# Connecting to an AWS IoT Core



## AWS IoT Core Quick Start Guide

This guide provides directions for connecting Banner Engineering's DXM to an AWS IoT Core instead of the Banner CDS.

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 relevant sections are **Sign up for an AWS account**, **Create a user and grant permissions**, and **Open the AWS IoT Console**.

For more complete information about setting up a DXM1200 Wireless Controller, refer to the instruction manual (p/n 216539).

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 and use the DXM Configuration Software under **Tools > Reprogram** to load the latest firmware.

### Connect to the DXM

Follow these steps to connect the DXM to the configuration software.

- 1. Download, install, and launch the DXM Configuration Software. (must be version 4.10.26 or newer)
- 2. Apply power to the DXM Wireless Controller.
- Connect either the USB cable or Ethernet cable between your computer and the DXM. Depending on the model of the DXM Wireless Controller, your USB and Ethernet ports may be found in different places on the device. Please refer to the manual for your DXM model for more information.

4. In the configuration software: Go to the Connect to DXM screen and connect the software to the DXM.

- Serial (USB cable) Choose the Comm Port from the drop-down list 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.

### Create IoT Resources in AWS IoT Core

- 1. Go 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. Additional guidance for these steps can be found in the AWS IoT Documentation: Create IoT Resources.

Create your AWS IoT Core certificate			
Certificate crea	ted!		
fter you close this page.	save them in a safe place. Certificat ice, you need to download the foll 36f043b68b.cert.pem		any time, but the private and public keys cannot be retrieved
A public key	36f043b68b.public.key	Download	
A private key	36f043b68b.private.key	Download	
You also need to downloo A root CA for AWS IoT Dov Activate	ad a root CA for AWS loT: vnload		

- a. On the left menu, go to Secure > Policies to create an AWS IoT Policy that allows your device to interact with AWS IoT.
- b. Go to Manage > Things. Click Create and then Create a Single Thing.
- c. Download the Certificate, Private Key, and Root CA for your thing. Verify your Certificate is Active.
- 2. Find your AWS IoT Endpoint.
  - a. To find the endpoint, go to the AWS IoT console.
  - b. In the navigation pane, select Settings.
  - c. The endpoint can be found under **Device Data Endpoint**. It should look similar to this: xxxxxxxxxxxxats.iot.xxxxxxxx.amazonaws.com.
  - d. Copy your endpoint and paste it into a safe place for future steps.

### Enter the AWS Certificate and Endpoint

- 1. On the DXM Configuration Software: Go to the Local Registers screen.
- 2. Use the **Edit Register** tab or the **Batch AWS IoT Core Configuration** tab to verify your selected registers are configured to push to AWS IoT Core.

Edit Register	Madife Multiple Depletors	Batch AWS IoT Core Configuration			
on register	Modify Multiple Registers	Batch Aws for Core Configuration			
Selected Reg	ister: 1				Clear Register
Register Over	view	Value Options		Storage / HTTP Connectivity	AWS IoT Core
			and a second	and the second se	
Name		Value type	None )*)	LCD permissions None	Push to AWS IoT Core
Name Register grou		Scaling	None v	LCD permissions None None	Push to AWS IoT Core     AWS IoT Core push group 1
Name Register grou Units	IP None		(cons ) (c)		

3. Go to the Settings > Cloud Services screen and verify the Push method is set to AWS IoT Core.

AWS Core parameters on the Settings > Cloud Services screen

Network Interface	Web Server	AWS IOT Core
Puth method  HTTP Cloud Puth ANS IoT Core Puth Interface Ethernet  Puth Interface Ethernet  Puth Pache Isonet I Ion Puth Pache Isonet I Ion Puth Pache Isonet I Ion Puth Pache Isonet IIII Ethernet refless per puth Interval  Pith pach Isonet Coreste	Include cell connection quality in nucleas	AVYS Thing Endpoint [cocococococov-ability cococococo aniazonaws.com] ID Port 8883 (c) EPrint debug messages to senial console Centificate Fac: Private Koy File: Root CA File: Select
HTTPS EUse HTTPS Certificate CN	Web Server Aufhentication Require Authentication Username Password Send Authentication	

- 4. In the AWS IoT Core section, enter your AWS IoT Endpoint.
- 5. Upload the Certificates and Keys that you downloaded from AWS ("Create IoT Resources in AWS IoT Core" on page 1).
- 6. (Optional) Modify the ID Name for reference if you are using multiple DXM Controllers.
- 7. Go to the Settings > AWS IoT Core screen.

AWS IoT Core configuration screen

Publish	API Traffic Publish
Add Publish Delete Selected Publish	Include in config
Enabled Topic Group Timer (hh.mm.ss)	Enabled
	Topic
E 10 00000	Timer (bhumm:ss) 00.00.00 @-
	Subscribe (For API commands only)
	Add Subscription Delete Selected Subscription
	Enabled Topic

- 8. Create Topic names under Subscribe or Publish and adjust the Groups and Times as required.
- 9. Cellular Connection Only If you are using a cellular connection instead of Ethernet, go to Settings > Ethernet and set your device's IP address to Static IP.
- 10. Save the XML configuration file.
- 11. Upload the XML configuration file to the DXM Controller.
  - a. Go to the **DXM** menu.

#### b. Click Send Configuration to DXM.

The DXM Controller reboots after the files are uploaded. The system begins pushing data to AWS IoT Core instead of Banner Cloud Data Services (CDS).

- 12. Verify your data is connecting with AWS IoT Core.
  - a. Go to the AWS IoT Core console and select Test in the navigation pane.
  - b. Select MQTT Test Client.
  - c. Under **Subscribe to a Topic**, enter the Publish Topics you created in the DXM Configuration Software.

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

- Online product page: https://www.bannerengineering.com/us/en/products/part.801553.html
- Instruction manual for the DXM1200 Wireless Controller (p/n 216539).

Document title: Connecting to an AWS IoT Core Part number: b\_5933667 Revision: D Original Instructions © Banner Engineering Corp. All rights reserved.