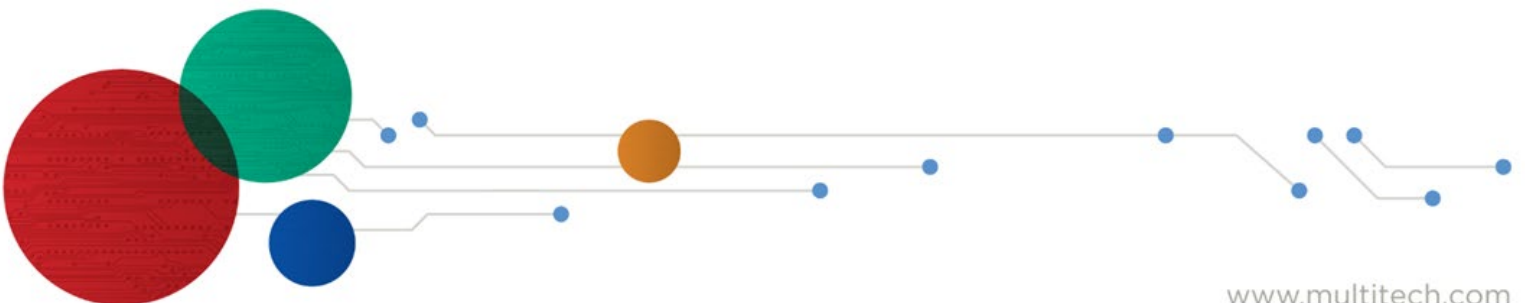


# How to Connect **Reveal™** LoRaWAN Sensors

---



## How to Connect Reveal LoRaWAN Sensors Guide

Document Number: RB00001

### Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. Copyright © 2022 by Multi-Tech Systems, Inc.

### Trademarks and Registered Trademarks

MultiTech, the MultiTech logo, Conduit®, SubGig® and BridgeBee® are registered trademarks and Reveal is a trademark of Multi-Tech Systems, Inc. All other products and technologies are the trademarks or registered trademarks of their respective holders.

### Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Multi-Tech Systems, Inc. Multi-Tech Systems, Inc. provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Multi-Tech Systems, Inc. may make improvements and/or changes in this manual or in the product(s) and/or the software described in this manual at any time.

### Legal Notices

See the [Legal Notices](#) section of the website for up-to-date information on MultiTech warranty, returns policy, privacy statement, terms of sale, and terms of service.

### Customer Support

MultiTech offers free technical support for Reveal sensors at: <https://support.radiobridge.com>

MultiTech also offers technical support plans and service packages to help our customers get the most out of their MultiTech products.

### World Headquarters

Multi-Tech Systems, Inc.

2205 Woodale Drive, Mounds View, MN 55112

# Contents

---

<b>Chapter 1</b>	<b>Overview .....</b>	<b>6</b>
	Introduction.....	6
	Stand-Alone vs Network Provider .....	6
	AppEUI / JoinEUI.....	6
	Revision History.....	7
	Document Conventions.....	7
<b>Chapter 2</b>	<b>The Things Network (TTN) .....</b>	<b>8</b>
	Register through the Console.....	8
	Add Your Gateway.....	8
	Add Devices to Console .....	8
	Connect your own TTN Account.....	9
	Create a New Application on TTN.....	9
	Create API Key on TTN.....	9
	Add Integration to the Console .....	9
	Add Integration to TTN.....	10
	Add Devices to Console .....	10
<b>Chapter 3</b>	<b>MachineQ.....</b>	<b>11</b>
	Registering Devices through the Console .....	11
	Using Your MachineQ Account.....	11
	Create the Output Profile .....	11
	Create the Application.....	12
	Bypassing the Console .....	14
	Add Devices to Console .....	14
<b>Chapter 4</b>	<b>Stand-Alone MultiTech Conduit AP/AEP .....</b>	<b>15</b>
	Add Gateway to the Console.....	15
	Bring the Gateway Online .....	15
	Update Gateway Firmware .....	15
	Enable the LoRa Network Server.....	15
	Install Python Script.....	16
	Add Devices to Gateway.....	16
	Add Devices to the Console.....	17
<b>Chapter 5</b>	<b>ChirpStack .....</b>	<b>18</b>
	Using the Reveal ChirpStack Server.....	18

Configure the ChirpStack Gateway .....	18
Add the ChirpStack Gateway to the Console .....	18
Add Devices to the Console.....	18
Using Your ChirpStack Server .....	19
Configuring HTTP Integration in ChirpStack .....	19
Configuring the Integration in the Console .....	20
Update Your ChirpStack Server Settings .....	21
<b>Chapter 6     Senet .....</b>	<b>22</b>
Registering Devices through Reveal.....	22
Using Your Senet Account .....	22
Request API Key.....	22
AppEUI.....	22
Contract ID and Profile ID.....	23
Notification Target .....	24
Senet Configuration on the Console.....	26
Add Devices to Console .....	26
<b>Chapter 7     Loriot.....</b>	<b>27</b>
Registering Devices through Reveal.....	27
Optional: Add Your Loriot Gateway.....	27
Using your Loriot.io account .....	27
Loriot.io Server Location .....	27
Loriot.io API Key .....	27
Loriot.io Application ID .....	28
Loriot.io Access Token .....	29
Loriot Output.....	29
Add Devices to Console .....	30
<b>Chapter 8     Kerlink Wansey Management Center (WMC) .....</b>	<b>31</b>
Registering Devices through Wanesy.....	31
Add Your Kerlink Gateway.....	31
Update Gateway Firmware .....	31
Configure using the Magic Link .....	32
Add the Gateway.....	32

---

Using your Wanasy Management Center account .....	33
Integrate your WMC Account.....	33
Push Configuration .....	33
Clusters.....	36
Add Devices to Console .....	36
<b>Chapter 9     Third Party Network Servers .....</b>	<b>38</b>
Sensor to Network Server .....	38
Network Server to Console .....	38

# Chapter 1 Overview

## Introduction

Reveal wireless sensors provide full sensor to cloud solutions for Internet of Things (IoT) applications. Reveal LoRaWAN sensors can connect to a variety of LoRaWAN compliant network servers, located either on a local gateway or as a cloud-based network server. From there, the sensor messages can be sent to the web-based console or a third-party application. This document provides instructions for connecting LoRaWAN sensors using several different methods.

For more information on the web-based console, visit <https://console.radiobridge.com>

## Stand-Alone vs Network Provider

A network provider for LoRaWAN will set up LoRa base stations and charge for accessing their network much like a cell phone provider will charge to connect your phone to their network. In some cases, however, it may be desirable to set up a stand-alone gateway that does not use a network provider. Reasons for this may include lack of coverage in remote area or simply reducing the cost when there are many sensors in the field.

## AppEUI / JoinEUI

The LoRaWAN AppEUI, now known as the JoinEUI (they are sometimes used interchangeably), is consistent among Reveal products and thus is not listed on the product labels. Earlier products use a generic, non-unique, JoinEUI, and newer products use a unique JoinEUI as described in the following table.

*Table 1 AppEUI/JoinEUI for Reveal Products*

AppEUI/JoinEUI	Description
01-01-01-01-01-01-01	Used in the following product families: RBS301, RBS304, RBS305, and RBS306
78-94-E8-00-00-00-00	Used in product families not listed above

Note that the AppEUI/JoinEUI can be modified at the time of manufacturing to match the end customer's requirements. Please contact Reveal for more details on customization and pre-configuration



## Revision History

Table 2 Revision History

Revision	Date	Description
1.0	August 2018	Initial release of the document
1.1	September 2018	Added section for general gateways
1.2	January 2019	Added support for TTN
1.3	February 2019	Added process ID for TTN
1.4	May 2019	Added APPEUI definition to TTN
1.5	June 2019	Added Senet
1.6	July 2019	Added Lorient
1.7	February 2020	Added ChirpStack
1.8	April 2020	Additional add gateway features, A
1.9	April 2020	Added new AppEUI/JoinEUI
1.10	June 2020	Added Kerlink integration
1.11	March 2021	New Python script for stand-alone MultiTech gateway
1.12	July 2021	Updated for TTN v3

## Document Conventions

Table 3  
Document  
Conventions

Font / Icon	Meaning
	Important notes
	Warnings and cautions

## Chapter 2 The Things Network (TTN)

The Things Network, also referred to as TTN, is a collaborative global LoRaWAN network. The TTN network server is located in the cloud and the gateways act as simple packet forwarders. Instructions for setting up a gateway and adding devices are provided on the website <https://www.thethingsnetwork.org> and are not repeated here.



Do not add devices to TTN directly. After this integration is set up, adding devices to the console will automatically add devices to your TTN account.

This section describes the setup required to link your TTN account with the console.

### Register through the Console

The easiest way to utilize TTN is to register your devices through the console. In this case, it is not necessary to set up your own TTN account or set up any integrations in the console. Go to:

<https://console.radiobridge.com/>

### Add Your Gateway

If there is TTN coverage in your area, it is not necessary to add your own gateway, but if adding coverage is necessary, this section describes the process to do so. Log into the console, select the Gateways tab on the left side, and click “Add Gateway.” Select the “TTN Gateway” from the listed network, fill in your Gateway EUI (Generally, it is your Gateway MAC ID with “00:00” inserted between the first three and last three bytes), select the appropriate frequency plan, and select the appropriate router zone.

Once the gateway is registered, you should see it in gateway list. Click the “Gateway Setup” link for the new gateway and note the gateway ID and gateway Key. This ID and Key need to be added to your gateway to complete the link. Once this is done you should see a connected status on the console as well as within your gateway.

### Add Devices to Console

When you add devices in the console, select The Things Network, select the option to use the Reveal account, and add the device.



## Connect your own TTN Account

If you already have a TTN account and wish to connect it to the console, follow the steps in this section.

### Create a New Application on TTN

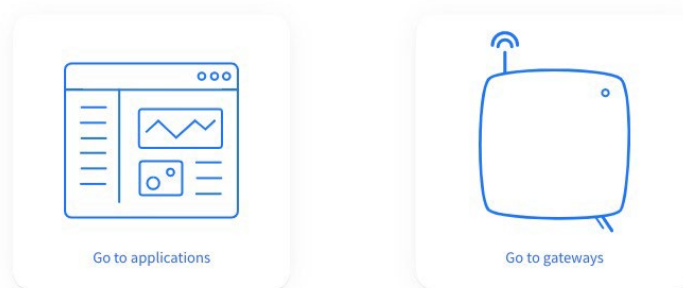
In your TTN console, go to Applications -> add application. Make sure you change your Application EUI to the Reveal AppEUI (see section on AppEUI/JoinEUI above). If this Application EUI is not set, it won't link correctly to the console.

### Create API Key on TTN

Go to your application on TTN and select API Keys -> Add API Key. Name the new key "console" and select: Grant all current and future rights. Click Create API key.

### Add Integration to the Console

Go to the console and select the Integrations tab -> The Things Network. Add the TTN application ID to the Application ID field and the API key generated in the last step to the API Key field. Note that the Application API Key is not the name of the key, but the randomly generated string that was created. Enter the Application server, Gateway Server, Identity Server, Join Server and Network server host address. You can find these on the TTN Home page (Check below screenshot). Click Update.



Version info  
**v3.14.0**

#### Component status

<div>Application Server</div> <div>nan1.cloud.thethings.network</div>	<div>Gateway Server</div> <div>nan1.cloud.thethings.network</div>
<div>Identity Server</div> <div>eu1.cloud.thethings.network</div>	<div>Join Server</div> <div>nan1.cloud.thethings.network</div>
<div>Network Server</div> <div>nan1.cloud.thethings.network</div>	

## Add Integration to TTN

Go to the TTN application and select Integrations -> Webhooks -> Add Webhook. Enter the fields as shown in the following table.

*Table 4 Parameters for TTN integration*

Parameter	Description
Webhook ID	Enter any name
Webhook Format	JSON
Base URL	Use the URL from the TTN tab on the console
Method	POST
Downlink API key	Leave this field blank
<b>Additional headers</b>	
Authorization	Use the Authorization Value from the TTN tab on the console
<b>Enabled messages</b>	
Uplink message	Tick and leave the path field as blank

## Add Devices to Console

Your console should now be connected to your TTN account. When you add devices in the console, select The Things Network and add the device. Adding and deleting devices in the console will now be reflected in your TTN account, and messages coming through TTN will appear in the console.

## Chapter 3 MachineQ

---

MachineQ is a LoRaWAN connectivity service from Comcast. The MachineQ network server is located in the cloud, and the MachineQ gateways forward packets between the network server and the LoRaWAN sensors. There is no configuration required on a MachineQ gateway, just plug it in and it is ready to go.

### Registering Devices through the Console

The easiest way to add MachineQ devices is to let console register them for you. In this scenario, you don't need your own MachineQ account or a direct engagement with MachineQ. There is no cost associated with registering through the console.

Log into the console and select the Devices tab on the left side of the page and click "Add Device." From there select the MachineQ icon and then "Register through RadioBridge". Once the device has been added, you will see sensor messages appear in the console.

<https://console.radiobridge.com/>

### Using Your MachineQ Account

If using your own MachineQ account is required, this section shows how to link MachineQ back end to the console.

#### Create the Output Profile

Go to the console, select Integrations along the left and then MachineQ along the top. The three settings under "MachineQ Output Profile Settings" including the URL, TokenType, and TokenValue will be used in the MachineQ backend setup.

In the MachineQ backend, go to the Integrations tab on the left, select "Output Profiles" along the top, and then click "Add Output Profile". Under REST Profiles select "add rest profile". Provide a name for the output profile and then enter the URL, TokenType, and TokenValue from the console as shown below.

Name\*

rblink

MOTT Profiles

[add mqtt profile](#)

REST Profiles

[add rest profile](#)

URL\*

https://console.radiobridge.com/lora\_c

TokenType ⓘ

Authorization

TokenValue

ZXIKcGRpSTZJbEp2ZVdadlplbFRNRTf

Click Submit to create the new profile.

## Create the Application

On the MachineQ window and select Integrations -> Application Management and then Get Started. Give the application a name and hit start. Copy the Client ID shown and paste into the client ID field on the console. Click next and do the same for the client secret. Hit done inside of MachineQ and the application will be created.

Back in the console, click on “Refresh Dropdowns” and you will see the output profile displayed as shown below.

Please enter following details to setup the MachineQ account.

**Client ID \***  
 From the machineQ application

**Client Secret \***

**APP EUI \***

Please fill your client ID and Client Secret to fetch the values for below dropdowns

[Refresh Dropdowns](#)

**Output Profile \***  
  
  
 Select the output profile created in machineQ

**Device Profile \***

**Service Profile \***

[Update](#)

[How to Connect MachineQ Account](#)

Machir

URL: http

TokenType

TokenVal

JuUllSelJ

5WVZKS

VTRQUOI

ak5qY3la

For the Decoder Type select “Unknown” and for Device Profile select “LoRaWAN-1.0.2- class A-FCC-20dBm”. Service profile should be on “default”. Click Update, and if everything was set up correctly you will get a message saying that the account detail has been saved. You can now add devices and see the uplink messages come through your MachineQ backend account and up to the console.

## Bypassing the Console

If the console is not used, and sensor messages will be sent directly from the end customer's MachineQ account to a third-party application, please refer to the table below for the parameters required to add the device to the MachineQ back end.

*Table 5 Parameters for MachineQ Setup*

Parameter	Description
Dev EUI	The Device ID listed on your sensor
App EUI	See section on AppEUI/JoinEUI above
App Key	Enter the Key listed on your sensor
Device Profile	LoRaWAN 1.0.2 Class A 20dBm
Decoder Type	Use "Unknown"
DevAddr Assign	Dynamic

## Add Devices to Console

Your console should now be connected to your MachineQ account. When you add devices in the console, select MachineQ and add the device. Adding and deleting devices in the console will now be reflected in your MachineQ account, and messages coming through MachineQ will appear in the console.

## Chapter 4 Stand-Alone MultiTech Conduit AP/AEP

This section describes the steps necessary to connect a stand-alone MultiTech Conduit AP or AEPLoRa gateway to the console. In the stand-alone configuration, the network server is located on the local gateway and a Python script is used to pass messages to the console.



A cloud-based network server is highly recommended vs a stand-alone setup. If you wish to use this method, we recommend contacting our support to discuss your application further.

### Add Gateway to the Console

Log into the console at [console.radiobridge.com](https://console.radiobridge.com), select the Gateways tab on the left side, and click “Add Gateway”.

Follow the menu to select MultiTech and give the gateway a name. Click on “Register Gateway” and note the link to the installation script that will be used in future steps.

### Bring the Gateway Online

To bring the gateway online, refer to the standard setup instructions from MultiTech. Note the gateway may default to a static IP of 192.168.2.1.

Be sure to set the DNS correctly in the network setup, as future steps will fail if the DNS is not correct.

### Update Gateway Firmware

Verify the gateway is running firmware version 5.3.0 or later. If it is not, follow the MultiTech instructions for upgrading the system firmware before proceeding to the next steps.

### Enable the LoRa Network Server

Navigate to the LoRaWAN tab on the left side of the screen, select network settings, and under Mode select “Network Server”.

The default settings should be in the correct state, but double check that the Channel Plan is “US915”, the frequency sub-band set to 1, and the network mode is set to “PublicLoRaWAN”. Click on Submit.

Click on Administration -> Access Configuration and check the box “Via WAN” under the SSH heading. Click Submit.

Go to Firewall->Settings and check the box “Allow Inbound”. Click Submit. Click Save and Apply.

## Install Python Script

Log into the gateway via SSH. You can use a program such as PUTTY on Windows or the Terminal on a Mac. The command will usually take the form:

```
ssh <user>@<gateway IP address>
```

Navigate to the home folder:

```
cd /var/config/home/admin
```

Run the wget command using the link provided by the console when the gateway was registered. The command will look like:

```
wget https://console.radiobridge.com/download-setup/<code>/multitech_sdk.tar.gz
```

Extract the files with the command:

```
tar -xzf multitech_sdk.tar.gz
```

Navigate to the extracted folder and execute the following commands to run the setup:

```
cd multitech_sdk
```

```
sudo chmod +x ./mqtt_gateway.sh
```

```
sudo ./mqtt_gateway.sh
```

```
sudo reboot
```

If you are prompted for a password in the above commands, use the admin password set for the gateway. You can close the SSH session.

After the gateway reboots, login through the web interface, click on LoRaWAN, and under network settings verify that the LoRa mode is set to “network server” and the status shows “running” in green.

## Add Devices to Gateway

Log into the gateway and go to LoRaWAN -> Key Management. Under Location select “LocalKeys” and click Add New.

Enter the fields as shown in the following table.

*Table 6 Parameters for Device Setup*

Parameter	Description
Dev EUI	The Device ID listed on your sensor
App EUI	See section on AppEUI/JoinEUI above



App Key	Enter the Key listed on your sensor
---------	-------------------------------------

Click OK.

Make sure the Enabled box is NOT checked under Local Network Settings. Once you have added all of your devices click on Submit then click Save.

Note that this only adds the devices to the gateway, they will still need to be added to the console. Adding a device to the gateway does not automatically add to the console, and adding to the console does not automatically add them to the gateway, so they must be added separately.

## Add Devices to the Console

As mentioned in the previous step, even though the devices have been added to the gateway, they will still need to be added to the console.

Log into the console and select the Devices tab on the left side of the page and click "Add New Device". Select the MultiTech stand-alone gateway in the Select Network screen. For the ID and Key, use the numbers found on the sensor label which is the same ID/Key pair entered on the gateway.

Reveal sensors can now connect to the console through the stand-alone gateway. Try creating sensor events and verify that you see messages in the console.

## Chapter 5 ChirpStack

ChirpStack is an open source LoRaWAN network server that can be deployed by end users who wish to maintain their own private installation. You can register devices through the console ChirpStack installation, or you can connect your own ChirpStack installation to the console. Both methods are described below.

### Using the Reveal ChirpStack Server

The easiest way to use ChirpStack is to let the console provision the device to the Reveal ChirpStack server. In this scenario, you don't need to install your own ChirpStack network server.

<https://console.radiobridge.com/>

### Configure the ChirpStack Gateway

You will need to set up a gateway to direct LoRaWAN traffic to the Reveal ChirpStack server. To do so, set the gateway to use the basic Semtech packet forwarder and point it to the IP address `chirpstack.radiobridge.com` port 1700 as shown in the following image.

The screenshot shows the 'LoRa' configuration tab. The 'Mode' dropdown is set to 'Semtech Forwarder'. Below this, the 'Network Server Address' is 'chirpstack.radiobridge.com'. The 'Port Up' and 'Port Down' are both set to '1700'. An 'Update' button is located at the bottom left of the configuration area.

### Add the ChirpStack Gateway to the Console

Go to the Gateways tab on the left, click Add New Gateway, and select ChirpStack.

Enter a name, description, and the Gateway EUI. Note that the Gateway EUI is often the MAC address with 0xFFFF as the middle two bytes. For example, if your 6-byte MAC address is 0x010203040506, then the 8-byte Gateway EUI may be 0x010203FFFF040506.

### Add Devices to the Console

Select the Devices tab on the left side of the page and click "Add New Device". From there select the ChirpStack icon and then "Register through RadioBridge". Once the device has been added, your sensors will connect through the ChirpStack network and you will see new messages appear in the console.

## Using Your ChirpStack Server

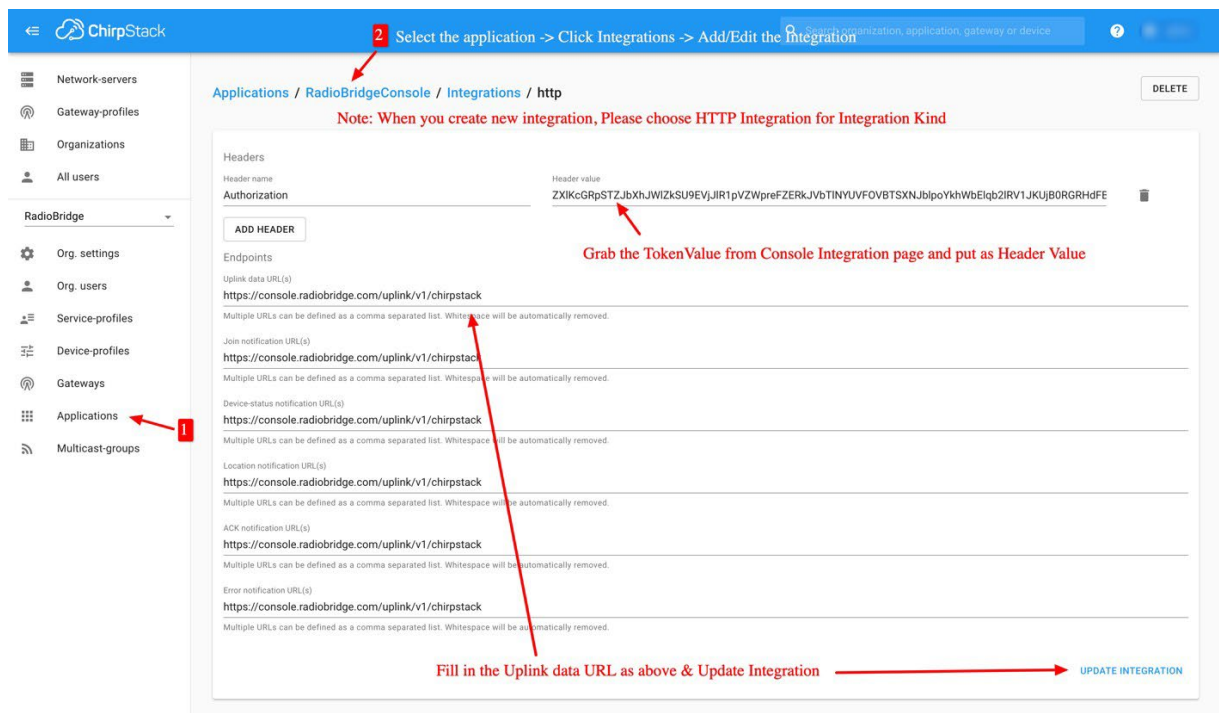
If you wish to use your own ChirpStack network server, this section shows how to link your ChirpStack backend to the console.

### Configuring HTTP Integration in ChirpStack

The first step is to configure the HTTP Integration to forward messages from your ChirpStack application server to the console. The image below illustrates the steps to configure HTTP Integration from the ChirpStack server:

1. Click Applications. Each application contains separate HTTP integrations, so click on the application which you want to use with Reveal
2. Go to the Integrations tab and click the Create button.
3. Click the `Add Header` button to add the Authorization header.
4. The Header value should be filled in with the TokenValue generated from the console as shown in the next section.
5. Fill in the URL fields with the URL provided in the console as shown in the next section.
6. Once done, click Update Integration to save.

See the screenshot below. Notice that the Header Value and the URLs come from the console as shown in the next section.



## Configuring the Integration in the Console

The image below illustrates the steps to configure HTTP Integration from the Reveal The image below illustrates the steps to configure HTTP Integration from the console:

1. Go to the Integrations tab and click the Create button
2. Enter the URL of the ChirpStack server into the field “ChirpStack Server Address”
3. Enter the ChirpStack account admin username into the “Admin Username” field
4. The JWT Secret is a secret key that is set into the ChirpStack application server configuration file. Enter this into the “JWT Secret” field
5. Enter the Application Name from the ChirpStack server in the “Application” field
6. Enter the Device Profile created from the ChirpStack server in the “DeviceProfile” field.
7. When complete, click Update.

The console is now linked to the ChirpStack server. When adding a new device, select ChirpStack and “Use Your Own Account”.

## Update Your ChirpStack Server Settings

The ChirpStack network server does not have the 500kHz channels enabled by default, and this is required for Reveal sensors to communicate with data rate 4 (DR4). If ChirpStack is not updated to include this, messages may be lost.

To update your ChirpStack server, please do the following:

1. Log into your network server using SSH
2. You can find the Chirpstack configuration file in the folder `/etc/chirpstack-network-server/chirpstack-network-server.toml`
3. Enter the command below to edit the above file `sudo nano /etc/chirpstack-network-server/chirpstack-network-server.toml`
4. In the editor find the line `enabled_uplink_channels= [0, 1, 2, 3, 4, 5, 6, 7, 64]`
5. Replace the above line with `enabled_uplink_channels=[]`
6. Save the file and restart the network server using the command below: `sudo systemctl restart chirpstack-network-server`

## Chapter 6 Senet

---

Senet is a LoRaWAN connectivity service. The Senet network server is located in the cloud, and Senet-enabled gateways forward packets between the network server and the LoRaWAN sensors.

### Registering Devices through Reveal

The easiest way to add Senet devices is to purchase service through Reveal and let the console handle the provisioning automatically. In this scenario, you don't need your own Senet account or a direct engagement with Senet.

Simply log into the console and select the Devices tab on the left side of the page and click "Add New Device". From there select the Senet icon and then "Register through Reveal". Once the device has been added, your Reveal sensors will connect through the Senet network and you will see new messages appear in the console.

### Using Your Senet Account

If using your own Senet account is required, this section shows how to link your Senet back-end to the console. To setup your Senet account, you will need API Key, APP EUI, Join EUI, Contract ID, and Profile ID as described in the next sections.

#### Request API Key

First you need to request the API key from Senet support. Send an email to [support@senetco.com](mailto:support@senetco.com) to request the API key for your account.

#### AppEUI

The default Reveal AppEUI is defined in the section on AppEUI/JoinEUI above. This AppEUI can be programmed to a custom value in the factory, and in the Senet back-end you can find the AppEUI assigned to your account as shown in below image.

The screenshot shows the 'Applications' tab in the Senet dashboard. A dropdown menu is open under 'Device Profiles', showing 'Contracts' and 'Device Profiles'. Red arrows point from text annotations to these menu items. Below the menu is a table with columns: ID, Name, Editable, App EUI, ADR, and F. The table contains two rows of data. A red arrow points to the 'App EUI' column header.

Contract ID can be found on contracts page

Profile ID can be found on Device Profiles page

ID	Name	Editable	App EUI	ADR	F
142	Default - 0101010101010101	Editable	0101010101010101	true	
166	Radio Bridge - Min DR 1	Editable	0101010101010101	true	

## Contract ID and Profile ID

You can find the contract ID and profile ID through Applications tab, please see the image below to find the contract ID and profile ID.

The screenshot shows the 'Applications' tab in the Senet dashboard. A dropdown menu is open under 'Contracts', showing 'Radio Bridge' and 'Radio Bridge - Senet Operations'. A red arrow points to the 'Radio Bridge - Senet Operations' item. Below the menu is a table with columns: ID, Name, and a search bar. The table contains two rows of data. A red arrow points to the 'ID' column header.

Contracts

ID	Name
100	Radio Bridge
87	Radio Bridge - Senet Operations

Showing 1 to 2 of 2 entries

## Notification Target

To receive messages in the console, you will need to set the notification target in the Senet back-end to point to the console. You can email Senet support to setthis for your account.

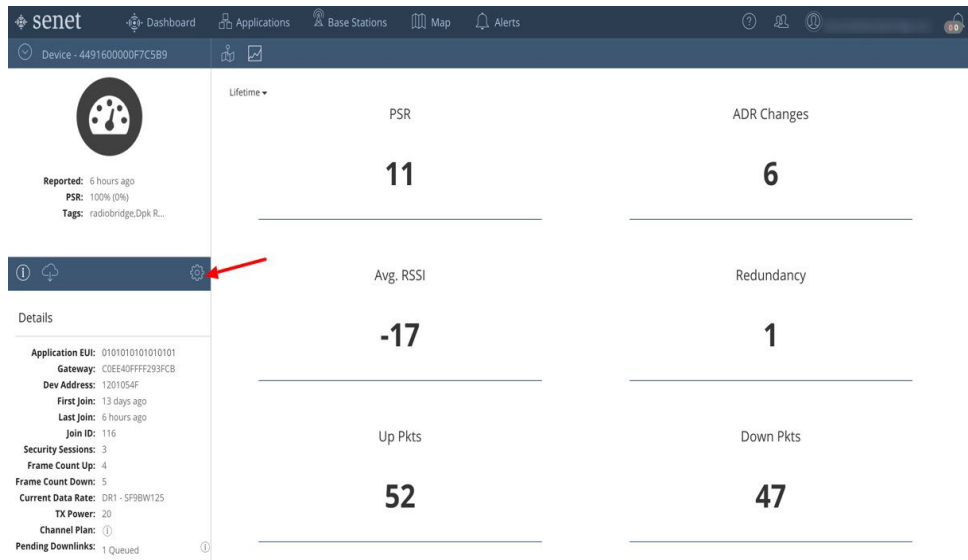
Alternatively, Senet allows to set the notification target for every device individually. To set the notification target for a device, go to the Senet console, click the Applications tab and edit a device to add the notification target. Please follow the screenshots below to set the notification target.

The screenshot shows the Senet console interface. The top navigation bar includes 'Dashboard', 'Applications', 'Base Stations', 'Map', and 'Alerts'. The 'Applications' tab is selected. Below the navigation bar, there is a sidebar on the left showing a tree view of applications. The main area displays a table of devices. A red arrow points to the 'Applications' tab, and another red arrow points to the 'Edit' icon (a square with a pencil) for the device with EUI 449160000F7BFC8.

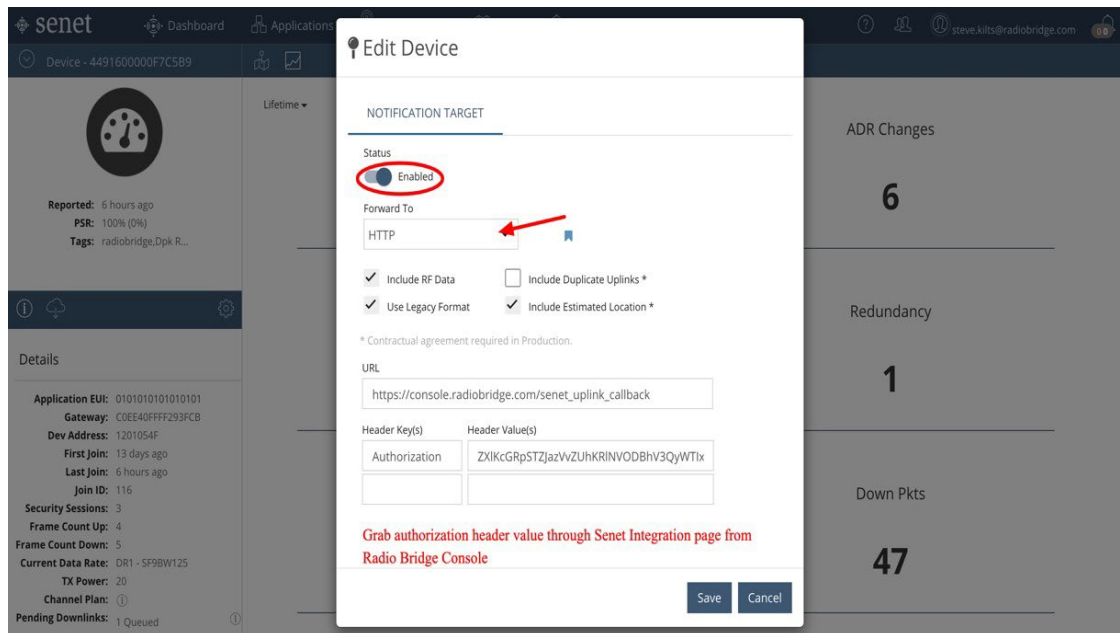
Dev EUI	Last Heard From	Redundancy	PSR	Avg SNR	Avg RSSI	Pkts Up	Pkts Down	Data Rate	Base Station	Lo
449160000F7BE38	06/19/2019 12:46:57.590 AM	7 8	100 100	10.55 10.72	-83 -83	434 683	427 673	2	647FDAFFFE0040DD...	0.0
449160000F7C5B9	06/18/2019 06:53:23.243 PM	1 0	100 0	11.82 0.00	-29 0	5 0	4 0	1	C0E40FFFFF293FCB	0.0
449160000F7BFC8	05/20/2019 10:53:06.285 PM	0 0	0 0	0.00 0.00	0 0	0 0	0 0	3		0.0

Showing 1 to 3 of 3 entries





The following image shows the notification target setting, you can find the Header key and value on RadioBridge console -> Senet integrations page.





Normally you do not want to set the notification target on each device. Rather, you should contact Senet and have them set the notification target for your account.

## Senet Configuration on the Console

To set up Senet on the console, go to the integrations tab and click Senet. Enter the contract ID and the profile ID into the fields shown below.

An authorization header is provided which can be given to Senet when requesting the permanent notification target described in the previous section.

**Senet Configuration**

Please enter following details to setup the Senet account.

**API Key \***  
AK2j...WoQhQznj  
This key can be obtained by contacting the Senet Support.

**App Eui \***  
01010101010101  
You can find App Eui inside applications tab in your Senet account.

**Join Eui \***  
01010101010101  
You can find Join Eui inside applications tab in your Senet account.

**Contract ID \***  
87

**Profile ID \***  
142

[Update](#)

[How to Connect Senet Account](#)

**Senet Uplink API Settings**

URL: [https://console.radiobridge.com/senet\\_uplink\\_callback](https://console.radiobridge.com/senet_uplink_callback)

Header:

Authorization: ZXIKcGRpSTZ3azVZUhKRINVODBHv3QyWT1xSlZWUmtjWGRlUldjOVBT  
SXN3blpoYkhWbE...aUTBWU01FNXd  
01VUhOWWVrdFr...XJNktVmpPV1FST  
WVTIIV1haVJWVI...2rMkIHUXpNeIFST  
WpJNE9HRTFORC...  
npNM1ptVxdOak5oTTRZek9EbGfOObUKtWIR3dIpXWWWimUT09

**This is the authorization key to set when setting up Notification Target**

We're Online!  
How may I help you today?

## Add Devices to Console

Your console should now be connected to your Senet account. When you add devices in the console, select Senet and add the device. Adding and deleting devices in the will now be reflected in your Senet account, and messages coming through Senet will appear in the console.

## Chapter 7 Lorient

Lorient.io is a LoRaWAN connectivity service. The Lorient.io network server is located in the cloud, and the Lorient enabled gateways forward packets between the network server and the LoRaWAN sensors.

### Registering Devices through Reveal

The easiest way to add devices is to let Reveal register them for you. In this scenario, you don't need your own Lorient account or a direct engagement with Lorient.

Simply log into the console and select the Devices tab on the left side of the page and click "Add New Device". From there select the Lorient icon and then "Register through Reveal". Once the device has been added, you will see sensor messages appear in the console.

### Optional: Add Your Lorient Gateway

In addition to registering devices through the console, you can also register your gateway if you need to supplement coverage. Note that this section describes adding your gateway through Reveal and not with your own account (which is described in the next section).

Go to the Gateways tab on the left, click Add New Gateway, and select the supported gateway you wish to use. You can follow the prompts to finish the gateway registration. You can now add new Lorient devices and begin receiving data in the console.

### Using your Lorient.io account

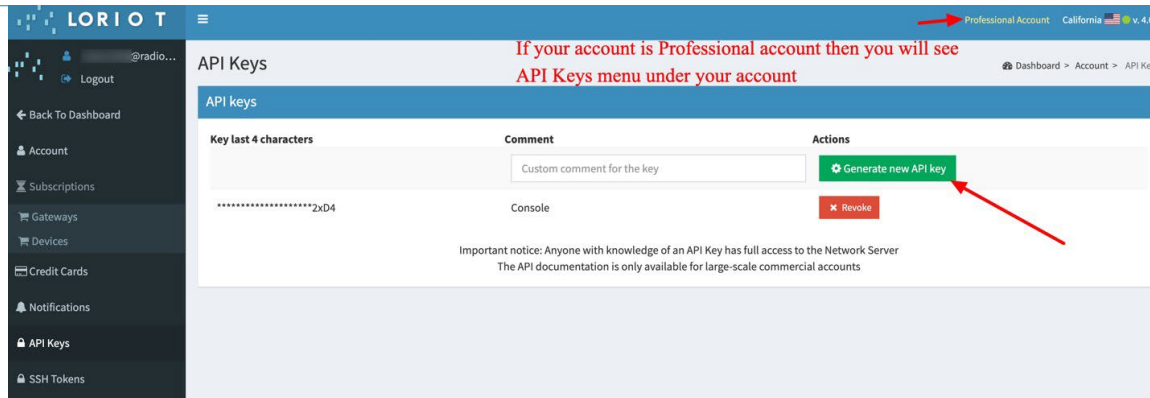
If you are planning to use your own Lorient account, this section shows how to link your Lorient.io back end to the console.

#### Lorient.io Server Location

First you need to determine your account region, for example: us1, us2 etc. You can find all allowed regions on Lorient login page (<https://lorient.io/login.html>)

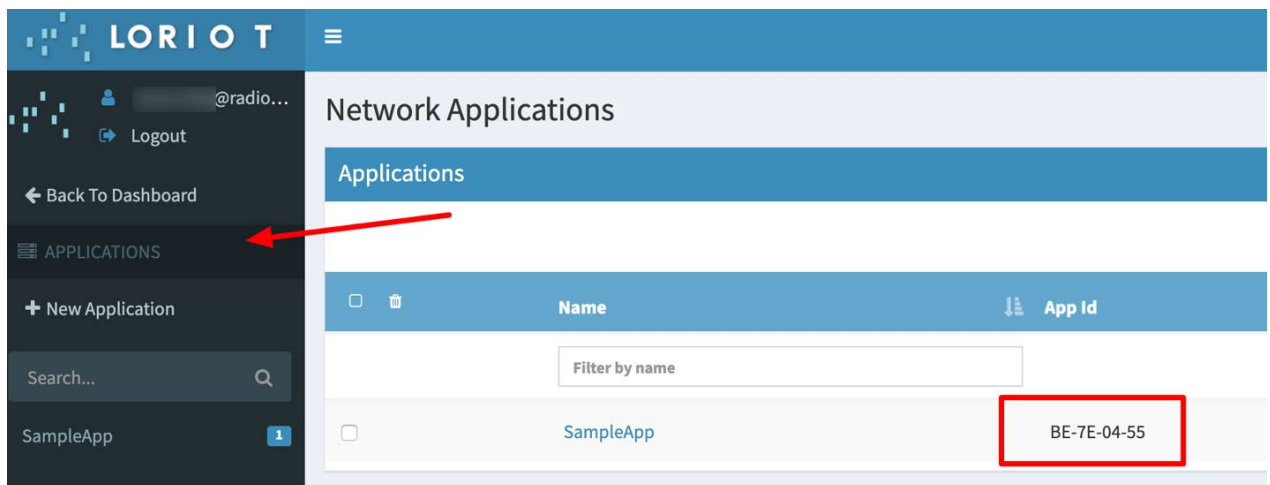
#### Lorient.io API Key

Login into your Lorient.io account, navigate to the Accounts -> API Keys -> Click Generate new API Key.



### Loriot.io Application ID

Navigate to Applications -> New Application (If not created) -> Copy the App ID as displayed in below screenshot (note this is different than the LoRaWAN AppEUI). Copy this ID (with no hyphens) to the console under Integrations -> Setup Loriot.



## Loriot.io Access Token

The access token is used to send the downlink config messages to the device & network. Navigate to Loriot Console -> Application -> Select the Application -> Click Access Tokens in left menu. Copy this access token to the console under Integrations -> Setup Loriot.

**Application Access Tokens**

**Security mechanism**

To connect to any of the application interfaces provided by LORIoT.io, you need to prove you are a legitimate user of the network application.

The public network is built for developers with ease of use in mind, so we don't require any complicated (but more secure) authentication mechanisms.

The only mechanism used is a security token (per-application). You will need to provide this token before any other interactions with the interface.

Note that anyone with knowledge of the token can access your data, so please keep the token as protected any of your passwords.

If you require a more secure authentication mechanism, please contact our [sales department](#).

**NEW! Updated token format**

With the latest update of our software, the format of the tokens has been changed. The token has been extended and now includes information about the application ID and the server origin, so that 3rd party platforms can use single value copy-paste to access our API.

You can continue using any legacy tokens you have already in place, we provide full backward compatibility.

Token parse scheme

**Application Tokens**

Authentication Tokens	Personalized Websocket URL	Revocation
...2PEluM9nbTneg==	...2PEluM9nbTneg==	Revoke

[Generate another authentication token](#)

**vgEAAwAAAA1kZXyubG9yaW90LmlvzXTU16ESI0rvJST-gsL\_xQ==**

## Loriot Output

To receive messages into the console, you will need to setup the Output as an HTTP Push. The screenshot below shows the steps to add a new Output.

You can find the Target URL and Authorization header value in your console under Integrations -> Setup Loriot -> Loriot uplink API. Copy the URL and Authorization value into the HTTP Push configuration window on Loriot.

## Add Devices to Console

Your console should now be connected to your Loriot account. When you add devices in the console, select Loriot and add the device. Adding and deleting devices in the console will now be reflected in your Loriot account, and messages coming through Loriot will appear in the console.

## Chapter 8 Kerlink Wansey Management Center (WMC)

The Wansey Management Center from Kerlink is a LoRaWAN connectivity service. The Kerlink network server is located in the cloud, and the Kerlink gateways forward packets between the network server and the LoRaWAN sensors.

### Registering Devices through Wansey

The easiest way to add devices is to let Reveal register them for you. In this scenario, you don't need your own Wansey account.

Simply log into the console and select the Devices tab on the left side of the page and click "Add New Device". From there select the Kerlink icon and then "Register through Reveal".

### Add Your Kerlink Gateway

In addition to registering devices through the console, you must also register your gateway to create coverage. Note that this section describes adding your gateway through Reveal, and not with your own WMC account.

First you need to Setup the Kerlink Gateway to Connect it with Wansey Management Center. Please follow the steps below to configure your Gateway.

### Update Gateway Firmware

1. To update the gateway, first ensure the gateway is connected to the local network.
2. Open a web browser and enter the IP assigned by your router.
3. On the login screen, the default admin login username is **admin** and the password is also **admin**. In the latest version, the default username is **admin** and the password is **pwd4admin**
4. To update the firmware, please click the link below to find the latest firmware version available to download

<https://wikikerlink.fr/wirnet-productline/doku.php?id=wiki:firmware:lastversion>

**NOTE:** Wikikerlink.fr website is protected using a username and password, If you don't have an account then you need to request [support@kerlink.fr](mailto:support@kerlink.fr) to get your account.

5. To run the upgrade, you will need to login into your Gateway terminal using SSH. The default username is root and password is a combination of pdmk-<last6 chars of gateway Board ID>

For example: If your gateway Board ID is XXXAPa010X9A, then password will be pdmk-010X9A

6. Create the updates folder if that doesn't exist

```
# mkdir /user/.updates
```

7. Copy the downloaded firmware using SCP command in the /user/.updates folder

```
# scp keros_2.4.0..ipk root@<ip_address>:/user/.updates/
```

8. Trigger the update for next reboot # kerosd -u
9. Reboot the device. # reboot

You can find more details using the link below [https://wikikerlink.fr/wirnet-ifemtocell/doku.php?id=wirnet-ifemtocell:software\\_updates](https://wikikerlink.fr/wirnet-ifemtocell/doku.php?id=wirnet-ifemtocell:software_updates)

## Configure using the Magic Link

Request a “magic link” from Kerlink support to finish the configuration to connect the Gateway with WMC panel. You will need to send an email to [support@kerlink.fr](mailto:support@kerlink.fr) with your Kerlink Gateway Serial number to activate the Gateway and generate a magic link. The magic link is an executable file, which configures everything in the gateway and enables Gateway to connect with WMC Network.

## Add the Gateway

Go to the Gateways tab on the left side of the console, click Add New Gateway, and select the supported gateway you wish to use. You can follow the below guide to finish the gateway registration.

10. Enter any name for your Kerlink Gateway.
11. You can obtain Kerlink Gateway EUI using below method:

Wirnet iBTS : 7276FF002E<last 6 characters of the CPU serial number>

Wirnet Station : 7276FF000<last 7 characters of the station barcode>

Wirnet iFemtoCell : 7276FF00<last 8 characters of the CPU board serialnumber>

12. If you are using iFemtoCell then you can find the EUI using below command.
  - a. First login into Gateway console using SSH.
  - b. Type the below command which will retrieve the EUI for your Gateway. cat /tmp/board\_info.json | grep -i eui



c. Output will look like

```
"EUI64": "7076FF0054040166",
```

d. Your EUI is “7076FF0054040166”, Copy that and put it into console.

13. Fill in other fields and click “Register Gateway”

14. You should see a successful message and gateway should connect with the Wanasy network in few mins. Gateway will blink as soon as it will connect with the Network.

You can now add new Reveal devices and begin receiving data in the console.

## Using your Wanasy Management Center account

If you are planning to use your own WMC account, this section shows how to link your WMC back end to the console.

### Integrate your WMC Account

Go to the Integrations page in your Reveal account, Click Kerlink to configure the network. Enter your Wanasy Management Center username and password to connect the WMC portal with Reveal

### Push Configuration

The Push Configuration allows WMC to push the uplink events to the console.

Login into your Wanasy account, navigate to the Administration -> Clusters -> Click Push Configurations

**Note:** It is important for you to configure the push configuration correctly, otherwise it may function incorrectly.

1. Enter the Configuration name (It can be anything)

Update push configuration \* required

Identity

Connection

Custom headers

Name \*

DpkKerlink

Type \*

☒ HTTP
 ☐ Websocket
 ☐ MQTT

Message detail level \*

☐ Payload
 ☐ Radio
 ☒ Network

CANCEL

NEXT

- Select the Type “**HTTP**”, Message detail level should be “**Network**”

- Copy the URL from the Kerlink Integrations page and setup as shown in the image below.

The screenshot shows the 'Update push configuration' form with a progress bar at the top. The progress bar has three steps: 'Identity' (blue dot), 'Connection' (yellow dot), and 'Custom headers' (blue dot). The 'Connection' step is active. Below the progress bar, the 'Connection' section contains the following fields:

- Url \***: `http://dev.console.radiobridge.com/uplink/v1/kerlink`
- User \***: `deepakmaurya@hotmail.com`
- Password \***: `.....`
- Data Up route**: `/dataUp`
- Data Down event route**: `/dataDownEvent`

At the bottom of the form, there are three buttons: 'PREVIOUS', 'CANCEL', and 'NEXT'.

- You need to enter your Reveal account username and password for the authentication.

The screenshot shows the 'Update push configuration' form with a progress bar at the top. The progress bar has three steps: 'Identity' (blue dot), 'Connection' (blue dot), and 'Custom headers' (yellow dot). The 'Custom headers' step is active. Below the progress bar, the 'Custom headers' section contains the following fields:

- Custom headers**: A table with two columns: 'key' and 'value'. There is a '+' button to add a new header and an 'X' button to remove a header.

At the bottom of the form, there are three buttons: 'PREVIOUS', 'CANCEL', and 'VALIDATE'.

- Click Next, Skip the Headers section, and click Validate to finish the setup.

## Clusters

Each device in your account belongs to a Cluster and Cluster defines the way you can route your data using Push Configuration and Payload type. If you already have a cluster then you can edit that and update the configuration as per below screenshot. Or if you don't have then please create the new cluster as per below instructions:

- Click the Add Cluster/Edit Cluster button to add/edit the cluster.
- Enter any name and Choose the Payload Type as **Base 64**
- Enable the push configuration
- Choose the Push Configuration created in Step 8.2.2
- Click Validate to save the cluster.
- In the console please make sure you choose the same cluster on IntegrationsPage.

**Edit cluster** \* required

Name \*

Payload type \* ☐ Hexadecimal ☒ Base 64

**Push**

☒ Enable ☐ Disable

Push configuration \*

CANCEL VALIDATE

## Add Devices to Console

Your console should now be connected to your WMC account. When you add devices in the console, select Kerlink and add the device. Adding and deleting devices in the console will now be reflected in your WMC Kerlink account, and messages coming through WMC will appear in the console.



## Chapter 9 Third Party Network Servers

This section provides the information required to connect the LoRaWAN sensors to a third party LoRaWAN network server not otherwise described in this document. The network server may reside on the gateway itself or in the cloud, and the server may push the data to the console or another third-party application.

### Sensor to Network Server

The LoRaWAN network server must use the connectivity parameters shown in the following table.

*Table 7 LoRaWAN Parameters*

LoRaWAN Parameter	Description
Activation Method	OTA (over the air activation). The sensor will send a join request and expect a join accept before any other messages can be sent.
Device EUI	This is the ID on the label located on the sensor itself. The barcode provided can also be used to read the Device EUI.
Application EUI	See the section on AppEUI/JoinEUI above. This can be customized in the factory for production orders, but most customers simply use this default.
Application Key	This is the Key on the label located on the sensor itself. The barcode provided can also be used to read the Application Key.

The sensors will send a join request when the battery is inserted, and if the join fails it will try again once per hour. To force a new join request, remove the battery and replace it. Often it takes a few minutes for LoRaWAN network servers to boot, so if it doesn't connect on the first attempt, wait a few minutes before replacing the battery again.

### Network Server to Console

The network server may pass data to the console application or directly to a third-party application. The advantage of the console is simple provisioning, automatic decode and interpretation of sensor data, a downlink interface for reconfiguring the sensors, database with message history, health status, and a

simple API interface. This section describes the steps required to connect a gateway not specifically listed in this document to the console.

The first step is to create security credentials for a new stand-alone gateway so that it can connect to the console. Log into the console at [console.radiobridge.com](https://console.radiobridge.com), select the Gateways tab on the left side, and click “Add Gateway”. Follow the menu to select the gateway type “Other Gateway”.

After the gateway has been created, select “Gateway Setup”. Use the API provided with a POST or GET call to send data from a gateway to the console. The response from this call will contain any downlink (sensor configuration information) if a new configuration message is pending. Note that the call has an authorization key that is unique to this gateway.

When adding a new LoRa device, select “Third Party Gateway” and select the name of the gateway you just created. The gateway is now authorized to send sensor data to the console.