Getting Started with Kerlink Gateways and AWS IoT Core for LoRaWAN

Getting Started Guide

Getting Started with Kerlink Gateways and AWS IoT Core for LoRaWAN

	Redaction	Validation	Approbation
Trigram	JCA	GBO	YDE
Date	2020-10-26		
Signature			

Version	Edits
1.0	Initial version
1.1	Add AWS IoT Core for LoRaWAN missing screens and update credential section
1.2	Update after AWS review
1.3	Update based on AWS template
1.4	Typo corrections
1.5	Update AWS information from template

Reference	Description
[1]	https://wikikerlink.fr/wirnet-productline/doku.php?id=wiki:lora:aws

Table of content

Table of figures

This guide will walk you through the unboxing, connection, and installation of Kerlink Wirnet iFemtocell Gateway to be used with AWS IoT Core for LoRaWAN.

When you order a Kerlink Wirnet iFemtocell Gateway with AWS IoT Core for LoRaWAN support, it comes preconfigured.

1 Unboxing

The package contains the following elements:

- Kerlink iFemtocell gateway
- LoRa Antenna (862-873MHz, 902-928MHZ, 3dBi, 50Ω; vertical polarization)
- AC/DC Power supply (Input 110-240V, output 12V, 0.5A jack connector) (EU or US plug depending on the reference ordered)

1.1 Cabling

First, connect the LoRa Antenna to the SMA connector on the Wirnet iFemtocell.
Then, plug an Ethernet cable to the Wirnet iFemtocell and to your network. The Wirnet iFemtocell will establish 2 connections to the Internet through your network: one to AWS, and one to Kerlink Wanesy Management Center.
Finally, connect the power jack to the Wirnet iFemtocell and plug the power supply to the wall socket.

Figure 1: Wirnet iFemtocell setup (EU version pictured)

1.2 First boot

The Wirnet iFemtocell will boot and eventually update its firmware to the latest version. Refer to the LEDs color to follow the bootstrap procedure.

To ensure the Wirnet™ iFemtoCell is started up, check the behavior of the LED indicators:

<table>
<tr><th>LED</th><th>Specification</th></tr>
<tr><td>LED 1: Power/Status</td><td>A solid Green for Power LED
A Status Red LED
<table>
<tr><th>Gateway Status</th><th>“Status LED” Behavior</th></tr>
<tr><td>Boot part 1</td><td>Fix on</td></tr>
<tr><td>Boot part 2</td><td>Heartbeat</td></tr>
<tr><td>Boot part 3</td><td>Blink every second</td></tr>
<tr><td>Run time</td><td>Off</td></tr>
<tr><td>Power down sequence</td><td>Heartbeat</td></tr>
<tr><td>Update</td><td>Blink / 0.4 second</td></tr>
<tr><td>Restore backup</td><td>Blink / 2 seconds</td></tr>
<tr><td>Restore stock</td><td>Blink / 4 seconds</td></tr>
</table></td></tr>
<tr><td>LED 2: Backhaul</td><td>RED during boot
The applicative software provided by Kerlink is installed:
• RED if applicative software is disconnected
• GREEN blinking during applicative software connection
• GREEN fix if applicative software is connected</td></tr>
<tr><td>LED 3: LoRa Data</td><td>RED during boot
The applicative software provided by Kerlink is installed:
• Applicative software management
• Rx: GREEN blinking
• Tx: RED blinking</td></tr>
</table>

Figure 2: Wirnet iFemtocell LEDs

Once LED 1 (Power/Status) and LED 2 (Backhaul) are solid green, your gateway is ready.

2 Connect to Kerlink Wanesy Management Center

Once the gateway online, you can connect to Kerlink Wanesy Management Center. This is the central place to monitor, configure and remotely access your gateway.

2.1 Log-in

Your sales contact will send you the credentials and URL to connect to WMC. Connect to the WMC instance and enter the username and password.

Figure 3: Wanesy Management Center login page

2.2 Gateway overview

Once logged-in, go to "**Management** >> **Gateway"** menu. You will find your gateway on that page.

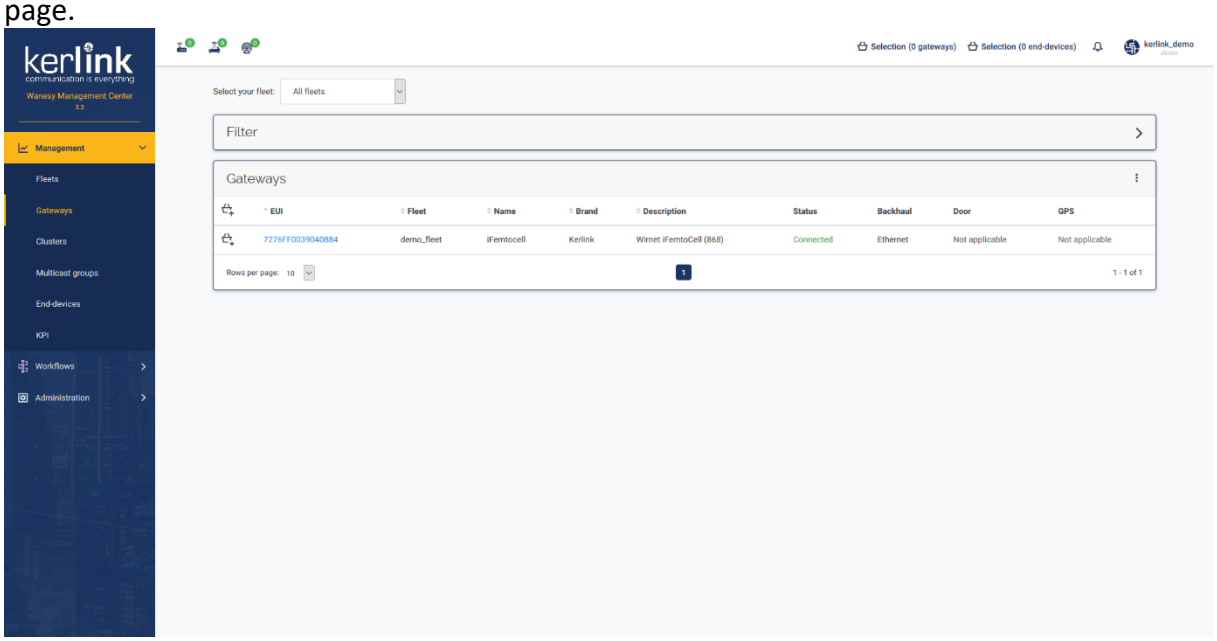

Figure 4: Wanesy Management Center - Gateway management page

Select your gateway by clicking on its EUI. You will get the gateway overview with all the details you need. In case of multiple gateways, look for your gateway EUI using the "Filter" window. Enter in the EUI search field the last 6 digits of your Gateway's Board ID located on the label at the back of the Wirnet iFemtocell.

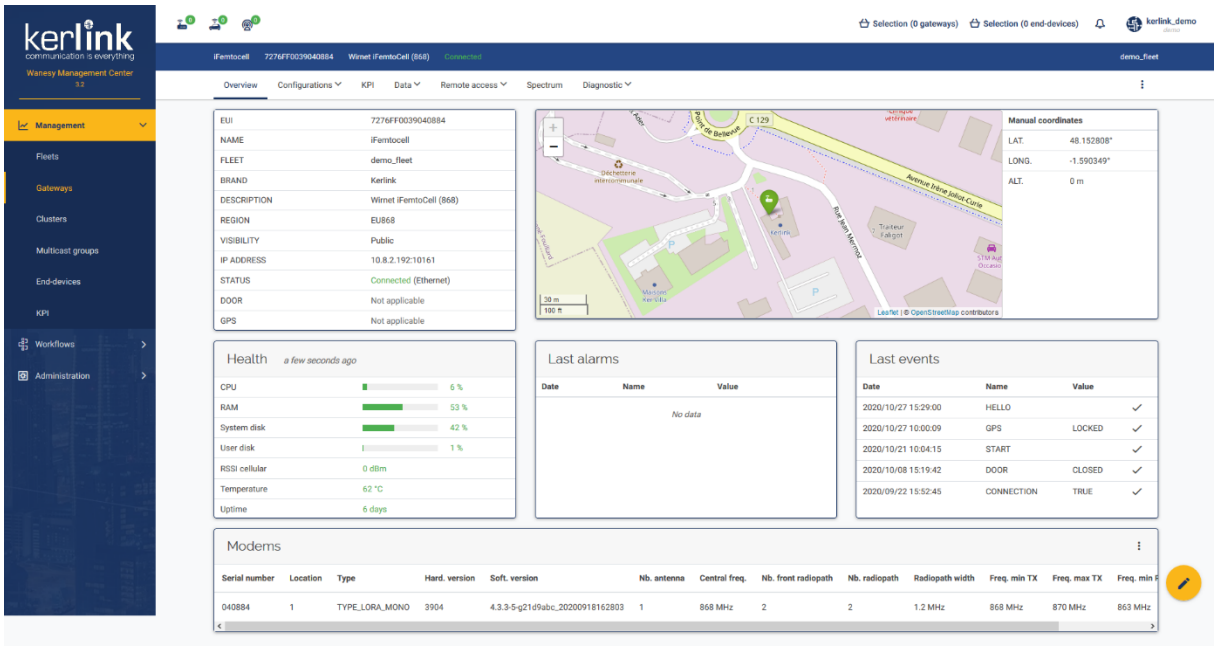

Figure 5: Wanesy Management Center - Gateway overview

Note or copy to your clipboard the **Gateway EUI** for the following registration on AWS.

You can use all the other menus to explore all the capabilities of your gateway and the associated service. This overview will be sufficient for the moment.

3 Setup your AWS account and Permissions

Note: The following sections (3.1, 3.2, 3.3) have been provided by AWS. Please contact AWS support for additional information.

If you don't have an AWS account, refer to the instructions in the guide here. The relevant sections are **Sign up for an AWS account** and **Create a user and grant permissions**.

3.1 Overview

The high-level steps to get started with AWS IoT Core for LoRaWAN are as follows:

1. Set up Roles and Policies in IAM
2. Add a Gateway (see section Add the Gateway to AWS IoT)
3. Add Device(s) (see "Getting Started with Kerlink WAL-e AWS IoT Core for LoRaWAN" in [1])

These steps are detailed below. For additional details, refer to the AWS LoRaWAN developer guide.

3.2 Set up Roles and Policies in IAM

3.2.1 Add an IAM Role for CUPS server

Add an IAM role that will allow the Configuration and Update Server (CUPS) to handle the wireless gateway credentials.

This procedure needs to be done only once, but must be performed before a LoRaWAN gateway tries to connect with AWS IoT Core for LoRaWAN.

- Go to the IAM Roles page on the IAM console
- Choose **Create role**.
- On the **Create Role** page, choose **Another AWS account**.
- For **Account ID**, enter your account id.
- Choose **Next: Permissions**
- In the search box next to **Filter policies**, enter *AWSIoTWirelessGatewayCertManager*.
    - If the search results show the policy named *AWSIoTWirelessGatewayCertManager*, select it by clicking on the checkbox.
    - If the policy does not exist, please create it as follows:
        - Go to the IAM console
        - Choose **Policies** from the navigation pane.
        - Choose **Create Policy**. Then choose the **JSON** tab to open the policy editor. Replace the existing template with this trust policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IoTWirelessGatewayCertManager",
            "Effect": "Allow",
            "Action": [
                "iot:CreateKeysAndCertificate",
                "iot:DescribeCertificate",
                "iot:ListCertificates",
                "iot:RegisterCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

        - Choose **Review Policy** to open the *Review* page.
        - For **Name**, enter *AWSIoTWirelessGatewayCertManager.* **Note** that you must enter the name as AWSIoTWirelessGatewayCertManager and must not use a different name. This is for consistency with future releases.
        - For **Description**, enter a description of your choice.
        - Choose **Create policy**. You will see a confirmation message showing the policy has been created.
- Choose **Next: Tags**, and then choose **Next: Review**.

- In **Role name**, enter *IoTWirelessGatewayCertManagerRole*, and then choose **Create role**.
    - **Note** that you must not use a different name. This is for consistency with future releases.
- In the confirmation message, choose **IoTWirelessGatewayCertManagerRole** to edit the new role.
- In the **Summary**, choose the **Trust relationships** tab, and then choose **Edit trust relationship**.
- In the **Policy Document**, change the **Principal** property to represent the IoT Wireless service:

```
"Principal": {
    "Service": "iotwireless.amazonaws.com"
},
```

After you change the Principal property, the complete policy document should look like this:

```
    {
    "Version": "2012-10-17",
    "Statement": [
      {
          "Effect": "Allow",
          "Principal": {
            "Service": "iotwireless.amazonaws.com"
          },
          "Action": "sts:AssumeRole",
          "Condition": {}
      }
    ]
  }
```

- Choose **Update Trust Policy** to save your changes and exit.

At this point, you've created the *IoTWirelessGatewayCertManagerRole* and you won't need to do this again.

3.2.2 Add IAM role for Destination to AWS IoT Core for LoRaWAN

Prepare your AWS account to work with AWS IoT Core for LoRaWAN. First, create an IAM role with permissions to describe the IoT end point and to deliver messages to IoT cloud. Then, update the trust policy to grant AWS IoT Core for LoRaWAN permission to assume this IAM role when delivering messages from devices to your account.

***NOTE** – The examples in this document are intended only for dev environments. All devices*

in your fleet must have credentials with privileges that authorize only intended actions on specific resources. The specific permission policies can vary for your use case. Identify the permission policies that best meet your business and security requirements. For more information, refer to Example policies and Security Best practices.

- In the IAM console, choose **Roles** from the navigation pane to open the **Roles** page.
- Choose **Create Role**.
- In **Select type of trusted entity**, choose **Another AWS account**.
- In **Account ID**, enter your AWS account ID, and then choose **Next: Permissions**.
- Choose **Next: Permissions**
- Search for your IAM policy. Type in the policy name to find your policy. Select it.
- Choose **Next: Tags**.
- Choose **Next: Review** to open the Review page. For **Role name**, enter an appropriate name of your choice. For **Description**, enter a description of your choice.
- Choose **Create role**.

Create the corresponding policy

- Go to the IAM console
- Choose **Policies** from the navigation pane.
- Choose **Create Policy**. Then choose the **JSON** tab to open the policy editor. Replace the existing template with this trust policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action":
  [
    "iot:DescribeEndpoint",
    "iot:Publish"
  ],
        "Resource": "*"
      }
    ]
}
```

- Choose **Review Policy** to open the Review page. For Name, enter a name of your choice. For **Description**, enter a description of your choice.
- Choose **Create policy**.

Update your policy's trust relationship.

- In the IAM console, choose **Roles** from the navigation pane to open the **Roles** page
- Enter the name of the role you created earlier in the search window, and click on the role name in the search results
- Choose the **Trust relationships** tab to navigate to the Trust relationships page.

- Choose **Edit trust relationship**. The principal AWS role in your trust policy document defaults to root. Replace the existing policy with this:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": {
            "Service": "iotwireless.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
      }
    ]
}
```

- Choose **Update Trust Policy**

3.3 Add the Gateway to AWS IoT

To connect to AWS IoT Core for LoRaWAN, Kerlink Wirnet iFemtocell Gateway comes with Basic Station pre-installed and enabled.
Basic Station is a LoRaWAN Packet Forwarder. It is a program that runs on Kerlink gateways which forward LoRaWAN RF packets to AWS IoT Core for LoRaWAN network server.

3.3.1 Preparation

To complete setting up your gateway, you need:

- LoRaWAN region. For example, if the gateway is deployed in a US region, the gateway must support LoRaWAN region US915.
- Gateway LNS-protocols. Currently, the LoRa Basics Station protocol is supported.
- Gateway ID: Gateway EUI you noted earlier.

3.3.2 Add the LoRaWAN Gateway

To register the Gateway with AWS IoT Core for LoRaWAN, follow these steps:

- Go to the AWS IoT Core console.
- Select **Wireless connectivity** in the navigation panel on the left.
- Choose **Intro**, and then choose **Get started**. This step is needed to pre-populate the default profiles.
- Under **Add LoRaWAN gateways and wireless devices**, choose **Add gateway**.
- In the **Add gateway** section, fill in the **GatewayEUI** and **Frequency band (RF Region)** fields.
- Enter a descriptive name in the **Name – optional** field. We recommend that you use the GatewayEUI as the name.

- Choose **Add gateway**
- On the **Configure your Gateway** page, find the section titled **Gateway certificate**.
- Select **Create certificate**.
- Once the **Certificate created and associated with your gateway** message is shown, select **Download certificates** to download the certificate (*xxxxx.cert.pem*) and private key (*xxxxxx.private.key*).
- In the section **Provisioning credentials**, choose **Download server trust certificates** to download the CUPS (`cups.trust`) and LNS (`lns.trust`) server trust certificates.
- Copy the CUPS endpoint to your clipboard and paste it into a new text file named cups.uri.
- Copy the LNS endpoint to your clipboard and paste it into a new text file named tc.uri.
- Choose **Submit** to add the gateway.

3.4 Prepare credentials for Basic Station

Basic Station only recognize certificates and keys with specific names, so you need to rename the files as follow:

- You should have `cups.trust`
- Rename lns`.trust` to `tc.trust`
- Copy the *xxxxx.cert.pem* to `cups.crt`
- Copy the *xxxxx.cert.pem* to `tc.crt`
- Copy the *xxxxxx.private.key* to `cups.key`
- Copy the *xxxxxx.private.key* to `tc.key`
- You should have the `cups.uri` and `tc.uri` file already.

3.5 Upload credentials to your Wirnet iFemtocell

To install those certificates on your gateway, login to Wanesy Management Center again. This time browse to your gateway and select **Remote access** >> **File Explorer**.

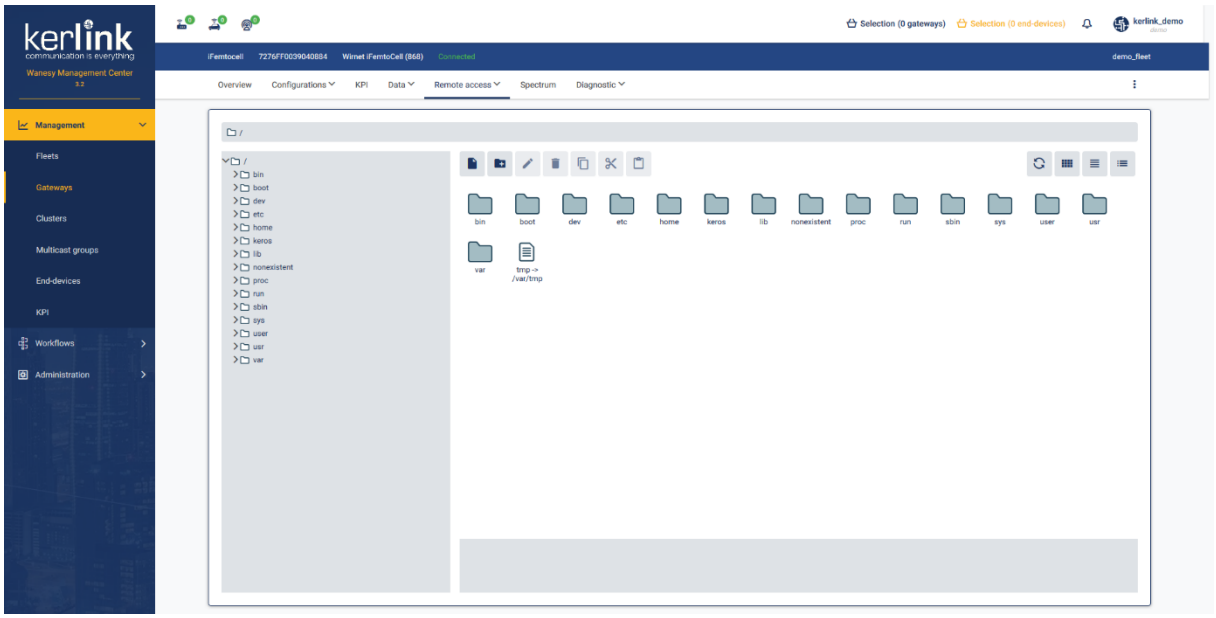

Figure 6: Wanesy Management Center - File Explorer

Navigate to `/etc/station/` folder and upload your credential files there using the "**Upload File**" menu for each.

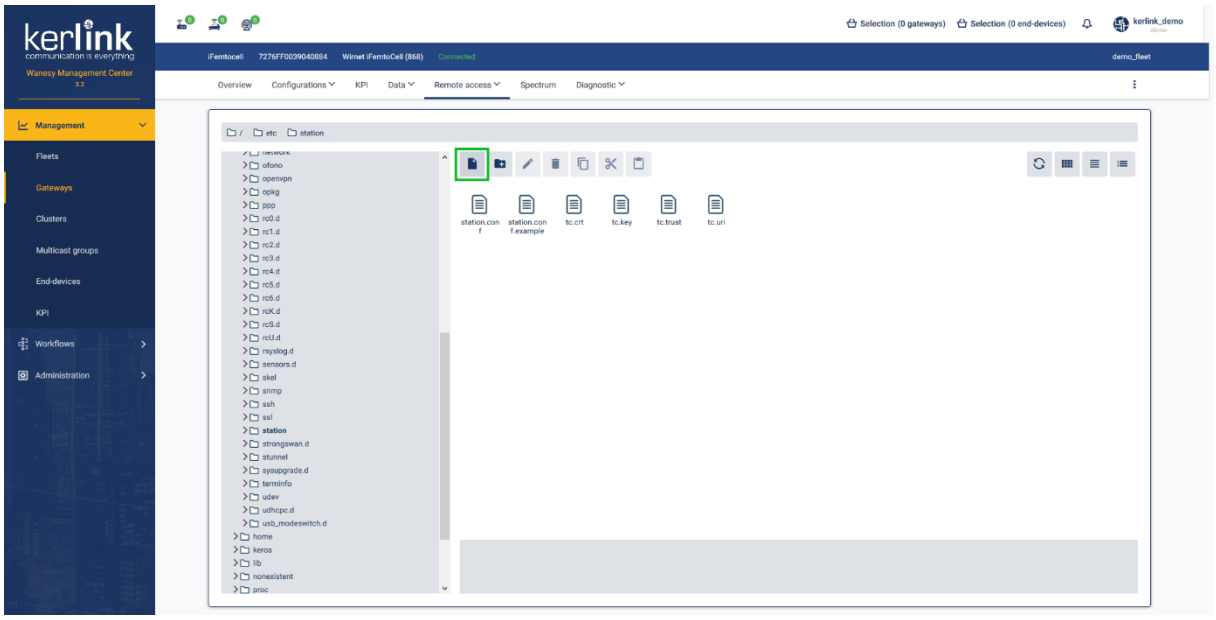

Figure 7: Wanesy Management Center: Upload file

3.6 Enable the credentials

To enable your credentials, go to **Remote access** >> **Command** and type the following command.

```
monit restart station
```

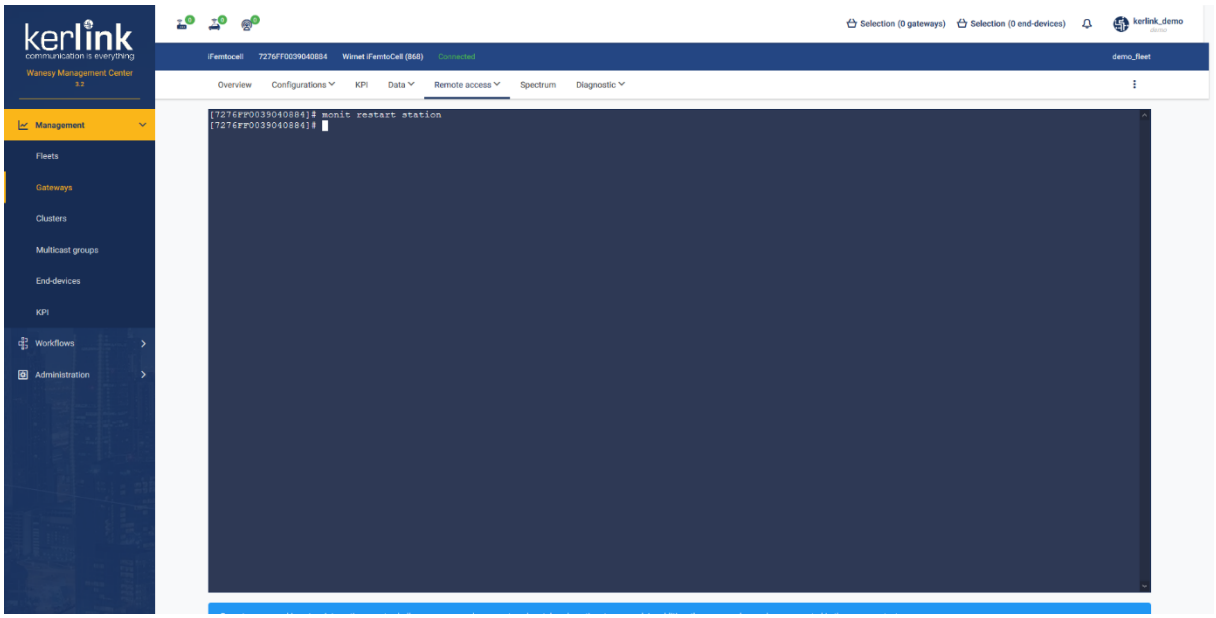

Figure 8: Wanesy Management Center - command

Going back to AWS IoT Core for LoRaWAN interface, you should see your gateway connected.

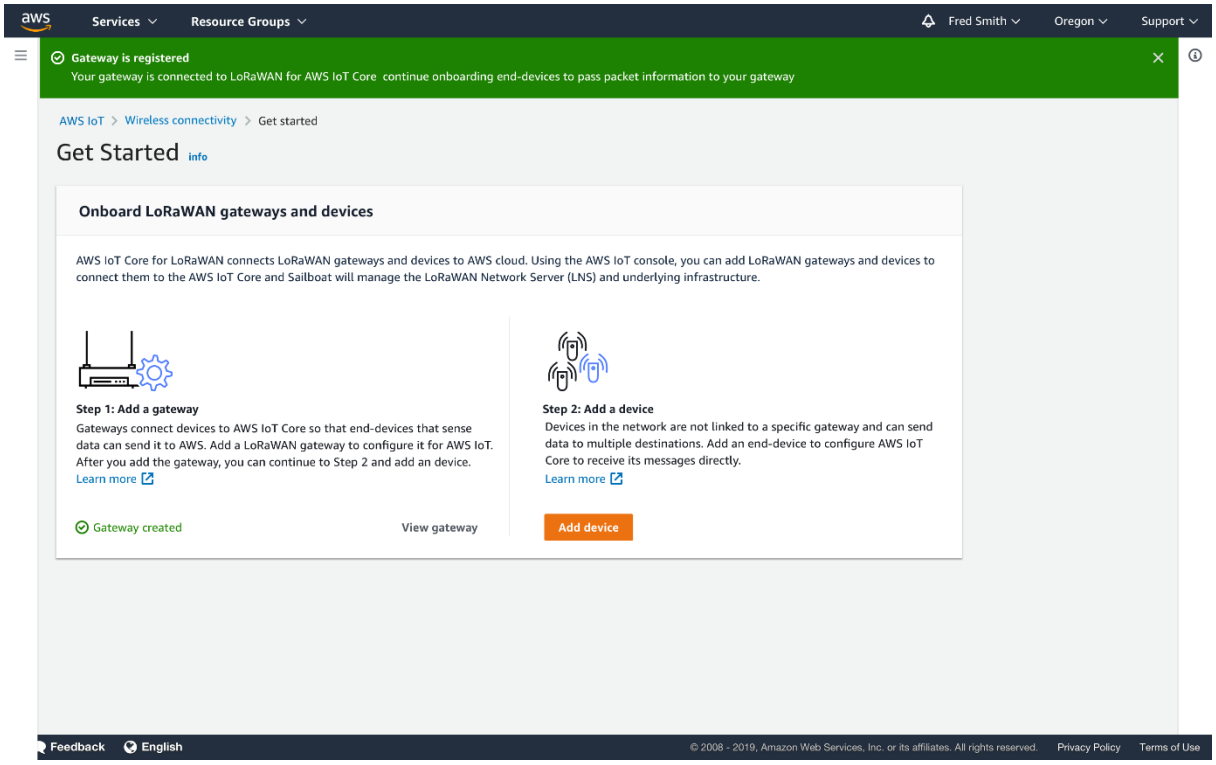

Figure 9: AWS IoT Core for LoRaWAN - Gateway created

Congratulations! You can now move to end-device on-boarding with AWS IoT Core for LoRaWAN. Refer to “Getting Started with Kerlink WAL-e AWS IoT Core for LoRaWAN” in [1].

End of Document