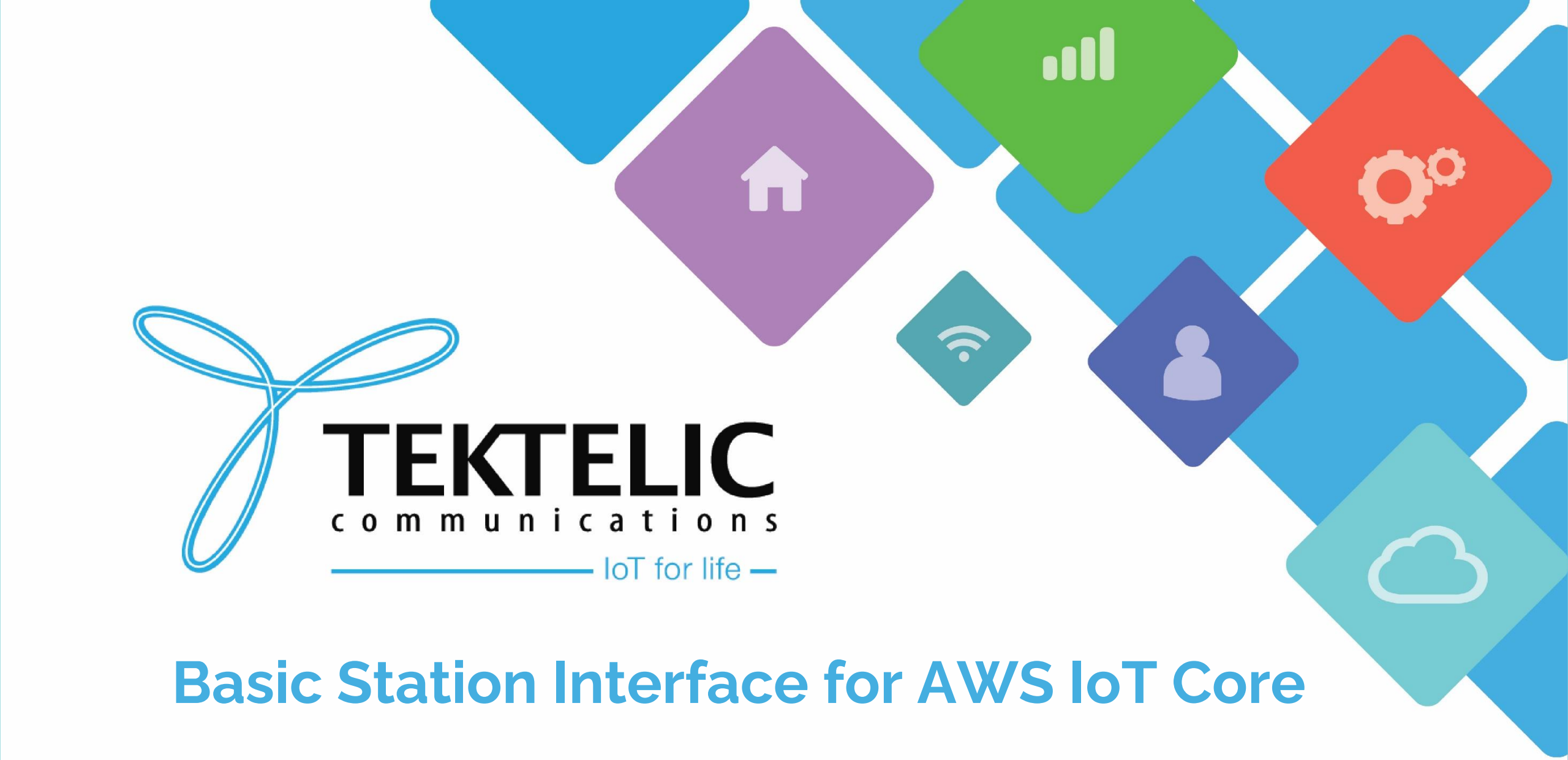

Basic Station Interface for AWS IoT Core

Introduction

- Reference guide to install a Basic Station interface on a gateway for AWS IoT Core.

- List requirements.

- High-level procedure steps:

1. Set up Roles and Policies in IAM.
2. Configure and add gateway on AWS.
3. Configure and add device on AWS.
    a. Verify device and service profiles.
    b. Set up a Destination to which device traffic will be routed and processed by a rule.
4. Configure gateway to connect to AWS.
    a. Install Basic Station.
    b. Configure Basic Station and other packages.

Requirements

- Gateway with the required BSP version and Basic Station installed
- AWS account

1. Set up Policies and Roles in IAM

The IAM role will allow the Configuration and Update Server (CUPS) to handle gateway credentials.

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

1.1.1 Set up Policies in IAM

If the policy **“AWSIoTWirelessGatewayCertManager”** does not exist, please create it with the following steps:

1. Navigate to the **IAM console.**
2. In the left navigation pane, select **Policies**.
3. Select **“Create Policy”,** then select the JSON tab to open the policy editor.
4. Replace the existing template with the following:

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

1.1.2 Set up Policies in IAM

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

Figure-1 Example Policy

1.1.3 Set up Policies in IAM (Continued)

5. Once the policy template has been replaced, select **“Next: Tags”** at the bottom right of the page. Then select **“Next: review”.**
6. Fill out the required fields:
   - Name: **AWSIoTWirelessGatewayCertManager**
   - Note: You MUST enter the name AS IS, you cannot use a different name. This is to ensure consistency with future releases.
   - Description: Enter a description of your choice.
7. Finalize policy by selecting **“Create policy”.** You will see a confirmation message showing the newly created policy.

1.2.1 Set up Roles in IAM

1. Navigate to the ***IAM console.***
2. In the left navigation pane, under **Access Management**, click **Roles** and **“Create role.”**
3. Select AWS account for trusted entity.
4. Ensure that **“This account (12 digit account ID)”** is selected.
5. In the field **“Filter policies…”** enter **“AWSIoTWirelessGatewayCertManager”.**
6. Tick off checkbox beside **“AWSIoTWirelessGatewayCertManager”,** the policy you have created earlier.

1.2.2 Set up Roles in IAM (Continued)

7. Fill out the required fields:
   - Name: **AWSIoTWirelessGatewayCertManagerRole**
   - Note: You MUST enter the name AS IS, you cannot use a different name. This is to ensure consistency with future releases.
   - Description: Enter a description of your choice.
8. Select the Role page from the navigation panel and then select **AWSIoTWirelessGatewayCertManagerRole**.
9. Select the **“Trust relationships”** tab then Select **“Edit trust policy”.**

1.2.3 Set up Roles in IAM (Continued)

10. In the **“Edit trust policy”** section, change the Principal property to represent the IoT Wireless service:

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

11. Select **“Update policy”** to save changes.

1.2.4 Set up Roles in IAM (Continued)

Figure-2 Trust Policy

1.3.1 Set up IAM Destination role

This section will prepare your AWS account to work with AWS IoT Core for LoRaWAN. The steps are as follows:

1. Create IAM policy.
2. Create IAM role with permissions to describe IoT endpoint and to deliver messages to IoT cloud.
3. Update the trust policy to grant AWS IoT Core permission to assume the IAM role when delivering messages from devices to your account.

1.3.2 Set up IAM Destination role (Continued)

1. Select **Policies** from the navigation pane.
2. Select **“Create Policy”**, then select the **JSON tab**.
3. Replace the existing template with the following:

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

1.3.3 Set up IAM Destination role (Continued)

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

Figure-3 Destination Policy

1.3.4 Set up IAM Destination role (Continued)

4. Continue with **“Next: Tags”** and enter any tags.
5. Continue with **“Next: Review”.**
6. Enter a name and description of your choice.
7. Finalize by selecting **“Create policy”**.

1.3.5 Set up IAM Destination role (Continued)

Next, create a role that will use the newly created policy.

1. Select **Roles** from the navigation pane.
2. Select **“Create Roles”.**
3. In **“Select trusted entity”** select **“AWS account”** and select “**This account”.** Then click Next.
4. In **“Add permissions,”** tick off the checkbox beside the policy you created earlier. Then click Next.
5. Enter a name and description of your choice.
6. Finalize by selecting **“Create role”.**

1.3.6 Set up IAM Destination role (Continued)

Then update the policy's trust relationship

1. Select **Roles** from the navigation pane.
2. Enter the name of the role you just created in the search window and click on the role name.
3. Select **"Trust relationships"** tab.
4. Select **"Edit trust policy"** and replace the policy with the following:

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

5. Finalize by selecting **"Update policy".**

1.3.7 Set up IAM Destination role (Continued)

Trusted entities

Entities that can assume this role under specified conditions.

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

Figure-4 Edited Trust Policy

2. Add Gateway to AWS IoT

To setup your gateway to connect to AWS IoT, here is an overview of the steps.

1. Create Gateway entity.
2. Download certificates.

2. Add Gateway to AWS IoT (Continued)

1. Navigate to **the AWS IoT Core console.**
2. In the left navigation pane, under **“LPWAN devices”,** select **“Gateways”.**
3. Select “**Add gateway”.**
4. Fill out the **“Gateway EUI”** as well as the **“Frequency band”** fields.
5. Finalize by selecting **“Add gateway”.**
6. Under **“Gateway certificate”,** select **“Create certificate”** and download the files.
7. Rename ***xxxx.cert.pem*** file to ***cups.crt*** and ***xxxx.private.key*** to ***cups.key***
8. Create a copy of ***cups.key*** and name it ***tc.key***
9. Create a copy of ***cups.crt*** and name it ***tc.crt***

2. Add Gateway to AWS IoT (Continued)

10. Under **“Provisioning credentials”**, select “**Download server trust certificates”** and keep them in a secure location.
11. Keep the ***cups.trust*** file as is.
12. Rename ***lns.trust*** file to ***tc.trust***
13. Copy the CUPS and LNS endpoints and save them for use while configuring the gateway.
    - Create **cups.uri** file with CUPS Endpoint URL:
      i.e.: **https://EXAMPLE.cups.REGION.amazonaws.com:443**
    - Create **tc.uri** file with LNS Endpoint URL:
    - i.e.: **wss://EXAMPLE.gateway.lorawan.REGION.amazonaws.com:443**

2. Add Gateway to AWS IoT (Continued)

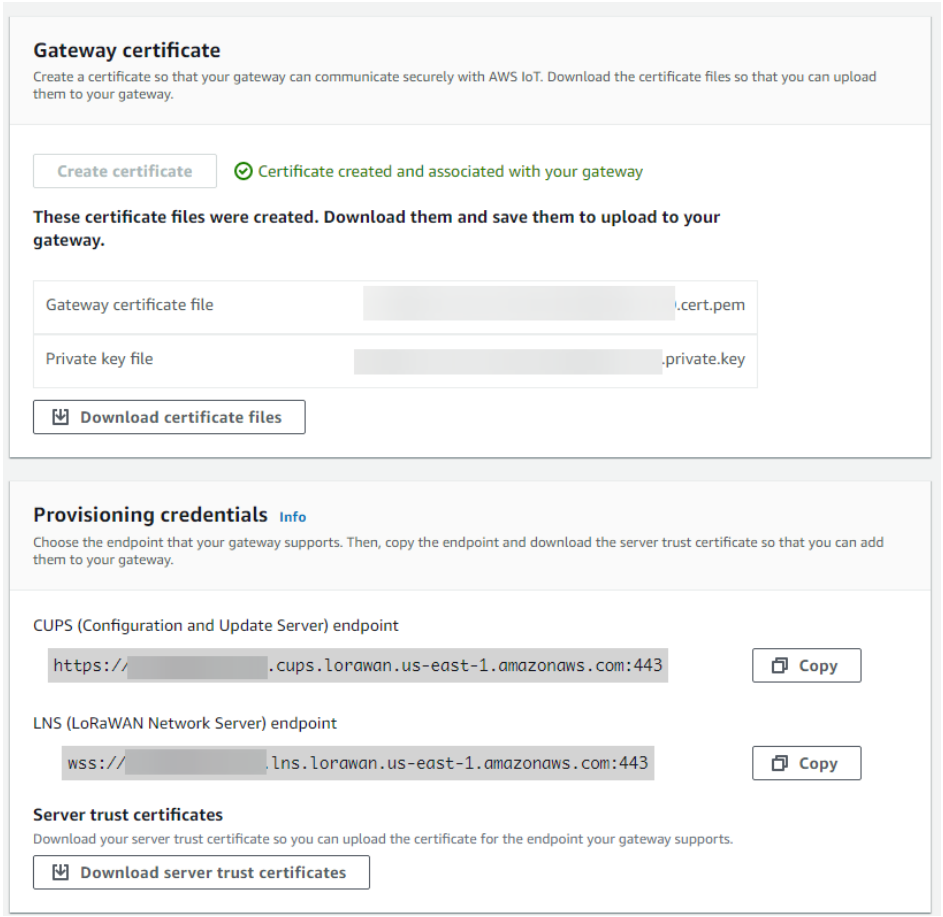

Figure-5 Gateway Certificates

2. Add Gateway to AWS IoT (Continued)

Ensure that you have the following 8 files created from the previous steps:

- **tc.uri**
- **tc.trust**
- **tc.key**
- **tc.crt**
- **cups.uri**
- **cups.trust**
- **cups.key**
- **cups.crt**

3. Add Device to AWS IoT

To add and configure a LoRaWAN device on AWS IoT, here is an overview of the steps:

1. Prepare requisite device information.
2. Verify device and service profile.
3. Set up Destination for device traffic
4. Register device

3. Add Device to AWS IoT (Continued)

Before configuring a device on AWS IoT Core, you must note the specifications of your device:

- The following regions are supported:
  - **EU868**
  - **EU433**
  - **US915**
- MAC Version on the device must be one of the following:
  - **V1.0.2**
  - **V1.0.3**
  - **V1.1**
- OTAA v1.0x and OTAA v1.1 are supported.
- ABP v1.0x and ABP v1.1 are supported.

3. Add Device to AWS IoT (Continued)

You will also require the following information from your device manufacturer:

- For OTAA v1.0x devices: DevEUI, AppKEY, AppEUI
- For OTAA v1.1 devices: DevEUI, AppKEY, NwkKEY, JoinEUI
- For ABP v1.0x devices: DevEUI, DevAddr, NwkSkey, AppSkey
- For ABP v1.1 devices: DevEUI, DevAddr, NwkSEnckey, FNwkSIntKey, SNwkSIntKey, AppSKey

Note: Tektelic Devices only support LoRaMAC v1.0.2. If you are using a Tektelic Device, please select **“OTAA v1.0.2”** when creating the Device Profile from the list.

For other devices, please reach out to the device manufacturer and select the appropriate in the device profile.

3. Add Device to AWS IoT (Continued)

AWS IoT Core for LoRaWAN supports device and service profiles.

- Device profiles contain the communication and protocol parameter values the device needs to communicate with the network server.
- Service profiles describe the communication parameters the device needs to communicate with the application server.

3.1.1 Add Device Profile

Some pre-defined profiles are available for device and service profiles. Before proceeding, verify that these profile settings match the devices you will be setting up to work with AWS IoT Core for LoRaWAN.

- In the AWS IoT Core console, in the left navigation pane, expand the **“LPWAN devices”** category. Then select **“Profiles”.**
- In the **“Device Profiles”** section, there are pre-defined profiles listed.
- Please check each profile to determine if any of them will work for you.

3.1.2 Add Device Profile (Continued)

If none of the profiles work, select **“Add device profile”** and set up the parameters as needed. For example, a US915 profile can have the following values:

- **MacVersion: 1.0.2**
- **RegParamsRevision: Regional Parameters v1.0.2rB**
- **MaxEirp: 13**
- **MaxDutyCycle: 10**
- **RfRegion: US915**
- **SupportsJoin: true**

***Note: The Tektelic US915 sensors require the above setting.**

3.1.3 Add Device Profile (Continued)

MacVersion	1.0.2
RegParamsRevision	Regional Parameters v1.0.2rB
RxDelay1	1
RxDataRate2	8
RxFreq2	9233000
FactoryPresetFreqsList	
MaxEirp	13
MaxDutyCycle	10
RfRegion	US915
SupportsJoin	true
Supports32BitFCnt	true

Figure-6 Example US915 Device Profile

3.1.4 Add Device Profile for EU 868(Continued)

EU868 profile can have the following values:

- **MacVersion: 1.0.2**
- **RegParamsRevision: Regional Parameters v1.0.2rB**
- **MaxEirp: 5**
- **MaxDutyCycle: 10**
- **RfRegion: EU868**
- **SupportsJoin: true**

***Note: The Tektelic EU868 sensors require the above setting.**

3.1.5 Add Device Profile (Continued)

MacVersion	1.0.2
RegParamsRevision	Regional Parameters v1.0.2rB
RxDelay1	1
RxFreq2	8695250
FactoryPresetFreqsList	
MaxEirp	5
MaxDutyCycle	10
RfRegion	EU868
SupportsJoin	true
Supports32BitFCnt	true

Figure-6 Example EU Device Profile

3.2.1 Add Service Profile

In the **“Service Profiles”** section, there are pre-defined profiles listed. Please check each profile to determine if any of them will work for you.

If not, select **“Add service profile”** and set up the parameters as needed.

As an example, the default service profile parameters are shown below. However, only the **AddGwMetadata** setting can be changed at this time.

- **UlRate: 60**
- **UlBucketSize: 4096**
- **DlRate: 60**
- **DlBucketSize: 4096**
- **AddGwMetadata: true**
- **DevStatusReqFreq: 24**
- **DrMax 15**
- **TargetPer: 5**
- **MinGwDiversity: 1**

Continue once you have both a device and service profile that works for you.

3.2.2 Add Service Profile

Profile configuration

Parameter name	Value
Arn	arn:aws:iotwireless:us-east-1:
UlRate	60
UlBucketSize	4096
DlRate	60
DlBucketSize	4096
AddGwMetadata	true
DevStatusReqFreq	24
DrMax	15
TargetPer	5
MinGwDiversity	1

Figure-7 Example Service Profile

3.3.1 Add Device to AWS IoT (Continued)

Because most LoRaWAN devices send data to AWS IoT Core in a format that can't be used by AWS services, traffic must be first sent to a Destination. A Destination represents the AWS IoT rule that processes a device's data for use by AWS services.

This AWS IoT rule contains the SQL statement that selects the device's data and topic rule actions that send the result of the SQL statement to the services that will use it.

3.3.2 Add Device to AWS IoT (Continued)

A destination consists of a Rule and a Role. To set up the destination:

1. In the AWS IoT Core console, within the navigation pane to the left, select **“LPWAN Devices”**, then **“Destinations”**.
2. Select **“Add destination”**.
3. Under **“Destination details”**, enter **“ProcessLoRa”** for **“Destination name”**, and optionally an appropriate description.
4. Under **“Rule configuration”**, create a rule named **“LoRaWANRouting”**. For now, the rule does not need to be configured. It will be configured in the separate Hello World example.
5. Finalize by selecting **“Add destination”**.

3.3.3 Add Device to AWS IoT (Continued)

With the Role and accompanying Rule created, register an endpoint device. Note that all TEKTELIC devices support LoRaWAN v1.0.2.

1. In the left navigation pane, select **“LPWAN devices”**, then **“Devices”.**
2. Select **“Add wireless device”.**
3. Under **“Wireless device specification”,** select **“OTAA v1.0.x”** for Tektelic Devices.
4. Fill out the remaining fields as per the OTAA/ABP choice you’ve made above.
5. (Optional) Enter a name and description for your device.
6. Under **“Profiles”,** select a suitable wireless and service profile.
7. Under **“Choose destination”,** select the newly created **ProcessLora** destination.
8. Finalize by selecting **“Next”,** then **“Add device”.**

4. Setup and Configure Gateway

With the certificates and gateway entity created, the gateway can now be configured to connect to AWS IoT Core. Here is an overview of the steps:

1. Install and prepare Basic Station on the gateway.
2. Configure the gateway.

4.1.1 Install Basic Station

- Installing Basic Station in a gateway with BSP older than the major+minor version of the 2021-08 system release will cause the gateway to be **CORRUPTED indefinitely.** Hence, ensure that the BSP is updated prior to installing Basic Station. The 2021-08 system releases are listed below. BSP Upgrade instructions can be found in the COMMUNITY section of the Support Portal.

Gateway	Major+Minor Version
Kona Micro	3.3.x
Kona Micro PoE	2.4.x
Kona Macro	4.3.x
Kona Mega	4.3.x
Kona Enterprise	Any version works

Table-1 BSP Version Requirements

4.1.2 Install Basic Station (Continued)

While there are various methods to install Basic Station on your Kona gateway, the following slides will install it with command line.

1. Login to the gateway using SSH
2. Check the current version of Basic Station if it is installed
3. Obtain Basic Station

4.1.3 Install Basic Station (Continued)

1. Login to the gateway using SSH. Use the following table for the credentials:

Username	Password	Notes
root	9-Digit Serial number of the Gateway (i.e. 1618B0052)	• Applies to gateways with serial numbers that start with 21 and below.
admin	Random string of characters provided on the test report.	• Applies to gateways with serial numbers that start with 22 and above. • **Some units in this category may still have root as the user and the serial number as the default password.**

Table-2 Username and Password

2. Check the current version of Basic Station if installed
   - **opkg info tektelic-bstn | grep Status**

NOTE: If the password is not on the test report, contact Tektelic Support and provide the following:
- T-code (i.e. **T000XXYY**), Revision (i.e. **E1**), and serial number (i.e. **1212A3434**)

4.1.4 Install Basic Station (Continued)

To install Basic Station, we recommend updating to the latest BSP version. The latest BSP version also includes the most up-to-date version of Basic Station. You can find instructions to update the BSP here:

- Through KonaFT
- Through the TEKTELIC CORE Network Server

Once the latest BSP update has been installed, you can install Basic Station with the following command:

- **opkg install tektelic-bstn**

4.2.1 Configure Gateway

In **/etc/default/config.json**, the following settings must be configured.

- “server_address”: “127.0.0.1”,

The following setting **MUST** be added under the **“gateway-conf” section**.

- “report_count”: 1,

NOTE: Customers with a US Micro/Enterprise gateway will need a config.json file configured for the 2nd sub-band of frequencies in US915. You can acquire that here:

(Knowledge Base -> Support -> Basic Station -> Basic Station Interface for AWS IoT core for LoRaWAN)

4.2.2 Configure Gateway (Continued)

If the MQTT bridge is installed, please configure it as follows:

- Insert a "#" in front of the following lines:
  - **"ns_host"** in **"mqtt-bridge.conf"** on gateways **older than 3.3.X** for Micro, 4.3.X for Macro/Mega
  - **"url"** in **"tektelic-bridge.ns.toml"** on gateways **newer than 3.3.0** for Micro, 4.3.X for Macro/Mega
- Remove the "#" in front of the following lines:
  - **"oam_host"** in **"mqtt-bridge.conf"** on gateways **older than 3.3.X** for Micro, 4.3.X for Macro/Mega
  - **"url"** in **"tektelic-bridge.oam.toml"** on gateways **newer than 3.3.0** for Micro, 4.3.X for Macro/Mega
- Once the changes have been made, restart the MQTT bridge with the following command:
  - **/etc/init.d/mqtt-bridge restart**

4.2.3 Configure Gateway (Continued)

- With the files generated, they will need to be transferred to the gateway. While there are various ways of accomplishing this, SCP will be used as an example.
- Run the following command in the folder of the files you created in section 2 to transfer them to the **/etc/bstn** directory on the gateway.

- **scp * root@gateway-ip:/etc/bstn**

4.2.4 Configure Gateway (Continued)

If you require admin credentials to access the gateway, please follow the additional steps to configure and place the files appropriately.

- **scp * admin@gateway-ip:/home/admin**

The following commands are then entered on the gateway:

- **sudo chown root:root /home/admin/***
- **sudo mv /home/admin/* /etc/bstn/**

NOTE: These commands will change ownership of *any* miscellaneous visible files within the home folder. If you do not want this, please create a new directory for the required files, modify and run the above commands.

4.2.5 Configure Gateway (Continued)

With the files transferred, SSH into the gateway and restart both Basic Station and TEKTELIC Packet Forwarder with the following commands:

- **/etc/init.d/tektelic-bstn restart**
- **/etc/init.d/pkt_fwd restart**

Best-In-Class, Carrier Grade & Most Cost Effective Portfolio of Gateways, Network Server, Sensors & Applications