Connecting to an AWS IoT Core



AWS IoT Core Quick Start Guide for DXM1200

This guide provides directions for connecting Banner Engineering's DXM1200 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 your 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.
- 3. 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.

Figure 1. Create your AWS foT Core certificate

Certificate crea	Certificate created!					
after you close this page.			any time, but the private and public keys cannot be retrieved			
A certificate for this thing	36f043b68b.cert.pem	Download				
A public key	36f043b68b.public.key	Download				
A private key	36f043b68b.private.key	Download				
You also need to downlo A root CA for Ain'S IoT Dev Activate	ad a root CA for AWS IoT: www.oad					

- 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.
- Find your AWS IoT Endpoint.
 - a) To find the endpoint, go to the AWS IoT console.

 - ats.iot.xxxxxxx.amazonaws.com.
 - d) Copy your endpoint and paste it into a safe place for future steps.

Enter the AWS

and Endpoint

- 1. On the DXM Configuration Software: Go to the Local Registers screen.
- 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.

Figure Z. AWS IoT Core settings

Edit Register	Modify Multiple Registers	Batch AWS to? Core Configuration						
Swiected Regis	ter: 1 📴							Clear Register
Register Overv	iew.	Value Options			Storage / HTTP Control	rdirity.		AWS IsT Core
Name		Value type	None	10	LCO permissions	None	14	Push to AVS IsT Care
Register proup	•	Scaling	None	1.	SD card logging	None	(*)	AINS IOT Core push group 1
UNIS	None	slign type	Unsigned		Claud settings	None	14	Apply Scale / Offset for AWS InT Core
					Protocol conversion	None		To Bubble union union channess

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

Figure 3. AWS Core parameters on the Settings > Cloud Services screen

Show advanced settings		
Network Interface	Web Server	AWS InT Care
Push method	Server name / 19° (such kannends sen Page (outh aspc Hool header Galerway 10 to (0.00 m) (Case)0000000-0000-0000-0000-00000000000	Abh's Thing Eindpaier coccessococcon-abl let assococco amazonaws cam
Puch packet formal (50%) Apply pucket formal (50%) Sample count Fuch part Ethernet retries per puch interval Prom puch debug mescages to certar concore Ethernet User HTTPS Certificate CN		Certificates Certificates File: Private Kiny File: Root CA File: Sellect Sellect

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

Figure 4. AWS for Core configuration screen

Pater	API Traffic Publish
AM Public Device Dation	Include in carific
Enabled Tapic Group Tener(McNet121)	Enabled
	Taper
	Buboular (Far KPI sammands anly)
	Att Subscription Delete Selected Subscription
	Enamed Nape

- Create Topic names under Subscribe or Publish and adjust the Groups and Times as required.
- 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 addition 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).

