

# Remote monitoring

Information on integrating radio sensors with Rappt.IO

- [Remote monitoring overview](#)
- [Integrating LoRaWAN sensors with Rappt.IO](#)
- [LoRa Gateway configuration](#)

# Remote monitoring overview

Rappt.IO supports the [remote monitoring of devices \(traps, bait stations etc\) equipped with sensors](#).

The sensors are typically small, battery-powered devices that detect the state of a trap (open/sprung) or the bait levels in a bait station. They transmit this information, normally over a LoRaWan (low-power, wide-area network) radio network, to a gateway or hub, which will then forward the information to Rappt.IO via the Internet.

Sensors are becoming increasingly inexpensive and batteries can last for 2 to 5 years.

The distance a sensor can transmit is very dependent on the terrain. 15km or more is possible over LoRaWan, but 5km to 10km is typical.

The advantages of having sensor-equipped traps or bait stations are many:

- The work effort in servicing installations can be significantly reduced, especially with live capture traps - you only need to service traps that have caught something.
- They can provide critical early detection and incursion information for predator-free areas.
- They are useful for managing contractors and staff. Project administrators can see which traps and stations have been serviced, and when.
- Sensors are very effective for engaging landowners and volunteers - people are much more motivated to service traps if they know there has been some activity.
- For gas and self-resetting traps, it can provide immediate information on activity and can be used to make decisions on placement.

## Remote monitoring products and systems

If you are interested in setting up remote monitoring, you have a few options. For those with a technical bent and interested in building your own sensors or networks we have information on building and [integrating LoRaWan sensors](#) with Rappt.IO and [configuration examples for gateway devices](#).

There is also a range of off-the-shelf products available from various suppliers:

### WheroNet IoT

<https://wheronet-iot.co.nz/>

WheroNet sells sensors (that can be retrofitted to most standard traps), and pre-configured, solar-powered gateways. These are open LoRaWan devices (no subscription costs).

### Predator Free Franklin

<https://predatorfreefranklin.nz/shop-pff/>

PF Franklin created the “T?whiti Smart Cage” which has a Zip autolure and LoRaWan sensor pre-installed. To use this you will need to have a gateway within range - they may be able to [help you with that](#) if you are in the Franklin area.

## **Econode**

<https://www.econode.nz/>

Econode provides the pre-built SmartTrap and sensors that can be fitted to a range of traps. Their product is widely used on a range of predator control projects around New Zealand.

## **Encounter Solutions**

<https://encounter.nz/>

Encounter Solutions provides the Celium platform which is a solution of sensor-equipped traps and network hubs. Their product is widely used on a range of predator control projects around New Zealand.

## **eTrapper**

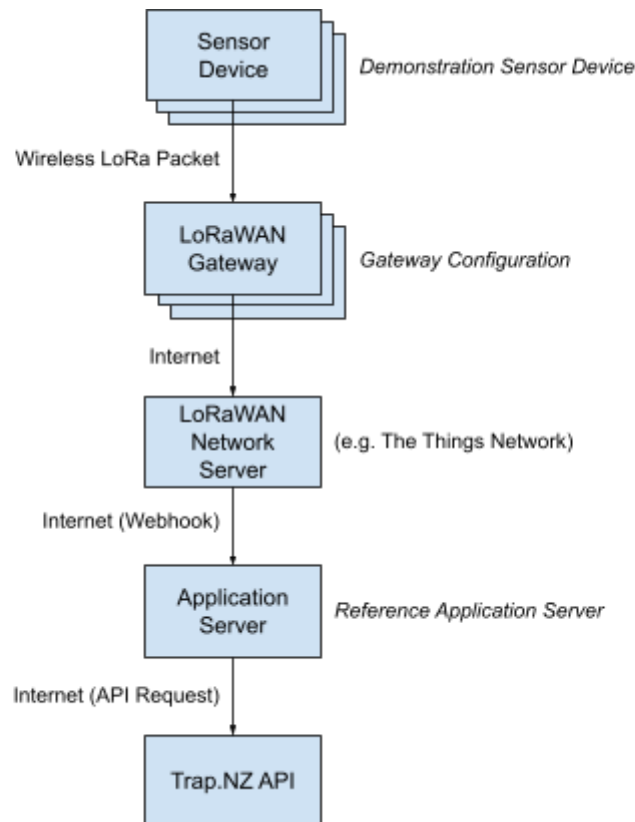
<https://www.etrapper.co.nz/>

eTrapper provides trap sensors, and also a bait station sensor device that measures the level of bait in Philproof bait stations. This information is transmitted to Rappt.IO and allows you to view the bait levels of your stations on the website and app.

# Integrating LoRaWAN sensors with Rappt.IO

This is a blueprint for projects to use to affordably configure sensors to submit data to Rappt.IO using LoRaWAN, a low power long range wide area network protocol.

We provide three components. A *gateway configuration* document explains how to take an off-the-shelf gateway device and set it up to provide LoRaWAN network coverage to nearby sensor devices. A *demonstration sensor device* provides a proof of concept end device, which senses and reports the status of a trap. A *reference application server* receives messages from a sensor via a LoRaWAN network server and relays those messages on to Rappt.IO.



## Gateway Configuration

Our [gateway configuration](#) targets the off-the-shelf [Mikrotik wAP LR9 kit](#). It describes how to configure the device to act as a LoRaWAN gateway for The Things Network.

## Demonstration Sensor Device

Our demonstration sensor device is based on the common [TTGO T-Beam](#) hardware from LILYGO. It is assembled with a 0.96 inch OLED display, an 18650 Li-ion battery, and a switch between two pins to sense trap status.



Pictured is an assembled demo device. The OLED display is visible on the left of the board. The LoRa antenna attaches to the top. The battery is attached underneath the board (not visible). The blue wire at the bottom of the board represents the switch to sense trap status.

The software and documentation for this device can be found at <https://github.com/Groundtruth/sensor-trap-demo-device>.

Once assembled and programmed, the device will connect to a LoRaWAN network and transmit status information both periodically and on status-change events. It implements some basic power-saving measures and reports its battery status. When a debug button is pressed, the OLED displays some diagnostic information about the state of the device. The software can be configured for varying LoRaWAN connection parameters, and various sensor message timings.

Particular attention has been paid to the logic around sending heartbeat messages and safely recording the trap's status. For the case of live traps, it is vital that a sensor never report "set" (open) when it is actually "sprung" (closed).

This hardware is easy to procure and assemble, and the software demonstrates the required functions for a sensor trap. However, the work here was limited in scope and it should be noted that it should not be deployed without further thought. Future work to produce a deployable sensor would involve optimising for lower cost, longer battery life, and performing testing to establish reliability in the field. The current state of this work should provide a starting point for this future work.

## Reference Application Server

The reference application server receives messages from sensor devices, forwarded by a LoRaWAN network server such as The Things Network. It uses client code generated from the Rappt.IO OpenAPI spec to create sensor records on Rappt.IO corresponding to incoming sensor messages.

The software and documentation for the reference application server can be found at

<https://github.com/Groundtruth/sensor-trap-reference-application>.

The reference application server is written in Typescript with minimal dependencies. It opens an HTTP server to receive messages from a The Things Network webhook. The device of an incoming message is uniquely identified by its LoRaWAN DevEUI (device extended unique identifier), which is used to look up corresponding device parameters such as its Rappt.IO sensor ID and expected timeout. An appropriate sensor message is constructed and sent to the Rappt.IO API. The software produces log messages which can be used to monitor and alert for error conditions.

The software can be configured with authorization details for a Rappt.IO sensor provider account. Device configuration is read dynamically from a JSON file, so device information can be updated without restarting the software. Other functions of the software (e.g. webhook listener, device information lookup, sensor message format) are written so as to be easily customised by a sensor provider.

The software is published so that a sensor provider (a person or organisation producing and supporting sensor devices) could adapt and run it for their own devices, or look to it for inspiration on how to implement their own application server.

# LoRa Gateway configuration

## Overview

This document describes how to take an off-the-shelf gateway device and set it up to provide LoRaWAN network coverage to nearby sensor devices. The device used in this example is a [Mikrotik wAP LR9 kit](#) which operates in the 902-928 MHz frequency range

The instructions would also apply to the wAP LR8 kit (863-870 MHz) and other Mikrotik IoT gateway devices.

The LR9 is weatherproof and can be purchased from many NZ suppliers such as [PB Tech](#), [Go Wireless](#), [Ascent](#), etc. We recommend attaching an external antenna (such as the MikroTik LoRa Antenna kit) for better coverage and range.

As with most Mikrotik products it allows for flexible configurations - it includes a 2.4Ghz Wifi radio and can operate as either an access point, or a client to connect to a nearby WiFi access points wirelessly. In this example the device is set up as an access point (i.e. a hotspot) connected to the internet via ethernet (e.g. a residential installation with a lan cable connected to a router).

This setup uses the gateway's built in web interface. Power users will want to use Mikrotik's free [Winbox](#) configuration tool - an [example config](#) file is provided.

## Gateway setup

1. Connect the gateway device via ethernet to your network and power it up. You will be able to connect to it wirelessly - it will have a hotspot name such as Mikrotik-E6B3F9
2. Open your browser and connect to the address <http://192.168.88.1/> and close the initial welcome screen
3. Change the Quick Set drop down to PTP Bridge AP default configuration as follows:

RouterOS v6.49.7 (stable)

Quick Set WebFig Terminal

WISP AP

active

Wireless

Wireless Protocol ☒ 802.11 ☐ nstreme ☐ nv2

Network Name

Frequency  MHz

Band

Channel Width

Country

MAC Address 48:8F:5A:E6:B3:7F

Use Access List (ACL) ☐

Security ☐ WPA ☒ WPA2

Encryption ☒ aes ccm ☐ tkip

WiFi Password  ☒ Hide

Wireless Clients

Configure

Mode ☒ Router ☐ Bridge

Address Acquisition ☐ Static ☒ Automatic ☐ PPPoE

IP Address  Renew Rel

Netmask 255.255.255.0 (/24)

Gateway 192.168.7.1

MAC Address

Firewall Router ☐

Local Net

IP Address

Netmask 255.255.255.0 (/24)

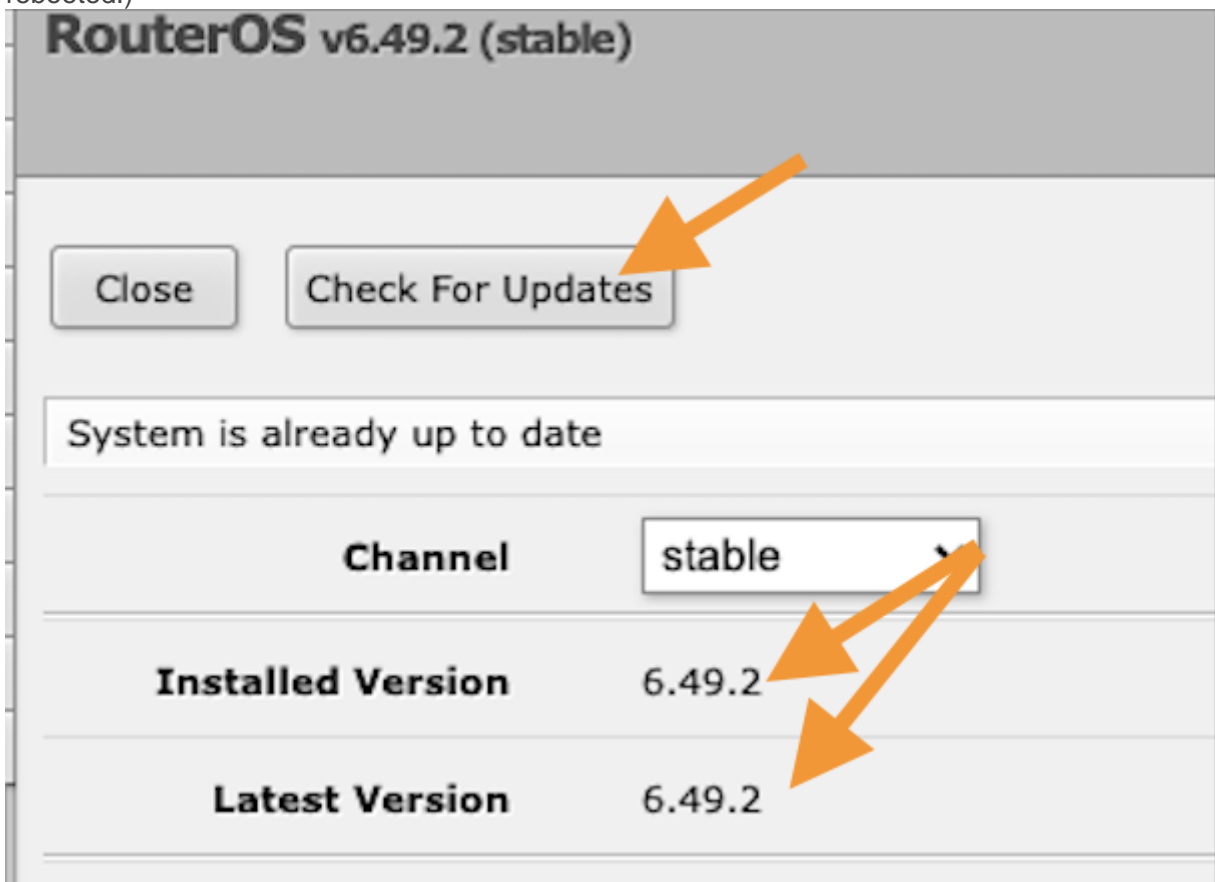
Bridge All LAN Ports ☐

Note this address

- The **Network Name** will become the visible hotspot name
- Set the **Country** to New Zealand
- Set **Security** to WPA2
- Set a good **Wifi Password**
- Make sure **Address Aquisition** is set to Automatic and take a note of the **IP Address** provided
- Turn **Firewall Router** *off* (unchecked). This will allow you to connect to the gateway over the LAN as well as via WiFi.
- Set an admin password (at the bottom of the screen) and apply the configuration.

The gateway will reboot. You will be able to connect to it wirelessly as before (with the new hotspot name), or you can connect to it over the LAN using the IP Address listed.

4. On the Quick Set page, use 'Check for updates' to install the latest firmware (reconnect after it has rebooted.)



5. Click the WebFig tab to open the LoRa > Servers tab. If it is not already listed, add the following:

	Name	Address	Up port	Down port
-	TTN V3 (au1)	au1.cloud.thethings.network	1700	1700
-	TTN V3 (eu1)	eu1.cloud.thethings.network	1700	1700
-	TTN V3 (nam1)	nam1.cloud.thethings.network	1700	1700
-	TTN-EU	eu.mikrotik.thethings.industries	1700	1700
-	TTN-US	us.mikrotik.thethings.industries	1700	1700
-	TTS Cloud (au1)	au1.cloud.thethings.industries	1700	1700
-	TTS Cloud (eu1)	eu1.cloud.thethings.industries	1700	1700
-	TTS Cloud (nam1)	nam1.cloud.thethings.industries	1700	1700



(you can delete the other entries)

6. Under the Devices tab, configure the LoRa router:

The screenshot shows the RouterOS v6.49.7 (stable) configuration interface for the LoRa router. The left sidebar contains a menu with options: CAPsMAN, Wireless, Interfaces, PPP, Bridge, Switch, Mesh, IP, MPLS, Routing, System, Queues, Dot1X, Files, Log, RADIUS, Tools, LoRa, MetaROUTER, Partition, Make SupoutLrif, Undo, Redo, Hide Passwords, Safe Mode, Design Skin, WinBox, Graphs, and End-User License. The main configuration area is titled "RouterOS v6.49.7 (stable)" and contains the following settings:

- Enabled:** ☒ (Red arrow points to this checkbox with the text "Enable".)
- Status:** Disabled
- Name:** gateway-0 (Red arrow points to this field with the text "Leave as default".)
- Hardware ID:** [Redacted]
- Gateway ID:** [Redacted]
- Firmware ID:** 63705e9
- Network Servers:** TTN V3 (au1) (Red arrow points to this dropdown with the text "As defined in network tab".)
- Channel plan:** AU 915 Sub 2 (Red arrow points to this dropdown with the text "AU 915 Sub 2".)
- Antenna Gain:** 6 dBi (Red arrow points to this field with the text "As per your antenna spec".)
- Forward:** ☒ Valid, ☒ Error, ☐ Disabled
- Network:** ☒ Public, ☐ Private
- LBT:** ☐
- Src. Address:** [Redacted]
- Band:** 902-928
- Locks:** [Redacted]
- Spoof GPS:** [Redacted]

## Network service setup

The gateway can now be added to the Things Network. [Create an account](#) on the website first and then **Register a gateway**.

## Register gateway

Register your gateway to enable data traffic between nearby end devices and the network.

Learn more in our guide on [Adding Gateways](#).

Gateway EUI ?

Reset

← Cut and paste your gateway ID

Gateway ID ? \*

← This field will be auto-populated

Gateway name ?

← Choose a name to identify your gateway

Frequency plan ? \*

← Select this plan

☐ Require authenticated connection ?

Choose this option eg. if your gateway is powered by [LoRa Basic Station](#)

Share gateway information

Select which information can be seen by other network participants, including [Packet Broker](#)

☒ Share status within network ?

☒ Share location within network ?

Register gateway

After a few minutes you should see the gateway connected. Set the location settings so that the gateway will be visible to other users.