
# Onboarding MultiTech Gateway for AWS IoT Core for LoRaWAN®

Published 12/12/2020

# Contents


*1 Document Information ..... 3*

1.1 Naming Conventions ..... 3

1.2 Revision History (Version, Date, Description of change) ..... 3

*2 Overview ..... 3*

2.1 MultiTech QuickStart, Conduit® AP, Conduit®, and Conduit® 300 ..... 3

2.2 DataSheet & Standard Kit Contents: ..... 3

2.3 User Provided Items: ..... 4

2.4 3rd Party Purchasable Items ..... 4

2.5 Additional Hardware References ..... 4

*3 Setup your AWS Account and Permissions ..... 4*

3.1 Overview ..... 4

3.2 Set up Roles and Policies in IAM ..... 4

3.2.1 Add an IAM Role for CUPS server ..... 4

3.2.2 Add IAM role for Destination to AWS IoT Core for LoRaWAN ..... 6

3.3 Add the Gateway to AWS IoT ..... 7

3.3.1 Preparation ..... 7

3.3.2 Add the LoRaWAN Gateway ..... 7

*4 Set up the Gateway ..... 7*

4.1 Set up Gateway Hardware ..... 7

4.2 Set up Gateway Software ..... 8

4.3 Additional Software References ..... 9

4.4 Configure the Gateway Device ..... 9

# 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)

| | | |
|---|---|---|
| 1.0 | 12-Dec-2020 | Initial Version. |

# 2 Overview

## 2.1 MultiTech QuickStart, Conduit® AP, Conduit®, and Conduit® 300:

MultiTech QuickStart AWS IoT Core for LoRaWAN® provides everything needed to rapidly get your LoRaWAN sensor application up and running on AWS – all in one box. The QuickStart kit is designed to enable you to obtain sensor information from an off-the-shelf sensor and display it in the cloud within minutes of opening the box. QuickStart kit – the industry’s most configurable, manageable, and scalable communications kit for industrial IoT applications.

MultiTech Conduit® AP: The Conduit® AP conveniently provides deep in-building connectivity and improved performance for network operators and enterprises connecting thousands of IoT assets by harnessing the power of the LoRaWAN® protocol.

The MultiTech Conduit®: The Conduit® (MTCDT Series) is a quick-to-deploy and simple-to-scale, programmable IoT gateway designed for versatility.

MultiTech Conduit® 300: The new Conduit® 300 Series gateway developer kit featuring mPower™ Edge Intelligence enables streamlined edge-to-cloud orchestration, management and analytics together with a high performance, secure processor to support Dockers and containers for easy programmability and built-in compatibility with leading IoT software platforms.

mPower™ Edge Intelligence:
mPower™ Edge Intelligence is an embedded software offering, building on its popular application enablement platform, to deliver programmability, network flexibility, enhanced security and manageability for scalable Industrial Internet of Things (IIoT) solutions.

NOTE: LoRaWAN BASIC STATION is supported in mPower Version 5.3 and is available for download for MTCAP, MTCDT, MTCDT3.

## 2.2 DataSheet & Standard Kit Contents:

You can find datasheets and other info for these devices here:

MultiTech QuickStart https://www.multitech.com/brands/quickstart-iot-solutions
MultiTech Conduit® AP Access Point: https://www.multitech.com/brands/multiconnect-conduit-ap
MultiTech Conduit®: https://www.multitech.com/brands/multiconnect-conduit
MultiTech Conduit® 300: https://www.multitech.com/brands/conduit-300-dev

## 2.3 User Provided Items:

A PC/Laptop with Ethernet capability.

## 2.4 3rd Party Purchasable Items

Look up more products at https://www.multitech.com/products/product-selector or Contact sales@multitech.com for additional sensors.

## 2.5 Additional Hardware References

- https://www.multitech.com/
- https://www.multitech.com/AWSBUY
- https://www.multitech.com/products/product-selector
- https://www.multitech.com/onboard
- https://www.multitech.com/connect

# 3 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**.

## 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 section Add a LoRaWAN Device to AWS IoT)
    a. Verify device and service profiles
    b. Set up a Destination to which device traffic will be routed and processed by a rule.

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 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

### 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 (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.
- Make sure your MultiTech gateway is on mPower™ version 5.3.0 or higher you can find the firmware download here: http://www.multitech.net/developer/downloads/

### 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 do not recommend you leave it blank.
- 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).
  (You will open these files in a notepad application and copy paste the contents into the gateway UI basic station configuration)
- 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 and LNS endpoints and save them for use while configuring the gateway.
- Choose **Submit** to add the gateway.

# 4 Set up the Gateway

## 4.1 Set up Gateway Hardware

- Connect the Ethernet cable from the gateway to the computer/laptop.
- Screw in the LoRa antenna to the connector to gateway.
- If you have a cellular gateway screw in the cellular antenna and insert your SIM.
- Plug in the gateway to a power supply to power it up.

- Gateway will go through the boot process
- Gateway will be up and ready when the 'status' LED is flashing
- Change Adapter settings to Connect to Gateway:
    - On a Windows computer go to the control panel
    - Select Network and Internet
    - Select Network and sharing Center
    - Select Change Adapter Settings
    - Right Click Ethernet
    - The Ethernet Dialog Box will open, select Internet Protocol Version 4(TCP/IPv4) and click the Properties button
    - Select Use the Following and fill out the following fields accordingly
        - IP Address: Enter an IP Address on the default subnet
            Example: 192.168.2.XXX
        - Subnet Mask: 255.255.255.0 [Note:] leave the DNS address blank you do not need an IP address for this configuration.

## 4.2 Set up Gateway Software

- Open a web browser and enter the device's default ip address http://192.168.2.1
- A security window will open, click on the Advanced button to bypass, then click on "Proceed to 192.168.2.1"
- This will open up **commissioning mode**, create username and strong password
- Log into the gateway with new username to admin & strong password
- This will take you to the First-Time Setup Wizard
- Click Next, Click Next again to skip the Call Home Setup. Set the Date, Time and Time Zone
- Exit the First-Time Setup Wizard
- OPTION 1: Configure the Gateway Ethernet as a WAN interface.
    - Navigate to Setup -> Network Interfaces
    - Click the edit Icon next to eth0
        - Set the following
        - **Direction:** WAN
        - **Mode:** Static
        - **IP Address:** Set your desired ip address on the same subnet as your router
            Ex. If router ip is **192.168.1.1** set ip address to **192.168.1.xxx**
        - **Mask:** 255.255.255.0
        - **Gateway:** 192.168.1.151 ←Point to your router's ip address
        - **Primary DNS server:** 8.8.8.8
        - Click **Submit**
- OPTION 2: Configure the Gateway Cellular as a WAN interface:
    - Navigate to cellular -> Cellular Configuration
    - Check the radio button for Enabled.
    - Provide an APN if it's an ATT SIM.
    - Enable Keep Alive to your preferred hostname.
    - Click Submit.
- Navigate to Administration -> Access Configuration
- Make sure the following are checked.
    - **HTTP Redirect to HTTPS**: all checked
    - **HTTPS via WAN ( optional for cellular as WAN)**
    - **SSH via LAN & via WAN ( SSH via WAN is optional on cellular)**
    - **ICMP Settings**: All checked
- Click **Submit**

- Click **Save and Apply**, the gateway will reboot (Click "Ok" when prompted).
- Check Internet Access on the Gateway:
    - For Ethernet as WAN Remove your Ethernet port from computer and plug into your router
    - Wait for the gateway to boot up
    - On Windows, in the search window type "cmd" and select "Command Prompt"
    - From the Command Line SSH into your gateway set ip address
    - $ ssh admin@192.168.1.151 or ssh admin@192.168.2.1
    - Once logged into the gateway, type and enter "ping google.com" check in the gateway has internet access. You should see bytes of data being sent.
    - example:
        - Pinging www.google.com [172.217.8.164] with 32 bytes of data:
        - Reply from 172.217.8.164: bytes=32 time=25ms TTL=114

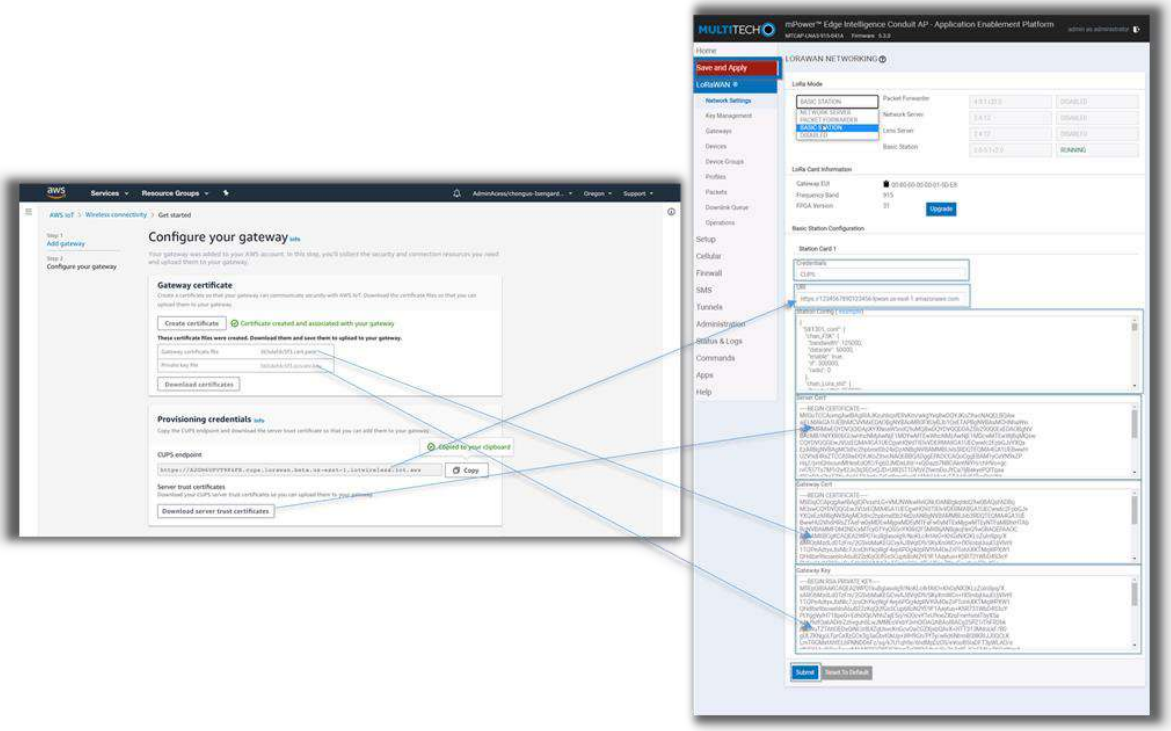
## 4.3 Additional Software References

There is additional support available for MultiTech gateways at:

- http://www.multitech.net/developer/
- You can raise a support ticket at https://support.multitech.com/

## 4.4 Configure the Gateway Device

- LoRa and Basic Station Configuration:
    - To setup basic station select "**LoRaWAN**" on the main UI then "Network Settings" (this should be the default).
    - Change the "Mode" combobox to "**BASIC STATION**". The fields on this page now correspond to each of the files that Basic Station needs to initiate a connection (more information about this can be found in the Semtech Basic Station documentation at https://doc.sm.tc/station/)
        - Credentials: set it to "CUPS". (AWS uses CUPS authentication, not LNS. You can read more about LNS and CUPS here https://doc.sm.tc/station/credentials.html#files-types)
        - URI: URI of the network server. The URI will be provided/generated when you create a gateway on AWS. See Add the LoRaWAN Gateway for details on how to get the CUPS endpoint.
        - Station config: This is the same as a Semtech UDP packet forwarder file. Use the example file from the UI already populated for you.
        - Server Cert: This is the *.trust downloaded from AWS earlier. Copy and paste the contents of the file into this field.
        - Gateway Cert: This is the *.crt file downloaded from AWS earlier. Copy and paste the contents of the file into this field.
        - Gateway Key: This is for the *.key file downloaded from AWS earlier. Copy and paste the contents of the file into this field.
    - After filling each of the fields click "Submit" at the bottom of the page, then "Save and Apply"




If you need further assistance you can contact https://support.multitech.com/ for further support.