# Overview of the system

The Wittra devices form a wireless **mesh network** over the Sub-GHz RF band. Sensor and positioning data is collected by the IoT devices and posted to the cloud. The data can easily be accessed via our **Wittra portal** by adding an integration; For further information please have a look at **Accessing your data**.

# Wittra IoT Devices

A Wittra system is composed of several different devices:

- **The Gateway** is the link between the wireless network and the Internet. It is mains-powered, and communicates securely with both the IoT devices and the cloud. Inside the Gateway resides a component called the Border Router, in charge of all wireless communication within the IoT network.
- **Mesh Routers (MRs)** are wireless range-extenders. They relay data wirelessly over the mesh network. They are also used as anchor for RSSI positioning. They are always-on, and as such, require external power.
- **Positioning Beacons (PBs)** are used as anchor for both RSSI and Time-of-Flight positioning. Like mesh routers, they are always-on, and as such, require external power.
- **TrakSense360s** are battery-powered sensors that can be positioned using RSSI (against mesh routers and positioning beacons) and/or Time-of-Flight (against positioining beacons).

The Wittra product suite includes the devices above and more, including click-on sensors and accessories. Read more about our products **here**.

# Positioning and Sensing

TrakSense360 have built-in tracking and sensing capabilities. They can also be extended with external click-on sensors, with specialized sensor elements. For tracking, TrakSense360 relies on and combines two technologies:

- **RSSI** (Received Signal Strength Indicator) positioning is achieved by measuring the radio signal strength between the device and surrounding Mesh Routers or Positioning Beacons. The information is then posted and used for trilateration. The drawback with RSSI positioning is it is not accurate if the distance between tag and measuring infrastructure is too large (typically not more than 15 metres or so).
- **ToF** (Time-of-Flight) positioning is based on a series of send-receive (ping-pong) sessions between the device and surrounding Positioning Beacons (NB: Mesh Routers are not able to participate to ToF). The propagation delay of the wireless signal is measured, posted, and used again for trilateration; sometimes in combination with RSSI data. This is much more difficult to do than measuring RSSI signals, but the advantage is consistent accuracy over much larger distances. As an example, the Wittra network has

shown an accuracy of plus/minus a few metres at a distance of 100 metres from the network infrastructure.

**NB: ToF is only available in the EU at the time of writing (Feb 2022); with US support expected to come within months.**

Depending on the local environment, you can expect better than ±10 metres accuracy in general, and even ±5 metres most of the time outdoors or in an office environment.

**WiPE** (Wittra Intelligent Positioning Engine) is a service that runs on the Gateway. WiPE takes all the RSSI and ToF timing data and combines it to produce a unique Latitude / Longitude coordinate (plus height) for each TrakSense360, each time a position update is requested by the TrakSense360 device. (There are advantages in combining both RSSI and ToF data together for improved accuracy and consistency). This coordinate is then transported to the specified data End Point (either the Wittra portal or a third party computing resource) where it can be displayed on a map GUI.

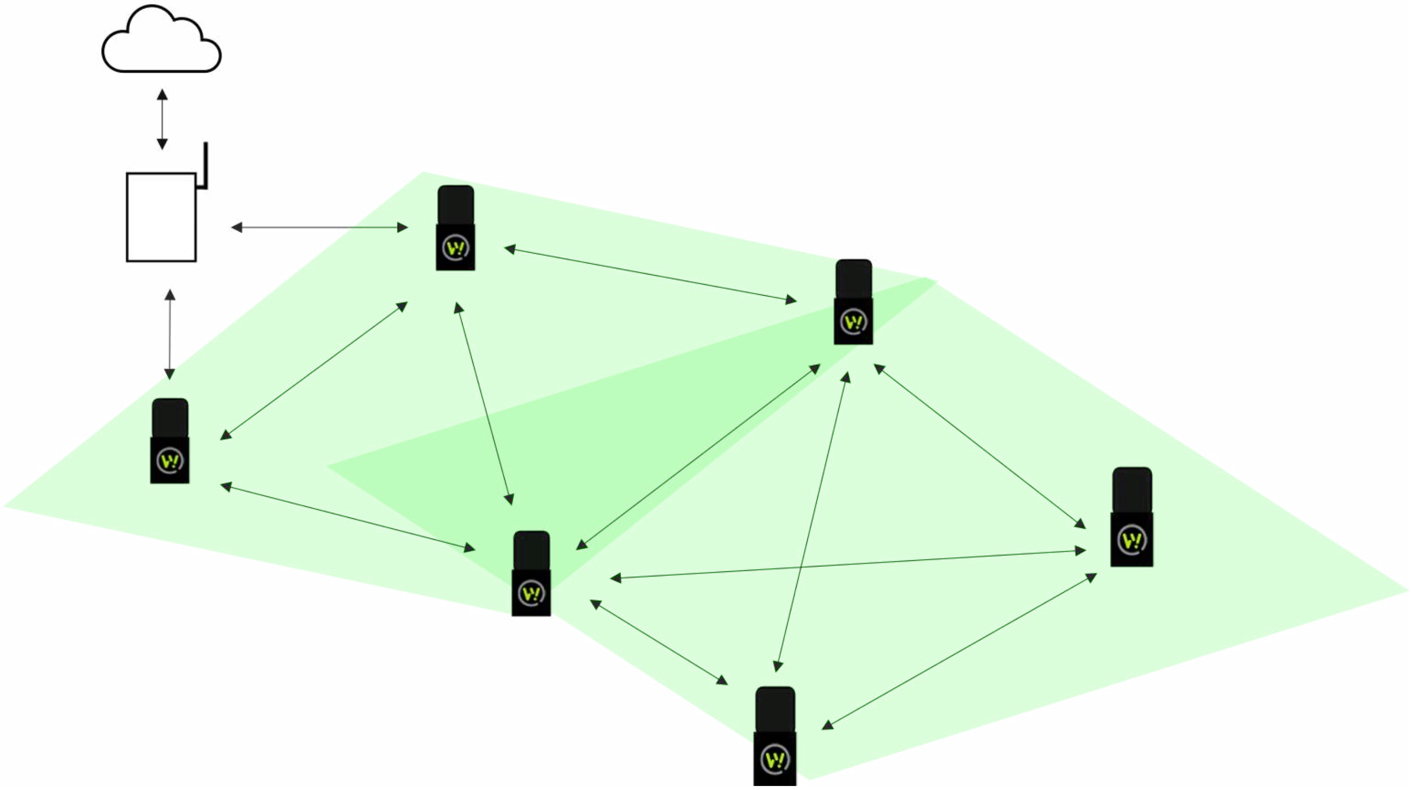
Read more about positioning **here**.

# Networking

The Wittra IoT network is built on standard protocols. Devices run IPv6 for low-power wireless network, via 6LoWPAN. Routing is achieved with RPL and frequency hopping through Wi-SUN and IEEE 802.15.4g. At the application layer, CoAP is used from tag to gateway.

Read more about networking standards **here**.

## Mesh Network



In a mesh network, data can be routed from one node to another to reach the end destination (in our case a gateway). By using a mesh network we extend the range of a network further than one single hop. Mesh networks are self-healing and redundant in the sense that data can be re-routed when nodes fail along the path. We currently support networks up to 500 devices.

In our mesh network we have TrakSense360, mesh-routers, positioning beacons, and a border-router (attached to the gateway).

- A TrakSense360 is a battery-powered leaf node in the mesh network. It collects sensor data and positioning information (RSSI and/or Time-of-Flight), posts these to the cloud via the gateway, and goes back to sleep.
- A mesh-router has the main purpose of forwarding data packets, which is useful for range extension. Additionally, it can be used as an anchor for RSSI positioning. Mesh routers are always-on and listening for data to forward and for positioning probes.
- A positioning beacon is an anchor for both RSSI and Time-of-Flight posititioning. It is always-on and listening for positioning probes.
- A border-router sits inside a gateway. It is the end destination of data packets in a mesh network. The border-router conveys the data to the gateway which then sends the data up securely, via HTTPS, to our backend.

Read more about networking **here**.

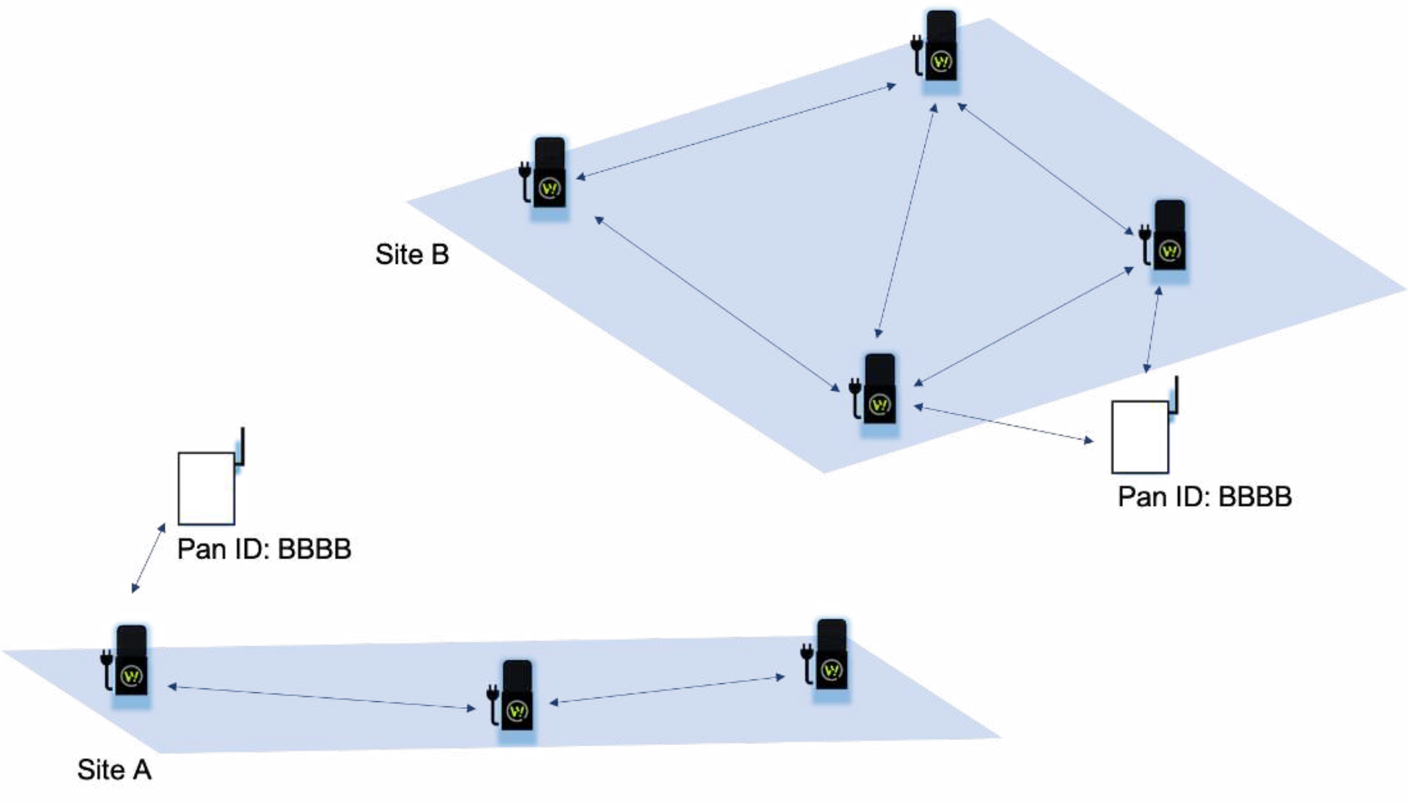
## Frequency Hopping

Our solution operates in the Sub-GHz frequency band, and uses Frequency Hopping (FH) for increased reliability. The devices switch frequency several times per second, to mitigate the impact of any individual bad channel. When a transmission fails on a bad channel, new attempts will be performed over different channels, increasing the likelihood to eventually succeed.

Note that the Sub-GHz band is much less prone to interference than the 2.4 GHz band, since there are fewer products on the market that uses this spectrum and at the same time government regulations impose limits on the radio usage per device. However, interference still exists and that is why FH is key to building robust networks.

## Network PAN ID

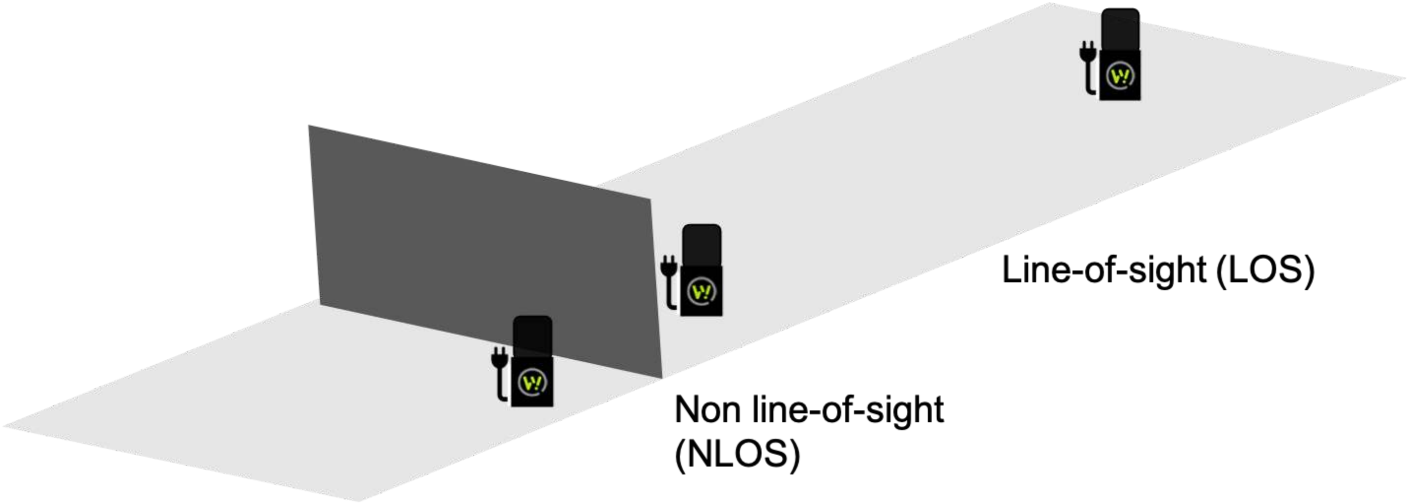
The PAN ID is a unique ID for a group of physically co-located IEEE 802.15.4 devices, each local network should have its own ID. Networks near each other mustn't have the same PAN ID. It is randomly selected at deployment but can be changed at any point of time in the **Wittra portal**. The PAN ID can be used to connect two networks, so a TrakSense360 can move in between sites.



## Expected range

The radio in Wittra devices runs Sub-GHz in the industrial, scientific and medical (ISM) frequency band. By communicating in this frequency domain you have a better range than for example the higher frequency band of 2.4 GHz. You also have a better penetration meaning you can communicate in harsher radio environments such as construction sites and in cities, where line of sight is not an option.

The expected range of the system depends if you have line of sight or non-line of sight and how high up you can put the mesh-routers. But in average the range is around 100-200m.



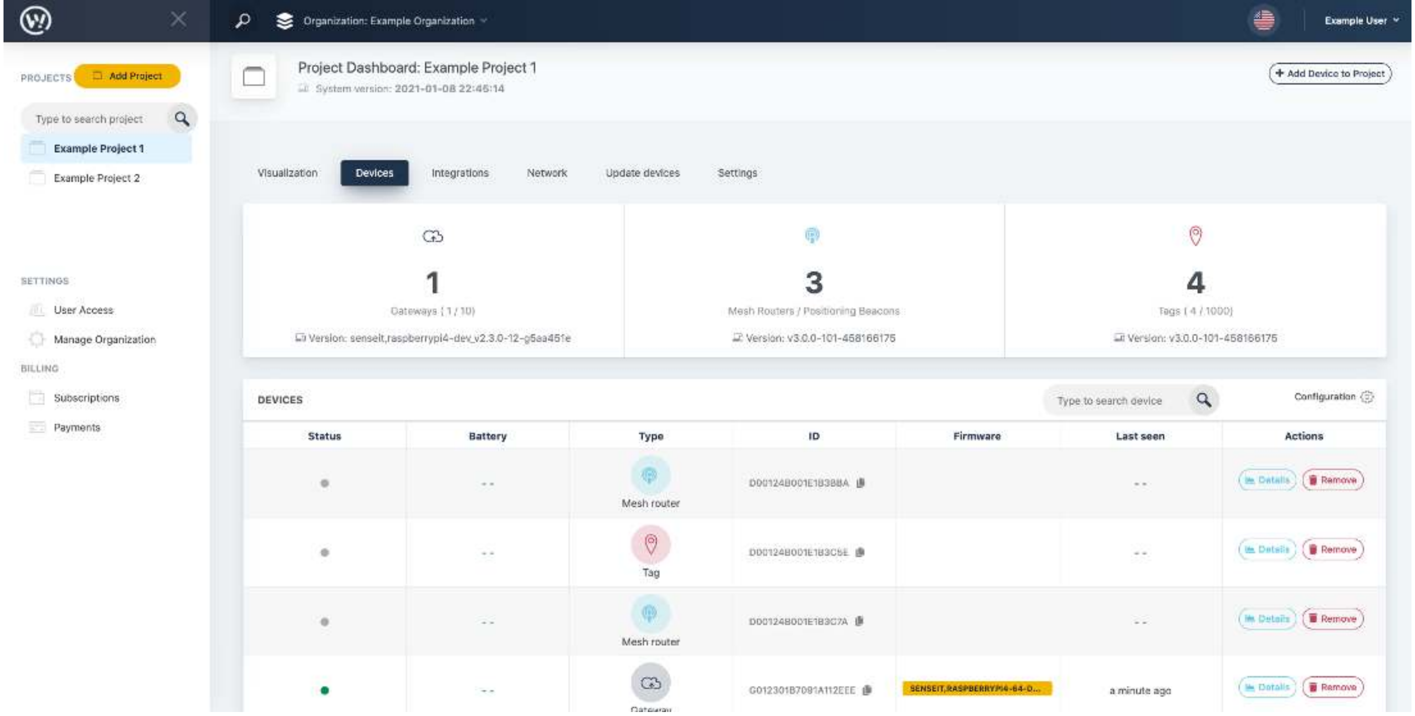
## Security

We use a Secure-by-design approach where we incorporate security from the early architecture design stage and throughout the evolution of the products. The key protections we have are summarized below:

- **Spoofing** is mitigated using an authentication process utilizing JWTs that are signed by a private key stored in a TPM on the gateway which are checked in registered devices on our cloud service, where the respective public key is stored.
- **Tampering** is mitigated using DTLS/TLS to encrypt the data sent between TrakSense360 and gateway, and between gateway and Wittra portal. One caveat is that with the current protocol bridging between CoAP and HTTP in the gateway, **the gateway has to be a trusted device**.
- **Confidentiality** is obtained by running CoAP over DTLS from TrakSense360 to gateway and by running HTTP over TLS from gateway to Wittra cloud service. The HTTP/TLS link is verified using an X.509 certificate provided by the server (in this case Google Cloud Platform) and issued by a trusted authority. The CoAP/DTLS link is verified with a Pre-Shared Key (PSK) which is randomly generated at deployment. This key must be kept secret and therefore **the gateway has to be treated as a trusted device**. See Updating security settings for more information.
- **Elevation of Privileges** is handled by standard Linux account authentication and authorization mechanisms in the gateway. On our Wittra cloud service it is handled by Googles Cloud Identity and Access Management (IAM).

# Overview of Wittra portal

Wittra portals provide a rich user interface for administration and maintenance of Wittra solutions. The following screenshot gives you an overview of the Wittra portal.



Project Dashboard: Example Project 1

System version: 2021-01-08 22:46:14

1

Gateways ( 1 / 10)

Version: senseit,raspberrypi4-dev_v2.3.0-12-g5aa451e

3

Mesh Routers / Positioning Beacons

Version: v3.0.0-101-458166175

4

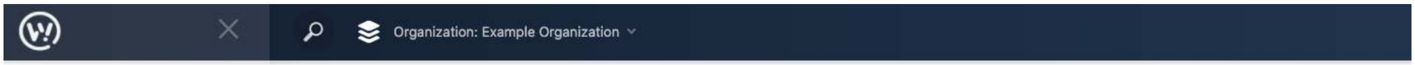
Tags ( 4 / 1000)

Version: v3.0.0-101-458166175

DEVICES

| Status | Battery | Type | ID | Firmware | Last seen | Actions |
|---|---|---|---|---|---|---|
| ● | -- | Mesh router | D00124B001E1B388A |  | -- | Details Remove |
| ● | -- | Tag | D00124B001E1B3C5E |  | -- | Details Remove |
| ● | -- | Mesh router | D00124B001E1B3C7A |  | -- | Details Remove |
| ● | -- | Gateway | G012301B7081A112EEE | SENSEIT,RASPBERRYPI4-64-D... | a minute ago | Details Remove |

## Top bar

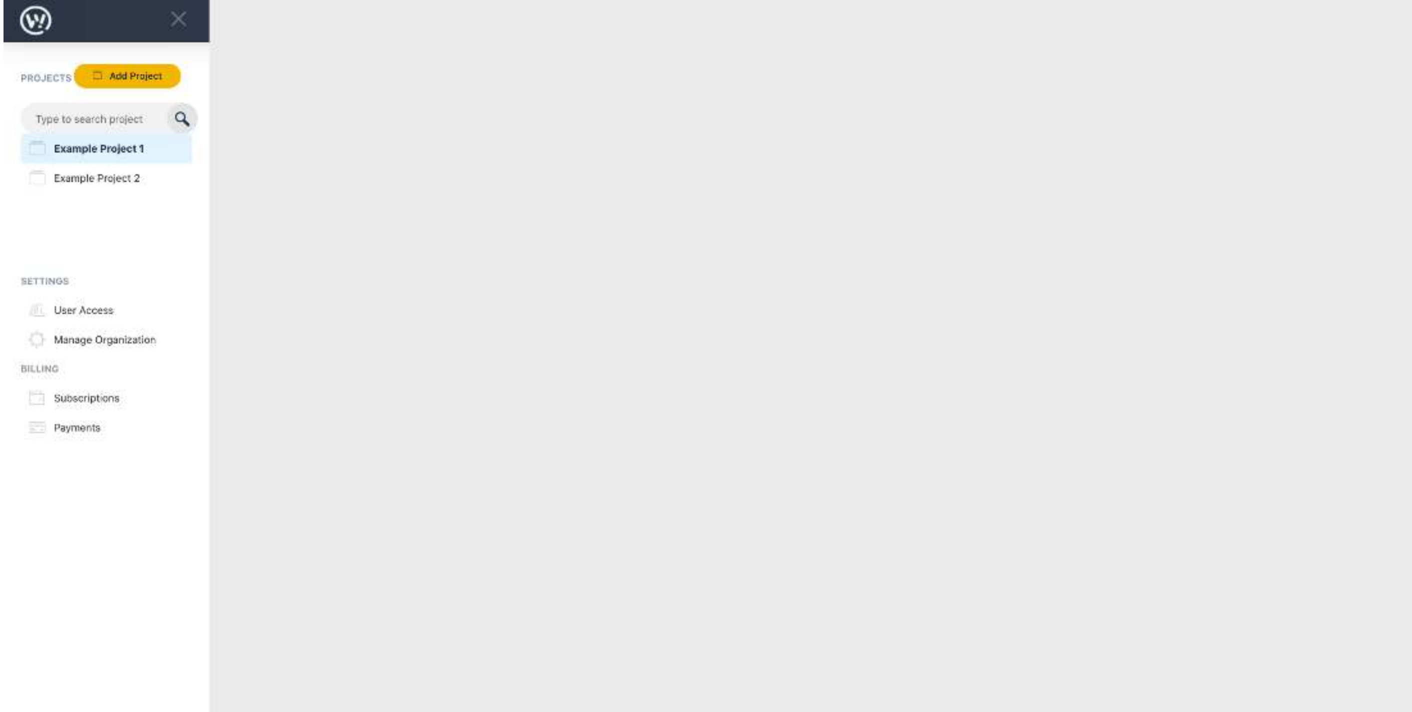


Indicates the name of the organization(s). You can also search through the list using the search functionality.

On the top right there is a ? symbol with quick links to guides and walkthroughs.

On the very right you can find your account related information. Here you can edit your user profile information and log out of the portal.

## Side panel



Shows the list of projects that is under the current organization. You can also search through the list using the search functionality.

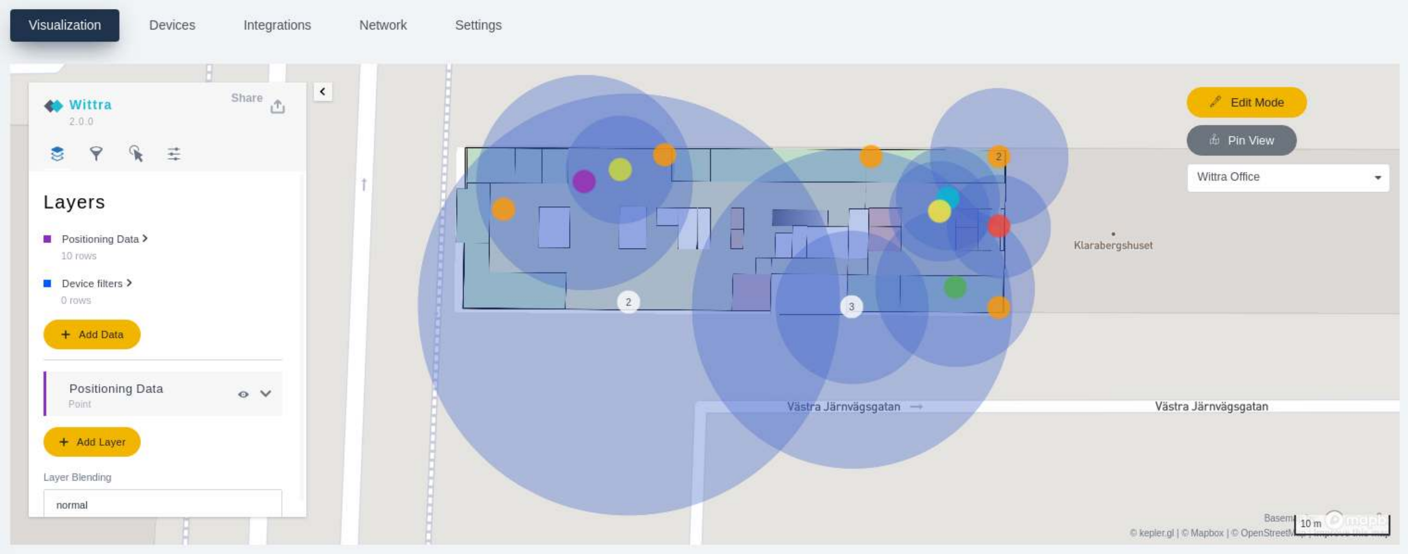
On the bottom left you have an admin view where you can manage your user permissions, organization information and billing.

# Project Dashboard

The Project Dashboard is where all the information related to the deployment is displayed. Following sections will describe the functionality of each tabs.

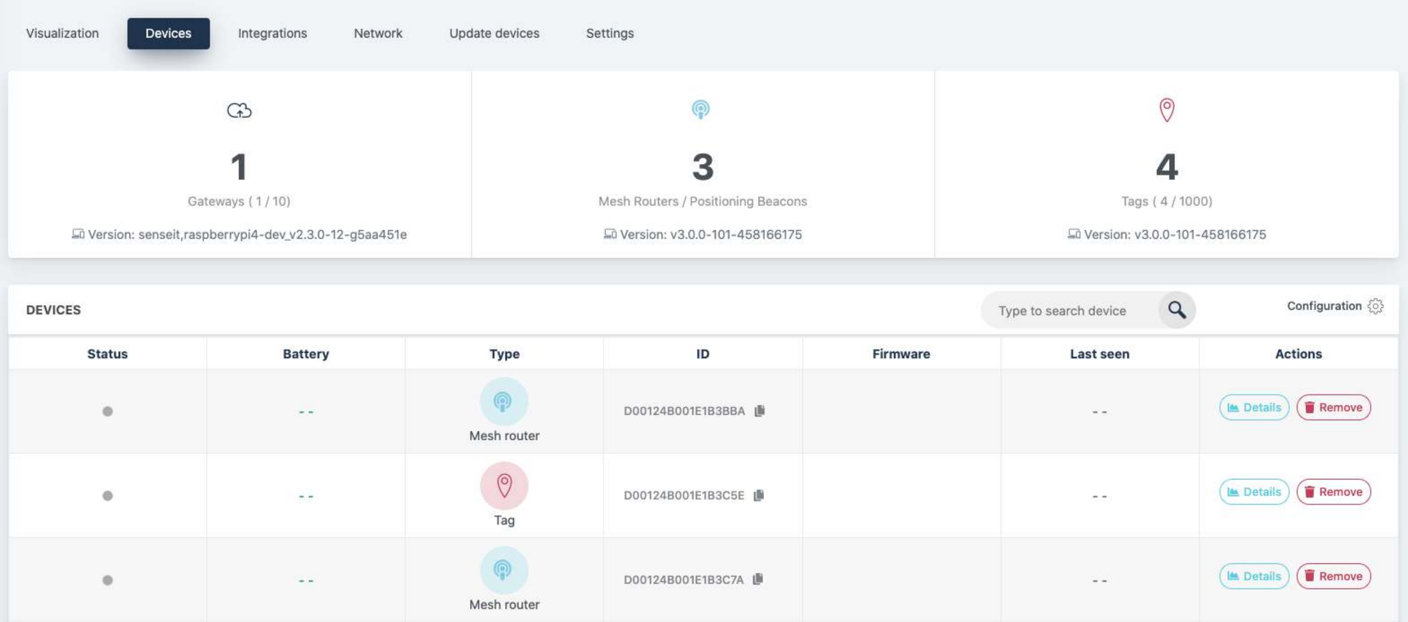
## Map

Here you can get an overview of the deployment on a map. For further information, please have a look at Position your devices



## Devices

This view provides a list of devices that are added to your project. You can filter them based on the types of devices by clicking on the checkboxes next to device IDs or device names.



1
Gateways ( 1 / 10)
Version: senseit,raspberrypi4-dev_v2.3.0-12-g5aa451e

3
Mesh Routers / Positioning Beacons
Version: v3.0.0-101-458166175

4
Tags ( 4 / 1000)
Version: v3.0.0-101-458166175

DEVICES

Type to search device

Configuration

| Status | Battery | Type | ID | Firmware | Last seen | Actions |
|---|---|---|---|---|---|---|
| ● | - - | Mesh router | D00124B001E1B3BBA |  | - - | Details Remove |
| ● | - - | Tag | D00124B001E1B3C5E |  | - - | Details Remove |
| ● | - - | Mesh router | D00124B001E1B3C7A |  | - - | Details Remove |

## Firmware

For each device, there is a field indicating which firmware version it is running. The firmware version could be highlighted in one of the following colors.

- **Green:** Device firmware is up-to-date with the system version for the project, and the system version is the most recent version.
- **Blue**: Device firmware is up-to-date with the system version for the project.
- **Blue, with a percentage**: The device is currently undergoing an automatic firmware update.
- **Yellow**: Device firmware is outdated.

### Last seen and Last boot

The gateway, TrakSense360 and mesh-routers regularly indicate their presence in the network.

In the **Project Dashboard** project view, the time when a device last reported can be seen in the `Last Seen` column. If the device report interval is within normal limits the device is marked with a green indicator. If a device is disconnected or has left the network, the indicator will turn gray.

Under the `Last Boot` column, the device reports the last time it re-started.

### Details and Update

The Details view for each device allows you to configure the device, see **Configure your system** for more information.

You can select which devices to manually update, see **Updating your system** for more information.

## Integrations

Here one can create an integration using Webhooks. For further information, please have a look at **Accessing your data**.

## Network

The network tree visualizes the overall architecture of the mesh network, depicting the link quality between the devices. It should be used during the deployment of the system. For further information, please have a look at the **Deployment Guide**

## Settings

Here you can configure the **System version** and **Network settings**. You can also change the name of the project. If you ever need to delete the project, you can do it here. Note that this step is permanent, and hence, follow the warnings carefully.

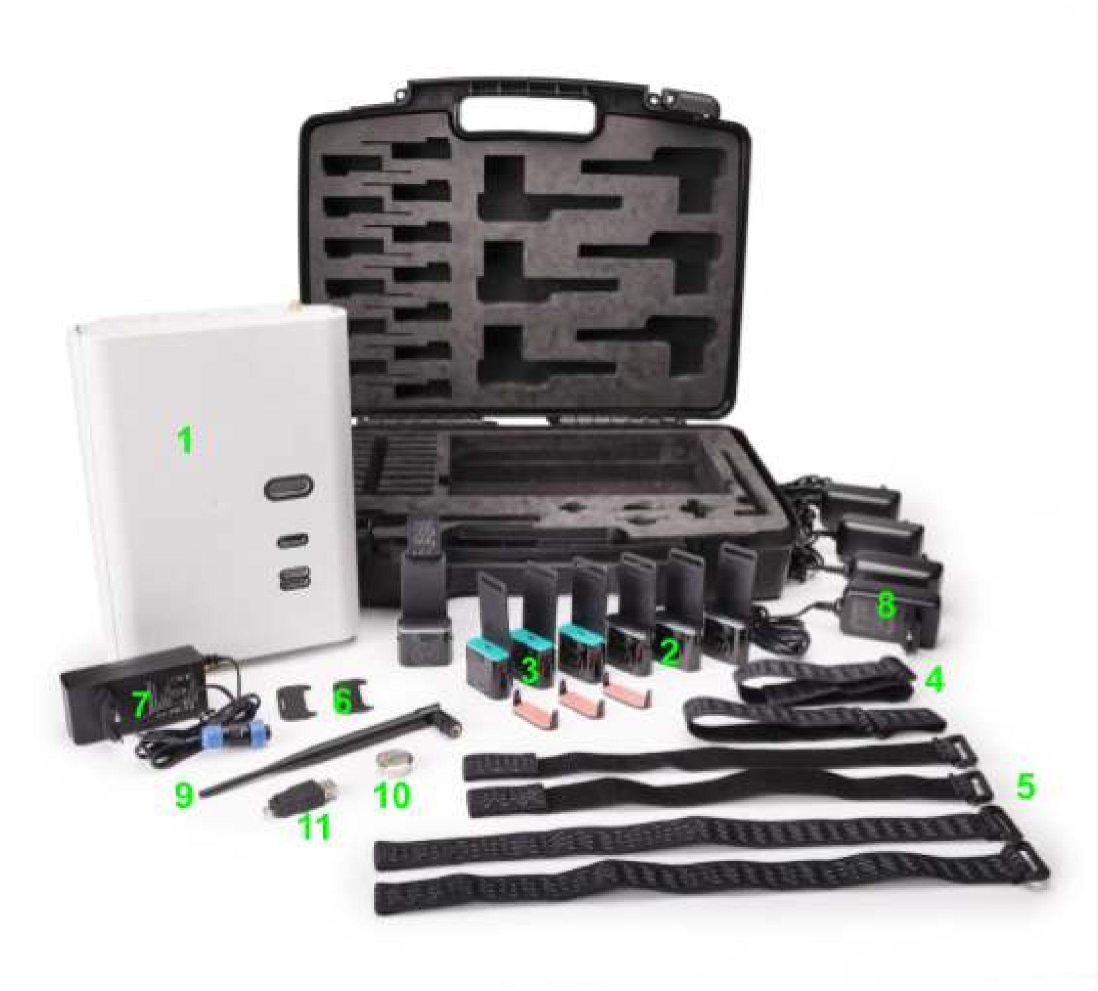
# Getting started

This guide will help you get started with your IoT Solution from Wittra. This means:

> **NOTE: Do you have any issues getting started? Check out our Troubleshooting section.**

## Meeting your IoT Solution

Open the WITTRA™ IOT OUT OF THE BOX, and get to know what it includes.



```text
1)  Gateway                  x1     2) TrakSense360         x4
3)  Mesh-Router              x3     4) Cradle               x7
5)  Velcro band              x4     6) Release Key          x2
7)  Power Supply Unit 12V    x1     8) Power Supply Unit 5V x4
9)  External Antenna         x1    10) Magnet               x1
11) USB OTG adapter          x1
```

## A TrakSense360 or a Mesh-router?

Mesh-routers have a TM (™) printed on the front of the device, next to the Wittra logo. To distinguish further between mesh-routers and TrakSense360, remove the cradle the devices sit in. On the back of each device there is a model number.

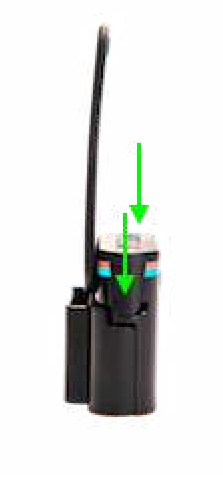
- Mesh-routers are marked with model number `MESHROUTER-1.0-<EU/US>`
- TrakSense360 are marked with model number `SENSORTAG-1.0-<EU/US>`

# Powering your devices

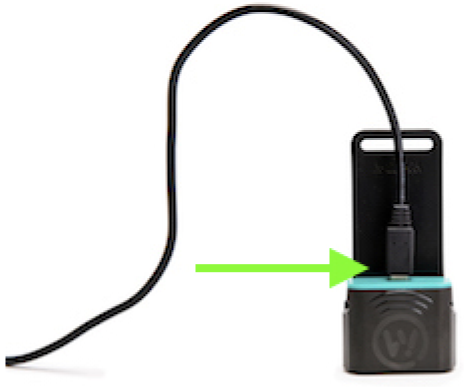
Before you can get started with your IoT Solution you have to charge the devices.

## Charging the TrakSense360

1. Collect all TrakSense360. Initially you need to charge them because they are shipped with low charged batteries.
2. Unmount the protection cover with your hands or by using the accompanying release key from the box according to the pictures below. Place the release key in front of the TrakSense360 and push it towards the TrakSense360. The protection cover will be pushed up and can now be removed.



3. Connect the Power Supply Unit 5V according to the picture. The Power Supply Unit 5V is included in the box.



4. The first initial charging time is approximately 3 hours. Check out the troubleshooting section to see **how to know when your TrakSense360 is fully charged**.

## Power the mesh-routers

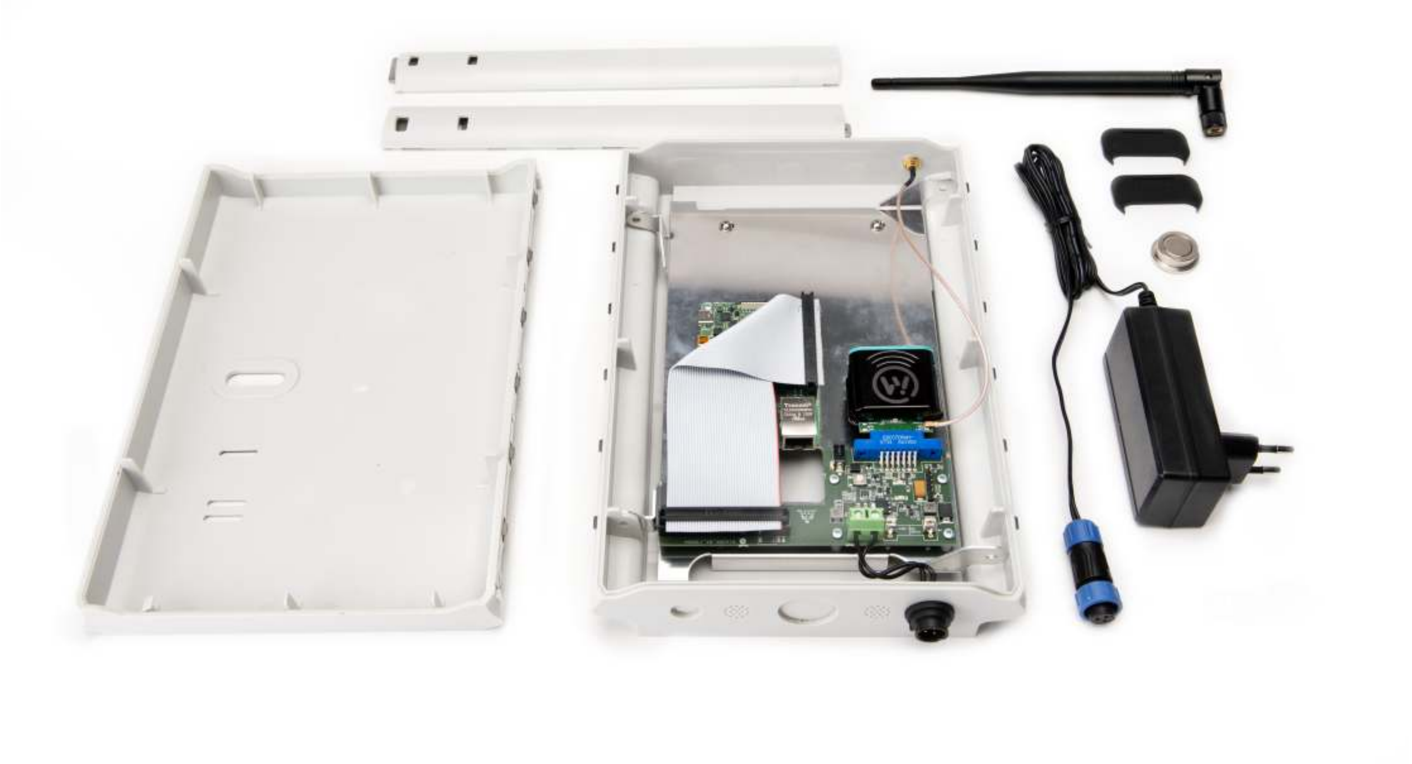
When the TrakSense360 are fully charged, plug in the mesh-routers to the power supply. The mesh-routers should always be connected to a power supply.

# Set up your gateway

The gateway allows your IoT Solution to connect to the Wittra portal.

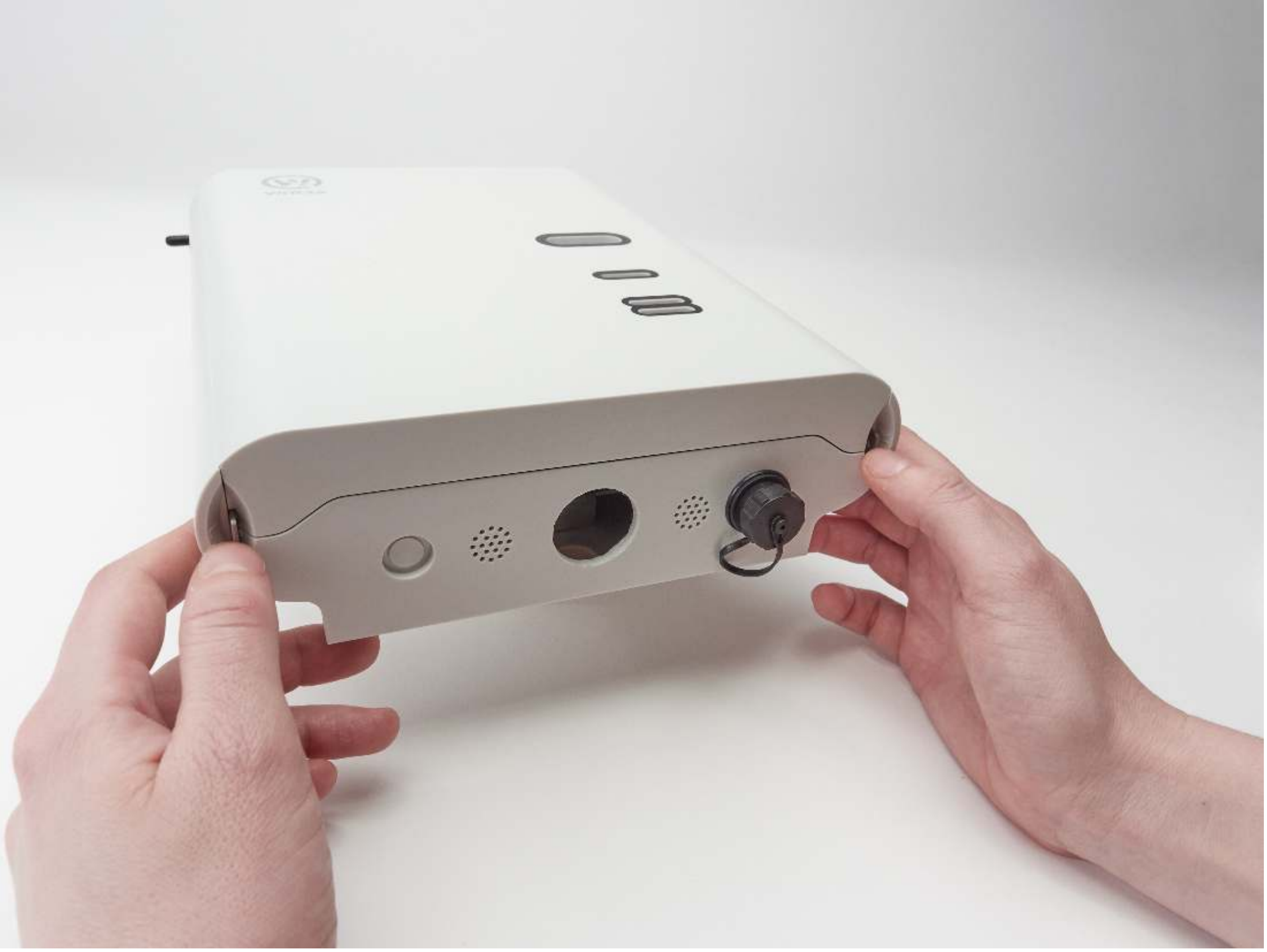
## Mount the antenna

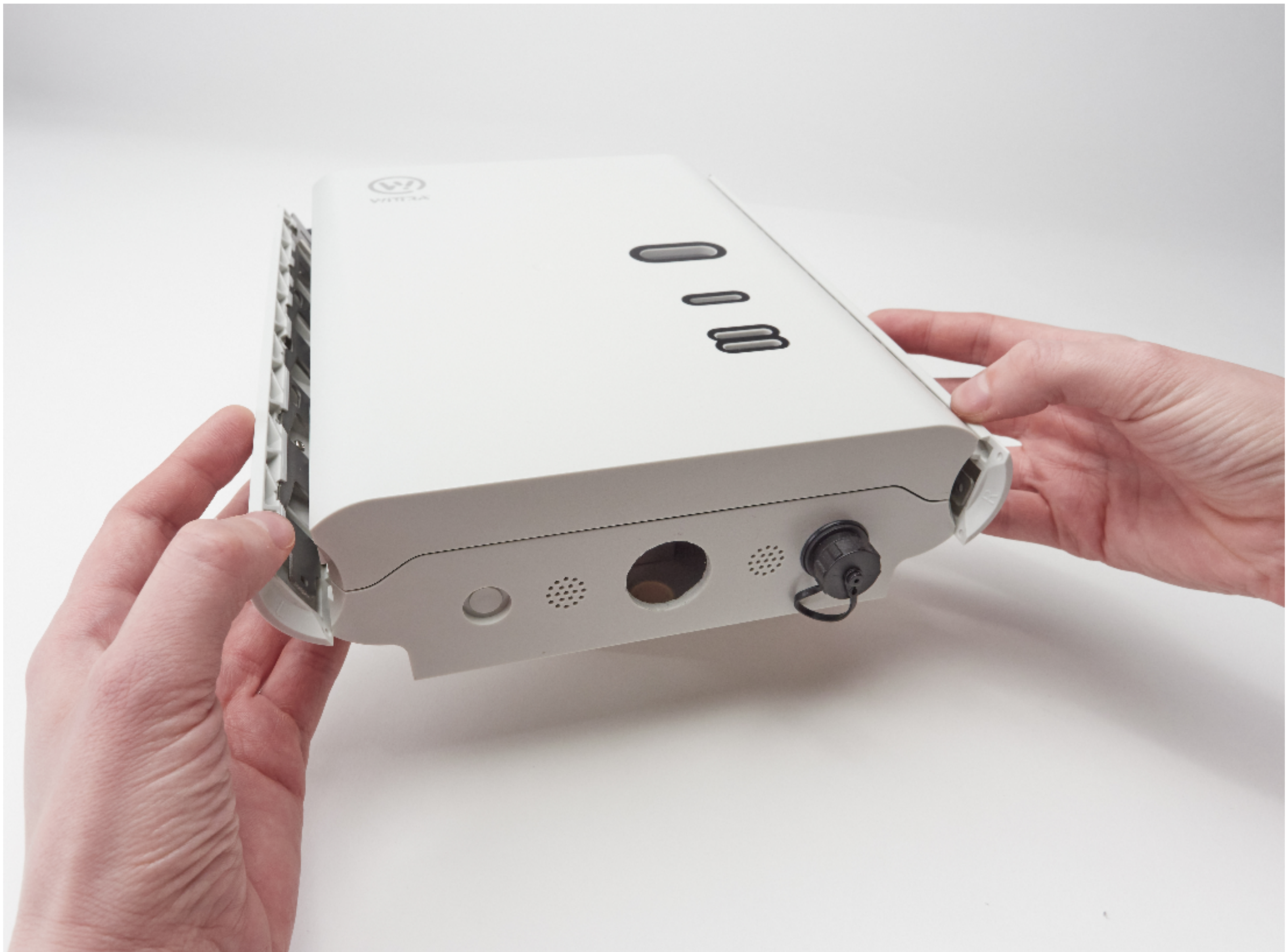
Start by mounting the antenna on top of the gateway. The antenna is included in the box.

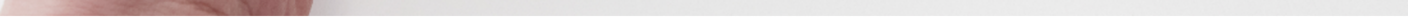


## Open your gateway

Press the two metal clips on the bottom of the casing as in shown in picture below.



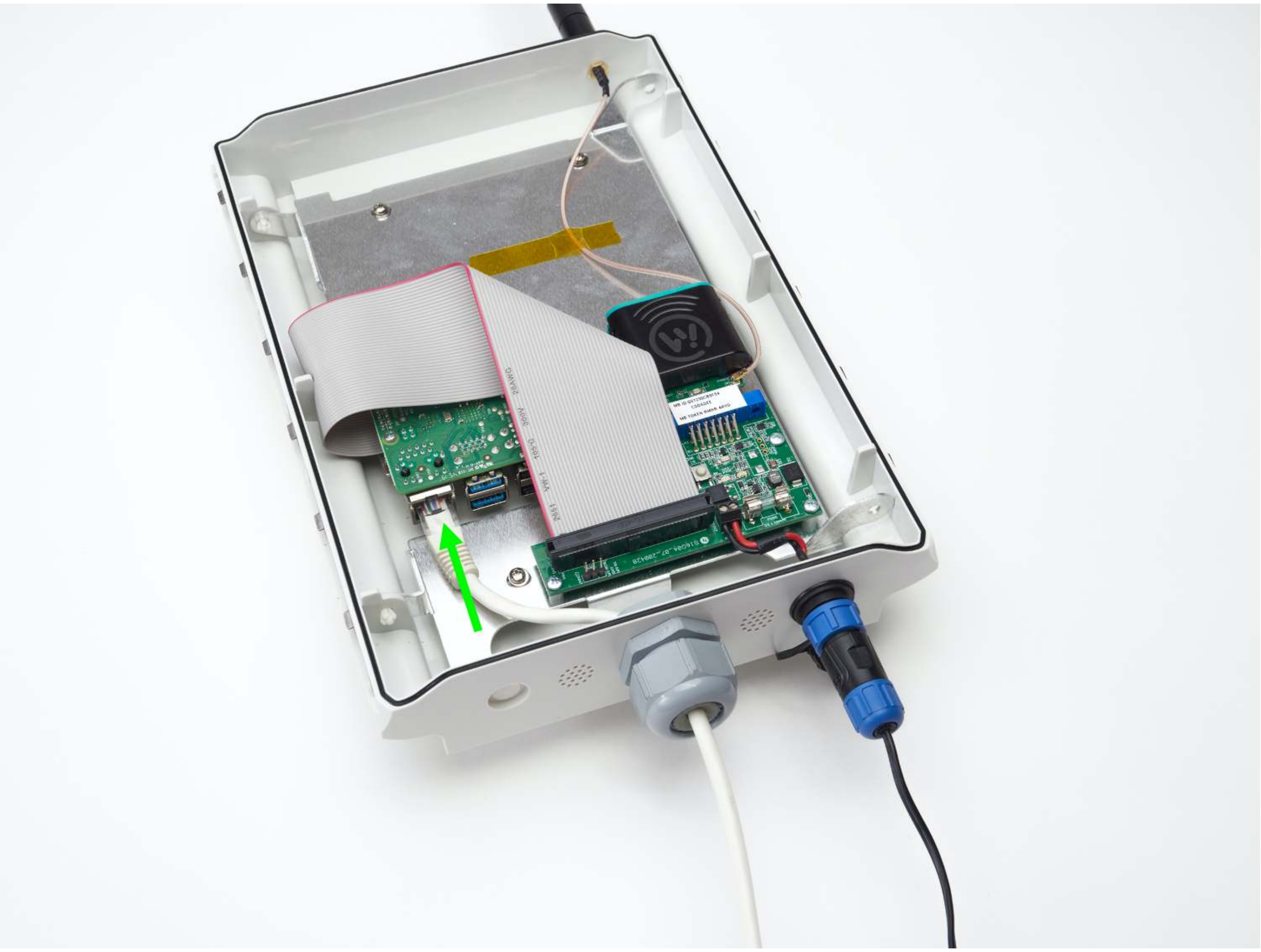




To assemble the gateway casing once again, please note that the side parts are nonsymmetrical and need to be mounted on the correct side.

## Setup an Internet connection

Plug in an Ethernet network cable in the Gateway according to the picture and connect the other end of the cable to your router or switch. When the cable is connected, continue with the **Power the Wittra Gateway** step.



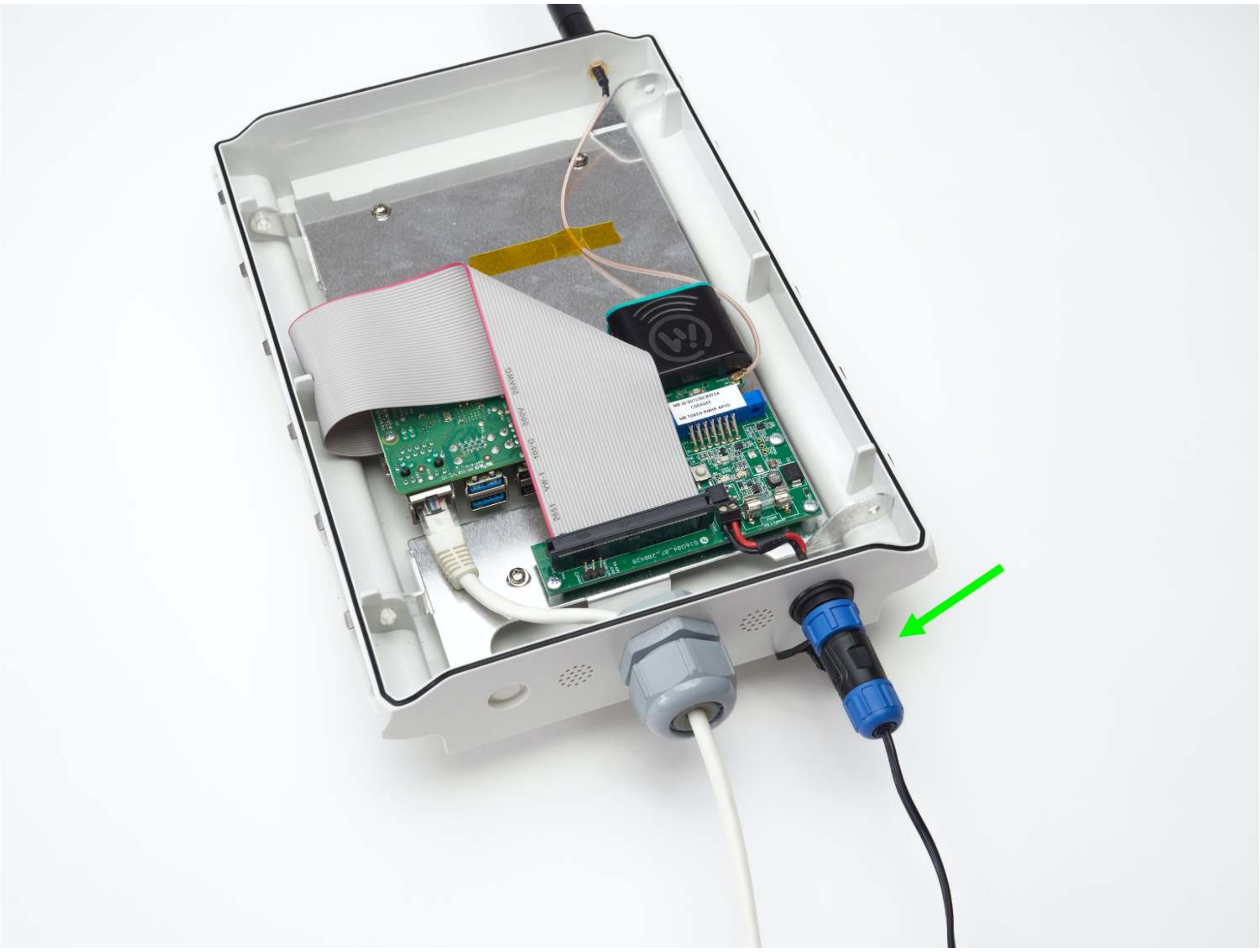
Ethernet Cable

> **NOTE: The Ethernet cable is not included in your IoT Solution.**

If your network is using DHCP for dynamic configuration of network parameters then attaching a cable is all you need to do. If you require to set up a static IP address, netmask, gateway, etc. refer to **Static IP Setup**.

## Power the Wittra Gateway

1. Connect the 12V Power Supply according to the picture. The 12V Power Supply is included in the box.



2. Wait 3 minutes for the Gateway to boot and start.

This Table depicts the Raspberry Pi's two LED indicators:

| LED Color | Blink pattern | Status |
|---|---|---|
| Red LED | Steady on | The Gateway is powered. |
| Green LED | Steady off | The Gateway is not connected to any network. (There might be a link-local connection, but no IP address has been acquired) |
| Green LED | 1 short blink and then 1 second off | The Gateway has connected to the local network but has not yet verified that there is Internet access. |
| Green LED | Steady on | The Gateway has connected to the network and was also successful in accessing the Internet. |

Please refer to the **troubleshooting** section for more help.

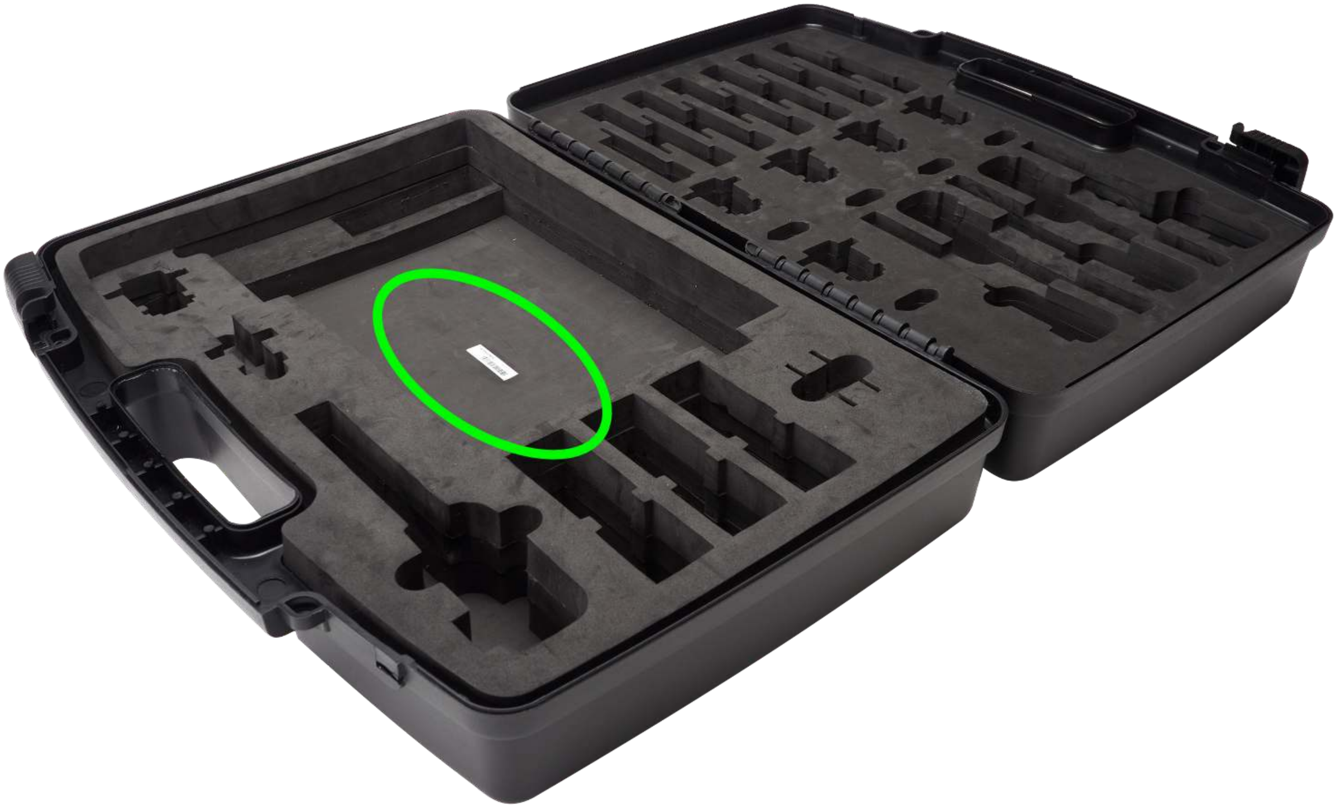
After you have verified that the gateway is connected to your local network you can reseal the gateway by putting the cover back on.

# Using the Wittra portal

You are now ready to register your IoT Solution in the Wittra portal. Go to the portal and follow the instructions to finish setting up your IoT Solution.

You should perform the following steps in the portal:

1. Setup an organization.
2. Activate a subscription.
3. Setup a project.
4. Register the devices. You will need to enter your batch token to register your devices. The batch token is printed on a sticker inside your WITTRA™ IOT OUT OF THE BOX, it should be visible after removing your gateway from the box, see picture below.



# The next steps

- Overview of Wittra portal for more detailed information on the Wittra portal and its offerings.
- Accessing your data for inspiration of what you can build with your data and how to set up an integration.

- Deployment for guidance on how to install your system.
- Updating your system to have your system run with the latest features.

# Updating your system

Wittra regularly releases improved software for all your devices. This page describes the various parts included in updating your devices to the latest releases.

There are two ways to update your Wittra devices (i.e. TrakSense360 and mesh-routers):

- Manual
- Automatic

Manual update is required for:

- First time use
- PAN ID change
- Security update (e.g. DTLS key update)

An automatic update can take up to 24h. Therefore it's recommended to do a manual update when you want to do a quick update of your system.

## What is a system version?

The gateway, mesh-routers and TrakSense360 each have their own firmware version. The system version indicates a collection of firmware versions intended to work together.

It is recommended to always update the system version when possible, as it may fix bugs in the system, add new features, improve reliability, or contain security updates. To update to the latest system version, navigate to the `Settings` tab in the Project Dashboard.

> **NOTE: When you have updated the system version under `Settings` , the system will start the automatic update. If you want to speed things up, do a manual update.**

## Updating your devices

In the Project Dashboard, go to the `Devices` tab. You will find information there on the current version for every device in your project. If any device is out-of-date, it will be indicated here, and you can update it by clicking the `Update` button and follow the wizard.

The gateway and border router will download their new firmware directly and update to it. When the gateway system is updating, a blue LED will blink. When the border router is updating, a red LED will blink.

> **NOTE: Do not power off the gateway while the blue LED is blinking, or has just stopped blinking. Instead, wait for the gateway to connect to the internet before powering off.**

Mesh-routers and TrakSense360 will need to download the firmware either manually or automatically over 6LoWPAN in order to be updated.

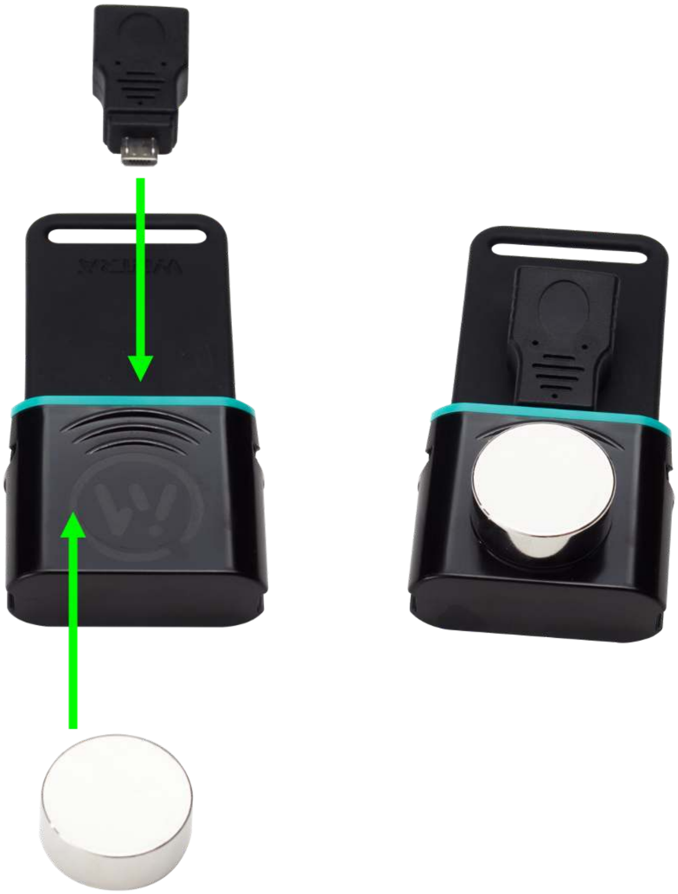
## Manual update

The manual update method is the faster one, but is limited in range and requires manual intervention (reboot the device in manual update mode).

To update your TrakSense360 and mesh-routers manually, you will have to collect the devices you wish to update and place them close to the gateway. Set the TrakSense360 and mesh-routers in manual update mode by using the included magnet and OTG adapter from the box.

**Step 1.** Unmount the protection cover using the accompanying TrakSense360 tool from the box or carefully with you hands. Place the TrakSense360 tool in front of the TrakSense360 and push towards the TrakSense360 and then push up. The protection cover will be released.

**Step 2.** With the micro-USB port protection cover off, place the included magnet on the device. It should be placed roughly in the area indicated by the picture below. With the magnet in place, insert the OTG adapter into the micro-USB port and then remove it again.



The device's LED should start advertising two short blinks followed by a pause to indicate that it has entered manual update mode, after which a device is ready to start the firmware download. If the device does not enter manual update mode, repeat Step 2 until it successfully enters manual update mode.

**Step 3.** Do this for all of the devices that you would like to update.

Manual firmware update will take approximately 2 minutes per device.

## Automatic update

If you do not take any further action, nodes will be automatically upgraded over 6LoWPAN. There is no need to gather the devices nor reboot them into manual update mode. Note that this procedure is significantly slower, and could take between several hours and up to a day (due to lower bandwidth and spectrum regulations).

> **NOTE: The devices remain fully operational during the download, though once they are ready to reboot you may experience a short disconnection.**

# Updating network settings

If you need to change your network and security settings ( `Settings` tab in the Wittra portal), you must get your devices back into manual update mode, as the new configuration would break 6LoWPAN connectivity.

Select your new settings, apply them, and set your devices into manual update mode as described in **Manual update**.

# Deployment Guide

This guide will help you deploy the infrastructure of your system so you can start using your IoT Solution from Wittra. Your Gateway, Mesh Routers (MRs), and Positioning Beacons (PBs) form a fixed infrastructure, enabling you to create your own network to collect and transport sensor and positioning data. The TrakSense360 devices, however, are not part of the fixed infrastructure; they are mobile devices that send and receive data through the network, using the fixed infrastructure.

To learn more about the different device types, as well as about network and positionning, read the **System Overview page**

> **NOTE: Do you have any issues? Check out our Troubleshooting section.**

# General considerations

Bear in mind you will need to go to the site and confirm there is mains power available for the chosen locations (unless you plan to run the infrastructure devices on battery power alone, which will then eventually require battery replacement/charging).

Another Golden Rule to follow (if possible) is to install the Mesh Routers and Positioning Beacons in “clear air”, meaning as far as possible from large metal objects and surfaces (e.g. metal poles, metal beams, sheet metal etc.). If it is impossible to avoid these types of objects, the Wittra device will still function but the effective communication distance might be reduced in some directions.

***General rules to follow for the Mesh Routers:***

- *Outdoors:* MRs can be placed 100m - 200m apart provided they are elevated at least 3 metres above ground level. This allows the antennas to operate efficiently and achieve reliable data links for the mesh.
- *Indoors:* MRs can be placed 30m - 100m apart depending on how many obstructions lie between the MRs. The quality of the radio links can be seen in the Wittra portal so it is easy to check this during installation.

***General rules to follow for the Positioning Beacons:***

- *Outdoors:* PBs should be placed not more than 100m apart for good positioning accuracy, as well as being elevated at least 3 metres above ground level. If there are obstructions (trees, buildings) between the PBs then you might need to reduce this distance. In addition, there should not be more than 100m - 200m between each PB and the nearest MR (the positioning signals from the PBs need to be sent into the mesh network, so every PB needs a good quality radio link to at least one MR).

- *Indoors:* PBs should be placed no more than 50m apart to maintain good positioning accuracy. For a heavily obstructed environment (a lot of walls or other physical obstacles) this distance might need to be reduced. Again, the Wittra portal can be used to assess radio link quality.

# Deploying your system

The following steps describe the setup process for network infrastructure, assuming you already **have a running Gateway**.

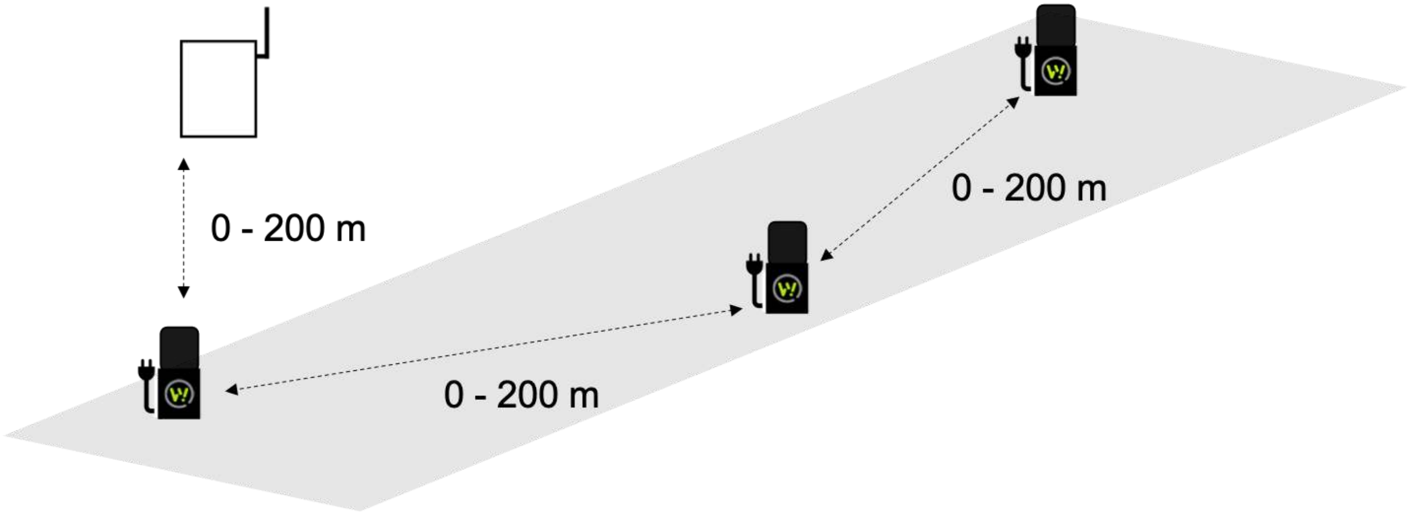
**Step 1: Planning**

There are two separate considerations when planning the network:

1. Placing the Mesh Routers (MRs) in optimal locations to enable routing of data from TrakSense360 tags to the Gateway;
2. Placing Positioning Beacons (PBs) in optimal locations to capture signals from the TrakSense360 tags for positioning.

Place MRs within the site in a way that any location where tracking/sensing is required has MRs or the Gateway within reach (30-200m dependeing on environment, see "General considerations" above). Ensure that there exists at least one or more multi-hop paths (for redundancy, multiple paths are preferred) from any point to the Gateway via MRs.

You can then proceed and place PBs following the boundaries of your site, then add more in the middle, to form a grid with 50-100m spacing ("General considerations").



**Step 2: Install MRs and PBs**

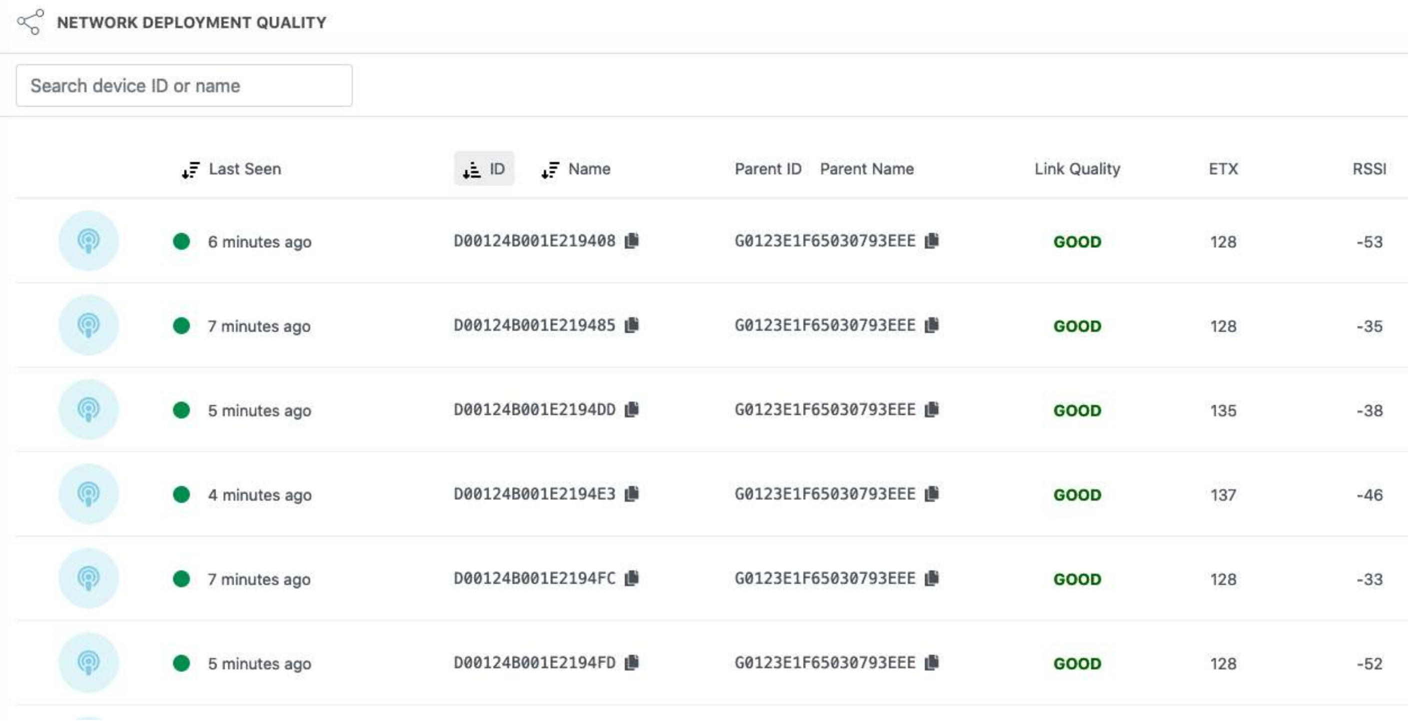
Deploy now all MRs and PBs as planned in step above. **Important:**

- MRs and PBs should be placed at least 3m above the ground if possible, and upside down, i.e., with the rubber tail down.
- MRs and PBs should be placed as far as possible from large metal surfaces (see "General considerations").
- All MRs and PBs must be externally powered.

### Step 3. Check connectivity

Check the link quality status under `NETWORK` tab in the web-portal.

- Go to the **Wittra portal**.
- Select your project and navigate to the `Network` tab.
- Your deployment will be visible under `NETWORK DEPLOYMENT QUALITY` , but please note that it could take between five to ten minutes before the deployment data is visible. It will be updated in real-time as new network data is received.
- The table lists all the MRs and PBs in the deployment along with deployment data (their parent, the link quality between them, and when they was last seen).

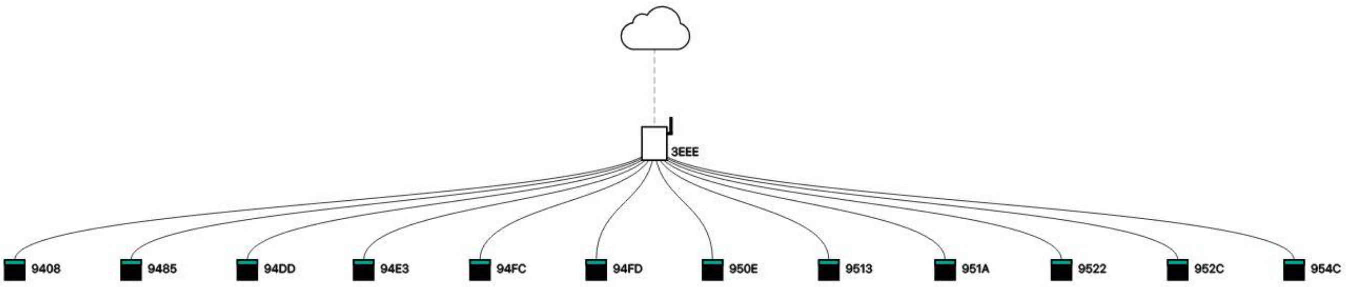


NETWORK DEPLOYMENT QUALITY

Search device ID or name

| | Last Seen | ID | Name | Parent ID | Parent Name | Link Quality | ETX | RSSI |
|---|---|---|---|---|---|---|---|---|
| | ● 6 minutes ago | D00124B001E219408 | | G0123E1F65030793EEE | | GOOD | 128 | -53 |
| | ● 7 minutes ago | D00124B001E219485 | | G0123E1F65030793EEE | | GOOD | 128 | -35 |
| | ● 5 minutes ago | D00124B001E2194DD | | G0123E1F65030793EEE | | GOOD | 135 | -38 |
| | ● 4 minutes ago | D00124B001E2194E3 | | G0123E1F65030793EEE | | GOOD | 137 | -46 |
| | ● 7 minutes ago | D00124B001E2194FC | | G0123E1F65030793EEE | | GOOD | 128 | -33 |
| | ● 5 minutes ago | D00124B001E2194FD | | G0123E1F65030793EEE | | GOOD | 128 | -52 |

- Below the table is the network tree depicting the network topology in a graphical way.



The link quality between each device and its parent should be *GOOD* or *OK* at least. The ETX and RSSI values are also shown in the table to get a better understanding of the link quality. `RSSI` should ideally be below `-85dbm` , and `ETX` represents the average number of requests needed to transmit a packet over the air, encoded as an integer (divide by 128 to obtain the real value, e.g. reported `ETX = 192` , then `192 / 128 = 1.5` requests in average to transmit a packet).

**Step 4. Fix connectivity (if necessary)**

If the indication shows *BAD/ERROR*, move the device in question closer to the Gateway or its closest Mesh-router and repeat Step 2.

> **NOTE: Radio range and link quality depends on multiple parameters, for example, physical obstructions (like walls, metal frames, building materials, etc.), radio and electronic interference from other appliances, etc.**

TrakSense360 within your network can now start sending data. Check out **Accessing your data**

# Accessing your data

When your devices are registered and updated they are ready to deliver data. This document describes the different ways you can monitor and make use of the Wittra IoT solution.

You can configure your devices to send data at a set interval or when a certain event occurs. Check out **Configure your system** for more information.

There are two main ways that you can use to access your data; a *push* approach and a *pull* approach.

In the **push approach**, the Wittra Portal pushes data to an external system in real time, when the data arrives. That is done through an *integration*.
In the **pull approach**, an external system may request data from the Wittra Portal, current or historical, at its convenience. That is done through a REST API.

# What is *data*?

When referring to *data* in the Wittra Portal, it may be important to distinguish between *device data* and *event data*.

**Device data** is the kind of data that is produced by the devices in a Wittra IoT Network. That could be data from the sensors of a device, such as temperature and movement, but also meta-data such as the list of neighbors of a device.
**Event data** is the kind of data that is produced by the Wittra Portal. Typically, that kind of data is produced when various actions are taken in the portal, such as when someone adds one or several devices to a project.

Both device data and event data can be accessed through integrations (push) and the REST API (pull).

# Integrations

The Wittra Portal offers two types of integrations for having data pushed to an external system; a general-purpose *Web Hook* and an integration towards *Cumulocity*. To set up an integration, go to the project in which your devices are located and click on the *Integrations* tab.

## Web Hook

Web Hook integrations require a URL to which data will be sent. Once a URL has been provided, the Wittra Portal will attempt HTTP POST requests to that URL, with the data payload as the body of the request. The data is sent as JSON, as denoted by the `Content-Type` header, which is set to `application/json` .

For details on the format of the JSON content, see *Device data* and *Event data* below.

For a quick start on how an implementation can be done, there are examples published in a **source code repository**.

## Cumulocity

Integrations with Cumulocity require that you have an account in the Cumulocity platform, and a *tenant* with an associated *tenant domain* and *tenant ID*.

When the integration has been saved, the devices in your project in the Wittra Portal should appear in the list of devices in the corresponding area in the Cumulocity portal. Any sensor data that is pushed to the Wittra Portal from a device in your project will be propagated to Cumulocity.

# REST API

To access the REST API, you need an API key. API keys are tied to a specific organization, in contrast to integrations, which are tied to a specific project. Once an API key has been registered, that API key may be used to access and modify data in all projects in its organization.

Generate an API key by clicking *Manage API Keys* in the left menu, in an organization in the Wittra Portal.

The base URL for the REST API is `https://api.wittra.se/` . To authorize, the `Authorization` header is used, where the API key is sent as a password, together with the organization ID as a username. The values are separated by a colon ( `:` ) and they are base64-encoded.

Below, an example follows.

```
Authorization: Basic enU1dk5pQXY5dEpYWm1tSlNGTXY6Zk1YMm9qZ05Ebk0yUkNTbTRYa2RvSXBDZ
```

In the above example, the base64-encoded string corresponds to `zu5vNiAv9tJXZmmJSFMv:fMX2ojgNDnM2RCSm4XkdoIpCg3WQtQ02VWOxzakb99YOSfbq` where `zu5vNiAv9tJXZmmJSFMv` is the ID of the organization and `fMX2ojgNDnM2RCSm4XkdoIpCg3WQtQ02VWOxzakb99YOSfbq` is the API key in use.

The following endpoints that are commonly used to access device data.

```
GET /v1/organizations/<organization ID>/projects/<project ID>/devices
GET /v1/organizations/<organization ID>/projects/<project ID>/devices/<device ID>
GET /v1/organizations/<organization ID>/projects/<project ID>/data
```

The REST API can be used not only to retrieve data, but also to perform certain actions (e.g. add a device to a project). For a comprehensive list of all available endpoints, see the **API documentation**.

# Device data

The JSON-encoded data is sent to the URL specified in the integration in the body of a POST request. Requests are made when a device sends sensor data or when a device is added, changed or removed in the portal.

The format for the request body when a piece of sensor data is transmitted is shown below.

```json
{
  "deviceId": <string>,
  "gatewayId": <string>,
  "integrationId": <string>,
  "organizationId": <string>,
  "payload": {
    "accelerometer": {
      "x": <float>,
      "y": <float>,
      "z": <float>
    },
    "battery": {
      "chargingStatus": "NOT_PLUGGED" | "CHARGING" | "FULLY_CHARGED",
      "percentage": <int>,
      "voltage": <float>
    },
    "location": {
      "accuracy": <float>, // in meters
      "latitude": <float>,
      "level": <int>,  // floor level
      "longitude": <float>
    },
    "magnetometer": {
      "x": <float>,
      "y": <float>,
      "z": <float>
    },
    "neighbors": [ // list of the nearest Mesh Routers and Positioning Beacons
      {
        "id": <string>,
        "rssi": <int>
      },
      {
        "id": <string>,
        "rssi": <int>
      },
      ...
    ],
    "temperature": <float>, // in °C
    "usage": {
      "moving": <int>, // in seconds
      "stationary": <int> //in seconds
    },
    "humidity": {
      "humidity": <float>, // relative humidity in percentage
      "temperature": <float> // °C
    },
    "light": <int>, // in lux
    "pressure": {
      "pressure": <float>, // in hPa
      "temperature": <float> // in °C
    }
  },
  "payloadId": <string>,
  "payloadType": "DATA",
  "projectId": <string>,
  "source": "p" | "e", // p = periodic posting, e = event-based posting
  "timestamp": <string> // ISO 8601-formatted timestamp
}
```

Remarks about the `payload` object:

1. Not all fields in the object must be present in all posts.
2. It could happen that a field is not included e.g. due to the sensor being configured not to send data.
3. The `humidity` , `light` , and `pressure` fields require a click-on sensor on the TrakSense360 to be available.

Below is an example of a what a device data payload could look like.

```json
{
  "deviceId": "D00124B001E21957B",
  "gatewayId": "G0123E1F65030793EEE",
  "integrationId": "DSMwMVes3g2Y0UJPMagx",
  "organizationId": "q3FLvOBERo4WRnRBXdFk",
  "payload": {
    "accelerometer": {
      "x": 0.031,
      "y": -0.281,
      "z": 0.979
    },
    "battery": {
      "chargingStatus": "NOT_PLUGGED",
      "percentage": 100,
      "voltage": 4.651
    },
    "location": {
      "accuracy": 2.7626049469781595,
      "latitude": 59.319177001667875,
      "level": 3,
      "longitude": 18.07548276736835
    },
    "magnetometer": {
      "x": 0.66,
      "y": 1.063,
      "z": -0.745
    },
    "neighbors": [
      {
        "id": "D00124B001E1B3CFC",
        "rssi": -43
      },
      {
        "id": "D00124B001E21954C",
        "rssi": -53
      },
      {
        "id": "D00124B001E2194F4",
        "rssi": -47
      },
      {
        "id": "D00124B001E219503",
        "rssi": -51
      },
      {
        "id": "D00124B001E2193DF",
        "rssi": -49
      }
    ],
    "temperature": 26.847,
    "usage": {
      "moving": 0,
      "stationary": 299
    },
    "humidity": {
      "humidity": 29.847,
      "temperature": 28.678
    },
    "light": 250,
    "pressure": {
      "pressure": 1013.3518,
      "temperature": 27.91
    }
  },
  "payloadId": "YTAp5BrQTDWN2EAIV7Fu",
  "payloadType": "DATA",
  "projectId": "f6IFRnCcKpVLoBNdUkyM",
  "source": "p",
  "timestamp": "2021-06-04T13:43:35.293000+00:00"
}
```

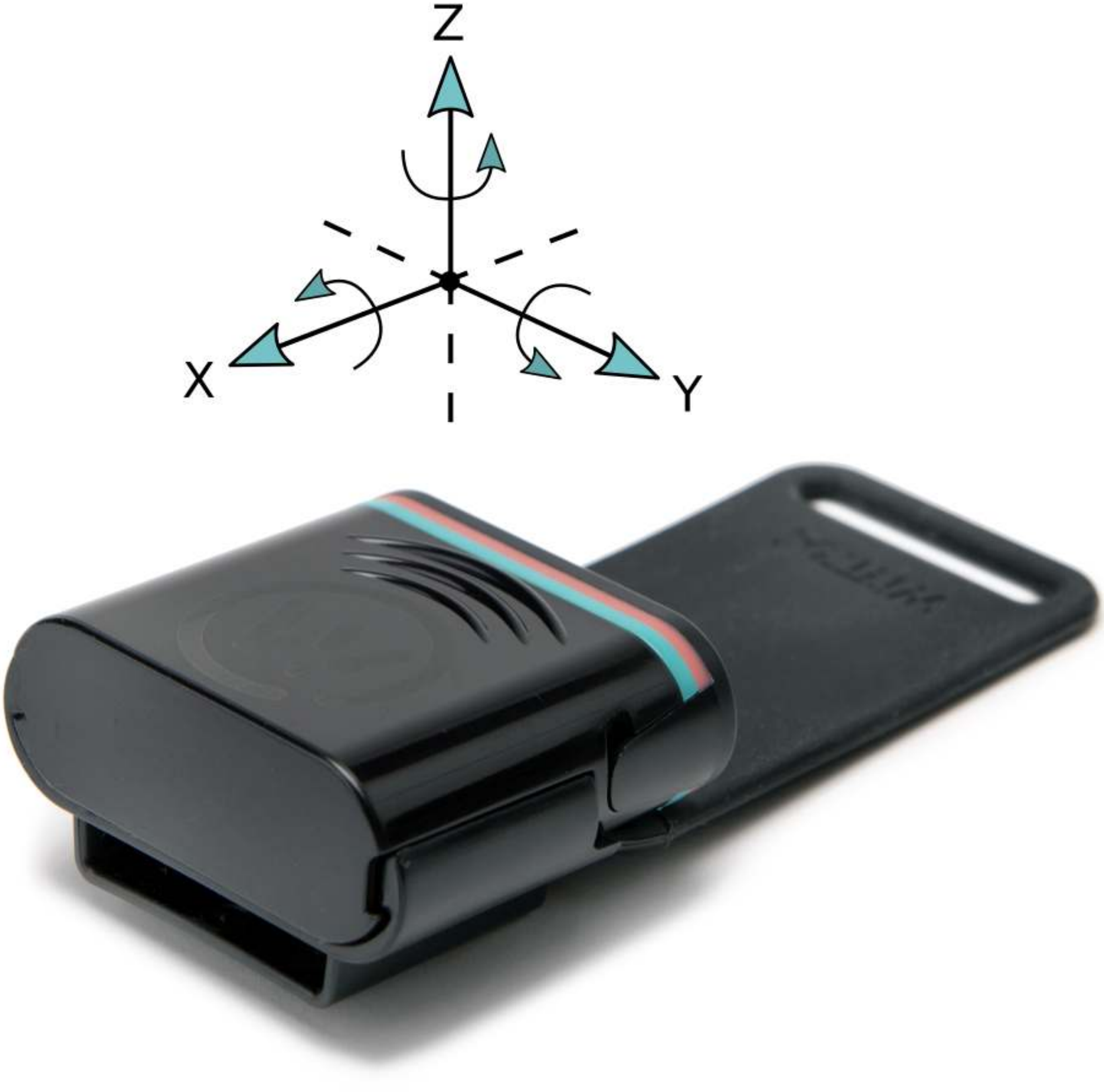
# Event data

An example of what a request body can look like when an event from the portal is transmitted is shown below.

```json
{
  "eventType": "DEVICE_UPDATED",
  "integrationId": "gr2QznINzfolbWsBoT6B",
  "organizationId": "q3FLvOBERo4WRnRBXdFk",
  "payload": {
    "changes": {
      "name": {
        "new": "An example",
        "old": null
      }
    },
    "deviceId": "D00124B001E219580"
  },
  "payloadId": "T4AvsBg9T2Y5LpEPOCD6",
  "payloadType": "EVENT",
  "projectId": "44z92iTpbo2sDfirAATJ",
  "timestamp": "2021-06-04T13:47:48.256000+00:00",
  "userId": "5R94c5TaElfe97pCzPI5BxXRQdp1"
}
```

# Device orientation

The axes provided by the `accelerometer` and `magnetometer` fields can be interpreted by the following picture.



For example, if the TrakSense360 is lying like the picture shown above, the accelerometer should report a Z value of ~1 g, due to the floor pushing up on the TrakSense360 with a force matching the gravitational pull to the center of the earth.

# Positioning your devices

This guide will help you set up the system for positioning.

## Setting up a system for positioning

Following steps describe the set up process.

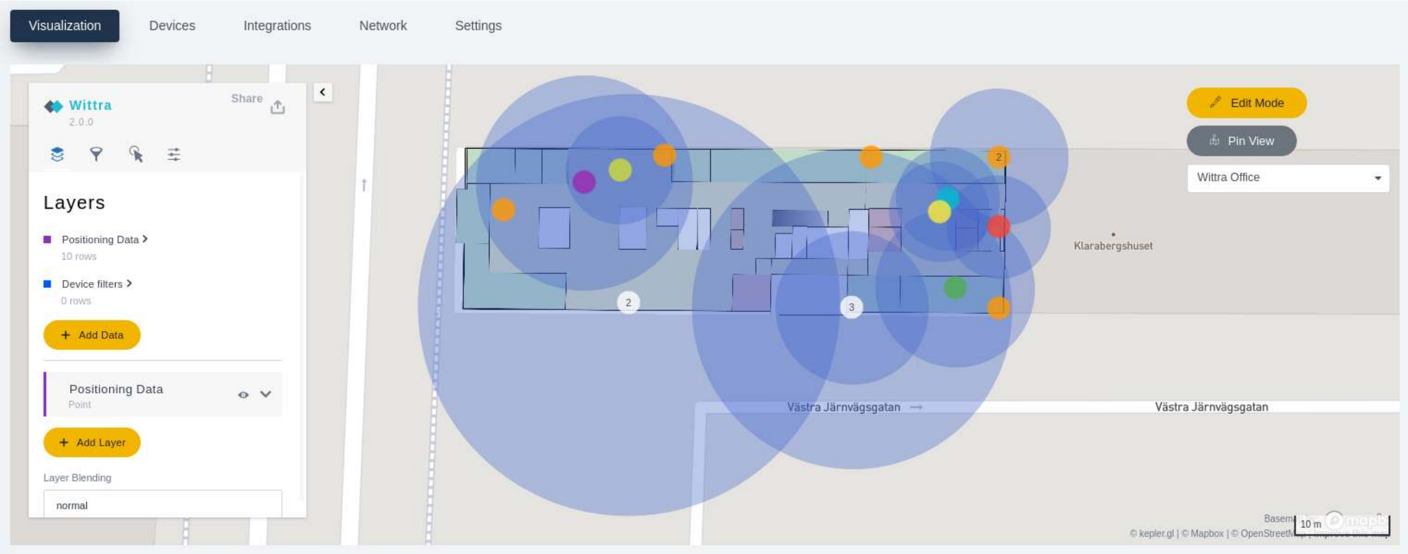
**Step 1.** Go to the `Map` tab and click the *Edit mode* button on the right-hand side.

**Step 2.** Choose the `Position Devices` in the menu to the right and click the mesh-router you want to position in the menu to the left. Before you can place your mesh-router, you have to assign it to a floor level. If you have no need to distinguish between floors, choose the default level 0. Once you have placed your mesh-router, you can always right click on it to change the associated floor.

When the mesh-routers have appeared on the map, drag them to their true location. To ensure higher accuracy, it is recommended to use a drawing (e.g. a floor plan of the site) as a layer on top of the map. Learn more about layers in the Map layers section.

> **NOTE: All mesh-routers need to be placed on the map for the positioning algorithm to work. It is also important that the mesh-routers are deployed to cover the entire site where you want to position your TrakSense360, see Deployment guide.**

**Step 3.** TrakSense360 will show up on the map on their derived position in the configured time frame of the TrakSense360. Depending on the link quality between the TrakSense360 and its neighbors, the position will have varied accuracy, which is illustrated as circles around the TrakSense360 on the map. E.g. a large circle means low accuracy.



## Map Layers

**Step 1.** Under the `Map` tab click the *Edit mode* button on the right-hand side and select *Floors*.

**Step 2.** Choose the Floor where you want to add your floorplan to by clicking the Edit symbol. Click *Select Floor Plan* and upload a file of your floorplan or site drawing, in JPG or PNG format. Save the file by clicking *Save*.

> **NOTE: The floorplan has to have a known scale, so it can be fitted correctly on the map, as the correct latitude and longitude of the mesh-routers are a vital input to the positioning algorithm.**

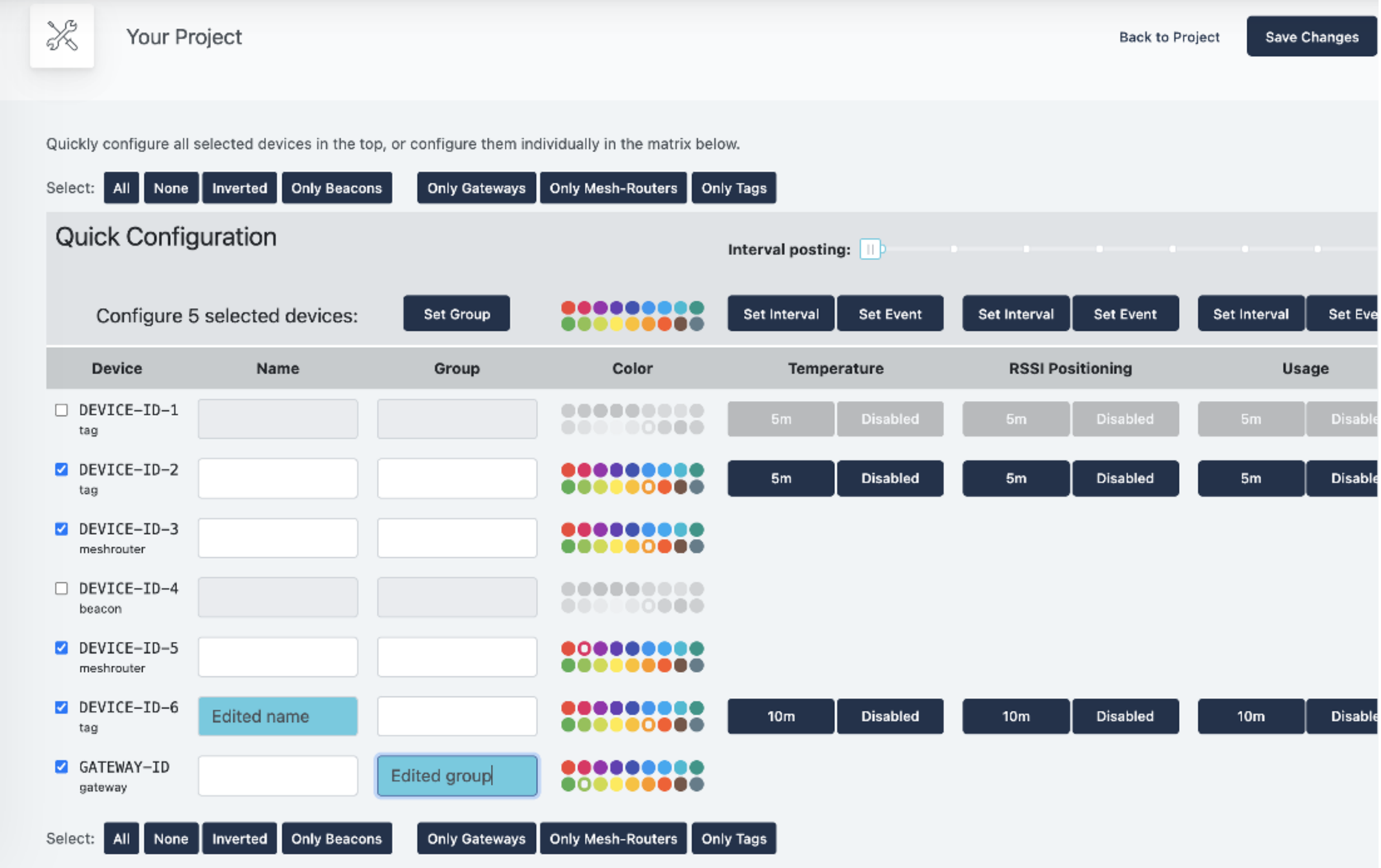
**Step 3.** Zoom into your site location on the map. Select your level on the left-hand side, and the floorplan will appear on the map. Drag and drop the corners to fit the map, and check so the scale is the same as the map scale, visible in the bottom right.

**Step 4.** Click *Exit Edit Mode* on the right-hand side menu. Choose the Floor in the drop down menu labeled *Select Floor*.

# Configure your system

## Devices

You configure your devices by selecting the devices you want to configure under the the `Devices` tab and clicking *Manage*.



Your Project
Back to Project
Save Changes

Quickly configure all selected devices in the top, or configure them individually in the matrix below.

Select: All None Inverted Only Beacons Only Gateways Only Mesh-Routers Only Tags

Quick Configuration

Interval posting:

Configure 5 selected devices:

Set Group
Set Interval Set Event Set Interval Set Event Set Interval Set Eve

| Device | Name | Group | Color | Temperature | | RSSI Positioning | | Usage | |
|---|---|---|---|---|---|---|---|---|---|
| ☐ DEVICE-ID-1<br>tag | | | | 5m | Disabled | 5m | Disabled | 5m | Disable |
| ☑ DEVICE-ID-2<br>tag | | | | 5m | Disabled | 5m | Disabled | 5m | Disable |
| ☑ DEVICE-ID-3<br>meshrouter | | | | | | | | | |
| ☐ DEVICE-ID-4<br>beacon | | | | | | | | | |
| ☑ DEVICE-ID-5<br>meshrouter | | | | | | | | | |
| ☑ DEVICE-ID-6<br>tag | Edited name | | | 10m | Disabled | 10m | Disabled | 10m | Disable |
| ☑ GATEWAY-ID<br>gateway | | Edited group | | | | | | | |

Select: All None Inverted Only Beacons Only Gateways Only Mesh-Routers Only Tags

## Gateway

The gateway serves as a proxy for the data, passing it on from the network up to cloud. It is not a configurable device in the same sense as a mesh-router and a TrakSense360.

What you can configure is a *Name* for your gateway for easier identification, as well as a *Group*. A group can be used when filtering devices on the map in `Visualization` tab.

## Mesh-Router

The mesh-routers route data in the network and they are an instrumental part of positioning. If the mesh-routers do not have a good connection between each other, the network will not perform as intended. To monitor the network connection, mesh-routers post the signal-strength (dB) and link quality of its neighbors.

There are two ways of setting a posting interval for a mesh-router. Under *Settings*, you can activate *Interval-based data* and/or *Event-based data* posting.

- For interval-based data you set the posting interval by using the slider above.
- For event-based data you set the difference in signal-strength (dB) for what should count as an event. You also set the sampling interval (s) for an event.

> **NOTE: The battery-lifetime and congestion likelihood is affected by how often you set the posting interval.**

You can set a *Name* for your mesh-router for easier identification, as well as add your mesh-router to a *Group*. A group can be used when filtering devices on the map in `Visualization` tab.

## TrakSense360

The TrakSense360 posts sensor data up to the Wittra portal on a configurable interval.

There are two ways of setting a posting interval for a TrakSense360: *Interval-based data* and *Event-based data* posting. Event-based data is only applicable for Battery, Temperature, Network, and Usage (Moving/Stationary).

Under *Settings* for each sensor, you can activate *Interval-based data* and/or *Event-based data* posting.

- For interval-based data you set the posting interval for **all** sensors by using the slider under *Sensor data posting interval*.
- For event-based data you set a trigger for a specific event per sensor and set the sampling interval (s) for an event.

You can set a *Name* for your TrakSense360 for easier identification, as well as add your TrakSense360 to a *Group*. A group can be used when filtering devices on the map in `Visualization` tab.

### Data tab

For each TrakSense360, you see all sensors' current values, and how it has changed between posts. We currently support the following sensors:

- Battery
- Temperature
- Usage (moving/stationary)
- Accelerometer
- Magnetometer

### Network tab

For each TrakSense360, you can see a table of its closest neighbors and the signal strength between the TrakSense360 and its neighbor. The signal strength of a TrakSense360's neighbors affects the positioning functionality.

# Settings

You can configure your full system under the `Settings` tab in your project.

## System version

Here you can set your system's **System version**. Once you have set your system version, an **automatic update** is triggered and the TrakSense360 and mesh-routers will be automatically upgraded over 6LoWPAN. The automatic procedure may take up to 24 h, so to speed things up you can collect your devices and set them in Manual update mode, as described in **Manual Update**

## Network settings

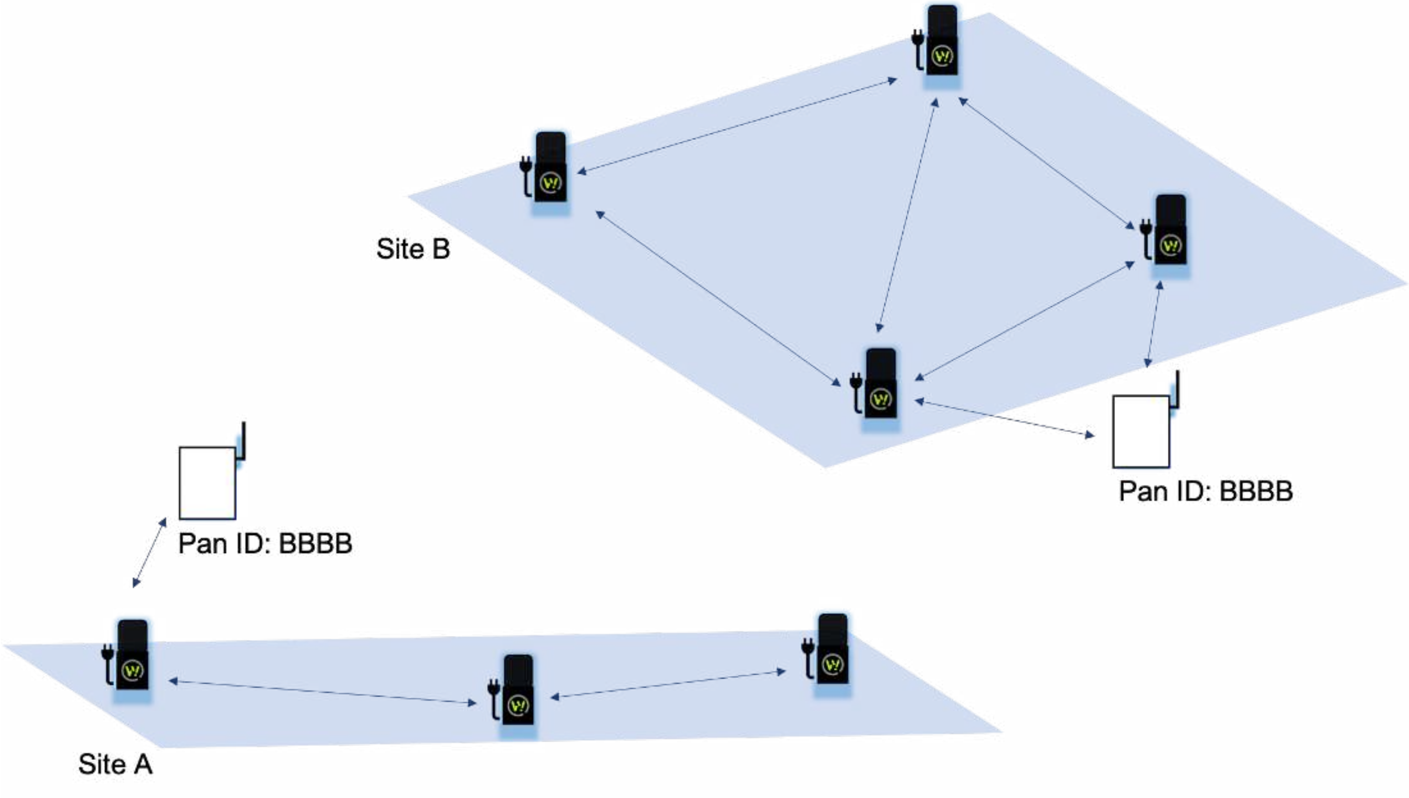
Here you can set a PAN-ID for your network, if you want to connect two networks e.g. on two different sites. To setup roaming between two sites, they both neeed to have the same PAN-ID.

### Roaming

You can enable roaming between two or more networks. Note that these networks should not be within range of each other. To enable roaming, follow these steps:

1. Copy the `security.txt` file from gateway B and replace the `security.txt` file in gateway A with this copy.
2. Change the PAN-ID of gateway A to the one of gateway B

> **NOTE: You will need to manually update all the devices in network A for this change to take effect.**



## Re-naming project

Here you can re-name your project.

## Delete Project

Here you can delete your project. Note that this step is permanent, and hence, follow the warnings carefully.

# Updating security settings

We use a secure-by-design approach where we incorporate security from the early architecture design stage and throughout the evolution of the products. Read more about security measures employed in **Secure system**.

It's good practice to update security settings from time to time. Another reason could be to enable roaming between two sites, see more information on **Roaming**

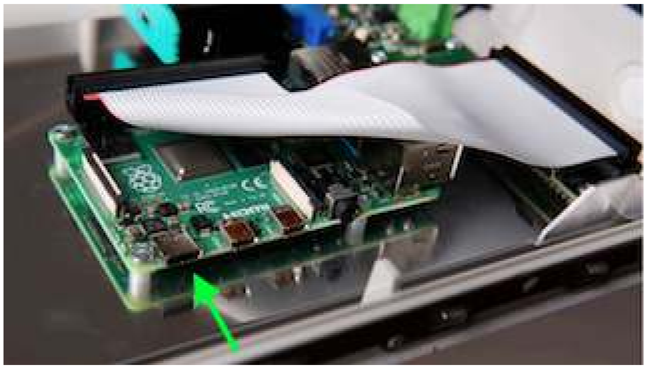
## Updating DTLS keys

Follow these steps on the gateway.

1. Disconnect the 12 V Power Supply if it is connected.

2. Connect a USB-A to USB-C cable with the USB-A end into a computer and the USB-C end into the Gateway.

> **WARNING! The Gateway cannot be powered by the 12 V Power Supply when connecting the USB-C cable to the Raspberry Pi, because this can damage the USB port of the computer!**


USB cable

> **NOTE: You need to provide the USB-A to USB-C cable yourself.**

> **NOTE: A USB-C to USB-C cable will not work according to raspberrypi.org. If the computer doesn't have a USB-A connection, you need to use a USB-C/USB-A adapter.**

3. Wait for the gateway to boot. It can take up to 3 minutes.
4. A virtual USB flash drive will be mounted and show up in the device list on your computer.
5. Open the USB flash drive, and open `security.txt` and follow the guidelines in the file.
6. Safely eject/unmount the virtual USB flash drive.
7. Unplug the USB-A to USB-C cable.
8. Continue with **Power the Wittra Gateway**.
9. Collect all your devices and do a manual update. Follow the steps in **Manual update**

> **NOTE: You will need to manually update all the devices in the network for this change to take effect.**

# Troubleshooting

Have an issue? Look here for support.

# General

## Unboxing and Getting Started

### My IoT Out of the Box is not working

1. Look through this page to see if a more specific question matches the issue you have experienced.
2. See My Gateway is not working.
3. Ensure that all hardware looks intact. If not, please contact the supplier.

## Can I set up my sensor network outdoors?

In short, yes. However, there are two main considerations for this:

1. It is only the TrakSense360 that is weatherproof. If you set up the gateway or the mesh-routers outdoors they need to be protected from different weather conditions, such as rain.
2. The gateway is a **trusted device**, which should be located where you have physical protection against malicious agents.

## Where do I find my batch token?

The batch token is printed on a sticker inside your IoT Out of the Box, it should be visible after removing your Gateway from the kit.

## I do not have a power supply/power cable

The devices require standard Micro-USB charging devices, see details in the respective device datasheet. The hardware can be purchased from your Wittra hardware supplier or any supplier who offers a standard micro-USB charger that follows the requirements in the datasheet and Micro-USB standards.

## I don't have an USB-A to USB-C adapter

The adapter can be purchased from any supplier offering the standard adapter according to the USB standards.

## My IoT Out of the Box is missing parts

Please contact the supplier from whom you purchased the "IOT OUT OF THE BOX".

## How many TrakSense360 and mesh-routers can I connect to the network

Your subscription will state the number of devices you can connect to your network. The maximum number of mesh-routers are depending on the number of TrakSense360 and traffic in your network. Please contact Wittra Customer Support for further information and network dimensioning.

## My device does not blink when I am charging it

When external power is detected, the device blinks once. It will slowly pulse while charging, then stop as soon as the battery is full. If a device never blinks even when connecting power, try resetting it. If it still does not work, it probably means the internal battery is broken, and the device needs replacement. You are welcome to contact our **customer support**.

# Other Issues

## I can't find a solution to my problem

If you cannot find the solution to the problem(s) you are experiencing you can contact our **customer support**.

## How do I contact customer support?

The email address to our customer support is **support@wittra.se**. Also, you can find more information on the **support page**.

## I would like to buy more TrakSense360, gateways and mesh-routers

Please contact your Wittra hardware supplier for additional sales.

## I would like to return my IoT Out of the Box

Please contact your supplier from whom you purchased the "IOT OUT OF THE BOX".

## I would like to return my gateway

Please contact your supplier from whom you purchased the gateway.

## I would like to return my mesh-router

Please contact your supplier from whom you purchased the mesh-router.

## I would like to return my TrakSense360

Please contact your supplier from whom you purchased the TrakSense360.

## I have lost my release key for the USB connector cover protection

Please contact your Wittra hardware supplier for additional sales.

# Gateway

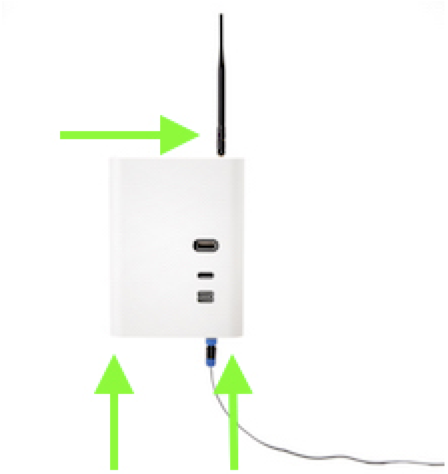
## Unboxing and Getting Started

### How do I install a new Gateway?

Please have a look at the Set-up your Wittra Gateway section in the Getting started guide.

### I can’t open my Gateway

The Gateway is opened by pushing the two side locks upwards. These can be found on the underside of the gateway (marked by two green arrows in the picture below). Note that the right side lock can only be fastened on the right side and the left side lock can only be fastened on the left side.



### How do I see if my Gateway is working?

In the Wittra portal, navigate to the project for which you have registered the gateway. Once in the project view, you can see a list of gateways on the left-hand side. You should now be able to locate your gateway ID in the list. If the gateway's status shows up as green it is working.

If you have not yet registered the gateway, go to the Wittra portal and follow the registration instructions. If you have registered the gateway but it is not in the list of gateways on the portal, please see section My gateway is not working.

### Why is the gateway blinking?

The gateway starts blinking to indicate when it is updating. There are two blinking patterns:

- A blue LED will blink during the gateway system's update process.
- A red LED will blink during the border router's update process.

## Why is my Gateway communicating with connman.net?

ConnMan is a connection manager used by the Gateway to maintain Internet connectivity. The Gateway is expected to initiate traffic to connman.net. If this traffic is blacklisted by your firewall, you can safely whitelist the website.

## My Gateway is not working

If you have a gateway that is **not** visible on the portal go to part 1, otherwise go directly to part 2.

### Part 1. Gateway is offline in portal

Please start by opening the gateway casing and check that the power LED on the Raspberry Pi shows a steady red and that the motherboard's (the board on which the border router is mounted) LED shows a steady green. If not please check that all cables are plugged in correctly and that the gateway is powered up.

If you got the gateway powered up, please proceed with the steps below.

The green LED on the Raspberry Pi itself indicates the network connection state. First check that the green LED on the Raspberry Pi itself is lit a solid green, which indicates that the Raspberry Pi has been able to connect to your LAN and the Internet.

If the LED is not a steady green light this might indicate that something is wrong with the LAN itself. Otherwise it could indicate that the gateway can connect to the LAN, but is not able to connect to the Internet.

This table depicts the two LED indicators of the Raspberry Pi:

| LED Color | Blink pattern | Status |
|---|---|---|
| RED LED | Steady on | The Gateway is powered. |
| Green LED | Steady off | The Gateway is not connected to any network.(There might be a link-local connection, but no IP address has been acquired) |
| Green LED | 1 short blink and then 1 second off | The Gateway has connected to the local network but has not yet verified that there is Internet access. |
| Green LED | Steady on | The Gateway has connected to the network and was also successful in accessing the Internet. |

After having verified that the Raspberry Pi is able to connect to the LAN and the Internet, try restarting your gateway to see if the error disappears and that the gateway shows up on the Wittra portal with status green (online).

If the gateway still does not appear online in the portal the problem can be that port 443 is blocked on your network. In this case the physical LED would still indicate that the gateway can connect to the network, but some services on the gateway can not connect to Wittra's cloud services as this requires port 443 to be open for outgoing TCP traffic.

If that does not help, please revisit the setup instructions in the **Getting started documentation** and verify that you have set up the Internet connection correctly.

#### Part 2. Gateway is online in portal but is not working correctly

If the Gateway is online on the Wittra portal it means it has been set up correctly to the Internet. First try and restart your gateway to see if the error disappears.

If that is not the case, please try and update the gateway on the **Wittra portal**.

If the gateway still is not working, try to perform the update procedure again.

## Configuration and Settings

### How do I connect my Gateway to my router via an Ethernet cable?

Please look in the **Setup an Internet connection** section of the **Getting started** documentation.

# Mesh-Router and Positioning Beacon

## General

### How do I charge my mesh-router or positioning beacon?

The device could be charged using a standard Micro-USB charger but should always be deployed and installed using fixed power.

### How do I see when my device is fully charged?

When charging, your device's LED will pulse slowly. Once the battery is fully charged, the LED will turn off. When plugging external power, if the battery is already full, the LED will blink twice before turning off.

### I need to reset my device

The mesh-router and positioning beacon are reset the same way as a **TrakSense360**.

## Mounting and Attaching

### Can I use my mesh-router or positioning beacon in cold climate

The temperature ranges for mesh-router and positioning beacon specified in the mesh-router **datasheet**

### Do I need to protect my mesh-router and positioning beacon in heavy rain?

The mesh-router and positioning beacon should not be exposed to heavy rain. If you are mounting your device outdoors, please set it up under rain cover, e.g. under the eaves of a building.

## Upgrade and Updates

### After an update of the mesh-router, the mesh-router is not working

Please allow some time to pass after an update to allow the mesh-router to come back online. It might be the case that other devices in the mesh network have not finished updating yet. Please also ensure that the mesh-router is plugged into a power source.

If the problem persists after other mesh-routers are online with the same version, try using your OTG adapter to reboot the device close to a mesh-router which is showing up as online in the portal.

If the device still is not coming online, try to perform the update procedure again.

# TrakSense360

## General

### How do I charge my TrakSense360?

Remove the USB connector cover protection using the included release key tool. This will expose the micro-USB charging port. To charge, plug in the included USB charger using a micro-USB cable.

### My TrakSense360 doesn't seem to charge

If the TrakSense360 is not indicating a **charge pattern** and is not posting data, try to **reset the TrakSense360** using the OTG adapter.

If the problem persists, please contact the support of your supplier from whom you purchased the TrakSense360.

### How do I see when a TrakSense360 is fully charged?

When charging, your TrakSense360 will blink slowly. The LED will be on for three seconds, then off for three seconds, and so on. Once the battery is full, the LED will stop blinking in this pattern.

### I need to reset my TrakSense360

Use the OTG adapter included in the kit to plug into the micro USB connector at the top of the device, you should see two quick blinks which indicate that the device has rebooted and the OTG adapter can be unplugged.

### Do I need to protect my TrakSense360 in heavy rain?

Your TrakSense360 is designed for full exposure to all types of weather. Just ensure that the USB connector cover is properly attached.

## Configuration and Settings

### Can I change the interval when the TrakSense360 is sending data?

Yes, in the **Wittra portal**, it is possible to set the update interval for each sensor and TrakSense360.

## Upgrade and Update

### I need to update my TrakSense360

When a TrakSense360 needs an update its version will be marked in orange in the **Wittra portal**, at the top of the project page the **Update devices** button will take you through the update wizard.

### After an update of the TrakSense360, the TrakSense360 is not working

Please allow some time to pass after an update to allow the TrakSense360 to come back online. It might be the case that other devices in the mesh network have not finished updating yet. Please also ensure that the TrakSense360 has a sufficient battery charge.

If the problem persists after other mesh-routers and TrakSense360 are online with the same version, try using your OTG adapter to reboot the device close to a mesh-router which is showing up as online in the portal.

If the device still is not coming online, try to perform the update procedure again.

# API

## General

### Where do I set my Webhook address?

Please look at Register an integration for information on how to register a Webhook.

### The Webhook is not working

Make sure that the Webhook server is reachable from the internet, i.e. that no firewall blocks incoming TCP traffic on the port used by the server. Take a look at our examples on how to set up a test Webhook server.

### What is the format of the streamed sensor data?

Please look at Data payload for more information regarding the payload in the data stream.

### What type of sensor data do I receive?

Please look at Sensor data for more information regarding the sensor data in the data stream.

### Where do I find examples of what applications and services I can build?

There are examples and accompanying documentation available in Wittra's examples GitHub repository.

### Can I have more than one integration/Webhook?

Yes, you can add multiple integrations to your project. Note that the same data will be sent to all integrations. This can be useful if you want your data to go into multiple existing systems.

# Datasheets

Datasheets for Wittra Products are available for download in PDF format using the links below.

- Wittra IoT Out of the Box
- Wittra TrakSense360
- Wittra Mesh-Router
- Wittra Gateway

# Release Notes

# 14 January 2022

## Portal Version 6.0.4

- Improved support for external sensor.
- Removal of accuracy indicator on the map.
- Support for adding devices using QR code and adding multiple devices to projects.
- Bug fixes.

## System Version 5.3.1

- Time-of-Flight positioning.
- Improved security of release pipelines.
- Improved network scalability and positioning.

# 5 November 2021

## Portal Version 6.0.0

- Improved Cumulocity integration.
- Bug fixes.

## System Version 5.2.1

- Improved manual and automatic update procedures.
- Improved network scalability.
- Improved gateway stability.

# 10 September 2021

## System Version 5.1.0

- Improved network scalability and positioning accuracy.
- Event-based data posting is now supported in the LPTH click-on sensor.
- New gateway internal controlling services.
- Gateway positioning algorithm updates.
- Fixed a bug where devices would fetch configurations more often than expected.

- Various bug fixes.

## Portal Version 5.1.0

- Better email validation before inviting users to join the organization or project.
- Stricter validation for names when creating an organization or project.
- 'Subscription' is split into two views - 'Active Subscription' and 'Switch Tier'.
- Show the owner of the organization along with the email-id under User Access.
- Option to select/deselect all the permissions at once under User Access.
- Added integration examples to enhance Software Integrator's experience.
- Various bug fixes.

# 16 July 2021

## System Version 5.0.0

- Support for clip-on hardware.
- Improvements to the WIPE (positioning) algorithm.
- Improvements to the automatic update process for increased efficiency.
- The gateway reports its IP addresses to the cloud service.
- Improved network performance by optimizing radio usage.
- Improved proximity and RSSI probing and responses.

## Portal Version 5.0.0

- Support for clip-on hardware.
- Possibility to integrate a project in the portal with Cumulocity.
- New table with network link quality data.
- Possibility to move devices between projects.
- Bug fixes.

# 4 June 2021

## System Version 4.1.0

- Introduced RSSI-based 3D positioning of TrakSense360.
- The internal logic in the proximity feature has been improved.

## Portal Version 4.10.0

- Support for managing floors in the map, to facilitate 3D positioning of TrakSense360.
- When adding, changing or removing devices, events are propagated to the integrations of the project in question.
- Increased responsiveness and other improvements to the device list in the project view.
- Improved list of neighbors in the device drawer.
- Devices can no longer be configured in the device drawer. To configure a device, go to the Manage devices view in the project.

# 18 May 2021

## System Version 4.0.0

Please note that this is a new major version. If you upgrade to this version, you need to upgrade all devices in the IoT network, and not just a subset of them. The update needs to be performed manually.

- New logging functionality in the gateway, to allow for easier troubleshooting and customer support.
- Improved security through increased entropy in the DTLS keys.
- The border router capacity size is now increased to support up to 500 devices in a network.
- Gateways can now be rebooted remotely.
- The functionality of the LED has changed. When a device is connected to a charger, the LED will pulse if the device is charging or be steady ON if the device is fully charged. When a device is not connected to a charger, the LED will be off.

- Data from adjacent Wittra networks will now be filtered out.
- Improved the joining procedure for networks that are populated by many mesh-routers.
- Multiple bug fixes to increase long-term network stability, scalability and battery lifetime.

# 12 May 2021

## Portal Version 4.9.0

- New price model.
- Possibility to configure all your devices in just a few clicks. This is accessible from the Manage button in the device list of a project.
- Improved responsiveness and overall speed when navigating in organizations and projects.
- Storage of historical device data.
- Possibility to set permissions users that have been invited to organizations, even if they haven't responded to the invitation.
- Improved views for users with mobile devices or narrow windows.
- Bug fixes.

# 18 March 2021

## System Version 3.4.0

- The calculation that limits a device from sending too much data now takes the region (Europe or North America) into account.
- Increased the size of each data block when sending firmware to devices, resulting in faster automatic updates.
- Adjusted timings when the device is joining a network to save battery power.
- Fixed a bug that caused the gyroscope to report too small values.
- Fixed a bug when devices posts data that could previously cause the device to run out of free memory.

- The initialization sequence for each device has been refactored for improved stability.
- Various bug fixes.
- Cloud config automatically propagates to GW services.
- Gateways can now update up to three devices simultaneously, in Manual Update Mode.
- New version of Tunslip6 for the border-router in the gateway.
- Gateway contains software license information in the file system.
- Various bug fixes.

## Portal Version 4.6.1

- Possible to see why a device has rebooted in the in detailed view of a service.
- These release notes are now present in the home page of the portal, as well as in the documentation.
- Users that are added to an organisation are now only invited, and not directly added.
- Some columns/cells in the device table have had descriptions added, visible when hovering above them.
- Possibility to upgrade and downgrade between subscription tiers.
- Each project is now tied to a specific region; Europe or North America.
- Clarifications in the modal for performing manual firmware updates.
- Clarifications when changing the system version for a project.
- Possibility to edit the name of a project.
- Added a column with timestamps indicating when a device was started (uptime).
- Improved and extended documentation.
- Many bug fixes.

# 1 March 2021

## System Version 3.3.0

- Improved Manual Update OAD procedure.
- Bug fixes in security chip.
- Minor changes to the HW PIN driver.
- The network traffic through the border router is now monitored, and if the region specific regulations are exceeded it will turn off radio traffic. (This previously existed only on TrakSense360 and MRs.)
- Several improvements to RSSI proximity, to achieve higher accuracy and faster responsiveness.
- Fixed an issue where devices would be unable to transmit.
- If a device is put into Manual Update Mode when there is an automatic update running, the device will no longer boot back into the old application.

## Portal Version 4.4.2

- Editing the PAN ID of a network is now done in the project settings view.
- Improved the map view when many devices are at located close to each other.
- Several bug fixes.

# 12 February 2021

## System Version 3.2.0

- TPM bug fixed in mb-watchdogd on the gateway.
- Several improvements have been done to ensure network stability.

## Portal Version 4.3.0

- New flow for manually updating device firmware.
- Refined network deployment tool.
- Possibility to leave organizations.

# 28 January 2021

### Portal Version 4.1.1

- Optimization of realtime data propagated to the portal
- Minor bug fixes
- Performance update to the data fetching in the portal

## 22 January 2021

### System Version 3.1.0

Please note that this is a new major version. If you upgrade to this version, you need to upgrade all devices in the IoT network, and not just a subset of them.

- Introduced experimental support for geographical positioning of TrakSense360. This is built upon RSSI values from TrakSense360 and mesh-routers, and requires no additional hardware.
- Introduced support for Frequency Hopping, which removes the need to set a specific frequency for the Sub-GHz network, between TrakSense360, mesh-routers and gateways. This increases reliability as well as throughput, allowing for larger networks to be built and more data to be sent.
- TrakSense360 now post battery information, with an expected remaining percentage.
- Now supports greater distance 6LoWPAN updates over the Wittra network
- When upgrading firmware automatically, the estimated time until completion is now sent by the devices that are being updated.
- COAP stability enhancements w.r.t. reconnection and timeout
- TrakSense360 now post a heartbeat message every five minutes.
- TrakSense360 now post the total transmission (TX) time.
- The underlying operating system for TrakSense360 and mesh-routers has been changed to TI-RTOS.
- Radio usage for each device is now reported to the cloud portal.
- Temperature and battery data can now be received in the cloud portal as event-based data. The configuration is done in the portal.
- Devices now report their uptime for the duration that they have been on.

### Portal Version 4.0.3

- The portal has been reworked in its entirety. With the new portal, you will get crucial information about your Wittra IoT devices with fewer clicks, and it is easier to get an overview of your Wittra system.

- It is now possible to put labels on devices, allowing to group devices e.g. in the same building or on the same floor.

- It is now possible to upload image layers on top of the map, e.g. custom blueprints of a building.

- True position of gateways and mesh-routers can be set in the map for a project.

- The portal displays battery information received from the TrakSense360.

- If the location of a TrakSense360 has been measured with the aforementioned experimental RSSI-based positioning, it will show up in the new *Visualization* tab, in the view for a project in the portal.

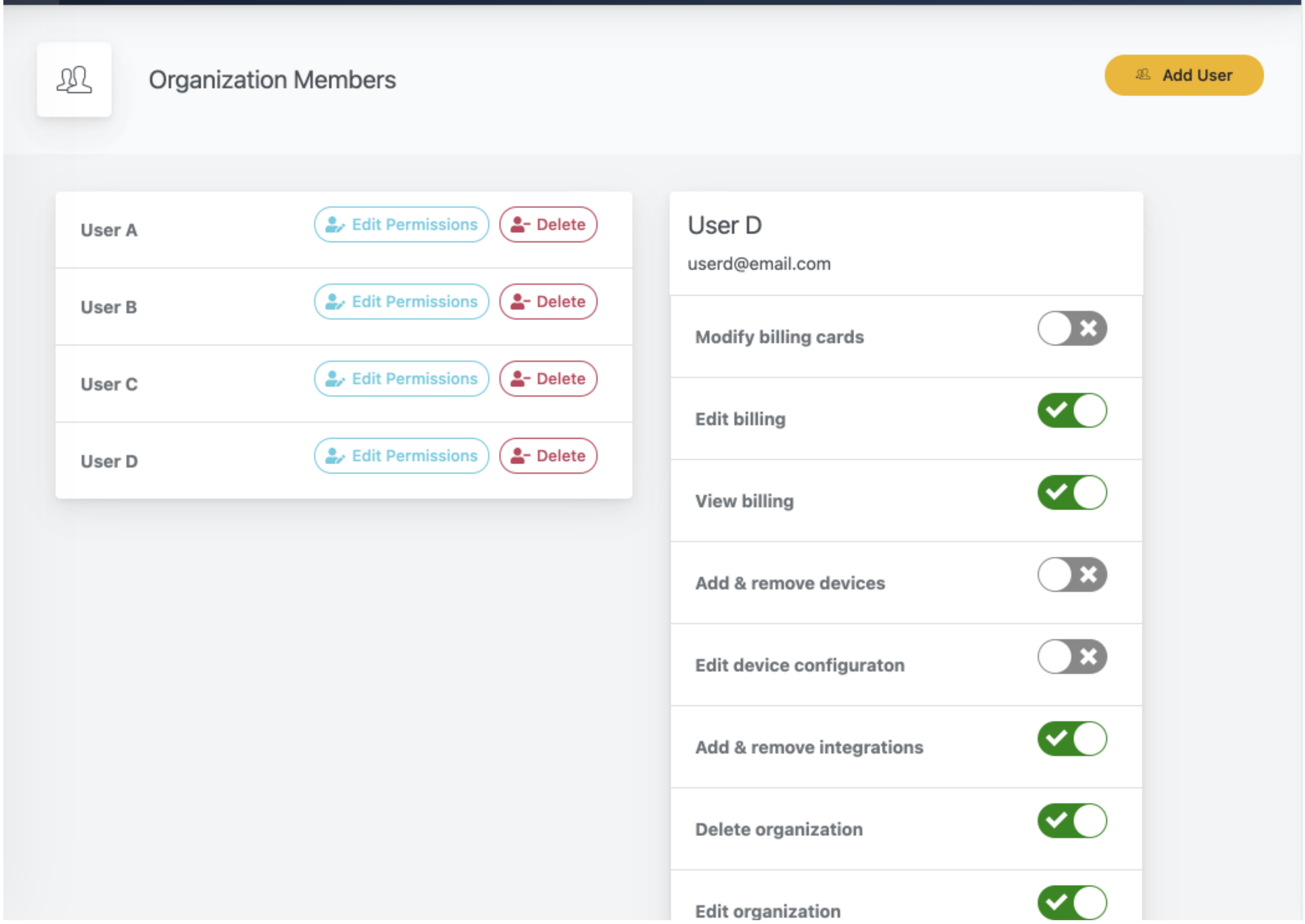
- The portal is now event-driven in the sense that both changes and new data are now instantaneously displayed.

- Automatic update of the system is now available. With one click, all devices in a project can now be automatically updated within 24-hours.

- It is possible to choose any supported system version for a project, instead of only the latest.

- Deployment tool. A graph showing the relationship between the components in a Wittra IoT network. Deployment tool

- Permissions have been added on an organization level. It is now possible to restrict or grant users permissions to certain views and actions in the portal.



| | | |
|---|---|---|
| User A | Edit Permissions | Delete |
| User B | Edit Permissions | Delete |
| User C | Edit Permissions | Delete |
| User D | Edit Permissions | Delete |

User D

userd@email.com

| | |
|---|---|
| Modify billing cards | ✗ |
| Edit billing | ✓ |
| View billing | ✓ |
| Add & remove devices | ✗ |
| Edit device configuraton | ✗ |
| Add & remove integrations | ✓ |
| Delete organization | ✓ |
| Edit organization | ✓ |

- In the portal, Data Endpoints have been renamed to Integrations.
- It is possible to configure devices to report data only when changes happen (event-based), in addition to reporting at fixed intervals.
- There is an option to configure multiple devices at the same time.
- New payment system:
    - A dedicated Billing page with all billing information. Billing
    - You can now add one or several payment cards to your organization and choose from which card Wittra will charge at the end of the month.
    - Pay outstanding bills directly in the portal.

## Support

If you are having issues getting started with the Wittra IoT Solution, check out our getting started guide If you cannot find your solution there, we also encourage you to look through the Troubleshooting section. You're also welcome to contact us at support@wittra.se for further assistance.

Wittra also offers technical support plans and service packages to help our customers get the most out of the Wittra products. If you are interested in more information about support plans and service packages, please contact support@wittra.se.

# Hardware support

If you have issues with your hardware please check out the Troubleshooting section. If there would be any hardware failure please use the Warranty Claims Checklist to verify any hardware failure. In the case of hardware failure please check the Wittra Claims Process for Warrant Handling as guidelines on how to move forward with your hardware issues.

The initial step of the process is to apply for a claim template and Return Material Authorization (RMA) number from Wittra. The claim is to be made via support@wittra.se

**Important! Mark email as "Request for RMA number "**

# Legal

Legal documents about Wittra's products and service, as well as compliance and operating information.

## Regulatory Compliance and Safety Information

Responsible party: Wittra Networks AB
Contact: support@wittra.se

### Gateway

| | EU | US |
|---|---|---|
| Product Name | GATEWAY 1.0 EU | GATEWAY 1.0 US |
| Model Number | GATEWAY-1.0-EU | GATEWAY-1.0-US |
| Part Number | 1000186 | 1000347 |

> *WARNING Gateway*
> **Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.**
> **This product shall only be connected to the external power supply provided by Wittra, rated at 5V DC, and a maximum current of 1500 – 2000 mA.**
> **This product should not be used within 20 cm of the body.**

### Instructions for safe use

To avoid malfunction or damage to your Gateway please observe the following:
Keep the device away from water, fire, humidity or hot environments.

Do **not** expose it to exaggerated heat or cold, the Gateway is designed for reliable operation at normal ambient room temperatures.

Do **not** attempt to disassemble, repair or modify the device.

Do **not** use a damaged charger or USB cable to charge the device.

Do **not** use any other chargers than those recommended.

Do **not** use the device where wireless device are not allowed.

Do **not** disassemble, crush, puncture, short external contacts, or dispose of the battery in fire or water.

Take care whilst handling the Gateway to avoid mechanical damage or discharge that might cause electrical damage.

# Border Router

| | **EU and US** |
|---|---|
| Product Name | BORDER ROUTER 1.0 |
| Model Number | BORDER-ROUTER-1.0 |
| Part Number | 1000239 |

> *WARNING Border Router*
> **Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.**
> **This product shall only be connected to an external power via the Gateway.**
> **This product should not be operated at temperatures below -10 or over +60 Degrees Celsius.**

## Instructions for safe use

To avoid malfunction or damage to your Border Router please observe the following:

Keep the device away from water, fire, humidity or hot environments.

Do **not** attempt to disassemble, repair or modify the device.

Do **not** use a damaged charger or USB cable to charge the device.

Do **not** use any other chargers than those recommended.

Do **not** use the device where wireless device are not allowed.

Do **not** disassemble, crush, puncture, short external contacts, or dispose of the battery in fire or water.

Do **not** expose it to exaggerated heat or cold, the Border Router is designed for reliable operation at temperatures ranging from -10 to +60 Degrees Celsius.

Do **not** attempt to remove or otherwise separate the device from the casing, this might cause mechanical or electrical damage to the product.

Do **not** remove the Border Router from the inside of the Gateway, this will cause the whole Network to go down and might also damage the Gateway and/or Border Router.

Take care whilst handling to avoid mechanical damage.

# TrakSense360

| | EU | US |
|---|---|---|
| Product Name | SENSOR TAG 1.0 EU | SENSOR TAG 1.0 US |
| Model Number | SENSOR-TAG-1.0-EU | SENSOR-TAG-1.0-US |
| Part Number | 1000158 | 1000348 |

> *WARNING TrakSense360*
> **Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.**
> **This product shall only be connected to an external power supply rated at 5 V DC, and minimum current of 100 mA. Any external power supply used with the TrakSense360 shall comply with relevant regulations and standards applicable in the country of intended use.**
> **This product is only deemed waterproof according to IP67 if the protection cover to the microUSB charger is on.**
> **This product should not be operated at temperatures below -10 or over +60 Degrees Celsius.**

## Instructions for safe use

To avoid malfunction or damage to your TrakSense360 please observe the following:
Keep the device away from water, fire, humidity or hot environments.
Do **not** attempt to disassemble, repair or modify the device.
Do **not** use a damaged charger or USB cable to charge the device.
Do **not** use any other chargers than those recommended.
Do **not** use the device where wireless device are not allowed.
Do **not** disassemble, crush, puncture, short external contacts, or dispose of the battery in fire or water.
Do **not** expose it to water, moisture or place on a conductive surface whilst in operation when the protection cover is off.
Do **not** expose it to exaggerated heat or cold, the TrakSense360 is designed for reliable operation at temperatures ranging from -10 to +60 Degrees Celsius.
Do **not** charge the battery at temperatures outside of room temperature between +10 to +45 Degrees Celsius.
Do **not** attempt to remove or otherwise separate the device from the casing, this might cause mechanical or electrical damage to the product.
Take care whilst handling to avoid mechanical damage.

# Mesh-Router

| | EU | US |
|---|---|---|
| Product Name | MESH-ROUTER 1.0 EU | MESH-ROUTER 1.0 US |

| | EU | US |
|---|---|---|
| Model Number | MESHROUTER-1.0-EU | MESHROUTER-1.0-US |
| Part Number | 1000240 | 1000349 |

> *WARNING Mesh-Router*
> **Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.**
> **This product shall only be connected to an external power supply rated at 5 V DC, and minimum current of 100 mA. Any external power supply used with the Mesh-Router shall comply with relevant regulations and standards applicable in the country of intended use.**
> **This product is only deemed waterproof according to IP67 if the protection cover to the microUSB charger is on.**
> **This product should not be operated at temperatures below -10 or over +60 Degrees Celsius.**

### Instructions for safe use

To avoid malfunction or damage to your Mesh-Router please observe the following:
Keep the device away from water, fire, humidity or hot environments.
Do **not** attempt to disassemble, repair or modify the device.
Do **not** use a damaged charger or USB cable to charge the device.
Do **not** use any other chargers than those recommended.
Do **not** use the device where wireless device are not allowed.
Do **not** disassemble, crush, puncture, short external contacts, or dispose of the battery in fire or water.
Do **not** expose it to water, moisture or place on a conductive surface whilst in operation when the protection cover is off.
Do **not** expose it to exaggerated heat or cold, the Mesh-Router is designed for reliable operation at temperatures ranging from -10 to +60 Degrees Celsius.
Do **not** charge the battery at temperatures outside of room temperature between +10 to +45 Degrees Celsius.
Do **not** attempt to remove or otherwise separate the device from the casing, this might cause mechanical or electrical damage to the product.
Take care whilst handling to avoid mechanical damage.

## Compliance Information

This equipment complies with the relevant provisions of the ROHS Directive for the European Union.

This equipment is in conformity with the protection requirements of Directive 2014/53/EU (RED) on the harmonisation of the laws of the Member States.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

Industry Canada Class B Emission Compliance Statement:
RSS-Gen & RSS-247 statement:
This equipment complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

ISED Radiation Exposure Statement:
This equipment complies with Industry Canada RSS-102 and Safety Code 6 radiation exposure limits set forth for an uncontrolled environment.

## WEEE Directive Statement for the European Union

In Common with all Electronic and Electrical products the devices should not be disposed of in household waste. Alternative arrangements may apply in other jurisdictions.

## Warnings

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Shielded Ethernet cable must be used with this unit to ensure compliance with the Class B FCC limits.

# Terms of Service

Describes the rules you agree to when using our service.

Check out the Wittra **Terms of Service (https://www.wittra.se/terms-of-service)**.

# Privacy Policy

Explains what information we collect and why as well as how we use it.

Check out the Wittra **Privacy Policy (https://www.wittra.se/privacy-policy)**.

# Legal Notice

Check out the Wittra **Legal Notice (https://www.wittra.se/legal-notice)**.

# Licenses

Check out the list of **Third party licenses (https://docs.wittra.se/#/licenses)** used.

© 2019. Wittra © 2021.