TigoGateway 1TE

PROFINET

USER MANUAL

Revision 1.2

Jan 2024

Table of Contents

List of Figures

List of Tables

Revision Control

Author Name	Description	Rev.	Date
CoreTigo	Original Document	1.0	May 2023
CoreTigo	Second version specific to TigoGateway 1TE model	1.1	Oct 2023
CoreTigo	Updates – Regulations, images	1.2	Jan 2024

Acronyms and Abbreviations

Term	Meaning
ACT	System Activity
AL	Application Layer
API	Application Programming Interface
CM	Configuration Manager
DCP	Discovery and Basic Configuration Protocol
DS	Data Storage
DSlot	Double Slot
DU	Diagnosis Unit
FAT	File Allocation Table
FE	Functional Earth
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
Q	Queue
RSSI	Received Signal Strength Indication
SM	System Management
SMI	Standardized Master Interface
SSlot	Single Slot
SW	Software
TBD	To be determined
VS	Vendor Specific
W-Device	Wireless Device (for example, TigoBridge)
W-Master	Wireless Master (for example, TigoGateway)

1. Introduction

1.1. About

This User Manual describes the TigoGateway 1TE device.

TigoGateway 1TE is an industrial-grade IP20 IO-Link Wireless Master with Edge Computing functionality. It supports up to 8 IO-Link Wireless Devices simultaneously and includes interfaces to a variety of Industrial Ethernet and IIoT protocols. The IO-Link Wireless connectivity enables to control sensors and actuators wirelessly, with low latency and high reliability, deterministic and scalable performance.

The TigoGateway 1TE includes Edge computing capabilities, with a Linux OS that is used for a variety of advanced applications, and implementation of business logic (including the TigoEngine software installed on the Gateway). It allows to upload high-resolution OT generated data to the cloud with a secure connection.

The TigoGateway 1TE is Docker enabled.

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. Electrical Connection

The TigoGateway's products family shall be supplied by an isolated power source that meets the following requirements:

- Limited-Energy Circuit in accordance with UL/CSA 61010-1
  or
- Limited Power Source (LPS) in accordance with (UL/CSA 60950-1 or EN 62368-1, Annex Q)
  or
- Class 2 supply source which complies with the National Electrical Code (NEC), NFPA 70, Clause 725.121 and Canadian Electrical Code (CEC), Part I, C22.1.

2.3. Intended Use

- The TigoGateway 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 0°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 IP20.
- The TigoGateway enclosure can never meet IP67 requirements.

Note:
The TigoGateway is intended for indoor use.

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

2.4. 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.

2.5. 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.

2.6. Information and Data Security

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

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

- Install it behind a firewall (recommended).
- Make the TigoGateway 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. Contains FCC ID: 2ATSM-TGRFCM1.

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 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. The distance between user and device should be no less than 20cm.

This radio transmitter [26463-TIGOGW] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

- Antenna Part Number: TLW2.5A-SMA-Male
- Manufacturer: CoreTigo Ltd.
- Peak Gain: 1.6 dBi

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 Peak Gain (1.6 dBi). La distance entre l'utilisation et l'appareil ne doit pas être inférieure à 20 cm.

2.8. Requirements

2.8.1. Hardware

Installation of the product requires the following hardware:

- TigoGateway IO-Link Wireless Master
- 24 V DC SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage) Power Supply
- RJ45 Plug Adapter
- CAT5 - Ethernet Cable with RJ45 Connectors
- PROFINET Supported PLC (not mandatory)

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

- PC or Notebook with a minimum of 1 additional Ethernet Port and Internet Access/PLC

2.8.2. Software

Three software tools enable the installation, setup, maintenance and control of the TigoGateway, in addition to a viable internet browser:

- TigoEngine – IO-Link Wireless configuration tool
- Linux Cockpit – Linux OS web-based management system
- Docker – Containers management tool

3. Getting Started

3.1. Product Description

TigoGateway 1TE is an industrial-grade IP20 IO-Link Wireless Master with Edge Computing functionality.

TigoGateway 1TE supports up to 8 IO-Link Wireless Devices per track, and includes interfaces to a variety of Industrial Ethernet and IIoT protocols. The IO-Link Wireless connectivity enables the control of sensors and actuators wirelessly, with low latency and high reliability, deterministic and scalable performance.

Key functionalities include:

- Interfaces to a variety of Industrial Ethernet protocols and other communication protocols such as OPC UA, HTTP and REST API
- PLC control of sensors and actuators under deterministic constraints
- Edge processor running an Embedded Linux OS that can be used for On-Prem application (including the TigoEngine software which is preinstalled on the TigoGateway)
- Uploading of high resolution OT data to the Cloud with a secure connection via MQTT TLS
- Docker enabled

3.2. Product Overview

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 side label attached to the device's housing.

For further details see Technical Data.

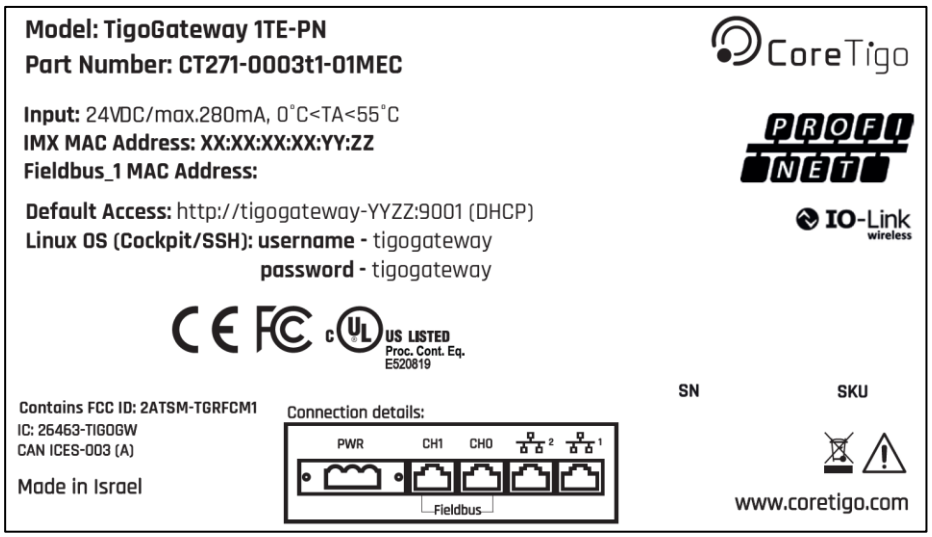


Figure 1: Example of TigoGateway Side Label

3.2.1. Network Topology

The network topology in which the TigoGateway is used is described in the diagram below.

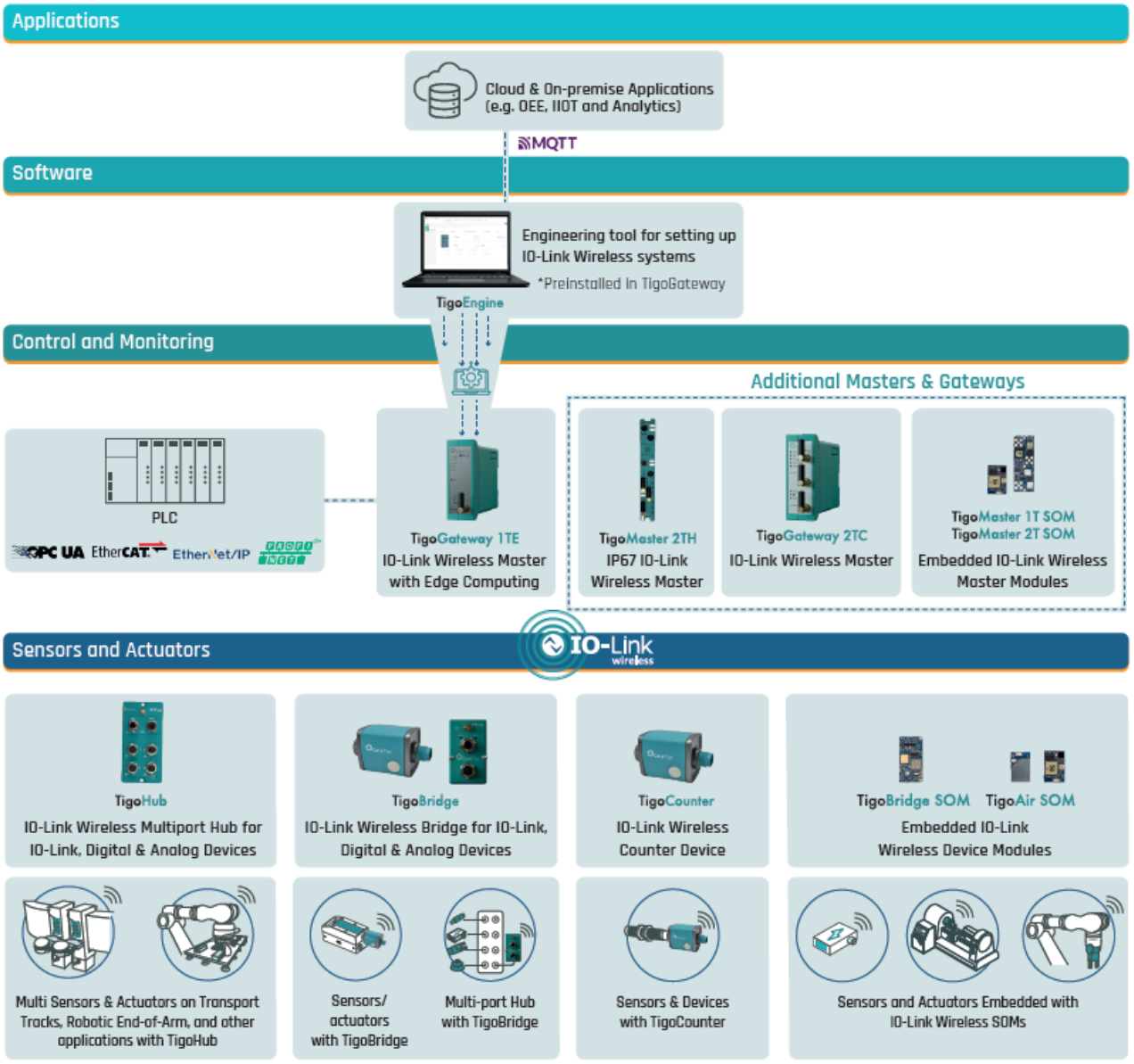
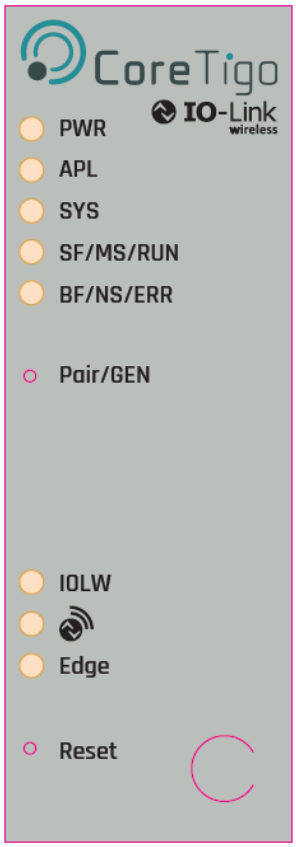
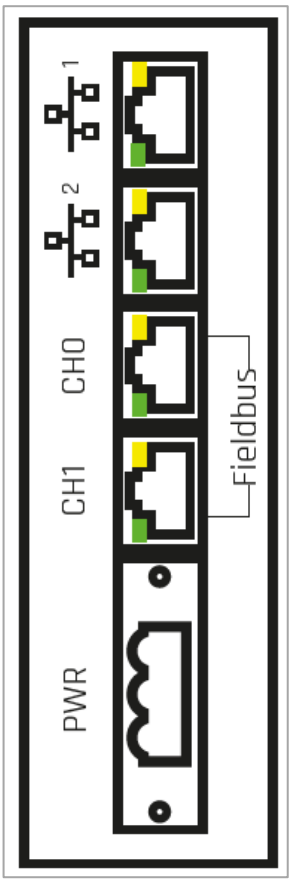


Figure 2: TigoGateway Network Topology

3.2.2. LEDs

The positions of the LEDs on TigoGateway are illustrated in the schematic diagrams below.

Table 4: Front and Bottom Panel LEDs

Front Panel	Bottom Panel
	
Legend: 1. PWR – On/Off 2. APL – IOLW Master Configured 3. SYS – Firmware Running 4. SF/MS/RUN – System Failure 5. BF/NS/ERR – Bus Failure 6. Pair/GEN - General 7. IOLW - IOLW Connected 8. QSI – Quality Signal Indicator 9. EDGE – Edge Operational	Legend: 10. PWR – On/Off (Connector) 11. LAN1 – RJ45 Ethernet Port 1 12. LAN2 – RJ45 Ethernet Port 2 13. CH0 – RJ45 Ethernet Port 3 14. CH1 – RJ45 Ethernet Port 4

3.2.3. LED Indications

The tables below indicate the states of each LED on the TigoGateway.

3.2.3.1. PWR LED

Table 5: Power LED

LED Type	Color	State	Description
PWR		On	All processes are powered
		Off	One or more processes is not powered

3.2.3.2. APL LED

Table 6: APL LED

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.

3.2.3.3. System LED

Table 7: System LED

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 TigoGateway, or a hardware defect during a firmware reset.

Table 8: 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

3.2.3.4. TigoGateway Device Status (PROFINET)

The **SF** (system failure) and **BF** (bus failure) LEDs indicate the status of the TigoGateway.
The LNK and ACT LEDs indicate the status of the PROFINET.

The following table describes the LED states of the TigoGateway.

Table 9: TigoGateway Device Status

LED	Color	State	Description
SF (System Failure)		Off	No error
		Flashing (1 Hz, 3 s)	DCP signal service is initiated via the bus.
		On	Watchdog timeout - channel, generic or extended diagnosis present - system error
BF (Bus Failure)		Off	No error
		Flashing (2 Hz)	No data exchange
		On	No configuration or low speed physical link or no physical link.

Table 10: LED States

LED Status	Definition
Flashing (1 Hz, 3 s)	The indicator turns on and off for 3 seconds with a frequency of 1 Hz: “on” for 500 ms, followed by “off” for 500 ms.
Flashing (2 Hz)	The indicator turns on and off with a frequency of 2 Hz: “on” for 250 ms, followed by “off” for 250 ms.

3.2.3.5. IO-Link Wireless and Edge Computing LEDs

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

Table 11: Lower Front Panel LEDs Status

LED	Color	State	Description
IOLW		On	All paired ports are in operation mode or no port is paired
		On	When a paired device sends an event and all ports are operational, the LED initially turns yellow for a user-configured duration, after which it turns green. In the case of multiple events, the LED indication restarts from the time of the last event occurrence.
		On	one of the paired ports is not in operation mode
		On	One or more of the paired ports falls within the QSI threshold range, but none of them are below it.
		On	The paired ports are beyond the upper limit of the QSI threshold

LED	Color	State	Description
			range.
		On	One or more of the paired ports falls below the lower limit of the QSI threshold range.
Edge		On	IMX finishes the Power-Up process

3.2.3.6. Ethernet LEDs

Table 12: Ethernet Status (Bottom Panel)

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

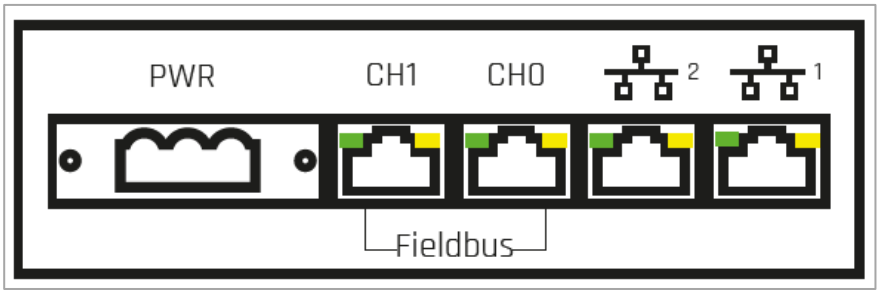


Figure 3: Bottom Panel

Table 13: LED States

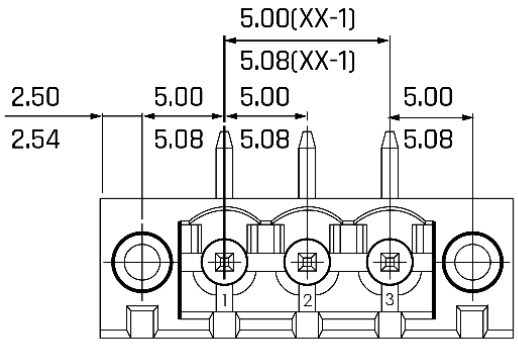
LED Status	Definition
Flickering (Load Dependent)	The LED turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: On for approximately 50 ms, followed by Off for 50 ms. The LED turns on and off in irregular intervals to indicate low Ethernet activity.

3.2.4. Connection Points

3.2.4.1. Power Supply

The device's power is supplied via a 3-pin terminal block about 15mm in length (PWR IN).

Table 14: Power Supply Connectors

PWR IN	Pin	Description
	1	+24 V DC Power In
	2	Ground
	3	Earth

3.2.4.2. Ethernet

Users must use the following connectors to establish a connection with the interface ports of the TigoGateway.

- Connector **CH0** for Ethernet interface port 1
- Connector **CH1** for Ethernet interface port 2

Table 15: EtherNet Connectors

Connector	Location	Dimensions	Description
CH0-OT	Bottom Panel	STD	RJ45 Ethernet port with link and active LED
CH1-OT	Bottom Panel	STD OT	RJ45 Ethernet port with link and active LED
LAN1-IT	Bottom Panel	STD IMX8	RJ45 Ethernet port with link and active LED
LAN2-IT	Bottom Panel	STD IMX8	RJ45 Ethernet port with link and active LED

3.2.4.3. SMA Antenna

The TigoGateway 1TE is equipped with one SMA antenna for a single IO-Link Wireless Track. A track supports up to 8 IO-Link wireless devices. The types of data transferred (e.g. length and data type) may vary depending on the connected devices.

Table 16: Top Panel Connectors

Connector	Location	Dimensions	Description
SMA T1	Top Panel	STD	T1 Antenna (all variants of board)

Table 17: 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, SMA antennas must be mounted for proper device functioning.

4. Installation Overview

Warning:

Comply with all safety instructions relevant to the TigoGateway and to the mounting tools.

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

Make sure that the TigoGateway is not damaged. A damaged TigoGateway must not be put into operation.

TigoGateway can only be used in an indoor location.

4.1. Hardware Installation

This section describes how to mount and ground the TigoGateway.

4.1.1. Select the Mounting Location

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

- The TigoGateway should be hung on a DIN rail which is a metal rail of a standard type widely used for mounting circuit breakers and industrial control equipment inside equipment racks. Standard DIN Rails are available in 35mm (7.5 and 15mm deep), 32mm and 15mm widths and are supplied in 1 m (3'3") and 2 m (6'6”) lengths.
- The TigoGateway must not be mounted in the shearing areas of moving system parts (otherwise it might be damaged).
- The cables for the TigoGateway 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 TigoGateway and connecting all required cables to it.
- The mounting location must meet the TigoGateway’s vibration and shock resistance requirements.
- The diagnostic LEDs of the TigoGateway must be visible when it is mounted.
- The TigoGateway must not be mounted on or near highly inflammable materials.
- To prevent the TigoGateway 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 TigoGateway requires the assembly of a DIN rail on a convenient wall. TigoGateway is attached to the DIN rail from the rear side as shown below.

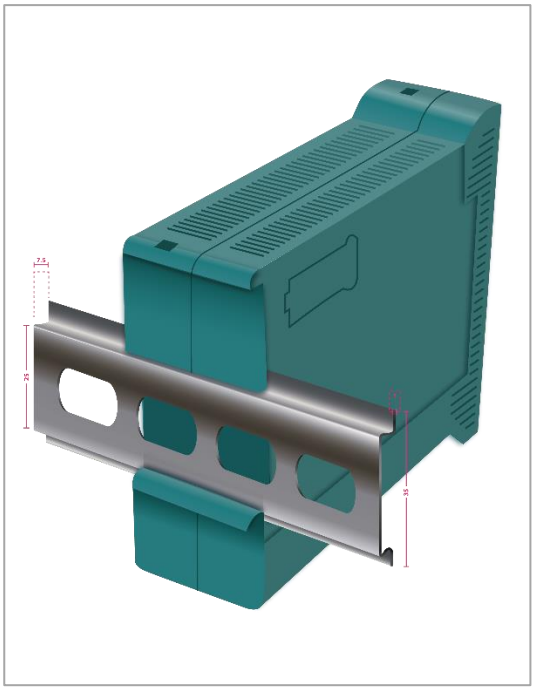


Figure 4: TigoGateway Bracket for DIN Rail

4.1.3. Mount the TigoGateway

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

1. Disconnect the system from the power supply.
2. Ensure sufficient equipotential bonding in the system.
3. Secure unit in the desired position on the DIN rail (inner width 25mm, outer width 35mm, depth 7.5mm).
4. Mount the TigoGateway's two SMA antennas (X1, X2).

   All SMA antennas (X1, X2) must be mounted for proper TigoGateway operation.

4.1.4. Ground the TigoGateway

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

Ground the TigoGateway as follows:

1. Connect TigoGateway 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 TigoGateway is mounted on a non-conductive base.
2. Make sure that the contacts are attached solidly and that the cable cross-section is sufficient.

4.1.5. Demount the TigoGateway

1. Disconnect the part of the plant to which you have mounted the TigoGateway from the power supply.
2. Verify that the plant on which the TigoGateway is mounted is de-energized.
3. If the TigoGateway is dirty, clean it first.
4. Before demounting from the DIN rail, disconnect the cables.
5. Remove the TigoGateway 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. When the TigoGateway is in operation, let it cool down before touching it or use gloves.

Warning:

If the demounted TigoGateway 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 collection point.

4.2. Connect TigoGateway

Warning:

- Danger of electrical shock.
- Operate the TigoGateway 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.

Fuse Protection

The maximum supply current must not be exceeded and must be fused with an external fuse (16 A). Otherwise, there is a risk of malfunction and damage to the printed circuit board and the connecting plug.

Connection Example with TigoBridge

The connection example described below 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.

Process:

1. Connect the Ethernet cable to the **CH0** connector of the TigoGateway and to the Controlling IPC and/or to PLC.
2. Connect the power cable to the **PWR** connector of the TigoGateway.
3. Connect the wired IO-Link device with the cable to the W-Bridge.
4. Connect the power cable (+24 V DC SELV or PELV) to the power connector of the W-Bridge.
5. Switch on the power supply units of the TigoGateway and TigoBridge.

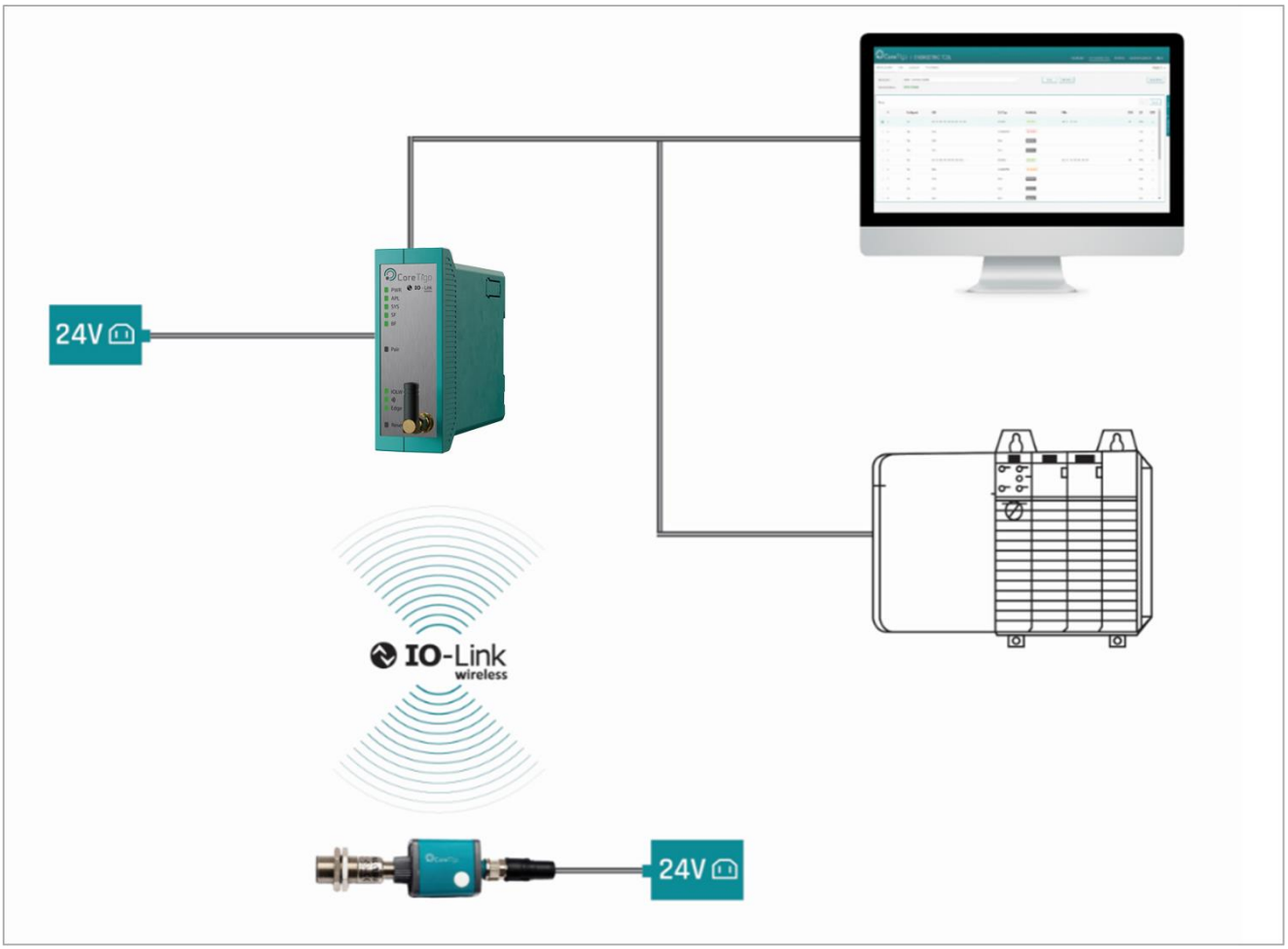


Figure 5: Connection Example with TigoBridge

4.3. Login to TigoGateway

To login to TigoGateway follow the below procedure.

1. Connect Ethernet cable to TigoGateway LAN1 port.

   Important: make sure Ethernet cable is connected to Network with DHCP capabilities as TigoGatway requires to get an IP from the network.

2. Use the URL provided by CoreTigo, which appears on the left side-label http://tigogateway-YYZZ:9001/ ,see Product Overview.

   The TigoGateway home page opens.

3. From here the user can access the three software tools detailed in Software Setup.
4. On the landing page connect the TigoEngine using the **GET STARTED** button
5. Use the SW Key provided with the TigoGateway to activate your TigoEngine License

References:

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

6. Connect to the TigoGateway to start IOLW configuration, for more information see 0 – TigoEngine configuration

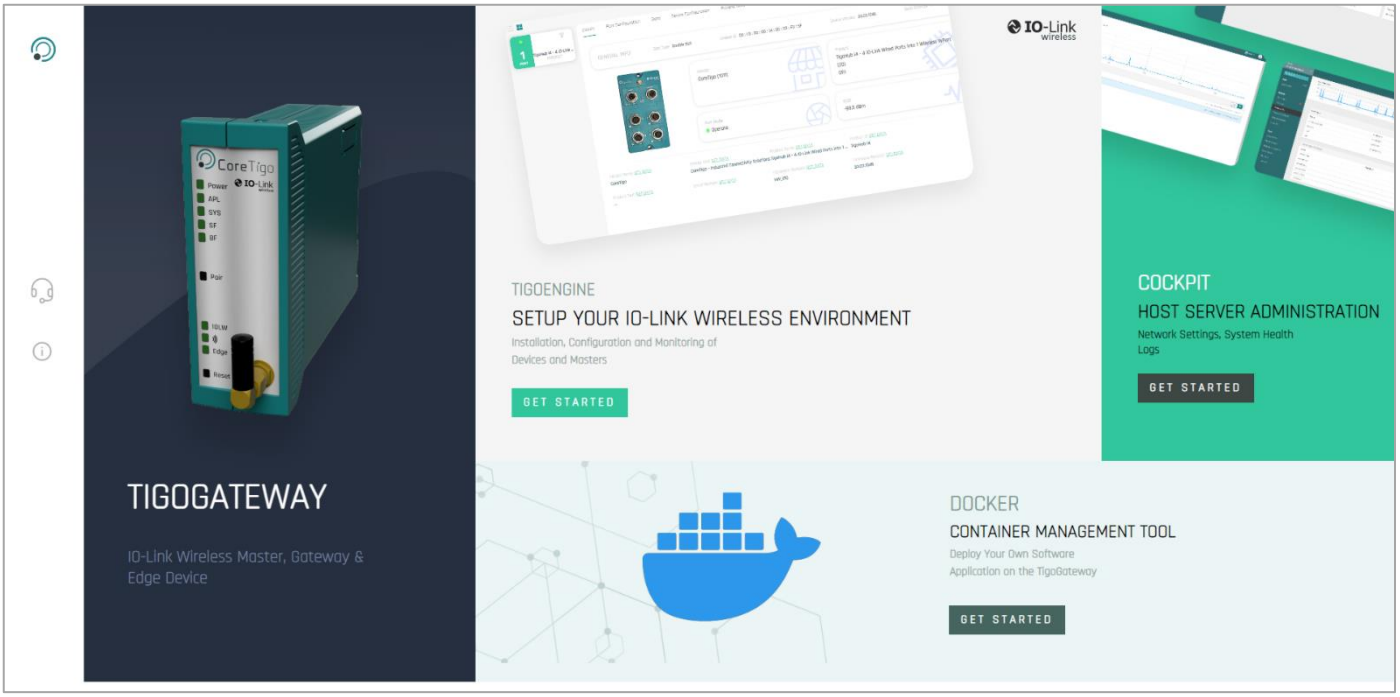


Figure 6: TigoGateway Homepage

4.4. Built-In Software

Three software tools enable the installation, setup, maintenance and control of the TigoGateway, in addition to the available internet browser:

- TigoEngine – IO-Link Wireless configuration tool
- Linux Cockpit – Linux OS web-based management system
- Docker – Containers management tool

4.4.1. TigoEngine

TigoEngine is a software-based management platform for the efficient setup of IO-Link Wireless masters and devices. It enables installation, configuration, and monitoring of an IO-Link Wireless system.

Note:
The TigoEngine is already installed on the TigoGateway, and the user will be provided with a suitable license.

Reference:
For further information please refer to the *TigoEngine User Manual*.

Online and offline setup of IO-Link Wireless components is possible, with a variety of options to connect to IO-Link Wireless masters. With its intuitive user interface, TigoEngine simplifies the deployment and maintenance of an IO-Link Wireless system.

TigoEngine can connect to IO-Link Wireless masters using either of the following physical interfaces:

- UART over USB
- Ethernet

TigoEngine Key Functionalities

- IO-Link Wireless Master communication and configuration
- Scanning for available IO-Link Wireless devices within range of an IO-Link Wireless master
- Pairing and connecting IO-Link Wireless devices to the relevant IO-Link Wireless masters
- Configuration of IO-Link Wireless device parameters based on IODD
- Wireless channel blacklist configuration per master
- Loading parameters from an IO-Link sensor
- Bulk configuration of devices via uploaded files
- Firmware upgrade—updating wireless devices using FOTA
- Third party software integration via an MQTT publisher—exporting process data from TigoEngine to third party software (requires an MQTT broker on the third party software side)
- Performance Monitoring:
    - Packet Error Rate (PER) real-time display—enables analysis of latency and network interferences
    - Link Quality Indication (LQI)
    - Received Signal Strength Indication (RSSI)

4.4.2. Linux Cockpit

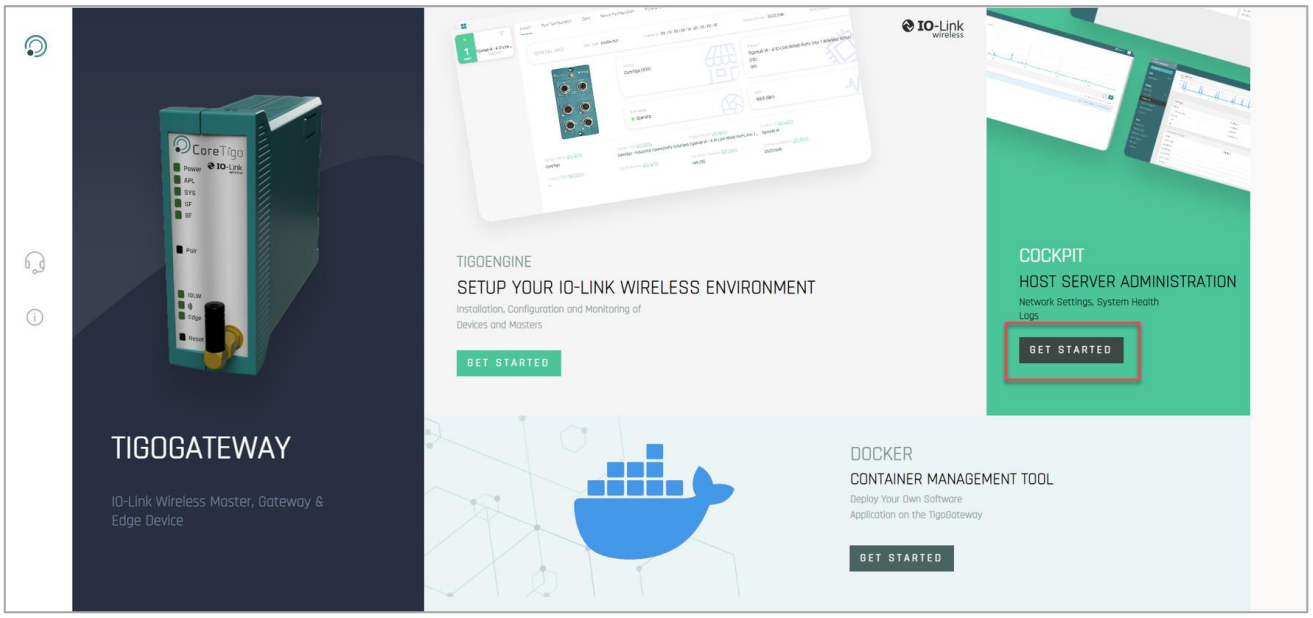
Cockpit is a web-based graphical interface for servers, intended for general use. It resembles a desktop interface, but for individual servers.

Cockpit makes Linux discoverable i.e. there is no need to remember commands at a command-line. The user can see the server in a web browser and perform system tasks easily with a mouse, such as starting containers, administering storage, configuring networks, and inspecting logs.

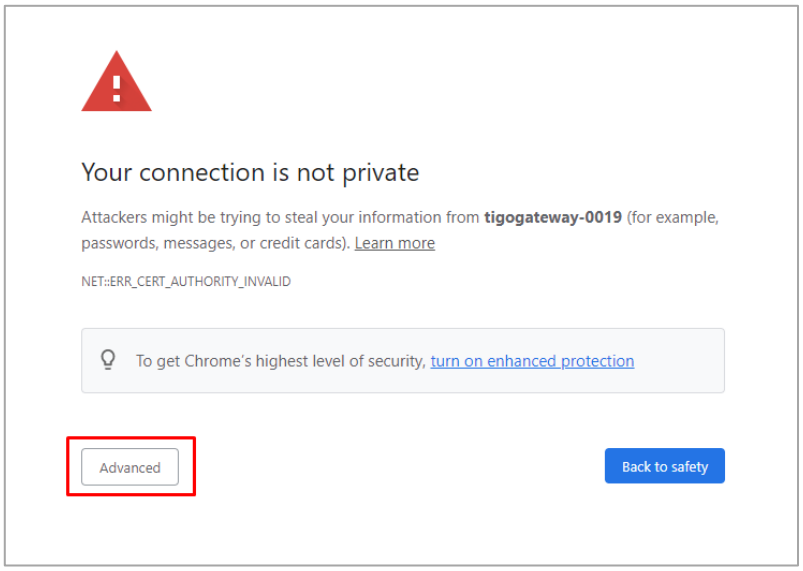
Cockpit uses APIs that already exist on the system. It does not reinvent subsystems or add a layer of its own tooling. By default, Cockpit uses the system's normal user logins and privileges. Network-wide logins are also supported through single-sign-on and other authentication techniques. It runs on demand only.

Cockpit Usage Process

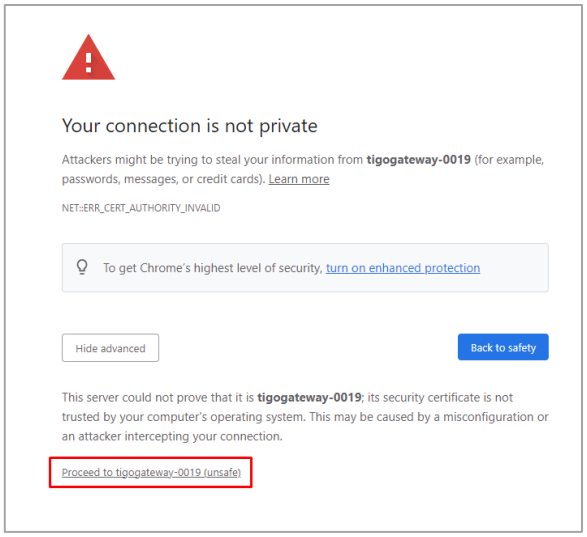
1. From the home page click the **Get Started** button in the **Cockpit** area of the page.



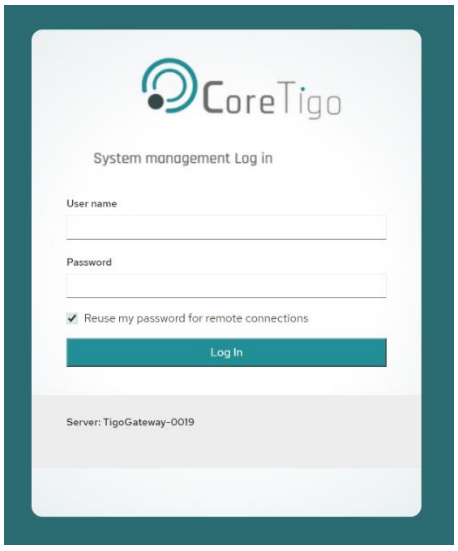
2. In the warning page which opens, click on **Advanced.**



3. Click on the **Proceed to TigoGateway** link.

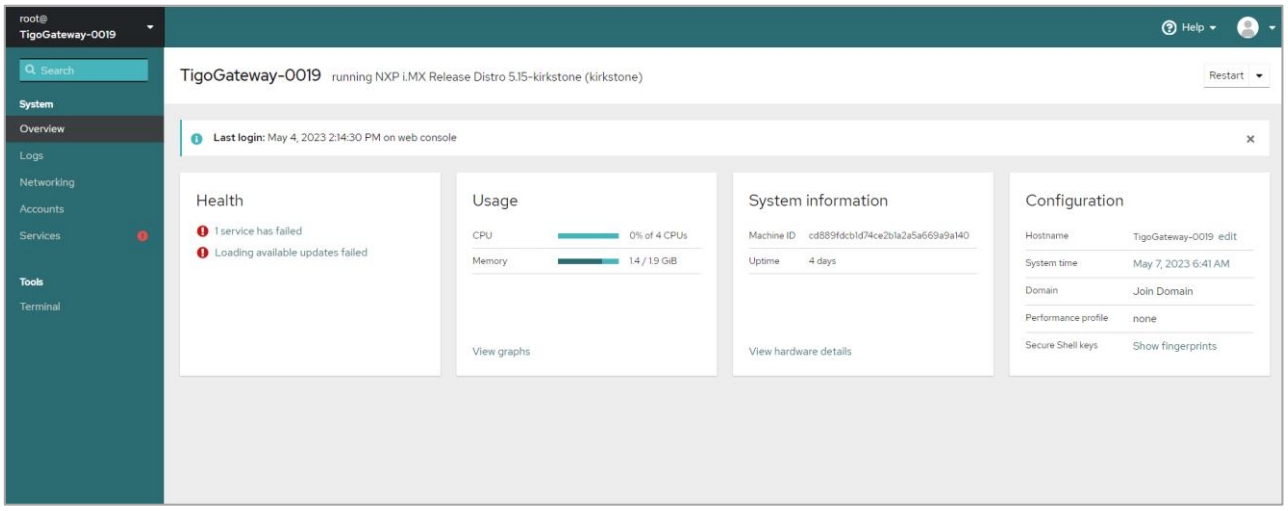


The **Login** window opens.



4. Enter the Username (tigogateway) and Password (tigogateway) provided to you by CoreTigo.
5. Click the **green** **Log In** button.

   The TigoGateway Cockpit dashboard opens.



6. If the condition **Limited Access** appears in the toolbar, click the **green** **Turn On Administrative Access** button.

   Apart from other functions available in the Linux Cockpit, the most useful function for TigoGateway users is the **Networking** capability, which affords access to the network cards of the device.

   The user can then change the settings for the network cards available.

   Other functions available are mostly for information purposes as displayed in the dashboard. Some drill-down capability is available from the items in the side-panel menu, to access further details and configure settings at each level, such as **Logs**, **Accounts**, **Services**.

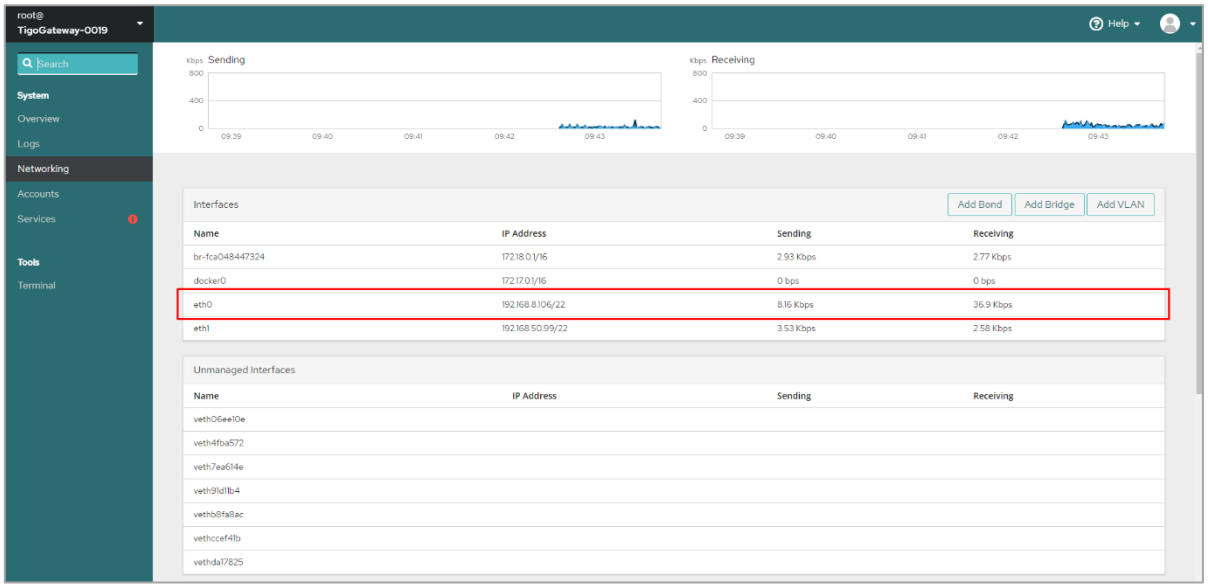
   From the **Terminal** menu item in the side-panel menu, the user can create command lines, similar to regular Windows functionality.

   Cockpit supports a large list of optional and third-party applications.

Reference:

- Red Hat Customer Portal product documentation

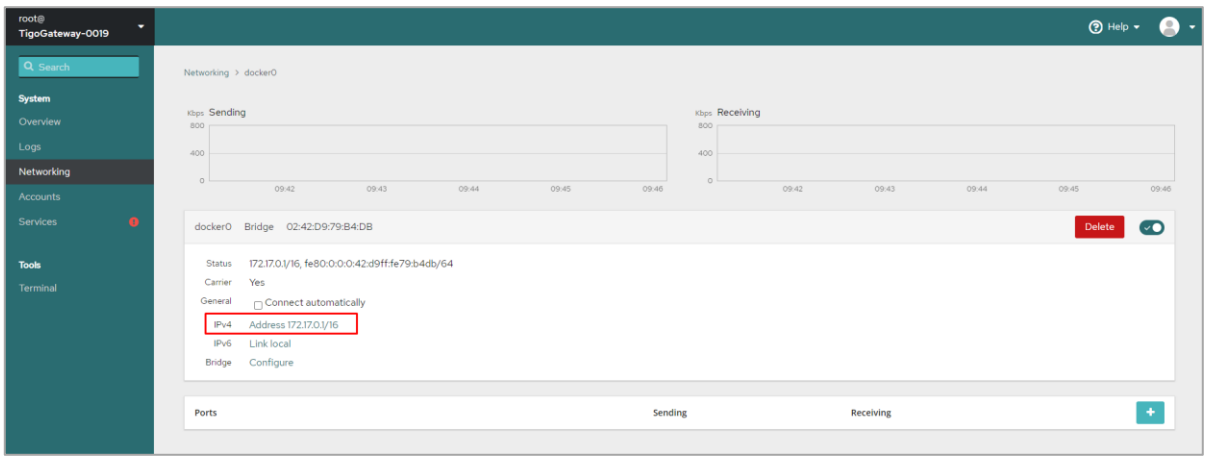
7. To view networking functionality, click the **Networking** item in the side-panel menu.



   In the **Interfaces** list, the interfaces **eth0** and **eth1** equilibrate to the **LAN1** and **LAN2** ports on the bottom panel of the TigoGateway.

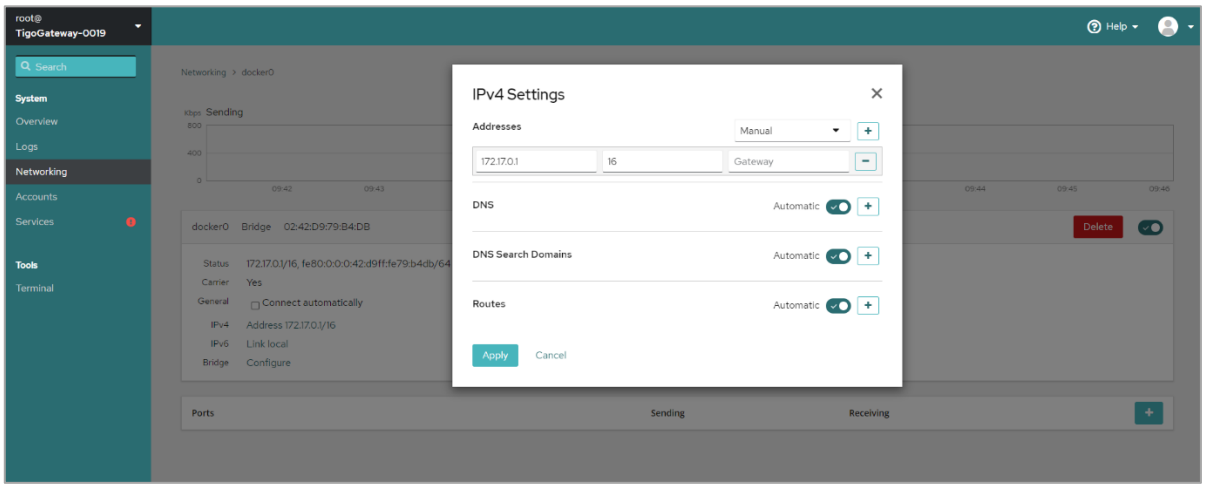
8. To configure settings for these interfaces click on their names in the list.

   The details are displayed when you click on one of them.

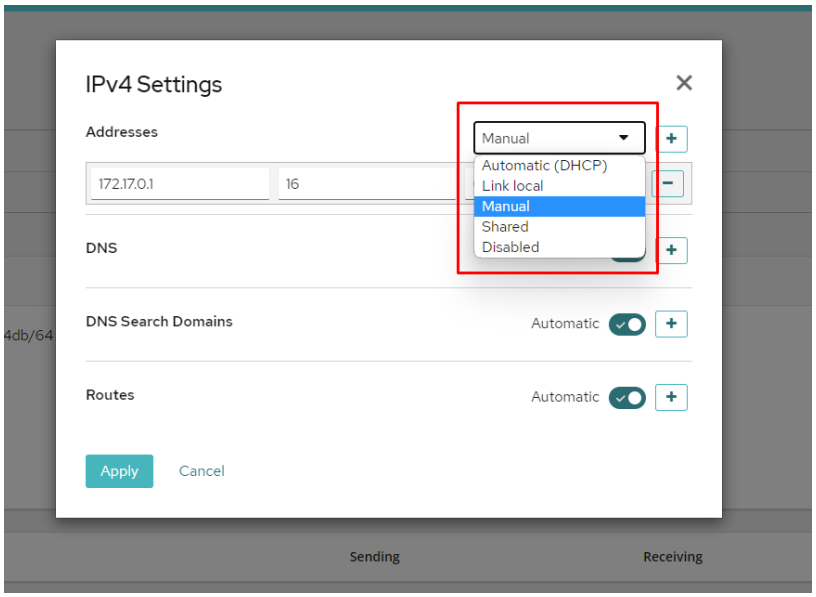


9. Click the **Automatic (DHCP)** link listed alongside the item **IPv4**.

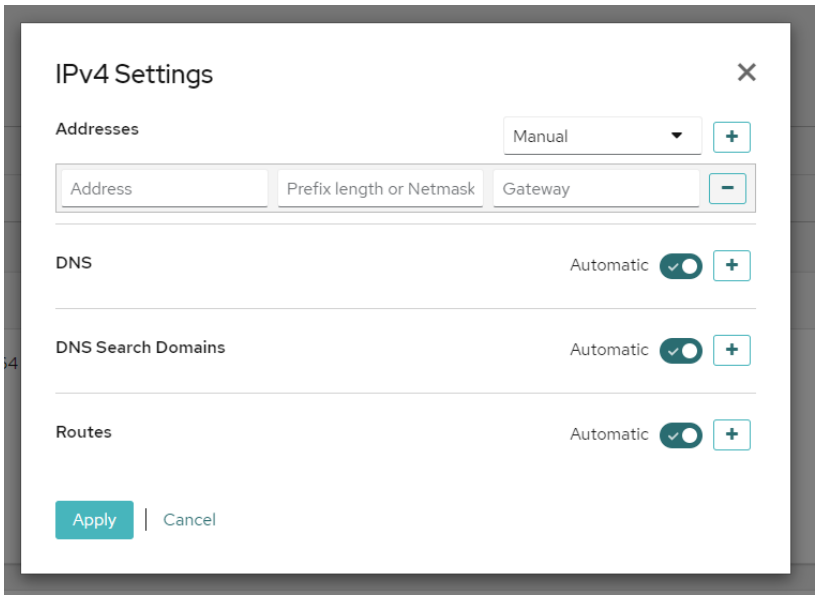
The **IPv4 Settings** window opens.



10. Open the dropdown list available in **Addresses**.



11. Here you can fix a static IP Address through the **Manual** menu option which opens another window in which you can insert an appropriate IP address.



4.4.3. Docker

Docker is a set of platform-as-a-service products that use OS-level virtualization to deliver software in packages called Containers. The software that hosts the Containers is called Docker Engine.

A Container is a standard unit of software that packages up code and all its dependencies, to ensure the application will run quicker and more reliably from one computing environment to another. A Docker Container image is a lightweight, standalone, executable package of software that includes everything needed to run an application such as code, runtime, system tools, system libraries and settings.

Container images become Containers at runtime and Docker Container images become Containers when they run on the Docker Engine.

Containerized software runs on the OS supported by Docker, regardless of the infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.

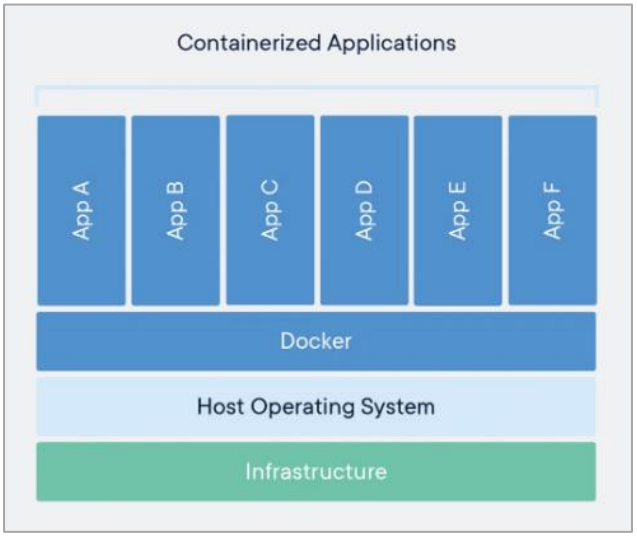


Figure 7: Containerized Applications

For further details on the Docker functionality, please refer to the following.

References:

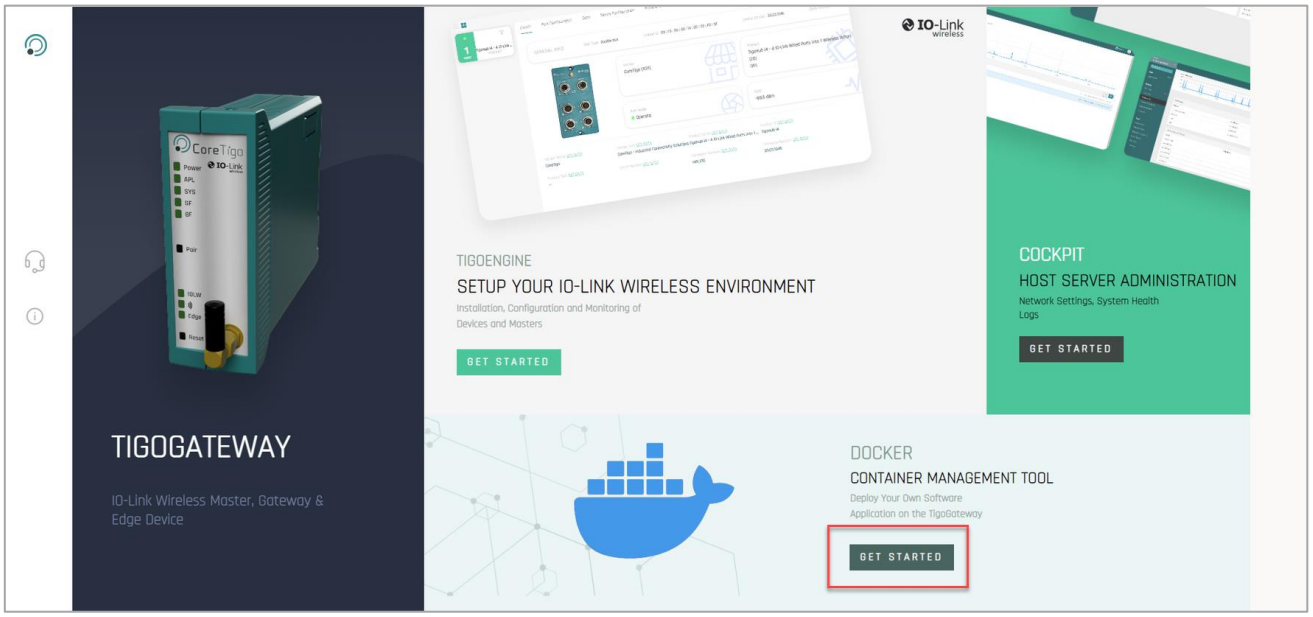
- Docker: Accelerated, Containerized Application Development
- Welcome - Portainer Documentation

The Docker is used to promote a new business logic and upload it to a virtual application.

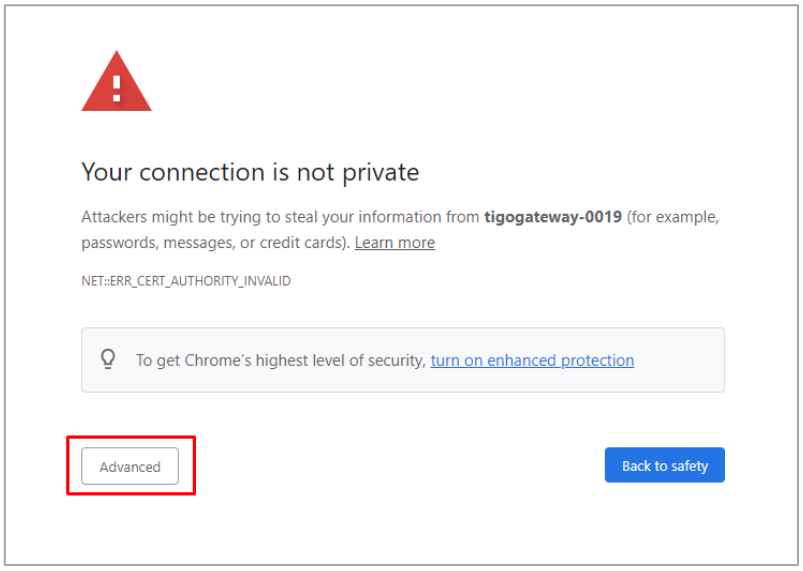
Refer also to Docker Configuration.

Docker Usage Process

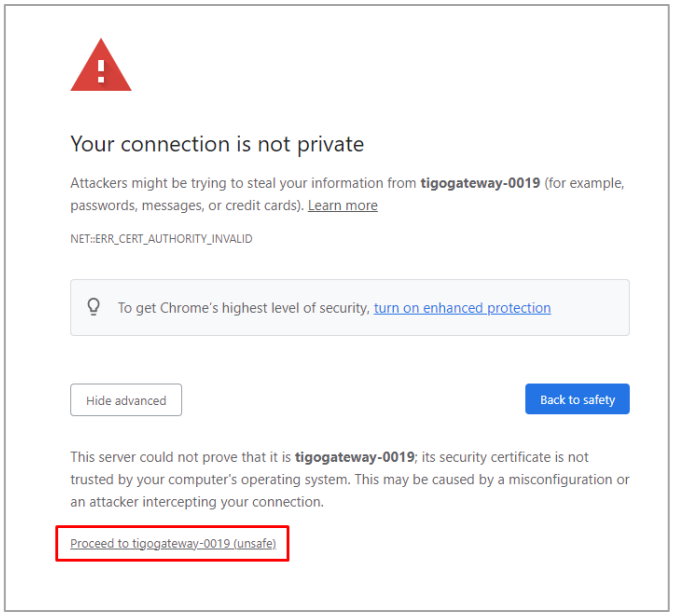
1. From the home page click the **Get Started** button in the **Docker** area of the page.



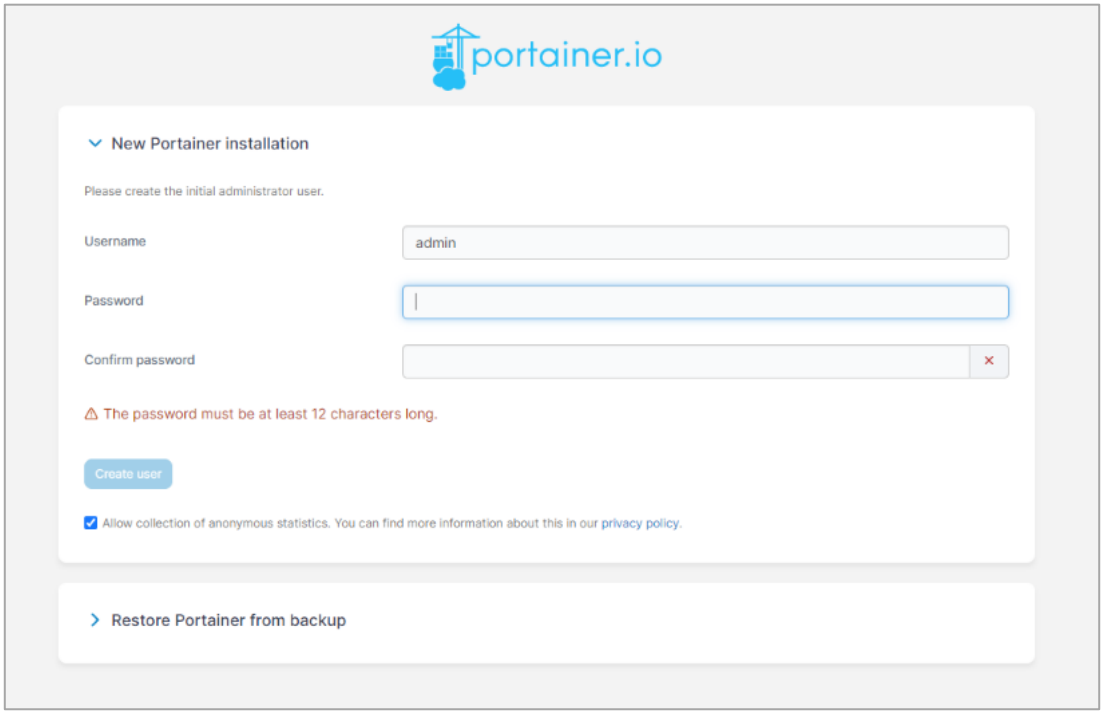
2. In the warning page which opens, click on **Advanced.**



3. Click on the **Proceed to TigoGateway** link.

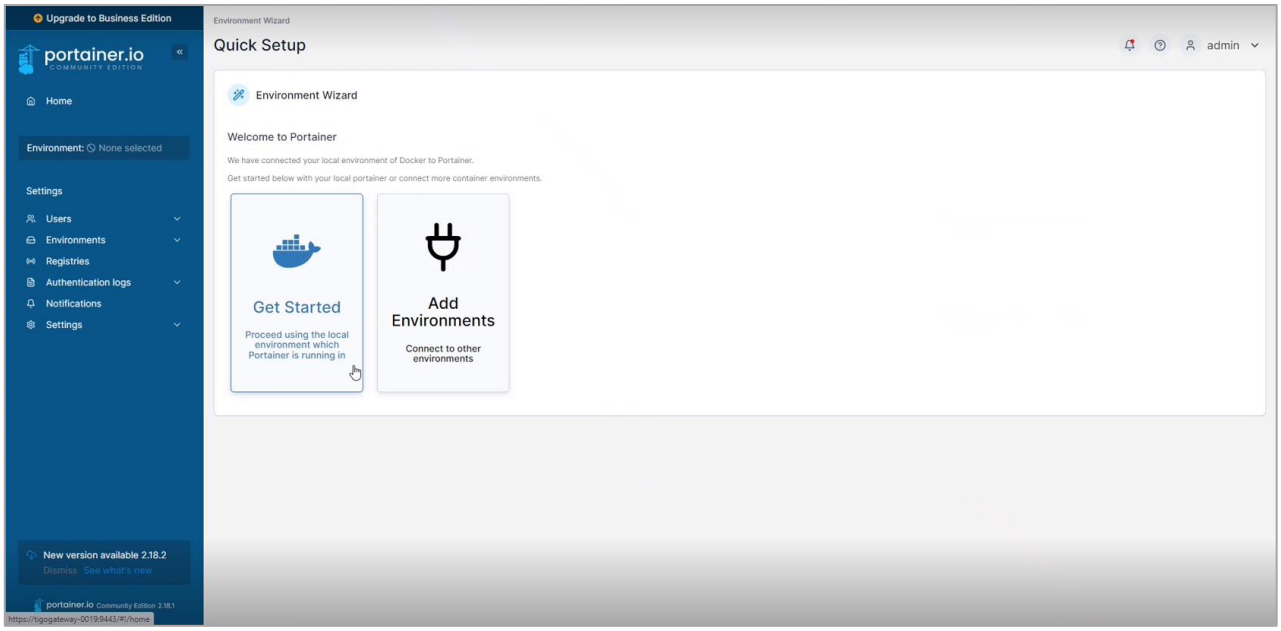


The **Login** window opens.

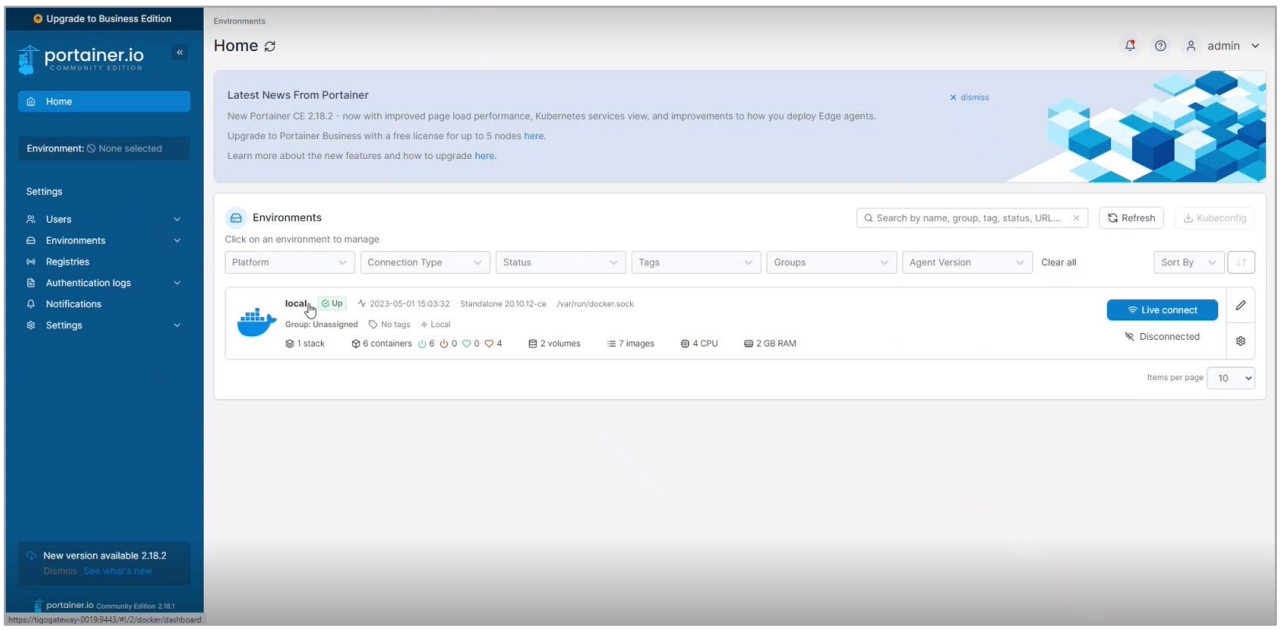


4. Enter the Username and Password provided to you by CoreTigo, and confirm the password.

The **Quick Setup** page opens.

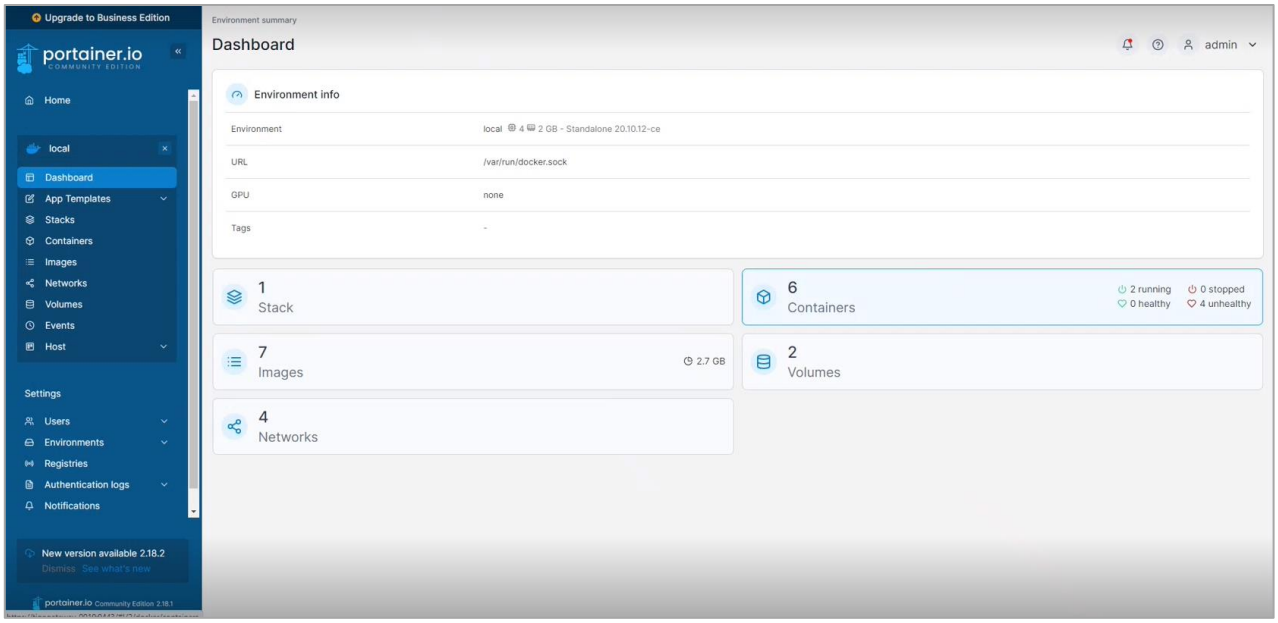


5. Click the **Get Started** box (initial setup only) to access the **Home** page.



This page is normally accessed from the side-panel menu, when required.

6. Click the **blue** **Docker** icon.The **Dashboard** opens, displaying an overview of the product setup.



5. Configuration

Before the TigoGateway can operate together with its connected devices, it must be configured.

Configuration has the following levels:

- PROFINET IO-Link configuration – for input/output data of the PROFINET I/O modules/submodules.
- IO-Link Wireless Master configuration – of TigoGateway parameters (e.g. track mode).
- Port configuration – of parameters for the wireless ports (subslots), for connected IO-Link Wireless devices and TigoBridge devices, and for Standard IO mode.
- (Optional) MQTT Client configuration – if MQTT communication is used, then the parameters of the MQTT client in the TigoGateway need to be configured.

Configuration is performed using one or more tools together with a GSDML file.

Two GSDML files are available, and which GSDML file the user selects determines which tool(s) he/she can use to configure each of the above levels.

5.1. Introduction

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

- TigoGateway:
  - Input/output data of the PROFINET I/O modules/submodules.
  - Parameters for the IO-Link Wireless Master (e.g. track mode).
  - Parameters for the wireless ports (e.g. wireless slot number).
  - MQTT Client parameters – if the MQTT communication is to be used, then the MQTT Client in the TigoGateway requires MQTT Client parameters to be set.
- Connected IO-Link devices:
  - IO-Link device parameters.

To set parameters, use the following tools:

- **Configuration Software of the PROFINET IO-Controller**

  The PROFINET IO-Controller must be configured to exchange process data with the TigoGateway device. The configuration software of the PROFINET IO-Controller requires a GSDML file to configure the device.

  The configuration software of the PROFINET IO-Controller imports the GSDML file, and the user can make the configuration settings and parameterizations for the device. Load the configuration to the PROFINET IO-Controller.

  The PROFINET IO-Controller performs the configuration and parameterization of the TigoGateway device.

- **TigoEngine**

  TigoEngine is software that enables the user to do the following:

  - Set all parameters for the TigoGateway, its connected IO-Link devices, and the MQTT Client in the TigoGateway.
  - Monitor the TigoGateway and IO-Link devices in any system connected to TigoEngine.

- **Linux Cockpit**

  Linux Cockpit is a web-based graphical interface for servers, intended for general use, enabling the user to do the following:

  - Configuration of the IMX8.
  - Setting the IP address of the IMX8.
  - Basic user management functionality.

5.2. Configure TigoGateway

5.2.1. Choose a GSDML File

The table below details which configuration tool(s) each GSDML file can be used with, and which configuration levels it is suitable for.

The following guidelines might also help you to decide which GDSML file to select:

- If you want to use one configuration tool for every level of configuration (except MQTT communication), you can do so with the Expert file and the PROFINET IO-Controller.
- If you want to use TigoEngine for IO-Link Wireless Master configuration or Port configuration, you need to use the PDCT GSDML file.

Table 18: Configuration Tool and GSDML File Combinations

Configuration Tool	GSDML File Available for Use with Tool	Configuration Level					Comment
		CPU	IO-Link	IO-Link Wireless Master	Port	MQTT client	
PROFINET IO-Controller and its Configuration Software (PLC configuration tool)	GSDML-V2.35-CoreTigo-TigoMaster-Expert-20211202	Defined by the Linux Cockpit	Applicable	Applicable	Applicable	N/A	The software for the PROFINET IO-Controller enables you to configure parameters and then load the configuration to the IO-Controller, which in turn configures the TigoGateway.
	GSDML-V2.35-CoreTigo-TigoMaster-PDCT-20211202	Defined by the Linux Cockpit	Applicable	N/A	Applicable	N/A	
TigoEngine							See TigoEngine
Linux Cockpit							See Linux Cockpit

5.2.2. Import the GSDML File to the PROFINET IO-Controller Software

1. Make sure to have a copy of the desired GSDML file.
2. Open the PROFINET IO-Controller Software (TIA Portal).
3. Select **Options** > **Manage General Station Description (GSD) Files**.

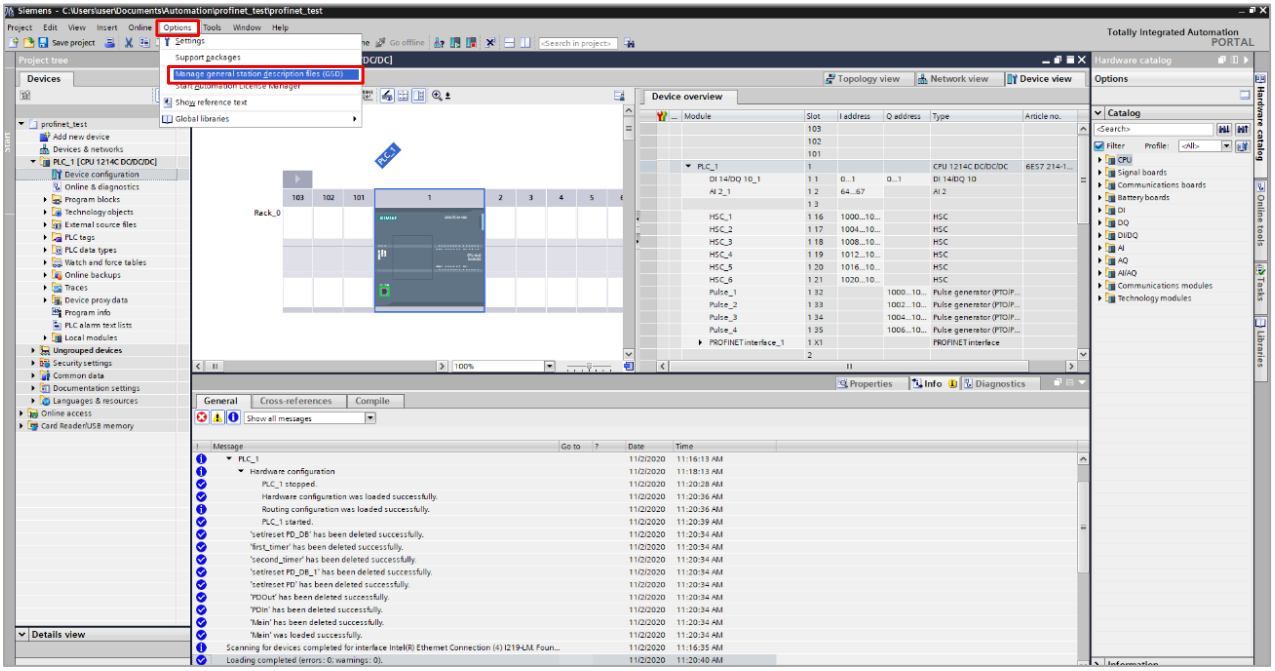


Figure 8: Manage General Station Description (GSD) Files

4. In the **Manage General Station Description Files** window, make sure that the **Installed GSDs** tab is selected.
5. Click the ellipsis (**…**) button.

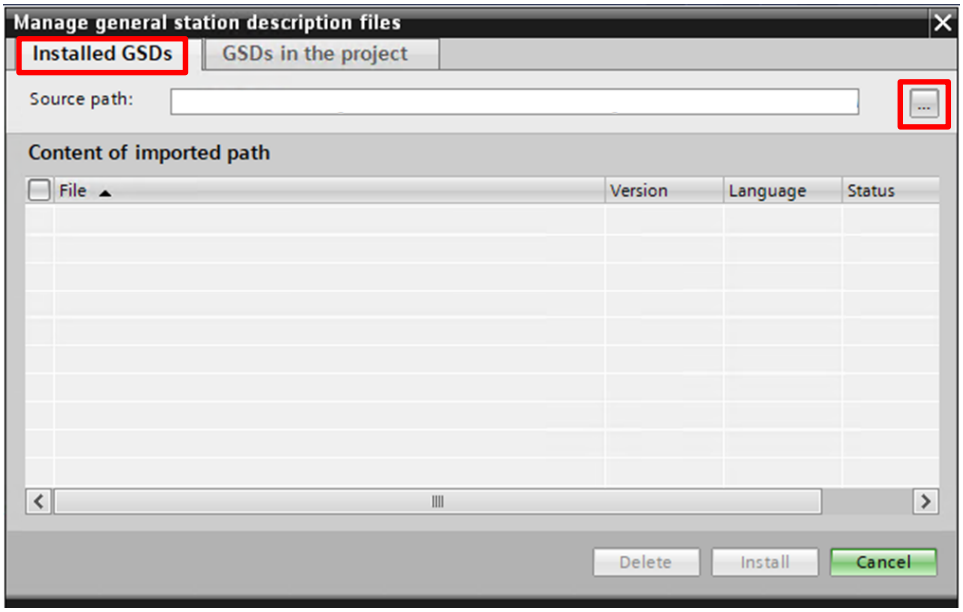


Figure 9: Manage General Station Description Files - Installed GSDs Tab

6. Select the **Source Path** for the GSDML file.

7. A list of available GSD files appears under **Content of imported path**.

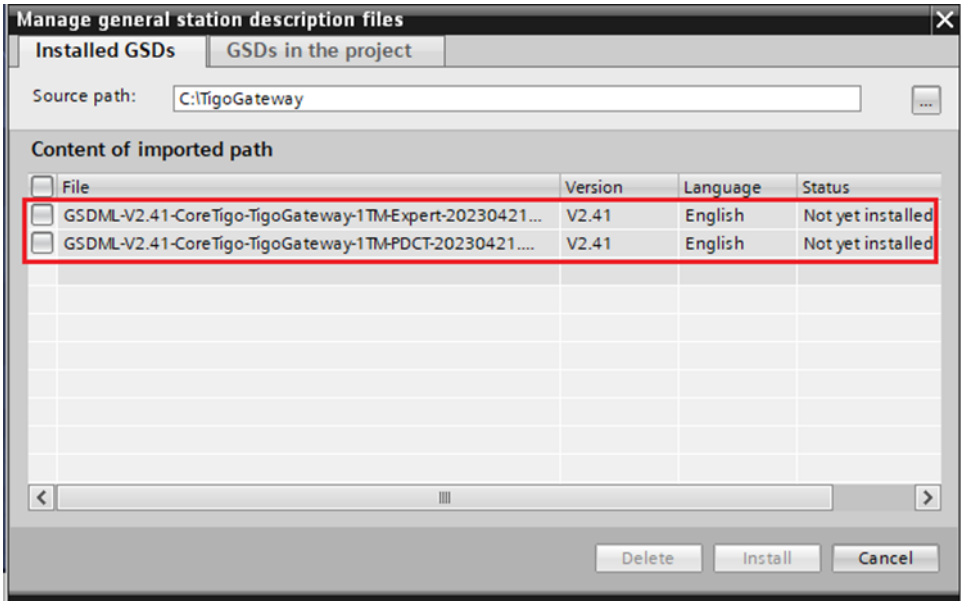


Figure 10: List of Available GSD Files

8. Select the desired GSDML file from the list.
9. Click the **Install** button.

   When the installation is complete, a new module (TigoGateway) is added to the **Hardware catalog** under **Other field devices**.

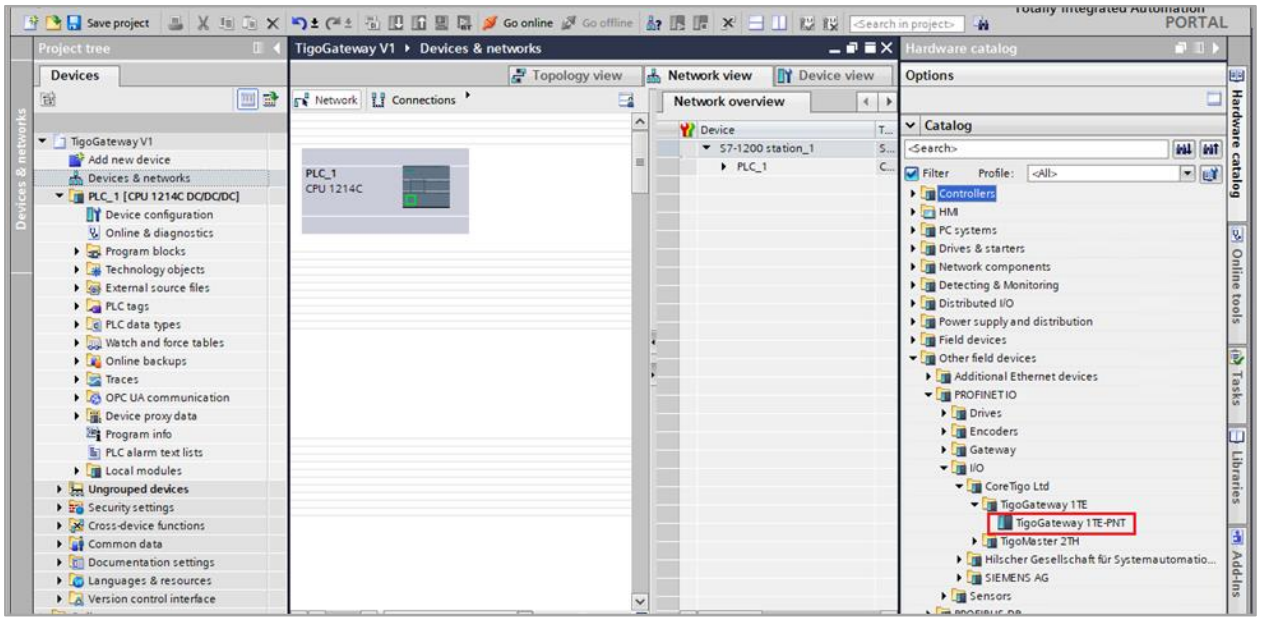


Figure 11: New Module Added to Hardware Catalog

5.2.3. Configure the IP Address

1. In the **Hardware catalog** pane, locate the TigoGateway, and then drag it to **Devices & networks** > **Topology view**.
2. In the **Network View** tab, draw a connection between the TigoGateway and PLC.

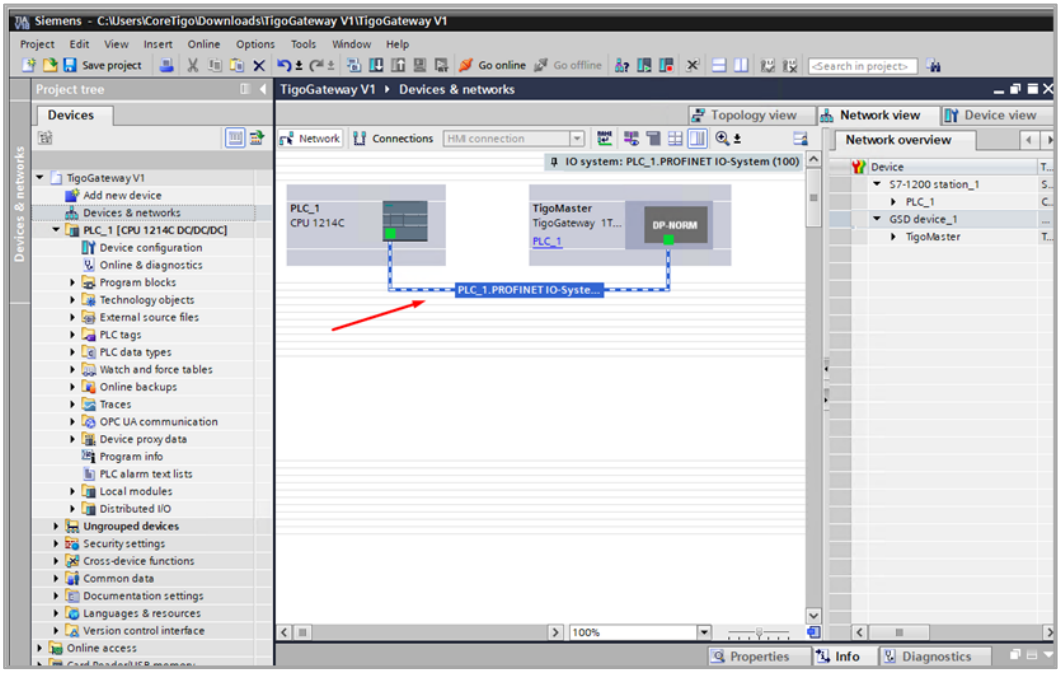


Figure 12: Network View

3. Select the TigoGateway and go to the **Device view** tab.
4. Click on the TigoGateway (which is outlined in **Red**) to open configuration fields.

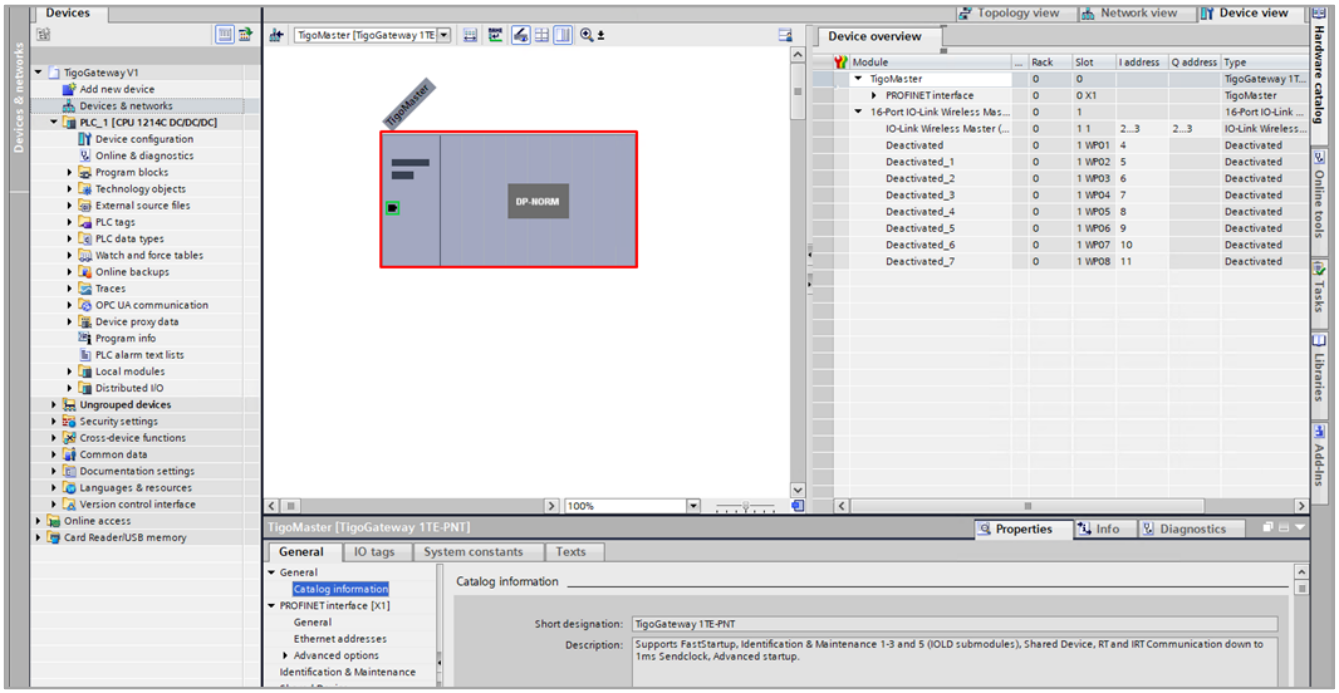


Figure 13: Device View

5. In the **General** tab, go to **PROFINET interface [x3]** > **Ethernet addresses**.
6. Under **IP protocol**, set the desired **IP address**.

7. Under **PROFINET**, make sure the **PROFINET device name** is correct.

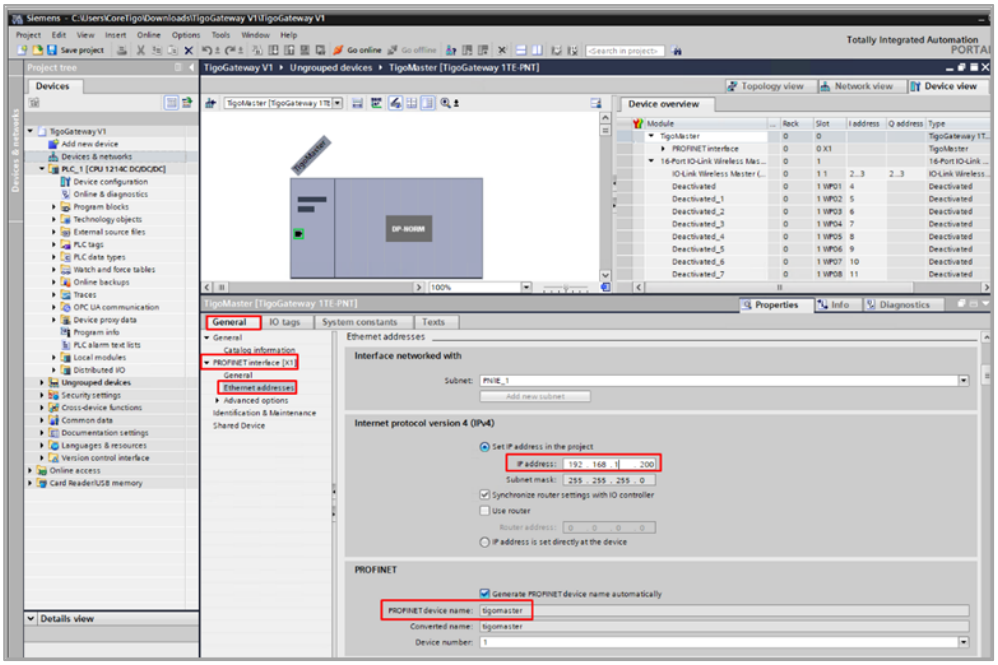


Figure 14: Ethernet Addresses

5.2.4. Configure Ports (Subslots)

TigoGateway has a modular structure that includes various slots and subslots: see the table below.

The eight subslots are IO-link wireless ports that need to be configured as detailed in this section.

Table 19: Slots and Subslots of TigoGateway

Slot	Subslot	Submodule	Description
0	1	DAP	Device access point TigoGateway IO-Link Wireless device (fixed)
	32768	PN-IO	PROFINET interface (fixed)
	32769	X31	Ethernet interface, PROFINET IO port 1 (fixed)
	32770	X32	Ethernet interface, PROFINET IO port 2 (fixed)
1	1	IO-Link Wireless Master	IO-Link Wireless master (fixed) 2 input bytes and 2 output bytes
	2	Configuration port WP01	Each port (subslot) needs configuring, as detailed in the rest of this section.
	3	Configuration port WP02	
	4	Configuration port WP03	
	5	Configuration port WP04	
	6	Configuration port WP05	
	7	Configuration port WP06	
	8	Configuration port WP07	
	9	Configuration port WP08	

To configure ports:

1. Go to the **Device View** tab.

   Here you can see a table of the various modules of TigoGateway.
   Note the **Slot** column (which combines slot and subslot), and in particular the rows for slot/subslot **1 WP01**–**1 WP08**: these are the IO-Link wireless ports, which need to be configured.

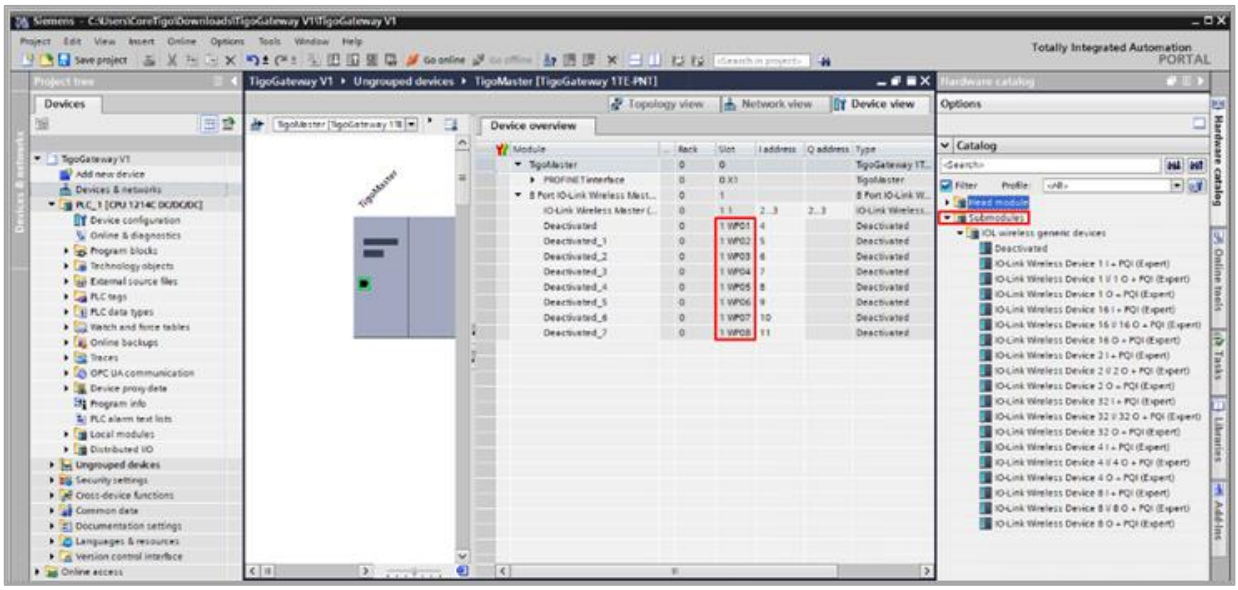


Figure 15: Device View Tab – Wireless Ports 1 WP01–1 WP08

2. In the **Catalog** pane, go to **Submodules** -> **IOL wireless generic devices**.

   Here you can see a list of the IO-Link wireless device types.
   For details of each device type see the table below.

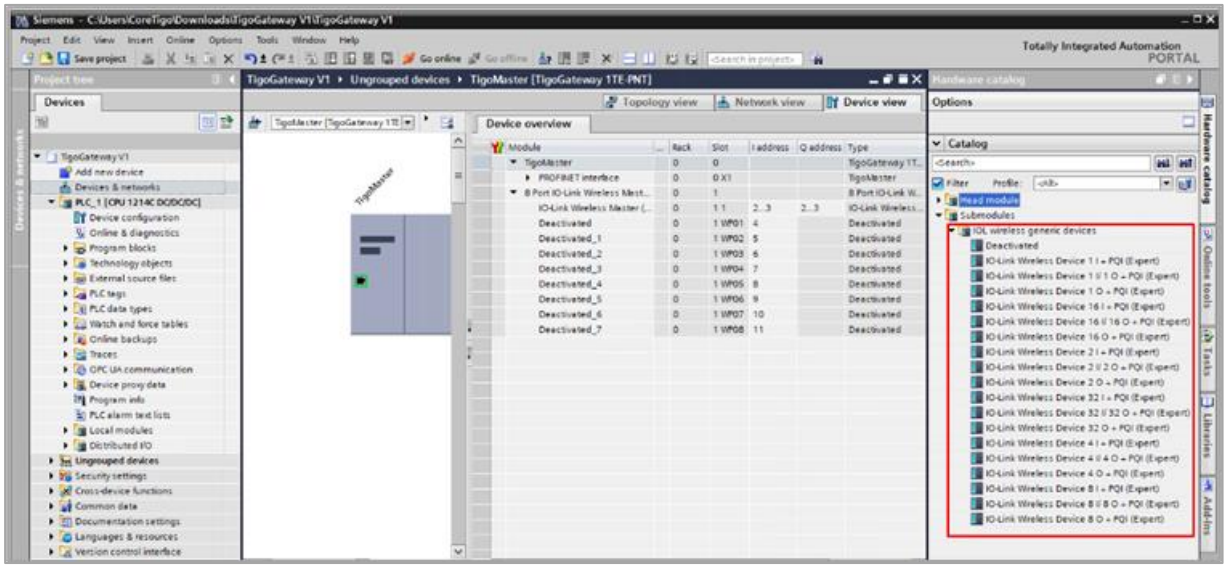


Figure 16: IO-Link Wireless Device Types

Table 20: IO-Link Wireless Device Types

Device Type	Description	Input Process Data Size (PD_IN)	Output Process Data Size (PD_OUT)
IO-Link 1 I + PQI	IO-Link with 1 byte input data and port qualifier information	1 byte + 1 byte PQI	-
IO-Link 1 I / 1 O + PQI	IO-Link with 1 byte input data and 1 byte output data and port qualifier information	1 byte + 1 byte PQI	1 byte
IO-Link 1 O + PQI	IO-Link with 1 byte output data and port qualifier information	-	1 byte
IO-Link 16 I + PQI	IO-Link with 16 bytes input data and port qualifier information	16 bytes + 1 byte PQI	-
IO-Link 16 I / 16 O + PQI	IO-Link with 16 bytes input data and 16 bytes output data and port qualifier information	16 bytes + 1 byte PQI	16 bytes
IO-Link 16 O + PQI	IO-Link with 16 bytes output data and port qualifier information	-	16 bytes
IO-Link 2 I + PQI	IO-Link with 2 bytes input data and port qualifier information	2 bytes + 1 byte PQI	-
IO-Link 2 I / 2 O + PQI	IO-Link with 2 bytes input data and 2 bytes output data and port qualifier information	2 bytes + 1 byte PQI	2 bytes
IO-Link 2 O + PQI	IO-Link with 2 bytes output data and port qualifier information	-	2 bytes
IO-Link 32 I + PQI	IO-Link with 32 bytes input data and port qualifier information	32 bytes + 1 byte PQI	-
IO-Link 32 I / 32 O + PQI	IO-Link with 32 bytes input data and 32 bytes output data and port qualifier information	32 bytes + 1 byte PQI	32 bytes
IO-Link 32 O + PQI	IO-Link with 32 bytes output data and port qualifier information	-	32 bytes
IO-Link 4 I + PQI	IO-Link with 4 bytes input data and port qualifier information	4 bytes + 4 bytes PQI	-
IO-Link 4 I / 4 O + PQI	IO-Link with 4 bytes input data and 4 bytes output data and port qualifier information	4 bytes + 4 bytes PQI	4 bytes
IO-Link 4 O + PQI	IO-Link with 4 bytes output data and port qualifier information	-	4 bytes
IO-Link 8 I + PQI	IO-Link with 8 bytes input data and port qualifier information	8 bytes + 8 bytes PQI	-
IO-Link 8 I / 4 8 O + PQI	IO-Link with 8 bytes input data and 8 bytes output data and port qualifier information	8 bytes + 8 bytes PQI	8 bytes
IO-Link 8 O + PQI	IO-Link with 8 bytes output data and port qualifier information	-	8 bytes

3. Configure each IO-Link wireless port (subslot).
4. Select the type of device that is / will be connected to the port being configured, and drag it into the port's row in the **Device View** tab.

In the example below, port **WP01** is being configured for **IO-Link Wireless Device 32 I / 32 O + PQI**.

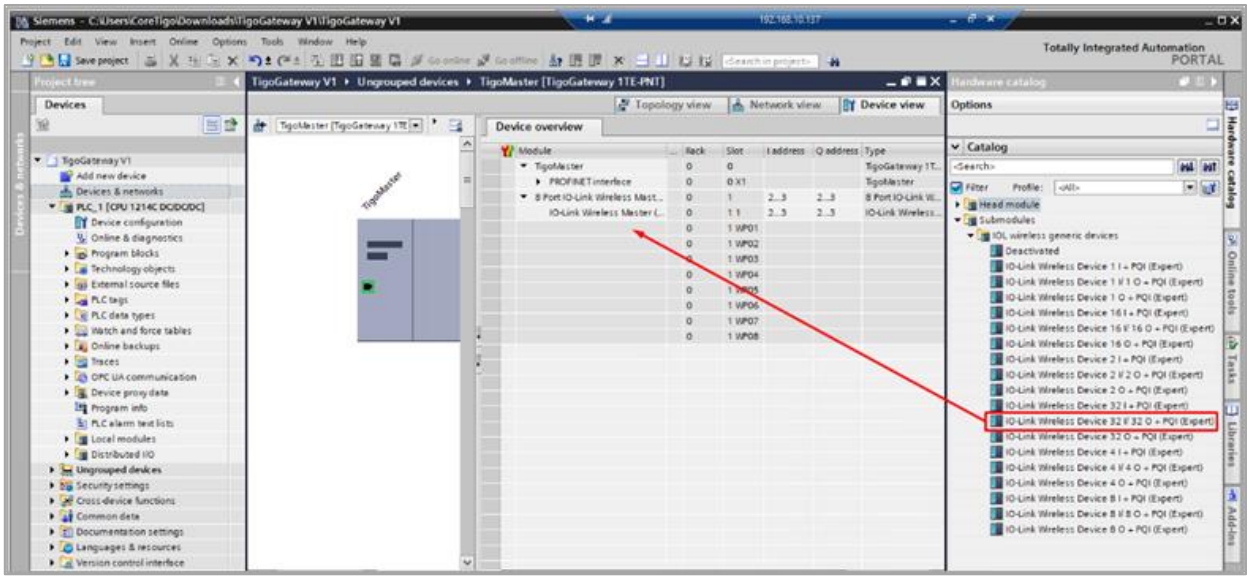


Figure 17: Setting a Port's Device Type

A **Device Inspector** pane appears (outlined in **Red** in the image below).

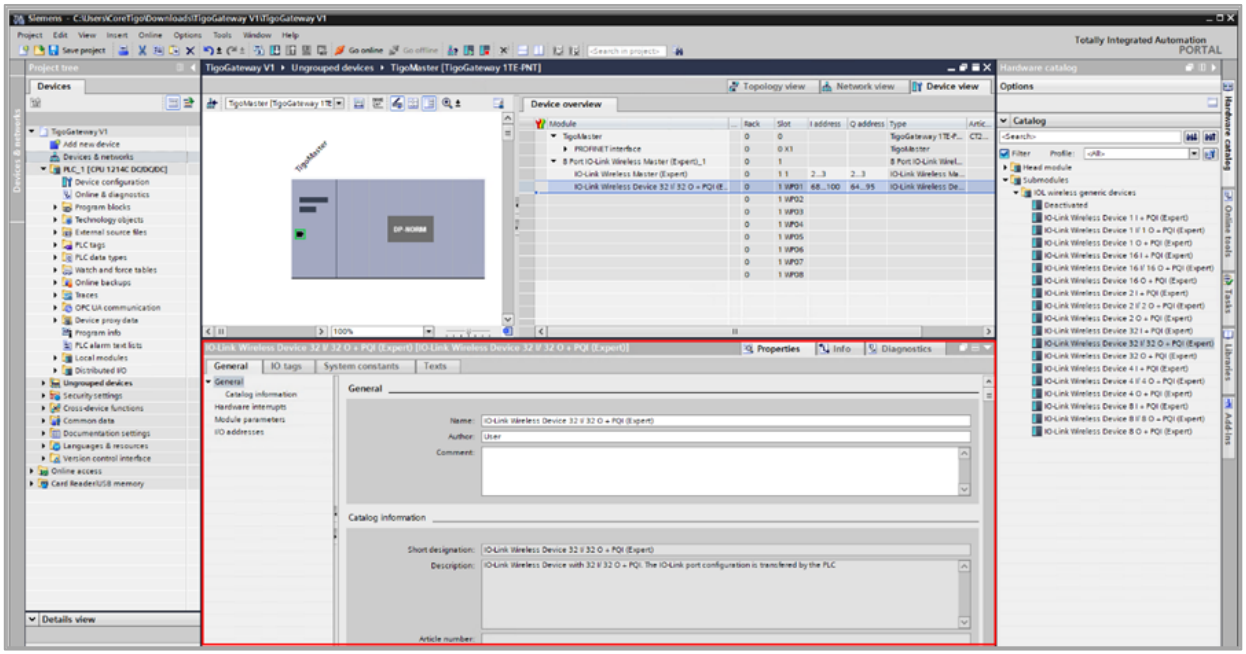


Figure 18: Device Inspector Pane

5. In the **General** tab (of the inspector pane) select **Module Parameters.**

Here you can configure the other parameters of the port whose device type you have just set (in our example, port WP01).

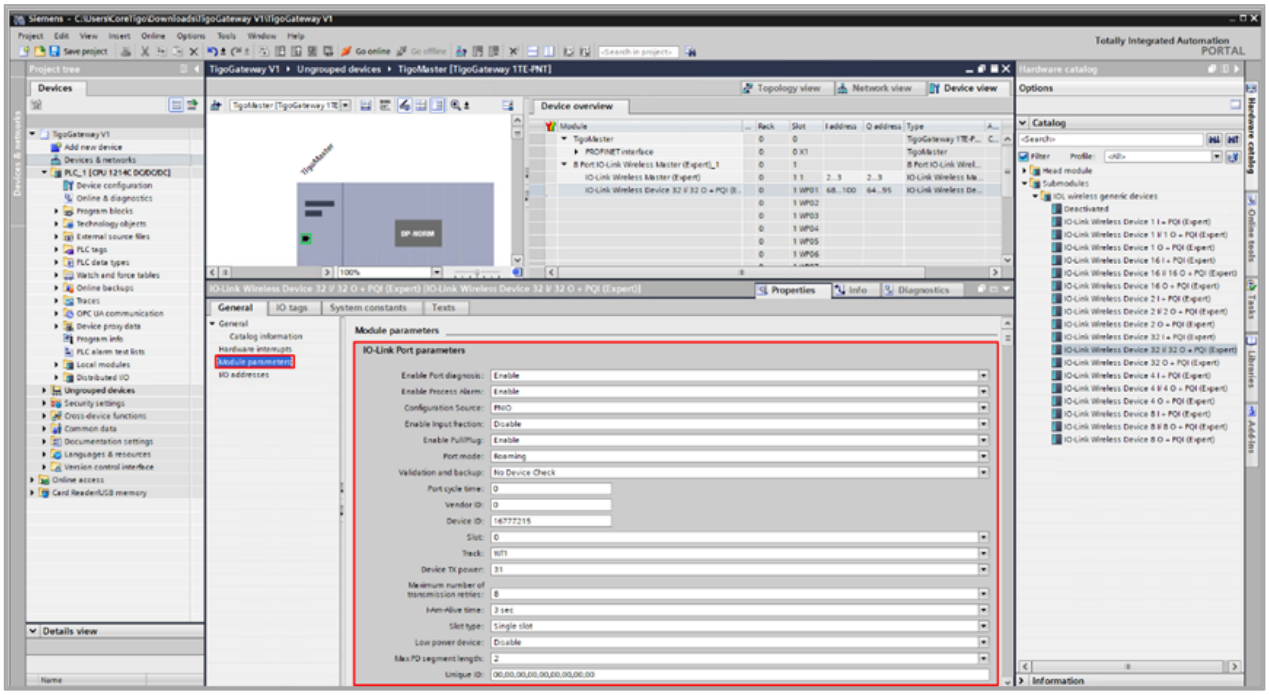


Figure 19: Module Parameters

6. In the **Unique ID** box, type the ID of the wireless-device connected to the port.

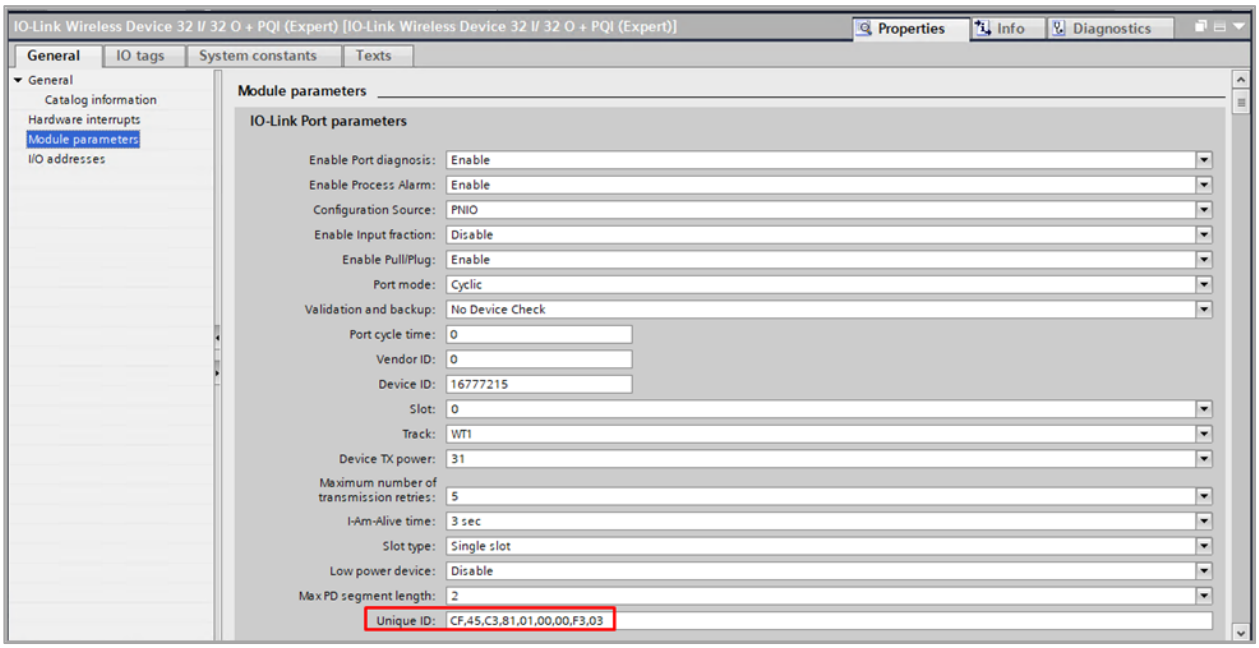


Figure 20: Unique ID

7. Change the value of any other parameters as needed by the system: for details of the various parameters and their possible values, see Parameters.
8. Compile and download in order to apply the current settings.

9. In the **Project Tree**, under the relevant PLC go to **PLC Tags** > **Show All Tags.**

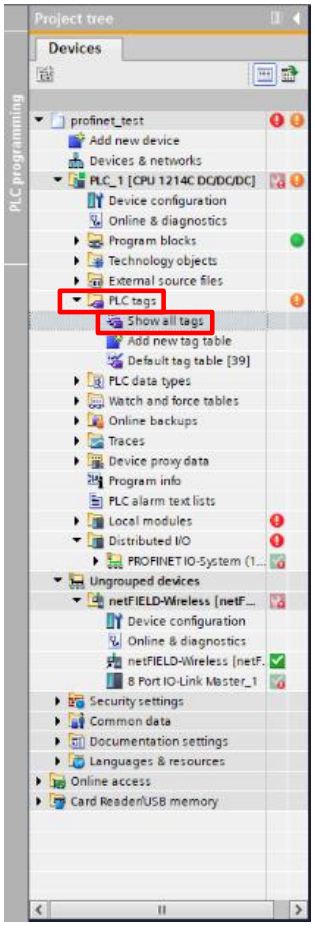


Figure 21: Show All Tags

10. In the **Tags** tab, set the W-Device tags.

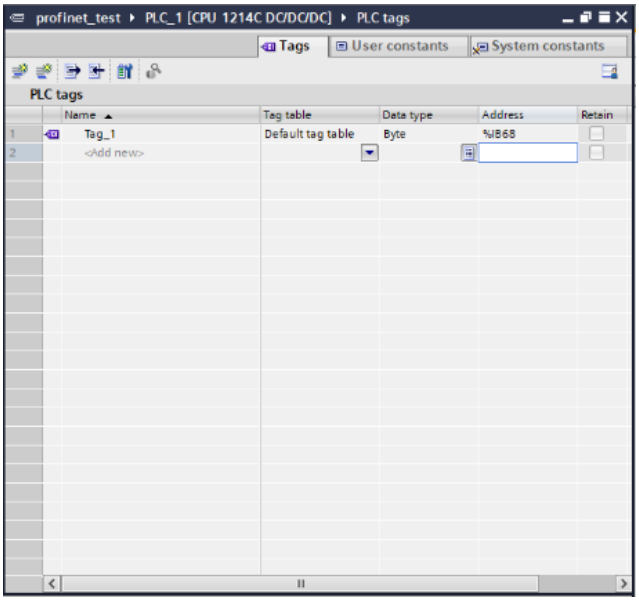


Figure 22: Tags Tab

11. In the **Project Tree**, under the relevant PLC go to **Watch and Force Tables > Watch Table_1.**

12. In **Watch Table_1**, set the watch parameters.

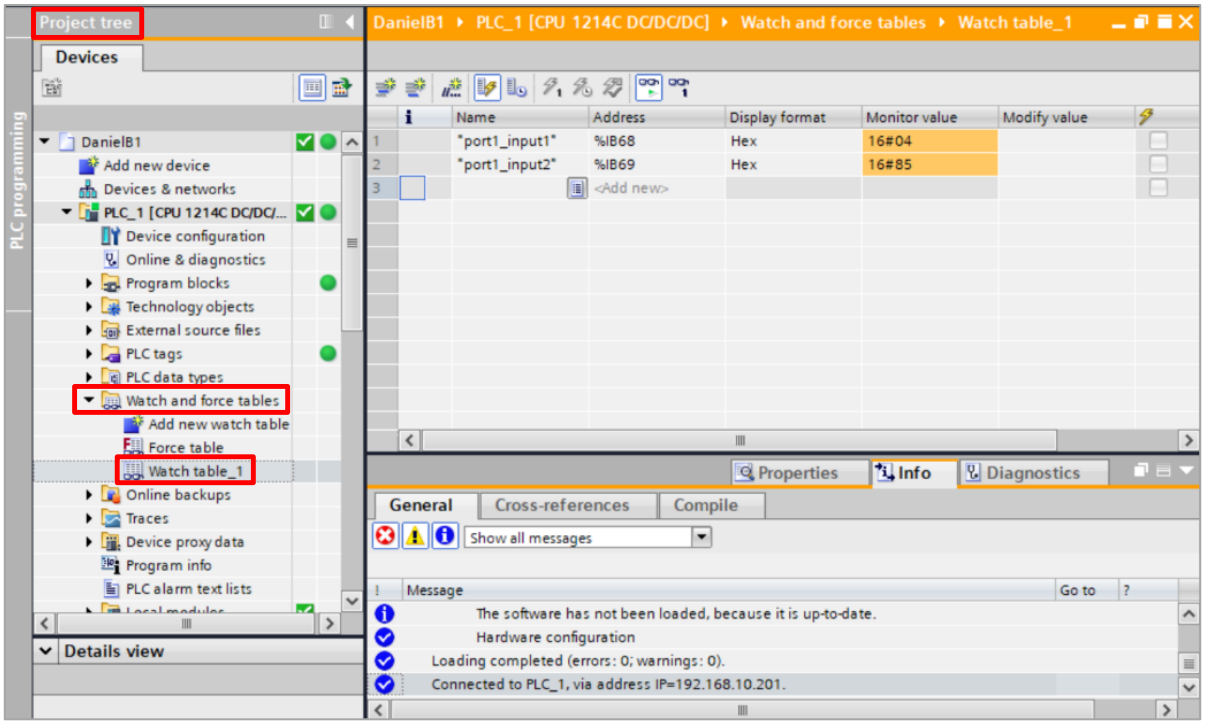


Figure 23: Watch Table

13. Use **Watch Table_1** to monitor W-Device data for the TigoBridge, and for IO-Link Wireless sensors and actuators.

5.3. TigoEngine Configuration

In order to use the TigoEngine it is necessary to have a valid user license.

Licenses are granted by CoreTigo. Some are for a limited period with an expiry date, and some are perpetual. After expiration of the license the user will only be able to access the TigoEngine if the license has been renewed by CoreTigo.

After successful installation of the TigoEngine you will be prompted to activate your account.

References:

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

TigoEngine supports multiple TigoGateway connections.

TigoEngine's **Masters** view is used for connecting a new TigoGateway to TigoEngine and keeping a record of connected TigoGateways.

Note: To activate your account online TigoEngine should have access to TCP port 443 (TigoEngine access https://licensing.coretigo.com/ems).

Proceed as follows:

1. Type in the Product Key you received from CoreTigo.
2. Click the **SUBMIT** button.

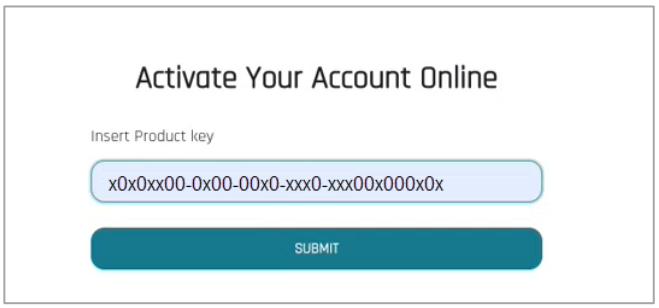


Figure 24: Insert the Product Key

You are directed to the Login screen.

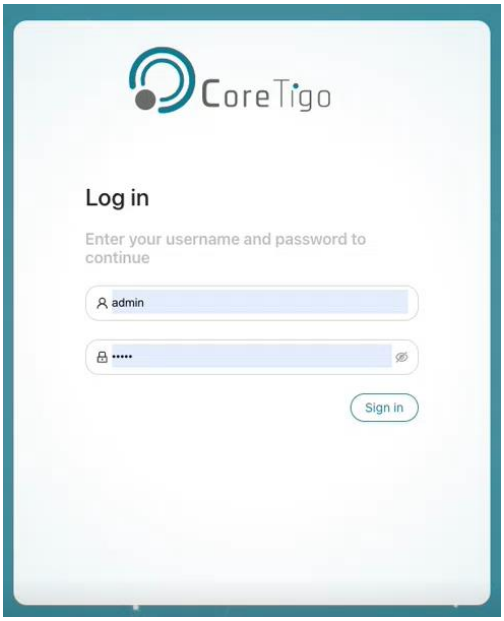


Figure 25: TigoEngine Login Screen

3. Enter your credentials and click the **Sign in** button.

There are 2 levels of access to TigoEngine:

- **Administrators** (**Admin**) have access to all features, including user management (registering new users and editing/deleting any user profile).
- **Users** can access all features except user management.

All access to TigoEngine requires user authentication, either with a TigoEngine **username** and **password** or with a Single Sign On such as Microsoft Azure.

After TigoEngine has been installed, the System Administrator logs in to TigoEngine using the default Administrator's authentication credentials, which are:

- **User** = **admin**
- **Password** = **admin**

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

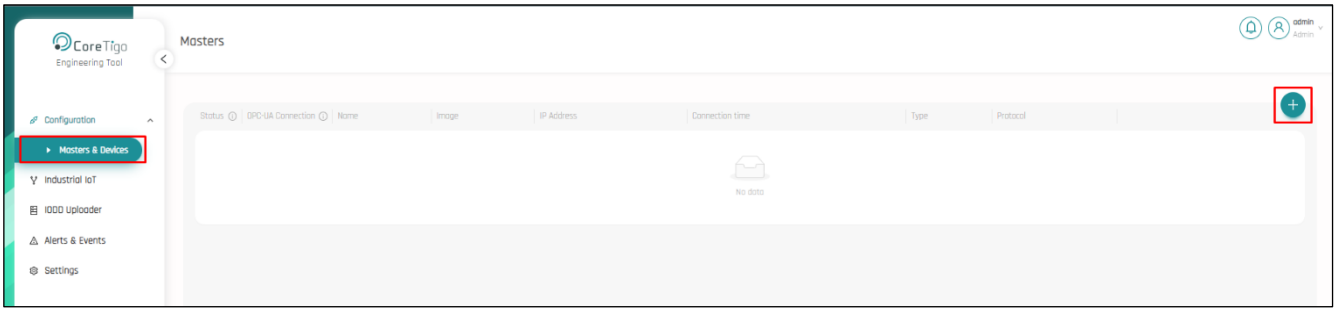


Figure 26: Connect New Master Button

5. In the **Connect New Master** window, set the following:

- **Name** – type the desired name for this TigoGateway.
- **IP** – type the IP address of the TigoGateway that you want to connect to TigoEngine.

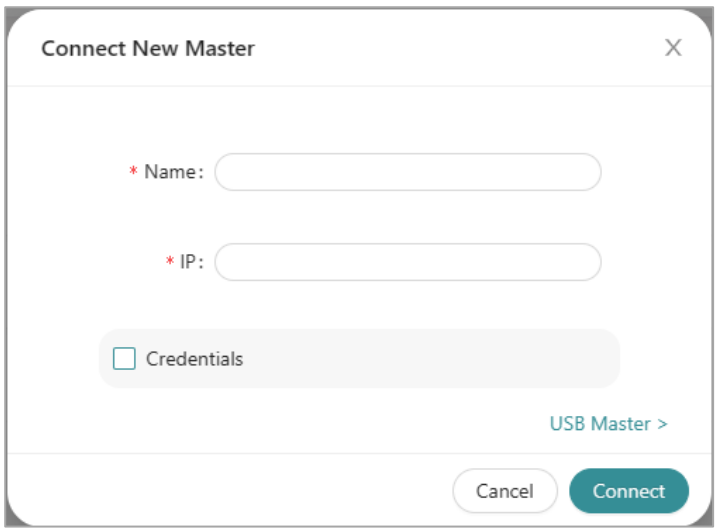


Figure 27: Connect New Master

6. Click **Connect**.

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

   Disconnect the TigoGateway or **Edit**/**Delete** its details in TigoEngine by selecting it and then clicking the relevant button in the **Actions** column.

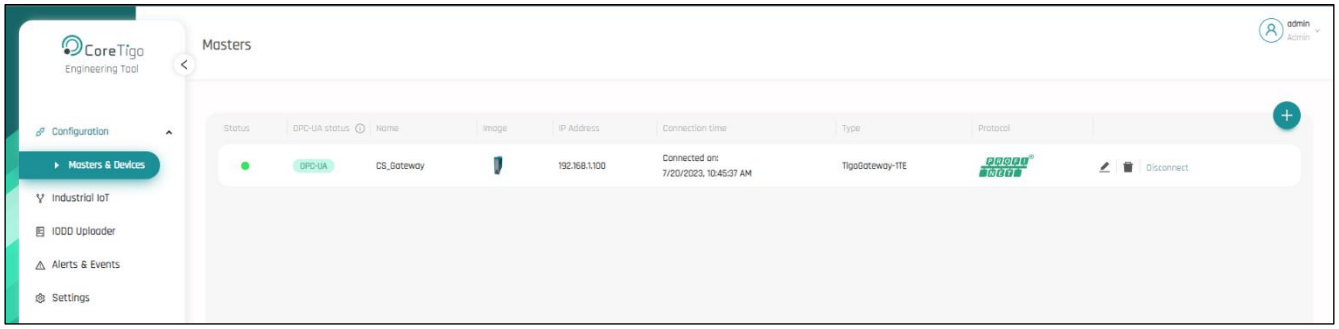


Figure 28: Masters View –TigoGateway Connected

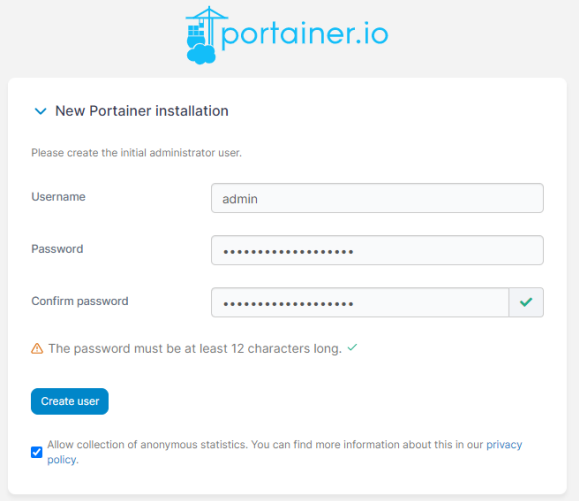
Note: The status indication (●) shows the HTTP connection to the wireless master. When it is green, the user can scan ,pair and configure the wireless ports.

The OPC UA connection indication (OPC-UA) shows the OPC UA connection to the wireless master. When it is green, data exchange (process data & MQTT) between the wireless master and TigoEngine is active.

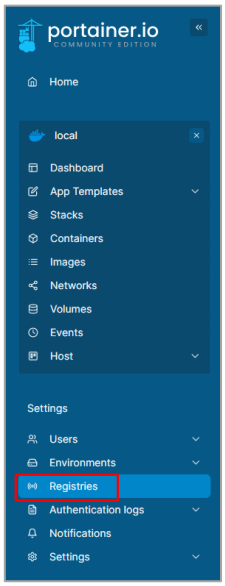
5.4. Docker Configuration

Proceed as follows:

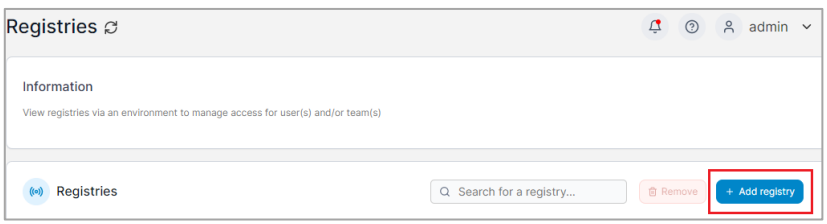
1. Select “Get Started” from the Docker section in the TigoGateway landing page.
2. If this is the first time you are logging in, then you should create a username and password.
    a. NOTE: if a username and password are not created, you will be presented after a few minutes with a message that the Portainer needs to be restarted. In this case, you should restart the TigoGateway device.



3. To create a new registry, select **Registries** in the side-panel menu.

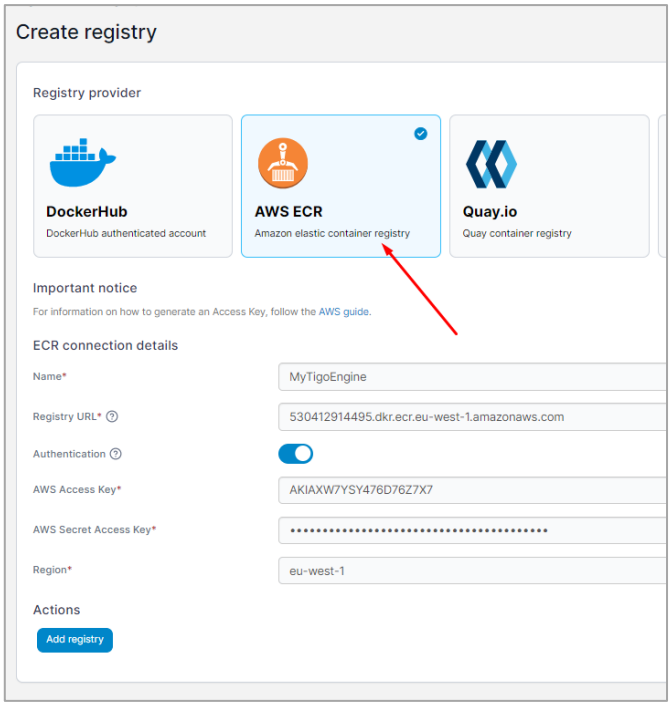


The **Registries** window opens.

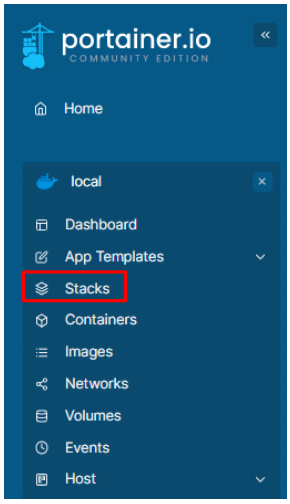


4. Click the **blue** **+Add Registry** button.

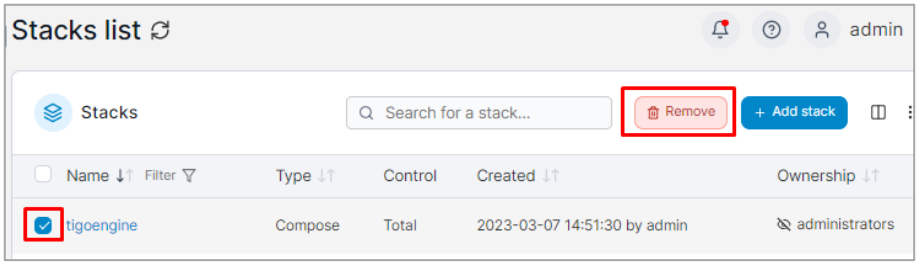
   The **Create Registry** window opens.



5. Select **AWS ECR** and enter the ECR connection details.
6. The next step is to delete an existing stack. Select **Stacks** in the side-panel menu.

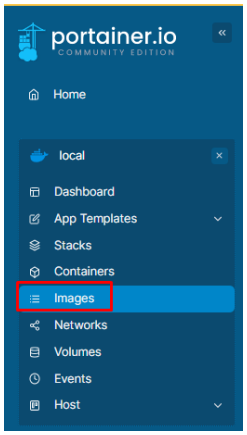


The **Stacks List** window opens.

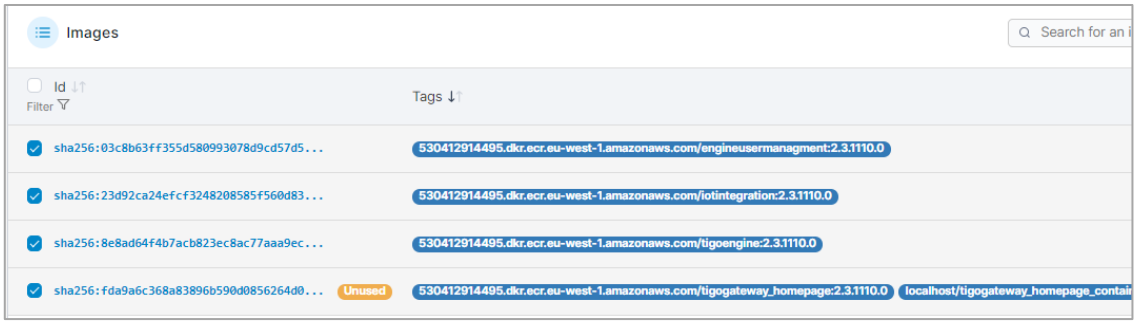


7. Select the stack or search for it.
8. Click the **red** **Remove** button.

   The stack is removed.
9. The next step is to delete existing images (virtual applications). Select the image(s) in the side-panel menu.

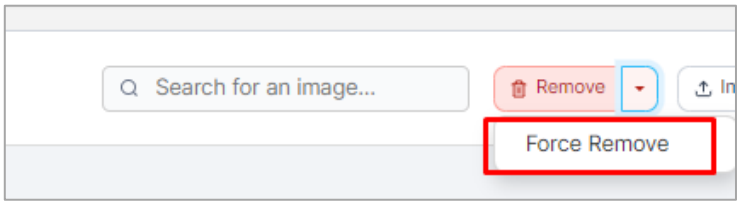


The **Images** window opens.



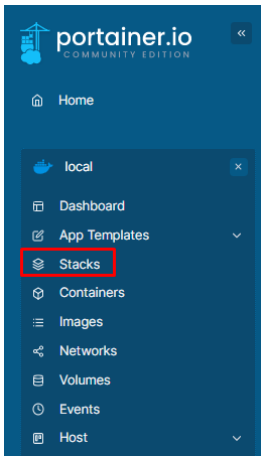
All images except the Portainer image should be selected.

10. Click **Force Remove**.

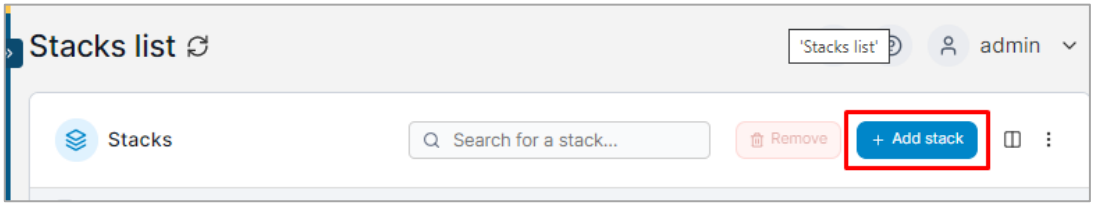


The images are removed.

11. The next step is to create a new stack. Select **Stacks** in the side-panel menu.

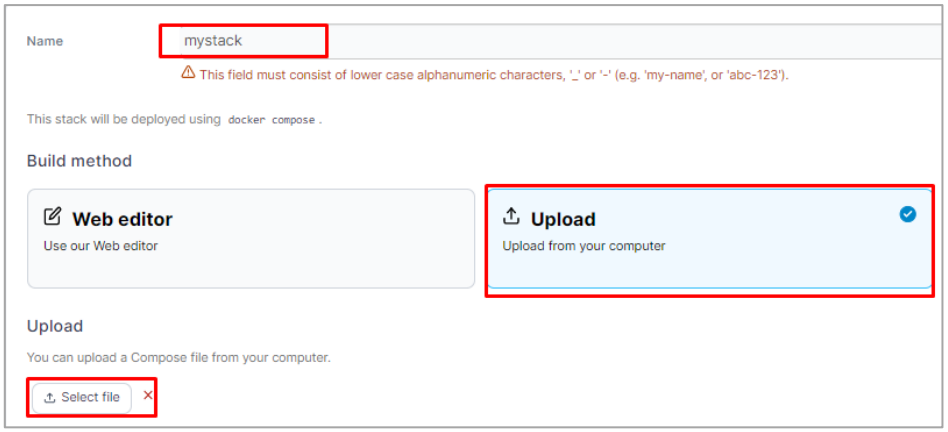


The **Stacks List** window opens.



12. Click the **blue** **+Add Stack** button.

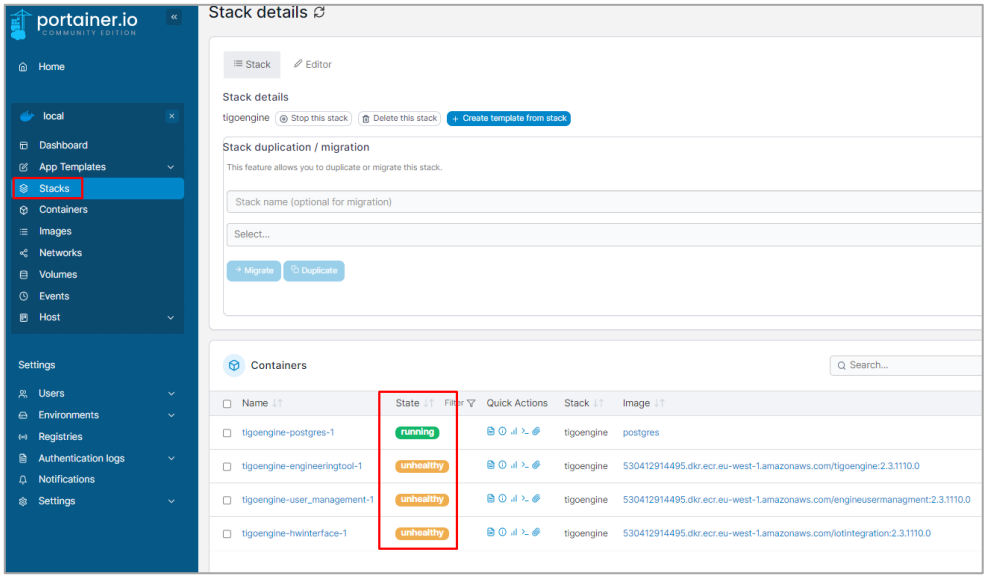
    The Stack details window opens.



13. Allocate a name to the stack.
14. Select the **Upload** option.
15. Click on **Select File** and get the updated **docker-compose.yml** file.
16. Under **Actions**, click the **blue** **Deploy the Stack** button.

    This process make take some time to complete.

17. After completion, check the **Stacks > Containers** list to verify the addition.



6. Commissioning

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

The IP Address can be set for the NetX card which connects to the industrial protocol types – PROFINET, Ethernet/IP, EtherCAT – or for the IMX8 card.

6.1. Set the IP Address with the Ethernet Device Configuration Tool

To set the IP address using the Ethernet Device Configuration tool:

1. Start the **Ethernet Device Configuration** software. (Download it from: **Ethernet Device Configuration**).
2. Check whether the checkmark for option **DCP** is set in the menu.
3. Go to **Options > Protocols**. If the checkmark for option DCP is not set, set it.
4. Click **Search devices**.

   The software lists all devices found in the local network.

   Under **IP address**, the window displays **0.0.0.0** (i.e. no IP address set) or the IP address set in the device (i.e. 192.168.1.100).

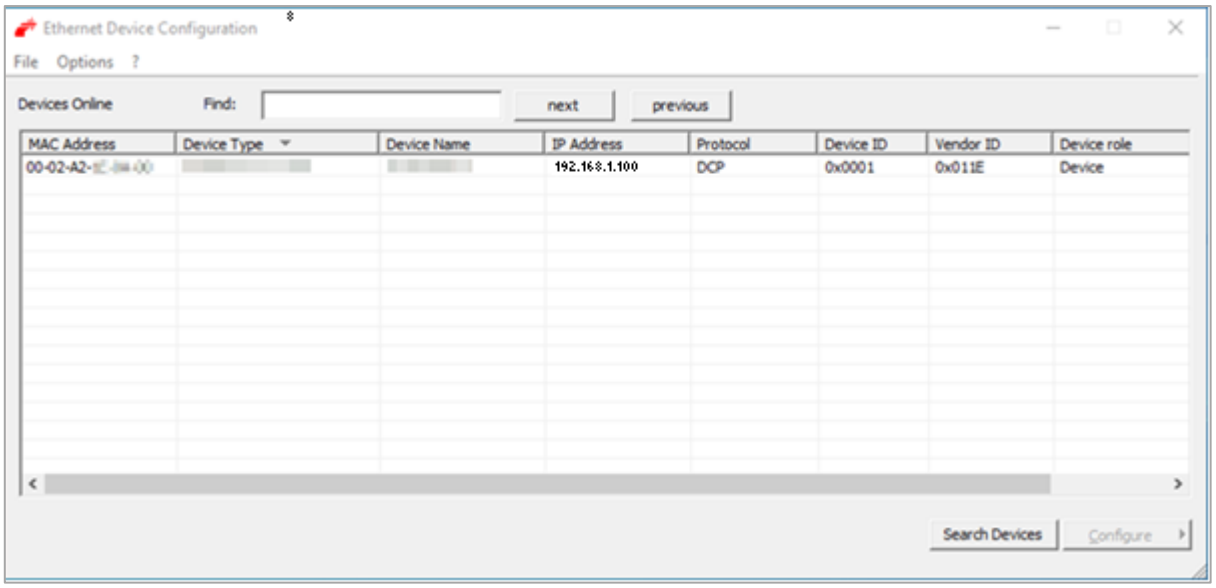


Figure 29: Ethernet Device Configuration

5. Use the MAC address or the device type, e.g. to identify the device.
6. Use the mouse pointer to select the corresponding device from the list of the devices found.
7. Click **Configure > Set IP Address**.

The dialog for setting the IP address will be displayed.

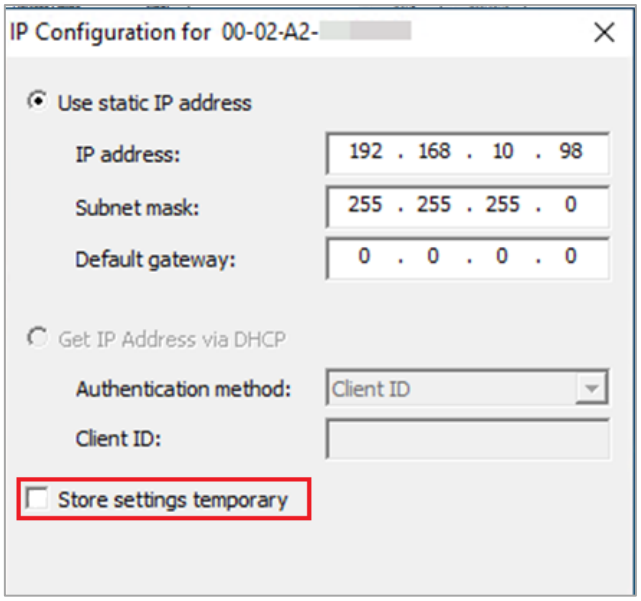


Figure 30: IP Configuration Dialog

8. Select the option **Use Static IP Address**.
9. Enter the IP address and subnet mask.

   The entry of the IP address for the standard gateway is optional.
10. Uncheck **Store settings temporary** to set it as permanent.
11. Click **OK**.

    The device is now accessible via its new IP address.

6.2. Use an OPC UA Client

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

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

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

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

6.2.1. Requirements

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

6.2.2. 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**.

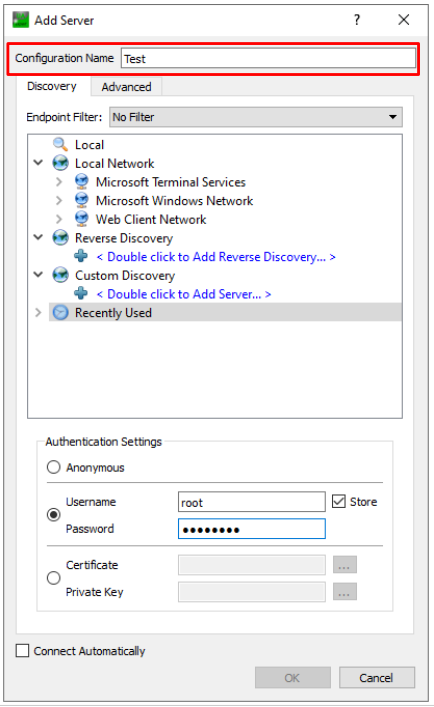


Figure 31: Add Server Dialog Box (Discovery Tab)

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

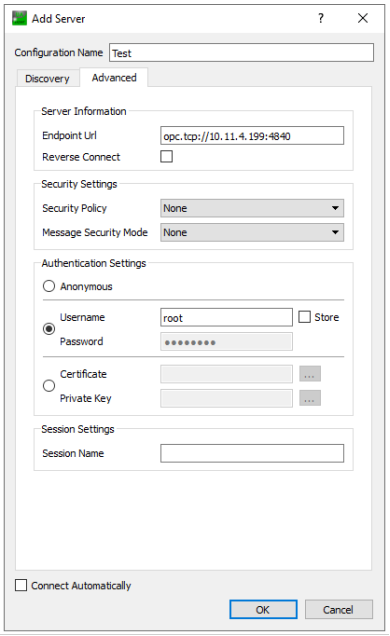


Figure 32: Add Server Dialog Box > Advanced Tab)

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

6. Click **OK**.

   In the project window, under **Project > Servers**, the UaExpert enters the server, for example, Test.

7. Open the **Context** menu of the server (Test) and select **Connect**.

   The connection starts.

6.2.3. Set the Device Date and Time Using OPC UA

6.2.3.1. Requirements

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

6.2.3.2. 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

6.2.3.3. Converting an IP Address to a Decimal Number

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

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

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

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

The decimal number in this example IP address is 3224725356.

6.2.3.4. Instructions

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

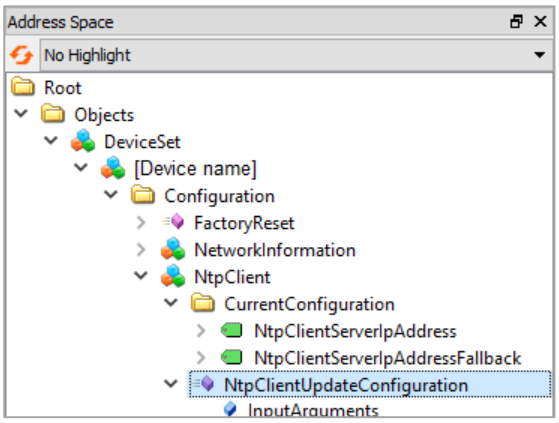


Figure 33: Path to NtpClientUpdateConfiguration

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

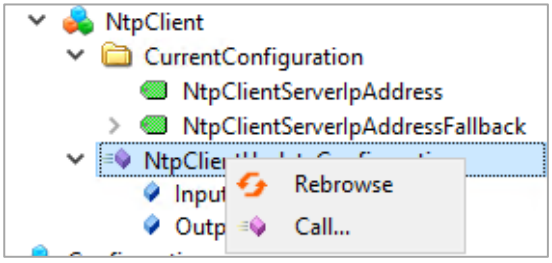


Figure 34: Right-Clicking NtpClientUpdateConfiguration

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

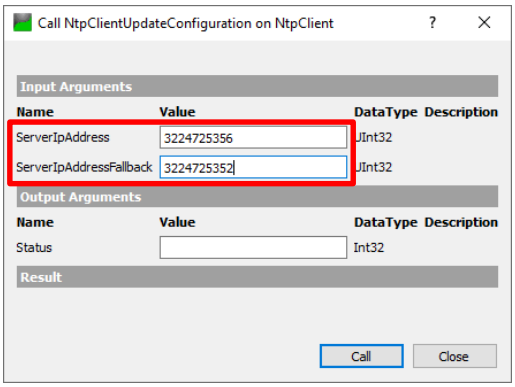


Figure 35: Call NtpClientUpdateConfiguration Dialog Box-Before Call

4. Click **Call**.

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

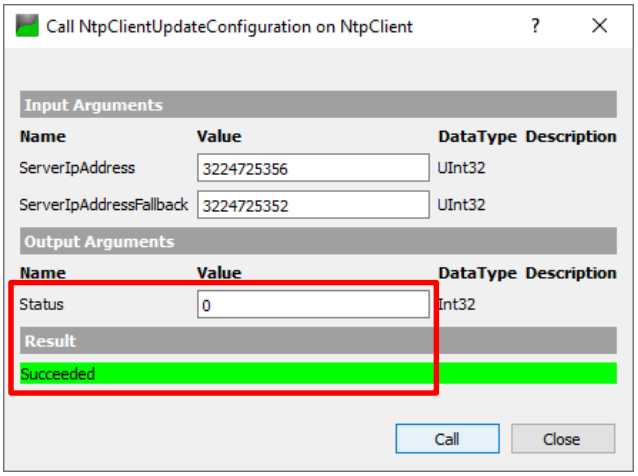


Figure 36: Call NtpClientUpdateConfiguration Dialog Box-After Call

6.2.4. OPC UA configuration for LEDs indications

The following section provides detailed instructions on how to configure OPC UA settings specifically for LED indications, focusing on QSI threshold and IOLW event timeout parameters.

6.2.4.1. QSI Threshold

1. To update QSI threshold range In the **Address Space** window go to **Root > Objects > DeviceSet > [Device name] > TigoGatewayLEDsConfig.**

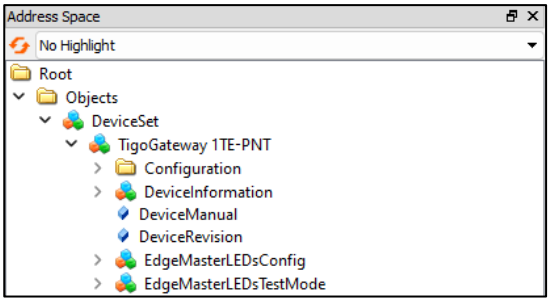


Figure 37: Path to TigoGatewayLEDsConfig

2. Modify the **value** column associated with the **QSI_TH_High/Low** to set the desired lower and upper limits.

#	Server	Node Id	Display Name	Value	Datatype
1	OPC UA Server	NS7|Numeric|1...	QSI_M	162	Byte
2	OPC UA Server	NS7|Numeric|721	QSI_TH_High	254	Byte
3	OPC UA Server	NS7|Numeric|720	QSI_TH_Low	0	Byte

Figure 38: Configuration of QSI Threshold

6.2.4.2. Event Timeout

The event timeout parameter determines the duration for which the **IOLW** LED indication remains yellow when a paired device sends an event and all ports are operational.

To configure the Event Timeout parameter:

1. Navigate to the TigoGatewayLEDsConfig (**Error! Reference source not found.**)
2. Select **Status_LED_Event_Period**

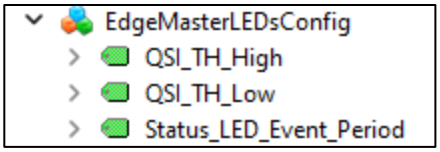


Figure 39: Status_LED_Event_Period

3. Modify the **value** column associated with the **Status_LED_Event_Period** parameter to set the desired duration. (Units are in seconds)

#	Server	Node Id	Display Name	Value	Datatype
1	OPC UA Server	NS7|Numeric|722	Status_LED_Eve...	300	UInt32

Figure 40: Configuration of Event Timeout

7. Parameters

The TigoGateway is supplied with default parameter values, many of which you can change to suit the needs of your application. Which parameter values you can change depends on which GSDML file and which configuration tool you are using.

After you have changed any parameter value, the PROFINET IO-Controller sends the new value to TigoGateway when starting communication.

Table 21: Port Parameters (When GSDML File = PDCT)

Parameter Group	Parameter	Default	Value Range	Description
Wireless IO-Link port parameters (for WT 01–WT 08)	Enable port diagnosis	1	0: Disable	PROFINET port diagnosis is deactivated: i.e. no diagnostic alarmsare triggered.
			1: Enable	PROFINET port diagnosis is activated.
	Enable process alarm (device notification)	1	0: Disable	PROFINET process alarms are deactivated.
			1: Enable	PROFINET process alarms are activated.
	Enable input fraction	0	0: Disable	Input fraction is deactivated.
			1: Enable	Input fraction is activated.
	Enable pull/plug	1	0: Disable	PROFINET pull/plug alarms are deactivated.
			1: Enable	PROFINET pull/plug alarms are activated.

Table 22: Port Parameters (When GSDML File = Expert)

Parameter Group	Parameter	Default	Value Range	Description
Wireless IO-Link port parameters (for WT 01–WT 08)	Enable port diagnosis	1	0: Disable	PROFINET port diagnosis is deactivated, i.e. no diagnostic alarms are triggered.
			1: Enable	PROFINET port diagnosis is activated.
	Enable process alarm (device notification)	1	0: Disable	PROFINET process alarms are deactivated.
			1: Enable	PROFINET process alarms are activated.
	Configuration source	1	0: PDCT	Configuration is done via a port and device configuration tool.

Parameter Group	Parameter	Default	Value Range	Description
			1: PNIO	Configuration is done via the PROFINET IO-Controller.
	Enable input fraction	0	0: Disable	Input fraction is deactivated.
			1: Enable	Input fraction is activated.
	Enable pull/plug	1	0: Disable	PROFINET pull/plug alarms are deactivated.
			1: Enable	PROFINET pull/plug alarms are activated.
	Port mode (operating mode of IO-Link port)	2	0: Deactivated	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.
	Validation and backup	No Device check	No Device Check	There is no device check for validation or backup of connected IO-Link devices (default).
			Type Compare, No Backup/Restore	A device check is performed for validation of connected IO-Link devices to the specified device type,without backup/restore.
			Type Compare, Restore Only	A device check is performed for validation or restore of connected IO-Link devices to the specified device type, without backup.
			Type Compare, Backup and Restore	A device check is performed for validation or backup/restore of connected IO-Link devices to the specified device type.
	Port cycle time	0	0 … 255	For details see Port Cycle Time.
	Vendor ID	0	0 … 65535	See ioddfinder.io-link.com or the documentation of the manufacturer of the connected IO-Link device.
	Device ID	16777215	0 … 16777215	
	Slot	0	0 … 7	Wireless slot number to be used for the port
	Track	0	0 … 2	Wireless track number to be used for the port

Parameter Group	Parameter	Default	Value Range	Description
	Device TX power	31	1 … 31	The transmit power level of the IO-Link device
Wireless IO-Link port parameters (for WT 01–WT 08)	Maximum number of transmission retries	8	2 … 31	Maximum number of retries for a transmission in OPERATE mode
	I-Am-Alive time	3 s	1.664 ms … 10 min	For details see I-Am-Alive Time
	Slot type	0	0: Single slot	Slot type is single slot
			1: Double slot	Slot type is double slot
	Low power device	0	0: Disable	The connected IO-Link device is not a low power device.
			1: Enable	The connected IO-Link device is a low power device.
	Max PD segment length	2	1 ... 32	The maximum length of the PDout data allocated to this specific wireless connection.
	Wireless Unique ID of the W-Device Byte 0	0	0 … 255	Unique ID of the IO-Link W-Device.
	Wireless Unique ID of the W-Device Byte 1	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 2	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 3	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 4	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 5	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 6	0	0 … 255	Unique ID of the IO-Link W-Device (continued).
	Wireless Unique ID of the W-Device Byte 7	0	0 … 255	
	Wireless Unique ID of the W-Device Byte 8	0	0 … 255	

Table 23: Wireless Master Parameters

Parameter Group	Parameter	Default	Value Range	Description
IO-Link Wireless Master configuration	Master ID	1	1 … 29	Master identifier
		0	0: disable	The channel cannot be used by the IO-Link Wireless Master

Parameter Group	Parameter	Default	Value Range	Description
	AHT (Adaptive Hopping Table)		1: enable	The channel can be used by the IO-Link Wireless Master
	Reconnect	0	0: enable	Reconnection attempts when connection is lost.
			1: disable	No reconnection attempts when connection is lost.
	Blacklist	255 255 240 240 240 240 240 240 240 255	-	List of frequency channels that the W-Master cannot use to communicate with W-Devices Bitwise coded 1 MHz channels 3-78 (2403 … 2478 MHz). Channels 1 (2401 MHz), 2 (2402 MHz), 79 (2479 MHz) and 80 (2480 MHz) cannot beused.
	Pairing timeout	5	5 … 60	Timeout for pairing in seconds
IO-Link Wireless Track (1–3) configuration	Track mode (operating mode of wireless track)	4	0: Stop	Track is inactive.
			1: Cyclic	Track is in cyclic-only mode and cannot perform service operations.
			2: Service	Track is in service mode. This is the same as cyclic mode except that the track can perform service operations such as scanning and pairing. Only 1 track at time can be set to Roaming or Service mode.
			3: Roaming	
			4: Auto	
	TxPower (Transmission power)	31	1 … 31	The maximum allowable value for thetransmission power is selected by theIO-Link Wireless Master.

7.1. Port Cycle Time

The Port Cycle Time parameter sets up the cycle time of a W-Port of the TigoGateway. 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 24: 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.

1 … 64	00	1 … 63	If the free-running mode is chosen with a time base of 0, the TigoGatewaystack will automatically configure the master cycle time to be the minimum master cycle time based on the PD Segmentation length, Slot Type, and Max Retry configurations.
65 … 127	01: 5ms	1 … 63	5 ... 315 ms (Time Base * Multiplier) For TigoBridge the minimum possible transmission time is 5 ms
128 … 255	10 ...11: reserved	1 … 63	Reserved. Do not use.

7.2. I-Am-Alive Time

The **I-Am-Alive Time** parameter controls TigoGateway and W-Device communication if no other messages are transmitted. The W-Device must send **I-Am-Alive** messages to the TigoGateway before timeout, otherwise the TigoGateway 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.

The table below shows the coding of the time base.

Table 25: Time Base of I-Am-Alive Time

Value	Time Base	Description
0	Reserved	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	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 26: Calculation of I-Am-Alive Time

Multiplier (Bits 8-15)	Time Base (Bits 0-7)	Calculated I-Am-Alive Time	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 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 TigoGateway 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

7.3. Unique ID Parameters: Example

If the unique ID of the TigoBridge is 03:F3:00:00:01:30:C0:45:CF, then the **Unique ID** parameters are set as follows:

- Byte 1 = CF
- Byte 2 = 45
- Byte 3 = C0
- Byte 4 = 30
- Byte 5 = 01
- Byte 6 = 00
- Byte 7 = 00
- Byte 8 = F3
- Byte 9 = 03

8. Status and Diagnostics

8.1. TigoGateway

See also LED indications.

8.2. IO-Link Diagnosis

8.2.1. Event Qualifier

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

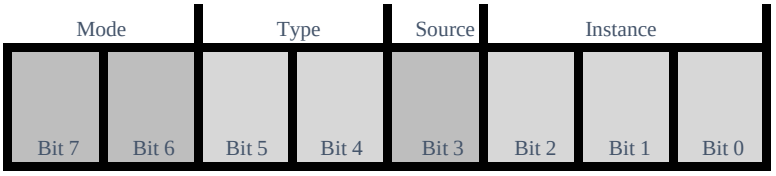


Figure 41: Event Qualifier

Table 27: 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 28: 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 theIOLW 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 29: 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
0x5000	Device hardware fault	Error	Exchange IO-Link Device
0x5010	Component malfunction	Error	Repair or exchange

Event Code	Description	Type	Remedy (Common)
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
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

Event Code	Description	Type	Remedy (Common)
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. TigoGateway 1TE Specifications

The table below describes the TigoGateway functionality.

Table 30: TigoGateway Functionality

Parameter	Specifications
Mechanical	
Dimensions	25mm X 105mm X 80mm
Mounting	DIN rail
Processors	
NXP IMX8 Arm A53	Application processor up to 1.5Ghz speed
NetX90	Industrial Ethernet Connectivity Processor
Interface	
Industrial Ethernet	PROFINET 2 x RJ45 – OT Ports (PLC or similar)
LAN RJ45	2 x RJ45 IT Ports (cloud or similar)
Electrical Data	
Input Operating Voltage	24V DC [*]
Radio	
TigoMaster SOM	1 Track (up to 8 IO-Link Wireless devices)
Frequency Range	Unlicensed 2401-2480 MHz ISM band
Communication	
IO-Link Wireless	
MQTT	
OPC UA	
Security	
TLS	
Antenna	
SMA Connector	
Certifications/ Compliance	
CE	• ETSI EN 301489-1,17 • ETSI EN 300328 • EN 62479 • EN IEC 61326-1 • EN IEC 61000-3-2 • EN IEC 61000-3-3 EN 55032, 55035
FCC	Contains 2ATSM-TGRFCM1
UL	UL 61010-1-2

Parameter	Specifications
ISED	• IC: 26463-TIGOGW • ICES-003 Issue 7 • RSS-247 Issue 2 • RSS-Gen Issue 5 • IC RF Exposure Report
Reach	Certified
RoHS	Certified
Ingress Protection	
IP 20	
Operating Environment	
Operating Temperature	0°C to +55°C
Maximum Temperature Gradient	3K per min
Storage Temperature	-40°C to 85°C
Operating Altitude	up to 2000m
Humidity	5 to 95% RH
Pollution	Degree 2

[*] The TigoGateway's products family should be supplied from a limited, Class 2, power supply or via an overcurrent protective device (fuse, breaker, etc.) rated 4A max., or less.

9.2. Protocol

Table 32: 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 PROFINET (EoE) File Access over PROFINET (FoE)
Supported state machine	ESM (PROFINET State Machine)
Supported of synchronization modes	Freerun: the application of the slave is not synchronized to PROFINET. 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

Feature	Description
Supported features	PDI watchdog PROFINET mailbox handling PROFINET state machine handling Master-to-slave SDO communication Slave-to-slave SDO communication Integrated CoE object dictionary (ODV3) Ethernet over PROFINET (EoE) handling File Access over PROFINET (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
Restrictions	PROFINET Slave stack AoE application interface not available FoE for firmware upload is supported, but application interface is not available ESC - PROFINET 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 PROFINET Master side No physical Read-Write commands supported (APRW, FPRW, BRW)
Reference to stack version	V5.1

Appendix A – 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.