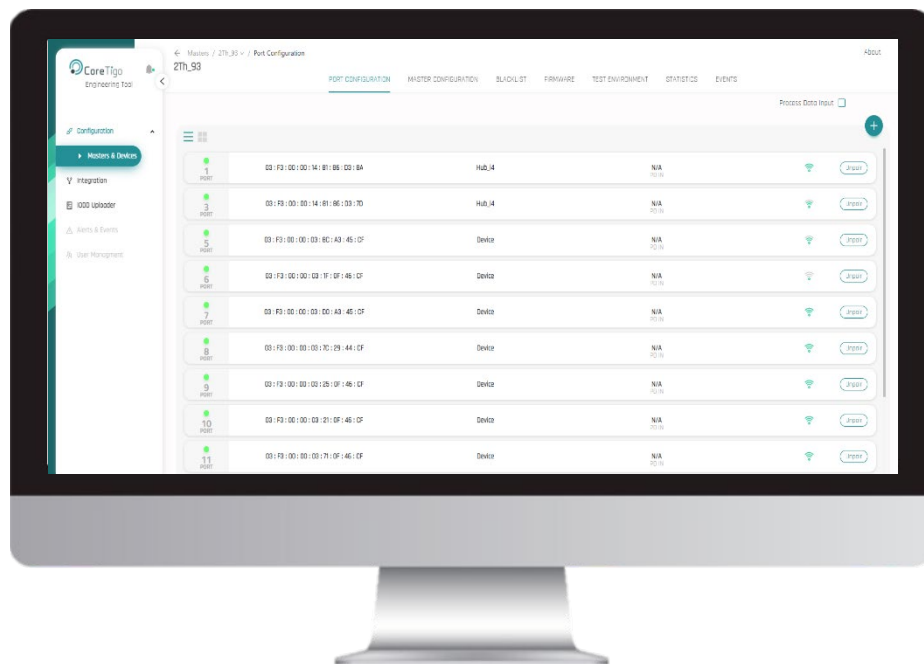




# TigoEngine

## User Manual

Revision 1.2





# Table of Contents

- 1. Introduction ..... 9**
  - 1.1. About 9
  - 1.2. Typographical Conventions 9
  - 1.3. Symbols 9
- 2. Safety ..... 10**
  - 2.1. General Safety Note 10
- 3. Overview ..... 10**
  - 3.1. TigoEngine Key Functionalities 10
- 4. System Requirements ..... 11**
- 5. Installation ..... 12**
- 6. User Management and Access to TigoEngine ..... 15**
  - 6.1. First Time Login to a New Installation 15
  - 6.2. Opening the User Management Window 15
  - 6.3. Registering a New User or Administrator 16
  - 6.4. Editing a Profile 18
  - 6.5. Setting Up Single Sign On 19
- 7. Masters View ..... 20**
  - 7.1. Connecting a New TigoMaster 2TH 20
  - 7.2. Connecting a New TigoMaster 2TS 22
  - 7.3. Actions Column 23
  - 7.4. Status Column 24
  - 7.5. Auto-Reconnect 25
- 8. Configuration Module > Masters Submodule ..... 26**
- 9. Navigation ..... 27**
  - 9.1. Opening a W-Master in a Specific View 27
  - 9.2. Navigating between W-Masters within a View 27
- 10. Master Configuration View ..... 28**
- 11. Port Configuration View ..... 30**
  - 11.1. Scanning for W-Devices 30
  - 11.2. Pairing a W-Master and W-Device 31
    - 11.2.1. Pairing from Scan Results 31
    - 11.2.2. Pairing without Scanning 32
  - 11.3. Advanced Configuration (IOLW Configuration) 33
  - 11.4. Unpairing a W-Master and W-Device 35
  - 11.5. Viewing Port Information 36
    - 11.5.1. Details Tab 37

11.5.2.	Port Configuration Tab	37
11.5.3.	Data Tab	38
11.5.4.	Device Configuration Tab	39
11.5.5.	Process Data Tab	40
11.5.6.	Events Tab	40
<b>12.</b>	<b>Blacklist View</b> .....	<b>41</b>
12.1.	Changing a Frequency to Prohibited or Permitted	41
12.2.	Changing a Channel/Bandwidth to Prohibited or Permitted	42
<b>13.</b>	<b>Firmware View</b> .....	<b>43</b>
13.1.	Upgrading W-Master Firmware	43
13.2.	Upgrading W-Device Firmware	44
<b>14.</b>	<b>Test Environment View</b> .....	<b>46</b>
14.1.	Running a Test	46
<b>15.</b>	<b>Statistics View</b> .....	<b>49</b>
15.1.	Collecting and Exporting Data	49
<b>16.</b>	<b>Events View</b> .....	<b>51</b>
<b>17.</b>	<b>Uploading IODD Files</b> .....	<b>52</b>
17.1.	Using the IODD Finder to Upload an IODD File	52
17.2.	Using the IODD Uploader	54
<b>18.</b>	<b>Integration with an MQTT Broker</b> .....	<b>56</b>
<b>19.</b>	<b>Troubleshooting</b> .....	<b>62</b>
19.1.	Troubleshooting with MQTT Explorer	62
<b>Appendix A – Working with MQTT</b> .....		<b>64</b>
Installing RabbitMQ		64
Creating MQTT Users		66
Using Command Prompt to Create an MQTT User		66
Using RabbitMQ to Create an MQTT User		66
<b>Appendix B – TigoEngine Installation using Docker</b> .....		<b>68</b>
Example:		68
AWS configure		68
<b>Appendix C – Setting IP Address with the BOOTP/DHCP Tool</b> .....		<b>70</b>
<b>Appendix D – Evaluation Agreement</b> .....		<b>72</b>
Warranty Disclaimer		73
Limitation of Liability		74
Term and Termination		75

## Table of Figures

Figure 1 – Welcome (Setup Wizard)	12
Figure 2 – End-User License Agreement (Setup Wizard)	12
Figure 3 – Select Installation Folder (Setup Wizard)	13
Figure 4 – Ready to Install (Setup Wizard)	13
Figure 5 – Completing (Setup Wizard)	14
Figure 6 – Opening the User Management Window	15
Figure 7 – Editing a User/Administrator Profile: Example	18
Figure 8 – Editing a User/Administrator Profile (continued)	18
Figure 9 – Setting Up Single Sign On	19
Figure 10 – Log In Window with Example Single Sign On Button	19
Figure 11 – Detailing the TigoMaster 2TH to Be Connected	20
Figure 12 – Detailing Non-Default Credentials	21
Figure 13: Masters View – Two TigoMaster 2TH Connected	21
Figure 14: Connecting a TigoMaster 2TS	22
Figure 15: New TigoMaster 2TS Listed in Masters View – Status Is Unconnected	22
Figure 16: Opening the Select Serial Port Window	22
Figure 17: Select Serial Port Window	23
Figure 18: Actions Column	23
Figure 19: Status Column	24
Figure 20: Configuration > Masters Submodule – Default View	26
Figure 21: Opening a W-Master in a Specific View – Example	27
Figure 22: Navigating to another W-Master within the Current View	27
Figure 23: Resetting the W-Master's Software	28
Figure 24: Master Configuration View (Advanced Parameters)	28
Figure 25: Track Configuration Parameters	29
Figure 26: Vendor Specific Read/Write Parameters	29
Figure 27: Port Configuration View	30
Figure 28: Scan Button	30
Figure 29: List of Available W-Devices in Range of Selected W-Master	31
Figure 30: Scan Results	31
Figure 31: Pair Button	32
Figure 32: Paired W-Device in Port Configuration View	32
Figure 33: Port Configuration Bar	32
Figure 34: IOLW Configuration Window	33
Figure 35: Unpair Button	35
Figure 36: Port Configuration View Tabs	36
Figure 37: Details Tab	37
Figure 38: Port Configuration View Tabs	37
Figure 39: Write ISDU	38
Figure 40: Read ISDU	39
Figure 41: Device Configuration Tab	39
Figure 42: Process Data Tab	40
Figure 43: Toggling a Frequency between Prohibited and Permitted – Example	41
Figure 44: Changing a Channel/Bandwidth to Prohibited or Permitted	42
Figure 45: Upload FW Version	43
Figure 46: Version	43
Figure 47: Start Upgrade	43
Figure 48: Port Checkbox	44
Figure 49: Upload FW Version	44
Figure 50: Version	45
Figure 51: Start Upgrade	45

Figure 52: Test Environment View	46
Figure 53: Test Mode Button in Off Position	46
Figure 54: Test Mode Button in On Position	46
Figure 55: Warning Dialog Box	46
Figure 56: Select Test Menu	46
Figure 57: Manual Stop Switch	47
Figure 58: Number of Cycles	47
Figure 59: Port Checkboxes	47
Figure 60: Start Test	47
Figure 61: Finished Test	48
Figure 62: Clear View	48
Figure 63: Port Selection	49
Figure 64: Collect	49
Figure 65: Results – Example	50
Figure 66: Export	50
Figure 67: Events View	51
Figure 68: IODD Finder	52
Figure 69: IODD Finder Results (IO-Link sensor/actuator data) – Example	53
Figure 70: GET DATA	53
Figure 71: IO-Link Device Description (IODD) – Example	54
Figure 72: IODD Uploader – Upload Area	54
Figure 73: Browsing to the IODD File and Uploading It	54
Figure 74: Uploaded Device Description (IODD)	55
Figure 75: Configuration Screen (Integration Wizard)	56
Figure 76: Connection Details Screen (Integration Wizard)	57
Figure 77: Data Screen (Integration Wizard)	58
Figure 78: Test Connection Screen (Integration Wizard)	59
Figure 79: Assign Devices Screen (Integration Wizard) – Integrate Devices Button	59
Figure 80: Select Devices to Integrate	60
Figure 81: Integrated Devices	61
Figure 82: MQTT Explorer – Connection Settings	62
Figure 83: Broken Topic List	63
Figure 84: Expanded Topic	63
Figure 85: Directory of c:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.17\sbin	64
Figure 86: Command Prompt: rabbitmq-plugins.bat enable rabbitmq_management	64
Figure 87: Message started 1 plugins Received	65
Figure 88: rabbitmq-plugins list Featuring rabbitmq_mqtt	65
Figure 89: Admin Tab	66
Figure 90: Adding a User	67

## Table of Tables

Table 1: Statuses	24
Table 2: Master Configuration Parameters (Advanced Parameters)	28
Table 3: Track Configuration Parameters	29
Table 4: Vendor Specific Read/Write Parameters	29
Table 5: IOLW Configuration Parameters	33

## Approval Table

Role	Name	Version	Date
Written By	Ortal Gvura-Angel	1.0	08/01/2021
Reviewed By	Daniel Brauch	1.0	
Approved By	Daniel Brauch	1.0	

## Revision Control

Author Name	Description	Revision	Date
Ortal Gvura-Angel	Creation	1.1	January 2021
Robert Collins	Rewriting, formatting, and updating	1.1	October 2021– June 2022
Robert Collins, Ofir Levi, Shoval Ben Shanan	User management added, updating Master View chapter	1.2	August 2022

## Acronyms and Abbreviations

Term	Meaning
FOTA	Firmware over the Air
IMA	I Am Alive (parameter)
IO	Input Output
IODD	IO Device Description
IOLW	In Out Link Wireless
ISDU	Indexed Service Data Unit
LQI	Link Quality Indication
MQTT	A message transportation protocol (the initials no longer stand for anything in the current version of the protocol)
PDIn	Process Data In
PDout	Process Data Out
PER	Packet Error Rate
RSSI	Received Signal Strength Indication
SW	Software
UID	Unique Identification
W-Device	Wireless Device
W-Master	Wireless Master





# 1. Introduction




## 1.1. About

This document relates to use of the TigoEngine management platform.

## 1.2. Typographical Conventions

- Enumerations are shown in a list form with bullet points.
- Instructional steps are shown in a numbered list form.
- Decimal numbers are shown without additional indicators and are not spelled out (e.g., 123).

## 1.3. Symbols

Symbol	Meaning
	<b>Note:</b> This symbol indicates a general note.
	<b>Warning:</b> This symbol indicates a security notice that must be observed.
	<b>Reference:</b> This symbol indicates a reference to other documentation (available on request).

## 2. Safety

### 2.1. General Safety Note

The users of this manual must be qualified for the installation, configuration, and monitoring of an IO-Link Wireless system using TigoEngine. All safety messages, integrated safety messages, property damage messages, and valid legal regulations must be observed by users.



CoreTigo Ltd assumes that users have the required technical capabilities.

---

## 3. Overview

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

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

### 3.1. 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 IO-Link Device Data (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
- 3rd party software integration via an MQTT publisher—exporting process data from TigoEngine to 3rd party software (requires an MQTT broker on the 3<sup>rd</sup> 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. System Requirements

- Operating system: Microsoft Windows (Installer) or Linux (with Docker)
- Database: PostgreSQL (included by default as part of the TigoEngine Windows Installer)
- CPU and memory: depend on the number of devices and transactions in the system. Consult your **CoreTigo** representative for recommendations.

## 5. Installation

1. TigoEngine can be downloaded from CoreTigo Customer Portal at [support.coretigo.com](http://support.coretigo.com) (Registration required).
2. Double-click the **TigoEngine.exe** file.
3. In the **Setup Wizard**, do the following:
  - a. In the **Welcome** page, click **Next**.

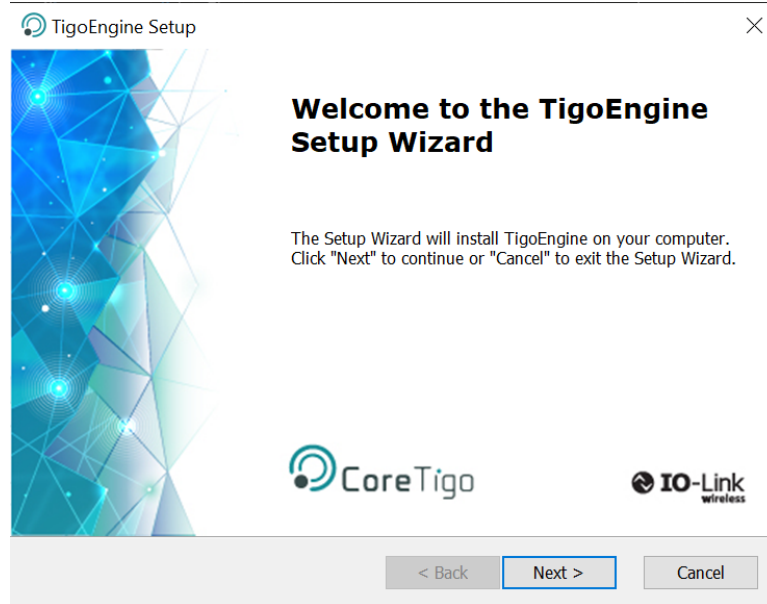


Figure 1 – Welcome (Setup Wizard)

- b. In the **End-User License Agreement** page, select **I accept the terms in the License Agreement**, and click **Next**.

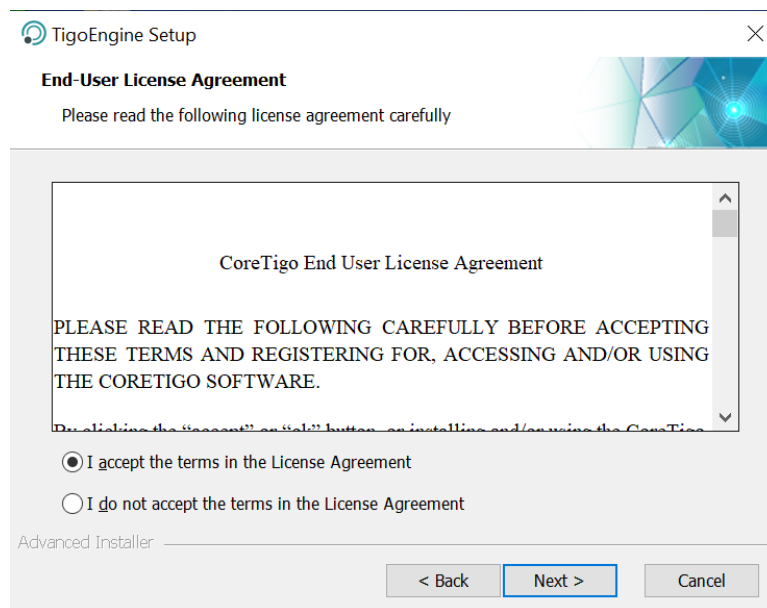
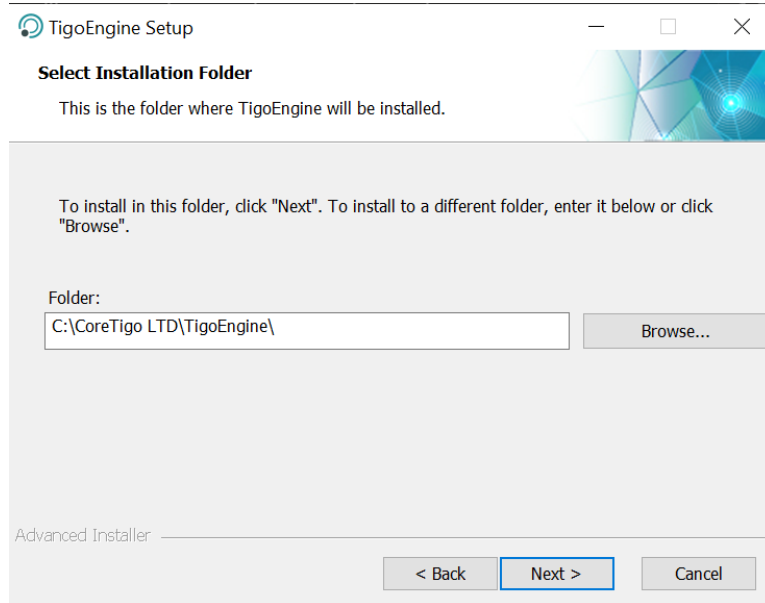


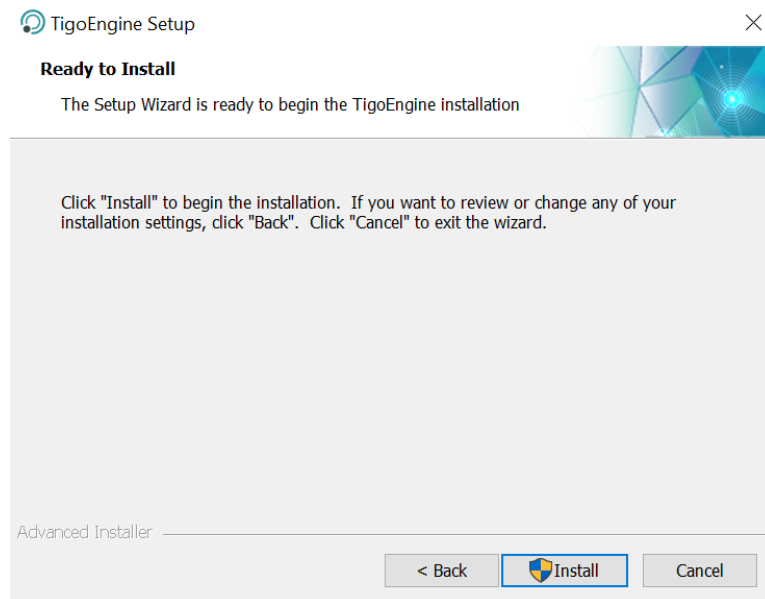
Figure 2 – End-User License Agreement (Setup Wizard)

- c. In the **Select Installation Folder** page, do one of the following;
- To install in the default folder, click **Next**.
  - To install in a folder other than the default, click **Browse** and select the desired folder.



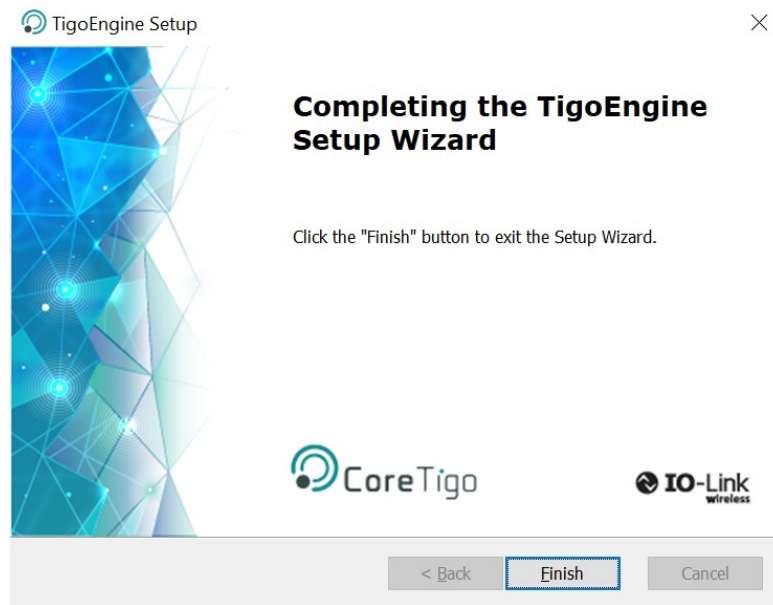
**Figure 3 –Select Installation Folder (Setup Wizard)**

- d. In the **Ready to Install** page, click **Install**.



**Figure 4 – Ready to Install (Setup Wizard)**

e. In the **Completing** page, click **Finish**.



**Figure 5 – Completing (Setup Wizard)**

## 6. User Management and Access to TigoEngine

There are 2 levels of access to TigoEngine:

- Administrators (**Admin**) have access to all features, including user management (that is, registering new users and editing/deleting any user's 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 (see section [6.5 Setting Up Single Sign On](#)).

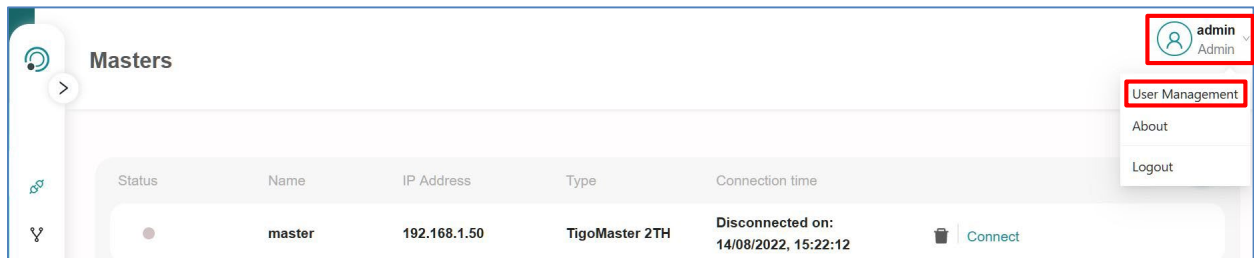
### 6.1. First Time Login to a New Installation

After TigoEngine has been installed, the system administrator needs to login to TigoEngine using the default administrator's authentication credentials, which are:

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

### 6.2. Opening the User Management Window

1. Make sure you are logged in as an administrator.
2. Click the name/icon of the logged-in profile:

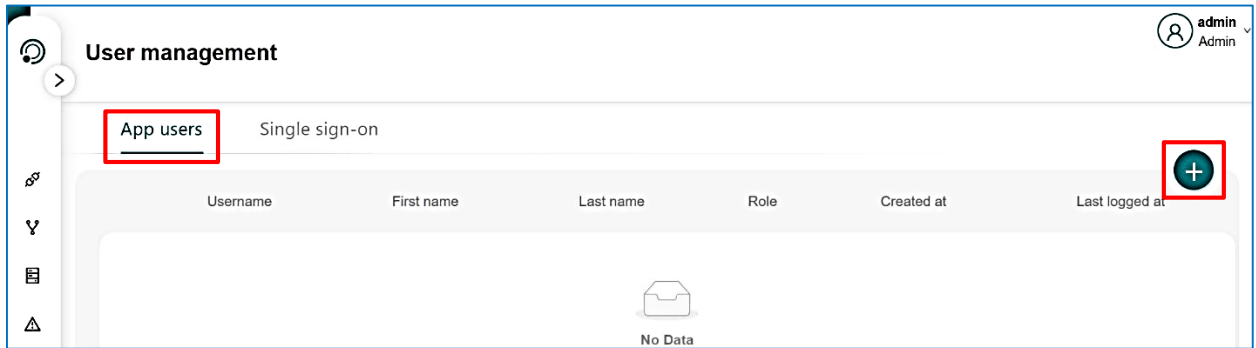


**Figure 6 – Opening the User Management Window**

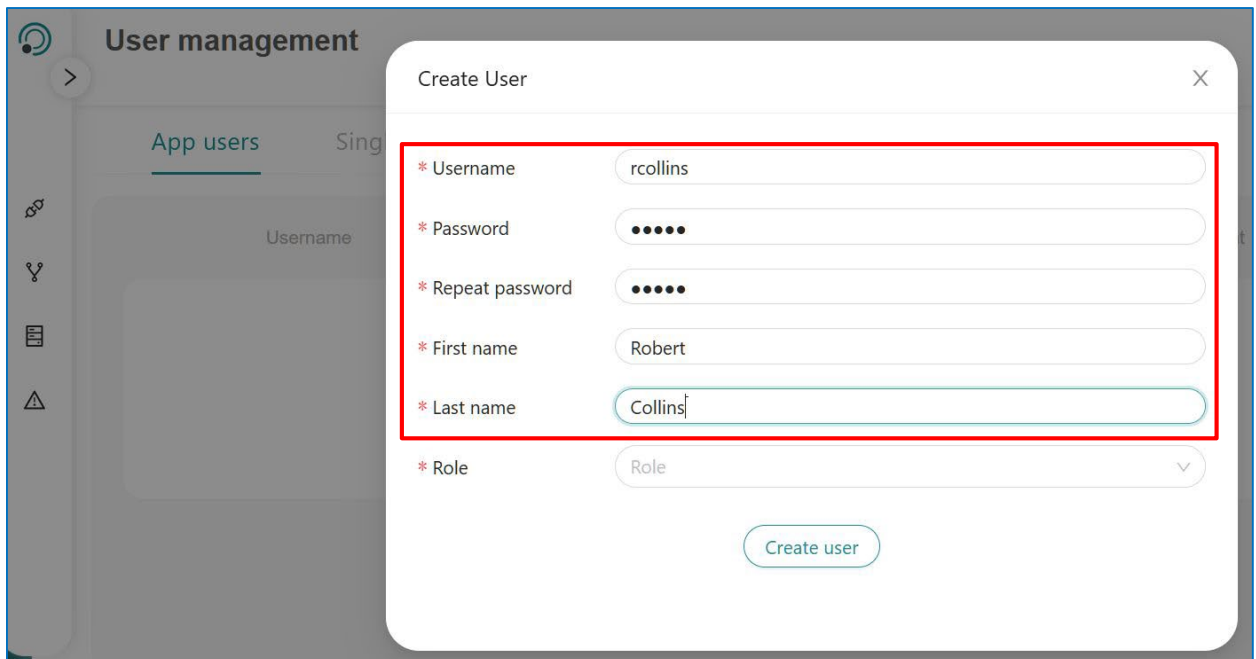
3. In the menu that opens, click **User Management** (see Figure 6).  
The **User Management** window opens.

### 6.3. Registering a New User or Administrator

1. In the **User Management** window > **App users** tab, click to  open the **Create User** window.



2. In the **Create User** window, type the **Username**, **Password**, **First name**, and **Last name** as appropriate.





3. In the **Role** field, set the desired level of access (**User** or **Admin**) for the profile.

The screenshot shows the 'Create User' form in the 'User management' interface. The form fields are: Username (rcollins), Password (masked with dots), Repeat password (masked with dots), First name (Robert), Last name (Collins), and Role (dropdown menu). The Role dropdown is open, showing 'User' and 'Admin' options. A red box highlights the Role field and its dropdown menu.

4. Click **Create user**.

The screenshot shows the 'Create User' form in the 'User management' interface. The form fields are: Username (rcollins), Password (masked with dots), Repeat password (masked with dots), First name (Robert), Last name (Collins), and Role (dropdown menu). The Role dropdown is closed, showing 'User'. A red box highlights the 'Create user' button.

## 6.4. Editing a Profile

1. In the **User Management** window > **App users** tab, click  next to the user/administrator profile that you want to edit.

In the example in Figure 7, the profile of Robert Collins is to be edited.

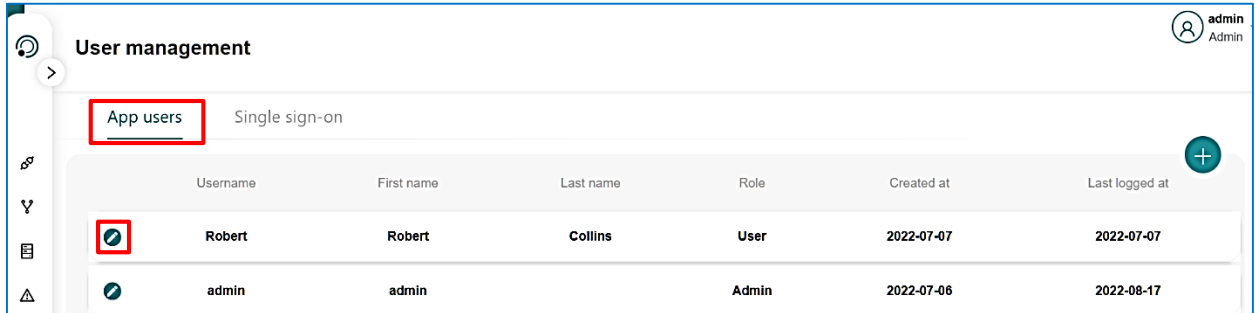


Figure 7 – Editing a User/Administrator Profile: Example

2. In the fields that appear, change the profile as desired and then click **Save Changes**.

Note that if TigoEngine currently has only one registered administrator (that is, only one profile where **Role = Admin**), you cannot change that profile's **Role** to **User**. There must always be at least one administrator.

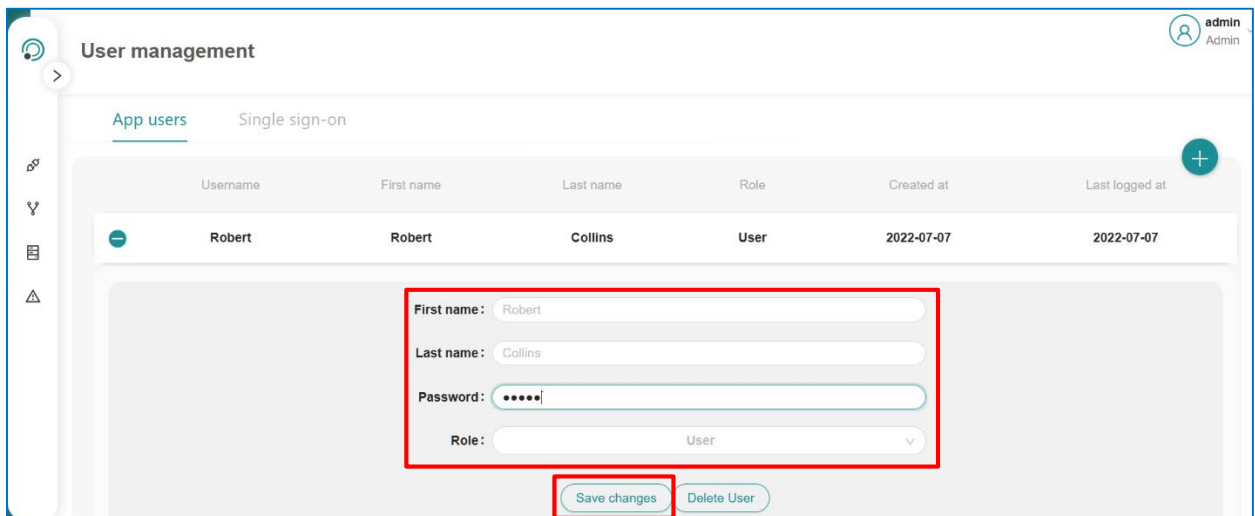
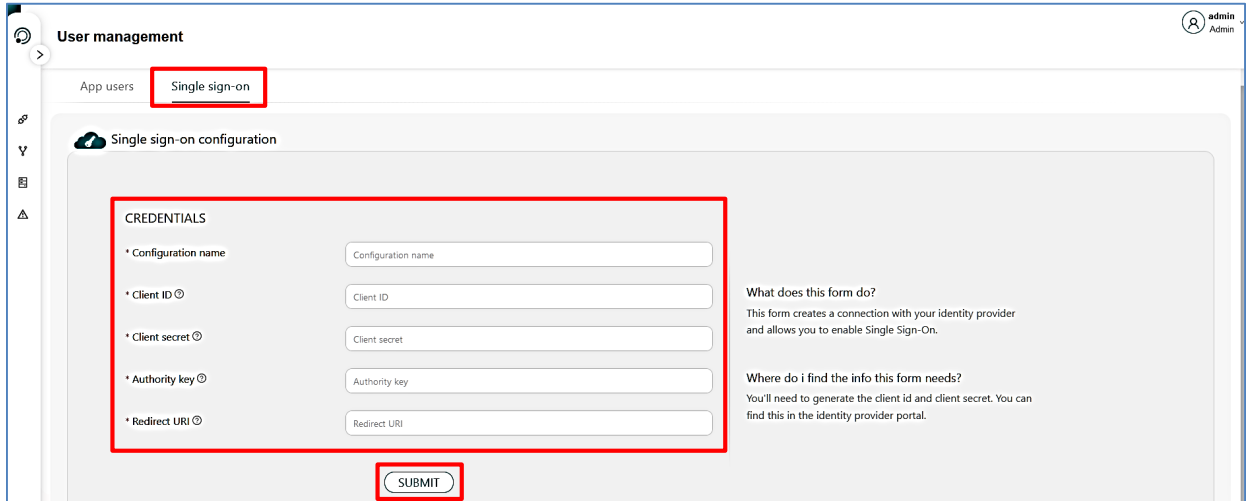


Figure 8 – Editing a User/Administrator Profile (continued)

## 6.5. Setting Up Single Sign On

1. In the **User Management** window > **SSO Config** tab, type the credentials of the active directory account to be used for single sign on (for example, Microsoft Azure).
2. Click **Submit**.



The screenshot shows the 'User management' interface with the 'Single sign-on' tab selected. The 'Single sign-on configuration' section contains a 'CREDENTIALS' form with the following fields:

- \* Configuration name: Configuration name
- \* Client ID: Client ID
- \* Client secret: Client secret
- \* Authority key: Authority key
- \* Redirect URI: Redirect URI

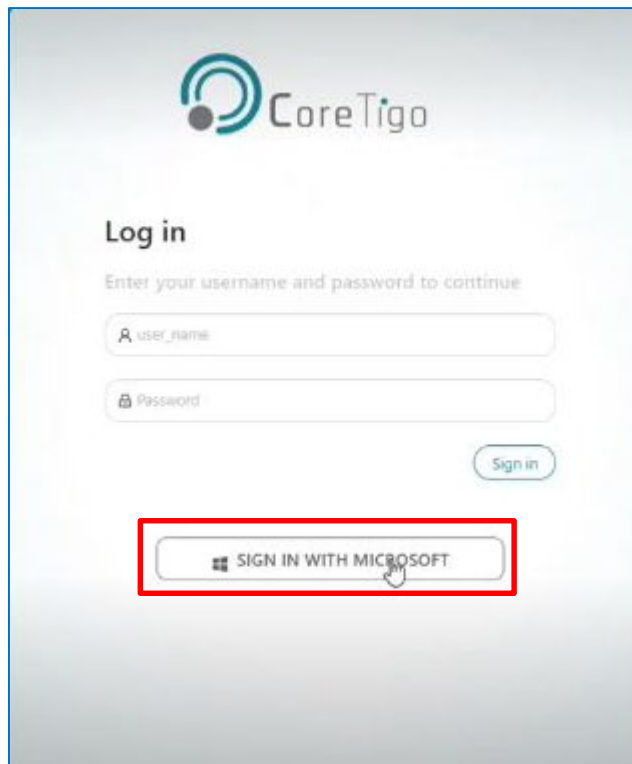
Below the form is a 'SUBMIT' button. To the right of the form, there is explanatory text:

**What does this form do?**  
This form creates a connection with your identity provider and allows you to enable Single Sign-On.

**Where do i find the info this form needs?**  
You'll need to generate the client id and client secret. You can find this in the identity provider portal.

Figure 9 – Setting Up Single Sign On

The **Log In** window now includes a single sign on button: for example, **SIGN IN WITH MICROSOFT**.



The screenshot shows the 'CoreTigo' login page. It features a 'Log in' section with the instruction 'Enter your username and password to continue'. There are two input fields: 'user\_name' and 'Password'. A 'Sign in' button is located to the right of the password field. Below these fields is a button labeled 'SIGN IN WITH MICROSOFT', which is highlighted with a red box in the image.

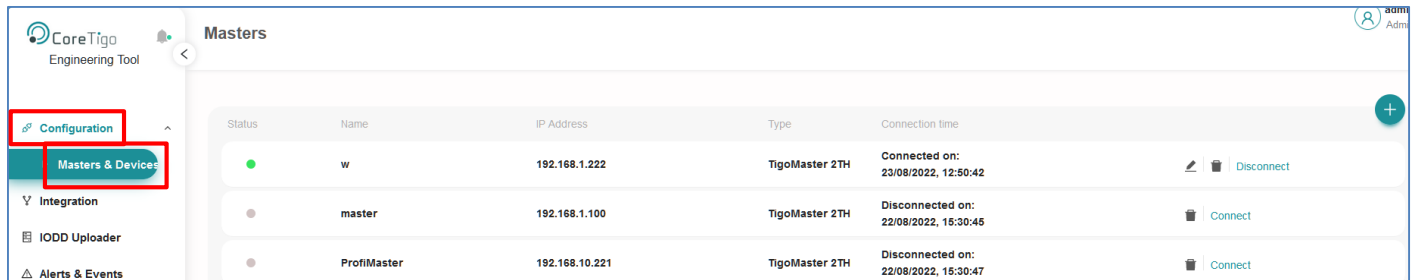
Figure 10 – Log In Window with Example Single Sign On Button

## 7. Masters View

In **Masters** view you can:

- See a list of all wireless masters connected to TigoEngine, together with basic information about them (such as IP address and connection time)
- Select a wireless master from the list and see further information about it (for example, its Port Configuration) in another view, and/or configure it in another view
- Connect a new w-master to TigoEngine: see section 7.1.

To open **Masters** view, go to **Configuration > Masters & Devices**.



### 7.1. Connecting a New TigoMaster 2TH

1. Make sure that you know the TigoMaster 2TH's IP address.

If the IP address has not yet been configured, you can configure it using, for example, one of the tools detailed in the TigoMaster 2TH User-Manual.

2. If the TigoMaster 2TH's credentials (User Name and Password) have been changed from the default using the WebServer, make sure you know the current credentials.
3. In TigoEngine's **Masters** view, click .
4. In the **Connect New Master** window, do the following:
  - a. Type the desired **Name** for the TigoMaster 2TH being connected.
  - b. Set **Master Type = TigoMaster 2TH**
  - c. Type the **IP** address of the TigoMaster 2TH.

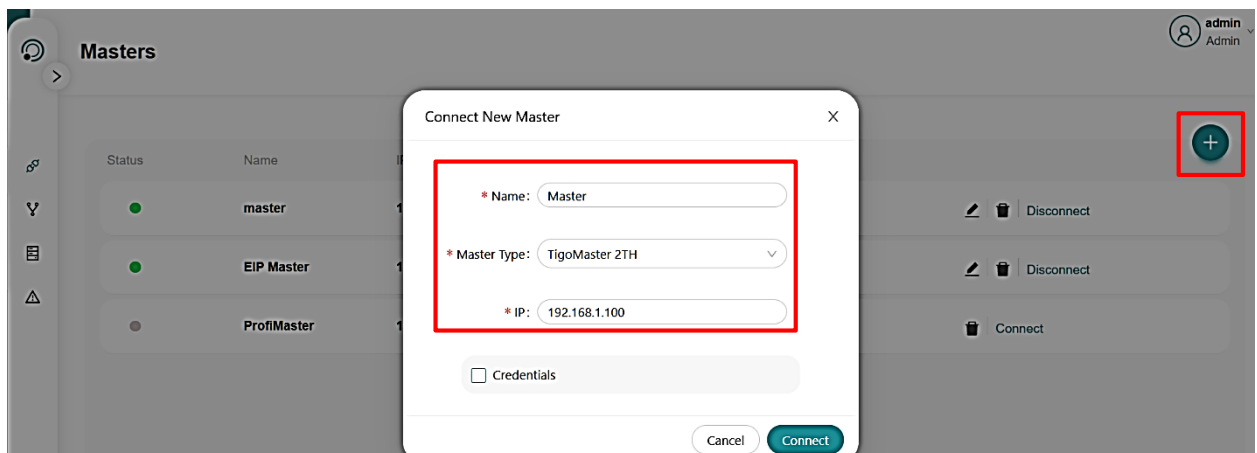


Figure 11 – Detailing the TigoMaster 2TH to Be Connected

- d. If the TigoMaster 2TH's credentials have been changed from the default, select the **Credentials** checkbox and type the current **User Name** and **Password**.

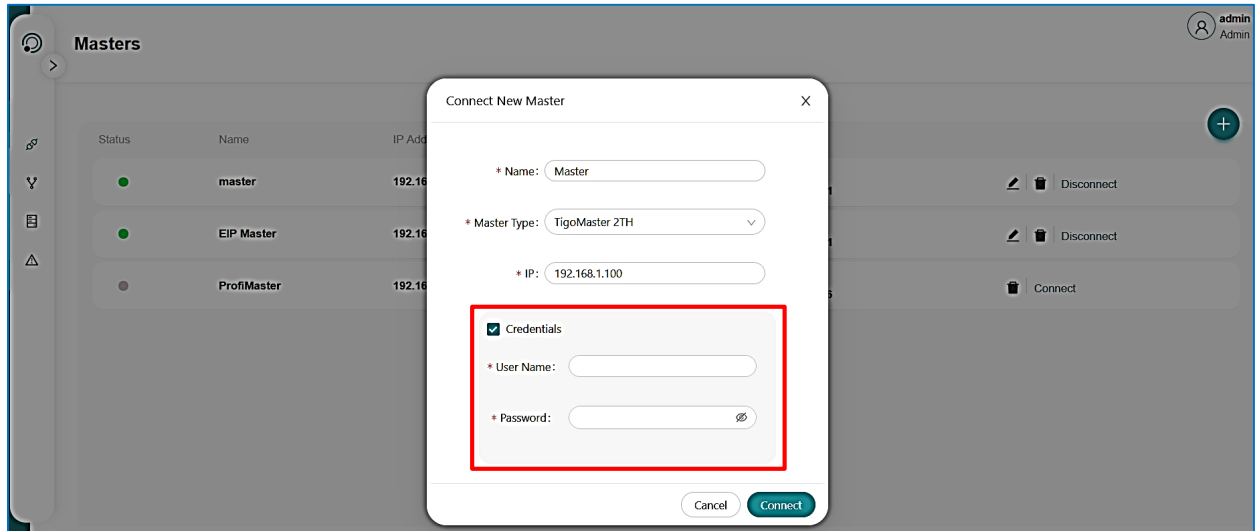


Figure 12 – Detailing Non-Default Credentials

- e. Click **Connect**.

When the TigoMaster 2TH is connected, its details appear in the table in **Masters** view.

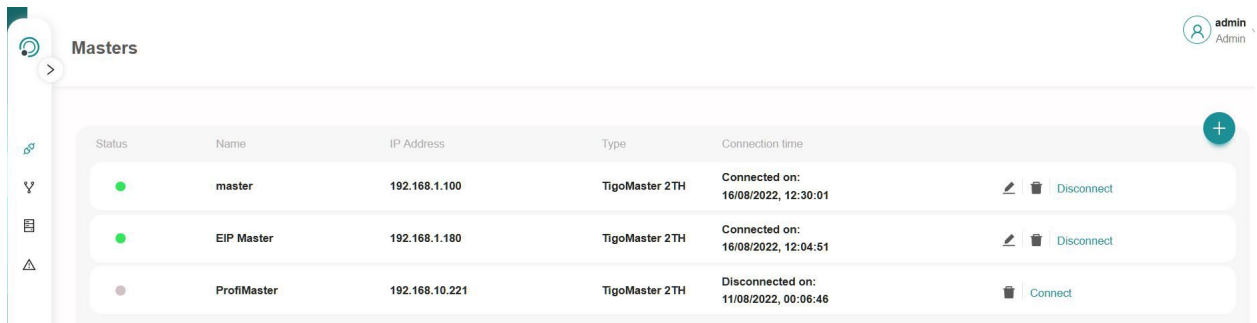


Figure 13: Masters View – Two TigoMaster 2TH Connected

## 7.2. Connecting a New TigoMaster 2TS

1. Run TigoGateway.exe (in the TigoGateway folder).
2. In TigoEngine's **Masters** view, click **+**.
3. In the **Connect New Master** window, set the fields as follows:
  - a. **Name** – type the desired name for the w-master being connected.
  - b. **Master Type = TigoMaster 2TS**

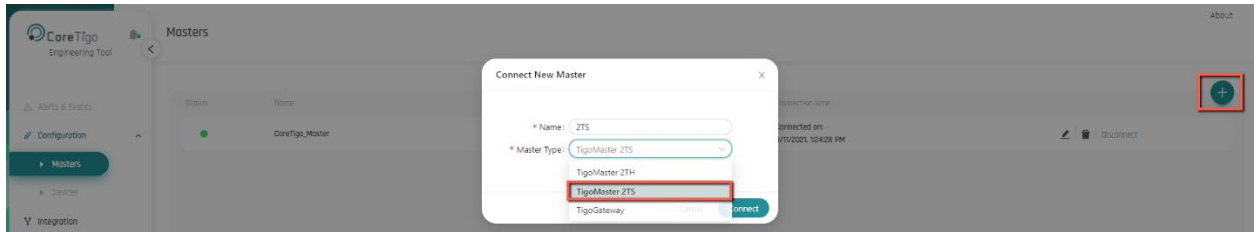


Figure 14: Connecting a TigoMaster 2TS

4. Click **Connect**.

The details of the TigoMaster 2TS appear in the table in **Masters** view:

- The current **status** of the TigoMaster 2TS is partly connected (orange disc).
- The **IP address** of the TigoMaster 2TS is set automatically.
- Next to the IP address is a message stating **COM Port Closed**.

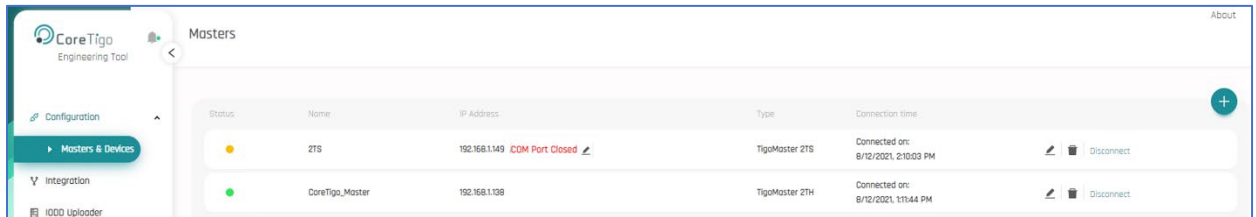


Figure 15: New TigoMaster 2TS Listed in Masters View – Status Is Unconnected

5. Next to **COM Port Closed**, click .

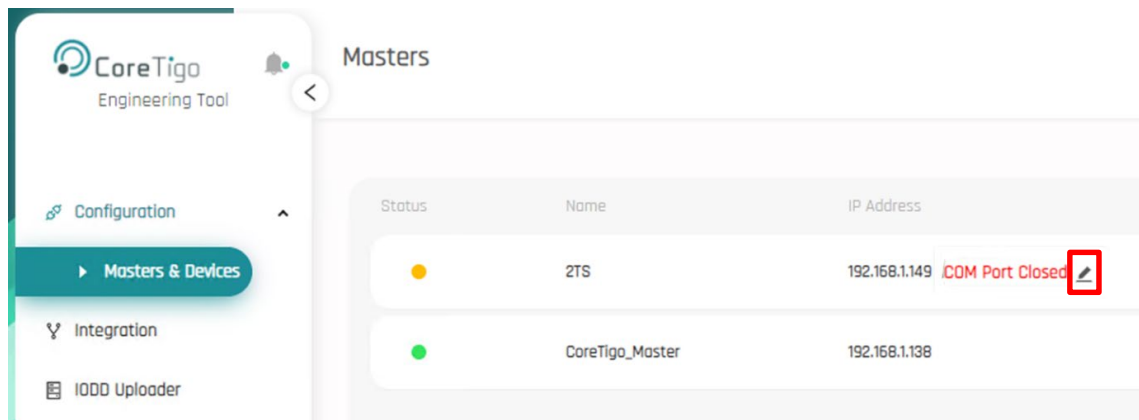
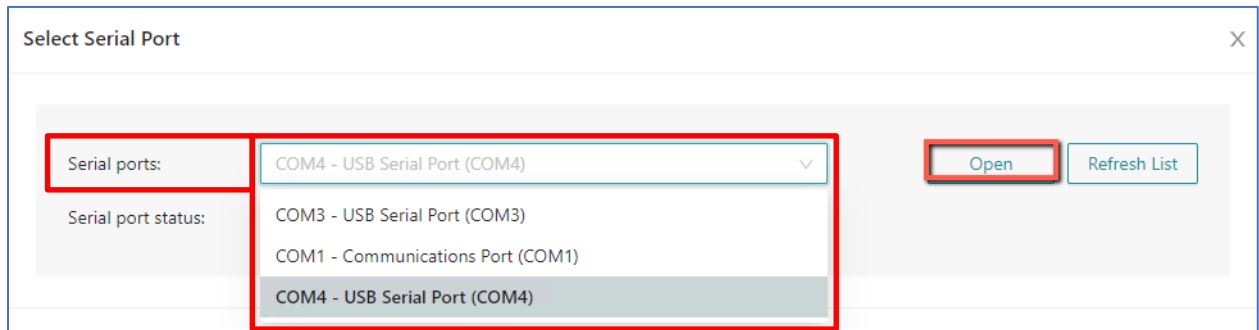


Figure 16: Opening the Select Serial Port Window

6. In the **Select Serial Port** window, do the following:
  - a. In the **Serial Ports** drop-down menu, select the relevant COM port.
  - b. Click **Open**.





**Figure 17: Select Serial Port Window**

In the **Masters** view table, the status of the TigoMaster 2TS changes to connected (green disc), and there is no message stating **COM Port Closed**.

### 7.3. Actions Column

The **Actions** column has the following buttons:

-  – opens the **Edit Master** window, where you can change the name of the relevant w-master
-  – removes the relevant w-master from the list in **Masters** View
- **Disconnect** – disconnects the relevant w-master from TigoEngine



**Figure 18: Actions Column**

## 7.4. Status Column

Each TigoMaster's current status is indicated by an image (a colored dot or a spinner) in the **Status** column. See Figure 19 and Table 1.

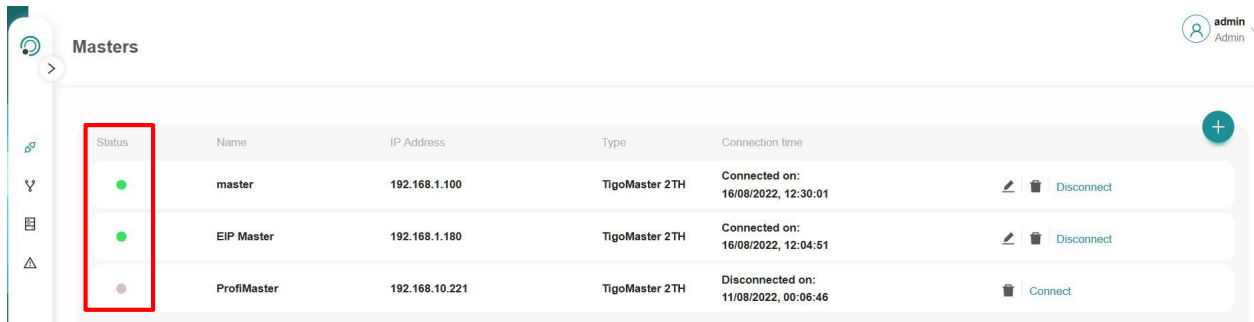


Figure 19: Status Column

Table 1: Statuses

Image in Status Column	Status	Description		Actions Available
		2TH	2TS	
 Spinner	Initializing	Connection requested. TigoEngine trying to connect.		Disconnect w-master Delete w-master
 Green disc	Connected	W-master connected		Disconnect w-master Delete w-master Edit w-master
 Orange disc	Partly connected	N/A	Connection established, but COM port is closed.	Disconnect w-master Delete w-master Edit w-master Configure COM port
 Red disc	Connection failure	Connection failed. TigoEngine trying to reconnect.	N/A	Disconnect w-master Delete w-master
 Grey disc	Inactive	W-master manually disconnected by user. TigoEngine is not trying to reconnect.	W-master disconnected. TigoEngine is not trying to reconnect.	Connect w-master Delete w-master



## 7.5. Auto-Reconnect

After a user has initiated connection of a TigoMaster 2TH (by clicking **Connect** in the **Connect New Master** window), TigoEngine continually tries to connect the TigoMaster 2TH until successful. If the connection later fails, TigoEngine automatically tries to reconnect, again continuing until successful. If TigoEngine closes while trying to connect or reconnect a TigoMaster 2TH (for example, because the computer is rebooted), as soon as TigoEngine restarts, it automatically resumes trying to connect/reconnect.

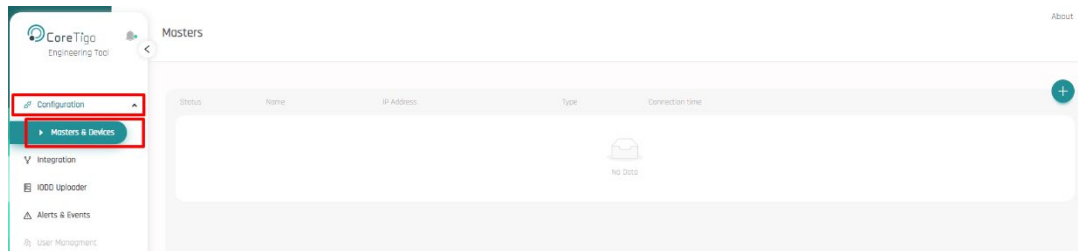
A user can stop TigoEngine trying to connect/reconnect a specific TigoMaster 2TH, by clicking **Disconnect** in the **Actions** column. The status of the TigoMaster is then inactive.

## 8. Configuration Module > Masters Submodule

The **Configuration > Masters & Devices** submodule (see Figure 20) provides various views for connecting w-masters to TigoEngine, configuring connected w-masters, and viewing information about them. The views are:

- **Masters** view (default/opening view): see section 7
- **Masters Configuration** view: see section 10
- **Port Configuration** view: see section 11
- **Blacklist** view: see section 12
- **Firmware** view: see section 13
- **Integrations** view: see section 14
- **Test Environment** view: see section 15
- **Statistics** view: see section 16

To open the Masters & Devices submodule, in the explorer pane select **Configuration > Masters & Devices**:



**Figure 20: Configuration > Masters Submodule – Default View**

## 9. Navigation

### 9.1. Opening a W-Master in a Specific View

To view/configure any of a w-masters properties that are not shown in **Masters** View (for example, its Firmware), do the following:

1. In **Masters** view, click the **name** of the desired w-master.  
The w-master opens in **Port Configuration** view.
2. In the Views bar, select the desired view (in this example, **Firmware** view).

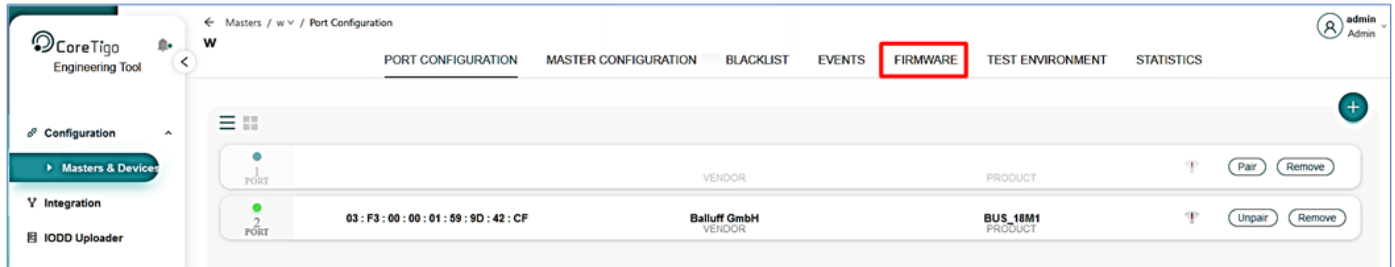


Figure 21: Opening a W-Master in a Specific View – Example

### 9.2. Navigating between W-Masters within a View

When you have finished viewing/configuring a specific w-master in a specific view (for example, the **Port Configuration** view), you can open another w-master in the same view, by doing the following:

1. In the path bar, click **v** next to the name of the currently open w-master.
2. From the drop-down menu, select the w-master that you want to open.

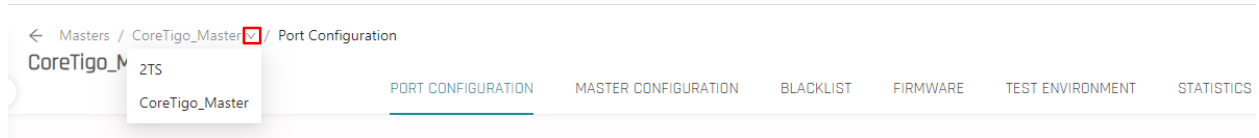
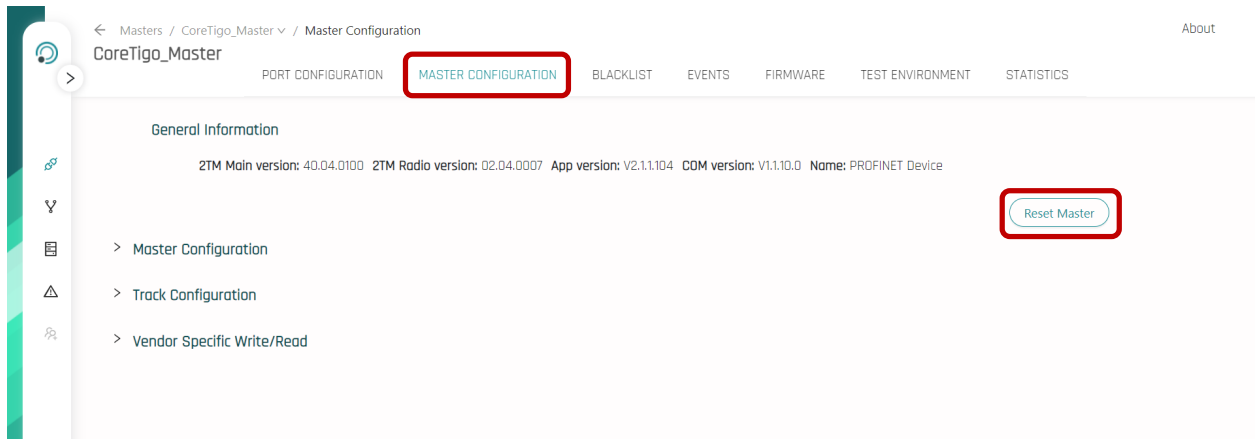


Figure 22: Navigating to another W-Master within the Current View

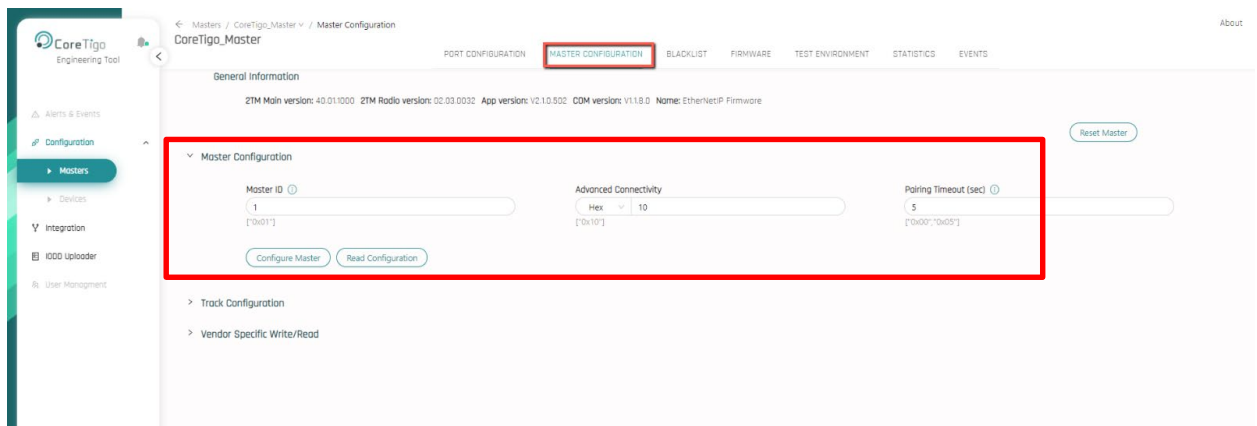
## 10. Master Configuration View

In **Master Configuration** view you can:

- **Reset** the selected w-master if it is a TigoMaster 2TH: see Figure 23
- View/configure the selected w-master's advanced parameters: see Figure 24 and Table 2
- View/configure the selected w-master's **track** parameters: see Figure 25 and Table 3
- View/configure the selected w-master's **vendor specific read/write** parameters: see Figure 26 and Table 4



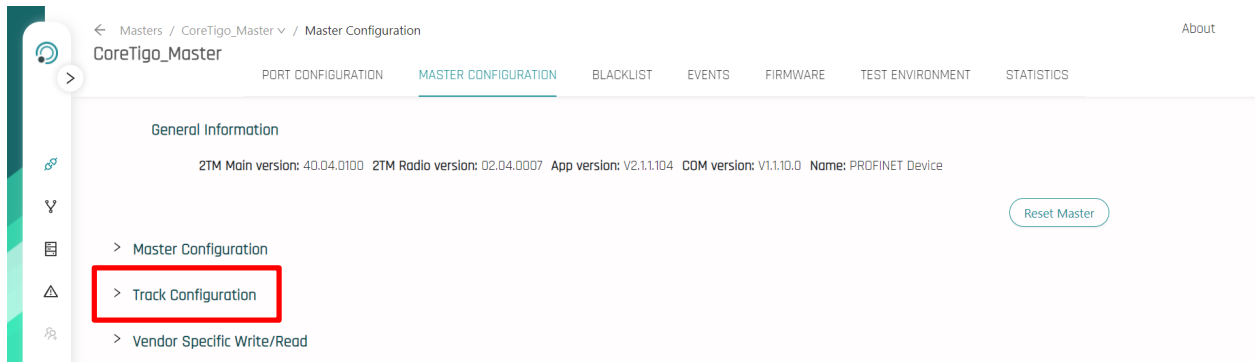
**Figure 23: Resetting the W-Master's Software**



**Figure 24: Master Configuration View (Advanced Parameters)**

**Table 2: Master Configuration Parameters (Advanced Parameters)**

Parameter	Description
<b>Master ID</b>	W-Master Identifier according to IOLW specification
<b>Advanced Connectivity</b>	Various advanced configuration parameters
<b>Pairing Timeout (sec)</b>	Timeout for pairing by button/UID in seconds



**Figure 25: Track Configuration Parameters**

**Table 3: Track Configuration Parameters**

Parameter	Description
<b>Track Mode</b>	Track operation mode: 0 – STOP 1 – CYCLIC 2 – SCAN 3 – ROAMING 4 – PAIRING
<b>TX Power</b>	Transmission strength

**Figure 26: Vendor Specific Read/Write Parameters**

**Table 4: Vendor Specific Read/Write Parameters**

Parameter	Description
<b>Port ID</b>	W-Port
<b>Arg Block ID</b>	Command number (e.g. for PDout commands use 1002)
<b>Arg Block Data</b>	Data block (e.g. PDout Valid byte + Data bytes)

# 11. Port Configuration View

In **Port Configuration** view, you can:

- Scan for available w-devices in range of the selected w-master: see section 11.1
- Pair the w-master with w-devices, and unpair them: see section 11.2
- Debug, monitor, and reset w-devices
- View information about ports and the w-devices connected to them: see section 11.5

## 11.1. Scanning for W-Devices

1. In **Port Configuration** view, click **+**.

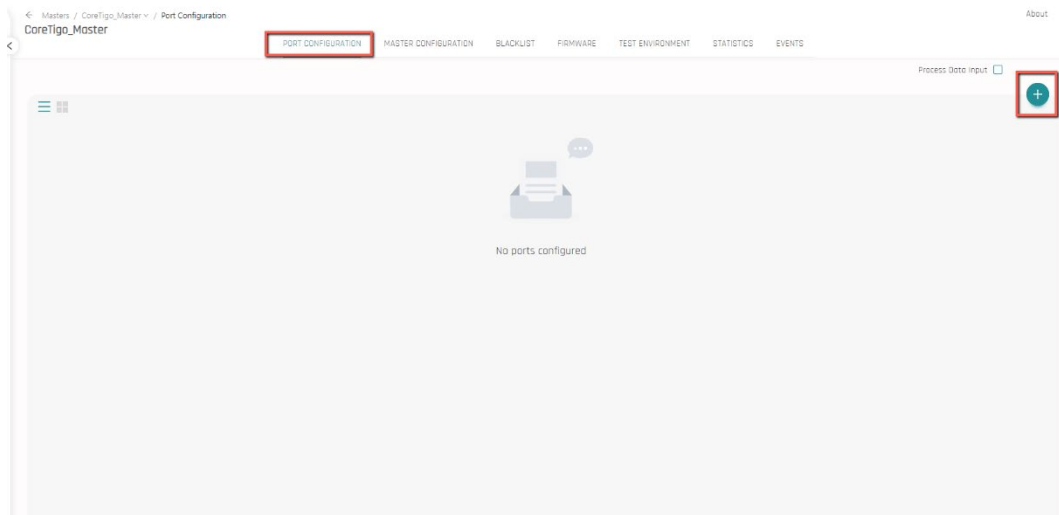


Figure 27: Port Configuration View

2. In the Port Configuration bar, click **Scan**.

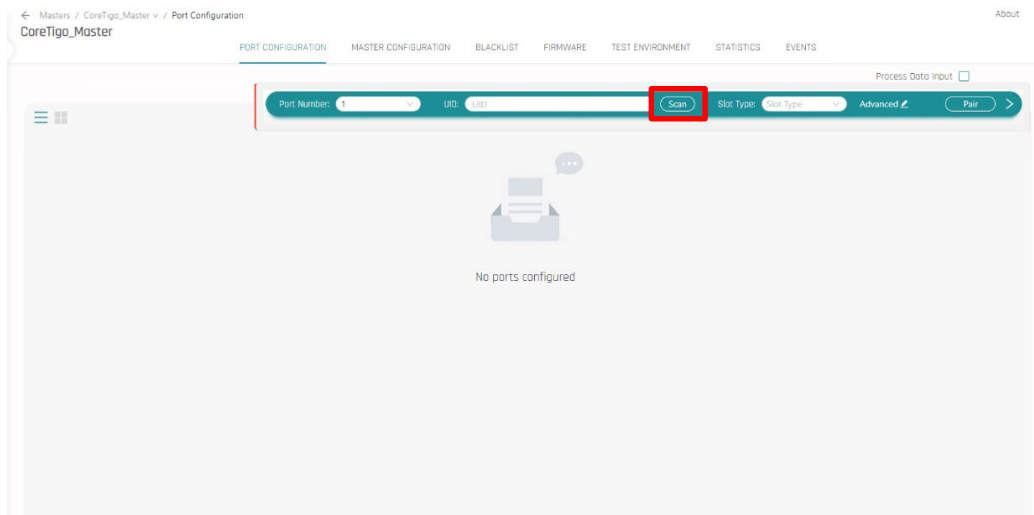


Figure 28: Scan Button

3. TigoEngine lists the available w-devices in range of the selected w-master. The list includes the following information about each w-device:
  - **UID** – the unique ID of the w-device (hexadecimal representation)
  - **Slot Type** – whether the w-device is using a single or double slot (as determined by its device type and the system requirements)

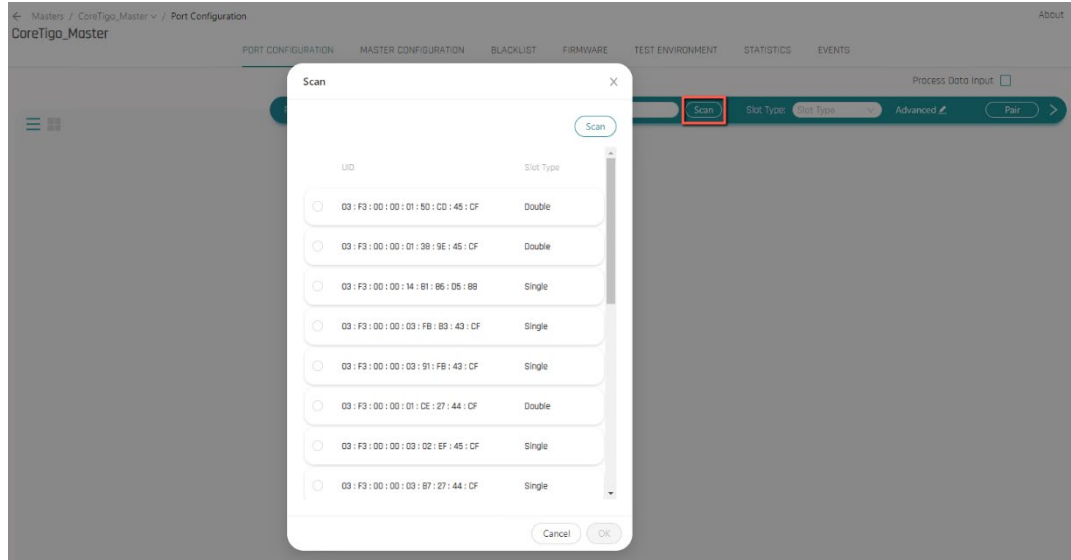


Figure 29: List of Available W-Devices in Range of Selected W-Master

## 11.2. Pairing a W-Master and W-Device

### 11.2.1. Pairing from Scan Results

1. In the **Scan** results (see section 11.1), select the w-device that you want to pair with the w-master.
2. Click **OK**.

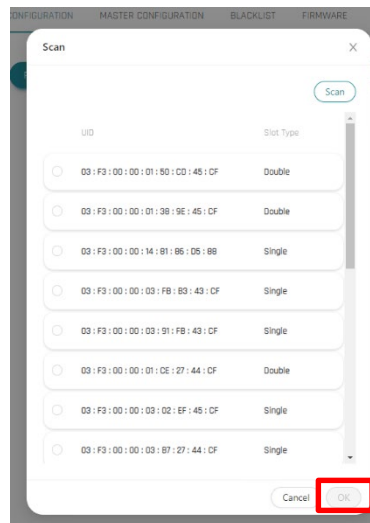


Figure 30: Scan Results

3. The **UID** of the selected w-device appears in the Port Configuration bar.
4. If desired, configure the selected w-device: see section 11.3.

5. In the Port Configuration bar, click **Pair**.

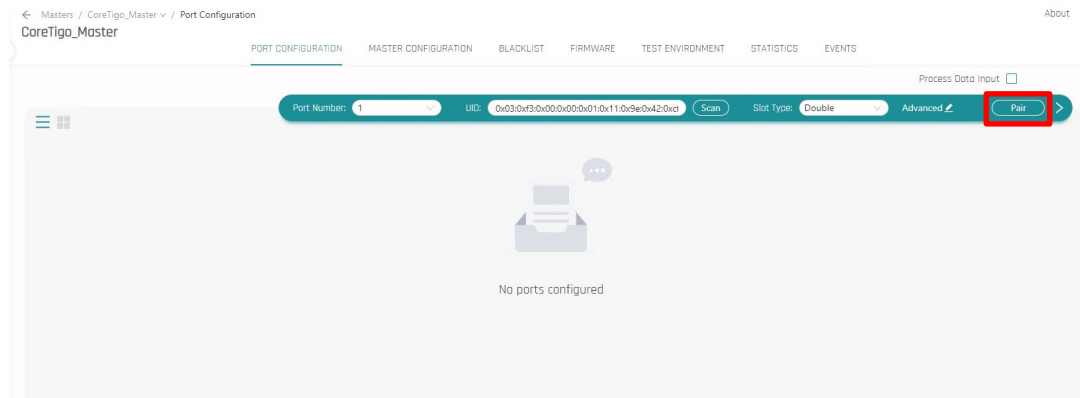


Figure 31: Pair Button

6. An auto-generated **Port Number** and the **Slot Type** of the selected w-device appear in the Port Configuration bar.
7. When pairing is successful, details of the paired w-device appear in the **Port Configuration** view table. Details include its port number, UID, and input data (if it supports PDIn).

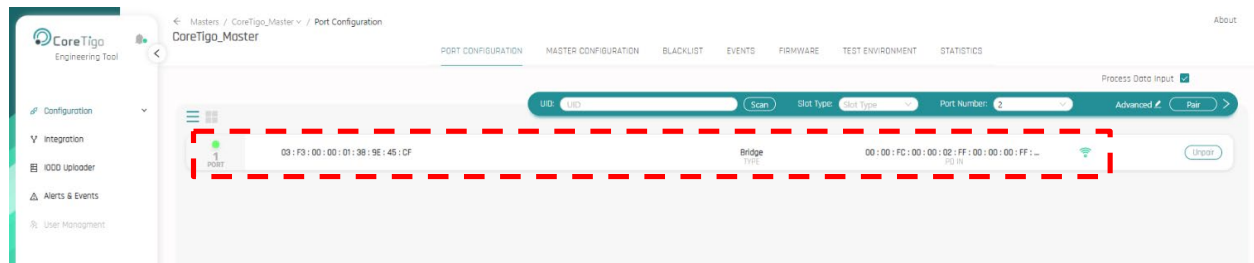


Figure 32: Paired W-Device in Port Configuration View

## 11.2.2. Pairing without Scanning

If you know the UID of the w-device that you want to pair with the selected w-master, you can pair them as follows:

1. In the Port Configuration bar, type the **UID** of the w-device that you want to pair with the w-master.

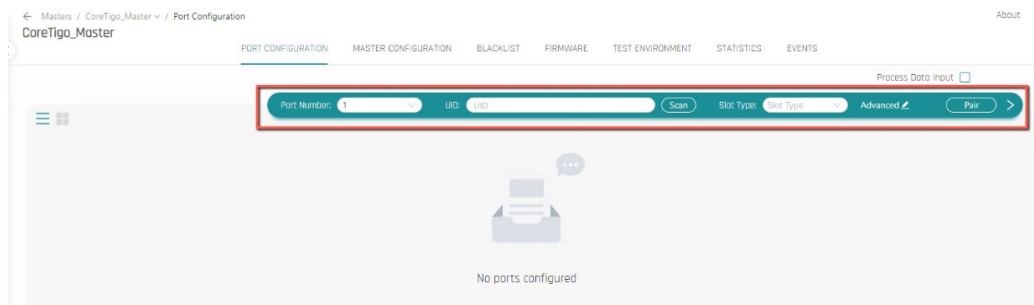


Figure 33: Port Configuration Bar

2. In the Port Configuration bar, click **Pair**.
3. When pairing is successful, details of the paired w-device appear in the **Port Configuration** view table. Details include its port number, UID, and input data (if it supports PDIn). See Figure 32.

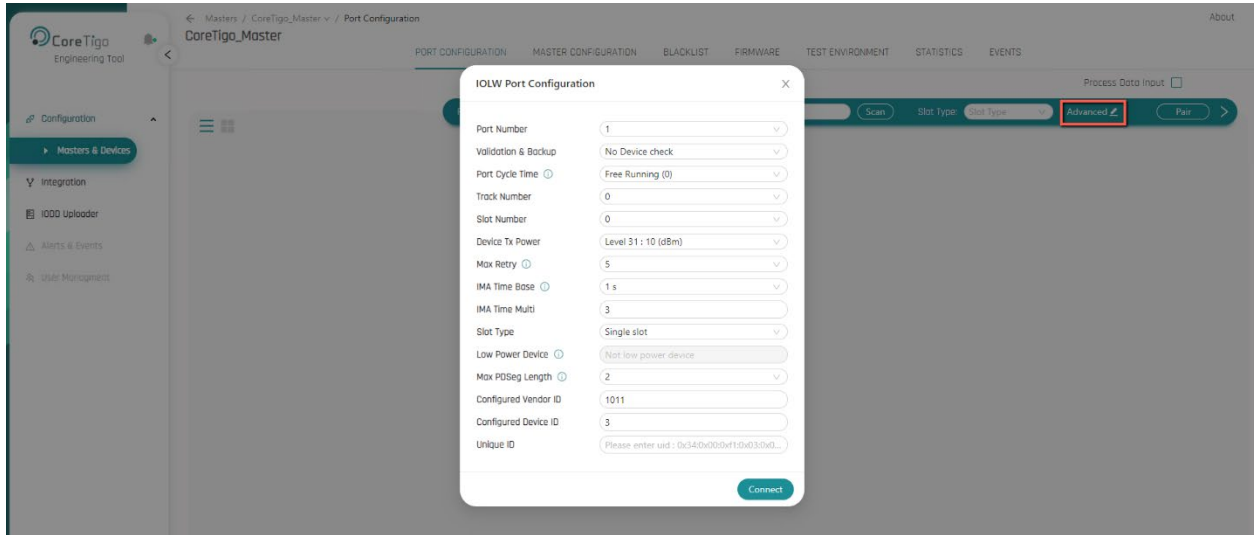


### 11.3. Advanced Configuration (IOLW Configuration)

The IOLW configuration details the parameters for a particular port and the w-device connected to it, or of a w-device in the scan results.

To view/modify the IOLW configuration of a specific available w-device in range of the selected w-master:

1. In the Port Configuration bar, type the **UID** of the desired w-device (either from the scan results or by typing it).
2. Clicked **Advanced**.
3. The **IOLW Configuration** window appears. Each of its parameters is detailed in Figure 34.



**Figure 34: IOLW Configuration Window**

**Table 5: IOLW Configuration Parameters**

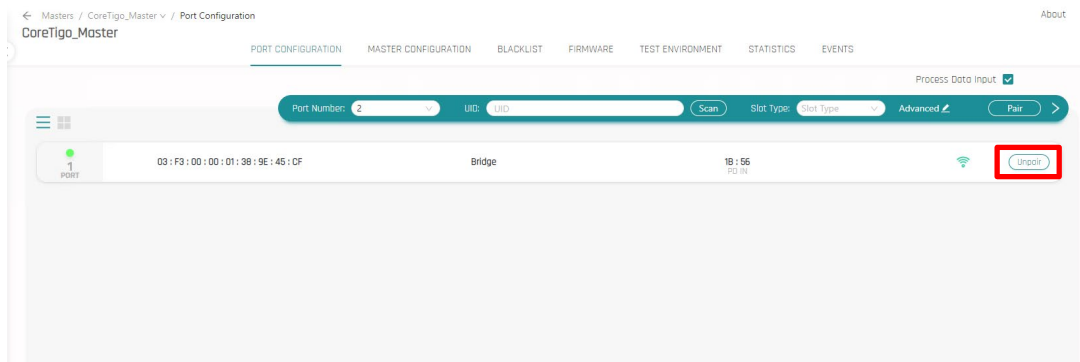
Parameter	Value Range	Description
<b>Port Number</b>	1–16 (if the selected w-master is 2 track)	
<b>Validation and Backup</b>	No device check (default)	No validation, backup, or restore of the selected w-device is performed
	Type compares*, no Backup/Restore	Validation of the selected w-device is performed, without backup/restore
	Type compares*, Backup only	Validation and backup of the selected w-device are performed, without restore
	Type compares*, Restore only	Validation and restore of the selected w-device are performed, without backup
	Type compares*, Backup and Restore	Validation, backup, and restore of the selected w-device are performed
	No type compares*, no Backup/Restore	Validation of the selected w-device is performed, without type compare, backup, or restore

Parameter	Value Range	Description
	No type compares*, Backup only	Validation and backup of the selected w-device are performed, without type compare or restore
	No type compares*, Restore only	Validation and restore of the selected w-device are performed, without type compare or backup
	No type compares*, Backup and Restore	Validation, backup, and restore of the selected w-device are performed, without type compare
<b>Port Cycle Time</b>		Port cycle time expected by the SMI client.  The expected cycle time of the port is set depending on the selected operating mode
<b>Track Number</b>		Wireless track number to be used for the port
<b>Slot Number</b>		Wireless slot number to be used for the port
<b>Device Tx power</b>		Transmission power level of the w-device
<b>Max Retry</b>		Maximum number of retries for a transmission in OPERATE mode
<b>IMA Time Base</b>		Requested IMA time for OPERATE mode  IMA = I am alive
<b>IMA Time Multi</b>		The IMA Time Multi is calculated by multiplying the IMA Time Base
<b>Slot Type</b>	Single slot or Double slot	Port parameter
<b>Low Power Device</b>	0x0 – Not Low Power 0x1 – Low Power	Is the selected w-device low power or not
<b>Max PDSEg length</b>		The maximum segment length of the PDOOut data to the message handler to distribute PDOOut data within multiple wireless cycles.  The value depends on the actual transmission capacity of the selected w-device.
<b>Configured Vendor</b>		Expected vendor ID of w-device.  Required to check the device for type compatibility

Parameter	Value Range	Description
<b>Configured Device</b>		Expected device ID of w-device.  Required to check the device for type compatibility.
<b>Unique ID</b>		Unique ID of the w-device (9 Bytes)

## 11.4. Unpairing a W-Master and W-Device

1. In **Port Configuration** view, select the relevant w-device/port.
2. Click **Unpair**.



**Figure 35: Unpair Button**

## 11.5. Viewing Port Information

When a specific port is selected in the **Port Configuration** view, you can view further information about the port in various tabs (see Figure 36). The tabs / types of information are:

- **Details**
- **Port Configuration**
- **Data**
- **Device Configuration**
- **Process Data**
- **Events**

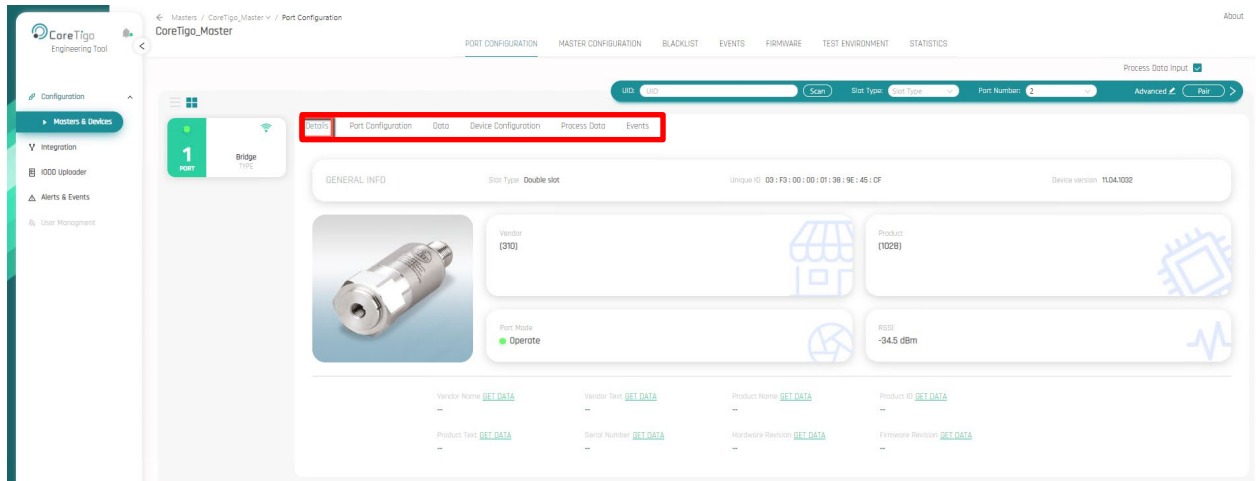


Figure 36: Port Configuration View Tabs

### 11.5.1. Details Tab

In the **Details** tab, you can:

- See details of the w-device(s) connected to the selected w-master. Details include unique ID, w-device type, version, vendor name, device name, and port name. These are taken from the IODD file repository, which is detailed in section 17.
- Upload IODD zip files as detailed in section 17.

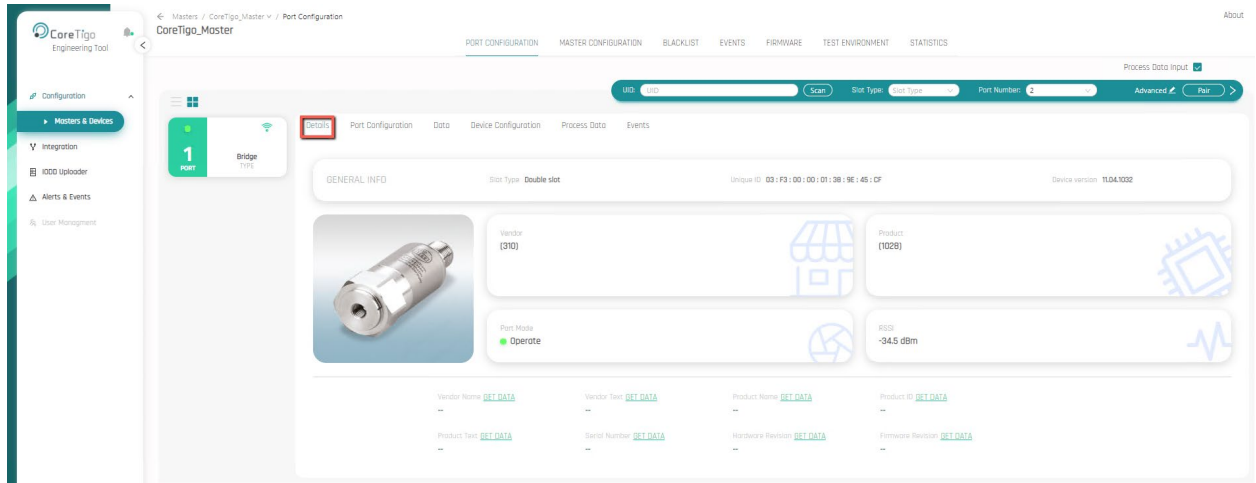


Figure 37: Details Tab

### 11.5.2. Port Configuration Tab

In the **Port Configuration** tab, you can see the parameter values of the port and the w-device(s) connected to it.

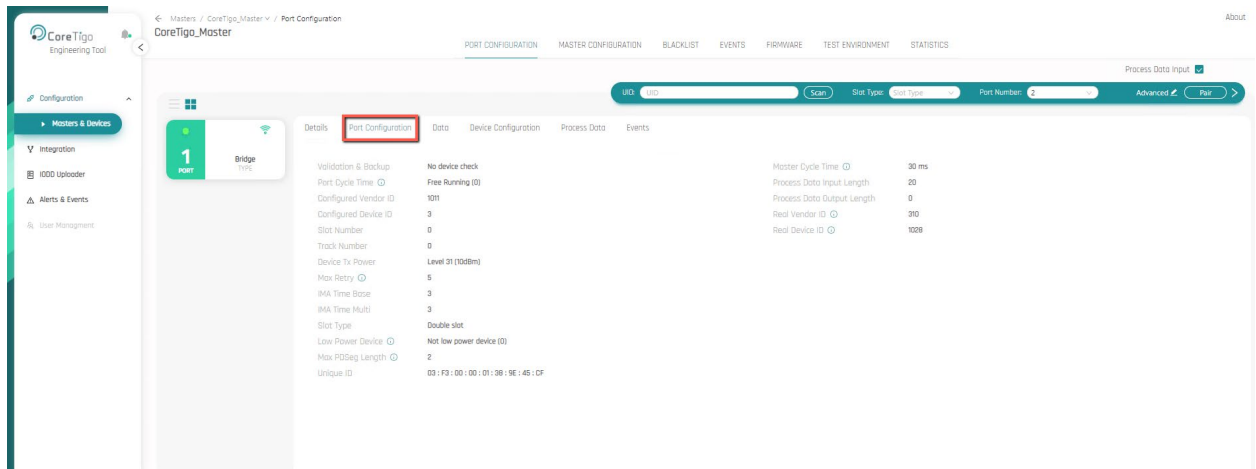


Figure 38: Port Configuration View Tabs

### 11.5.3. Data Tab

In the **Data** tab, you can send ISDU (Indexed Service Data Unit) read messages and write messages to the w-devices (IO-link sensors/actuators) connected to the port. These messages read or write (set) the values of the w-devices' parameters. The parameters are arranged in a structure of data objects, and each include the following:

- **Data:** the value to write to the ISDU data object (parameter) of the w-device, or the value that is read from it
- **Index:** the page number of the ISDU data object (parameter) to be read/written
- **Sub-Index:** the data element address within the ISDU data object

#### To send an ISDU write message:

1. Go to the **Port Configuration** view > **Data** tab.
2. Under **ISDU Write** enter the desired values for:
  - **Data**
  - **Index**
  - **Sub-Index**
3. Click **Write**.

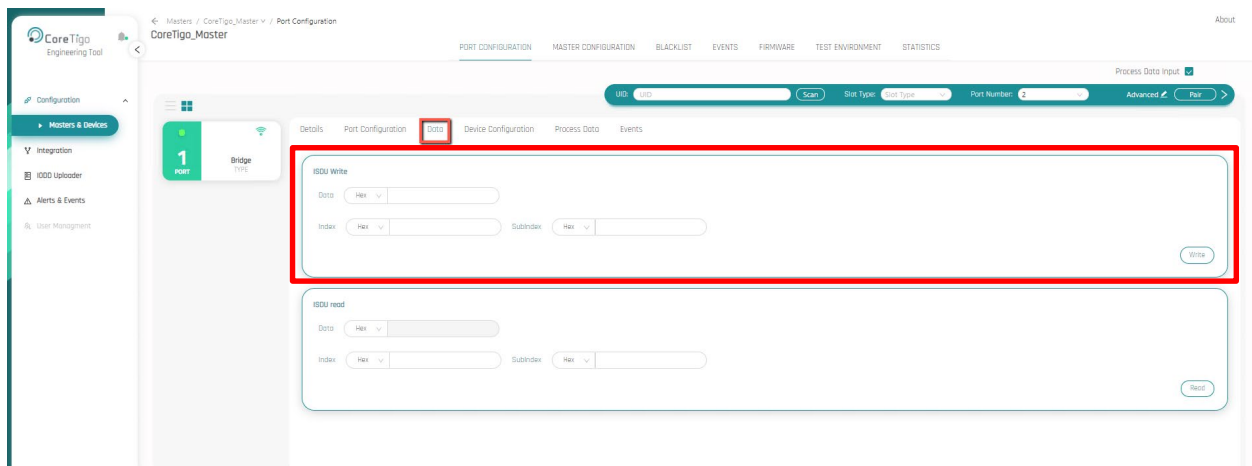


Figure 39: Write ISDU

### To send an ISDU read message:

1. Go to the **Port Configuration** view > **Data** tab.
2. Under **ISDU Write** enter the desired values for:
  - o **Index**
  - o **Sub-Index**
3. Click **Read**.

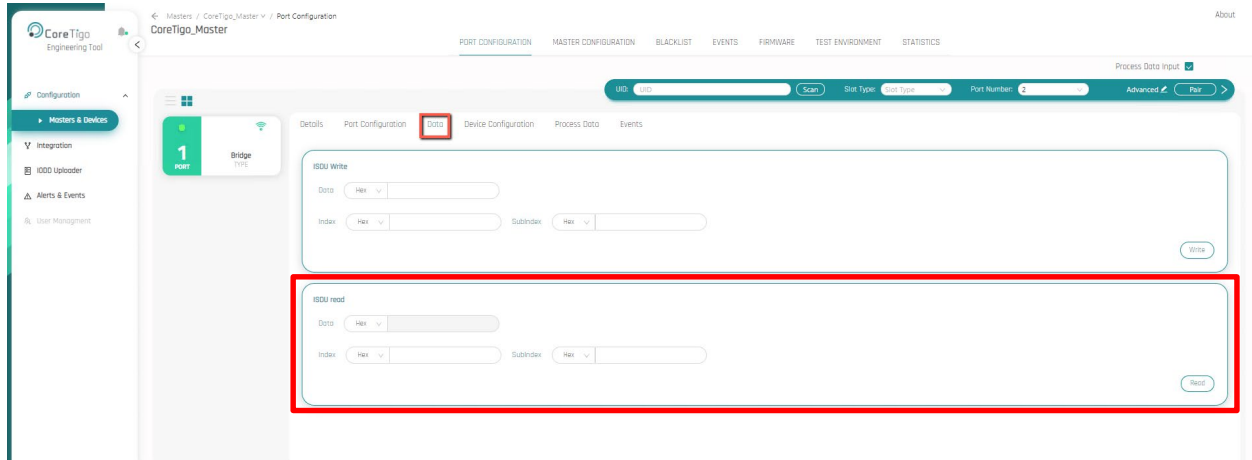


Figure 40: Read ISDU

### 11.5.4. Device Configuration Tab

In the **Device Configuration** tab, you can configure a connected w-device or read its parameters by uploading an IOLW configuration file. If an IODD file is already uploaded, then the w-device parameters appear in the tab.

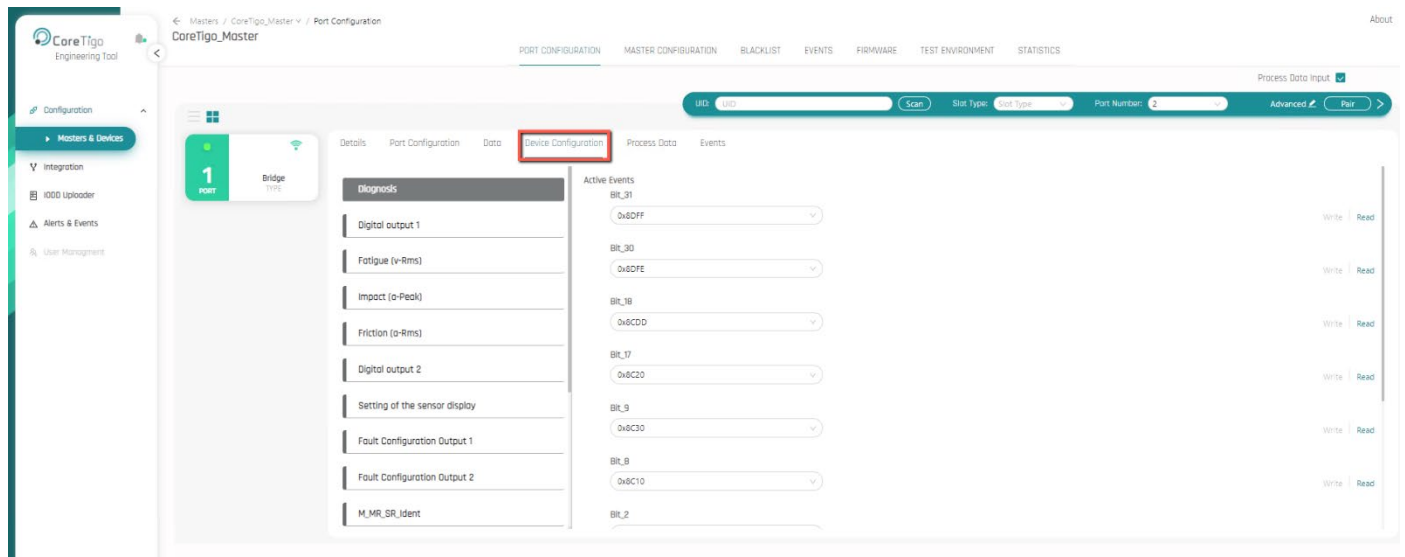


Figure 41: Device Configuration Tab

### 11.5.5. Process Data Tab

In the **Process Data** tab, you can do the following:

- View process data received from the connected w-device(s) in real-time (in the **Process Data Input** field). When the IODD of the device is uploaded, TigoEngine presents process data parsed. Otherwise data is displayed in a raw format and is intended for evaluating the correct operation of the w-device during development.
- Send out process data to the connected w-device(s) by means of the **Process Data Out** section of the tab.

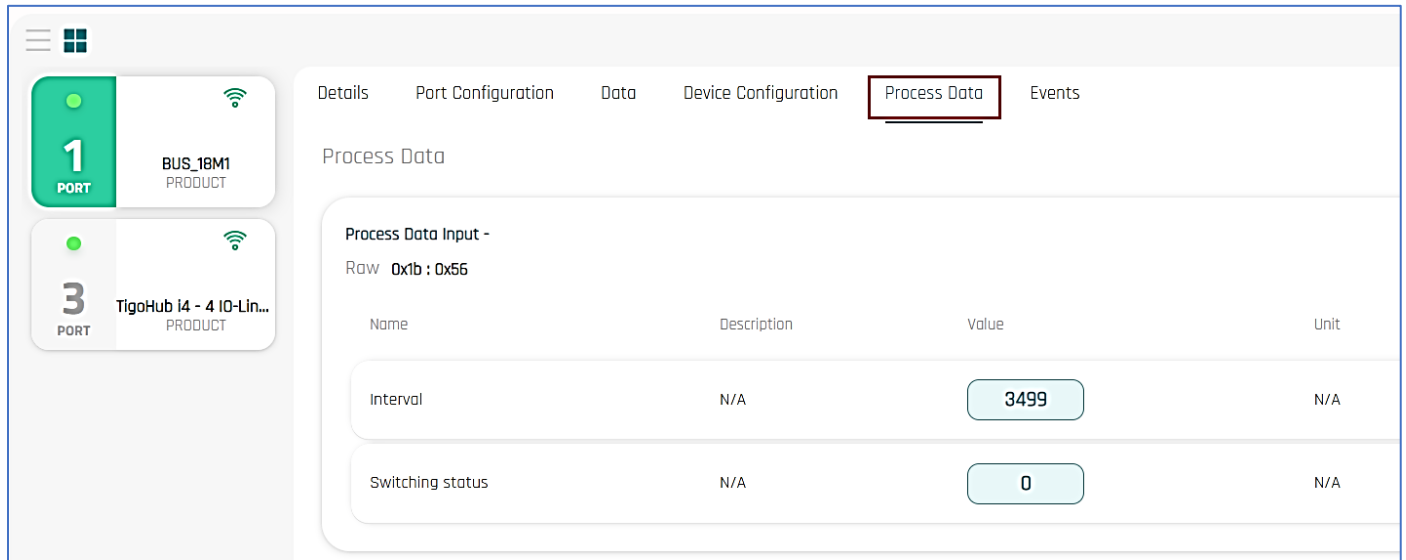


Figure 42: Process Data Tab

### 11.5.6. Events Tab

The Events tab is the same as [Events View](#). For details see section [16](#).



## 12. Blacklist View

In **Blacklist** view you can set which frequencies/channels/bandwidths the w-master is permitted/prohibited from using for communication with w-devices.

### 12.1. Changing a Frequency to Prohibited or Permitted

1. In **Blacklist** view, click the relevant frequency to change its state (that is, toggle it between prohibited and permitted).  
In the example in Figure 43, the **2406 MHz/2** frequency is being toggled to prohibited.
2. Click **Save Changes**.
3. Reset the w-master.

The screenshot displays the 'Blacklist' configuration page in the CoreTigo Engineering Tool. The page title is 'CoreTigo\_Master' and the breadcrumb is 'Masters / CoreTigo\_Master / Blacklist'. The navigation menu includes 'PORT CONFIGURATION', 'MASTER CONFIGURATION', 'BLACKLIST', 'FIRMWARE', 'TEST ENVIRONMENT', 'STATISTICS', and 'EVENTS'. The main content area shows 'Total Number of Blacklisted Channels: 0'. A frequency spectrum visualization shows three Wi-Fi channels: Wi-Fi Ch. 1, Wi-Fi Ch. 6, and Wi-Fi Ch. 11. Below the spectrum, a list of frequencies from 2402 MHz to 2480 MHz is shown. The frequency 2406 MHz is highlighted with a red box. Below the list, there are controls for 'Channel Range Selection', 'Bandwidth: 20 Mhz', and 'Channel: Select channel'. A 'Save Changes' button is highlighted with a red box.

Figure 43: Toggling a Frequency between Prohibited and Permitted – Example

## 12.2. Changing a Channel/Bandwidth to Prohibited or Permitted

1. In **Blacklist** view, select the relevant **Bandwidth**.
2. Select the relevant **Channel**.
3. Click **Prohibit** or **Permit** as desired.
4. Click **Save Changes**.
5. Reset the w-master.

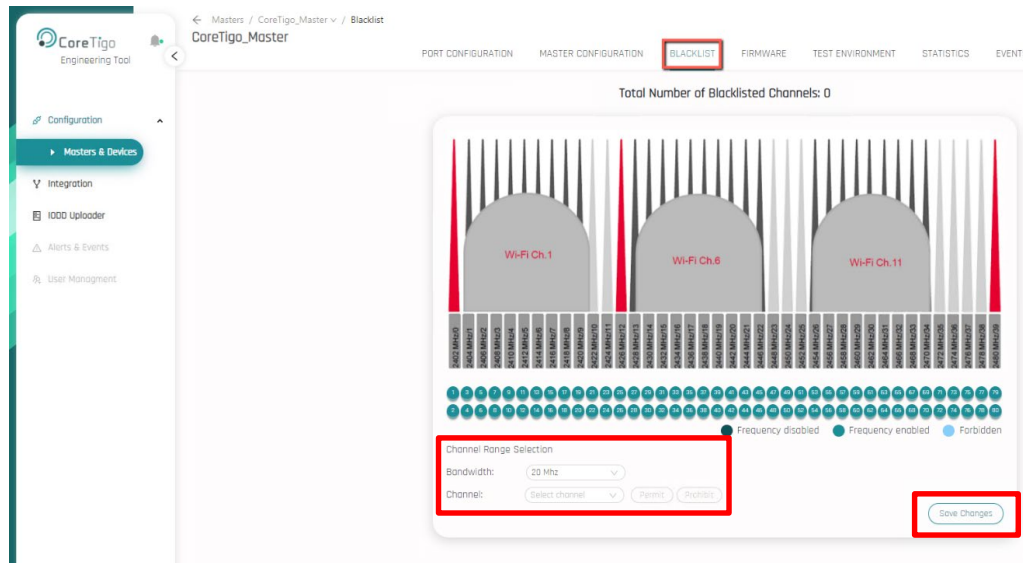


Figure 44: Changing a Channel/Bandwidth to Prohibited or Permitted

## 13. Firmware View

In **Firmware** view, you can upgrade the firmware of the selected w-master and its connected w-device(s).

### 13.1. Upgrading W-Master Firmware

1. Download the latest w-master firmware file from the CoreTigo Customer Portal.
2. In **Firmware** view, under **Master Upgrade** click **Upload FW Version**.

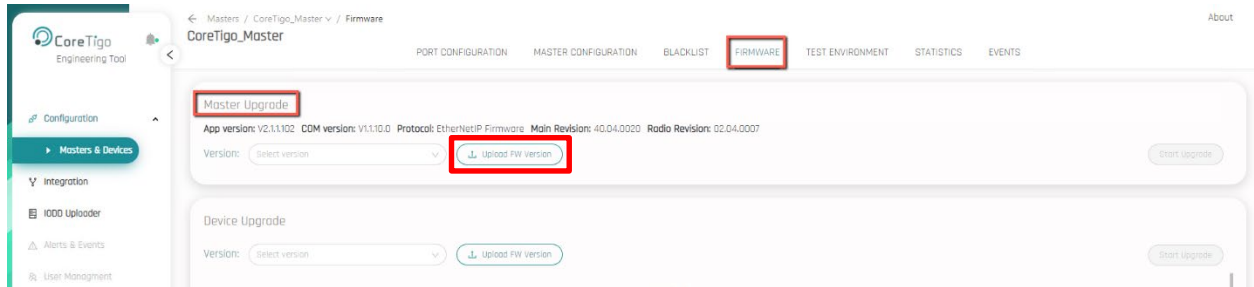


Figure 45: Upload FW Version

3. In the **Version** field, select the firmware file.

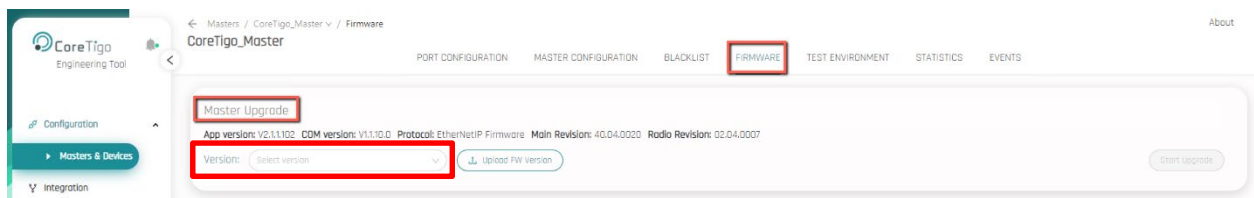


Figure 46: Version

4. Click **Start Upgrade**.

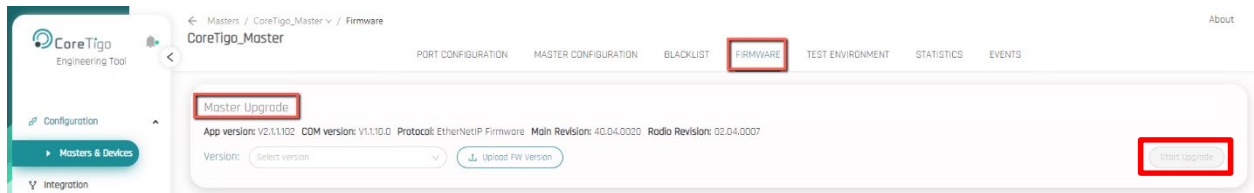


Figure 47: Start Upgrade

## 13.2. Upgrading W-Device Firmware

1. Download the latest firmware file for the relevant type of w-device from the CoreTigo Customer Portal.
2. In **Firmware** view, under **Device Upgrade** select the checkbox of each port connected to a w-device whose firmware you want to upgrade.

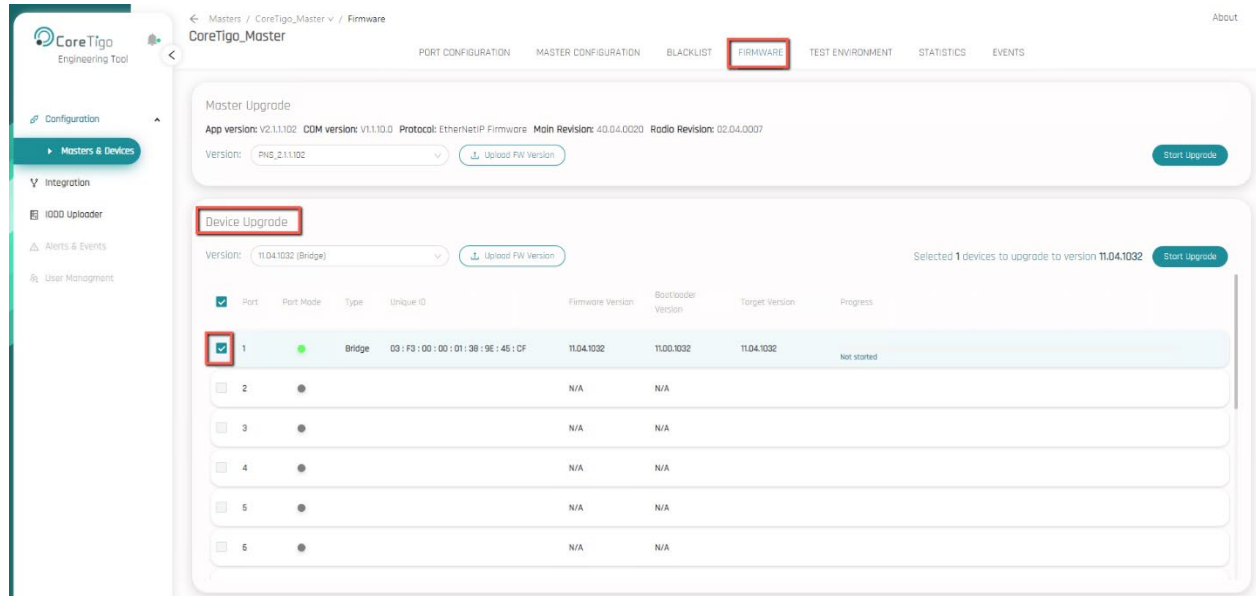


Figure 48: Port Checkbox

3. Under **Device Upgrade**, click **Upload FW Version**.

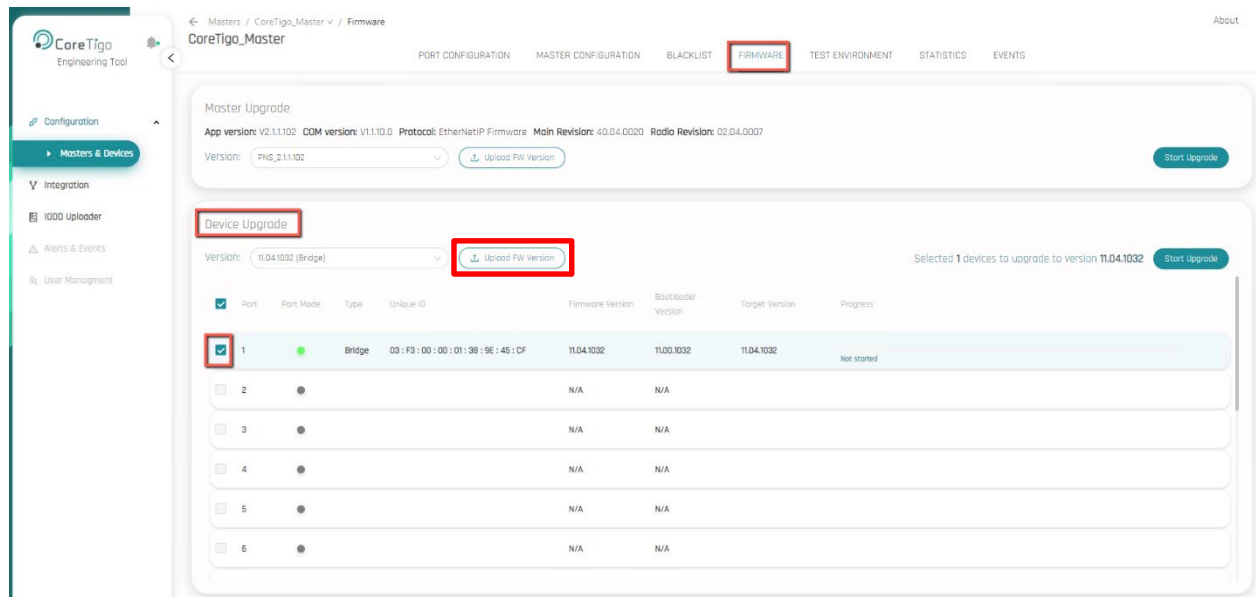


Figure 49: Upload FW Version

4. In the **Version** field, select the firmware file.

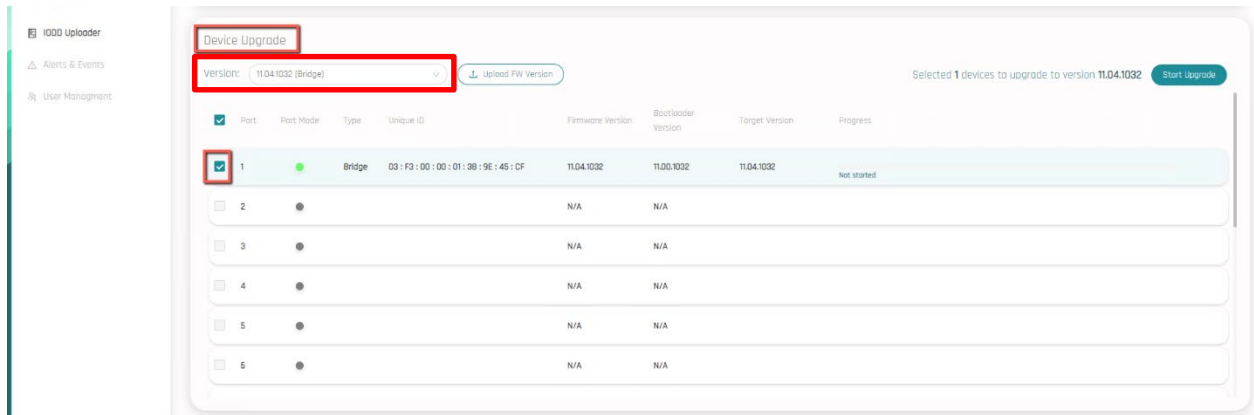


Figure 50: Version

5. Click **Start Upgrade**.

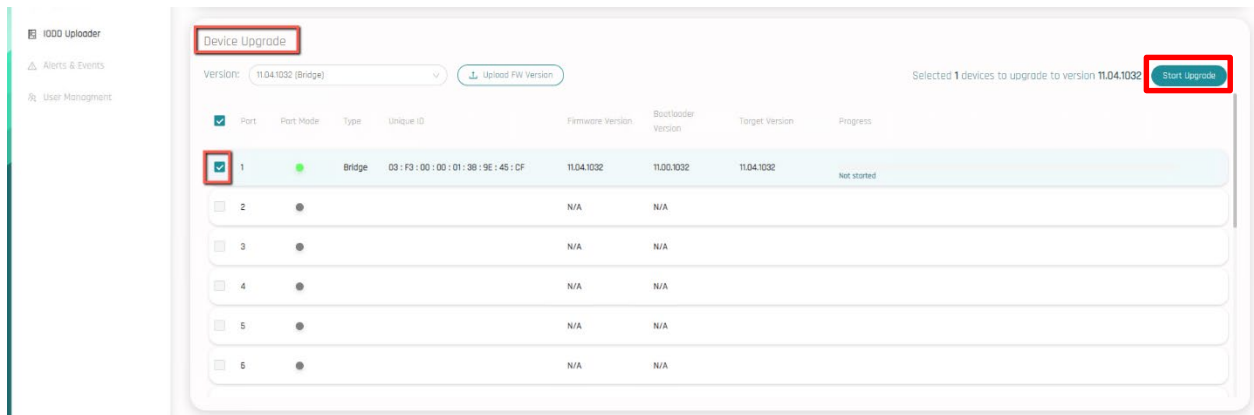


Figure 51: Start Upgrade

The FOTA process begins, and the w-devices are upgraded one after another. You can view progress in the Progress bar.

## 14. Test Environment View

In **Test Environment** view, you can run the following:

- Latency test
- PER test (PDin)
- PER test (PDout)

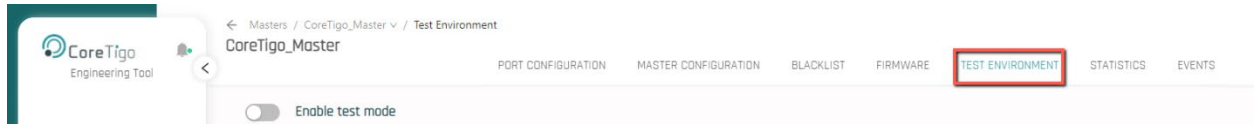


Figure 52: Test Environment View

### 14.1. Running a Test



#### Warning!

Running a test interferes with operational functionality. During a test, Process Data input and output are blocked on the port where the test is running.

1. In **Test Environment** view, toggle the **Test Mode** switch to the On position.

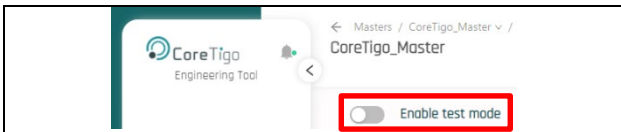


Figure 53: Test Mode Button in Off Position

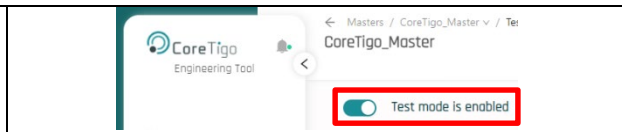


Figure 54: Test Mode Button in On Position

2. In the **Warning** dialog box, click **I understand**.

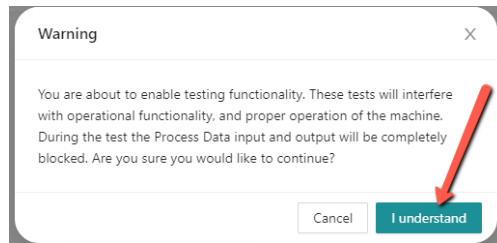


Figure 55: Warning Dialog Box

3. Select the desired test from the drop-down menu

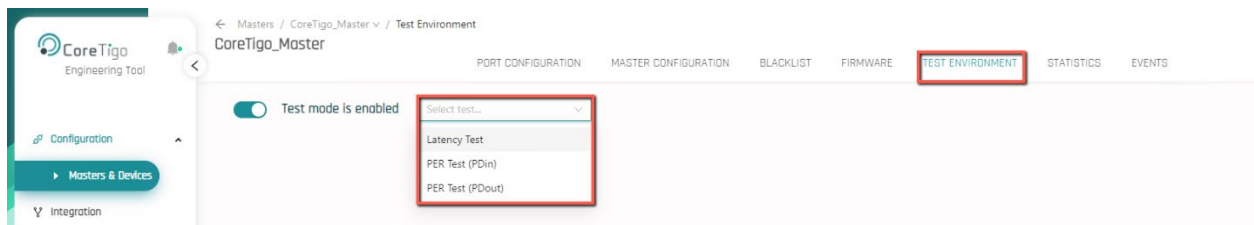


Figure 56: Select Test Menu

- Set the **Manual Stop** switch in the desired position:
  - If the switch is in the Off position (default), the test stops automatically (after the set number of cycles)
  - If the switch is in the On position, you need to stop the test manually by clicking the **Stop Test** button when desired.

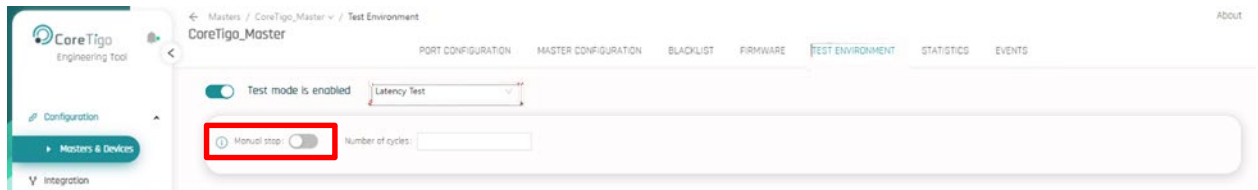


Figure 57: Manual Stop Switch

- Set the desired **number of cycles** for the test to run (up to a maximum of 4294967295).

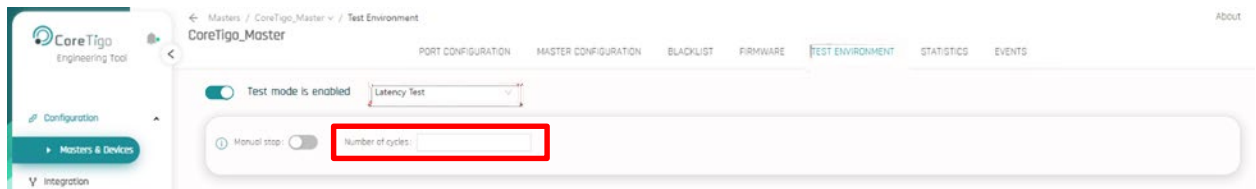


Figure 58: Number of Cycles

- Select the checkbox(es) of the port(s) that you want to run the test on.

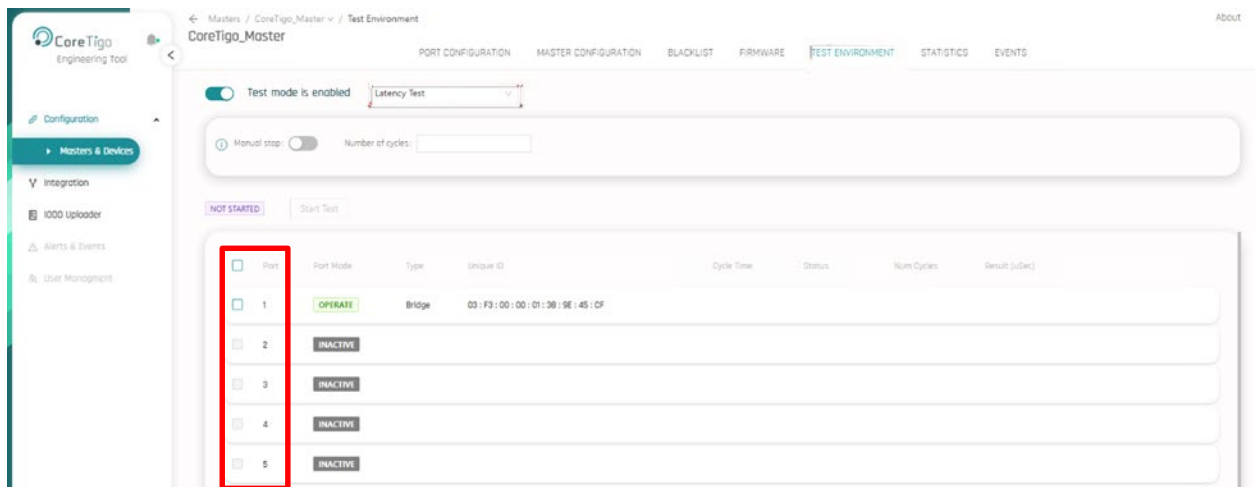


Figure 59: Port Checkboxes

- Click **Start Test**.

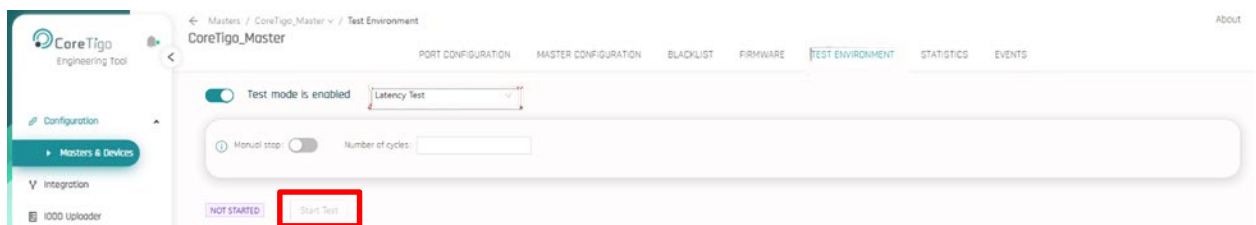
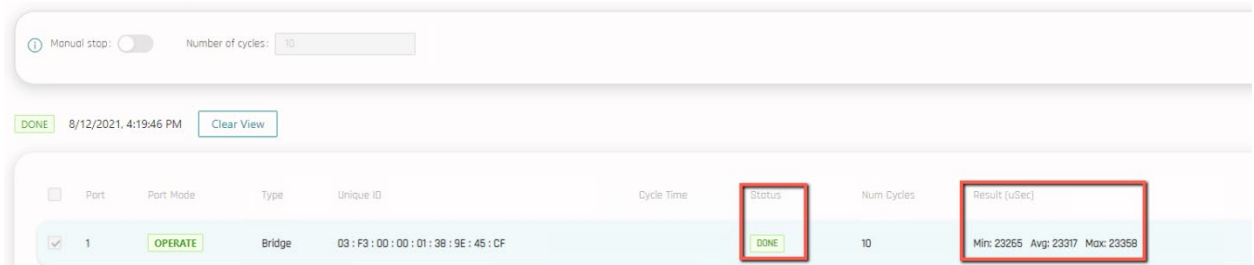


Figure 60: Start Test

8. When the test is finished, the following happen:

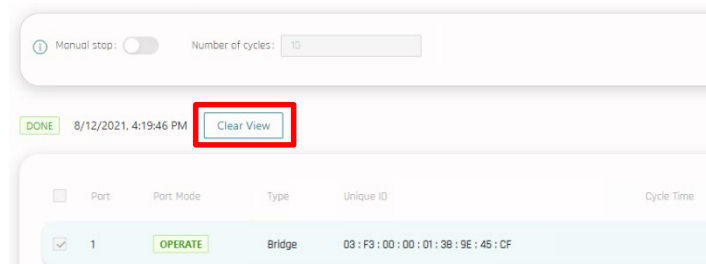
- **Done** appears in the **Status** column of the selected port(s).
- The raw results (in microseconds) appears in the **Result** column of the selected port(s).



**Figure 61: Finished Test**

9. After the test is finished, do one of the following:

- If you want to perform another test, click **Clear View** and repeat from step 3.



**Figure 62: Clear View**

- If you have finished testing, toggle the **Test Mode** switch to the Off position (see Figure 53) to restore operational functionality.



## 15. Statistics View

In **Statistics** view, you can collect and export the following data for each channel of each selected port (w-device):

- **Total** – total number of subcycles in channel
- **CRC Error** – number of CRC errors detected during the cycles
- **Sync Error** – number of sync errors detected during the cycles
- **PER (SubCyc)** –average number of both above errors (CRC + Sync Errors) per sub cycle
- **Avg RSSI(dBm)** – average RSSI taken from all subcycles in channel
- **Min RSSI(dBm)** – minimum RSSI taken from all subcycles in channel
- **Max RSSI** – maximum RSSI taken from all subcycles in channel

### 15.1. Collecting and Exporting Data

1. In **Statistics** view, select the port(s) of the w-devices that you want to collect data on.

The screenshot shows the CoreTigo Engineering Tool interface in the Statistics view. The 'STATISTICS' tab is selected. A table displays the status of various ports. Port 1 is selected, and the 'Collect' button is highlighted.

Port	Port Mode	Type	Unique ID	PER	Cleared on
1	OPERATE	Bridge	03 : F3 : 00 : 00 : 01 : ...	N/A	12 Aug, 14:...
2	INACTIVE				
3	INACTIVE				
4	INACTIVE				
5	INACTIVE				
6	INACTIVE				
7	INACTIVE				
8	INACTIVE				
9	INACTIVE				
10	INACTIVE				
11	INACTIVE				

Channel	Total #	CRC Error #	Sync Error #	PER (SubCyc)	Avg RSSI(dBm)	Min RSSI(dBm)
3	55788	2	0	0.00%	-41	-57
4	55792	0	0	0.00%	-41	-47
5	55795	2	1	0.01%	-42	-47
6	55799	17	0	0.03%	-42	-51
7	55804	1	0	0.00%	-42	-47
8	55807	1	0	0.00%	-41	-52
9	55811	55	1	0.10%	-41	-73
10	55814	1	0	0.00%	-40	-47
11	55818	0	0	0.00%	-40	-46
12	55821	139	1	0.25%	-40	-54
13	55825	0	0	0.00%	-40	-44

Figure 63: Port Selection

2. Click **Collect**.

The screenshot shows the CoreTigo Engineering Tool interface in the Statistics view. The 'Collect' button is highlighted with a red box, indicating it has been clicked. The table below it shows the same data as Figure 63.

Port	Port Mode	Type	Unique ID	PER	Cleared on
1	OPERATE	Bridge	03 : F3 : 00 : 00 : 01 : ...	N/A	12 Aug, 14:...
2	INACTIVE				

Channel	Total #	CRC Error #	Sync Error #	PER (SubCyc)	Avg RSSI(dBm)	Min RSSI(dBm)
3	55788	2	0	0.00%	-41	-57
4	55792	0	0	0.00%	-41	-47

Figure 64: Collect

3. TigoEngine displays the results for each selected port's w-device(s).

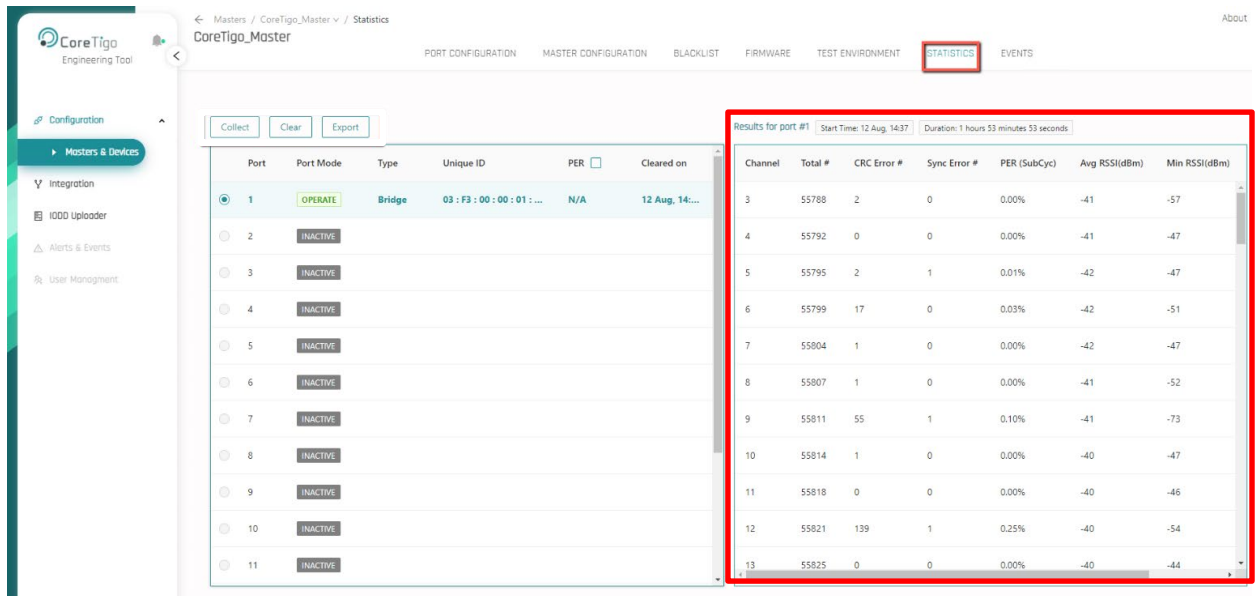


Figure 65: Results – Example

4. If you want to export the results to an Excel file, click **Export**.

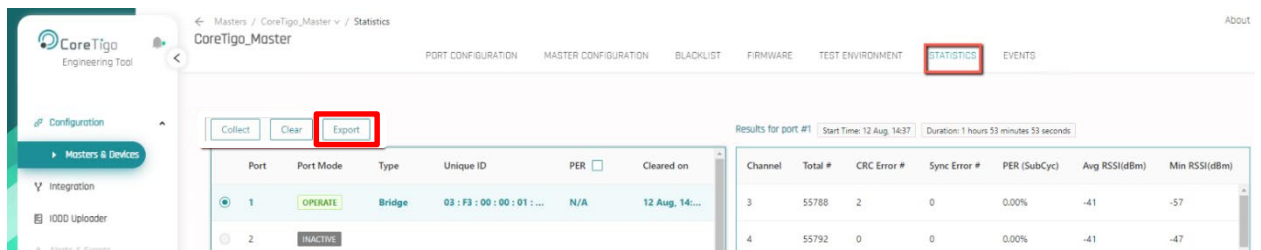


Figure 66: Export

## 16. Events View

In **Events** view, you can see the events and alerts for the w-devices connected to the selected w-master, as defined in the IO-Link spec, and parsed according to the IO-Link spec.

You can filter the list of Events/Alerts by port, event code, event type, and/or event mode.

You can also see events/alerts in the **Events** tab of **Port Configuration** view.

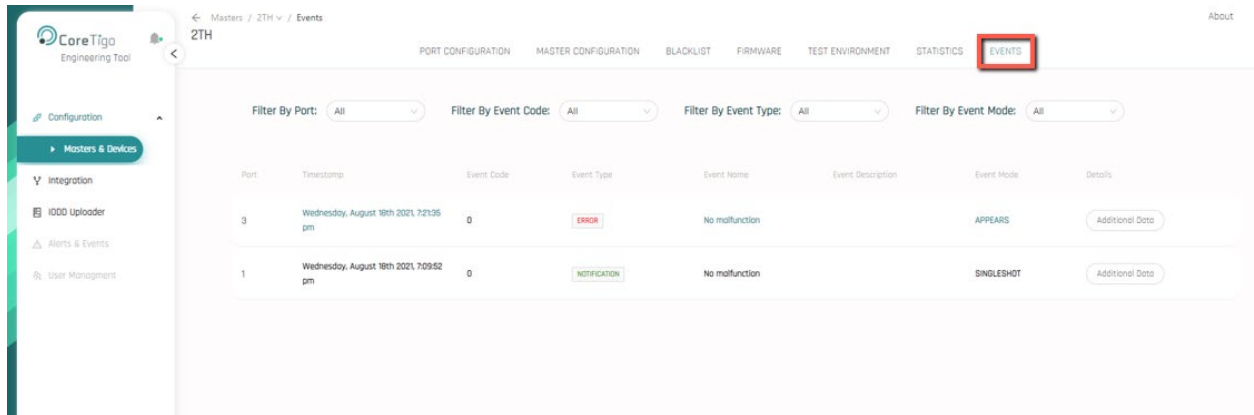


Figure 67: Events View

## 17. Uploading IODD Files

IO-Link devices need to be described by IO-Link Device Descriptions (IODD). IODD are complex structured XML files with numerous restrictions and interdependencies.

TigoEngine provides 2 ways to upload an IODD zip file:

- [Using the IODD Finder to Upload an IODD File](#): see section 17.1
- Using the IODD Uploader: see section 17.2

### 17.1. Using the IODD Finder to Upload an IODD File

1. After pairing a new bridge that is connected to an IO link sensor/actuator, go to **Port Configuration** view > **Details** tab.
2. Click **IODD finder** (under the camera icon).

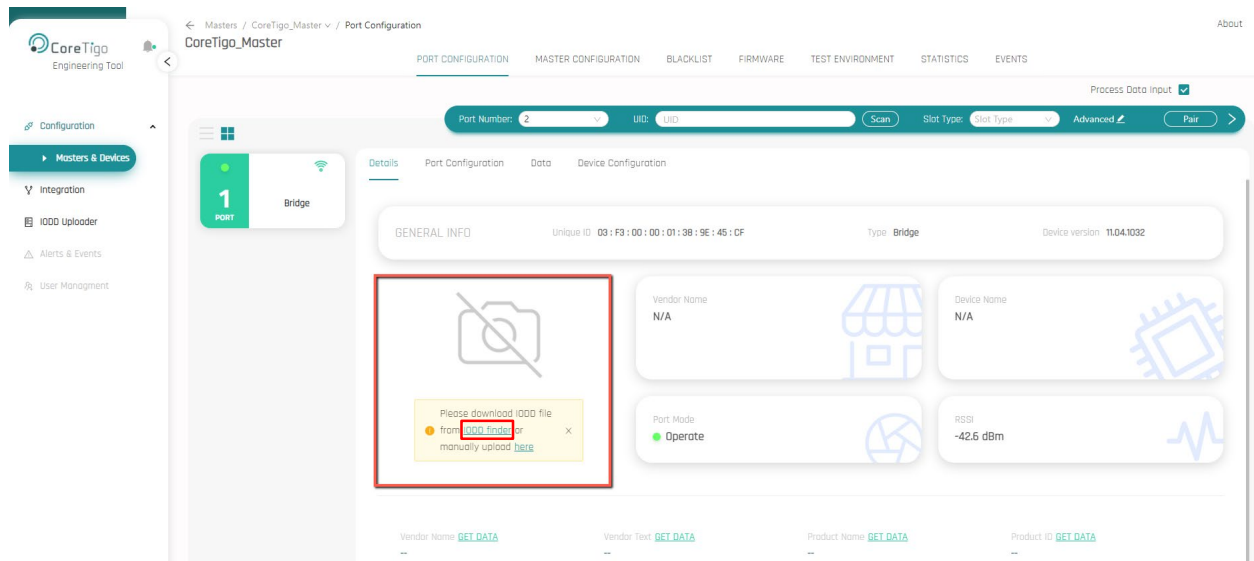
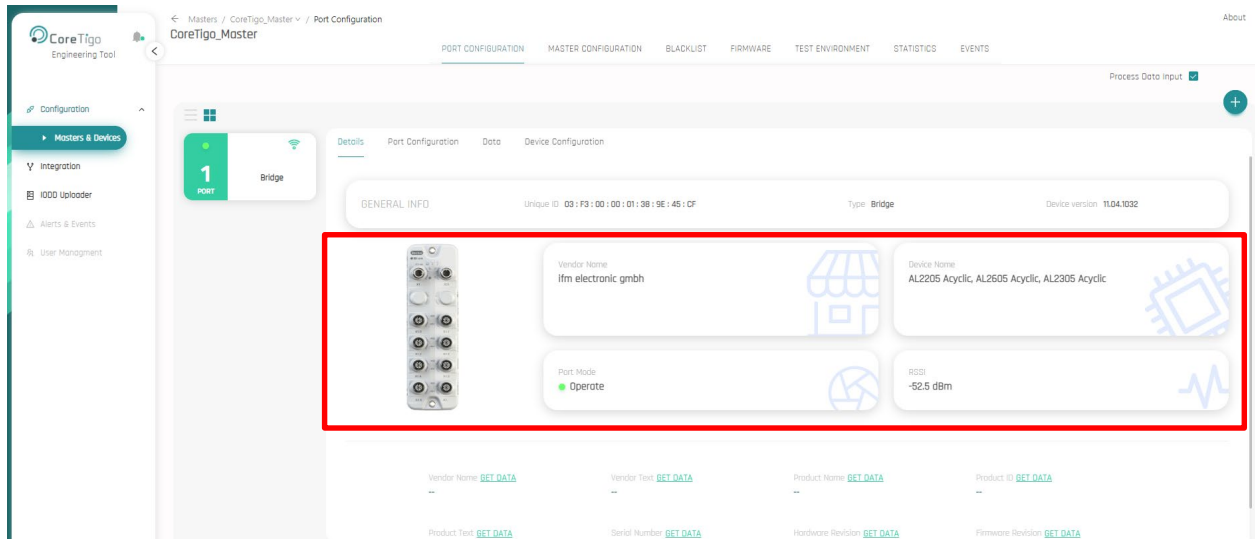


Figure 68: IODD Finder

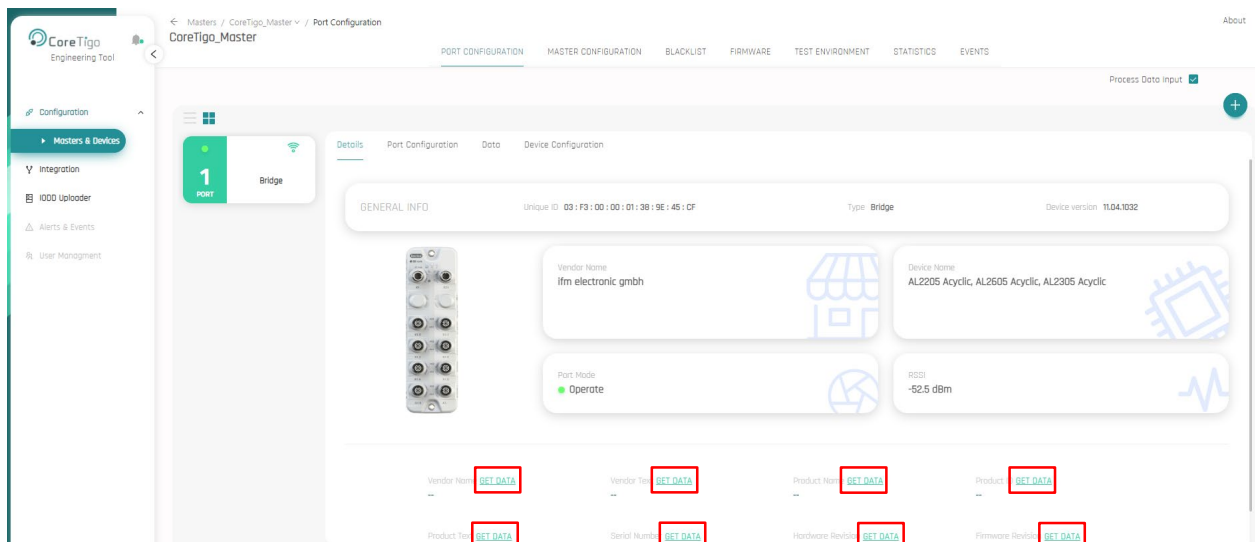
3. TigoEngine displays the following IO-Link sensor/actuator data: device picture, **Vendor Name**, **Device Name**, **Port Mode**, and **RSSI**. All data is taken from the IODD Finder web.



**Figure 69: IODD Finder Results (IO-Link sensor/actuator data) – Example**

4. Click **GET DATA** to display the full IODD, comprising the following:

- Vendor Text
- Product Name
- Product ID
- Product Text
- Serial Number
- Hardware Revision
- Firmware Revision



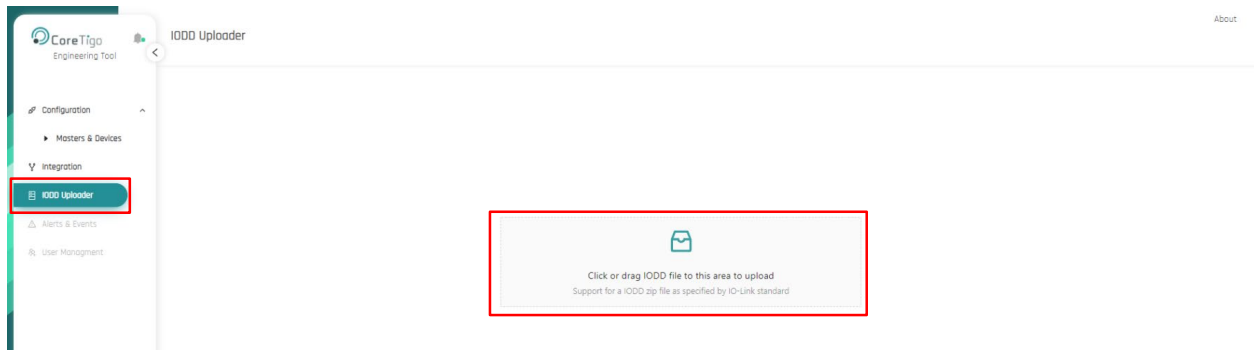
**Figure 70: GET DATA**

Vendor Name <a href="#">GET DATA</a> ifm electronic gmbh	Vendor Text: <a href="#">GET DATA</a> www.ifm.com	Product Name <a href="#">GET DATA</a> AL2605 Acyclic	Product ID <a href="#">GET DATA</a> AL2605
Product Text: <a href="#">GET DATA</a> IO-Link module	Serial Number <a href="#">GET DATA</a> 000011487239	Hardware Revision <a href="#">GET DATA</a> AA	Firmware Revision <a href="#">GET DATA</a> V1.15

**Figure 71: IO-Link Device Description (IODD) – Example**

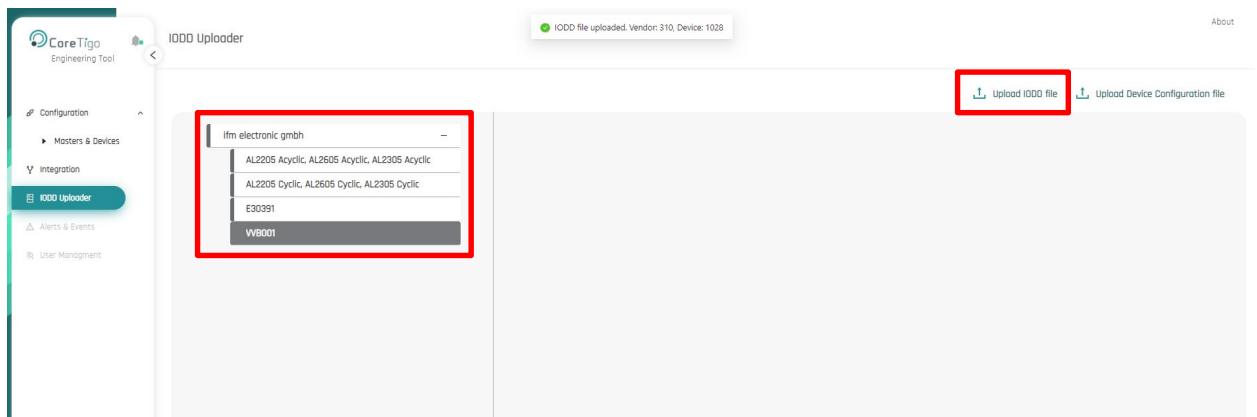
## 17.2. Using the IODD Uploader

1. In the explorer pane select **IODD Uploader**.
2. In the **IODD Uploader** pane, click the upload area.



**Figure 72: IODD Uploader – Upload Area**

3. Browse to the relevant IODD file.
4. Click **Upload IODD file**.



**Figure 73: Browsing to the IODD File and Uploading It**

5. TigoEngine displays the description of the device (IODD).

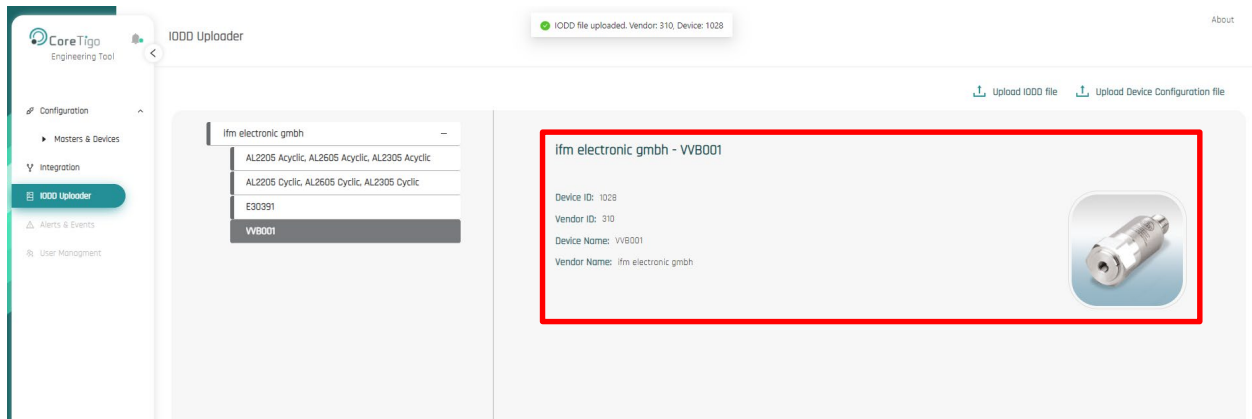


Figure 74: Uploaded Device Description (IODD)

## 18. Integration with an MQTT Broker

1. Make sure that:
  - o An MQTT broker is installed  
[To install an MQTT broker](#), see appendix A.
  - o At least one MQTT user is set up  
[To create an MQTT user](#), see appendix A
2. In the Explorer pane, select **Integration**.
3. In the **Integration** wizard's **Configuration** screen, do the following:
  - a. Set **Integration name** as desired.
  - b. Set **Integration type** = **MQTT**.
  - c. Click **Save and Continue**.

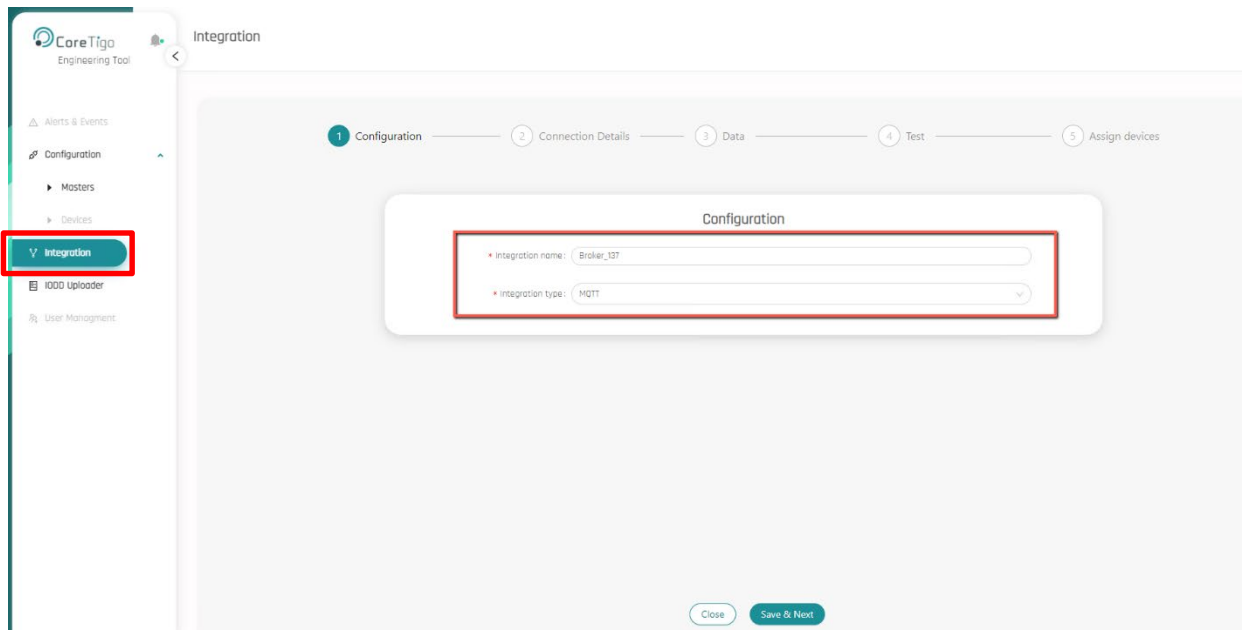


Figure 75: Configuration Screen (Integration Wizard)

4. In the **Connection Details** screen, under **Protocol Configuration** set:
  - o **Host** = <host IP /host name>
  - o **Port** = <port number>
  - o **Quality of service** = **At most once**
  - o **Client Id** = <client identifier>
  - o **Keep alive** = **50**
5. Under **Authentication**, set:
  - o **Authentication method** = **Username and password**
  - o **Username** = <user name of the account>
  - o **Password** = <password for the account>
6. Under **Topics (Structure of Data Received)**, make sure the following are selected:



- **Master ID**
- **Vendor ID**
- **Device ID**
- **Port**
- **Device UUID**

7. Click **Save and Continue**.

Configuration 2 Connection Details 3 Data 4 Test 5 Assign device

### Protocol Configuration

\* Host: 192.168.10.127

\* Port: 1883

\* Quality of service: At most once

\* Client id: 9952fce5-e8e5-4c22-bae1-3237f08ca50  Auto generated

\* Keep alive: 60 Seconds

Retain message:

Will message:

### Authentication

\* Authentication method: Username and password

Username: customer\_success Password: .....

### Topics (Structure of data received)

\* Topic: Preview: /<code>{</code>master\_id/</code>=</code>{</code>vendor\_id/</code>=</code>{</code>device\_id/</code>=</code>{</code>port/</code>=</code>{</code>...</code>

Close Back Save & Next

**Figure 76: Connection Details Screen (Integration Wizard)**

8. In the **Data** screen, under **Type and Format** set **Data Format = Raw data**.
9. Under **Publishing** set:
  - **Publishing rate = 1000 milliseconds**
  - **Maximum messages = 10**
10. Click **Save and Continue**.

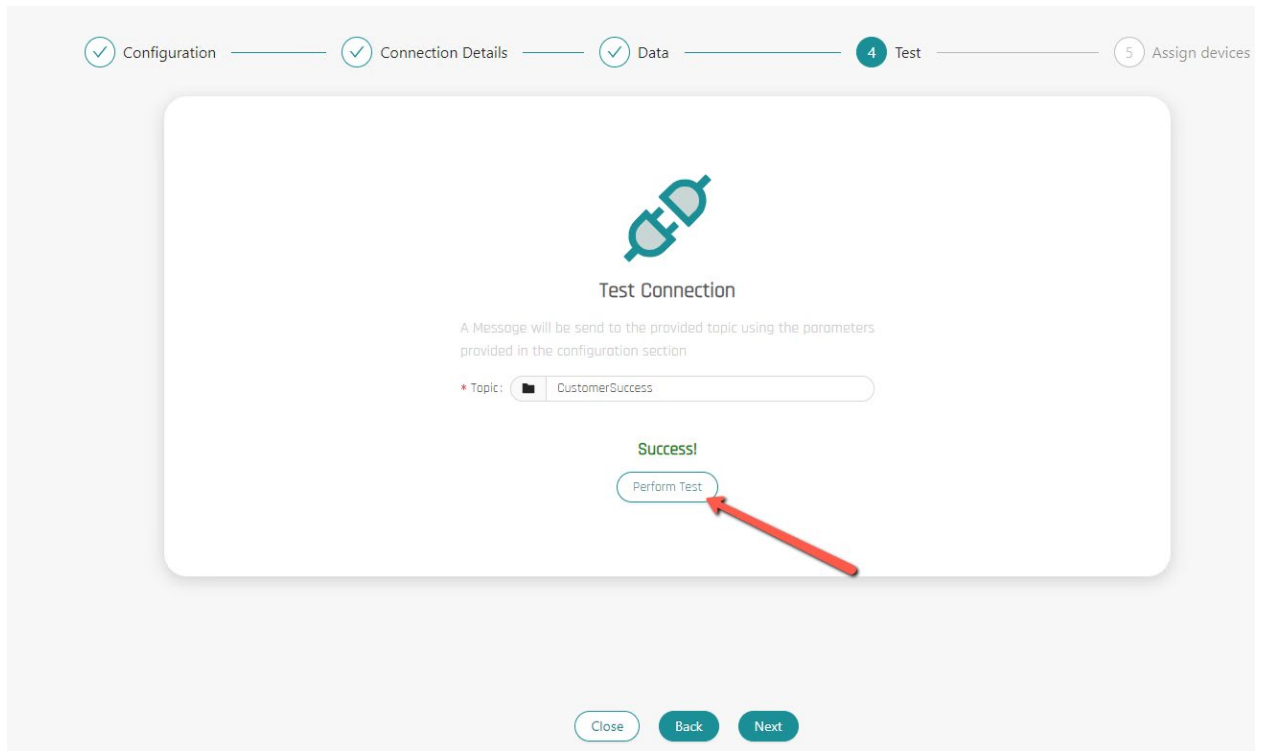
The screenshot displays the 'Data' screen of the Integration Wizard. At the top, a progress bar shows five steps: Configuration, Connection Details, Data (current step), Test, and Assign devices. The 'Data' section is divided into two main areas:

- Type & Format:** A dropdown menu for 'Data format' is set to 'Raw data'. Below it is a 'Preview' button.
- Publishing:** A 'Publishing rate' input field is set to '1000' with 'milliseconds' as the unit. Below it, a 'Maximum messages' input field is set to '10'.

**Figure 77: Data Screen (Integration Wizard)**

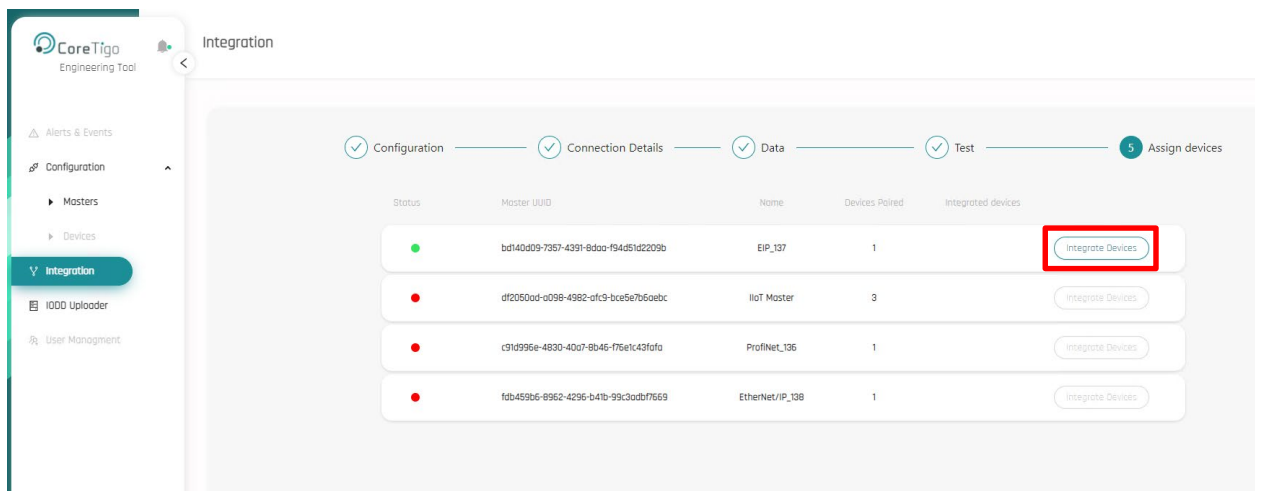
11. In the **Test** screen, click **Perform Test** and then do one of the following:

- If the result of the test is **Success!**, then click **Next**.
- If the result of the test is **Failure!**, then click **Back**, check and modify the entered details as required, and repeat the test.



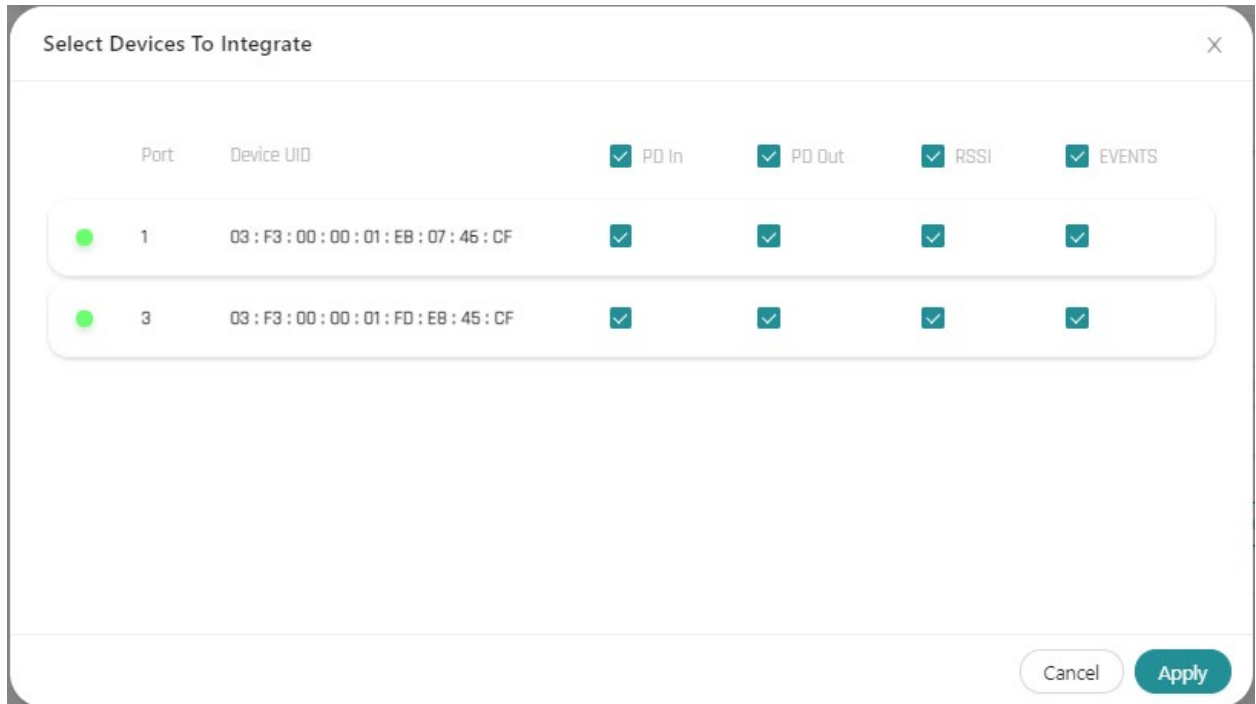
**Figure 78: Test Connection Screen (Integration Wizard)**

12. In the **Assign Devices** screen, click **Integrate Devices**.



**Figure 79: Assign Devices Screen (Integration Wizard) – Integrate Devices Button**

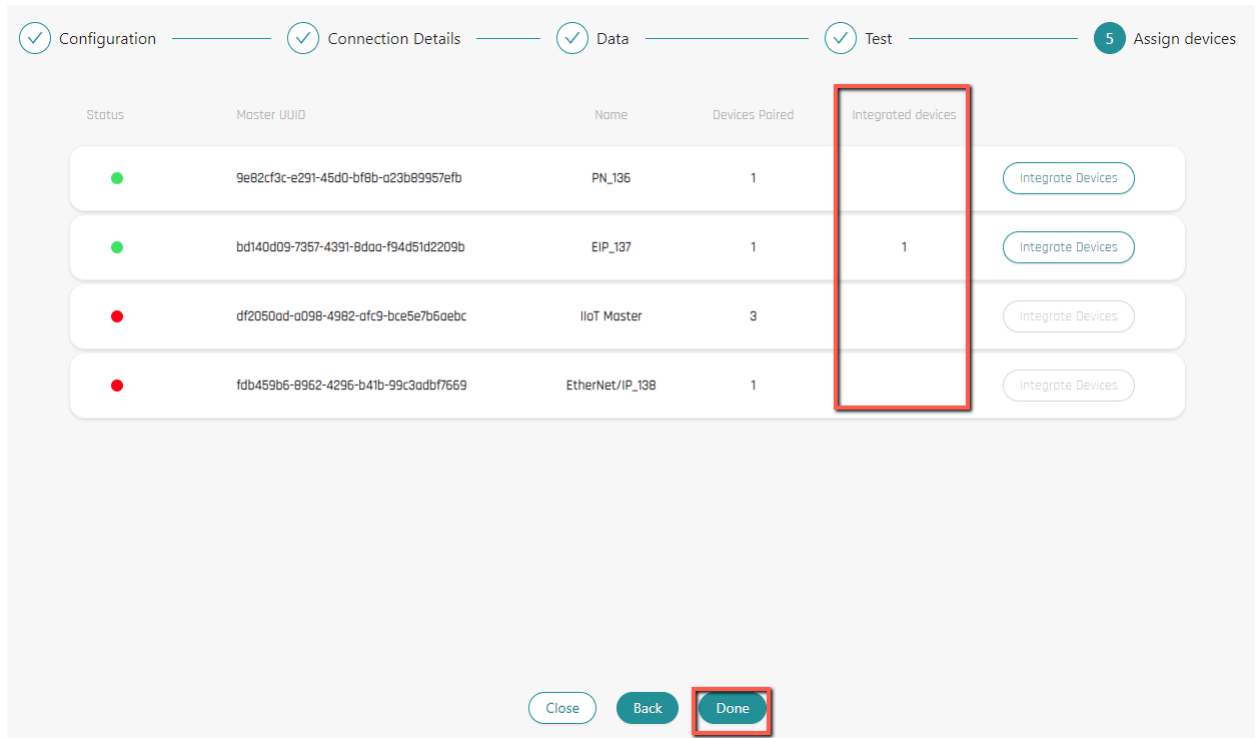
13. In the **Select Devices to Integrate** window, do the following:
- Select the desired data types (**PD In**, **PD Out**, **RSSI**, and/or **Events**).  
Note that when you select a specific data type, this automatically also selects the device(s) that have that data type.
  - Click **Apply**.



**Figure 80: Select Devices to Integrate**

14. In the **Assign Devices** screen, do the following:

- a. Make sure that **1** appears in the **Integrated devices** column of each device that was selected in the previous step.
- b. Click **Done**.



**Figure 81: Integrated Devices**

# 19. Troubleshooting

Problem	Probable Cause	Solution
Cannot access TigoEngine from a remote PC	The PC running TigoEngine is in a public network. Therefore, Windows blocks the network's access to web applications running on the PC.	Change the network definition to private
Firmware upgrade fails		Click <b>Clear</b> and repeat the firmware upgrade procedure
Integration with MQTT broker fails	One or more broken topics	Use MQTT Explorer (or another MQTT client) to find the broken topics: see section 19.1

## 19.1. Troubleshooting with MQTT Explorer

MQTT Explorer enables you to find broken topics that are preventing integration with an MQTT broker. You can download it from <http://mqtt-explorer.com/>.

To find broken topics:

1. In MQTT Explorer, set the **MQTT Connection** fields as shown in Figure 82.

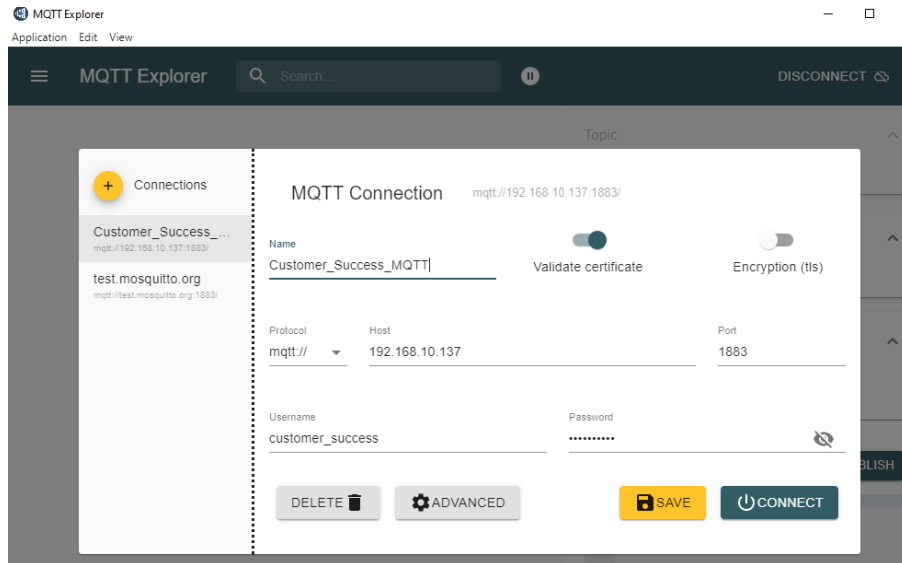


Figure 82: MQTT Explorer – Connection Settings

2. Click **Connect**.

3. MQTT lists the broken topic(s).

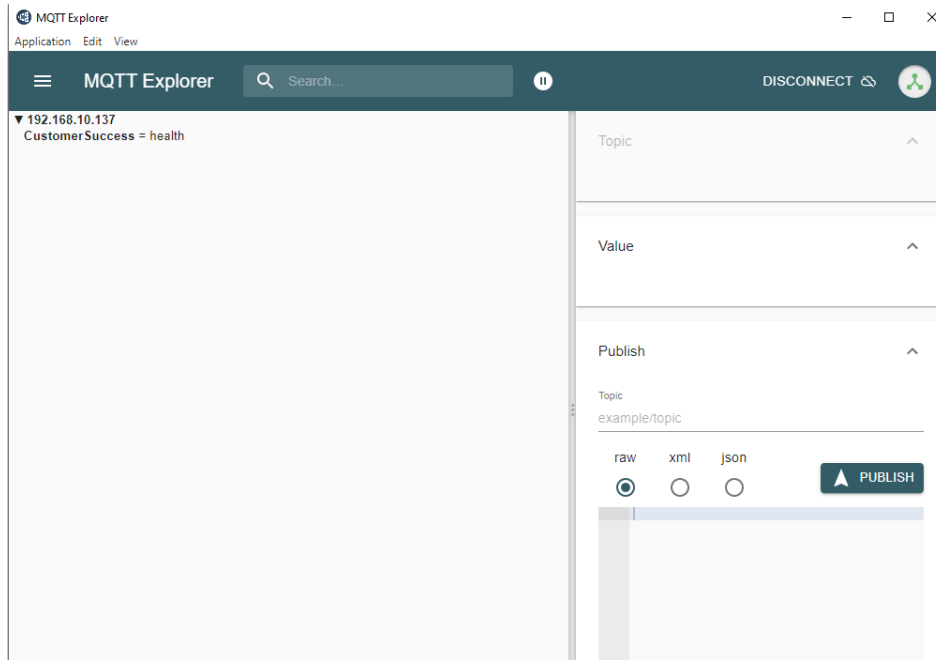


Figure 83: Broken Topic List

4. Expand the listed topic(s) to see details.

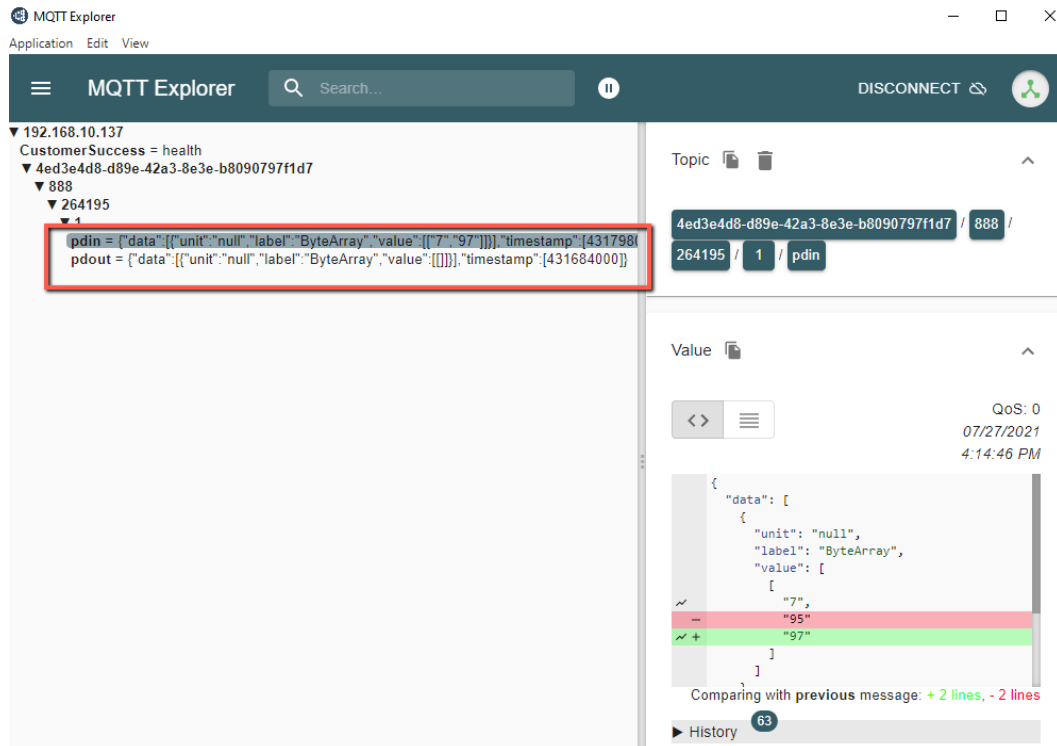


Figure 84: Expanded Topic

# Appendix A – Working with MQTT

To use TigoEngine with MQTT, you need an MQTT broker. This appendix describes how to [install RabbitMQ](#) and [create MQTT users](#) with RabbitMQ or Command Prompt.

To integrate MQTT with TigoEngine see section 18

## Installing RabbitMQ

1. Install **Erlang otp\_win64\_24.0.2** or higher.

You can download otp from <https://www.erlang.org/downloads>

2. Install **rabbitmq-server-3.8.17** or higher.

You can download rabbitmq-server from <https://www.rabbitmq.com/download.html>

3. In **Command Prompt**, run: `cd c:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.17\sbin`

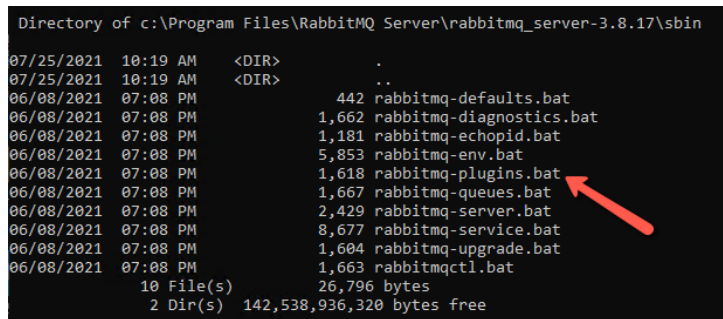


Figure 85: Directory of c:\Program Files\RabbitMQ Server\rabbitmq\_server-3.8.17\sbin

4. Write on command prompt: `rabbitmq-plugins.bat enable rabbitmq_management`

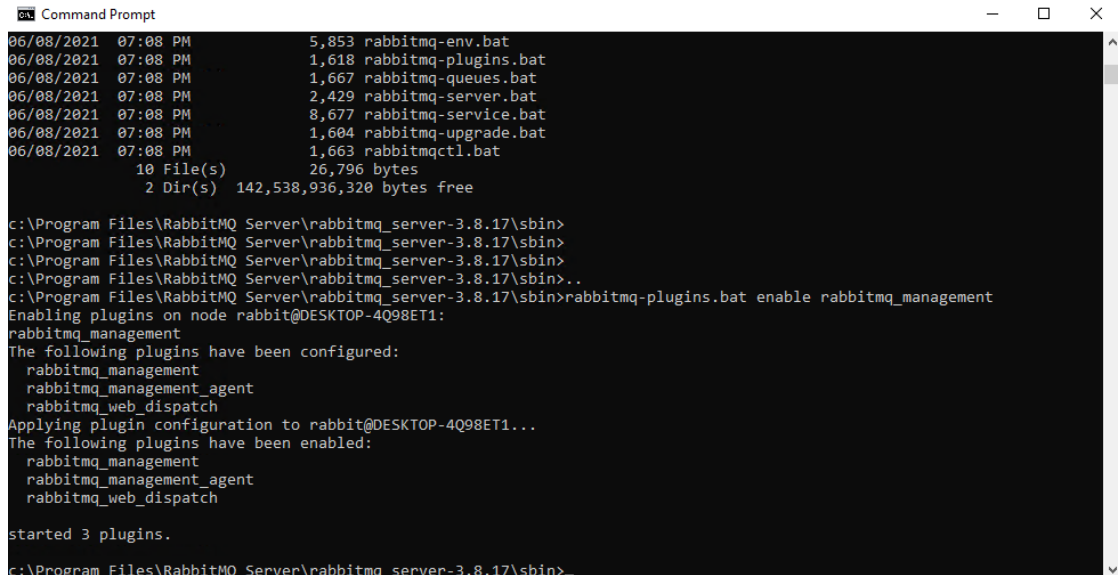


Figure 86: Command Prompt: `rabbitmq-plugins.bat enable rabbitmq_management`

5. Run the command prompt: `rabbitmq-plugins enable rabbitmq_mqtt`
6. When the configuration is complete, make sure that the message **started 1 plugins** has been received.



```
c:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.17\sbin>rabbitmq-plugins enable rabbitmq_mqtt
Enabling plugins on node rabbit@DESKTOP-4Q98ET1:
rabbitmq_mqtt
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_mqtt
  rabbitmq_web_dispatch
Applying plugin configuration to rabbit@DESKTOP-4Q98ET1...
The following plugins have been enabled:
  rabbitmq_mqtt
started 1 plugins.
```

Figure 87: Message started 1 plugins Received

- 7. Run the command: `rabbitmq-plugins list` and check that `rabbitmq_mqtt` is in the resulting list.

```
c:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.17\sbin>rabbitmq-plugins.bat list
Listing plugins with pattern "*" ...
Configured: E = explicitly enabled; e = implicitly enabled
| Status: * = running on rabbit@DESKTOP-4Q98ET1
|/
[ ] rabbitmq_amqp1_0          3.8.17
[ ] rabbitmq_auth_backend_cache 3.8.17
[ ] rabbitmq_auth_backend_http  3.8.17
[ ] rabbitmq_auth_backend_ldap  3.8.17
[ ] rabbitmq_auth_backend_oauth2 3.8.17
[ ] rabbitmq_auth_mechanism_ssl  3.8.17
[ ] rabbitmq_consistent_hash_exchange 3.8.17
[ ] rabbitmq_event_exchange     3.8.17
[ ] rabbitmq_federation         3.8.17
[ ] rabbitmq_federation_management 3.8.17
[ ] rabbitmq_jms_topic_exchange  3.8.17
[E*] rabbitmq_management        3.8.17
[e*] rabbitmq_management_agent  3.8.17
[E*] rabbitmq_mqtt              3.8.17
[ ] rabbitmq_peer_discovery_aws  3.8.17
[ ] rabbitmq_peer_discovery_common 3.8.17
[ ] rabbitmq_peer_discovery_consul 3.8.17
[ ] rabbitmq_peer_discovery_etcd  3.8.17
[ ] rabbitmq_peer_discovery_k8s  3.8.17
[ ] rabbitmq_prometheus          3.8.17
[ ] rabbitmq_random_exchange     3.8.17
[ ] rabbitmq_recent_history_exchange 3.8.17
[ ] rabbitmq_sharding            3.8.17
[ ] rabbitmq_shovel              3.8.17
[ ] rabbitmq_shovel_management  3.8.17
[ ] rabbitmq_stomp               3.8.17
[ ] rabbitmq_top                 3.8.17
[ ] rabbitmq_tracing             3.8.17
[ ] rabbitmq_trust_store         3.8.17
[e*] rabbitmq_web_dispatch       3.8.17
[ ] rabbitmq_web_mqtt            3.8.17
[ ] rabbitmq_web_mqtt_examples  3.8.17
[ ] rabbitmq_web_stomp           3.8.17
[ ] rabbitmq_web_stomp_examples  3.8.17
```


Figure 88: rabbitmq-plugins list Featuring rabbitmq\_mqtt

## Creating MQTT Users

You can create MQTT users in either of the following ways:

- [Using Command Prompt](#)
- [Using RabbitMQ](#)

---

 This section uses the example of creating (adding) a user whose **Username** is **User** and whose **Password** is **Pass**. However, you can create users who have any **Username** and **Password** that you want.

---

### Using Command Prompt to Create an MQTT User

In **Command Prompt**, enter the following;

- `rabbitmqctl add_user "User" "Pass"`
- `rabbitmqctl set_permissions -p / "User" ".*" ".*" ".*"`
- `rabbitmqctl set_user_tags "User" management`

### Using RabbitMQ to Create an MQTT User

1. Go to <http://XXX.XXX.XXX.XXX:15672>, where XXX.XXX.XXX is the MQTT broker IP address.
2. Log in with the following:
  - **Username = User**
  - **Password = Pass**
3. Click the **Admin** tab.
4. Expand the **Add a user** section of the tab.

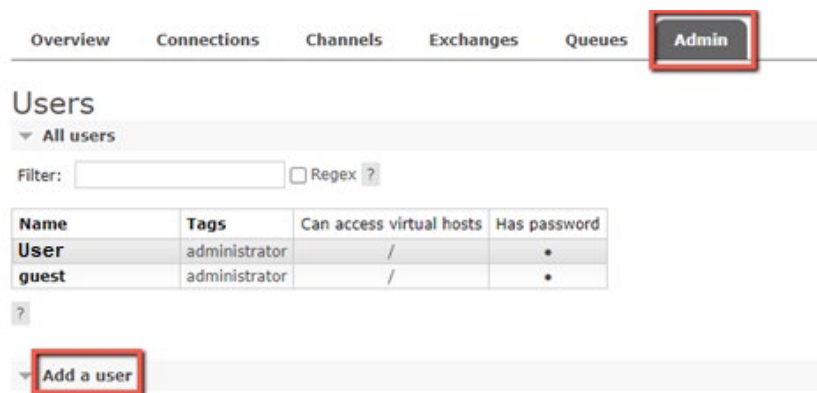


Figure 89: Admin Tab

5. In the **Add a user** section, do the following:
  - a. Set **Username** = **User**
  - b. Set **Password** as desired.
  - c. Click **Add user**.

Overview Connections Channels Exchanges Queues **Admin**

### Users

▼ All users

Filter:   Regexp ?

Name	Tags	Can access virtual hosts	Has password
User	administrator	/	•
guest	administrator	/	•

?

▼ **Add a user**

Username:

Password:  (confirm)

Tags:

Set Admin | Monitoring | Policymaker  
Management | Impersonator | None

**Add user**

Figure 90: Adding a User

## Appendix B – TigoEngine Installation using Docker

For Windows machine follow steps below:

1. Ensure you have docker installed. If not, a windows user may follow steps below:
  - a. Download and run Docker Desktop for Windows: [Installer.exe](#)
  - b. Download and install the [WSL2 Linux kernel update package for x64 machines](#)
  - c. Open PowerShell and run the following command to set WSL 2 as the default version when installing a new Linux distribution:  
`wsl --set-default-version 2`  
  
**NOTE:** In case this step fails, enable Hyper-V feature under ``turn windows features turn on/off``
  - d. Restart the computer
  - e. To ensure docker engine is running properly, open cmd and run the following command:  
`docker version`
2. Download [AWS Command Line Interface](#)
3. Open cmd and run the following command:  
`C:\> msixexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi`
4. Still on cmd, run the command: `aws configure` then press **Enter**.
5. In the next step, the AWS CLI outputs lines of text, prompting you to enter additional information: AWS Access Key ID, AWS Secret Access Key, Default Region Name and Default Output Format. You can find this information in the certificate package shared with you by CoreTigo.

Using the credentials received from CoreTigo, follow the next steps:

- a. Fill in the **AWS Access Key ID**, then press **Enter**.
- b. Fill in the **AWS Secret Access Key**, then press **Enter**.
- c. Fill in the **region name**, in the format as shown below in the example, then press **Enter**.
- d. When asked to fill in **output format**, leave it empty and just press **Enter**.

### Example:

#### AWS configure

AWS Access Key ID [None]: `ABCDEFGHIJK`

AWS Secret Access Key [None]: `AbCdEFghiJK/AbCdEFghiJK/AbCdEFghiJK`

Default region name [None]: `eu-west-1`

Default output format [None]: **leave empty and press Enter**

1. Run the following command:  
`aws.exe ecr get-login-password --region eu-west-1 | docker login --username AWS --password-stdin 530412914495.dkr.ecr.eu-west-1.amazonaws.com`

**NOTE:** If you copy the command from this manual, pay attention to have everything on ONE line, otherwise the command would consider the line break as “Enter” and the command wouldn’t work properly.

2. Open cmd and run the following command: `Set VER=x.x` (x.x is the version of TigoEngine. For example '3.2')
3. Copy the docker compose file to a directory of your choice (directory will be created containing data for the database). Ensure it has permission to write on.
4. Open cmd and navigate to the folder selected in the previous step. Then run the command:  
`docker-compose up -d`
5. Once process completed successfully, open browser and navigate to TigoEngine site:  
<http://localhost:9000>

## Appendix C – Setting IP Address with the BOOTP/DHCP Tool

The TigoMaster 2TH is delivered without a preset IP address. On startup, it sends requests to a DHCP server to get an IP address. If the network includes a DHCP server, you can use the BootP/DHCP tool to set an IP Address, as follows:

1. Make the following preparations.
  - Download the BootP/DHCP tool version 3.05 and above.
  - Note the hardware (MAC) address of the TigoMaster 2TH.  
The hardware address is on a sticker on the side of the TigoMaster 2TH and has a format similar to the following: 00-00-BC-14-55-35.
  - Make sure that the TigoMaster 2TH is installed on the relevant EtherNet/IP network.
  - Make sure that the workstation that you use to set the IP address has only one connection to the EtherNet/IP network on which the TigoMaster 2TH is installed.  
If the workstation has multiple connections to the EtherNet/IP network, the BootP-DHCP tool might fail to work.
  - Make sure that the TigoMaster 2TH is powered up.
2. Start the BOOTP/DHCP tool.

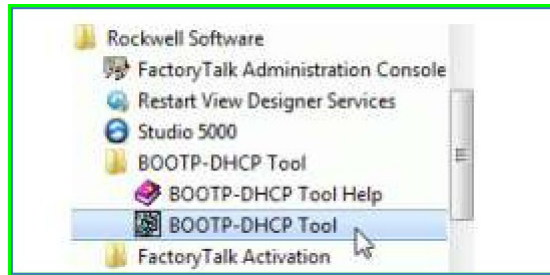


Figure 100: Starting the BOOTP/DHCP Tool

The BOOTP/DHCP tool displays the **Discovery History** pane, listing all devices found in the local network.

3. In the **Ethernet Address (MAC)** column of the **Discovery History** pane, find the MAC address that you noted in step 11 and select its row.

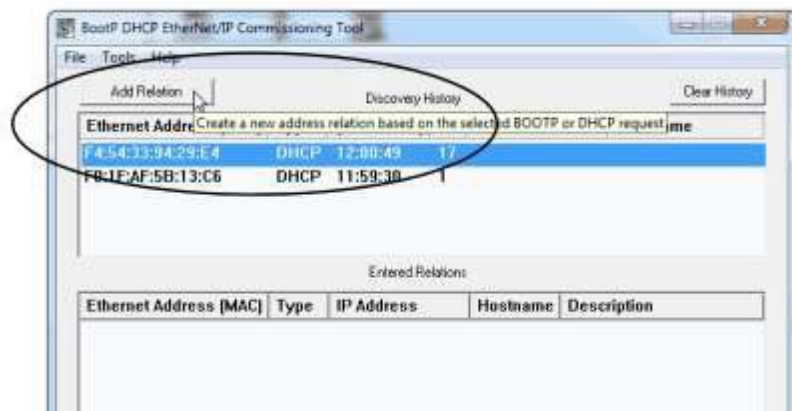
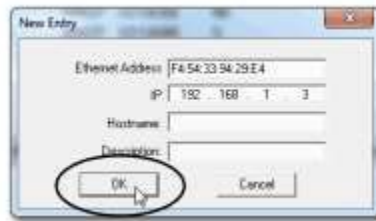


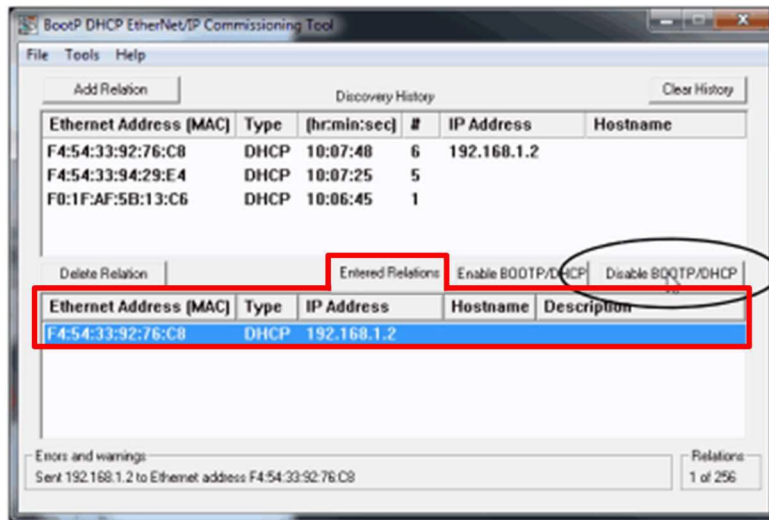
Figure 101: Discovery History

4. Click **Add Relation**.  
The **New Entry** dialog box appears.
5. In the **New Entry** dialog box, do the following:
  - a. Set the **IP address** as appropriate..
  - b. If desired, set the **Hostname** and **Description**.
  - c. Click **OK**.



**Figure 102: New Entry**

6. Wait for the MAC address and IP address of the TigoMaster 2TH to appear in the **Entered Relations** pane, and select their row.
7. Click **Disable BOOTP/DHCP**.



**Figure 103: MAC Address and IP Address of TigoMaster 2TH in Entered Relations Pane**



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

The TigoMaster 2TH now uses the assigned IP address and does not issue BOOTP or DHCP requests after power is cycled on the controller.

## Appendix D – 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.

## 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.

1. **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.

## 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.

- 1. 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.
- 2. 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.
- 3. 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.

- 4. 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.

## Term and Termination

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.
  2. Either party shall have the right to terminate this Agreement upon 7 days' prior written notice to the other party.
  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.
  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.
  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.
- 5. 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 and 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.