TEKTELIC COMMUNICATIONS INC.

KONA GWS WITH AWS IOT CORE FOR LORAWAN GETTING STARTED GUIDE

Document type: Getting Started Guide
Document status: Final
Last update: 2021-04-06

Table of Contents

1 Document Information

1.1 Naming Conventions

The term “downlink device” or “endpoint device” is used in this document to refer to a LoRaWAN device that connects to a LoRaWAN “Gateway”. The “Gateway” in turn, connects to AWS IoT Core for LoRaWAN.

1.2 Revision History (Version, Date, Description of change)

Revision: v0.3
Date: Apr. 06, 2021
Description of the change: Updated Section 6.4.d (For Class C)

2 Overview

Introducing the Developer Starter Kit containing the Versatile LoRaWAN® Smart Room Sensor and the Highly Scalable KONA Micro Gateway. The KONA Smart Room Sensor integrates practical functionality into a very small form factor. The Smart Room Sensor is an ideal solution for holistically monitoring the home and office environment. The device is capable of measuring and reporting temperature, humidity, light, movement, motion, shock, detecting leaks, open / closed doors and windows. It also supports battery status updates for easy maintenance. Paired with the KONA Micro IoT Gateway, which is designed for enterprise and lightweight industrial applications that require “Always On” connectivity. Configured with an internal 3G/4G modem and a built-in battery backup, the KONA Micro IoT gateway continues to operate and transmits sensor data to the network even when the main site has lost power.

3 Hardware Description

3.1 DataSheet

KONA Micro Gateway: https://tektelic.com/uploads/Brochures/Kona%20Micro.pdf

KONA Macro Gateway: http://tektelic.com/uploads/Brochures/Kona%20Macro.pdf

KONA Mega Gateway: http://tektelic.com/uploads/Brochures/KONA%20Mega%20EU.pdf

4 Setup your AWS account and Permissions

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**.

4.1 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)

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

4.2 Set up Roles and Policies in IAM

4.2.1 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 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.

4.2.2 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.*

First, create a policy with the permissions described above.

- 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**.

Now, create a role that will use the above policy.

- 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 created in the step above. 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**.

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**

5 Add the Gateway to AWS IoT

5.1.1 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 (DevEUI) or serial number. This is used to establish the connection between the LNS and the gateway. Consult the documentation for your gateway to locate this value.
- Your gateway's Basics Station version must be 2.0.5 or higher.

5.1.2 Add the LoRaWAN Gateway

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

- Go to the AWS IoT Core console (**console.aws.amazon.com/iot)** and login.
- 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** (found on the bottom of your gateway as GW ID) and **Frequency band (RF Region)** fields.
- Enter a descriptive name in the **Name – optional** field. We recommend that you use the Gateway EUI 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). We recommend that you store all the downloaded files in the same folder.
    - Then rename xxxx.cert.pem file to cups.crt and xxxx.private.key to cups.key.
    - Create a copy of *cups.key* and name it *tc.key*.
    - Create a copy of *cups.crt* and name it *tc.crt*.
- In the section **Provisioning credentials**, choose **Download server trust certificates** to download the CUPS (cups.trust) and LNS (lns.trust) server trust certificates.
    - Keep the cups.trust file as it is.
    - Rename the lns.trust file to tc.trust.
- Copy the CUPS and LNS endpoints and save them for use while configuring the gateway.
    - Create cups.uri file with CUPS Endpoint URL:
      e.g: https://EXAMPLE.cups.lorawan.REGION.amazonaws.com:443
    - Create tc.uri file with LNS Endpoint URL:
      e.g: wss://EXAMPLE.gateway.lorawan.REGION.amazonaws.com:443

Make sure that you have the following 8 files from the steps above as you'll need them to configure your gateway:

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

- Choose **Submit** to add the gateway.

6 Set up and Configure the Gateway

6.1 Set up Gateway hardware

KONA Micro Gateway Unboxing

KONA Gateway Setup steps.
Box contains:

- KONA Micro Gateway / Kona Macro Gateway / Kona Mega Gateway
- Power Adapter
- Ethernet Cable
- LoRa Antenna (Included with Micro, Purchase separately for Mega and Macro Gateways)

Setup:

- Remove items from box
- Connect LoRa Antenna to Micro Gateway
- Plug into power source
- Plug into ethernet source

Your KONA Gateway is now live and ready to connect!

Detailed Quick start guides are available for KONA Micro Gateway and Smart Room Sensors at
support@tektelic.com
https://support.tektelic.com/portal/en/kb/support

6.2 Set up Gateway Software

The minimum BSP version is required for this is, For Mega and Macro, BSP Version should be 4.x.x and for Micro, BSP version should be 3.x.x.

- Login to your Gateway using SSH. By default, user name is "root" and the password is "Gateway's 9-digit serial number" (You can find this information on the label on your Gateway)

You can check the BSP version on your gateway by issuing "system_version" command on the Gateway's console (using SSH).

6.2.1 Preparing Basic Station for the installation on BSP 3.0.x and 3.1.x (Micro) and 4.0.x and 4.1.x (Mega and Macro):

- Please create an account on our support portal (https://support.tektelic.com/portal/en/signin) and go to knowledge base -> Basic Station
- Download the Basic Station Package. (Basic-Station-packages-vx.x.x-for-Tektelic-gateways.tar.gz)
- Then, upload the Basic-Station-packages-vx.x.x-for-Tektelic-gateways.tar.gz to the directory /lib/firmware on the target gateway and extract it using following command.

```
tar -C /lib/firmware \
    -zxvf /lib/firmware/Basic-Station-packages-vx.x.x-for-Tektelic-gateways.tar.gz
```

- Add the feed location to the package manager configuration file by using following command:

```
echo "src/gz bstn file:///lib/firmware/Basic-Station-packages-vx.x.x-for-Tektelic-gateways" \
    > /etc/opkg/bstn-feed.conf
```

- Then enter the following command.

```
opkg update
```

6.2.1.1 Installing Basic Station packages using command line:

To install the basic Station packages, run the following command:

- opkg install tektelic-bstn curl libcurl4

6.2.2 Preparing Basic Station for the installation on Micro BSP 3.2.x, Mega/Macro 4.2.x or later:

- Obtain the ipk/bsp package by contacting our support team. Please create an account on our support portal (https://support.tektelic.com/portal/en/signin) or send an email to support@tektelic.com to contact us.
- Upload the ipk/bsp folder to the gateway and extract it into /lib/firmware.
- Add the feed location to the package manager configuration file by running following command.

```
echo "src/gz bstn file:///lib/firmware/bsp" > /etc/opkg/bstn-feed.conf
```

- Then enter the following command.

```
opkg update
```

6.2.2.1 Installing Basic Station packages using command line:

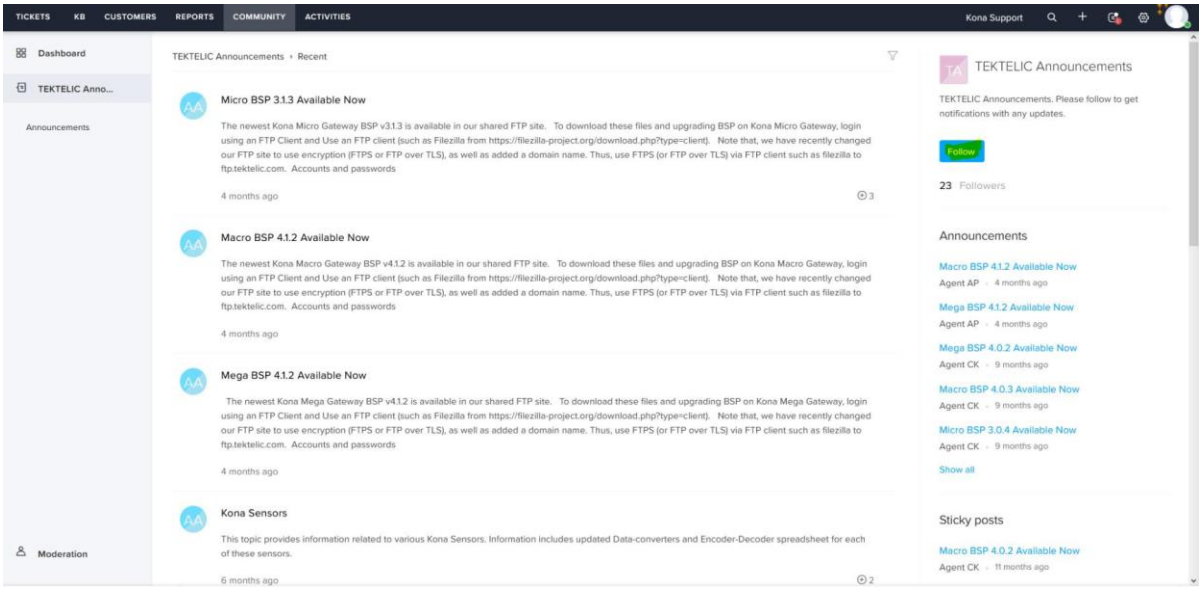
To install the basic Station packages, run the following command:

- opkg install tektelic-bstn curl libcurl4

Note:

Please create an account on our support portal (https://support.tektelic.com/portal/en/signin) and go to knowledge base for Gateway and Device Guides and Documentation.

To get up to date information about our new BSP Releases for Gateways and Firmware releases for Devices, please go to community in our support portal and select "FOLLOW" button under TEKTELIC announcements. Then you will receive email notifications whenever we release new software.



If you have any questions or issues reach out to support@tektelic.com, one of our Customer Support Specialists will assist you.

6.3 Additional Software References

None

6.4 Configure the Gateway

This configuration is applicable for Kona Mega, Kona Macro and Kona Micro gateways.

a. Login to your Gateway using SSH. By default, user name is “root” and the password is “Gateway’s 9-digit serial number” (You can find this information on the label on your Gateway)
b. Make sure Basic Station and Packet Forwarder are installed.
   - To check whether the packet forwarder is installed, enter “system_version” command on the console and look for Packet Forwarder, if it is listed then which means packet forwarder is installed.

```
root@kona-micro:~# system_version

Distributor ID:       Tektelic
Description:          Tektelic Kona Micro GNU/Linux 3.1.3
Release:              3.1.3

Product:              Kona Micro
u-boot:               2013.07-rc2-kona-micro-indoor-v0.7-gd941e52ab1
Linux kernel:         3.12.17-tektelic-2.3.0-kona-micro-indoor-g56fb3ac90d

System monitor:       tektelic-system-monitor-0.15-r6
SNMP agent:           tektelic-snmp-agents-1.1.0-r12
LTE connection mgr:   modem-connection-manager-0.42-r8
Network monitor:      kona-network-monitor-0.19-r7
NS switcher:          kona-ns-switcher-0.36-r13
Packet forwarder:     kona-pkt-forwarder-4.0.22-r121
LoRa HAL:             tektelic-lora-hal-3.6.1-r2
BIST manager:         tektelic-bist-manager-0.7-r4
BSP upgrade tool:     tektelic-upgrade-1.4.2-r30.p17
Backup tool:          tektelic-backup-1.5.1-r16
FPGA access tool:     tektelic-fpga-access-1.0.0-r7
TCS agent:            tektelic-tcs-1.3.2-r47

GPIO FPGA:            5007 build 0027
root@kona-micro:~#
```

- To check whether the Basic Station is installed, enter “opkg list-installed | grep bstn” command on the console.

```
root@kona-micro:~#
root@kona-micro:~# opkg list-installed | grep bstn
tektelic-bstn - 1.4.1-r58
root@kona-micro:~#
```

- If they are not installed, please reach out to us on our support portal (sign up required - https://support.tektelic.com/portal/en/signin), or support email – support@tektelic.com

c. Then make sure Basic Station and Packet Forwarder are running.
   - To check whether they are running, enter “ps aux | grep pkt” and “ps aux | grep bstn” command on the console, if they both show up with process id which means they both are running.
     For Packet Forwarder:

```
root@kona-mega:~# ps aux | grep pkt
pktfwd    1981  5.3  0.4  63276  2428 ?        Sl   01:21  57:18 /usr/bin/pkt_forwarder -c /etc/default/config.json -s
root     10366  0.0  0.0   1804   460 ttyO0    S+   19:10   0:00 grep pkt
```

     For Basic Station:

```
root@kona-mega:~# ps aux | grep bstn
root      2010  0.1  0.7  24388  3684 ?        SLl  01:22   1:40 /usr/sbin/tek_bstn -c /etc/default/bstn.toml -v 3
root     11161  0.0  0.0   1804   464 ttyO0    S+   19:10   0:00 grep bstn
```

   - If they are not running, please reach out to us on our support portal (sign up required - https://support.tektelic.com/portal/en/signin), or support email – support@tektelic.com

d. Configure Packet Forwarder:
   - For Class C only: (Mega and Macro GWs Only)
     Make sure to set "beacon_period": 0 in /etc/default/config.json file.
   - Update the “server address” in /etc/default/config.json file to 127.0.0.1. Then restart the packet forwarder. (/etc/init.d/pkt_fwd restart)

e. Configure Basic Station:
   - Keys and certificates required:
     - tc.uri
     - tc.trust

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

- Copy the previously downloaded and created keys and certificates (see section 4.3.2). and put them into /etc/bstn directory on your GW. (You can use winscp to transfer files from windows PC)
- By default, CUPS is enabled in the Basic Station to connect with Server. If you don't want to use CUPS then you can disable that by set "skip_cups=true" in /etc/default/bstn.toml file.
- Then enter the following command to restart the Basic Station.

  /etc/init.d/tektelic-bstn restart
- Now your Gateway should be able to connect to the server.
- You can find the packet forwarder log file in /var/log/pkt_fwd.log
- You can find the Basic Station log file in /var/log/syslog (If your GW has 3.0.x, 3.1.x, 4.0.x and 4.1.x BSPs)
- You can find the Basic Station log file in /var/log/bstn.log (If your GW has 3.2.x and 4.2.x or later)

If you have any questions or issues, please reach out to us on our support portal (sign up required - https://support.tektelic.com/portal/en/signin), or support email – support@tektelic.com

7 Support

If at any step you encounter problems – feel free to reach out to us on our support portal (sign up required - https://support.tektelic.com/portal/en/signin), or support email – support@tektelic.com