Aguardio

AGUARDIO – HPE ARUBA INTEGRATION GUIDE

Set up and configure HPE Aruba Networking Access Points to receive Aguardio Pipe Sensor data

1. Architectural Overview · Hardware Overview
2. Settings · Configuration
3. Connection · Verification · Troubleshooting

Aguardio's smart IoT sensors deliver unique data from water pipes and bathrooms. Digitalization of pipes with sensors enhances water & energy management plus optimizes buildings & operations via data (both for cold & hot water plus water for heating). The Pipe Sensor e.g. monitors water activity for water pipes and toilets (e.g. flushes), detects leaks, and enables Legionella risk management plus delivers data for optimization of heating.

PDF Click here to download Aguardio HUB guide

1. Architectural Overview and Hardware Overview

- Each Aguardio sensor is broadcasting a BLE signal every three seconds. This contains relevant measurement data.
- On average, the signal can be captured within 40 meters, but in some cases, it may be as low as 5 meters. Signal strength is influenced by factors such as sensor placement and physical obstacles like walls, which can significantly impact the Received Signal Strength Indicator (RSSI) value. To determine signal strength and signal reach from a specific location, various apps can be used, such as nRF Connect. Aguardio can guide on this.
- If the RSSI value in Aruba Central is displayed as too low, the HPE Aruba Networking Access Point might fail to pick up all messages from the sensor and this may result in data gaps. The placement of walls and their material can be the cause, to improve RSSI value consider installing an extra HPE Aruba Networking Access Point to collect data.
- If the HPE Aruba Networking Access Point fails to pick up at least one measurement every minute, the Aguardio Hub platform might not be able to show accurate information.
- If configured properly as shown in this guide, the HPE Aruba Networking Access Points scans for BLE advertisement messages from nearby devices based on your radio profile configuration.
- When the Aguardio app is installed on the HPE Aruba Networking Access Points, it filters incoming BLE advertisement data to the Aguardio Pipe Sensors and forwards any data collected to the Aguardio servers via a secure WebSocket connection (WSS).
- The connection expects an access token that verifies the client to the server. Once the data has been successfully transferred to the server, it can be viewed in the Aguardio Hub platform.

HPE ARUBA INTEGRATION GUIDE

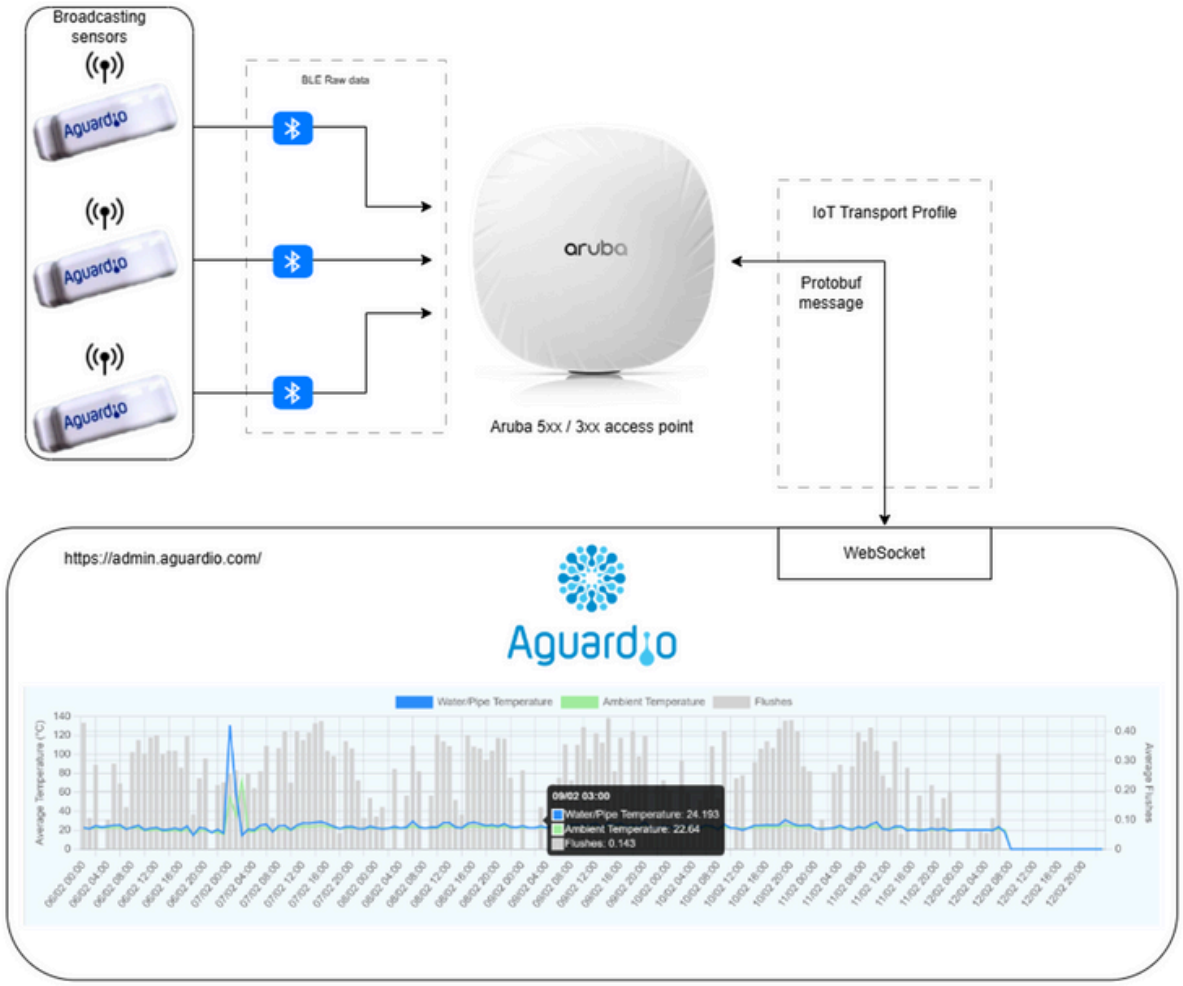


Figure 1: Architectural diagram of an Aguardio-Aruba setup

1.1 In order to configure an HPE Aruba Networking Access Points to handle Aguardio sensor data, it is necessary to have access to the Aruba Central platform. Please make sure that all devices have the required firmware version installed, as, specified in the requirements.

Component	Version Requirement	Notes
HPE Aruba Networking Access Points	Aruba AP – 3xx/5xx	BLE support required
Aruba AP firmware	AOS 10.4 LSR / AOS 10.7 SSR	Refer to release notes for AP hardware support.
Aguardio Pipe Sensor	1.2.0-rc2	There are different types of firmware – if you are unsure which version your device has, contact Aguardio support at ***support@aguardio.com***

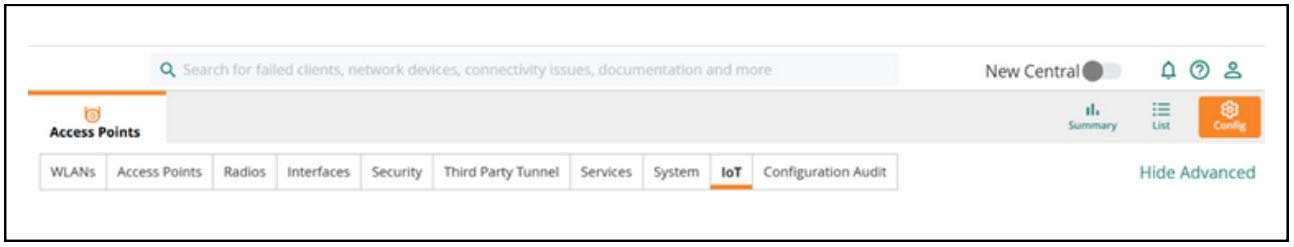
2. Settings and Configuration

The following step-by-step instruction contains the necessary configuration to set up Aguardio sensors with an HPE Aruba Networking Access Points

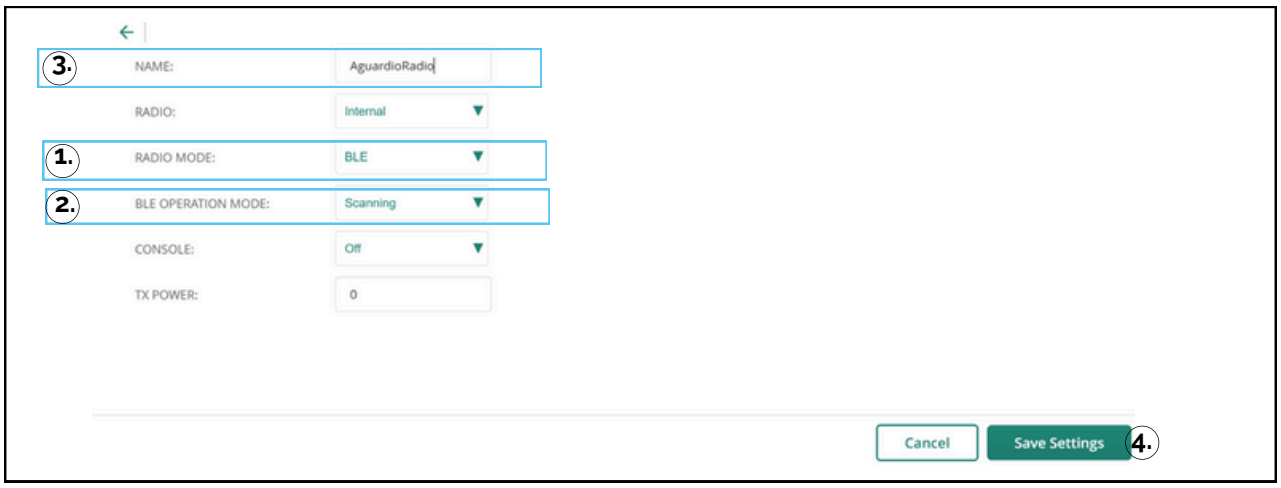
Radio Profile

2.1 In Aruba Central, select your preferred group to which your access point is assigned to.
Then select '***Devices***'.
If the device, site, or organization has not yet been set up, please check the Aruba guide, or contact Aruba support.

2.2 Select ***'Config'*** on the right - then go to the 'IoT' tab.

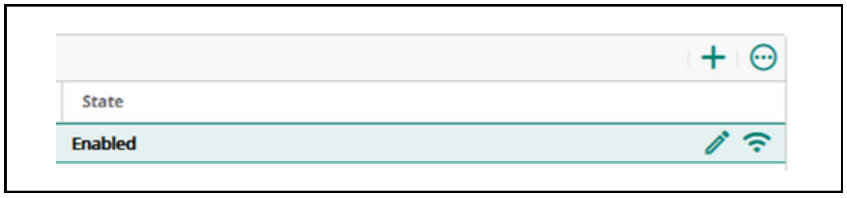


2.3 Create a new IoT Radio Profile using the '**+**' sign and **set the 'Radio Mode' to BLE (1)**.
Set 'BLE Operation Mode' to either **'Scanning'** or **'Both' (2)**, **name** your radio profile **(3)**,
click '**Save Settings**' (4).



2.4

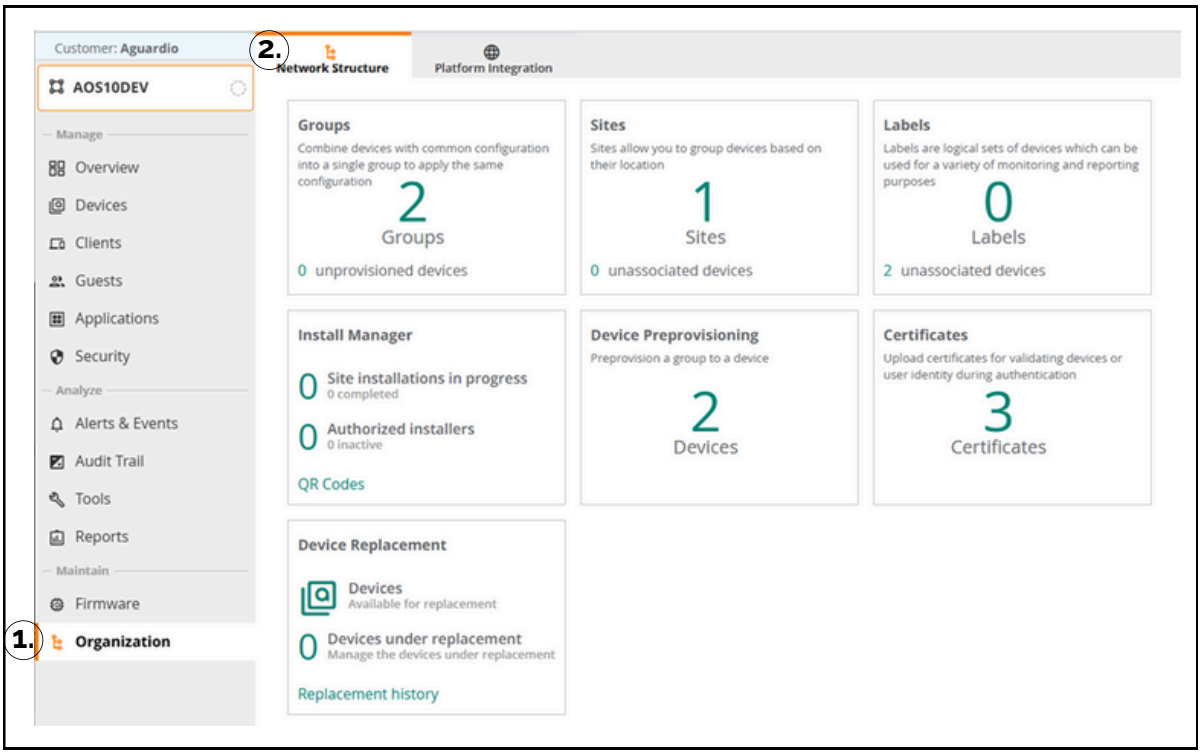
Enable the **radio** by hovering over the newly created profile, then click the signal button on the right side. Under '**State**' you should see '**Enabled**'.
If you would like to edit the radio profile, you may do so by clicking the pen button next to it.



2.5 Install Certificate

1 Navigate to ***'Organization'*** on the left-side menu,

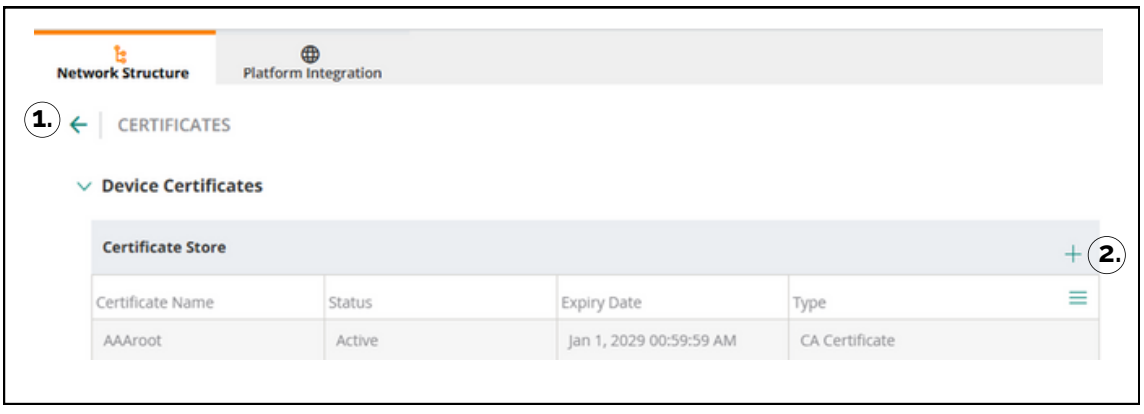
2. Select the '***Network Structure***' tab.



2.6 Install Certificate

1 Click the '***Certificates***' tile.

2. Add a new certificate by clicking the '+' sign next to 'Certificate Store'.

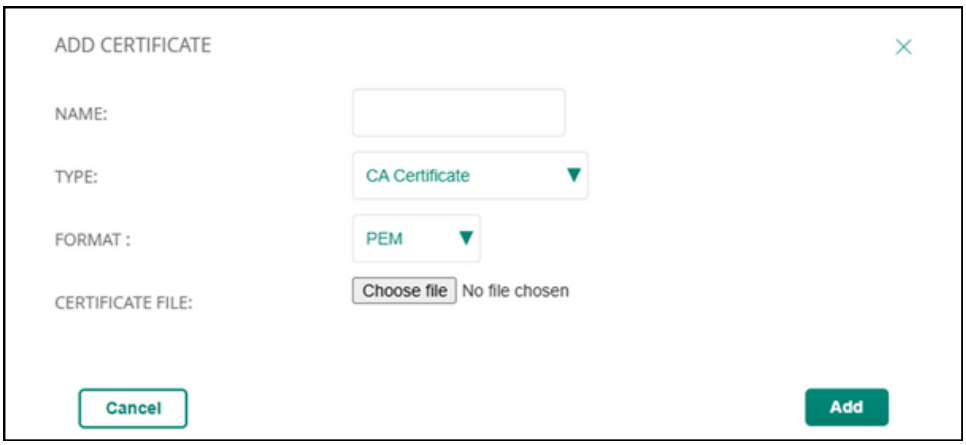


2.7 **Install Certificate**

Enter a name for the certificate, then select ***'CA Certificate***' as a Type from the drop-down list.
The Format should remain '**PEM**'. Aguardio uses a publicly signed certificate. You need to upload the necessary root certificate from Comodo CA limited. On the following page, download 'AAACertificateServices.crt':

https://crt.sh/?id=331986

You may find more information on the root certificate here:
https://www.sectigo.com/resource-library/sectigo-root-intermediate-certificate-files



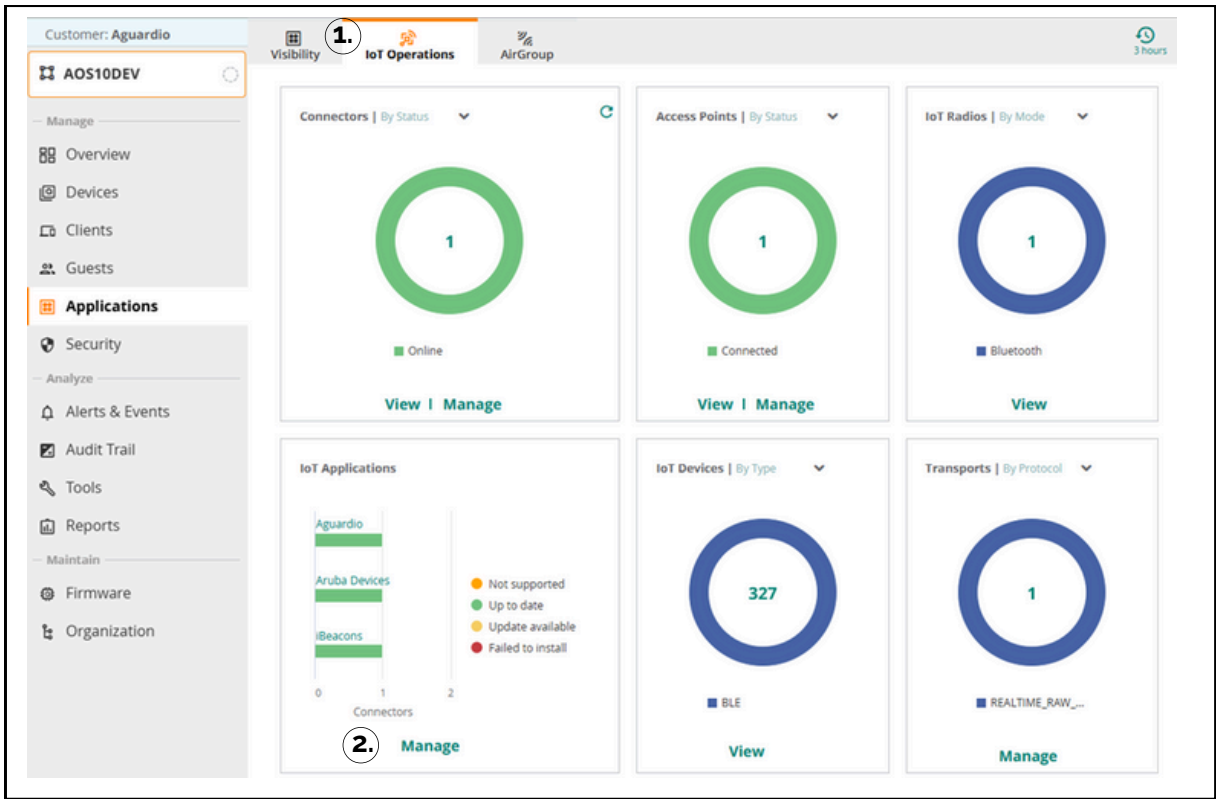
Trouble uploading the certificate?

Please send us a message marked ARUBA to ***support@aguardio.com***.

2.8 Installing Aguardio app

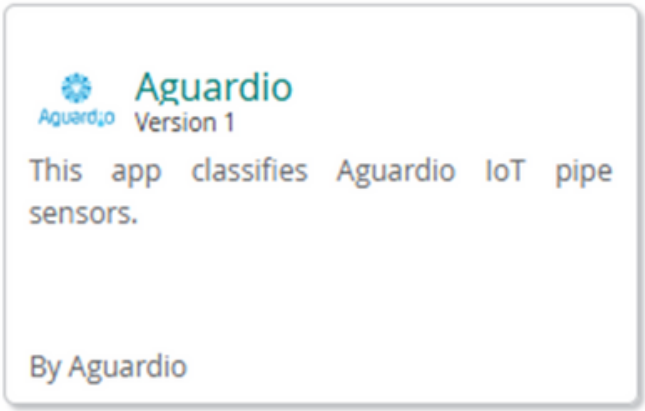
1. Navigate back to the ***'IoT Operations'*** dashboard under 'Applications'

2. On the bottom-left tile, 'IoT Applications', select '***Manage***'.

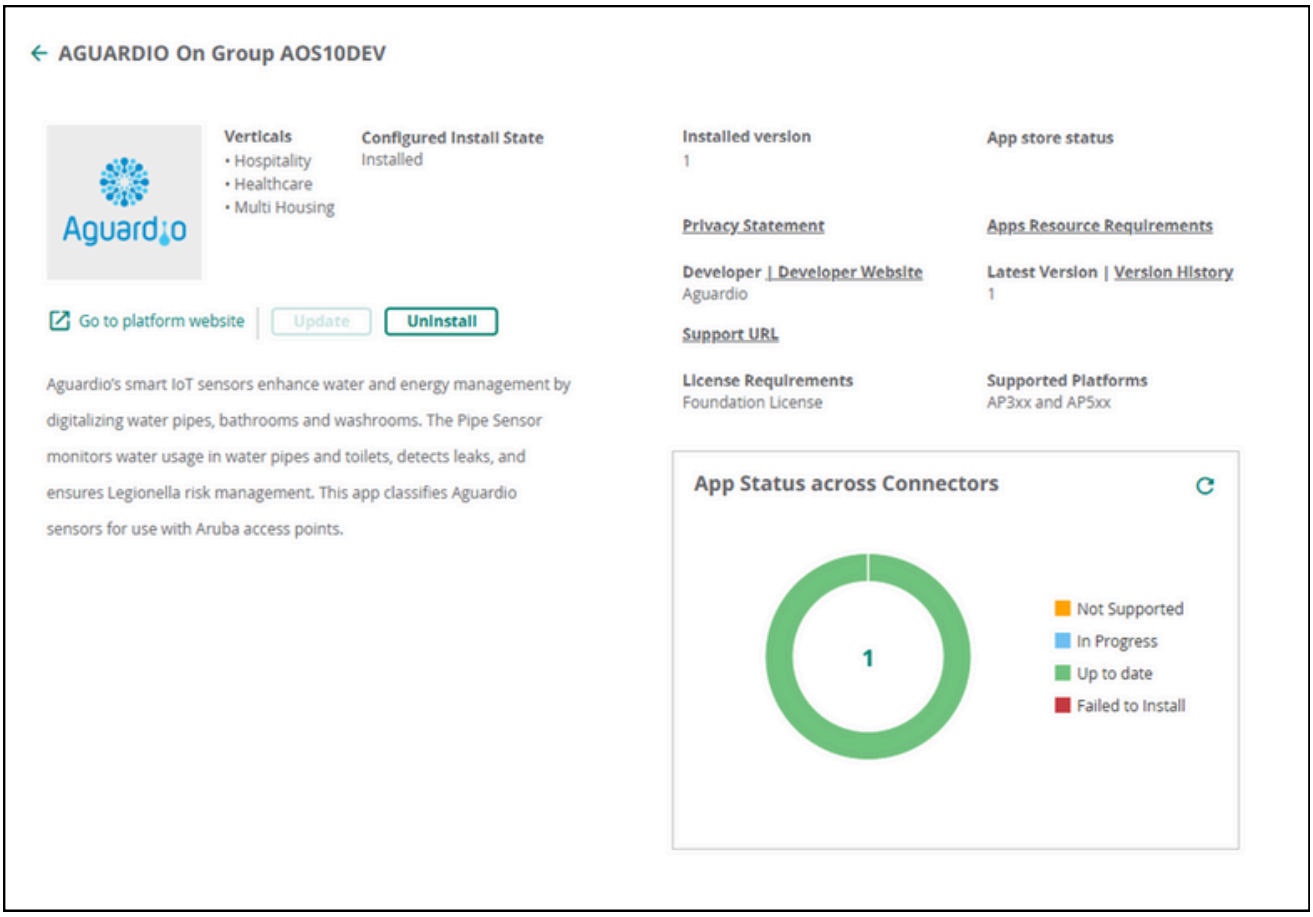


2.9 Installing Aguardio app

1. Browse for the ***Aguardio app*** from the available apps, then click on it.



2. Click '***Install***' on the application page, then refresh the status to confirm the successful installation.



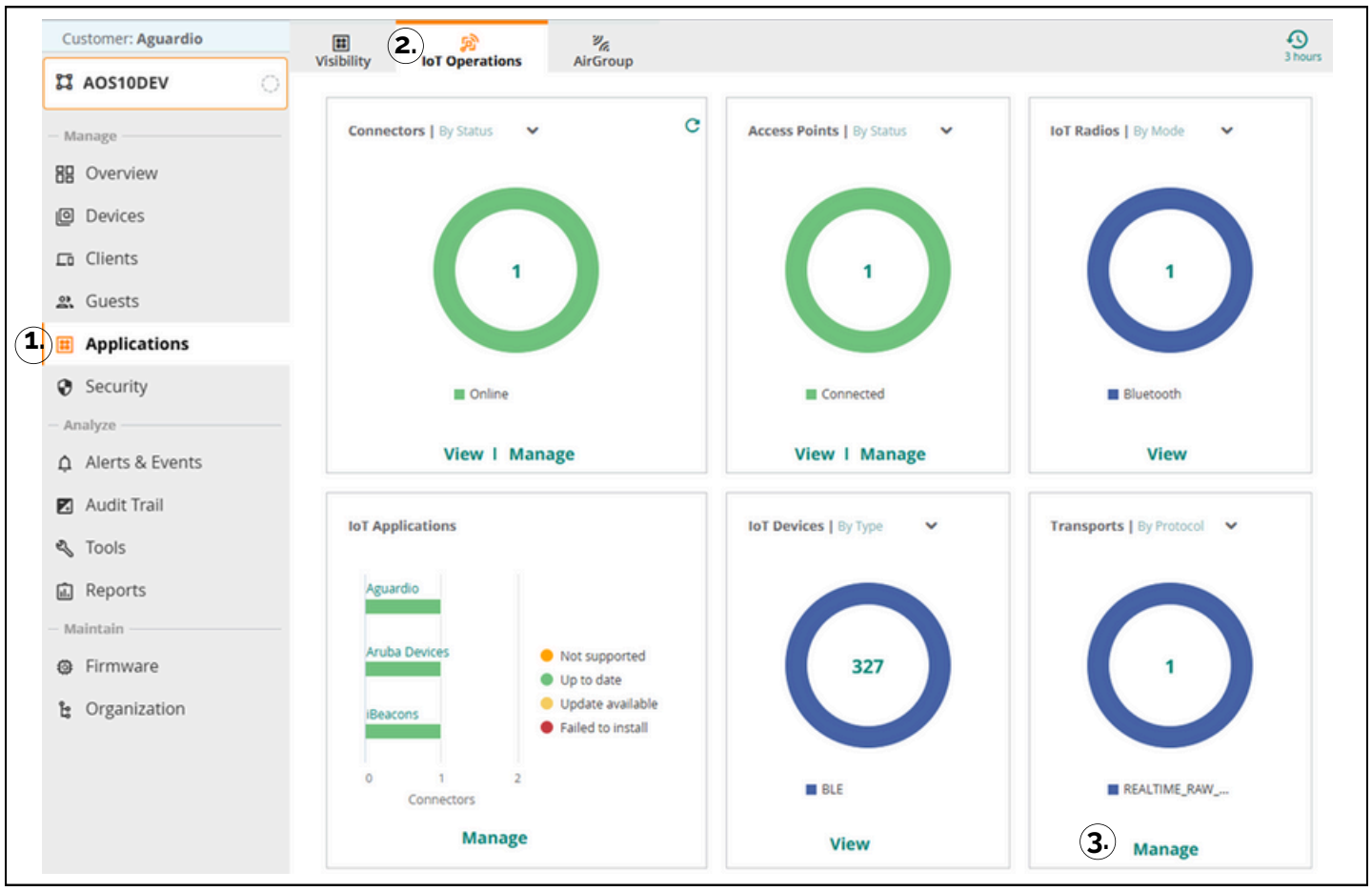
2.10 Transport Profile

1 Navigate to '**Applications**' on the left-side menu,

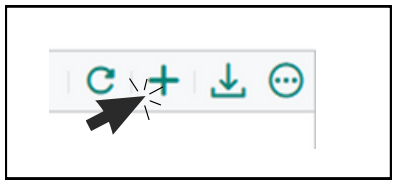
2. Select the '***IoT Operations***' tab.

You should see a dashboard with relevant information about your current IoT setup.

3. Click '**Manage**' on the '**Transports**' tile in the bottom right area of the dashboard,



4. Create a new Transport profile by clicking '+' on the right side.



2.11 Configure the Transport Profile

1. Enter a name for your Transport Profile – it is recommended to use a short, easy-to-remember name. ·Select the 'Data Frames' Stream Type.

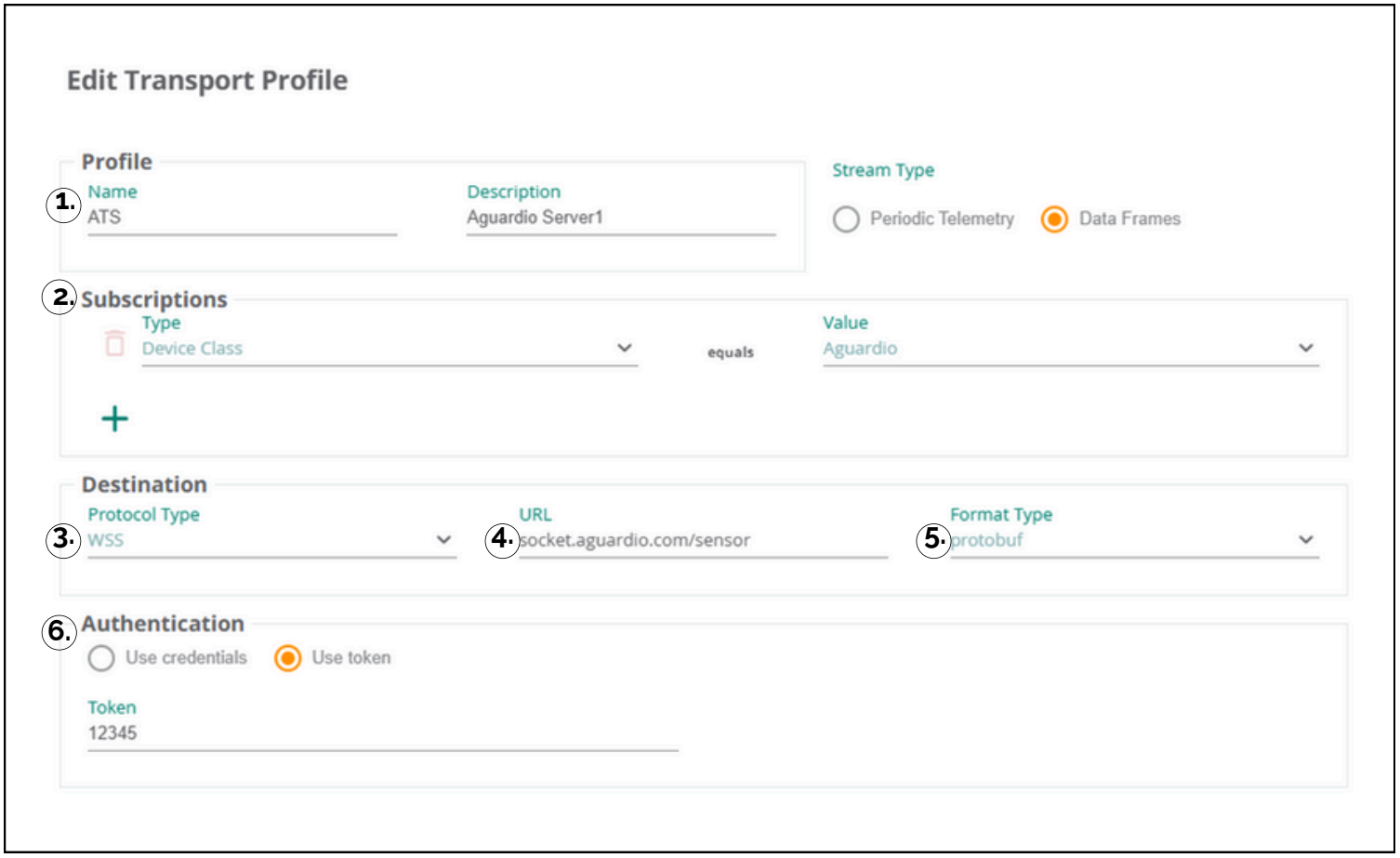
2. Under 'Subscriptions', select 'Device Class' as a Type, then select 'Aguardio' as a value from the drop-down menu.

3. Under 'Destination', set the Protocol Type to 'WSS'

4. Enter the following as a URL: socket.aguardio.com/sensor

5. Set the Format Type to 'protobuf'

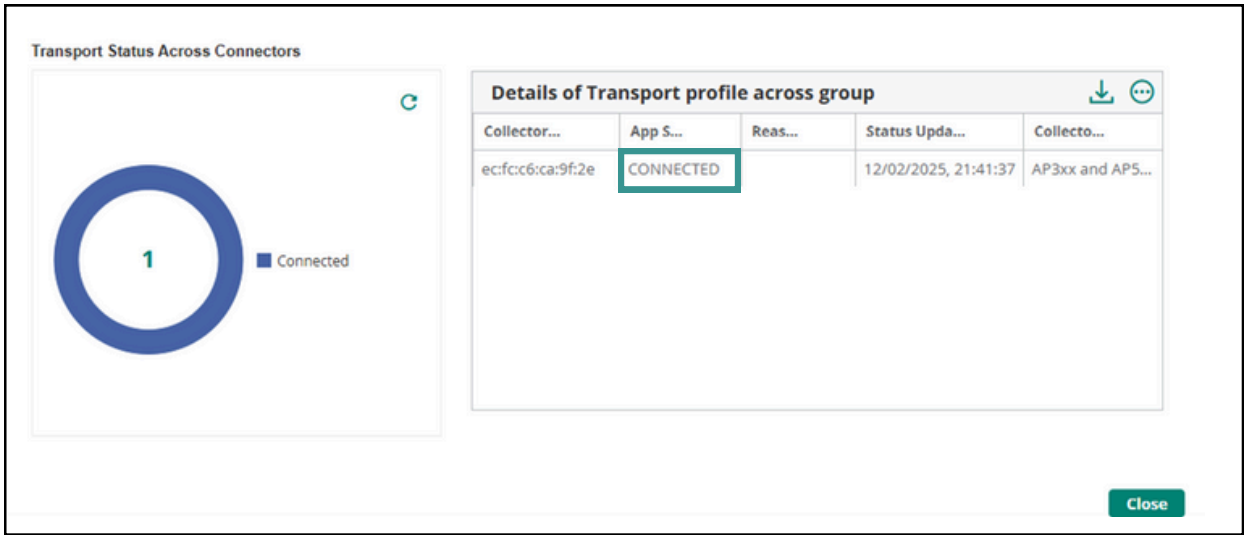
6. Under 'Authentication', select 'Use token', then enter your API key that you generated in the Aguardio Hub (***https://admin.aguardio.com/***) . If you have trouble accessing the Aguardio Hub, please send us a message at support@aguardio.com, or check out our Aguardio Hub guide at https://www.aguardio.com/downloads/



2.12 Transport Profile check

Ensure that the connection is working by clicking the circular symbol on your transport profile.

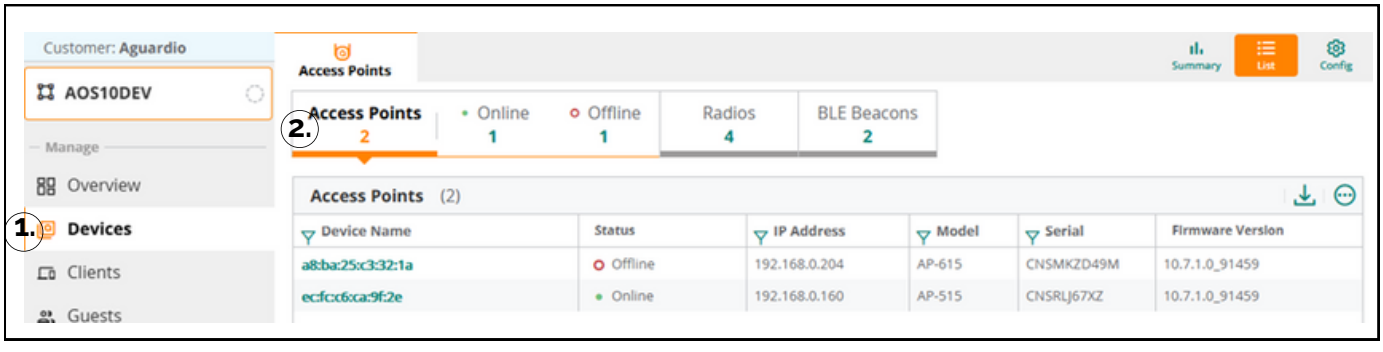
The 'App Status' column should read '**CONNECTED**' on your transport profile.



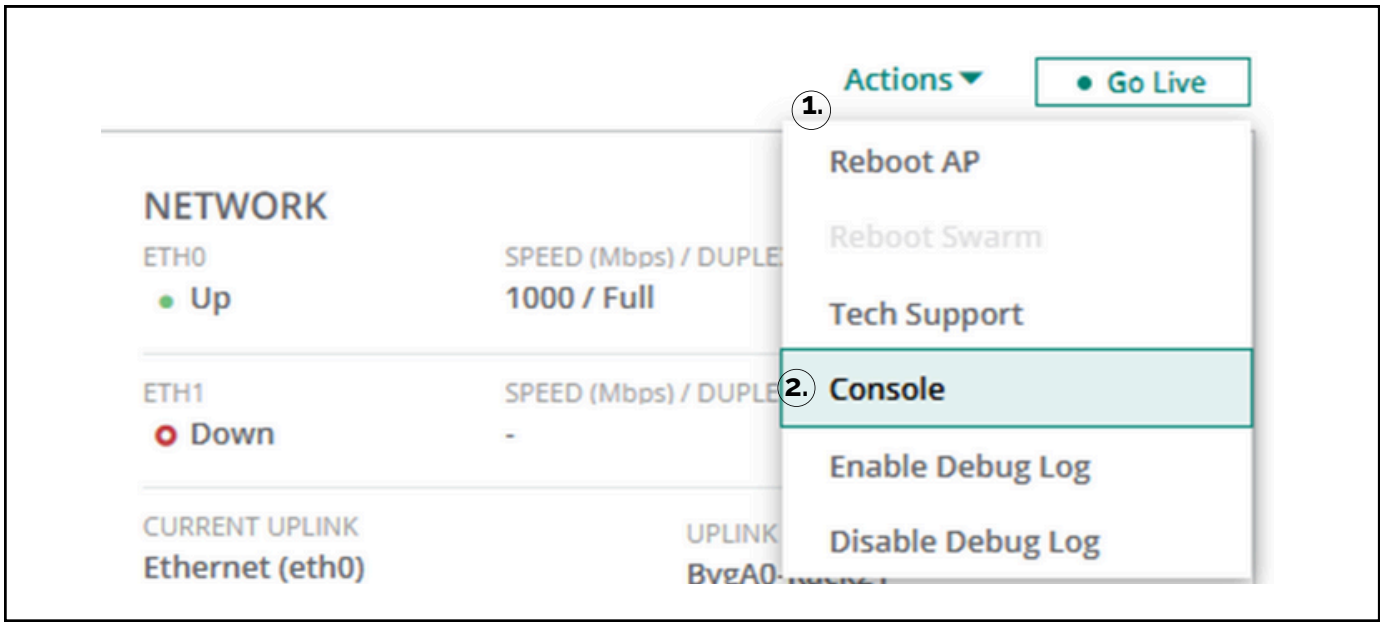
3. Connection, Verification and Troubleshooting

- The HPE Aruba Networking Access Point can be accessed with a console from the Aruba Central platform to perform troubleshooting.
- If you encounter any issues receiving data from the Aguardio sensors with your HPE Aruba Networking Access Point, please check the console commands to verify data, connectivity and app status in the console.
- Please note that the GUI of the Aruba Central may show outdated information.
- If you are unsure whether the status of the HPE Aruba Networking Access Point is up to date, please refer to the console to receive live information on the device.

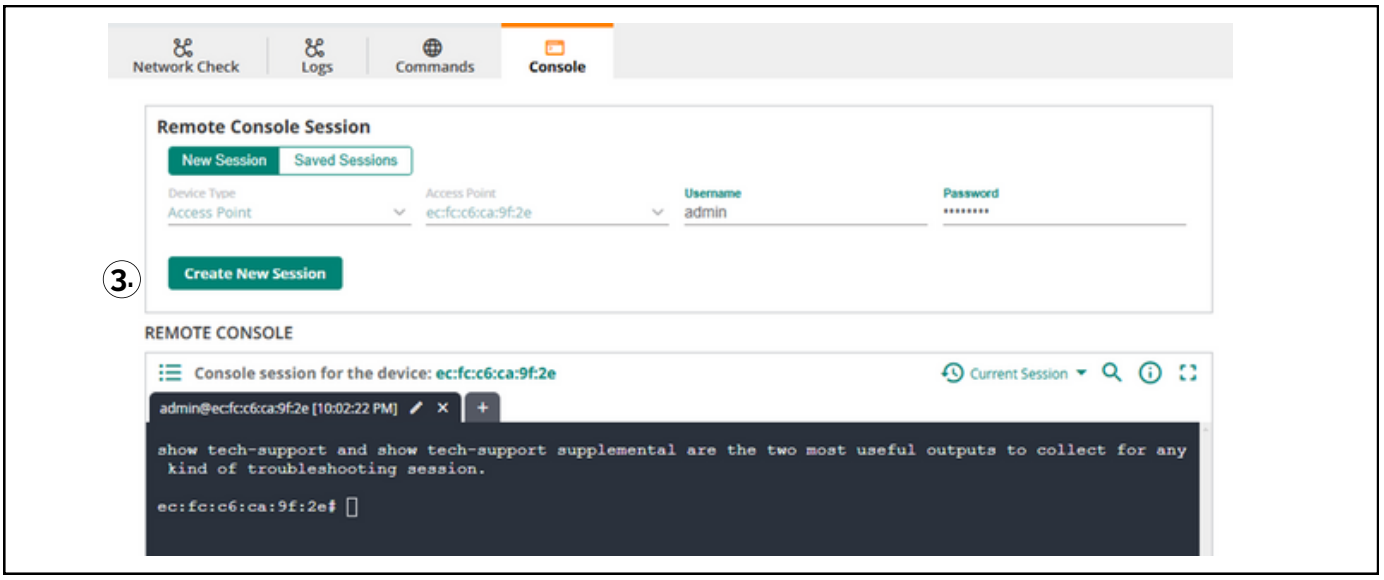
3.1 Select '***Devices***' on the left-side menu, then select the HPE Aruba Networking Access Points you would like to access by clicking its MAC address.



3.2 On the right, select '***Actions***', then '***Console***' from the drop-down menu.



3.3 Enter your HPE Aruba Networking Access Point's username and password, then click '***Create New Session***'



3.4 The following commands can help verify and confirm the status of your connection and the configuration of your HPE Aruba Networking Access Point:

Step verified	**Console Command**	**Notes**
Radio Profile	show iot radio-profile <profile_name>	To list all configured profiles, omit profile name.
Transport Profile	show ap debug aec-config transports <profile_name>	To list all transport profiles, omit profile name.
Certificate(s) Assignment	show ap debug aec-config certs	
Transport Profile Connection Status	show debug ble-relay report	
Transport Profile Connection Error log	show ap debug ble-relay ws-log <profile_name>	

3.5 The following additional console commands can be used (not a complete list):

Console Command	**Effect**
<command> ?	Lists the available sub-commands for the entered <command>
show ap debug ble-config	Shows a summary of radio and transport profile configuration
show ap debug ble-table all	Shows all Bluetooth devices scanned by the AP
show ap debug ble-table mac <macaddress>	Shows detailed information on the device specified by its MAC address
show ap debug ble-daemon	Shows the log for the connection
show ap debug ble-relay iot-profile	Shows detailed information on the transport profiles
show ap debug ble-relay report	Shows detailed report on the connection status
show ap debug aec disp-config-objs	Shows a list of apps that are currently running on the AP