecture
OS	Operating System
PDE	Process Data Exchange
PDin	Process Data Input
PDout	Process Data Output
PER	Packet Error Rate

Term	Meaning
Q	Queue
RSSI	Received Signal Strength Indication
SM	System Management
SMI	Standardized Master Interface
SSlot	Single Slot
SW	Software
TigoMaster	CoreTigo's W-Master Product
VS	Vendor Specific
W-Device	Wireless Device (for example, TigoBridge)
W-Master	Wireless Master (for example, TigoMaster 2TH)

1. Introduction

1.1. About

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 manual focuses only on use with the EtherCAT protocol.

Note:
EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

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:

Note:
This symbol indicates a general note.

Warning:
This symbol indicates a security notice which must be observed.

Reference(s):
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 technical capabilities required.

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 area:

- 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 EtherCAT 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

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
- EtherCAT 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

Note:
The abovementioned components are provided by CoreTigo Ltd. upon purchase.

2.8.2. Software

Configuration and commissioning of the product require the following software:

- TigoEngine
- Internet Browser

Note:
TigoEngine is provided by CoreTigo Ltd. upon purchase.

3. Getting Started

3.1. Product Description

The TigoMaster 2TH is an IO-Link Wireless Master that can be used in an EtherCAT network and can operate up to 16 IO-Link sensors/actuators via wireless connectivity. It is supplied with a software tool, TigoEngine, which can be used to configure it over the EtherCAT network. The TigoEngine can also be used to configure the parameters of any IO-Link Wireless sensors/actuators connected to the TigoMaster 2TH. Alternatively, various other configuration tools can be used, 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

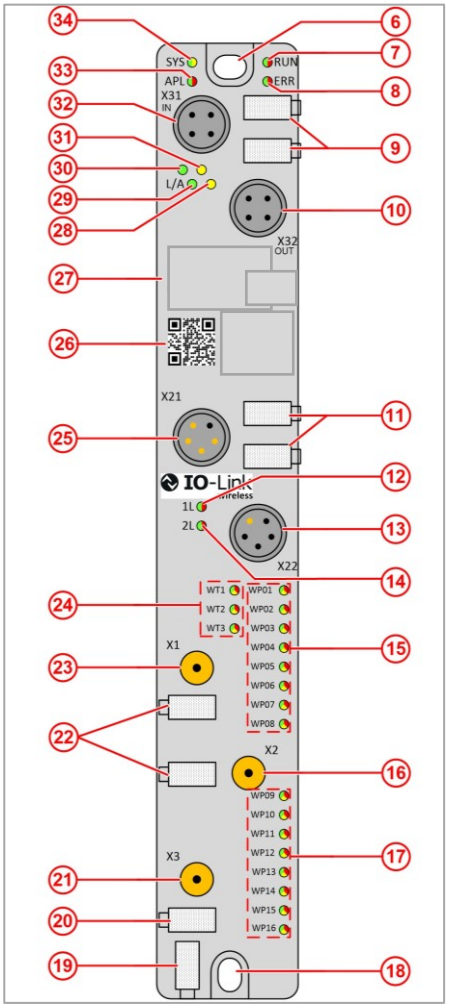


Figure 1: TigoMaster 2TH (EtherCAT Version)

The functionality illustrated in Figure 1 above is described in

Table .

Table 1: TigoMaster 2TH Functionality (EtherCAT Version)

Function	Number	Name	Description
Ethernet	(32)	X31	Ethernet interface, M12, D-coded, EtherCAT port 1 (CH0)
	(10)	X32	Ethernet interface, M12, D-coded, EtherCAT port 2 (CH1)
	(30)	L/A (X31)	Link/Activity LED for connector X31
	(31)	-	LED without function
	(28)	-	LED without function
	(29)	L/A (X32)	Link/Activity LED for connector X32
	(9)	-	Labeling fields Ethernet interfaces X31 and X32
LEDs	(34)	SYS	System status LED
	(33)	APL	Application status LED
	(7)	RUN	Run status LED
	(8)	ERR	Error status LED
Power supply	(25)	X21	Power supply input (PWR IN), M12, L-coded
	(13)	X22	Power supply output (PWR OUT), M12, L-coded
	(12)	1L (X21)	1L supply voltage status LED (DC 24 V)
	(14)	2L (X21)	2L supply voltage status LED (DC 24 V)
	(11)	-	Labeling fields power supply input X21and output X22
Antenna connectors and LEDs for IO-Link wireless radio module	(23)	X1	Connector for SMA antenna for IO-Link wireless connection to the IO-Link Devices 1 to 8
	(16)	X2	Connector for SMA antenna for IO-Link wireless connection to the IO-Link Devices 9 to 16
	(21)	X3	Connector for SMA antenna
	(22), (20)	-	Labeling fields SMA antennas X1, X2, and X3
	(24)	WT1 – WT3	IO-Link wireless track status LEDs
	(15)	WP01 – WP08	Port status LEDs for wireless IO-Link ports WP01 – WP08
	(17)	WP09 – WP16	Port status LEDs for wireless IO-Link ports WP09 – WP16
Identification	(26)	-	Data matrix code
Mounting	(6)	-	Mounting hole and grounding
	(18)	-	Mounting hole

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 9 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 . For any hardware installation, firmware must be updated.

Table 2: TigoMaster 2TH Hardware

Product Name	Description	Part Number	Hardware Revision
TigoMaster 2TH-CAT	IO-Link Wireless Master (EtherCAT Version)	CT241-0008t2-01	Rev01

Table 3: TigoMaster 2TH Software

Software	Name	Version
Engineering Tool	TigoEngine	3.1
Integrated Web Server	CoreTigo Web Server	1.2
PLC IDE	TwinCAT	3.1 build 4024

Table 4: TigoMaster 2TH Firmware

Protocol	File Name	Version
EtherCAT Adapter	UI197H001.nxi	2.2.0.802

3.2.4. Identification

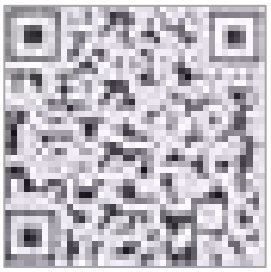


Figure 2: TigoMaster 2TH Identification Code

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

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

Examples of the data provided are:

- 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 indicate the states of each LED on the TigoMaster 2TH.

3.2.5.1. DS SMI Events

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 1L and 2L

LED	Color	State	Description4
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. TigoMaster 2TH Device Status

Table 9: TigoMaster 2TH Device Status

LED	Color	State	Description
RUN (Module Status)		Off	**INIT:** the device is in INIT state.
		On	**Device Operational:** the device is operating correctly.
		Flashing (2.5 Hz)	**Pre-Operational:** the device is in the Pre-Operational state.
		Single Flash	**Safe-Operational:** the device is in the Safe-Operational state.

Table 10: Communication Status EtherCAT Slave

LED	Color	State	Description
ERR (Network Status)		Off	**Off no error:** the EtherCAT communication of the device is in working order.
		Flashing (2.5 Hz)	**Invalid configuration:** General Configuration Error Possible reason: State change commanded by master is impossible due to register or object settings.
		Single Flash	**Local error:** slave device application has changed the EtherCAT state autonomously. Possible reason 1: A host watchdog timeout has occurred. Possible reason 2: Synchronization error, device enters Safe-Operational state automatically.
		Double Flash	**Application watchdog timeout:** An application watchdog timeout has occurred. Possible reason: Sync Manager Watchdog timeout.

Table 11: Definition LED States Communication Status

LED state	Definition
Flashing (2.5 Hz)	The indicator turns on and off with a frequency of 2.5 Hz: on for 200 ms, followed by off for 200 ms.
Single Flash	The LED shows one short flash (200 ms) followed by a long off phase (1,000 ms).
Double flash	The LED shows the following sequence: 1st short flash (200 ms) – short off (200 ms) – 2nd short flash (200 ms) – long off (1,000 ms)

3.2.5.5. Ethernet Status EtherCAT Slave

Table 12: Ethernet Status EtherCAT Slave

LED	Color	State	Description
L/A IN, L/A OUT Ch0: (30) , Ch1: (29)		On	**Link:** The device is connected to the Ethernet, but does not send/receive Ethernet frames.
		Flickering (load dependent)	**Activity:** The device is connected to the Ethernet and sends/receives Ethernet frames.
		Off	The device has no link to the Ethernet.
Ch0: (31) , Ch1: (28)		Off	The device does not send/receive Ethernet frames.

Table 13: Definition LED States Ethernet Status

LED State	Definition
Flickering (Load Dependent)	The LED 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 LED turns on and off in irregular intervals to indicate low Ethernet activity.

3.2.5.6. Wireless Track LEDs

Table 14: Wireless Track LEDs

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

Table 15: Wireless Port LED

LED	Color	State	Description
WP1 … WP16		On	Port operational.
		Blinking	Communication ready.
		On	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

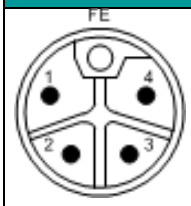
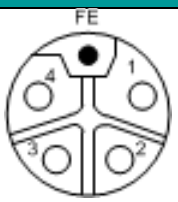
3.2.6.1. Power Supply

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 16: Power Supply Connectors

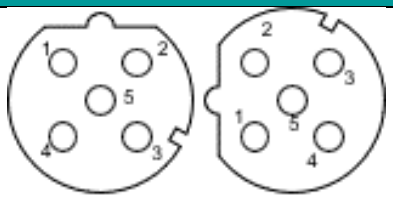
PWR IN	PWR OUT	Pin	Signal	Description
 M12, L-coded, male 5-pin (4 + FE) (X21)	 M12, L-coded, female 5-pin (4 + FE) (X22)	1	1L+	+24 V DC power supply for system and sensor, U1L.
		2	2L-	Reference potential for 2L.
		3	1L-	Reference potential for 1L.
		4	2L+	+24 V DC power supply for auxiliary/switched power supply, U2L.
		FE	FE	Functional earth.

3.2.6.2. Ethernet

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

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

Table 17: 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 18: 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

Note:
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.

3.2.7. Derating

Note the derating when you connect a device to Power Out on the TigoMaster 2TH, so 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 f low into the TigoMaster 2TH as a function of the ambient temperature (T).

Note that the derating curve in **Error! Reference source not found.** applies to operating conditions "without air f low 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.

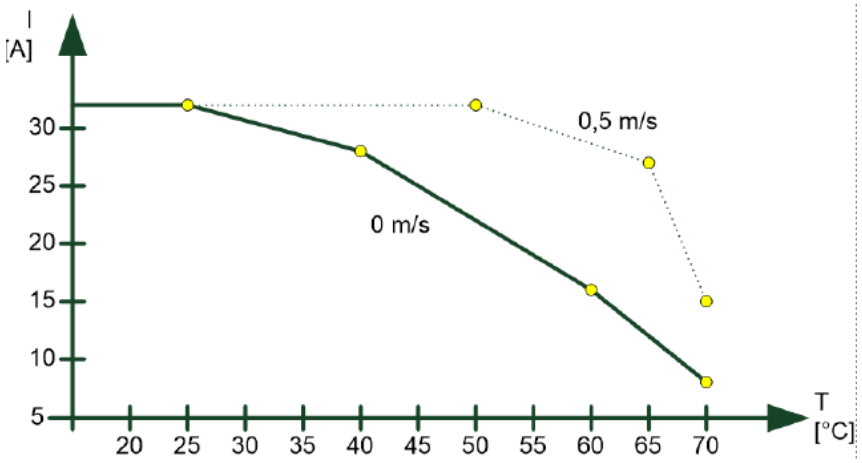


Figure 3: Derating TigoMaster 2TH

4. Installation Overview

Warning:
Comply with all safety instructions relevant to the TigoMaster 2TH (see section 2) 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 your 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 your system .
3. Make 2 M4 threaded screw holes as follows:.
    - Hold the TigoMaster 2TH in the desired position.
    - Mark the two points where the threads are to be cut (at the 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 Table .
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

You can now ground the TigoMaster 2TH: see section 4.1.4.

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.

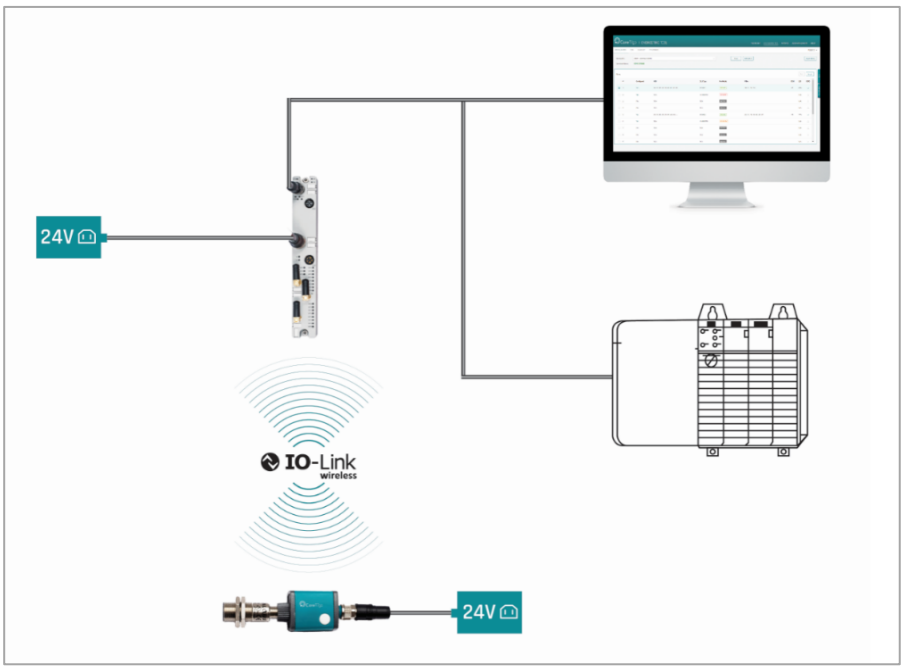


Figure 4: Connection Example with TigoBridge

5. Configuration

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:

- EtherCAT Master
  - Parameters for the exchange of process data
- TigoMaster 2TH:
  - Parameters for the IO-Link Wireless Master (for example. track mode)
  - Parameters for the wireless ports (for example, 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 for the EtherCAT Master**

  The EtherCAT Master must be configured to exchange process data with the TigoMaster 2TH. You do this with the configuration software for the EtherCAT Master and an ESI file (EtherCAT Slave Information file).

  The configuration software imports the ESI file, after which you can configure the relevant parameters in the software and then upload the configuration to the EtherCAT Master.

- **CoreTigo Web Server**

  The CoreTigo Web Server can be displayed in a web browser, and enables you to set all 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

Note:
If you intend to use TigoEngine, it must be installed before using either of the other tools to configure TigoMaster 2TH.

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

Table 19: Configuration Tools

Tool	EtherCAT Master Parameters	IO-Link Wireless Master Parameters	Port Parameters	IO-Link Device Parameters	MQTT Client Parameters (if MQTT communication used)
Configuration Software for the EtherCAT Master	Applicable	N/A	Applicable	N/A	N/A
TigoEngine	N/A	Applicable	Applicable	Applicable	Applicable
CoreTigo Web Server	N/A	Applicable	Applicable	Applicable	Applicable

Note

When EtherCAT communication is initiated, the EtherCAT Master transmits its configuration parameters to the TigoMaster 2TH. These override any port configuration parameters set by the CoreTigo Web Server or TigoEngine: parameters set using the EtherCAT Master have priority.

If you want to change parameters for the wireless ports permanently, set them with the configuration software for the EtherCAT Master.

5.2. Configure the EtherCAT Master

In order for the EtherCAT Master and the TigoMaster 2TH to exchange process data, you need to configure the EtherCAT Master using the ESI file (EtherCAT Slave Information file) for the TigoMaster 2TH.

Configuring the EtherCAT Master has the following stages:

1. Prerequisites—see section 5.2.1
2. Import the ESI File—see section 5.2.2
3. Define the Module for Each Port—see section 5.2.3
4. Set Parameters for the Ports—see section 5.2.4

5.2.1. Prerequisites

Make sure that:

- You have the latest ESI file:

  The ESI file name is in the format **CoreTigo_TigoMaster_2TH.xml.** It is provided separately and can be download from the CoreTigo Customer Portal https://support.CoreTigo.com/index.php.
- All components are connected to the system and to the power supply (as described in previous sections)
- The TigoMaster 2TH is connected to your EtherCAT Master (for example, TwinCAT)

5.2.2. Import the ESI File

This procedure uses the example of importing the ESI file in a TwinCAT programming environment.

1. Import the ESI file as follows:
   - In the configuration software for the EtherCAT Master, click the menu for your programming environment: for example, **TwinCAT**.
   - In the menu, select **EtherCAT Devices** > **Reload Device Descriptions**.

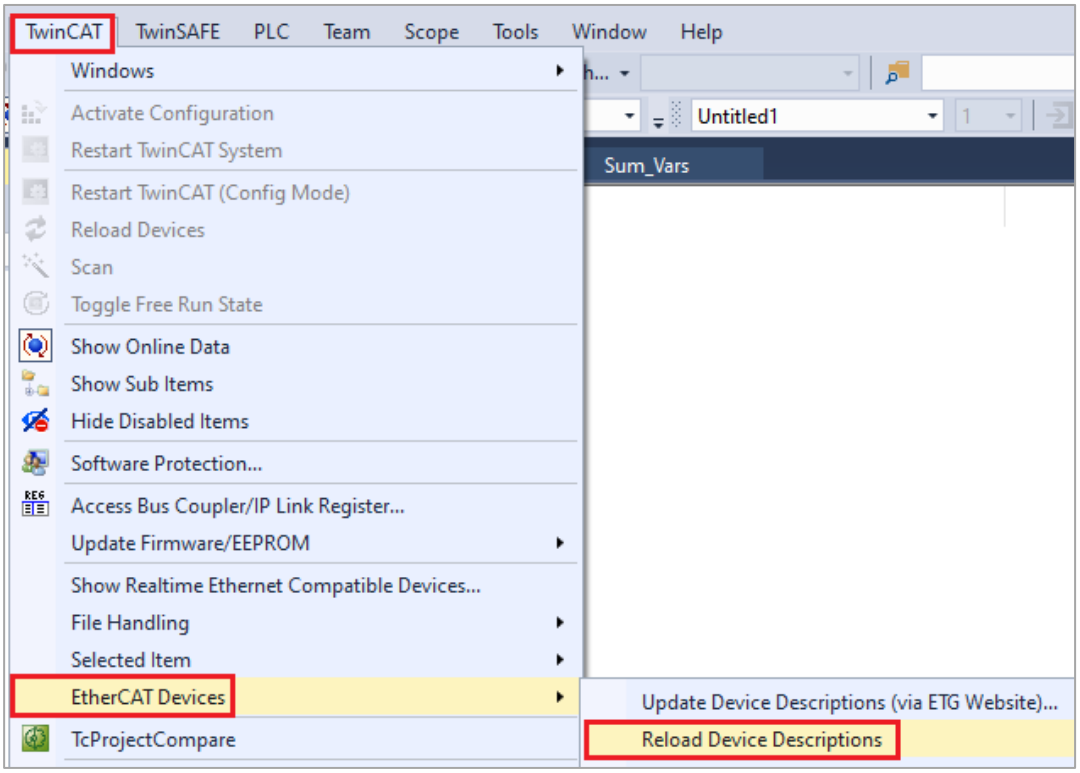


Figure 5: Import the ESI File

2. In the device catalog select the TigoMaster 2TH (EtherCAT), and add it to the configuration project.

   Note: Use the scan feature of the configuration software to add the TigoMaster 2TH to the project.

5.2.3. Define the Module for Each Port

Each wireless IO-Link port of the TigoMaster 2TH corresponds to a **slot** in the configuration software. There are 16 slots (ports), named WP01–WP16. Each slot has a **module** property that needs to be defined according to the type of device connected to it: that is, according to the device's quantity of bytes PDIN and quantity of bytes PDOUT.

Define each slot's module as follows:

1. In the configuration software for the EtherCAT Master, double-click **TigoMaster 2TH**.
2. In the main window, select the **Slots** tab.

In the **Slots** tab you can see that the default setting for each slot's module is **Slot Empty** (that is, disabled).

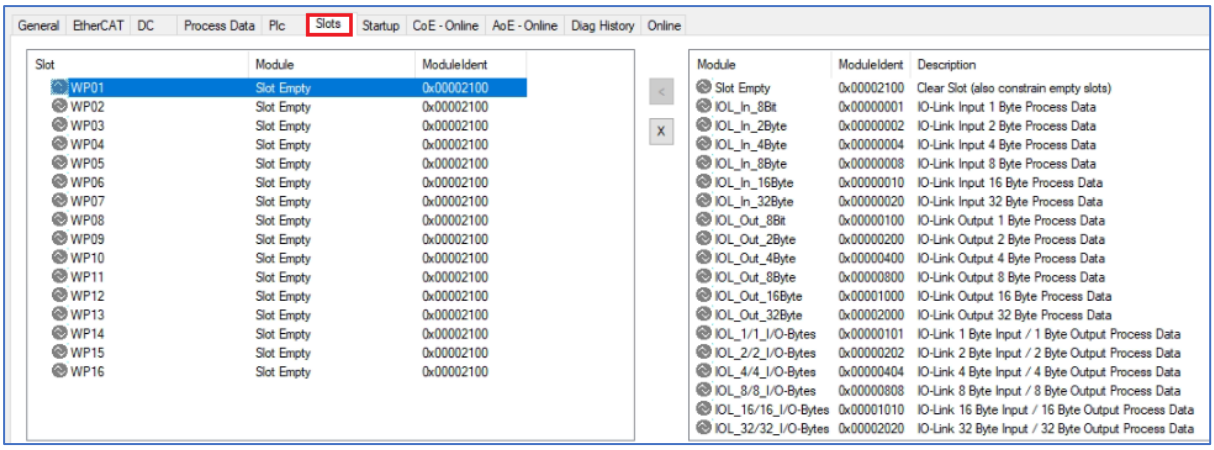


Figure 6: Slots Tab

3. Select the desired slot.

   In the example in the figure below, WP01 is selected.

4. Click  .

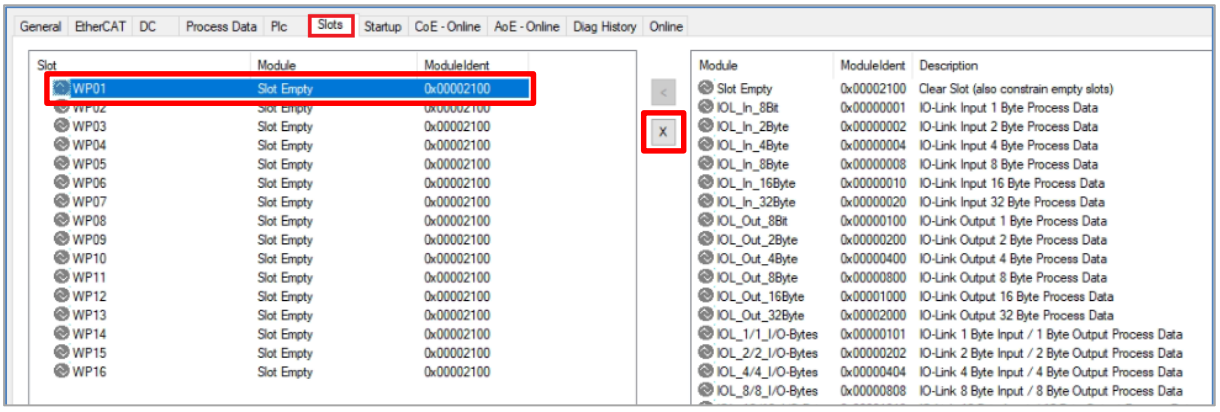


Figure 7: Clear a Slot's Current Module Setting

5. In the **Module** pane, select the relevant module (according to the size of the process data input and output by the device connected to the slot).

   For example, if the selected slot is connected to a device with 2 bytes PDIN and 4 bytes PDOUT, the relevant module would be IOL_4/4_I/O-Bytes, as shown in the figure below.

   The various modules are listed in Table .

6. Click  .

The selected module now appears in the following places:

- The selected slot's row in the **Slots** tab (in the **Module** column): see **Error! Reference source not found.**.
- The **Solution Explorer**: see **Error! Reference source not found.**.
- The **Startup** tab

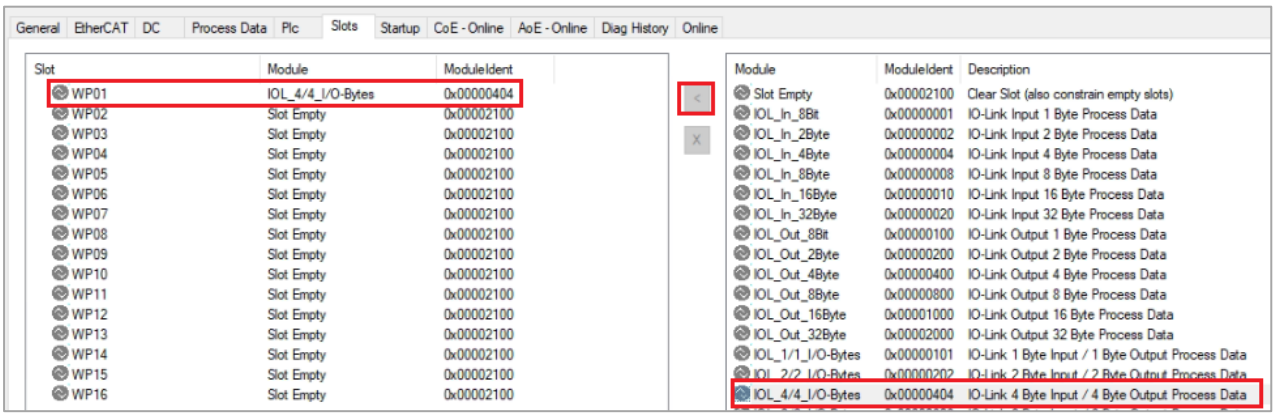


Figure 8: Set a Slot's Module

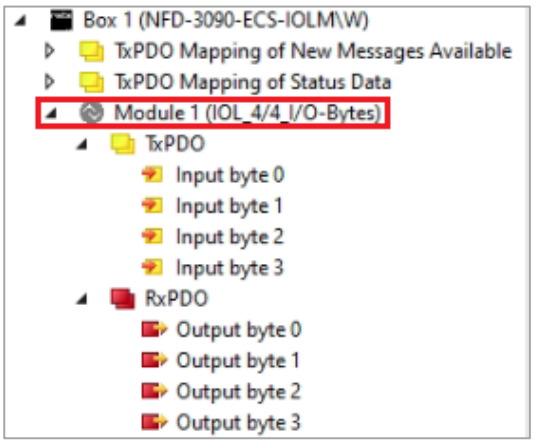


Figure 9: Module in Solution Explorer

Table 20: Modules

Module (Device Type)	Description
Slot empty	No device is connected to the wireless IO-Link port.
IOL_In_8Bit	IOL_In_8Bit IO-Link Input 1 Byte Process Data
IOL_In_2Byte	IOL_In_2Byte IO-Link Input 2 Byte Process Data
IOL_In_4Byte	IOL_In_4Byte IO-Link Input 4 Byte Process Data
IOL_In_8Byte	IOL_In_8Byte IO-Link Input 8 Byte Process Data
IOL_In_16Byte	IOL_In_16Byte IO-Link Input 16 Byte Process Data
IOL_In_32Byte	IOL_In_32Byte IO-Link Input 32 Byte Process Data
IOL_Out_8Bit	IOL_Out_8Bit IO-Link Output 1 Byte Process Data
IOL_Out_2Byte	IOL_Out_2Byte IO-Link Output 2 Byte Process Data
IOL_Out_4Byte	IOL_Out_4Byte IO-Link Output 4 Byte Process Data

Module (Device Type)	Description
IOL_Out_8Byte	IOL_Out_8Byte IO-Link Output 8 Byte Process Data
IOL_Out_16Byte	IOL_Out_16Byte IO-Link Output 16 Byte Process Data
IOL_Out_32Byte	IOL_Out_32Byte IO-Link Output 32 Byte Process Data
IOL_1/1_I/O-Bytes	IOL_1/1_I/O-Bytes IO-Link 1 Byte Input / 1 Byte Output Process Data
IOL_2/2_I/O-Bytes	IOL_2/2_I/O-Bytes IO-Link 2 Byte Input / 2 Byte Output Process Data
IOL_8/8_I/O-Bytes	IOL_8/8_I/O-Bytes IO-Link 8 Byte Input / 8 Byte Output Process Data
IOL_16/16_I/O-Bytes	IOL_16/16_I/O-Bytes IO-Link 16 Byte Input / 16 Byte Output Process Data
IOL_32/32_I/O-Bytes	IOL_32/32_I/O-Bytes IO-Link 32 Byte Input / 32 Byte Output Process Data

5.2.4. Set Parameters for the Ports

TigoMaster 2TH is supplied with default parameter settings, which you can change according to your system's needs (after you have defined the ports' modules as detailed in section 5.2.3). You change the settings of port parameters and IO-Link wireless device parameters in the **Startup** tab of the configuration software of the EtherCAT Master. When communication starts, the EtherCAT Master then sends these parameters to the TigoMaster 2TH.

Each parameter for each port is identified by an index and sub-index, where the index (for example, 0x8000) identifies the port, and the sub-index (for example, 01) identifies the parameter. The index and sub-index are separated from each other by a period, i.e.: 0x8000.01.
The indexes for each port are listed in **Error! Reference source not found.**.
he parameters are detailed in Table .

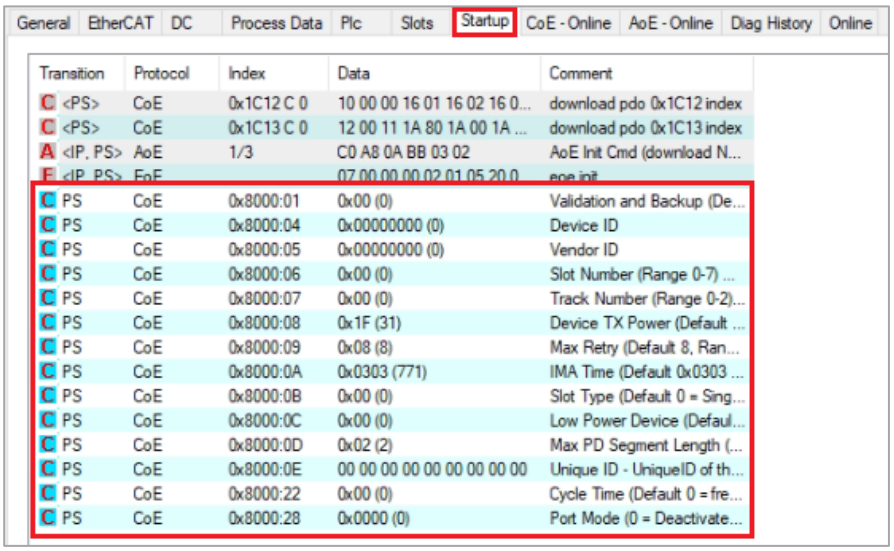


Figure 10: Startup Tab Showing the Parameters for Port WP01 (Index 0x08000)

To change the setting of a parameter:

1. In the **Startup** tab, double click the parameter.
2. Change the parameter setting as desired.
3. Click **Reload Devices** ( ) to apply the change.

Table 21: Port Indexes

Port	Index
WP01	0x8000
WP02	0x8010
WP03	0x8020
WP04	0x8030
WP05	0x8040
WP06	0x8050
WP07	0x8060
WP08	0x8070
WP09	0x8080
WP010	0x8090
WP011	0x80A0
WP012	0x80B0
WP013	0x80C0
WP014	0x80D0
WP015	0x80E0
WP016	0x80F0

Table 22: Port Parameters

Sub-Index	Example Index with Sub-Index	Parameter Name	Range of Values	Default	Description
01	0x8000.01	Validation and Backup	No Device check	No Device check	There is no device check for validation or backup of connected IO-Link Slave devices (default).
			Type compare,no Backup/ Restore		A device check is performed for validation of IO-Link Slave devices connected to the specified device type, without backup/restore.
			Type compare, Restore only		A device check is performed for validation or restore of IO-Link Slave devices connected to the specified device type, without backup.
			Type compare, Backup and Restore		A device check is performed for validation or backup/restore of IO-Link Slave devices connected to the specified device type.

Sub-Index	Example Index with Sub-Index	Parameter Name	Range of Values	Default	Description
04	0x8000.04	Device ID	0–16777215	1677721 5	Device ID The expected device ID of the connected wireless IO-Link Device (if validation is in use). For details of device IDs, see ioddfinder.io-link.com, or documentation of the relevant IO-Link Device. Value = 0 if no validation is used.
05	0x8000.05	Vendor ID	1–65535	0	Manufacturer ID The expected manufacturer ID of the connected wireless IO-Link Device (if validation is in use). For details of Manufacturer IDs, see ioddfinder.io-link.com, or documentation of the relevant IO-Link Device. Value = 0 if no validation is used.
06	0x8000.06	Slot number	0–7	0	Wireless slot number to be used for the port
07	0x8000.07	Track number	0–2	0	Wireless track number to be used for the port
0x8000.08,	0x8000.08	Device TX Power	1–31	31	Transmit power level of the W-Device
09	0x8000.09	Max Retry	2–31	8	Maximum number of retries for a transmission in OPERATE mode
0A	0x8000.0A	IMA Time	1.664 ms … 10 min	3 s	Requested I-Am-Alive time for OPERATE mode. See section 5.2.4.2 for details.
0B	0x8000.0B	Slot Type	0: Single slot	0	Slot type is single slot
			1: Double slot		Slot type is double slot
0C	0x8000.0C,	Low Power Device	0: Not Low Power	0	Is the connected W-Device low power or not
			1: Low Power		
0D	0x8000.0D	Max PD Segment Length	1–32	2	Maximum segment length of the PDOut data to the Message handler to distribute PDOut Data within multiple W-Cycles.
0E	0x8000.0E	Unique ID Byte 0	0–255	0	Unique ID of the W-Device

Sub-Index	Example Index with Sub-Index	Parameter Name	Range of Values	Default	Description
		Unique ID Byte 1	0–255	0	Unique ID of the W-Device
		Unique ID Byte 2	0–255	0	Unique ID of the W-Device
		Unique ID Byte 3	0–255	0	Unique ID of the W-Device
		Unique ID Byte 4	0 … 255	0	Unique ID of the W-Device
		Unique ID Byte 5	0–255	0	Unique ID of the W-Device
		Unique ID Byte 6	0–255	0	Unique ID of the W-Device
		Unique ID Byte 7	0–255	0	Unique ID of the W-Device
		Unique ID Byte 8	0–255	0	Unique ID of the W-Device
22	0x8000.22	Cycle Time	0–255	0	See section 5.2.4.1.
28	0x8000.28	Port Mode	0: Deactivated	0	The W-port is inactive. Input and output process data is 0.
			1: IO-Link Wireless cyclic		The W-port operates in cyclic mode.
			2: IO-Link Wireless roaming		The W-port operates in roaming mode.

5.2.4.1. Port Cycle Time

The Port Cycle Time parameter sets up the cycle time of a W-Port of the TigoMaster 2TH. The cycle time is encoded using **Time Base** values (bits 6+7) and **Multiplier** values (bits 0-5), as shown in the following table.

Table 23: Port Cycle Time Calculation

Value Range	Time Base (Bits 6+7)	Multiplier (Bits 0-5)	Resulting Cycle Time/Notes
0	0	0	Free-running mode. Note: If the free-running mode is chosen with a time base of 0, the W- Master stack automatically configures the Master Cycle Time to be the Minimum Master Cycle Time based on the PD Segmentation Length, Slot Type and Max Retry configurations.
1 … 64	00	1 … 63	

Value Range	Time Base (Bits 6+7)	Multiplier (Bits 0-5)	Resulting Cycle Time/Notes
65 … 127	01: 5ms	1 … 63 as multiplier	5 ... 315 ms (Time Base * Multiplier) For W-Devices and W-Bridges the minimum possible transmission time is 5 ms
128 … 255	10 ...11: reserved	1 … 63	Reserved. Do not use

5.2.4.2. I-Am-Alive Time

The **I-Am-Alive Time** parameter controls TigoMaster 2TH and W-Device communication if no other messages are transmitted. The W-Device must send **I-Am-Alive** messages to the TigoMaster 2TH before timeout, otherwise the TigoMaster 2TH reports a communication error (**ComLost**).

The **I-Am-Alive Time** parameter comprises a **Time Base** and **Multiplier**, and is calculated by multiplying them by each other.

Table shows the coding of the time base.

Table 24: Time Base of I-Am-Alive Time

Value	Time Base	Description
0	Reserved	Do not use
1	1.664 ms	Time base is 1.664 ms.
2	5 ms	Time base is 10 ms.
3	1 sec	Time base is 1 sec
4	1 min	Time base is 1 min
5 … 255	Reserved	Do not use

The multiplier has the value range of 1 … 255.

The **I-Am-Alive Time** parameter (**Multiplier** * **Time Base**) is calculated as shown in the following table:

Table 25: Calculation of I-Am-Alive Time

Multiplier (Bits 8-15)	Time Base(Bits 0-7)	Calculated I-Am-AliveTime	Value
1	1: 1.664 ms	1.664 ms	257
	2: 5 ms	5 ms	258
	3: 1 sec	1 sec	259
	4: 1 min	1 min	260
2	1: 1.664 ms	3.328 ms	513
	2: 5 ms	10 ms	514
	3: 1 sec	2 sec	515
	4: 1 min	2 min	516
3	1: 1.664 ms	4.992 ms	769
	2: 5 ms	15 ms	770
	3: 1 sec	3 sec	771
	4: 1 min	3 min	772
4 … 254	1 … 4	Multiplier * time base	Value of multiplier * 256 + value of the time base.
255	1: 1.664 ms	424.32 ms	65281
	2: 5 ms	1275 ms	65282
	3: 1 sec	255 s	65283
	4: 1 min	255 min (10 min is used)	65284

The TigoMaster 2TH verifies the calculated **I-Am-Alive Time** with the following limits:

- Minimum **I-Am-Alive Time** = **W-Sub-cycle duration** [ms] * (**MaxRetry** + 1)
- Maximum **I-Am-Alive Time** = 10 minutes

5.2.5. Prevent the Configuration Software of the EtherCAT Master from Configuring a Port

When EtherCAT communication is initiated, the EtherCAT Master transmits its configuration parameters to the TigoMaster 2TH. These override any port configuration parameters set by the CoreTigo Web Server or TigoEngine: parameters set using the EtherCAT Master have priority.

However, you can prevent the EtherCAT Master from transmitting a specific parameter as follows:

1. In the **Startup** tab, select the relevant parameter(s).
2. Press delete.

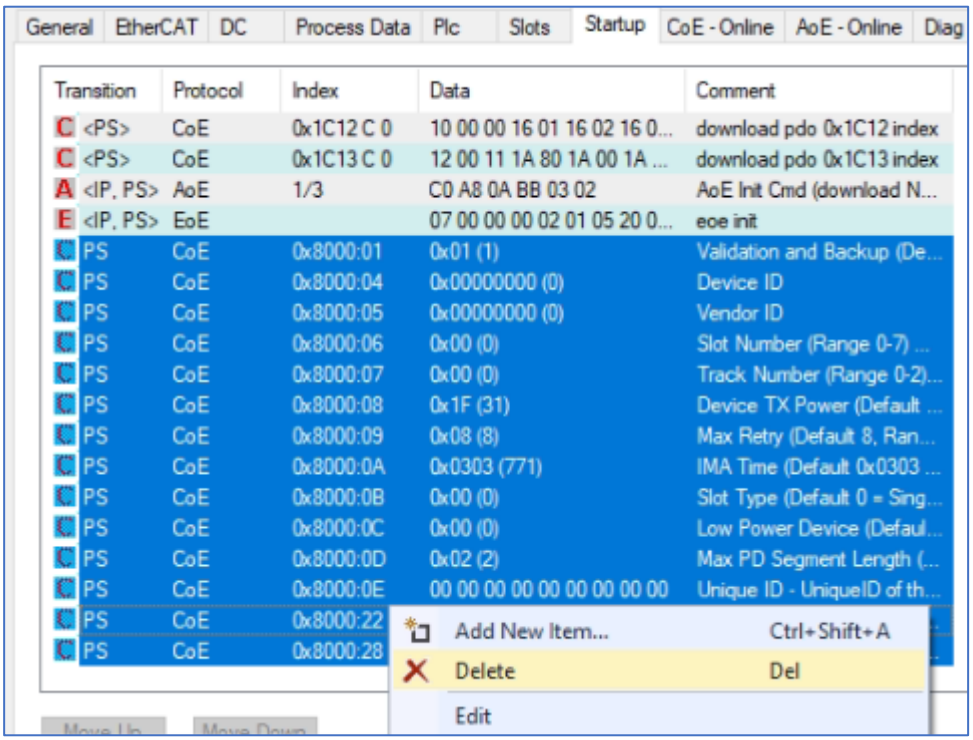


Figure 11: Delete Parameters from the Startup Tab: Example

5.3. Monitor and Write with the Configuration Software of the EtherCAT Master

5.3.1. Monitor Ports

The **CoE - Online** tab enables you to monitor various information, including:

- Online data for each port: see Figure
- The state of each port: see Figure

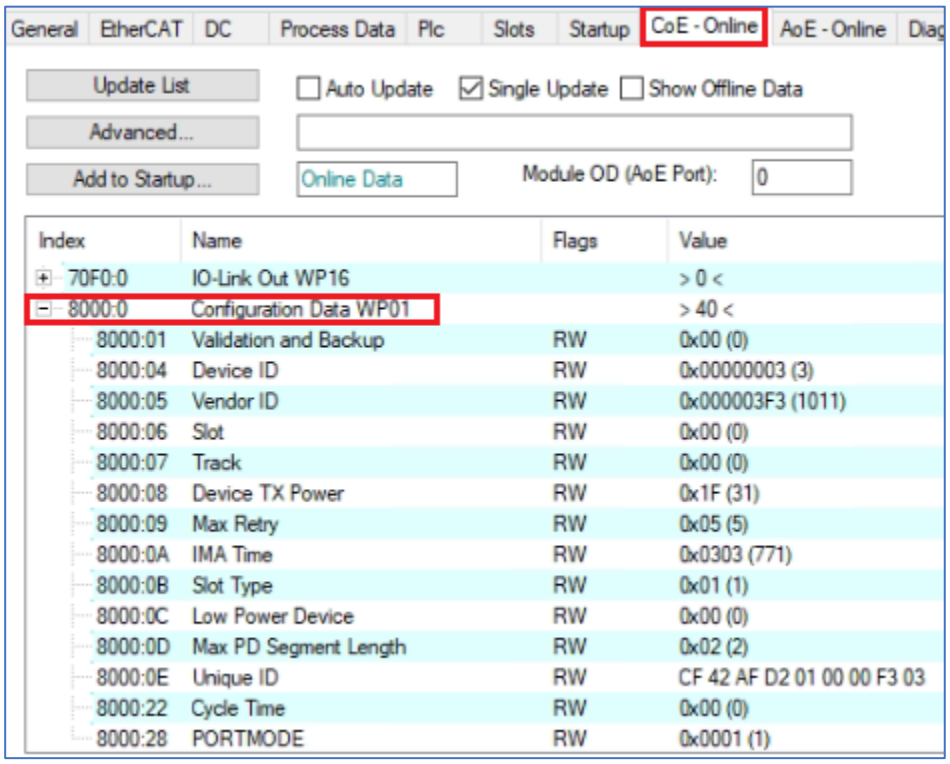


Figure 12: Monitor Port Configuration Data in the C0E-Online Tab

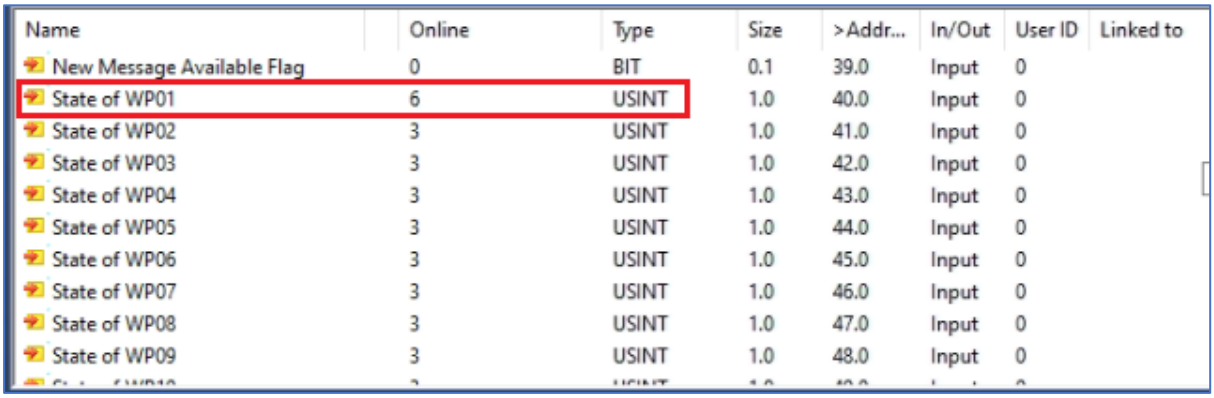


Figure 13: Monitor the State of a Port in the C0E-Online Tab

5.3.2. Monitor a PDIN Value

1. In the **Solution Explorer**, select the Input byte that you want to monitor.
2. Select the **Online** tab.
3. View the **Value** box.

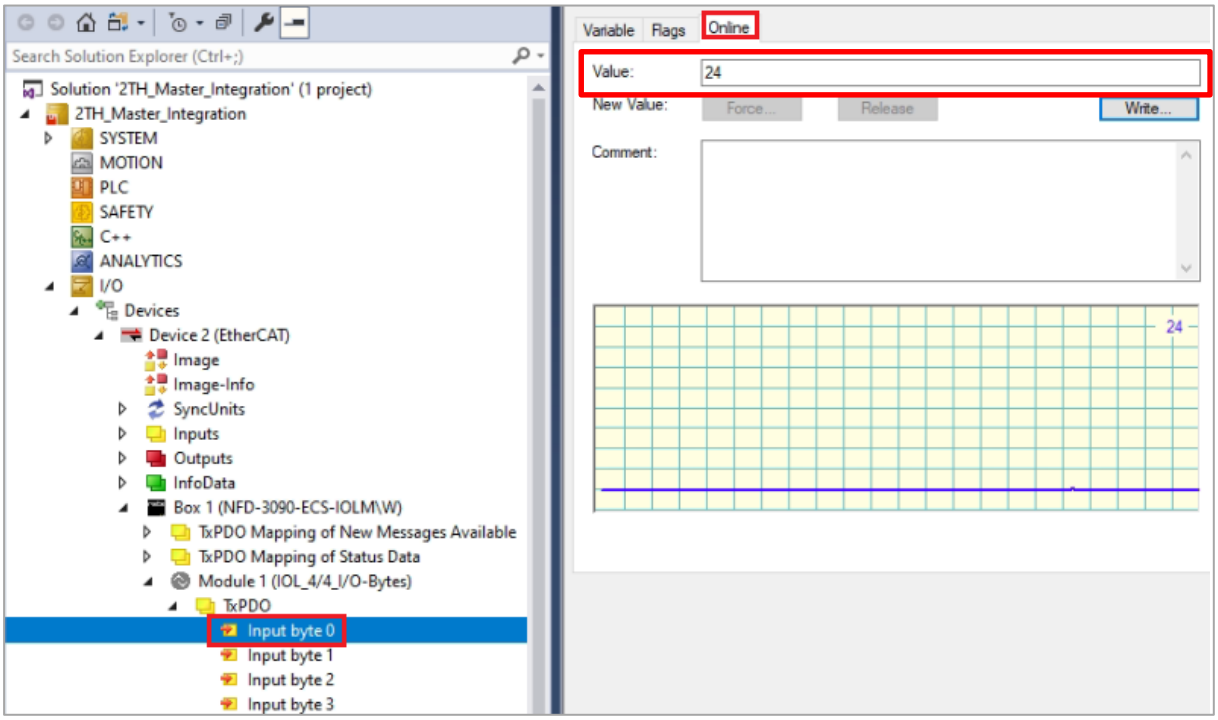


Figure 14: Monitor a PDIN Value

5.3.3. Write a PDOUT Value

1. In the **Solution Explorer**, select the Output byte that you want to write.
2. Select the **Online** tab.
3. Click **Write**.
4. In the **Set Value** dialog box, type the desired value in the **Dec** box.
5. Click **OK**.

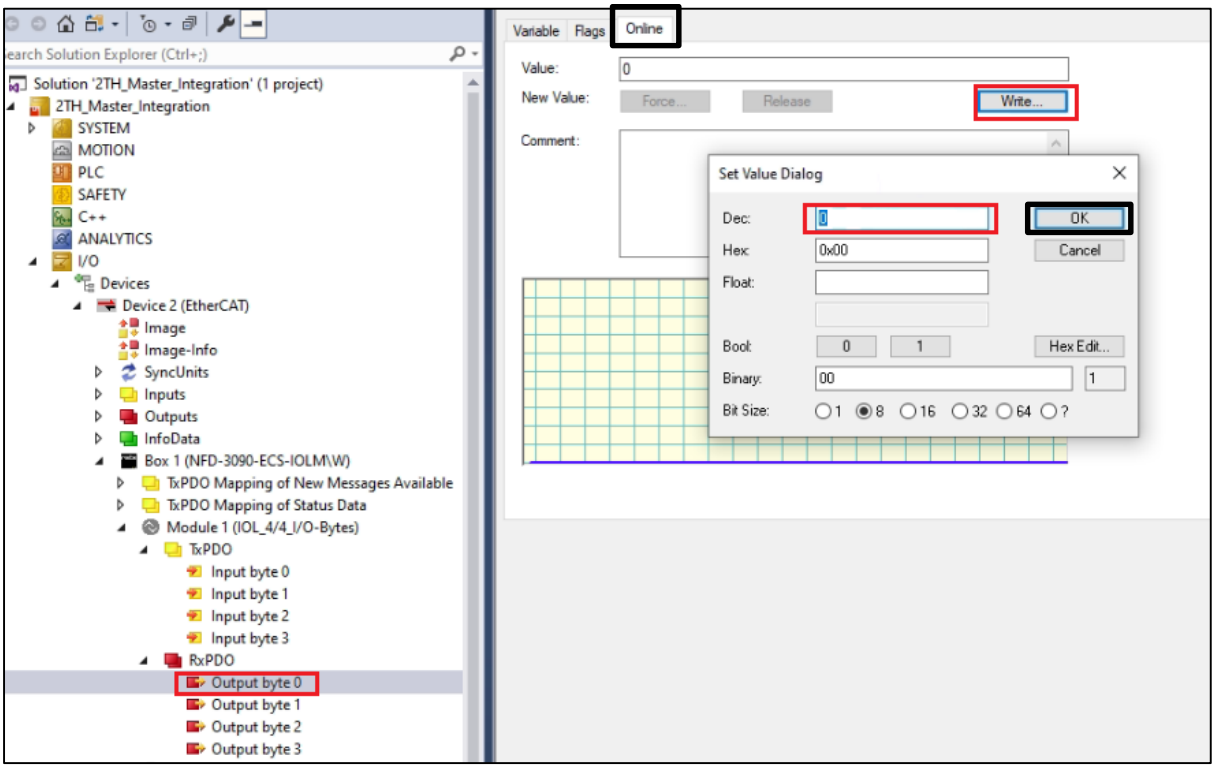


Figure 15: Write a PDOUT Value

5.3.4. TwinCAT as EtherCAT Master

Setting up TwinCAT as EtherCAT master on PC:

1. Install TwinCAT from **https://www.beckhoff.com/he-il/support/download-finder/software-and-tools/#**
2. Right click on "TwinCAT Config Mode" icon and select **Tools --> TwinCAT Switch Runtime**:

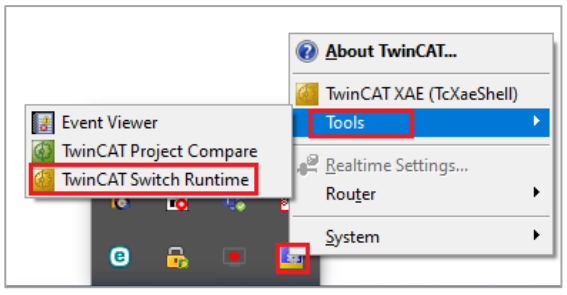


Figure 16: TwinCAT Switch Runtime (1)

The following window opens:

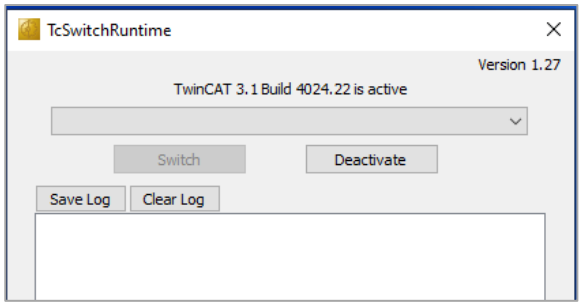


Figure 17: TwinCAT Switch Runtime (2)

3. Run TwinCAT shell and open new project.
4. Open TwinCAT menu and select **Show Realtime Ethernet Compatible Devices**.

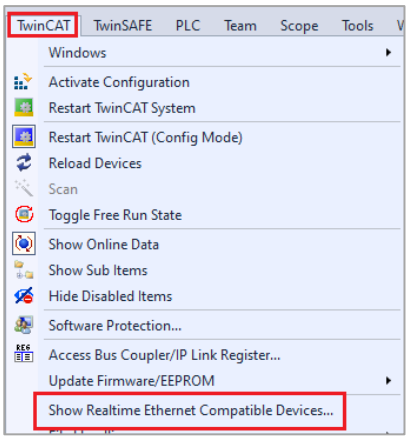


Figure 18: Show Realtime Ethernet Compatible Devices

5. Select your PC Ethernet interface under Incompatible devices and click install: (It will work only listed Ethernet adapters that TwinCAT supports)

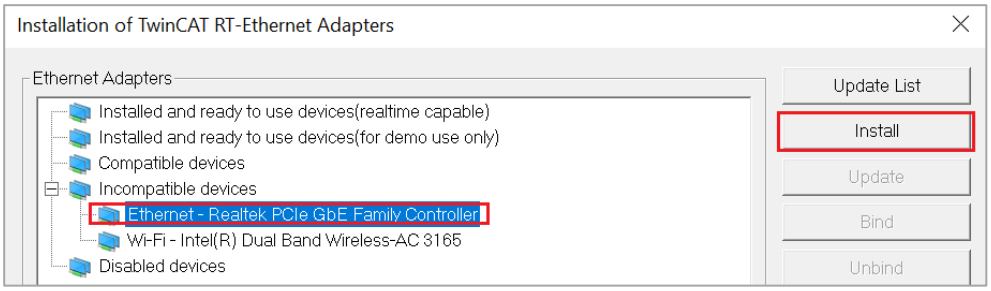


Figure 19: Select PC Ethernet Interface Under Incompatible Devices

6. Click **Install**.

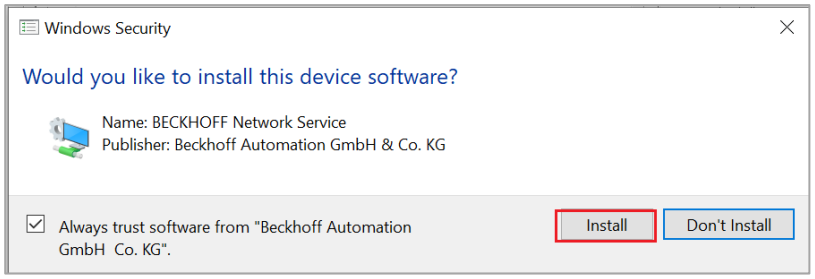


Figure 20: Install the Device Software

7. Now the PC Ethernet adapter will appear under "Installed and ready to use devices" and can be used as EtherCAT master:

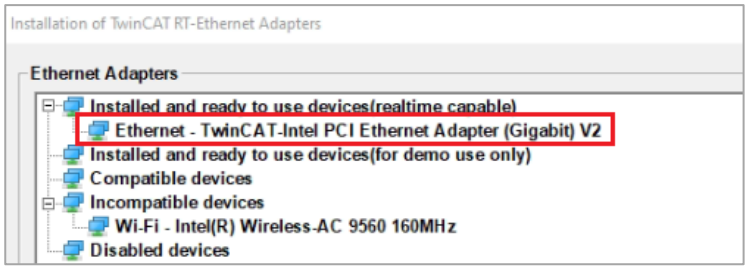


Figure 21: EtherNET Adapters Selection

8. Loading the ESI file (EtherCAT Slave Information).

- Download the ESI files from CoreTigo customer portal. (attached).
- Copy both files to C:\TwinCAT\3.1\Config\Io\EtherCAT
- Open the TwinCAT menu and select **EtherCAT Devices --> Reload Device Descriptions**

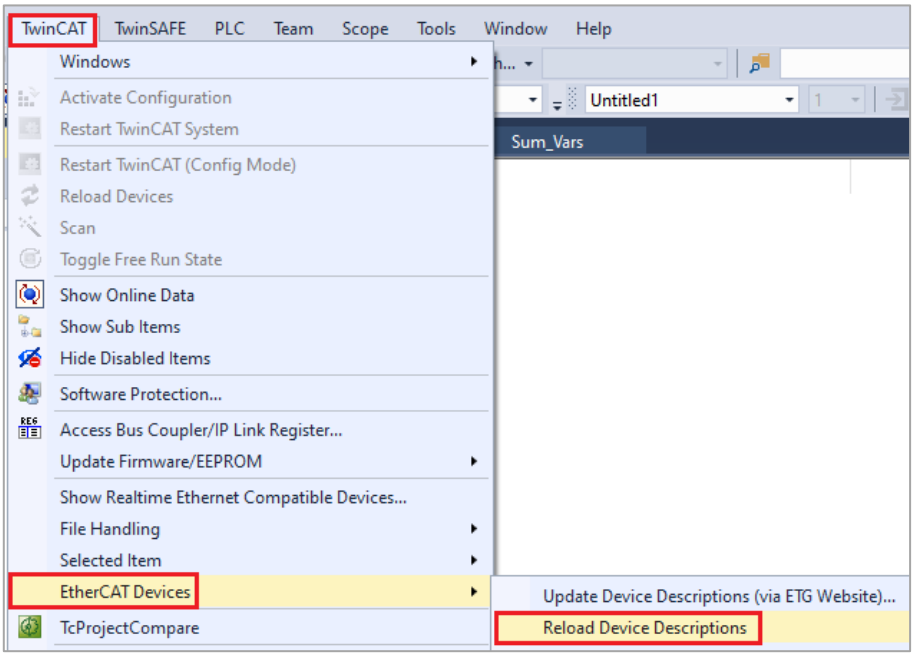


Figure 22: Reload Device Descriptions

9. Connect the 2TH Master EtherCAT to the PC.
10. Open the I/O branch under the solution explorer and right click on devices then select scan.

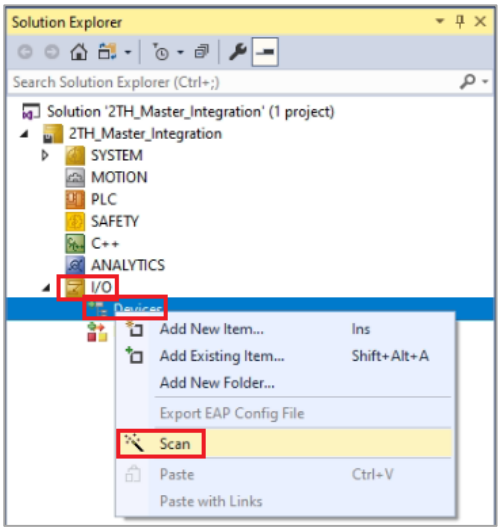


Figure 23: Select Scan in Menu

The scan will first find the PC Ethernet adapter as EtherCAT master to scan for EtherCAT slaves.

11. Click **OK.**

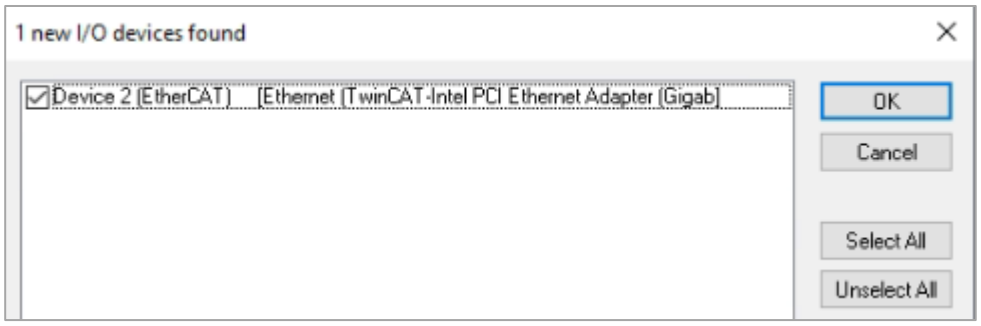


Figure 24: I/O Devices Found

12. It will prompt to scan for boxes - click **yes**: (This step will scan for EtherCAT slaves).

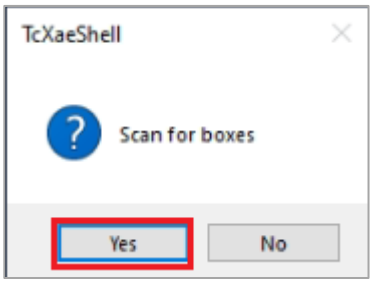


Figure 25: Confirmation to Scan for Boxes

13. It will prompt to Activate Free Run - click **yes**.

    The Device will appear as EtherCAT master (PC network adapter) and under Device, Box is CoreTigo 2TH master.

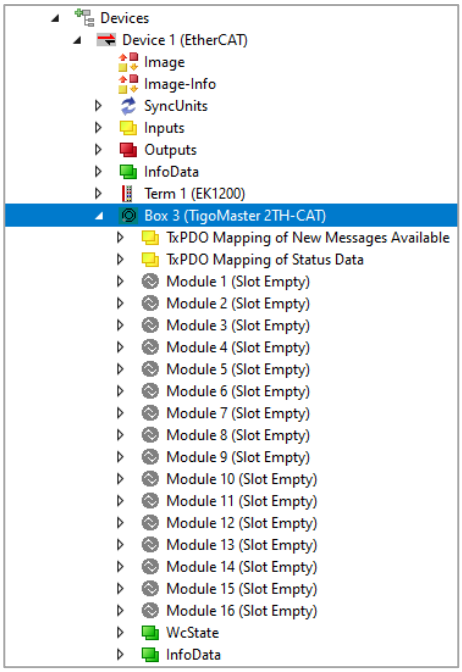


Figure 26: Box Selected

Setting IP address to 2TH Master EtherCAT (see section 5.3.4).

14. Double click on CoreTigo 2TH Master and on the main window select the tab EtherCAT.

15. Click on advanced settings.

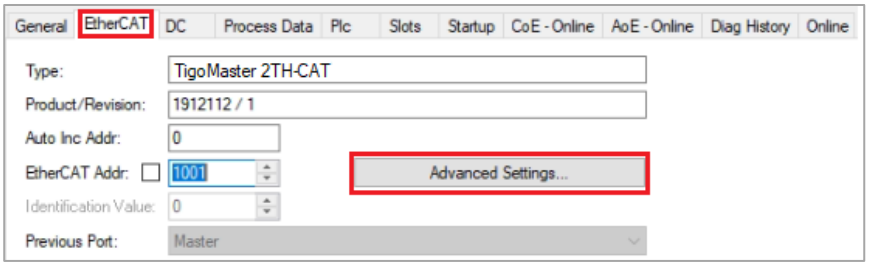


Figure 27: Advanced Settings

16. Open the Mailbox menu and select EoE.
17. Enter the desired IP address, subnet mask and click **ok**.

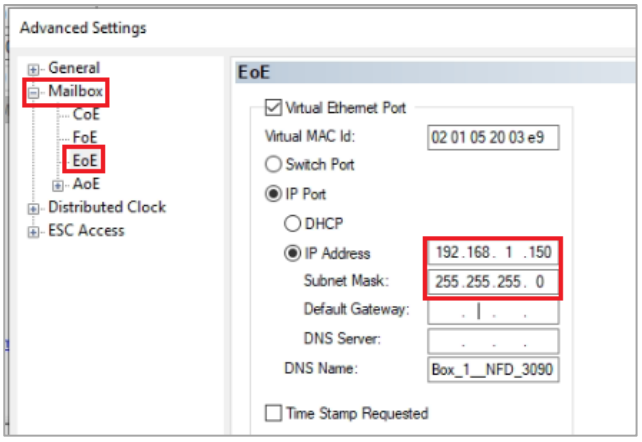


Figure 28: Enter IP Address

18. Click on **Reload Devices** to apply the changes.

Figure 29: Reload Devices Icon

19. Now the 2TH TigoMaster can be configured using TigoEngine.

Figure 30: TigoMasters Listing

20. Modules configuration: (each module is a wireless port).

21. Double click on CoreTigo 2TH Master and on the main window select the tab **Slots**.

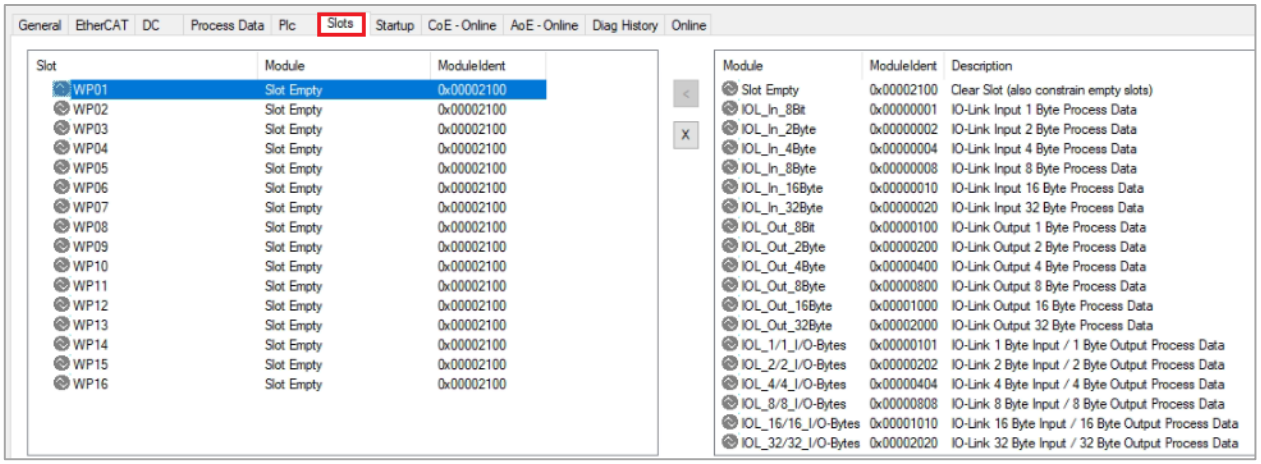


Figure 31: Double Click on the TigoMaster

All slots are disabled by default.

22. In order to enable a slot, select it, click on the X and select the size of the process data.

    In this example, a device paired to WP01 has 2 bytes PDIN and 4 bytes PDOUT so the "IOL_4/4_I/O-Bytes" will be used.

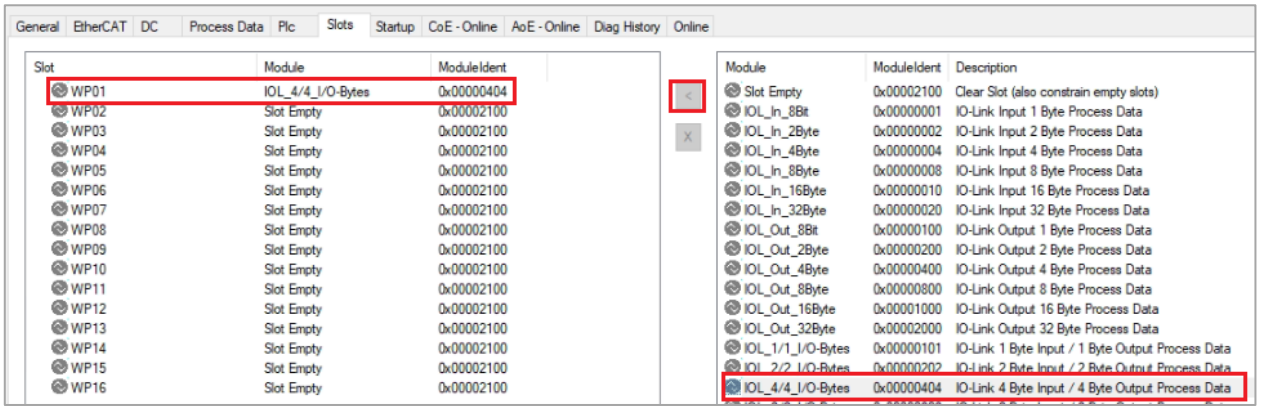


Figure 32: Slots Tab

23. Now under Module 1, TxPDO has 4 bytes and RxPDO has 4 bytes:

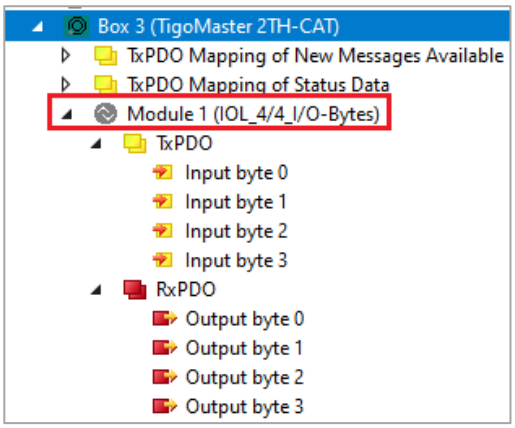


Figure 33: Module 1

24. In the **Startup** tab you can decide whether the configuration of the W-ports (slots) will be configured by the EtherCAT master or not.

    By default when defining a new module, the configuration parameters will be added to the Startup. (The index will be 0x8000 for Wport1, 0x8010 for Wport2,0x8020 for Wport3, etc..)

25. In order to edit the parameters, double click and change its value.

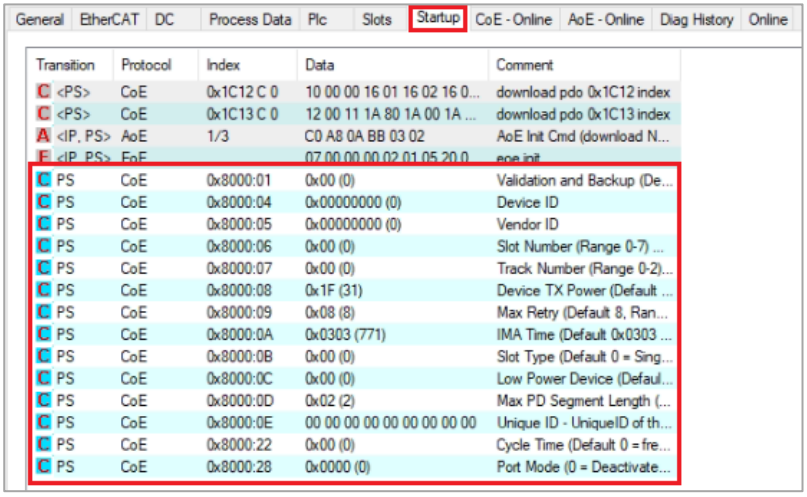


Figure 34: Startup Tab

26. If you want the EtherCAT master to not change the W-ports (slots) configuration, select all the rows and delete.

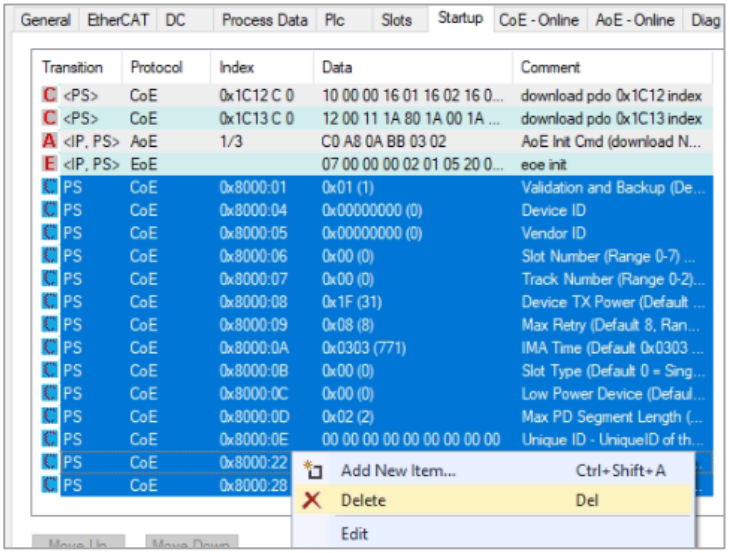


Figure 35: Delete Rows

In **CoE - Online** tab we can see the online data of the W-port.

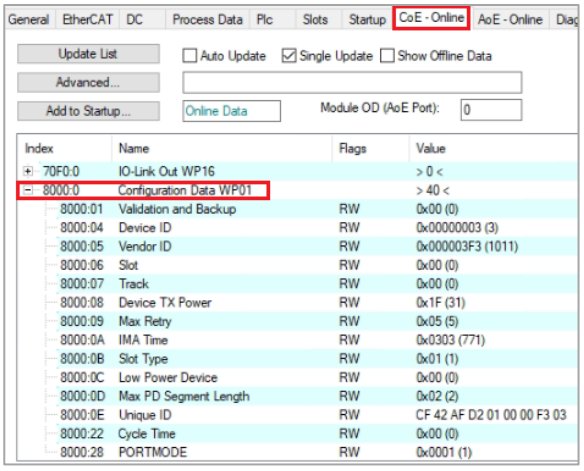


Figure 36: CoE-Online Tab

The state of the Wport can be monitored as well:

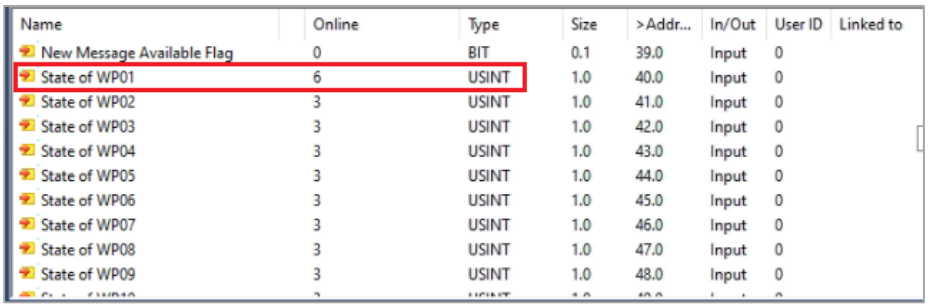


Figure 37: State of Wport

27. Click on **Reload Devices** to apply the changes.

Figure 38: Reload Devices Icon

28. Now the **PDIN** values can be monitored when selecting the required Input Byte and online.

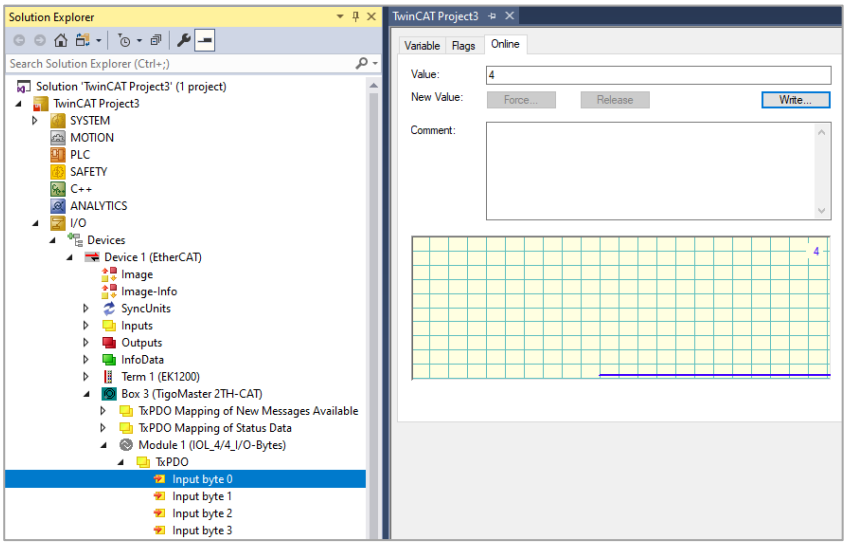


Figure 39: Select Input Byte

29. The **PDOUT** can be written as well by selecting the required output Byte and monitor.

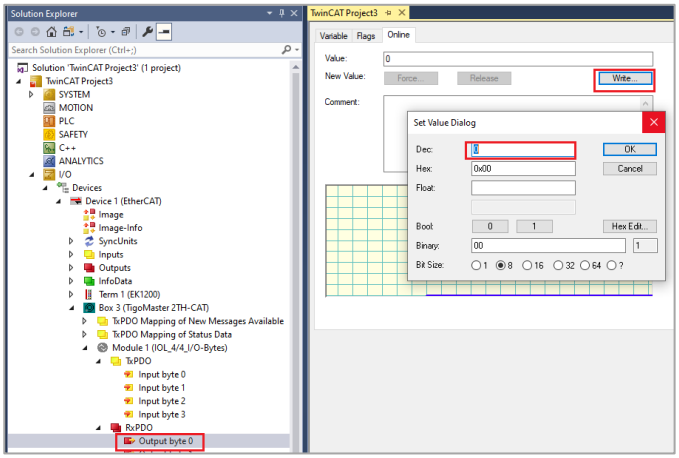


Figure 40: Select Output Byte

5.4. TigoEngine

Reference(s):
The TigoEngine – User Manual gives further details on how to configure TigoMaster 2TH using TigoEngine

5.4.1. 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.

5.4.2. Connect a New Master

Note:
Before connecting a new TigoMaster 2TH to the 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.

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

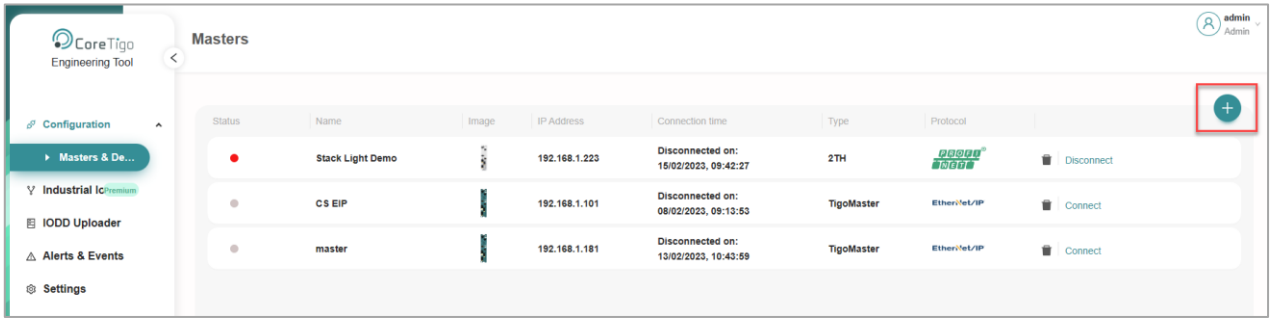


Figure 41: Connect New Master Button

2. 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 that you want to connect to the TigoEngine.
   - **Master Type** – select TigoMaster 2TH from the drop-down list.

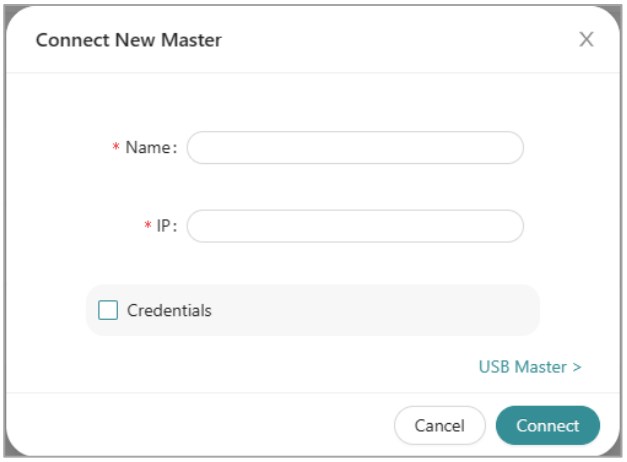


Figure 42: Connect New Master

3. 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.

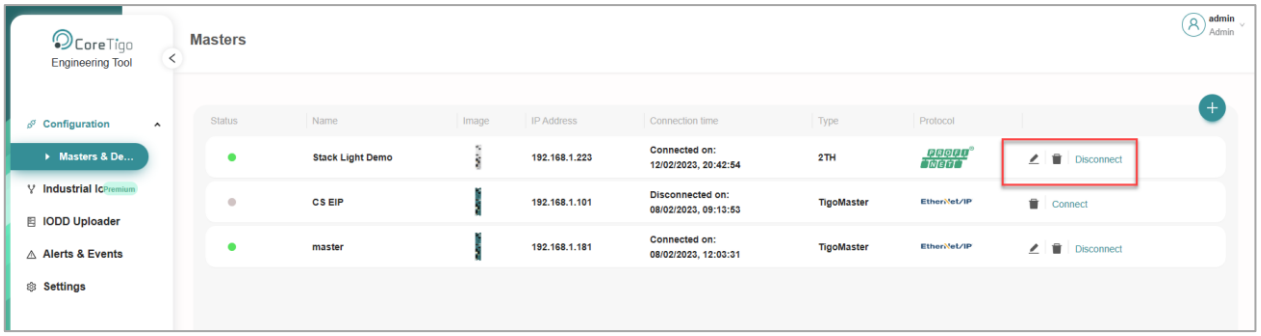


Figure 43: Masters View – Three TigoMasters 2TH Connected

5.4.3. Configure Parameters

For details of port parameters, see section 5.2.4 of this User Manual.

For further details of how to use TigoEngine, see the *TigoEngine User Manual*.

5.5. CoreTigo Web Server

The CoreTigo Web Server enables you 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 how you can use 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.

5.5.1. Prerequisites

To use the CoreTigo Web Server, you need the following:

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

    Username = root
    Password = password
- A note of the 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.

5.5.2. 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 26: 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
Wireless port WP01, WP02, WP03 …	(all)	Port-specific information and settings for the wireless IO-Link ports WP01, WP02, WP03 …	Device or port information

Menu	Tab	Description	Section
	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	

5.5.3. 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: 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.

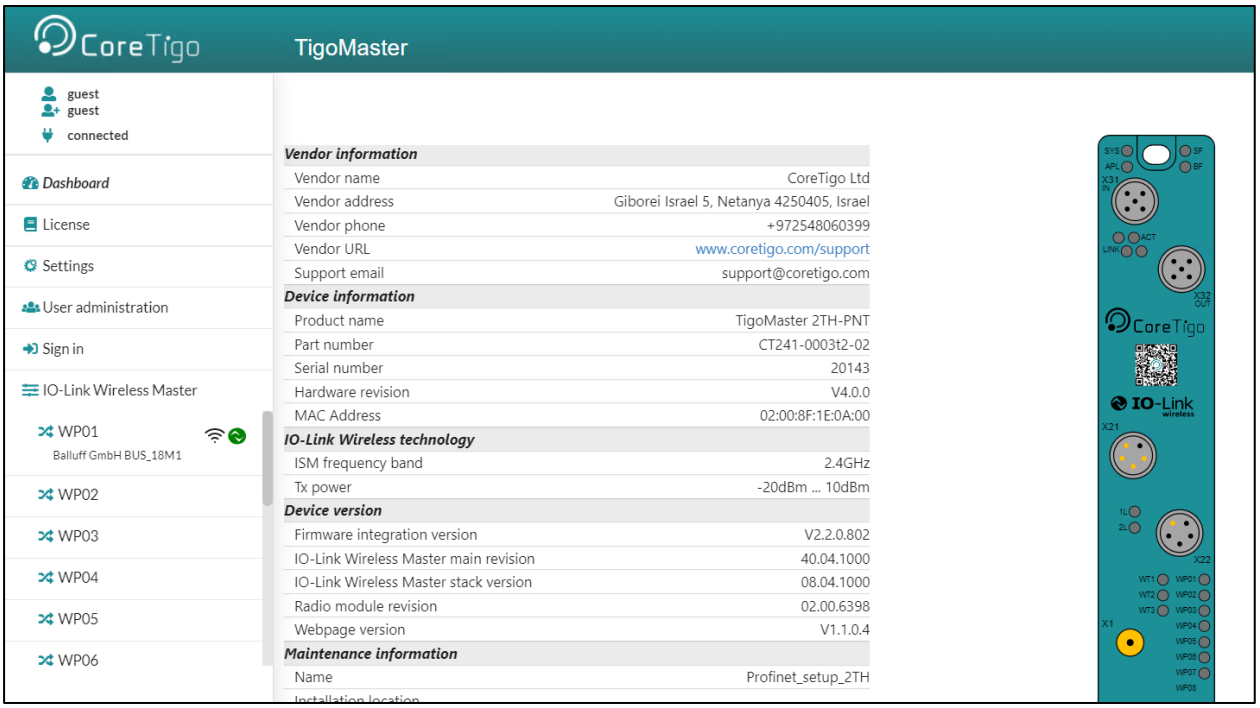


Figure 44: CoreTigo Web Server Dashboard

Table 27: 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.

5.5.4. 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.

5.6. 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 track0, track1, or track2

  For further details, see section 5.6.3.
- **Scan** tab – here you can scan for unconnected IO-Link devices. A scan result then shows the found devices.

5.6.1. Channel Selection

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

   The **Channel Selection** tab appears.

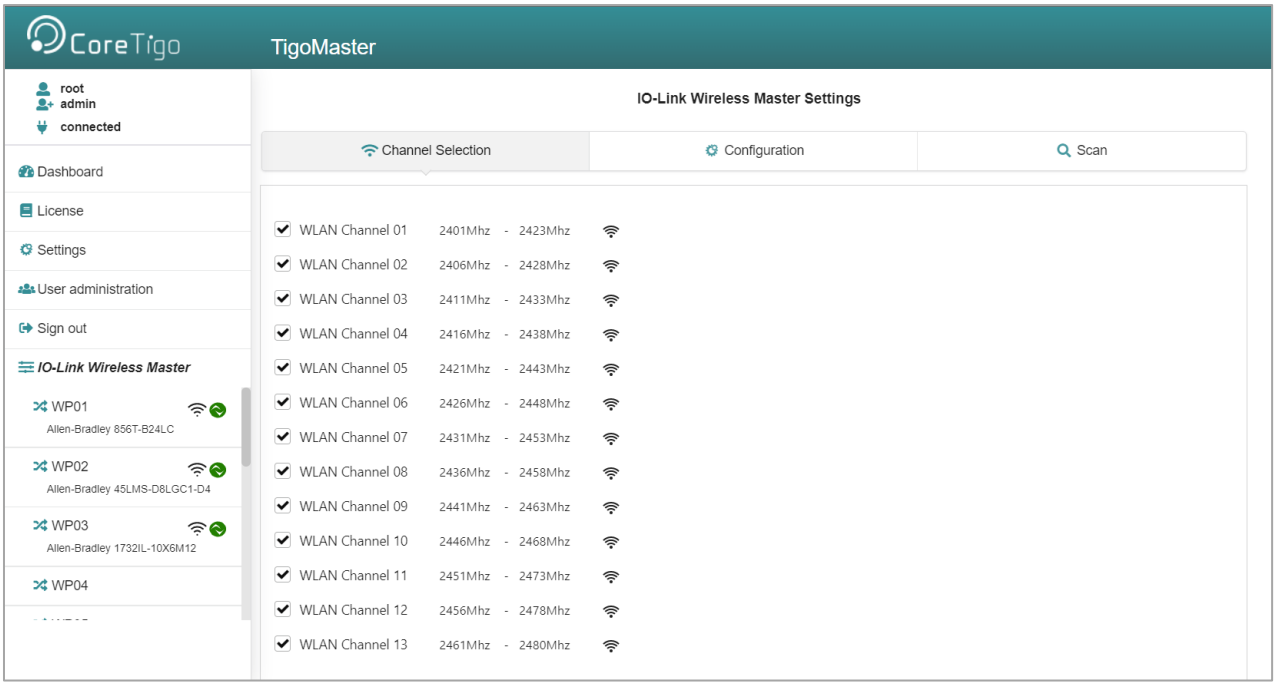


Figure 45: Channel Selection Tab

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

   The selected WLAN channels are configured.

Table 2: 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 partialy. Hover to indicate the help text. 	• checked” • unchecked (default)

5.6.2. 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.

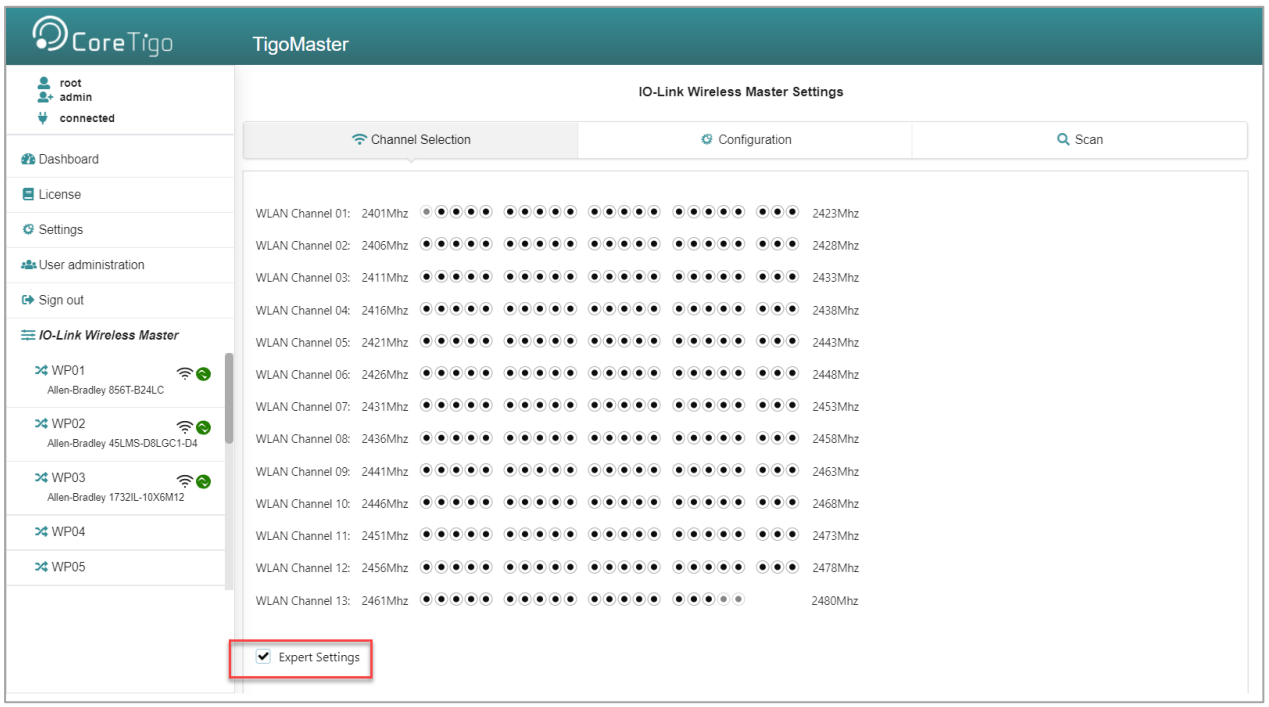


Figure 46: Expert Settings

5.6.3. 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.

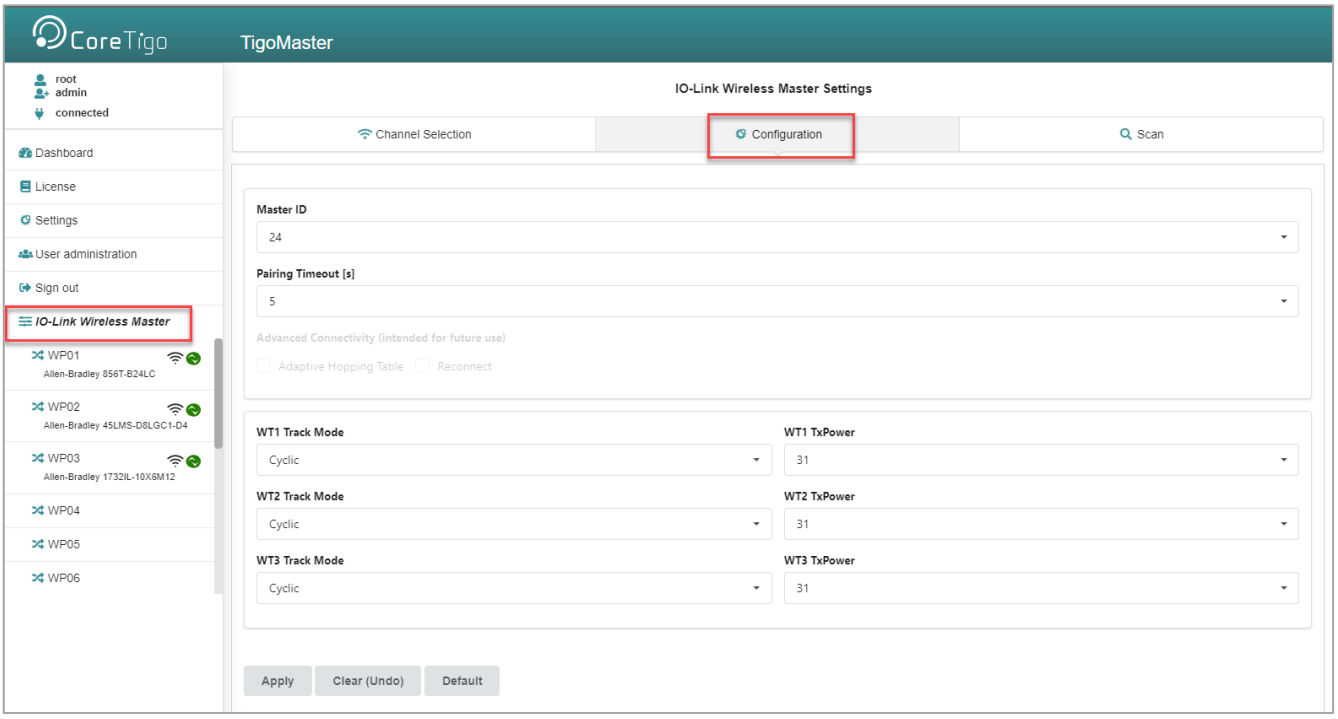


Figure 47: Configuration Tab

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

Table 29: 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.

5.6.4. 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.

5.6.5. Scan and Pair

5.6.5.1. Scan

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

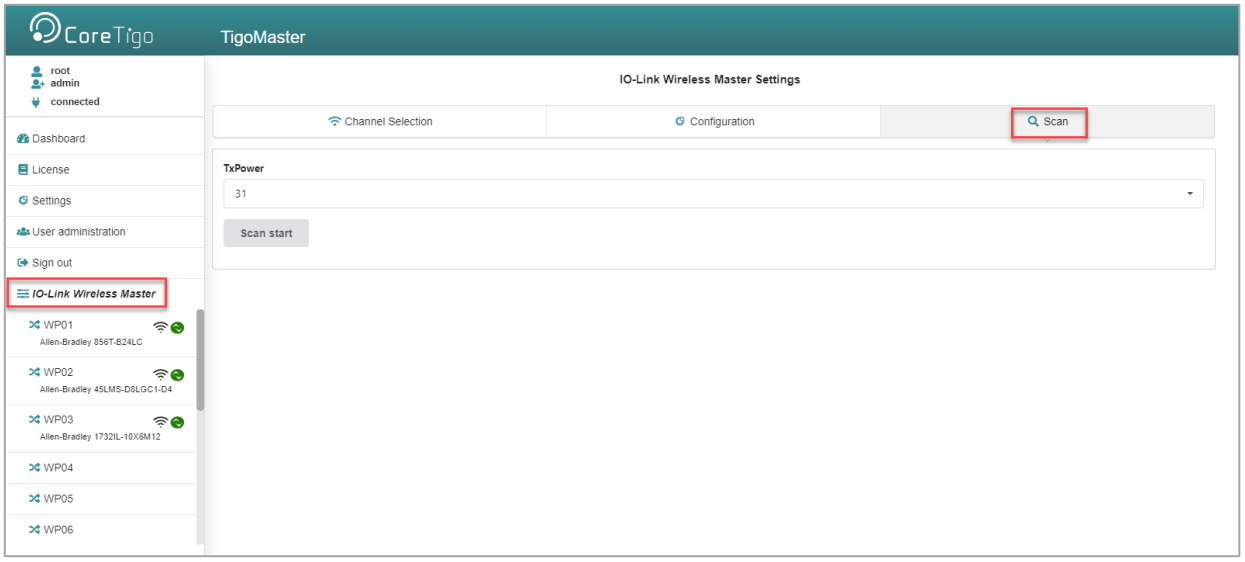


Figure 48: Scan Tab

3. Use the **Scan** tab, to scan for unconnected devices.
4. Select **TxPower**.

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

   The system searches for unconnected devices.

The scan result is displayed after a few moments.

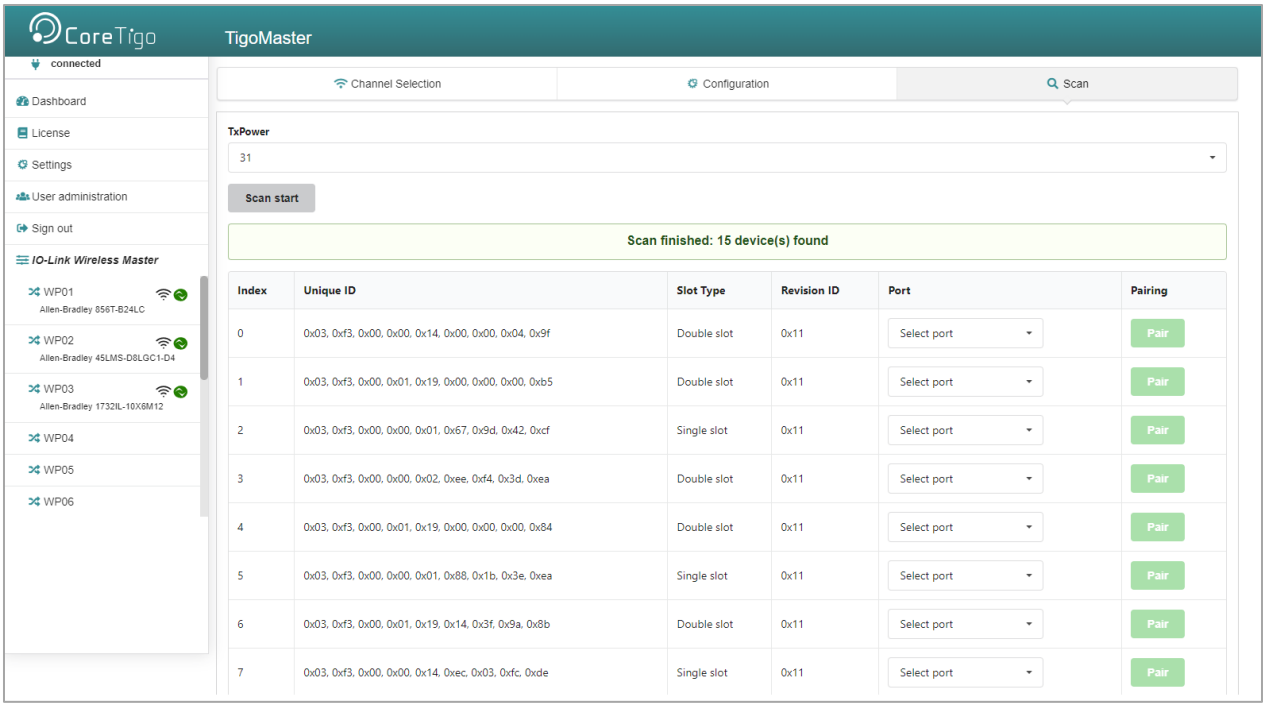


Figure 49: Scan Result

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 30: 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**)

5.6.5.2. Pair / Unpair

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

1. In the **Scan** tab in the scan result, select the **Port**.
2. Click 

.

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

   The message **Pairing successful** appears.

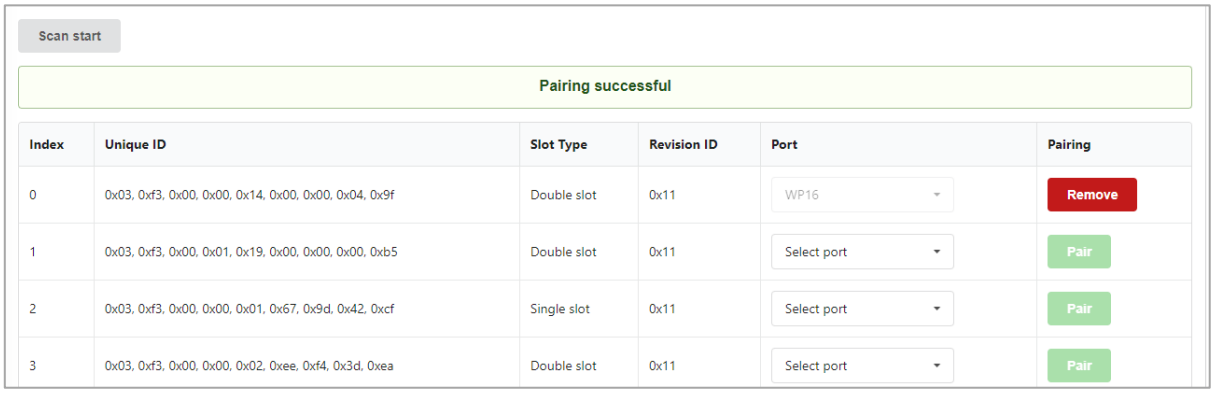
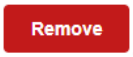


Figure 50: Pairing Successful

3. You can 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 51: Unpairing Successful

5.7. Device or Port Information

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

In the **Settings** tab you also 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.

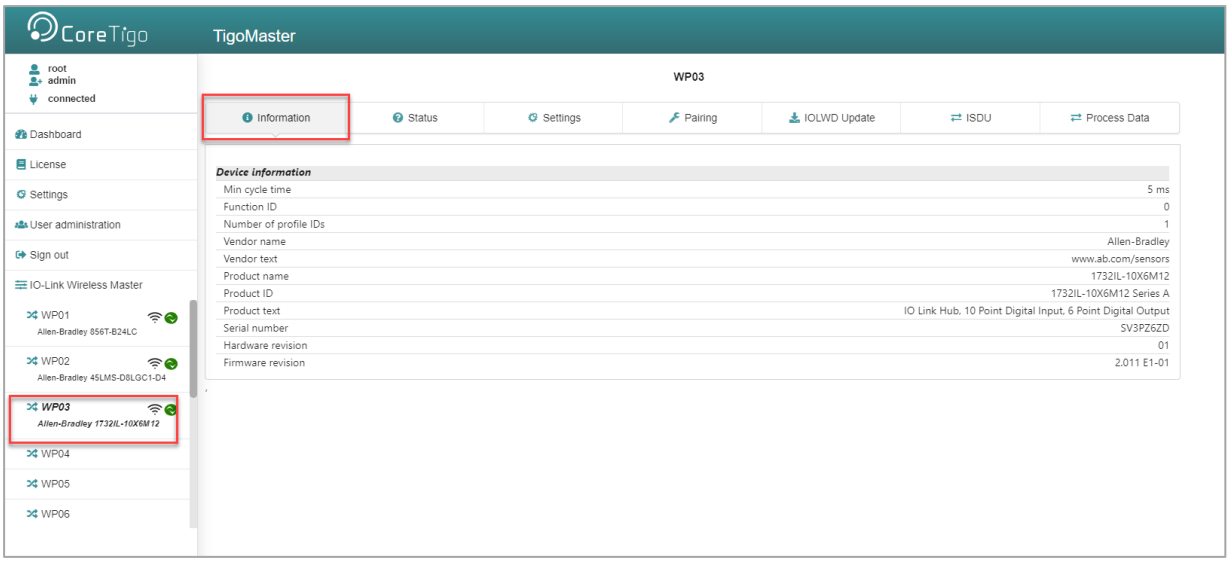


Figure 52: Information Tab

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

Table 31: 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)

5.7.1. 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.

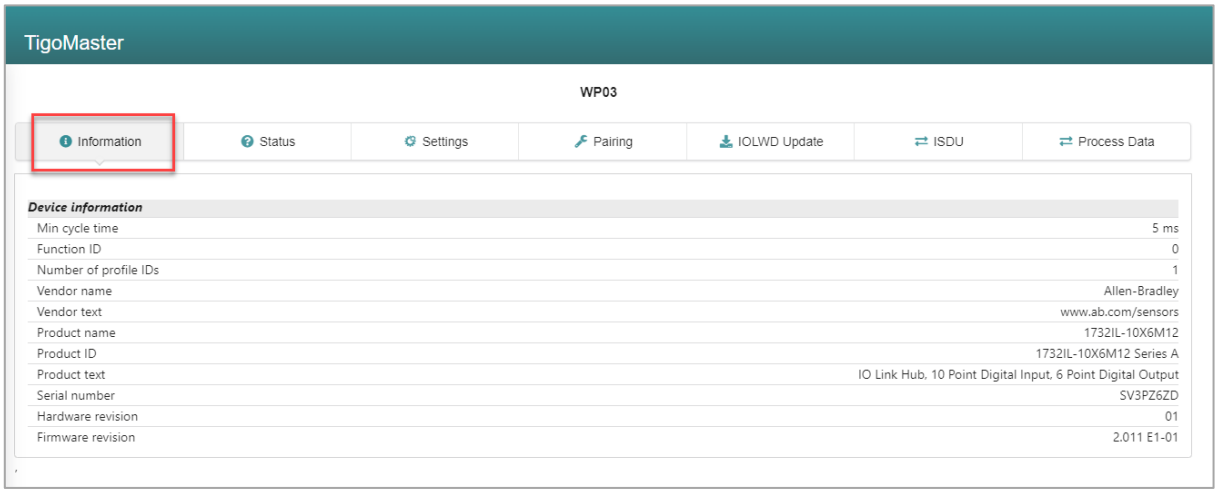


Figure 53: Information Tab – Device Information

Table 32: 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)

Parameter	Description	Value/Value Range
Product text	Description of function or characteristic of connected device.	Character string (up to 64 characters)
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)

5.7.2. 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.

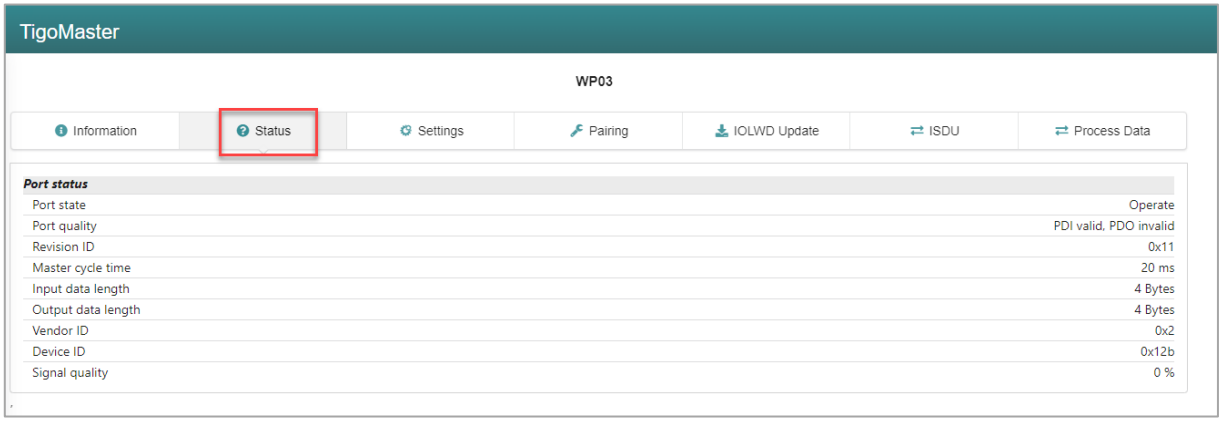


Figure 54: Port Status Tab

Table 33: 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.

Parameter	Description	Value/Value Range
Revision ID	Revision ID of the connected device. This parameter is specified by the connected device. It indicates software revision running on the connected device.	0: No device connected Others: Revision ID of 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 wireless IO-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 34: 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.

Value	Description
Communication lost	The communication to the device is broken down.
Revision fault	An error was found during revision check.
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.

5.7.3. 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.

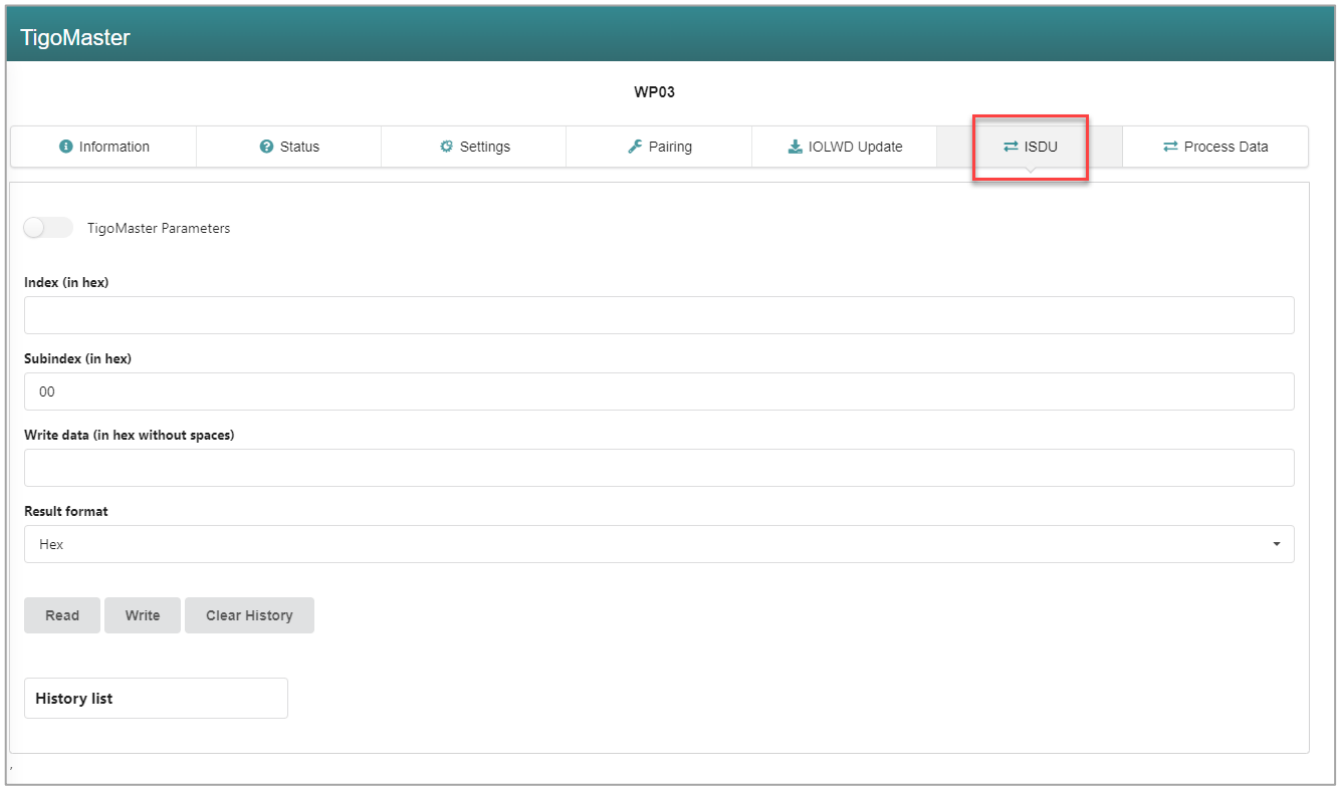


Figure 55: Display of On Request Data, Read/Write IO-Link Device Parameters

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.

5.7.3.1. 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.

5.7.3.2. 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.

5.7.3.3. 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 56: 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.

5.7.3.4. 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 following structure:

   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>)

5.7.3.5. 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.

5.7.4. 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.

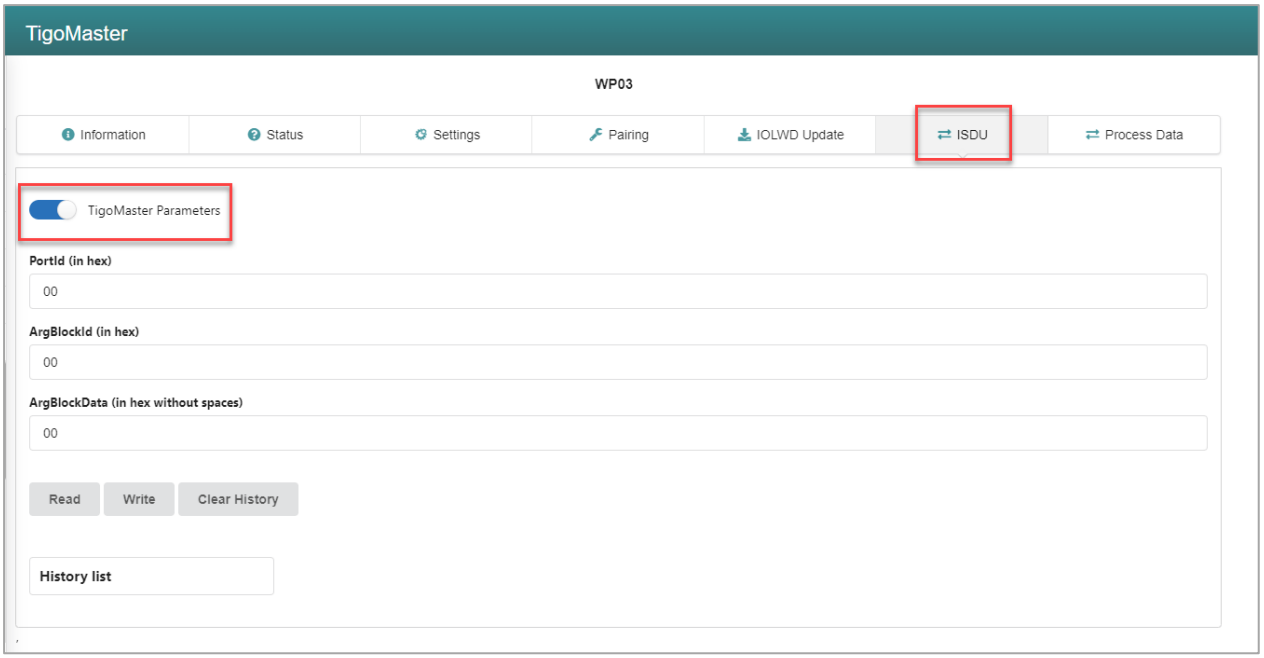


Figure 57: Display of the ISDU, Read/Write IO-Link Wireless Master Parameters

5.7.4.1. 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.

5.7.4.2. Access to IO-Link Wireless Master

To access the data of the IO-Link Wireless Master via **PortId** and **ArgBlockId** (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.

5.7.4.3. 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.

5.7.4.4. 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>)

5.7.4.5. 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.

5.7.5. 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.

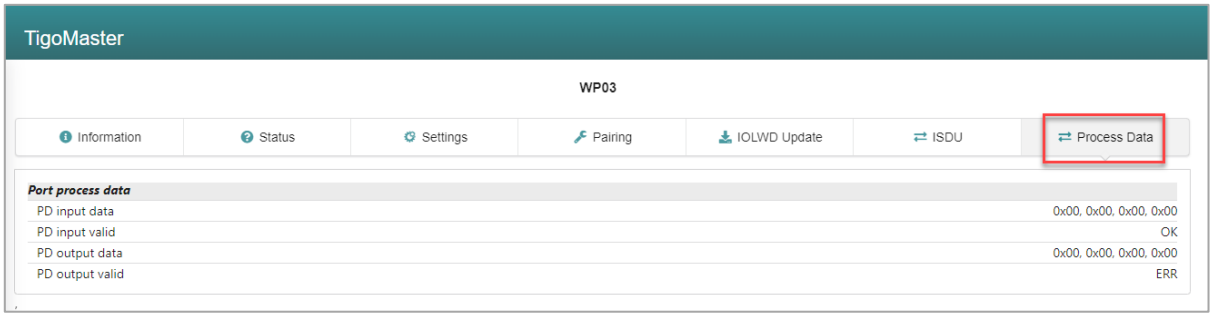


Figure 58: Display of the Process Data

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

Table 35: 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.

5.8. 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.

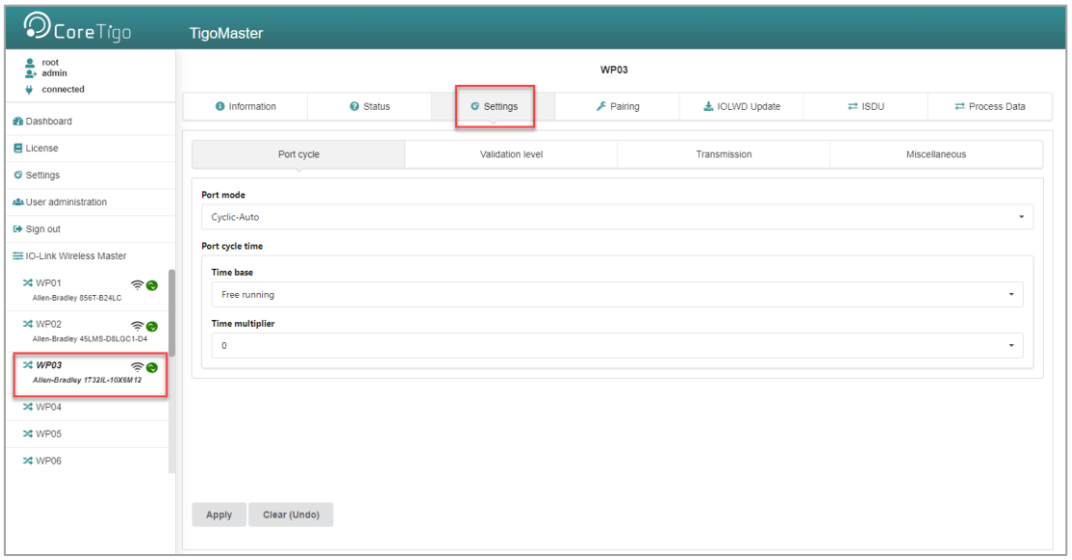


Figure 59: Settings Tab

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

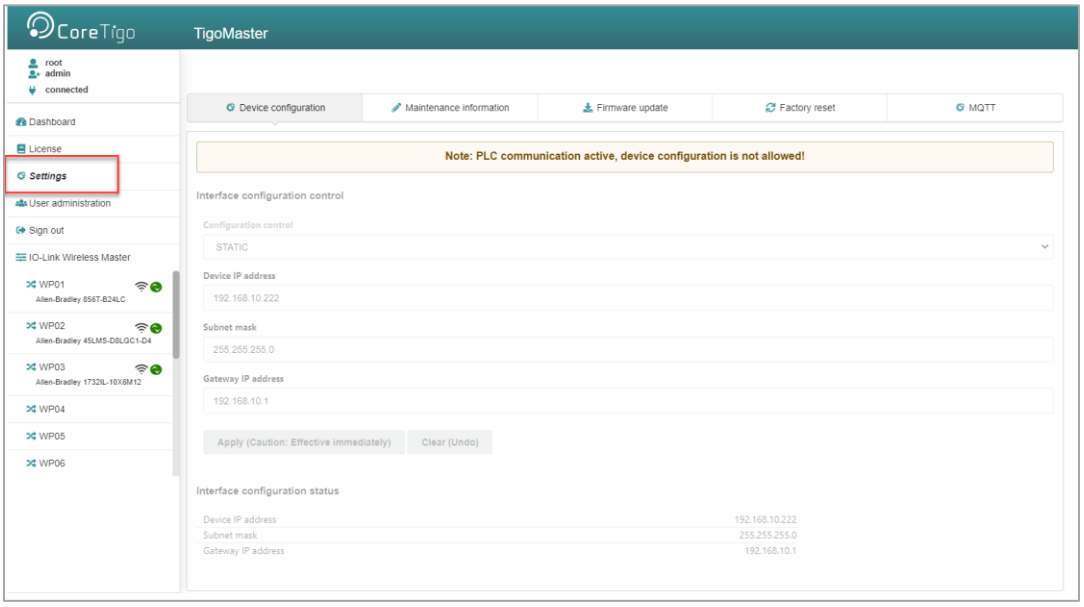


Figure 60: Device Configuration Subtab

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

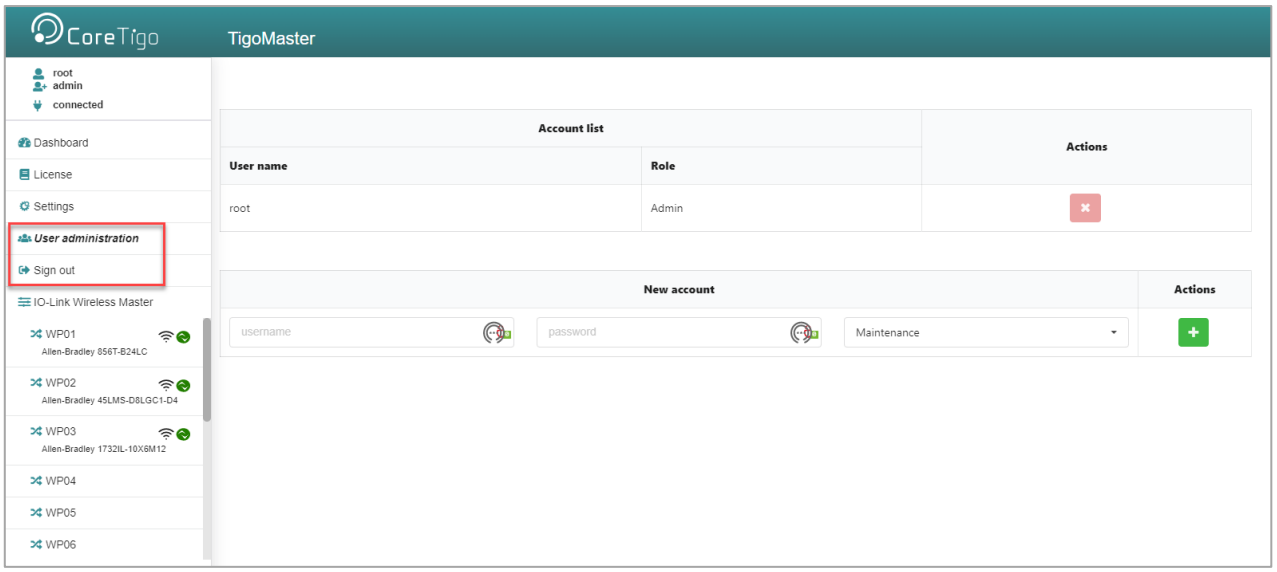


Figure 61: User Administration

5.8.1. 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.

5.8.1.1. Settings > Port Cycle

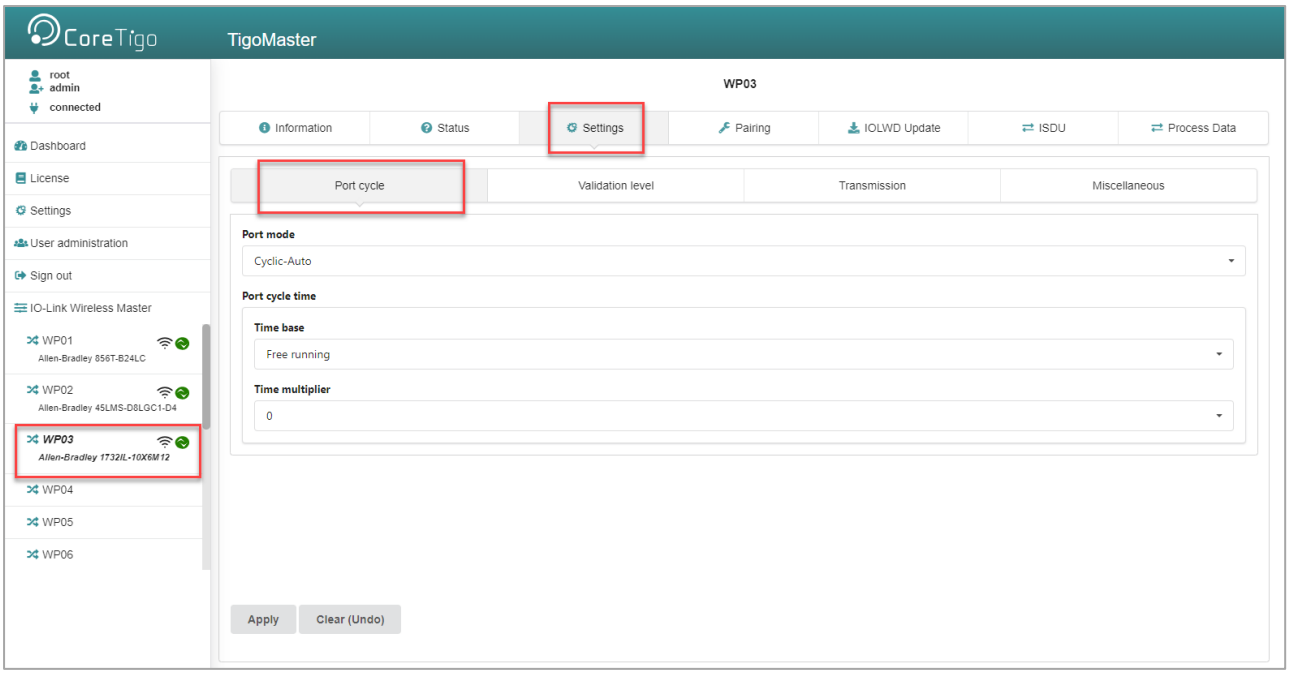


Figure 62: Settings Tab, Port Cycle Subtab

Table 36: 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 37: 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).`**

5.8.1.2. Settings > Validation level

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

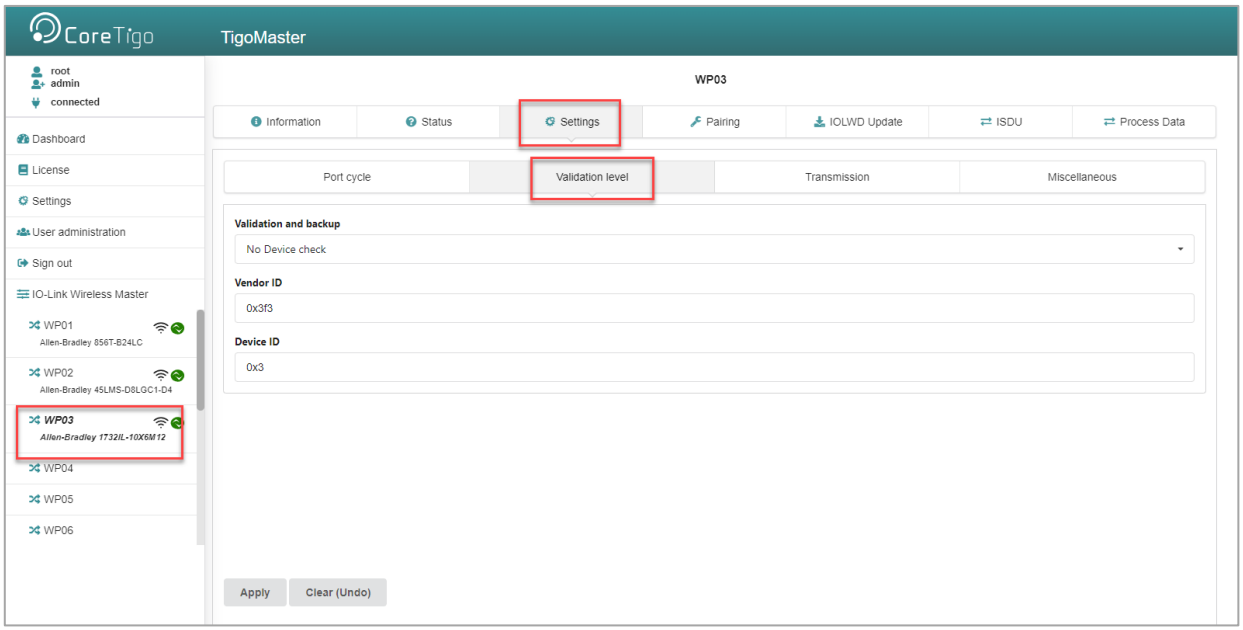


Figure 63: Settings Tab, Validation Level Subtab

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 38: 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 39: 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.	

5.8.1.3. Settings > Transmission

1. Open the **Transmission** subtab.

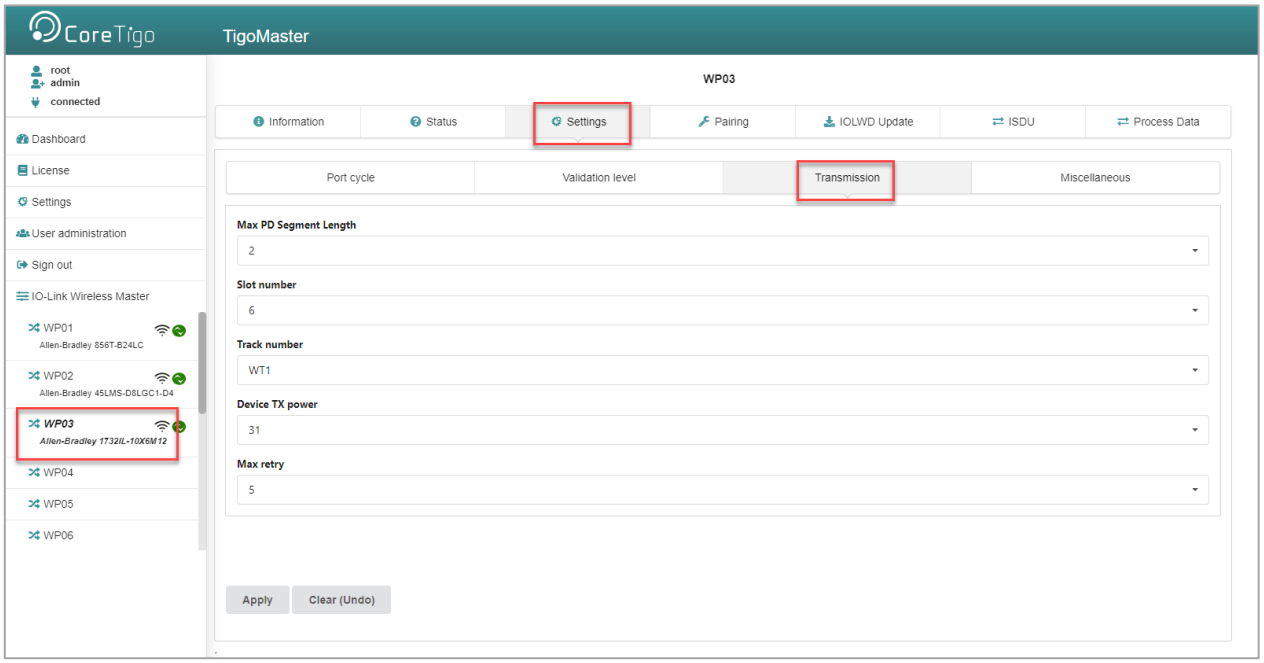


Figure 64: Settings Tab, Transmission Subtab

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

Table 3: 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

5.8.1.4. Settings > Miscellaneous

1. Open the **Miscellaneous** subtab.

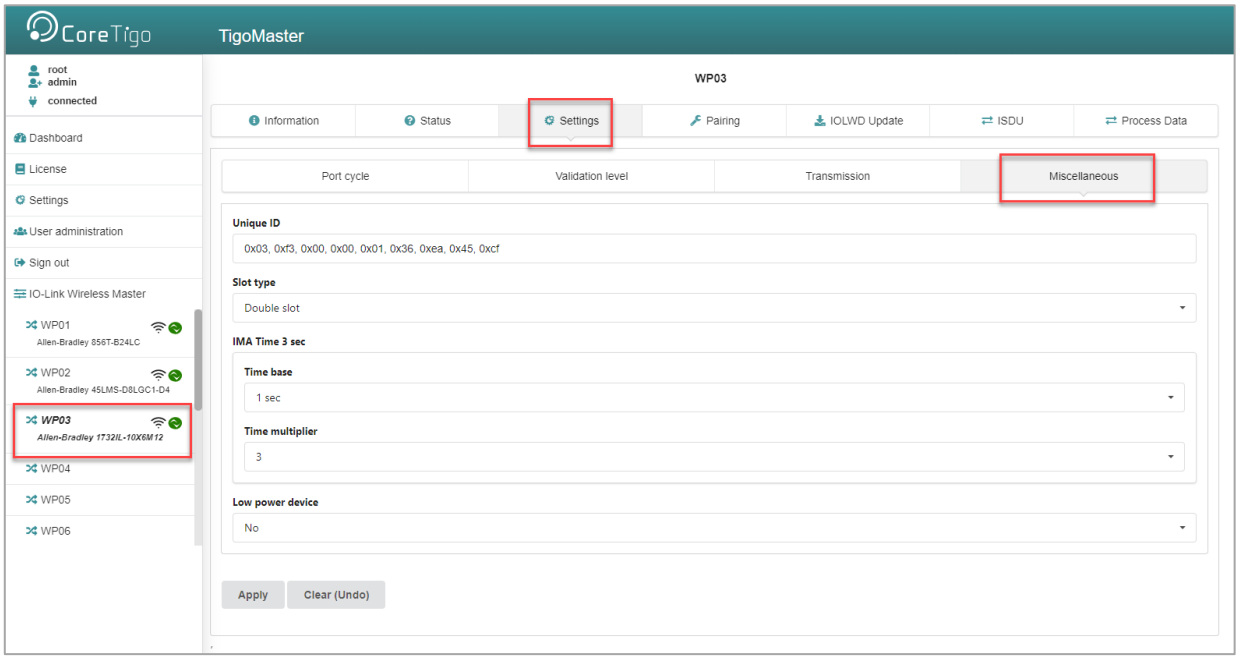


Figure 65: Settings Tab, Miscellaneous Subtab

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 41: 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 higher values 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.

5.8.2. IP Parameters

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

   The **Device configuration** tab is displayed.

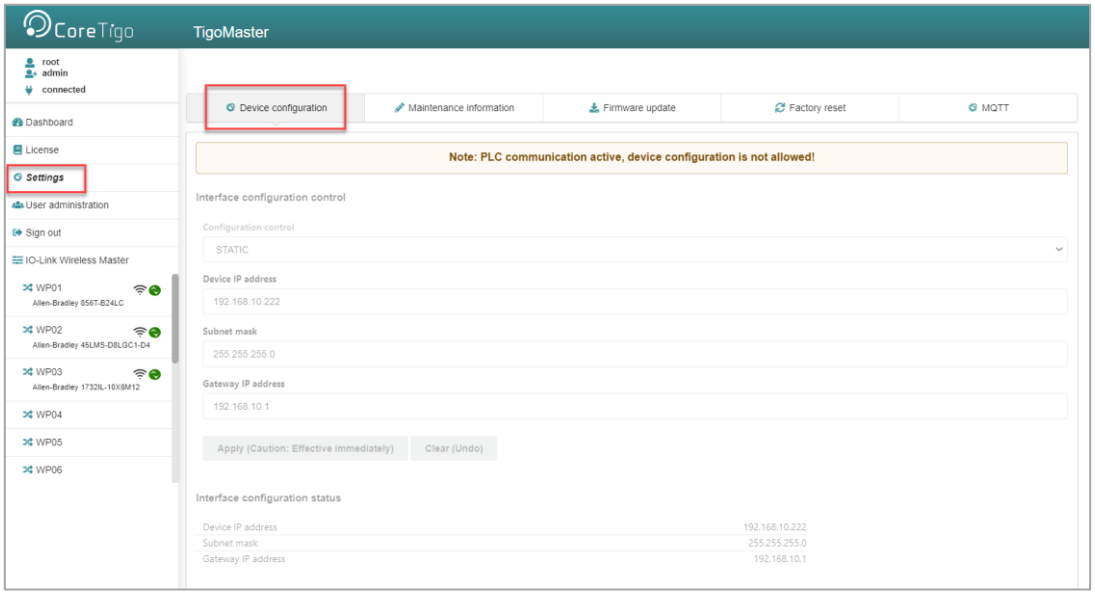


Figure 66: Device Configuration Tab

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

5.8.3. 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.

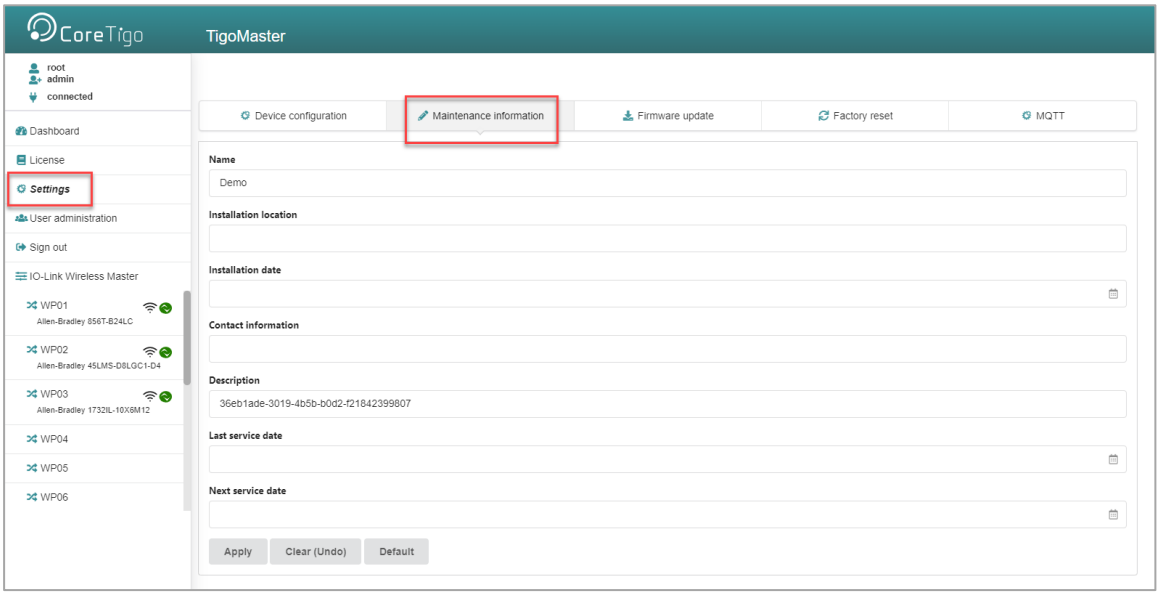


Figure 67: Maintenance Information Tab

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

Table 42: 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.

5.8.4. 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.

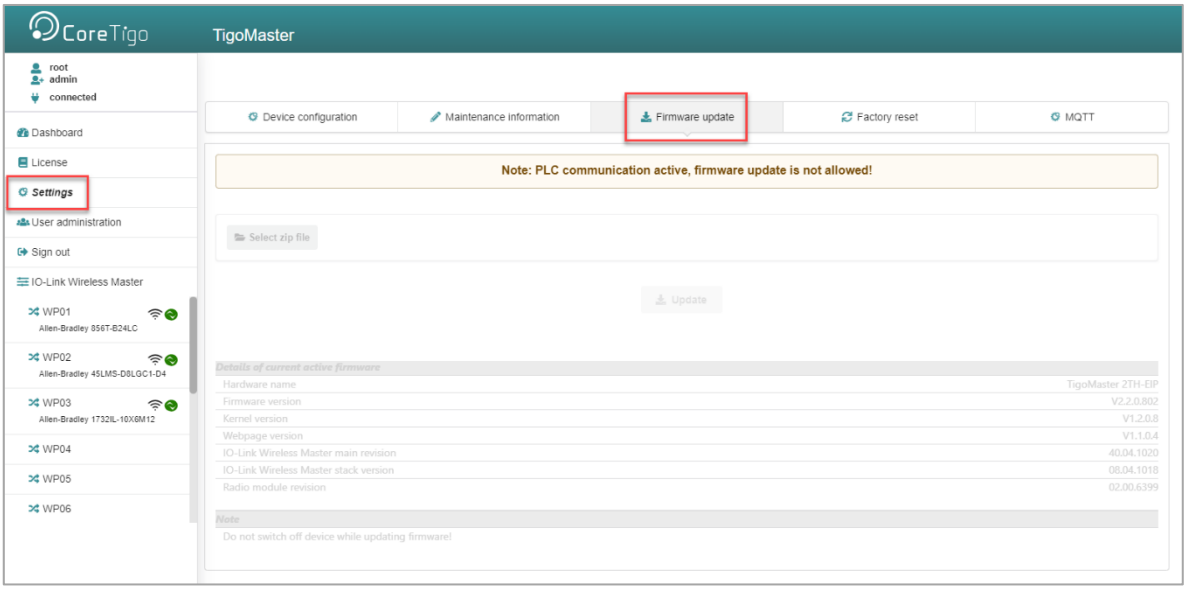


Figure 68: Firmware Update Tab

5.8.4.1. 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.

5.8.4.2. 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.

5.8.5. 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.

5.8.6. 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.

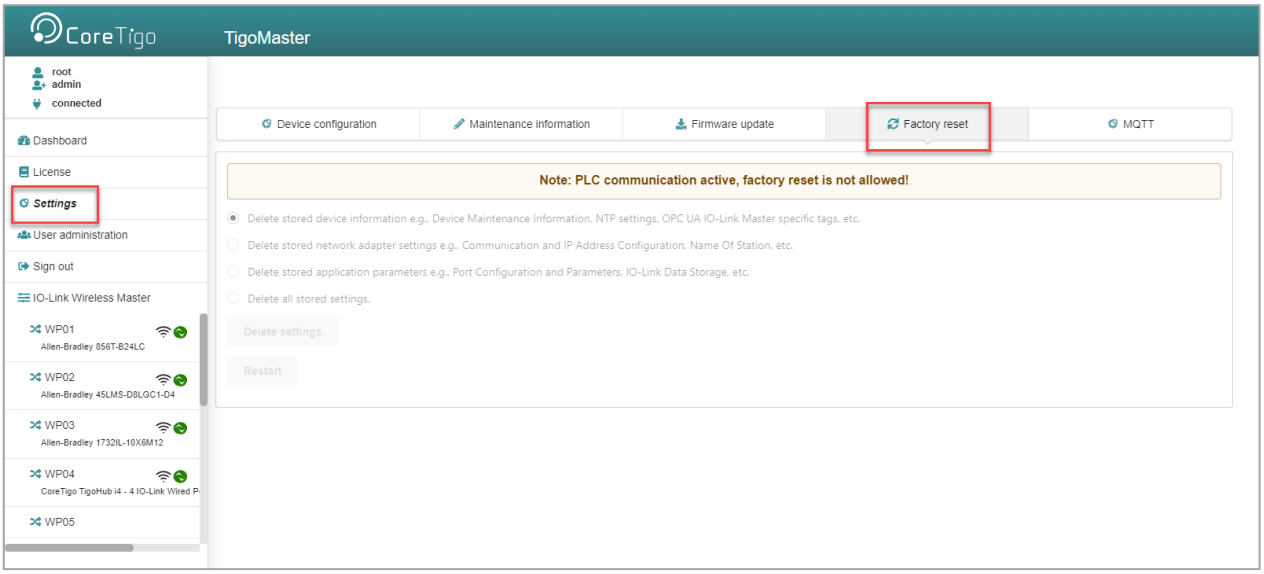


Figure 69: Factory Reset Tab

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 43: 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.

5.8.7. 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.

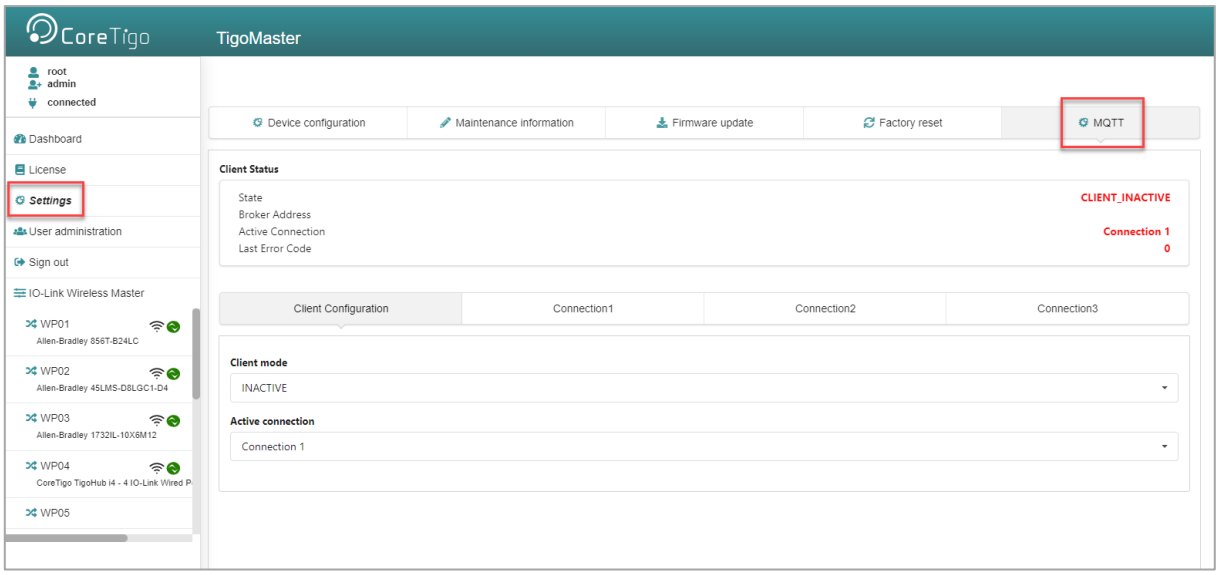


Figure 70: MQTT Tab

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

5.8.7.1. MQTT > Client Status and Client Configuration

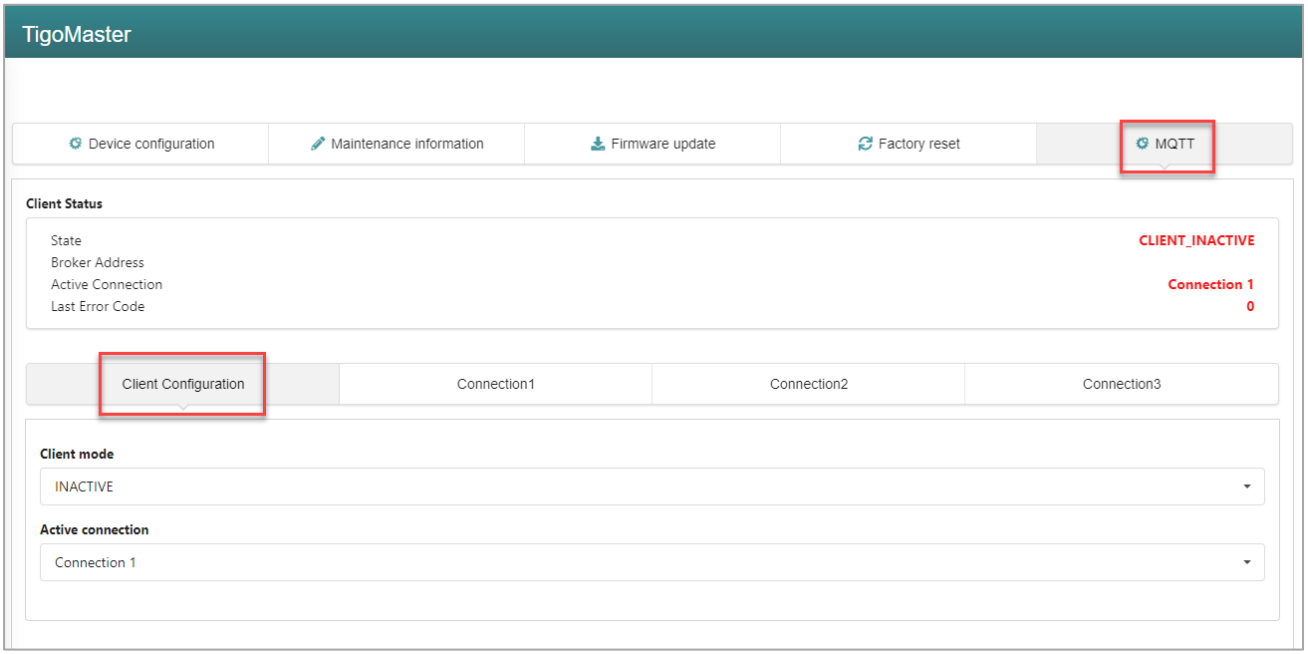


Figure 71: MQTT Tab, Client Status, Client Configuration Subtab

Table 44: 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_INACTIV" 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 45: 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

5.8.7.2. MQTT > Connection1 > IP Settings

1. Open the **Connection1** subtab.

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

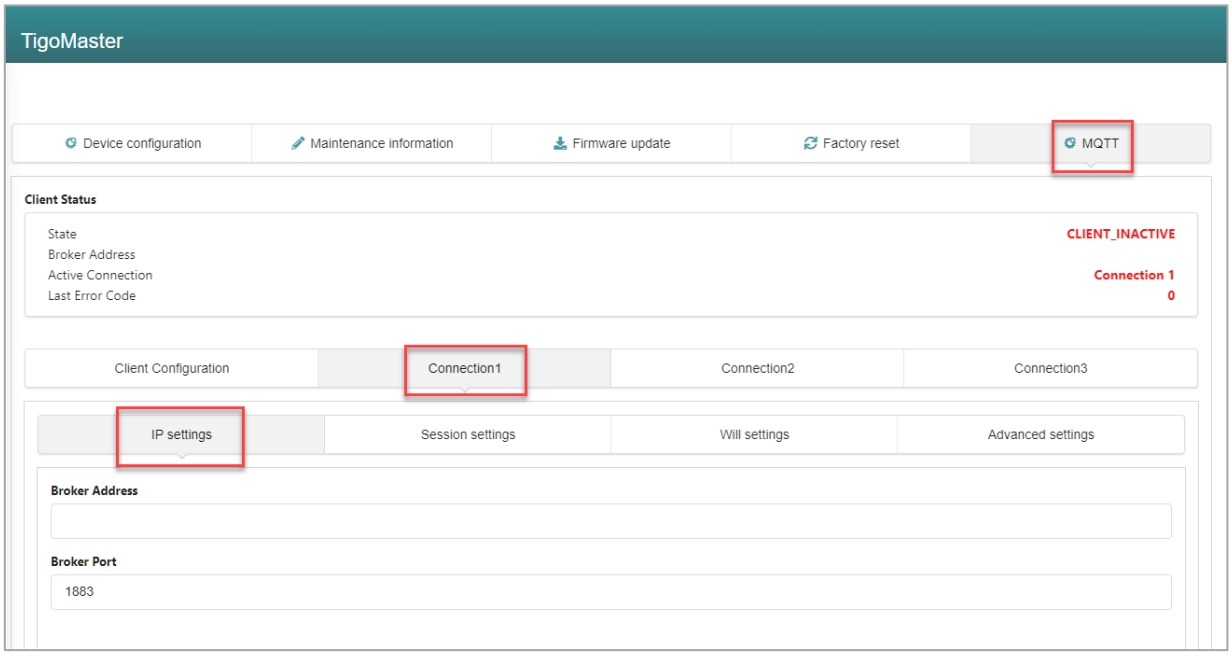


Figure 72: MQTT Tab, Connection 1 > IP Settings Subtab

Table 46: 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

5.8.7.3. MQTT > Connection1 > Session Settings

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

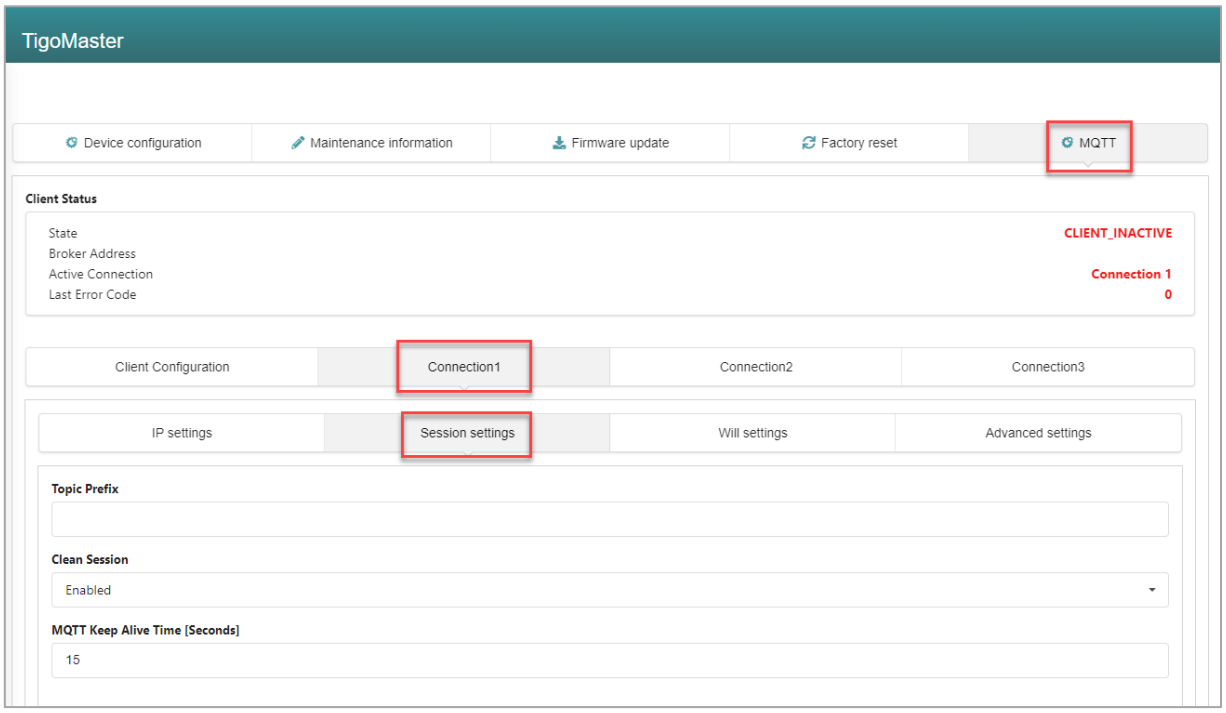


Figure 73: MQTT Tab, Connection1 > Session Settings Subtab

Table 47: 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. 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.	Specified in s. 0 = send no sign of life to the broker. Default: 0

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

5.8.7.4. MQTT > Connection1 > Will Settings

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

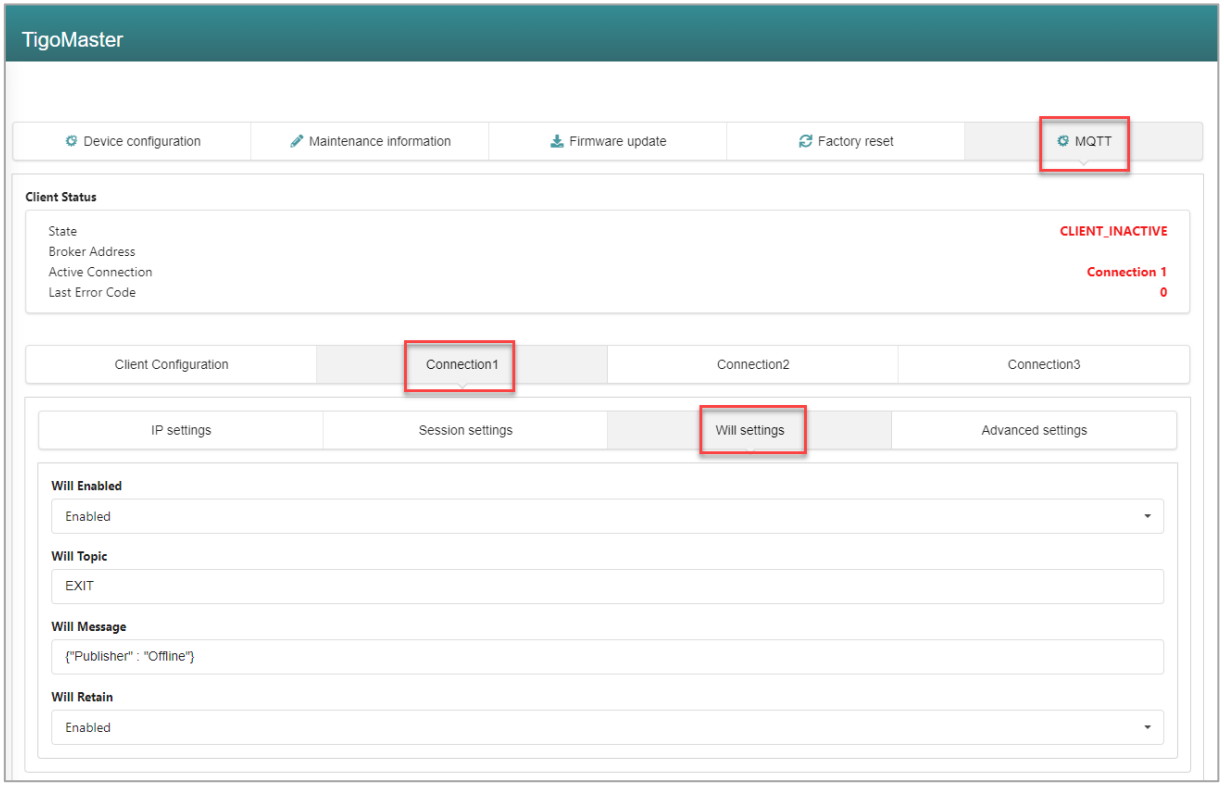


Figure 74: MQTT Tab, Connection1 > Will Settings Subtab

Table 48: 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]

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 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

5.8.7.5. MQTT > Connection1 > Advanced Settings

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

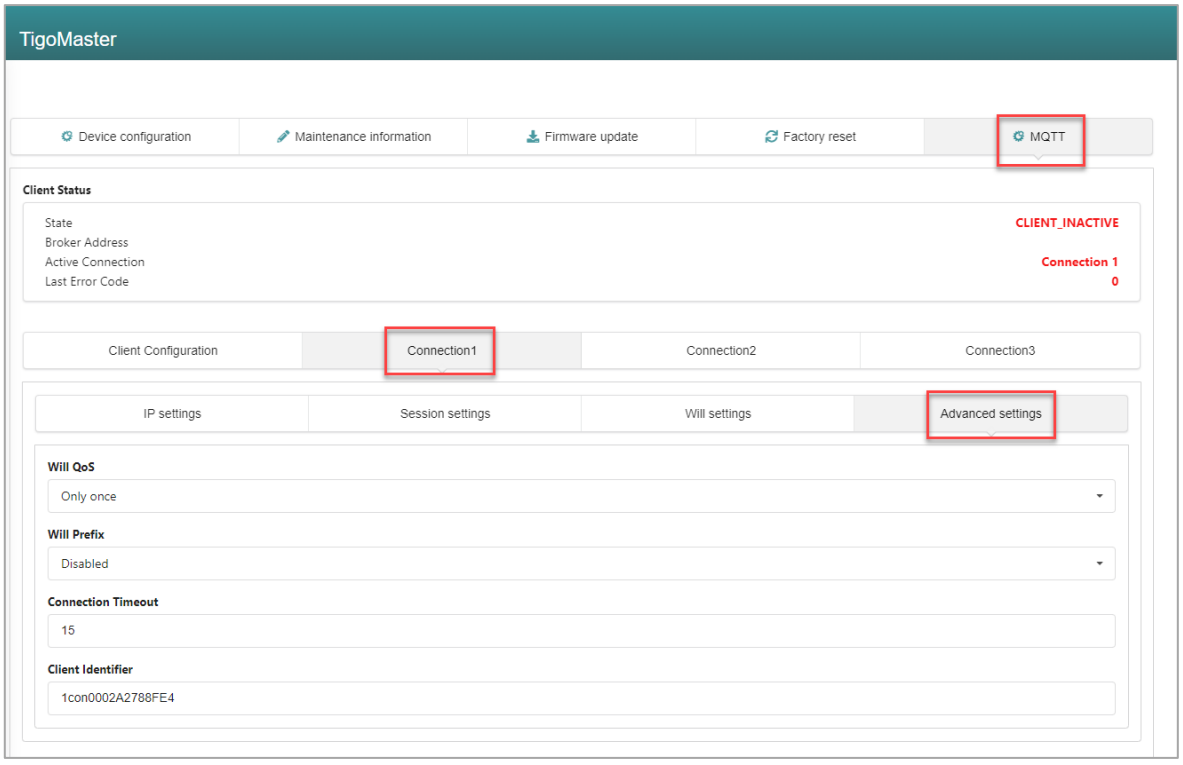


Figure 75: MQTT Tab, Connection1 > Advanced Settings Subtab

Table 49: 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

5.8.8. Log In and User Administration

5.8.8.1. 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 user name and password appears:

Figure 76: Menu Item Sign In - Input Mask for Username and Password

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

   If you have entered a known user name 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**.

5.8.8.2. 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).

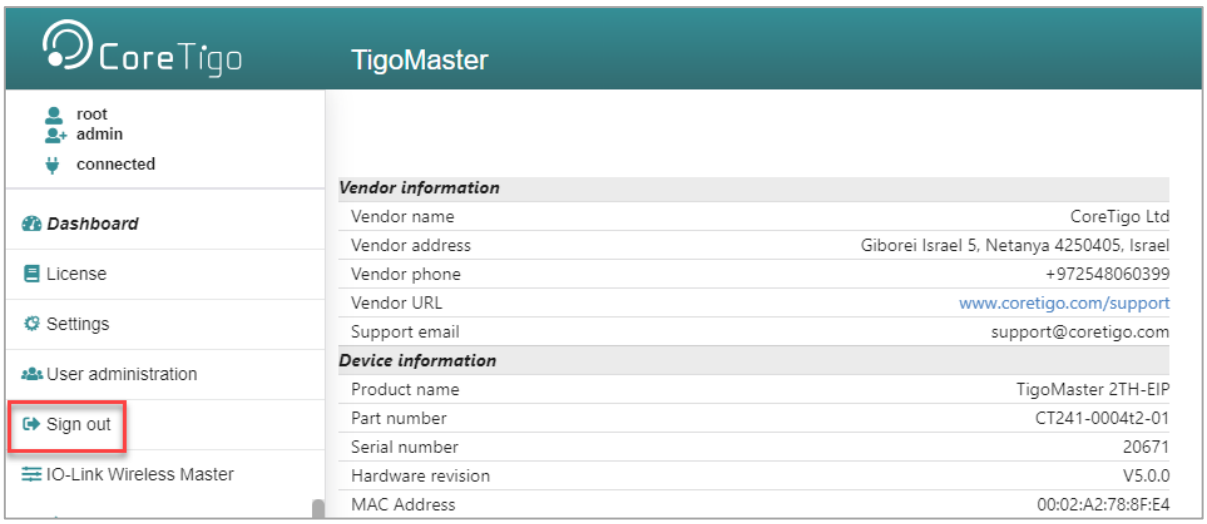


Figure 77: Menu Item Sign Out

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.

5.8.8.3. 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.

5.8.8.4. 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 user name “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.

5.8.8.5. 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.

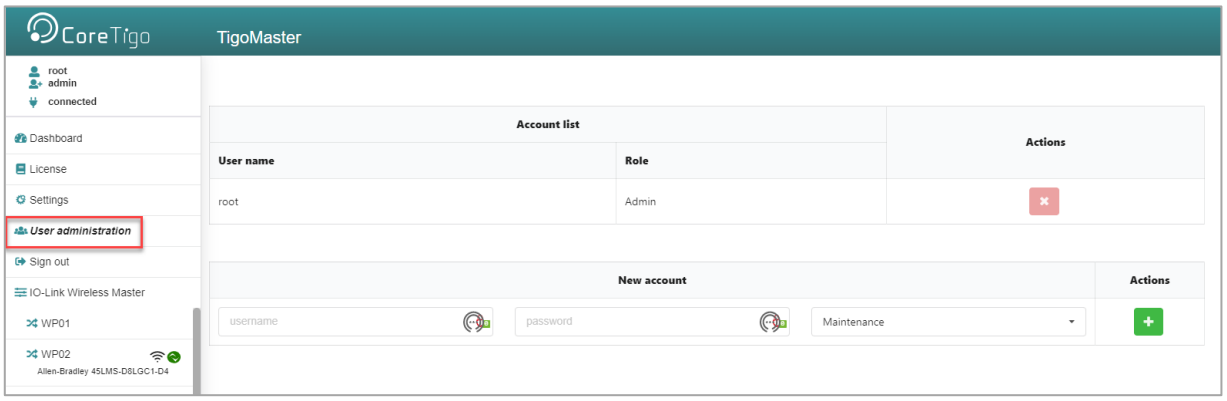


Figure 78: User Administration Screen

   Users can be divided into three roles:

   - Maintenance
   - Operator
   - Administrator

5.8.8.6. 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**.

5.8.8.7. Remove User

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

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

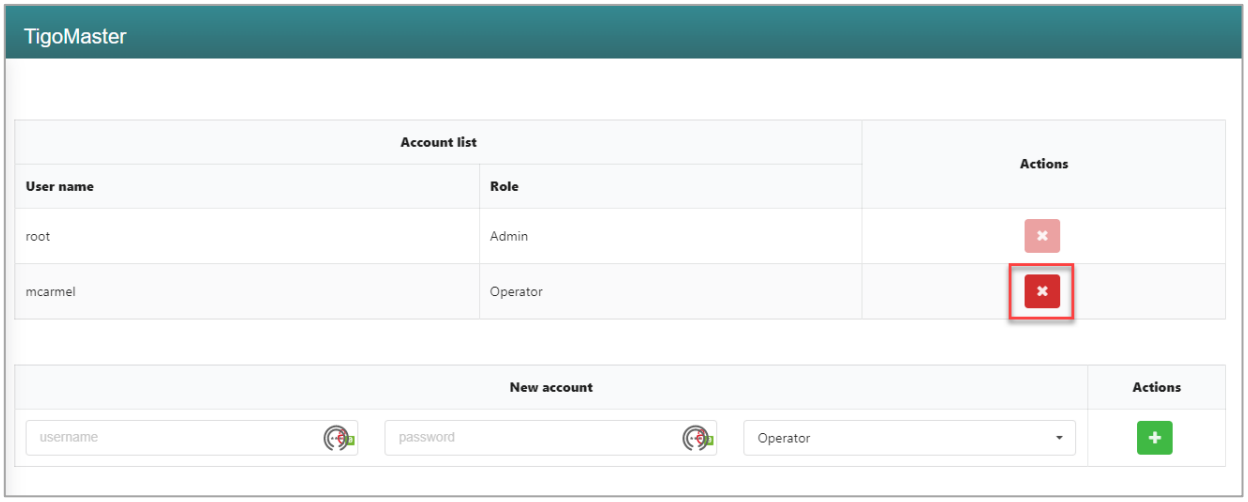


Figure 79: Remove a User

The user will be deleted.

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

6. Commissioning

6.1. Setting the 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. Therefore you need to set its IP address in order for it to use IP-based communication (for example, to connect to TigoEngine or to use the integrated OPC-UA Server). YSet its IP address in the EtherCAT Master, which then sends the address to TigoMaster 2TH.

EtherCAT communication with TigoMaster 2TH does not require an IP address.

To set the IP address for TigoMaster 2TH:

Note:
This procedure uses the TwinCAT programming environment as an example.

1. In the configuration software of the EtherCAT Master (TwinCAT), connect a new EtherCAT Master as follows:
   - In the **Solution Explorer**, expand the **I/O** branch.
   - Right-click **Devices** and then select **Scan**.

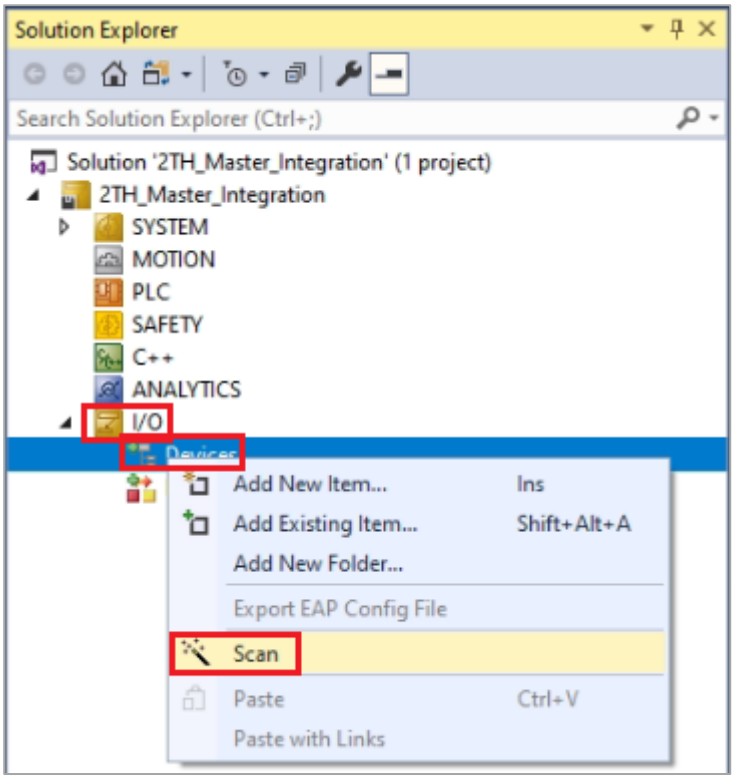


Figure 80: EtherCAT Master Scan

2. In the scan dialog box, click **OK**.

   The scan now finds the PC Ethernet adaptor (that is, the EtherCAT Master), and then prompts to scan for boxes (that is, EtherCAT slaves).

3. In the **Scan for boxes** dialog box, click **Yes**.

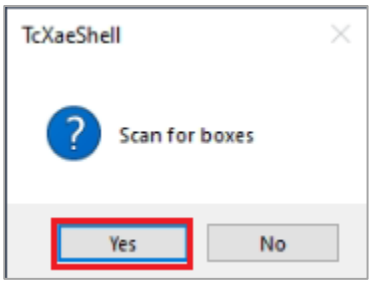


Figure 81: Scan for Boxes

4. In the **Activate Free Run** dialog box, click **Yes**.

   In the **Solution Explorer**, the following appear:

   - The EtherCAT Master is listed under **Devices,** as **Device 2 (EtherCAT)**
   - The TigoMaster 2TH is listed under **Device 2**, as **Box 1 (xxx-xxxx-xx-IOLM\W)**

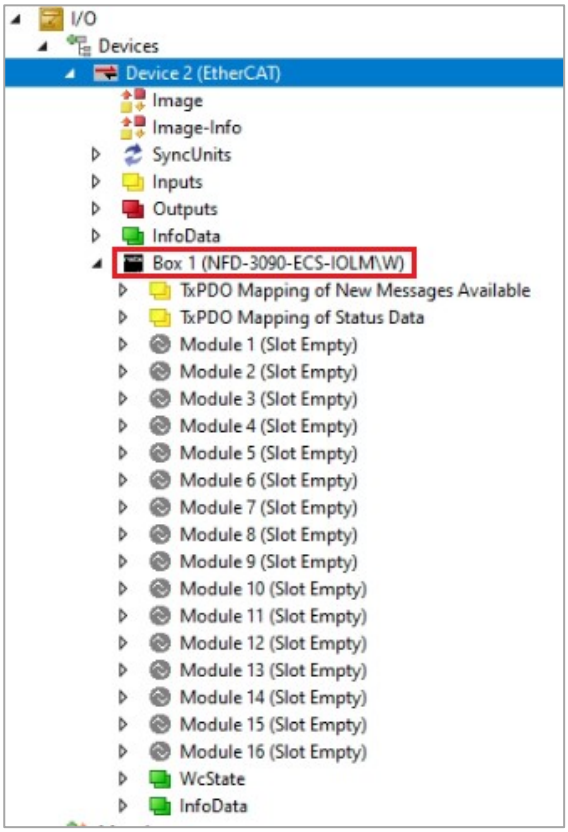


Figure 82: CoreTigo 2TH in the Solution Explorer

Proceed as follows:

1. In the **Solution Explorer**, double click the entry for CoreTigo 2TH (that is, **Box 1**).
2. Open the **EtherCAT properties** window for the TigoMaster 2TH.
3. Click **Advanced Settings**.

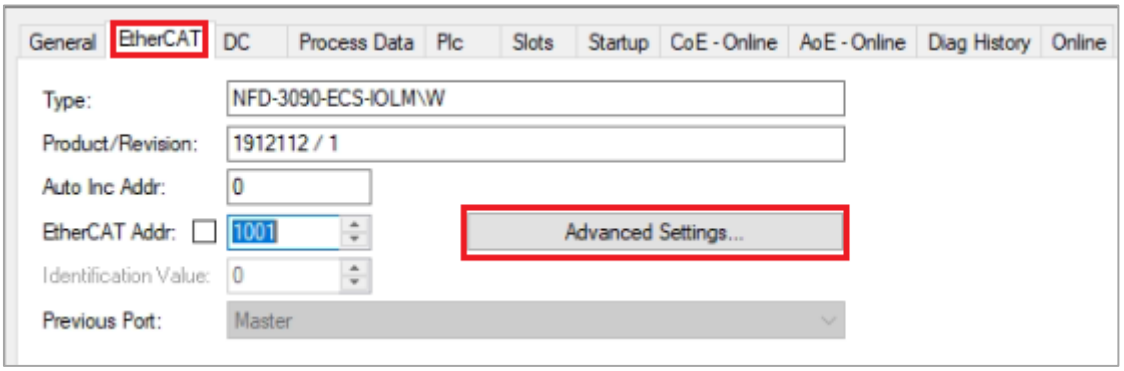


Figure 83: EtherCAT Properties Window

4. In the **Advanced Settings** window, select **Mailbox** > **EoE** (Ethernet over EtherCAT).

   The fields for setting the IP address appear.

5. Enter the **IP Address**, **Subnet Mask,** and **Default Gateway** (typically the default gateway is the IP address of the EtherCAT Master).

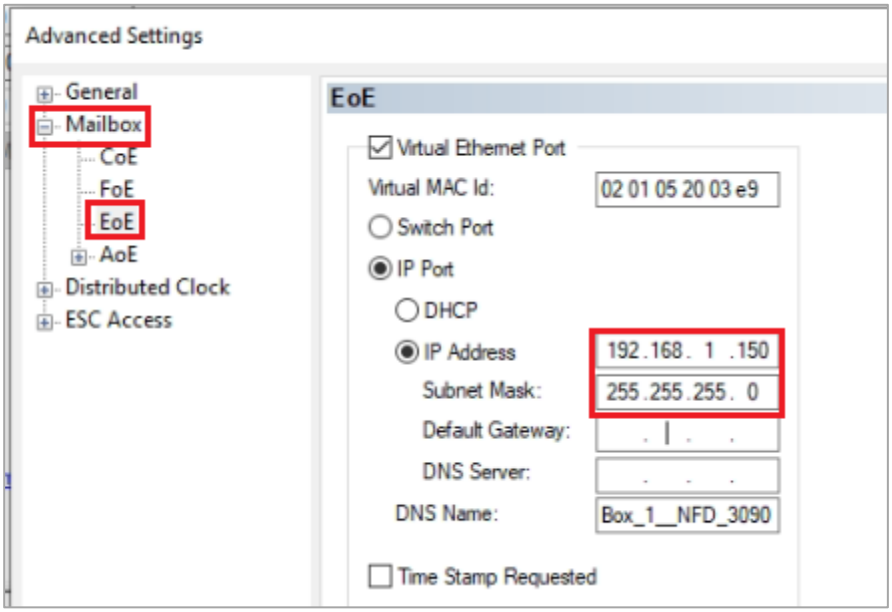


Figure 84: Setting the IP Address

6. Click **Reload Devices** ( ) to load the configuration to the EtherCAT Master.

6.2. Configuration with CoreTigo Web Server

6.2.1. Requirements

To allow the commissioning or configuration using the CoreTigo Wireless 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 Wireless Web Server.
- A login as admin.

6.2.2. Configuring the IO-Link Wireless Master

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

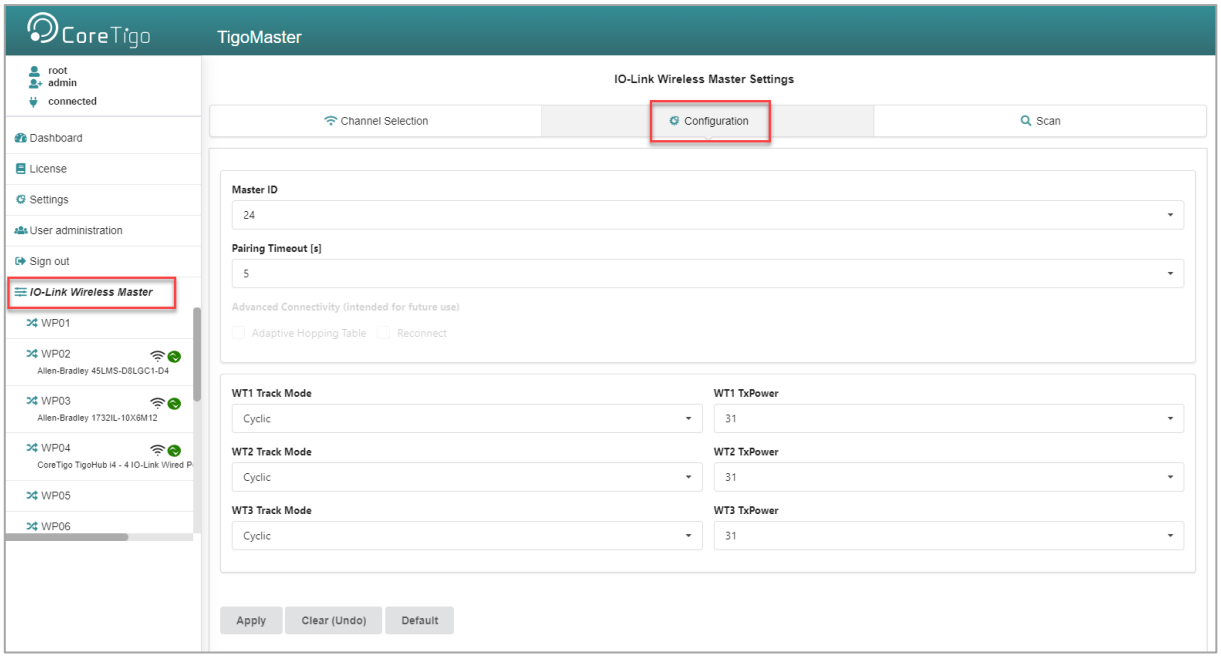


Figure 85: Master > Configuration Tab

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 50: 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.

Scan

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

Figure 86: 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 51: 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**)	

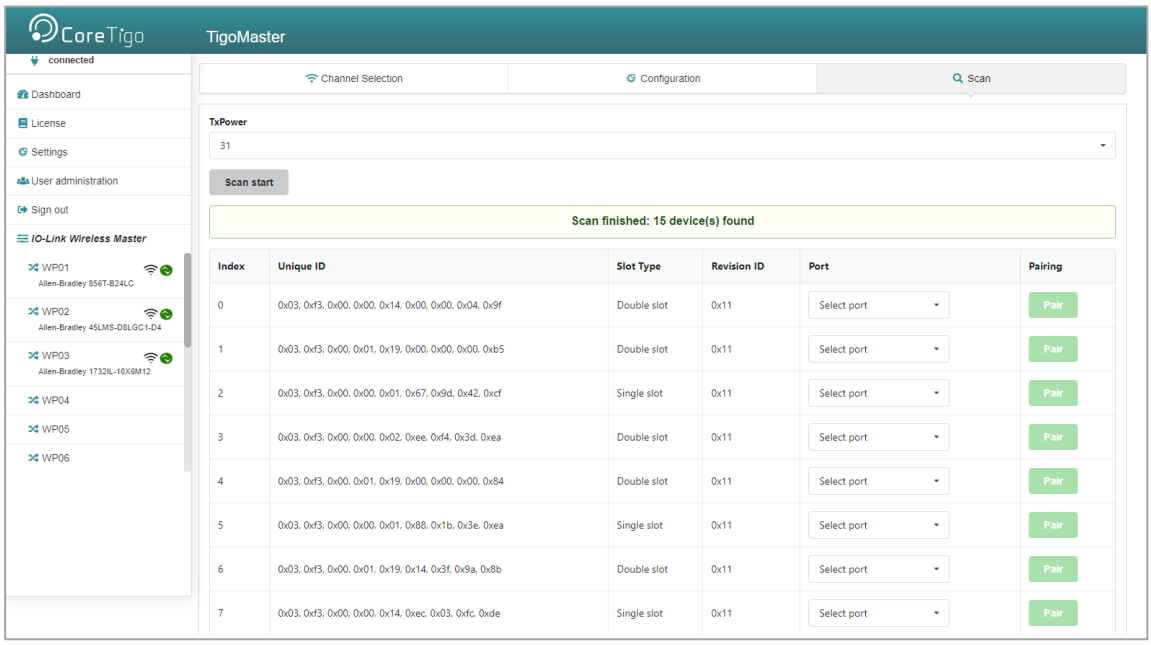


Figure 87: Scan Tab with Result

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 user name 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). The instruction in this section are based on UaExpert.

6.3.1. Requirements

- OPC UA client application installed on your local PC
- A user name 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**.

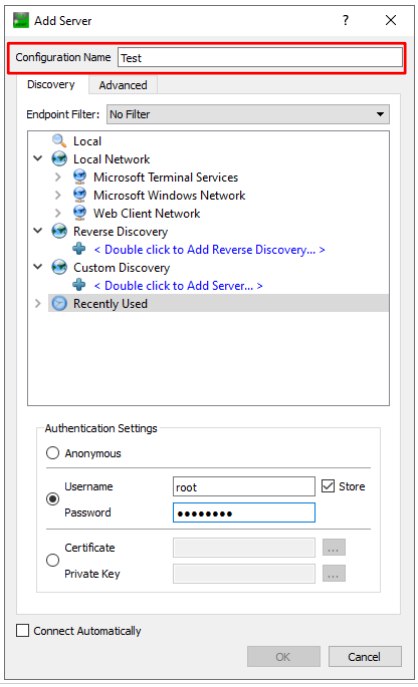


Figure 88: Add Server Dialog Box (Discovery Tab)

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

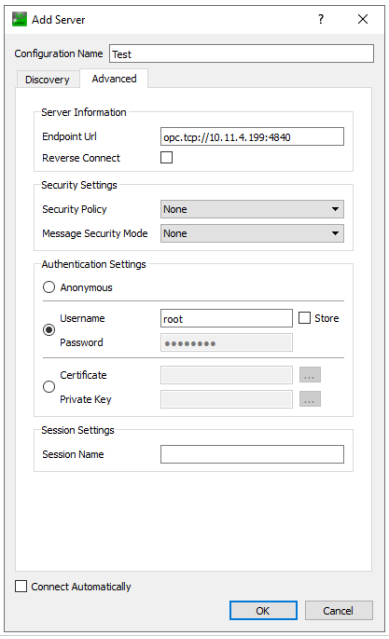


Figure 89: Add Server Dialog Box > Advanced Tab

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

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

   Connection starts.

6.3.3. Set the Device Date and Time Using OPC UA

6.3.3.1. Requirements

- OPC UA client.
- A user name and password that have write permission
- NTP Server IP address: see section 6.3.3.2
- 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, and 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.

6.3.3.4. Instructions

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

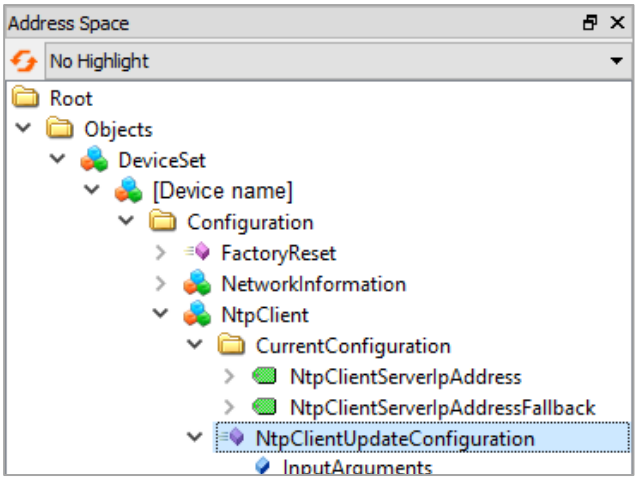


Figure 90: Path to NtpClientUpdateConfiguration

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

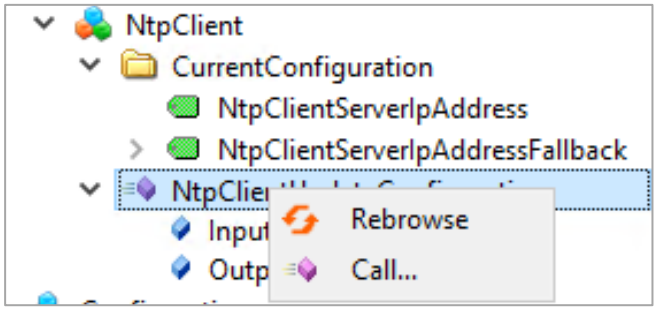


Figure 91: Right-Clicking NtpClientUpdateConfiguration

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

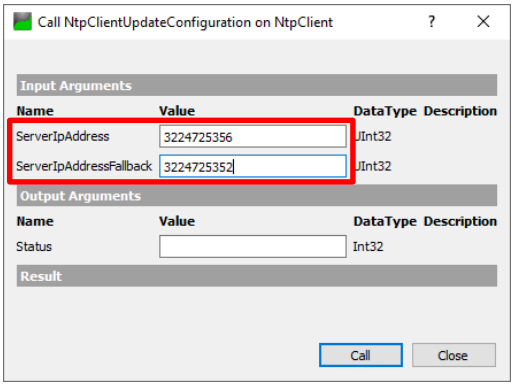


Figure 92: Call NtpClientUpdateConfiguration Dialog Box—Before Call

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

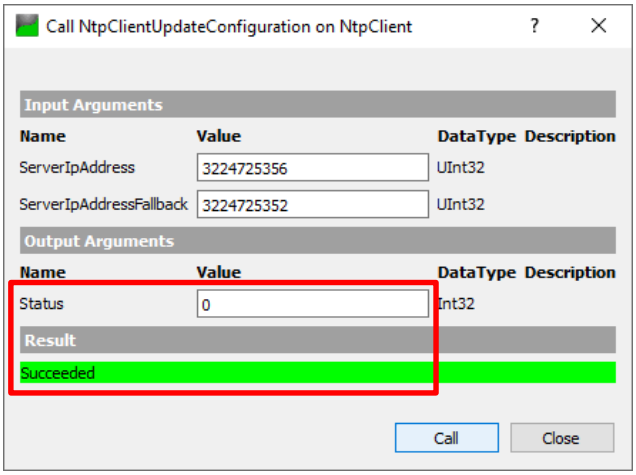


Figure 93: Call NtpClientUpdateConfiguration Dialog Box—After Call

7. Communication

7.1. Process Image

This chapter describes the process data. EtherCAT uses process data objects (PDO) to transfer process data. Process data from the EtherCAT Master to the TigoMaster 2TH are transferred with the objects 0x160x and are called receive PDOs (RxPDO). Process data from the TigoMaster 2TH to the EtherCAT Master are transferred with the objects 0x1A0x, 0x1A11, and 0x1A80, and are called transmit PDOs (TxPDO).

TigoMaster 2TH uses the following TxPDOs for the transmission of the input process data:

- One object 0x1A0x per wireless port with the IO-Link input data.
- Object 0x1A11 with the status **New message available**
- Object 0x1A80 with the status of the wireless IO-Link ports

TigoMaster 2TH uses the following RxPDOs for the transmission of the output process data:

- One object 0x160x per wireless port with the IO-Link output data.

7.1.1. Input Process Data

Object 0x1A0x: The contents of the objects 0x1A00 to 0x1A0F depend on the parameterized operating mode of the corresponding wireless port. For the IO-Link port operating modes, the object 0x1A0x contains process data. The assignment is:

- Object 0x1A00 is assigned to WP01,
- Object 0x1A01 is assigned to WP02, … and
- Object 0x1A0F is assigned to WP16.

The table below describes the assignment of the input process data to the wireless port.

Table 52: Objects 0x1A0x: Assignment of the IO-Link Input Data

Index.Subindex	Size	Name	Description
0x6000.01	1 Byte	Input byte 0	Object 0x1A00 with input data of the wireless port WP01. IO-Link input data of the IO-Link Device at WP01. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Input bytes corresponds to the length of the module used in the IO-Link WP01 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x6000.02	1 Byte	Input byte 1	
…	…	…	
0x6000.20	1 Byte	Input byte 31	
0x6010.01	1 Byte	Input byte 0	Object 0x1A01 with input data of the wireless port WP02. IO-Link input data of the IO-Link Device at WP02. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Input bytes corresponds to the length of the moduleused in the IO-Link WP02 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x6010.02	1 Byte	Input byte 1	
…	…	…	
0x6010.20	1 Byte	Input byte 31	

Index.Subindex	Size	Name	Description
0x60F0.01	1 Byte	Input byte 0	Object 0x1A0F with input data of the wireless port WP16. IO-Link input data of the IO-Link Device at WP16. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Input bytes corresponds to the length of the module used in the IO-Link WP16 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x60F0.02	1 Byte	Input byte 1	
…	…	…	
0x60F0.20	1 Byte	Input byte 31	

Object 0x1A11: Object 0x1A11 transmits the status **new message present**.

Table 53: Objects 0x1A11: New Message Present Assignment

Index.Subindex	Size	Name	Description
0x10F3.04	1 Bit	New Message Available Flag	New message available Overwrite mode: • 0: Latest message has been read • 1: Latest message has not been read Acknowledgement mode: • 0: No unconfirmed message • 1: Diagnostic messages are present that can be confirmed.
-	7 Bit	-	-

Object 0x1A80: Object 0x1A80 transmits the status of the wireless IO-Link port.

Table 54: Object 0x1A80: Assignment of the Wireless IO-Link Port Status

Index.Subindex	Size	Name	Description
0xF100.01	1 Byte	State of WP01	0: PAIRING_SUCCESS (W-Device has been paired) 1: PAIRING_TIMEOUT (W-Device hasn‘t been paired within the given timeout)
0xF100.02	1 Byte	State of WP02	
…	…	…	

Index.Subindex	Size	Name	Description
0xF100.10	1 Byte	State of WP16	2: PAIRING_WRONG_SLOTTYPE (W-Device has different SlotType than that requested) 3: INACTIVE (Communication disabled) 4: PORTREADY (W-Port configuration successful) 5: COMREADY (Communication established and inspection successful) 6: OPERATE (W-Port is ready to exchange Process Data) 7: COMLOST (Communication failed, new synchronization procedure required) 8: REVISION_FAULT (Incompatible protocol revision) 9: COMP_FAULT (Incompatible W-Device or Legacy-Device according to the Inspection Level) 10: SERNUM_FAULT (Mismatching SerialNumber according to the InspectionLevel)

7.1.2. Output Process Data

Objects 0x160x: The contents of the objects 0x1600 to 0x160F depend on the parameterized operating mode of the corresponding wireless port. For the IO-Link and Digital Output port operating modes, the object 0x160x contains process data.

The assignment is:

- Object 0x1600 is assigned to WP01,
- Object 0x1601 is assigned to WP02, … and
- Object 0x160F is assigned to WP16.

The table below describes the assignment of the output process data to the wireless port.

Table 55: Object 0x160x: Assignment of the IO-Link Output Data

Index Subindex	Size	Name	Description
0x7000.01	1 Byte	Output byte 0	Object 0x1600 with output data of the WP01 wireless port. IO-Link output data of the IO-Link Device at WP01. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Output bytes corresponds to the length of the module used in the IO-Link WP01 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x7000.02	1 Byte	Output byte 1	
…	…	…	
0x7000.20	1 Byte	Output byte 31	

Index Subindex	Size	Name	Description
0x7010.01	1 Byte	Output byte 0	Object 0x1601 with output data of the WP02 wireless port. IO-Link output data of the IO-Link Device at WP02. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Output bytes corresponds to the length of the module used in the IO-Link WP02 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x7010.02	1 Byte	Output byte 1	
…	…	…	
0x7010.20	1 Byte	Output byte 31	
…	…	…	…
0x70F0.01	1 Byte	Output byte 0	Object 0x160F with output data of the WP16 wireless port. IO-Link output data of the IO-Link Device at WP16. For a description of the data, see the manual of the manufacturer of the IO-Link Device used. The number of Output bytes corresponds to the length of the moduleused in the IO-Link WP16 slot and can be 1, 2, 4, 8, 16 or 32 bytes.
0x70F0.02	1 Byte	Output byte 1	
…	…	…	
0x70F0.20	1 Byte	Output byte 31	

7.2. OPC UA Server

An OPC UA client can connect to the server in TigoEngine 2TH (as detailed in section 6.3) and access the following parameters:

- Device Identification
- Sensor/Actuator Identification

Note:
For IP address, use the IP address of the TigoMaster 2TH.

7.2.1. Device Identification

The TigoMaster 2TH provides nodes for device identification. For example, the OPC UA client can read the version of the device firmware used in the software revision node (**Root > Object > DeviceSet > [Device Name]**).

Table details the nodes and **Error! Reference source not found.** shows them in the information model of t he device.

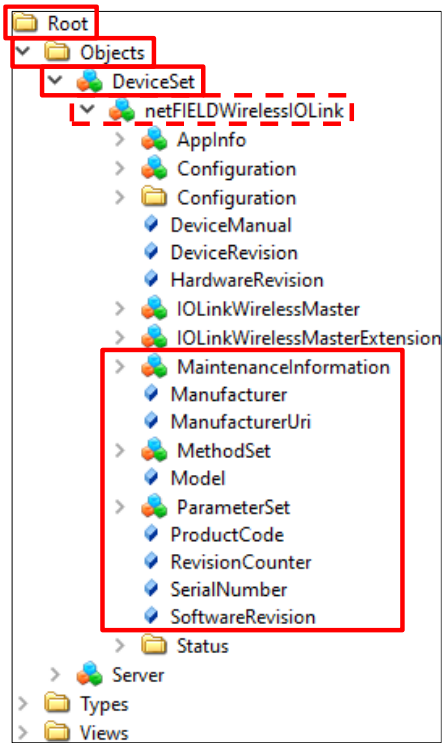


Figure 94: Device Information Model (Section)

Table 56: 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

7.2.2. Sensor/Actuator Identification

The device provides nodes for the identification of connected sensors/actuators. For example, the OPC UA client can read the version of the device firmware used in the software revision node (**Root > Object > DeviceSet > [Device Name] > IOLinkWirelessMaster > PortXX > Device**).

Table 57: Sensor/Actuator Identification Nodes

Node Name	Node Class	Access	Description
Manufacturer	Variable	Read	Device manufacturer
MinCycleTime	Variable	Read	Minimal 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

7.2.3. NTP Client Configuration

The OPC UA server provides nodes for configuring the NTP client. Each node is detailed in Table , and the path to the nodes is: **Root > Object > DeviceSet > [Device Name] > Configuration > NtpClient > Configuration > CurrentConfiguration**.

Table 58: NTP Client Configuration Nodes

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, as detailed in section 6.3.3.3. 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, as detailed in section 6.3.3.3. The value 0 disables the function.
NtpClientUpdateConfiguration	Method	Write	-	Method for writing the nodes NtpClientServerIpAddress and NtpClientServerIpAddressFallback.

7.3. MQTT Topics

7.3.1. General Parts of a topic

The description of a topic contains parts that will be substituted.

Table 59: Topic Parts

Topic Part	Description
{prefix}	Prefix of each topic. The prefix is a text used to identify a device. Configurable in the CoreTigo Web Server.
[MASTER_NUMBER]	Number for each master in the gateway. Typically, the gateway has one master and MASTER_NUMBER is 1.
[PORT_NUMBER]	Number for each port of a master. Forexample, if the master has 8 ports, PORT_NUMBER is 1 … 8.
[DEVICE_ALIAS]	String to identify a device connected to a port of a master: masterXportY. Example: master1port3.

7.3.2. Gateway Topics

Table 60: Gateway Topics

Topic	Description
{prefix}/iolink/v1/gateway/identification	Identification of the gateway: MAC address, serial number, product ID, vendorname, product name, hardware revision, firmware revision, product instance URI. For an example, see section 7.3.2.1.
{prefix}/iolink/v1/gateway/capabilities	Capabilities of the gateway: IODD supported, MQTT supported, For an example, see section 7.3.2.2.
{prefix}/iolink/v1/gateway/configuration	Network configuration of the gateway: IP configuration, IP address, subnetmask, standard gateway. For an example, see section 7.3.2.3.

You can find examples and details of the transferred JSON objects below.

7.3.2.1. Gateway Identification

Example of the gateway identification JSON object:

```
{
  "macAddress": "01:02:03:04:05:06",
  "serialNumber": "12345678",
  "productID": "TMP34Z",
  "vendorName": "SensorCompany",
  "productName": "FlowSensor34",
  "hardwareRevision": "V2.34",
  "firmwareRevision": "V1.23",
  "productInstanceUri": "sensor.tmp.23.com"
}
```

Figure 95: Gateway Identification JSON Object

7.3.2.2. Gateway Capabilities

Table 61: Gateway Capabilities JSON Key

JSON key	Description
ioddSupported	ioddSupported: true: IODD is available ioddSupported: false: IODD is not available
mqttSupported	mqttSupported: true: MQTT is available mqttSupported: false: MQTT is not available

Example of the gateway capabilities JSON object:

```
{
  "ioddSupported": true,
  "mqttSupported": false
}
```

Figure 96: Gateway Capabilities JSON Object

7.3.2.3. Gateway Configuration

Table 62: Gateway Configuration JSON Key

JSON key	Description
ipConfiguration	Possible values for ipConfiguration: • MANUAL: Assignment of the IP address by other device specific means. • DHCP: RFC 2131 defines the Dynamic Host ConfigurationProtocol, allowing automatic assignment of IP addresses. • DCP: defines the Discovery and Configuration Protocol, a link-layer protocol that allows the manual assignment of IP addresses.

Example of the gateway configuration JSON object:

```
{
  "ethIpv4":
    [
      {
        "ipConfiguration": "MANUAL",
        "ipAddress": "192.168.1.13",
        "subnetMask: "255.255.255.0",
        "standardGateway": "192.168.1.1"
      }
    ]
```

Figure 97: Gateway Configuration JSON Object

7.3.3. Master Topics

Table 63: Master Topics

Topic	Description
{prefix}/iolink/v1/masters	Available master number keys and identification information: Master number, serial number, location tag For an example, see section 7.3.3.1
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/capabilities	Capabilities of the master: Number of ports, max. power supply (of the device) Example: {prefix}/iolink/v1/masters/1/capabilities For an example, see section 7.3.3.2

Topic	Description
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/identification	Identification of the master: Vendor name, vendor ID, master ID, master type, serial number, product ID, productname, hardware revision, firmware revision, vendor URL, manual URL, application specific tag, location tag, function tag Example: {prefix}/iolink/v1/masters/1/identification For an example, see section 7.3.3.3
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/ports	Available port number keys: Port number, status info,device alias Example: {prefix}/iolink/v1/masters/1/ports For an example, see section 7.3.3.4
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/ports/[PORT_NUMBER]/capabilities	Read capability information of the port: Max power supply(of the port), port type Example: {prefix}/iolink/v1/masters/1/ports/4/capabilities For an example, see section 7.3.3.5
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/ports/[PORT_NUMBER]/status	Read current status of the port: Status Info, IO-Linkrevision, master cycle time Example: {prefix}/iolink/v1/masters/1/ports/4/status For an example, see section 7.3.3.6
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/ports/[PORT_NUMBER]/configuration	Read configuration of the port: Mode, validation and backup, cycle time, vendor ID, device ID, slot number, track number, device TX power, max retry, IMA time (I-am-alive time), slot type, device low power, max PD segment length, unique ID, device alias Example: {prefix}/iolink/v1/masters/1/ports/4/configuration For an example, see section 7.3.3.7
{prefix}/iolink/v1/masters/[MASTER_NUMBER]/ports/[PORT_NUMBER]/datastorage	Read data storage content of the port: Vendor ID, deviceID, IO-Link revision Example: {prefix}/iolink/v1/masters/1/ports/4/datastorage For an example, see section 7.3.3.8

You can find examples and details about the transferred JSON objects below.

7.3.3.1. Master List

Example of the master list JSON object:


```
[
    {
        "masterNumber": 1,
        "serialNumber":
        "A0A1A2A3A4",
        "locationTag": "slot 2"
    },
    {
        "masterNumber": 2,
        "serialNumber":
        "B0B1B2B3B4",
        "locationTag": "slot 3"
```


Figure 98: Master List JSON Object

7.3.3.2. Master Capabilities

Example of the master capabilities JSON object:


```
{
    "numberOfPorts": 8,
    "maxPowerSupply": {
        "value": 0.3,
        "unit": "A"
    }
}
```


Figure 99: Master Capabilities JSON Object

7.3.3.3. Master Identification

Example of the master identification JSON object:


```
{

  "vendorName": "Vendor GmbH",
  "vendorId": 26,

  "masterId": 42,

  "masterType": "Master acc. V1.0",
  "serialNumber": "IOLM123456",
  "productId": "PROD-123456",
  "productName": "IO-Link Master",
  "hardwareRevision": "3.2.1.444R",
  "firmwareRevision": "3.2.1.888R",

  "vendorUrl": "http://www.io-link.com/io-link-master",
  "manualUrl": "http://www.io-link.com/io-link-master/manual.pdf",
  "applicationSpecificTag": "Fallback reader",

  "locationTag": "Down under",
  "functionTag": "Code reading"

}
```


Figure 100: Master Identification JSON Object

7.3.3.4. Port List

Table 64: Port List JSON Key

JSON key	Description
statusInfo	Activated: statusInfo: DEVICE_ONLINE Deactivated: statusInfo: DEACTIVATED
deviceAlias	Possible values for "deviceAlias": • Distance_sensor • Pressure_sensor • Switching_sensor • Empty_port

Example of the port list JSON object:


```
[
    {
        "portNumber": 1,
        "statusInfo": "DEVICE_ONLINE",
        "deviceAlias": "Distance_sensor"
    },
    {
        "portNumber": 2,
        "statusInfo": "DEVICE_ONLINE",
        "deviceAlias": "Pressure_sensor"
    },
    {
        "portNumber": 3,
        "statusInfo": "DEVICE_ONLINE",
        "deviceAlias": "Switching_sensor"
    },
    {
        "portNumber": 4,
        "statusInfo": "DEACTIVATED",
        "deviceAlias": "Empty_port"
    }
]
```


Figure 101: Port List JSON Object

7.3.3.5. Port Capabilities

Table 65: Port Capabilities JSON Key

JSON key	Description
portType	Value for portType for IO-Link Wireless Master: WIRELESS_MASTER

Example of the port capabilities JSON object:


```
{

    "maxPowerSupply": {
        "value" : 0.3,

        "unit" : "A"

    },

    "portType" : "CLASS_A"

}
```


Figure 102: Port Capabilities JSON Object

7.3.3.6. Port Status

Table 66: Port Status JSON Key

JSON key	Description
statusInfo	Activated: statusInfo: DEVICE_ONLINE Deactivated: statusInfo: Deactivated

Example of the IO-Link wireless port status JSON object:


```
{

    "statusInfo": "DEVICE_ONLINE",
    "iolinkRevision" : "1.1",
    "masterCycleTime" : {

        "value" : "5.0",

        "unit" : "ms"

    }

}
```


Figure 103: Port Status JSON Object

7.3.3.7. Port Configuration

Table 67: Port Configuration, Configuration Values

JSON key	Values
mode	DEACTIVATED IOLINK_CYCLIC IOLINK_ROAMING
validationAndBackup	NO_DEVICE_CHECK TYPE_COMPATIBLE TYPE_COMPATIBLE_RESTORE_ONLY TYPE_COMPATIBLE_BACKUP_AND_RESTORE
slotNumber	0–7
trackNumber	0–2
deviceTxPower	1–31
maxRetry	2–31
imaTime	SINGLE_SLOT DOUBLE_SLOT
maxPdSegmentLength	1–32

An example of the IO-Link wireless configuration JSON object is below.

```
{
    "mode": "IOLINK_MANUAL",
    "validationAndBackup" :
    "TYPE_COMPATIBLE",
    "cycleTime" : {
        "value" : "5.0",
        "unit" : "ms"
    },
    "vendorId" : 26,
    "deviceId" : 333,
    "slotNumber" : 0,
    "trackNumber" : 1,
    "deviceTxPower" : 31,
    "maxRetry" : 2,
    "imaTime" : 771,
```

Figure 104: IO-Link Wireless Configuration JSON Object

Example of the cycle time object JSON object:

```
{
    "value" : "5.0",
    "unit" : "ms"
}
```

Figure 105: Cycle Time Object JSON Object

7.3.3.8. Port Data Storage

Example of the port data storage JSON object:

```
    "header": {
        "vendorId" : 15,
        "deviceId" : 65253,
        "iolinkRevision" : "1.1"
    },
    "content": "YmFzZTY0IGVuY3J5cHRlZCBjb250ZW50"
```

Figure 106: Port Data Storage JSON Object

7.3.4. Device Topics

7.3.4.1. Device List

Example of the device list JSON object:

```
[
    {
        "deviceAlias" : "DT35",
        "masterNumber" : 1,
        "portNumber" : 1,
    },
    {
        "deviceAlias" : "DT36",
        "masterNumber" : 1,
        "portNumber" : 2,
    },
    {
        "deviceAlias" : "DT37",
        "masterNumber" : 1,
        "portNumber" : 3,
    },
    {
        "deviceAlias" : "DT38",
        "masterNumber" : 1,
```

Figure 107: Device List JSON Object

7.3.4.2. Device Capabilities

Example of the device capabilities JSON object:

```
{
    "minimumCycleTime" : {
        "value" : 2.3,
        "unit" : "ms"
    },
    "supportedProfiles" : [10,32770]
}
```

Figure 108: Device Capabilities JSON Object

\

7.3.4.3. Device Identification

Example of the Device identification JSON object:

```
{

    "vendorId" : 26,

    "deviceId" : 42,

    "iolinkRevision" : "1.1",
    "vendorName" : "Vendor GmbH",
    "vendorText" : "IO-Link",

    "productName" : "Sensor Intelligence",
    "productId" : "PROD-123456",
    "productText" : "Light switch",
    "serialNumber" : "IOLM123456",
    "hardwareRevision" : "3.2.1.444R",
    "firmwareRevision" : "3.2.1.888R",

    "applicationSpecificTag" : "Fallback light switch at the end of
the belt",

    "locationTag" : "Down under",
    "functionTag" : "Check end of belt"

}
```

Figure 109: Device Identification JSON Object

7.3.4.4. Device Process Data

Example of the device process data JSON object for an IO-Link device:

```
{
    "getData" : {
        "iolink" : {
            "valid" : true,
            "value" : [12,22,216]
        },
        "iqValue" : false
    },
    "setData" : {
        "iolink" : {
            "valid" : true,
            "value" : [128,221,134]
        },
        "iqValue" : false
    }
}
```

Figure 110: Device Process Data JSON Object

7.3.4.5. Device Process Data Input

Example of the device process data input JSON object for an IO-Link device:

```
{
    "getData" : {
        "iolink" : {
            "valid" : true,
            "value" : [12,22,216]
        },
        "iqValue" : false
    }
}
```

Figure 111: Device Process Data Input JSON Object

7.3.4.6. Device Process Data Output

Example of the device process data output JSON object for an IO-Link device:

```
{
    "getData" : {},
    "setData" : {
        "iolink" : {
            "valid" : true,
            "value" : [128,221,134]
        },
        "iqValue" : false
    }
```

Figure 112: Device Process Data Output JSON Object

7.3.4.7. Device Events

Example of the device events JSON object

```
[
    {
        "time" : "2018-05-18T07:31:54.123z",
        "severity" : "WARNING",
        "origin" : {
            "master" : 1,
            "port" : 1,
            "device" : "Temp sensor 1",
        },
        "message" : {
            "code" : 16912,
            "mode" : "APPEARS",
            "text" : "Device temperature over-run - Clear source of
heat"
        }
    }
]
```

Figure 113: Device Events JSON Object

7.3.5. MQTT Topics

Table 68: MQTT Topics

Topic	Description
{prefix}/iolink/v1/mqtt/configuration	Read configuration of MQTT client: Client mode, server address, user name,user name, password, last will, keep alive time For an example, see MQTT Configuration.
{prefix}/iolink/v1/mqtt/connectionstatus	Configuration of MQTT client: Connection status, server address, up time For an example, see MQTT Connection Status.

Examples and details of the transferred JSON objects are below.

7.3.5.1. MQTT Configuration

Table 69: MQTT Configuration JSON Key

JSON key	Description
clientMode	Activated: "clientMode": "ACTIVE" Deactivated: "clientMode": "INACTIVE"

Example of the MQTT configuration JSON object:

```
{
    "clientMode" : "ACTIVE",
    "serverAddress" : "192.168.2.1./mqttserver",
    "username" : "iolink_json",
    "password" : "123456",
    "lastWill" : {
        "topic" : "my temperature sensor",
        "message" : "Process data transfer stopped",
        "qoS" : "0_ONLY_ONCE",
        "retain" : true
    },
    "keepAliveTime" : 0
}
```

Figure 114: MQTT Configuration JSON Object

7.3.5.2. MQTT Connection Status

Table 70: MQTT Connection Status JSON Key

JSON key	Description
connectionStatus	Possible values for "connectionStatus": CONNECTING CONNECION_ACCEPTED CLIENT_INACTIVE

Example of the MQTT connection status JSON object:

```
{
"connectionStatus" : "CONNECTION_ACCEPTED",
"serverAddress" : "192.168.2.1./mqttserver",
"upTime" : 123
}
```

Figure 115: MQTT Connection Status JSON Object

8. Status and Diagnosis

8.1. TigoMaster 2TH

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

8.2. IO-Link Diagnosis

8.2.1. Event Qualifier

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

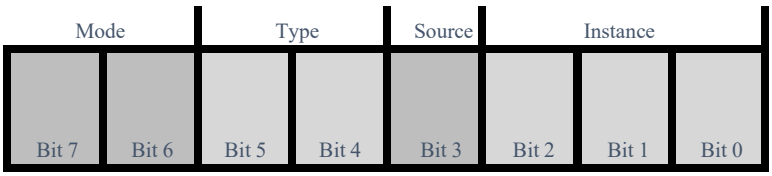


Figure 116: Event Qualifier

Table 71: 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

8.2.2. IO-Link Wireless Master Event Codes

Table 72: 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

8.2.3. 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 73: 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
0x4220	Device temperature underrun	Warning	Insulate IO-Link Device

Event code	Description	Type	Remedy (common)
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
0x8C41	Maintenance required	Warning	Refill
0x8C42	Maintenance required	Warning	Exchange wear and tear parts

Event code	Description	Type	Remedy (common)
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

9. Technical Data

9.1. Product Specifications

Table 74: Product Specifications

Category	Parameter	Value		
Product	Part number	1912.122		
	Product name	TigoMaster 2TH		
	Description	TigoMaster 2TH EtherCAT device		
	Function	IO-Link Master Wireless for EtherCAT 2 tracks, 16 channels		
Communication controller	Type	netX 90		
Integrated memory	RAM	16 MB SDRAM		
	FLASH	8 MB		
Ethernet communication	Real-Time Ethernet	EtherCAT Adapter		
Ethernet interface	Interface type	100BASE-TX, 10BASE-T, isolated		
	Auto-negotiation, Auto-crossover	Yes		
	Connectors	X31: Ethernet interface, M12, D-coded, EtherCAT port 1 X32: Ethernet interface, M12, D-coded, EtherCAT 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**
	EtherCAT communication	RUN	Run status	**Red**/**Green**
		ERR	Error status	**Red**/**Green**
(LEDS continued)	Ethernet	LINK (X31)	Link status, connector X31	**Green**

Category	Parameter	Value		
		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)		
	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		

Category	Parameter	Value
(Power supply 1L, 2L continued)	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
Ambient conditions	Ambient temperature (operation), Air flow, during measurement	-25 °C to +70 °C V ≤ 0,5 m/s
	Storage temperature range	-40 °C to +85 °C
	Max. temperature change	3 K / min
	Humidity	5–95% relative humidity, no condensation permitted
	Operating height	0–2000 m
	Humidity Operating height	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
	Protection class	IP67
Conformity	Reach & RoHS	Complied
Conformance with EMC directives (preliminary	CE sign	Yes
	UKCA	Yes
Approvals	FCC	FCC ID: 2ATSM-COR2TH
	ISED	IC ID: 26463-COR2TH
Firmware download	Software to download and update the firmware	TigoEngine and CoreTigo Web Server
Configuration	Configuration software	TigoEngine, CoreTigo Web Server, EtherCAT PLC

Table 75: 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
Mechanical specifications	Connector	Regular SMA-Male
	Height	25.6 mm

9.2. IO-Link Wireless Master

Table 76: O-Link Wireless Master Technical Data

Parameter	Value
Tracks and IO-Link Devices	2 wireless tracks for up to 16 IO-Link Devices
Radio frequencies	RFch (RF channel center frequency): 2403–2478 MHz (wireless channels 3 – 78,configurable). The IO-Link Wireless Master uses the frequencies (wireless channels) 2401 (1), 2402 (2), 2479 (79), 2480 (80) for network configurations purposes and cannot be configured forcommunication purposes.
Masters per cell	Max. 3 masters within a circle of 20 m diameter
Antennas	3 SMA antennas

9.3. Protocol

Table 77: Protocol Technical Data

Feature	Description
Maximum number of cyclic input data	1024 bytes
Maximum number of cyclic output data	1024 bytes
Acyclic communication (CoE)	SDO SDO Master-Slave SDO Slave-Slave (depending on master capability)
Type	Complex Slave
Supported protocols	SDO client and server side protocol CoE Emergency messages (CoE) Ethernet over EtherCAT (EoE) File Access over EtherCAT (FoE)
Supported state machine	ESM (EtherCAT State Machine)
Supported of synchronization modes	Freerun: the application of the slave is not synchronized to EtherCAT Synchronous with SYNCMAN Event: the application of the slave issynchronized to the SM2/3 Event Synchronous with SYNC Event: the application of the slave is synchronized to the SYNC0 or SYNC1 Event
Supported features	PDI watchdog EtherCAT mailbox handling EtherCAT state machine handling Master-to-slave SDO communication Slave-to-slave SDO communication Integrated CoE object dictionary (ODV3) Ethernet over EtherCAT (EoE) handling File Access over EtherCAT (FoE) server
Number of FMMU channels	8
Number of Sync Manager channels	4
Distributed Clocks (DC)	Supported with 32-bit timestamps and isochronous PDI functionality(Sync0, Sync1)
Ethernet interface	Two Ethernet Interfaces 100BASE-TX Integrated Dual-PHY (supports Auto-Negotiation and Auto-Crossover)
Data transport layer	Ethernet II, IEEE 802.3

Feature	Description
Restrictions	EtherCAT Slave stack AoE application interface not available FoE for firmware upload is supported, but application interface is not available ESC - EtherCAT Slave Controller No DC Latch functionality No support of bit-wise FMMU mapping (Exception: Fill Status of Transmit Mailbox) Restricted DC Sync signal generation No Single-Shot Mode support No Acknowledge Mode support Restricted DC Control Functionality No adjustment of Register Speed Counter Start (0x0930:0x931) No showing of Register Speed Counter Diff (0x0932:0x933) No MIO (PHY Management Interface) access from EtherCAT Master side No physical Read-Write commands supported (APRW, FPRW, BRW)
Reference to stack version	V5.1

9.4. OPC UA Server

Table 78: 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 „Monitored Items“ per session	20
Data coding	UA binary

9.5. MQTT Client

Table 79: MQTT Client Technical Data

Parameter	Description
MQTT	Client
Client services	Publish
Protocols	MQTT over TCP
Topic size	Max. 256 bytes individually per MQTT publication and up to 256 bytes of common topic prefix of the associated MQTT connection
Topics	Topic: Printable UTF-8 string, NUL-terminated, multi-byte encoding (MBCS) Payload: JSON
Will Topic	Max. 256 bytes
Quality of Service	QoS 0, QoS 1, and QoS 2
IP standard	IPv4
Port	1883 (default), MQTT unencrypted
MQTT standard	V3.1.1
Restriction	The Subscribe service is not supported.

9.6. Dimensions

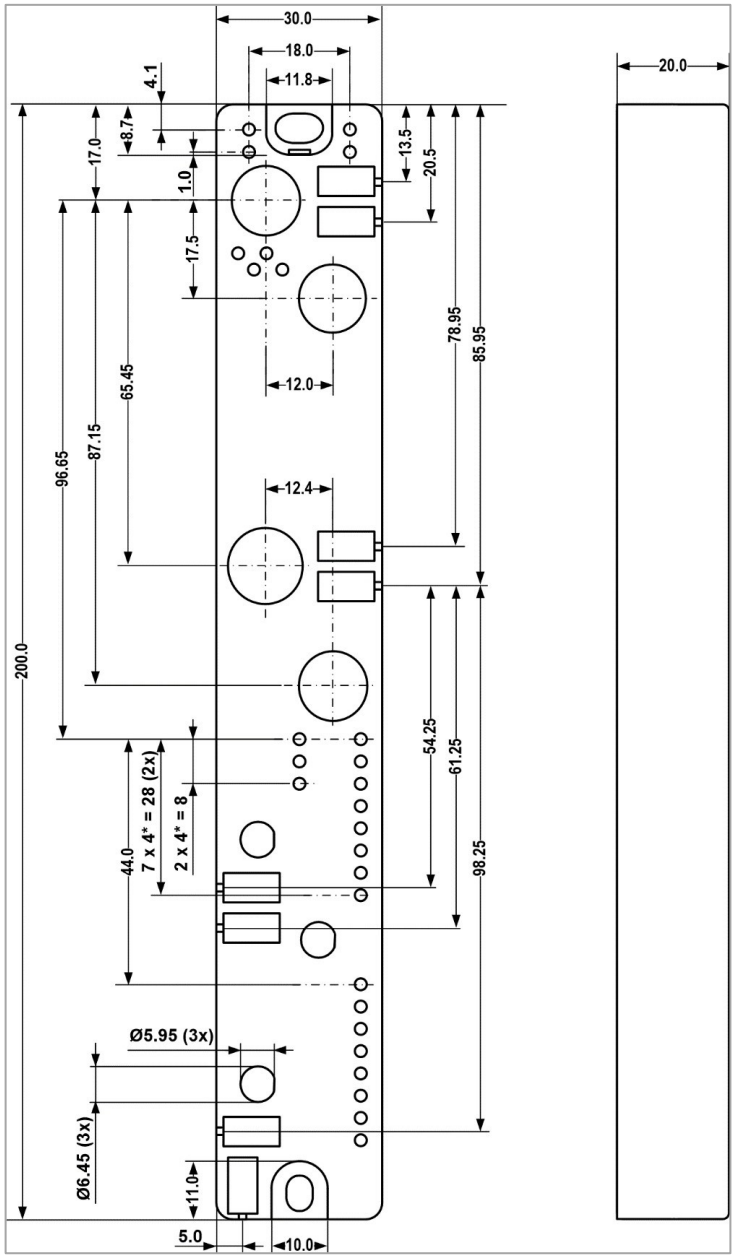


Figure 117: Dimensions

10. Approvals

CAUTION: Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The FCC Wants You to Know

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.

FCC Warning

CoreTigo LTD has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment.

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.

Interference Statement

This device complies with Part 15 of the FCC Rules and Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (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.

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.

11. Appendix A – Part Number

Part number: CT241-0008t2-01 (EtherCAT Version)

Generation: 2

Product Identifier: 4

Product Type: 1

Protocol: 0008

Character Identifier of Features: t2

Version: 01

Table 80: EtherCAT Version

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

12. 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.