Quick Start Guide for AWS IoT Core

This guide provides directions for connecting Banner Engineering's Cloud ID™ Kit to AWS IoT Core rather than Banner CDS™.

This kit consists of a DXM-Series Controller that is designed to easily pair with up to 40 wireless condition monitoring sensors, sold separately. For more information and guidance on the Banner Cloud ID™ Kit, please review the Setup Guide.

This guide assumes you have access to an AWS account. If you have not yet done so, set up your AWS account and permissions. More information is available in the AWS documentation here: Set up your AWS account.

The DXM requires firmware version 3.3.4 or newer. To download the latest firmware, check the software section of the DXM page on www.bannerengineering.com. Launch the DXM Configuration Software and go to **Tools › Reprogram** to load the latest firmware.

About the Hardware

Depending on the sensors purchased with the kit, users are provided with the following hardware:

- IP67-rated housing for use in challenging environments
- DC power supply included within the Banner Cloud ID Gateway
- Embedded cellular device that provides an optional connection to Verizon, AT&T, or multiple carriers for international regions
- External antennas to ensure reliable data transmission in all conditions
- Default Ethernet connection (users can also enable Cellular Data Services in minutes)
- Sensors selected and purchased in your kit

No additional items need to be provided by users to get started. For more information on this kit and compatible sensors, please refer to the following documents:

- Asset Monitoring Gateway with Cloud ID Sell Sheet (p/n 222399)
- Asset Monitoring Gateway with Cloud ID Setup Guide (p/n 222401)
- Asset Monitoring Gateway with Cloud ID Quick Start Guide (p/n 236146)

Set Up the Hardware for AWS IoT Core

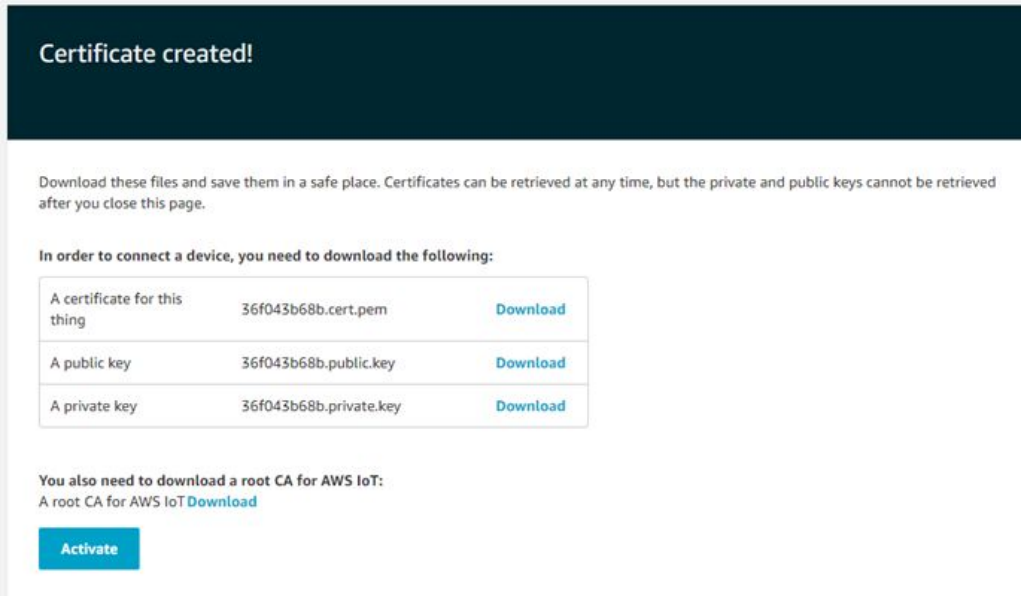
Follow these instructions to configure the DXM in the Banner Cloud ID™ Kit for AWS IoT Core.

1. Download, install, and launch the DXM Configuration Software. (must be version 4.10.26 or newer)
2. Download the AWS Cloud ID Kit files from www.bannerengineering.com.
3. Apply power to the DXM Wireless Controller and then connect either the USB cable or Ethernet cable.

   Note: Depending on the model of the DXM Wireless Controller in your kit, your USB and Ethernet ports may be found in different places on the device. Please refer to the Banner Cloud ID™ Kit manual as well as the manual for your DXM model for more information.
4. In the configuration software, go to the Connect to DXM tab and connect the software to the DXM:
   - Serial (USB cable) – Choose the **Comm Port** from the drop-down and click **Connect**. Use the refresh button if no comm port is showing up or working.
   - TCP/IP (Ethernet) – Enter the IP address of the DXM and click **Connect**. The computer and DXM must be on the same network. Either set the IP address of the computer to match the DXM in a static setup or set the DXM's IP address on the **Software Config › Ethernet** screen.
5. Go to **File › Open** and select the appropriate downloaded AWS Cloud ID Kit XML configuration file.

   There are two files, one for ATT and one for Verizon. Choose the correct file for the carrier your kit's DXM is using. The last letter of your model number will indicate this (A for ATT and V for Verizon).
6. Go to the **Settings › Script** screen and click **Upload file**. Choose the file named CloudIDKit.sb. (Verify the file properly loads by watching the Application Status area at the bottom of the software.)
7. After the ScriptBasic file uploads, the script name appears in the box next to the Upload file button. Verify the name of the file matches the file listed in Script to run at startup.

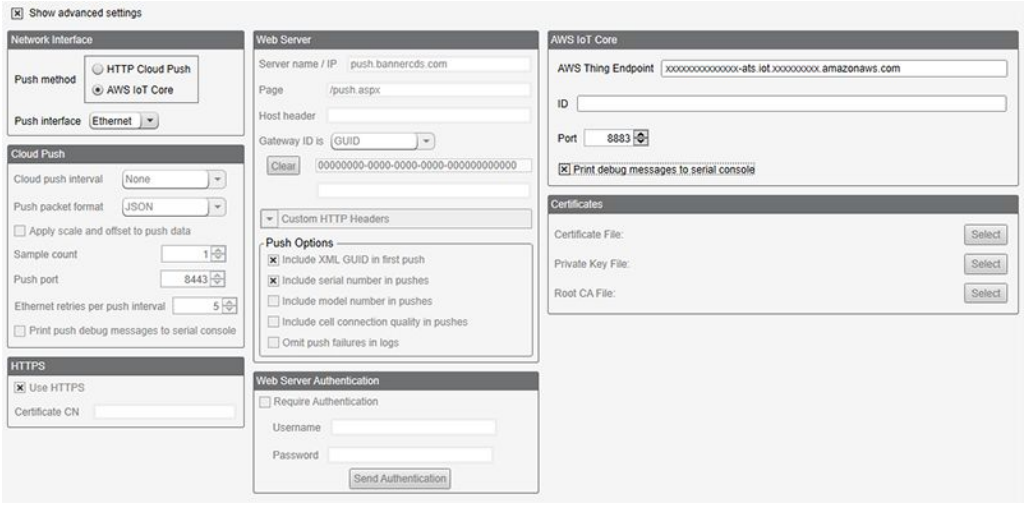
Create IoT Resources in AWS IoT Core



1. Navigate to the AWS IoT Console and create your IoT Resources in the cloud. You will need to create a **Policy** and a **Thing** with associated certificates and keys.
    a. Go to **Secure** on the left menu and select **Policies** to create an AWS IoT Policy that allows your device to interact with AWS IoT.
    b. Go to **Manage** in the left menu and select **Things**. Click **Create** and then **Create a Single Thing**.
    c. Download the **Certificate**, **Private Key**, and **Root CA** for your thing. Ensure your **Certificate** is Active.
    d. Additional guidance for these steps can be found in the AWS IoT Documentation here: Create IoT Resources.
2. Find your AWS IoT Endpoint.
    a. To find the endpoint, go to the **AWS IoT console**.
    b. Choose **Settings** in the navigation pane.
    c. The endpoint can be found under **Device Data Endpoint**. It should look similar to this: xxxxxxxxxxxxxx-ats.iot.xxxxxxxxx.amazonaws.com
    d. Keep this endpoint available for future steps.

Insert Certificates and Endpoint

Cloud Services screen for using AWS IoT Core



1. On the DXM Configuration Tool: Go to the **Settings › Cloud Services** screen and verify the **Push method** is set to AWS IoT Core.
2. Enter the **AWS Thing Endpoint** that you previously accessed from AWS IoT Core.
3. Upload the **Certificate**, **Key**, **Root CA File** generated from the creation of your AWS Thing.
    a. Use the Certificate File's **Select** button to select the **Certificate File**.

   b. Use the Private Key File's **Select** button to select the **Private Key File**.
   c. Use the Root CA File's **Select** button to select the **Root CA File**.
4. (Optional) Adjust the **ID** name for reference if you are using multiple DXM Controllers.
5. (Optional) Go to the **Settings › AWS IoT Core** screen and modify Topic Names under the **Subscribe** or **Publish** sections, but do not change groups or push times. The default names for **Subscribe** and **Publish** are EK. Do not adjust the Publish **Timers**. The DXM pushes to AWS IoT Core based on the publish timers defined in the script file.
6. For Cellular Connection Only—If you are using a cellular connection instead of an Ethernet connection, go to the **Settings › Ethernet** screen and set your device's **IP Address** to Static IP.
7. Save the XML configuration file.
8. Go to **DXM** on the menu bar and select **Send Configuration to DXM** to upload the new configuration file to the DXM. The DXM reboots after the files are uploaded. The system begins pushing data to AWS IoT Core instead of Banner Cloud Data Services (CDS)
9. Verify your data is connecting with AWS IoT Core.
   a. In your web browser, navigate to the AWS IoT Core console.
   b. Choose **Test** in the navigation pane.
   c. Select **MQTT Test Client**.
   d. Subscribe to "EK," or whatever topics you created to publish in the DXM Configuration Software.

The DXM Controller pushes data every five minutes on Ethernet and every 10 minutes on cellular. Note: the manual data push on the DXM device screen is for HTTP only, so you will need to wait 5 minutes to validate the MQTT connection with AWS IoT Core.

For additional information or instructions, please follow the instructions for the Banner Cloud ID Kit.

Document title: Banner Cloud ID™ Kit Quick Start Guide for AWS IoT Core
Part number: b_51143197
Revision: E