MQTT Steaming Protocol

MQTT (Message Queue Telemetry Transport) is a lightweight data streaming standard often used in IoT applications. It is based on publish-subscribe networks that can transport messages from devices to a broker ("server"). Clients connect to a central broker and publish data on a specific topic. Clients can also subscribe to topics (including using wildcards to easily subscribe to sets of topics), and will receive any updates published to that topic. An MR access point (specific models) can support this protocol and work as a forwarder using its Bluetooth radio.

- MQTT is supported on Wi-Fi 5 wave 2 APs as well as Wi-Fi 6 APs and later. Access Points that do not support the feature will not forward any MQTT message. If your network has APs which support MQTT, you will be able to navigate to Wireless > IoT radio settings in the dashboard, and find the new tab "MQTT" right next to Bluetooth.
- MQTT is only supported on MR 28.X firmware and later.
- Cisco Meraki MR devices only support MQTT version 3.1.1

Using MQTT, MRs can send messages received (scanned) on Bluetooth/Wi-Fi environments to a broker where users can manage them.
MQTT protocol uses different fields that can be useful for the user. Cisco Meraki MRs forward the following attributes:

- RSSI
- UUID (iBeacon)
- Minor (iBeacon)
- Major (iBeacon)
- Client MAC addr
- AP MAC addr
- AP Serial Number
- Timestamp
- Radio
- Network ID
- Raw Payload

⚠️ Cisco Meraki will **not** handle the broker side. MRs will only forward messages to the broker's IP. In MQTT terms, the MR will publish all the beacons it scans to the broker.
Configuration

To configure the MQTT service on MR, go to Wireless > IoT radio settings

If this option is not available, then your network may have APs which do not support MQTT. Try moving your MQTT-compatible APs to their own network to ensure availability of this option.

MQTT telemetry streaming

<table>
<thead>
<tr>
<th>Wireless</th>
<th>MONITOR</th>
<th>CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insight</td>
<td>Access points</td>
<td>SSIDs</td>
</tr>
<tr>
<td></td>
<td>Air Marshal</td>
<td>Access control</td>
</tr>
<tr>
<td></td>
<td><strong>Location heatmap</strong></td>
<td>Firewall &amp; traffic shaping</td>
</tr>
<tr>
<td>Organization</td>
<td>Splash logins</td>
<td>Splash page</td>
</tr>
<tr>
<td></td>
<td>Login attempts</td>
<td>SSID availability</td>
</tr>
<tr>
<td></td>
<td>PCI report</td>
<td>IoT radio settings</td>
</tr>
<tr>
<td></td>
<td>Bluetooth clients</td>
<td>Port profiles</td>
</tr>
<tr>
<td></td>
<td>RF spectrum</td>
<td>Radio settings</td>
</tr>
<tr>
<td></td>
<td>Health</td>
<td></td>
</tr>
</tbody>
</table>

IoT Radio Settings

Bluetooth MQTT

MQTT telemetry streaming

Disabled Enabled

Select Enable on Stream Telemetry via Access Points in order to display all Settings to be configured.
Broker Configuration

The first step is to configure the broker where MQTT messages will be sent. Add the broker by selecting the option Add or edit MQTT Brokers and then selecting New MQTT broker.

You will see the following window pop up:
• **Broker Name**: An identifier for the user. It can be any word.

• **Host**: IP of the broker you are going to configure.

• **Port**: Port used by MQTT server, by default servers use TCP port 1883.

• **Username**: Optional depending on the configuration of the server.

• **Password**: Optional depending on the configuration of the server.

• **Security**: Can be None or TLS security. If TLS security is selected, a new option will show for you to upload the certificate to be used.

Once all the fields are configured, click **Save**.
MQTT General Fields

Now you can select the fields to be populated for the MQTT messages.

MQTT broker
Select a MQTT broker for APs to publish to.

Demo
DETAILS
Host 172.16.10.226
Port 1883
Security None

Message fields
Select fields to populate in MQTT messages.

☑ RSSI  ☑ Unselect All
☑ AP MAC address
☑ Client MAC address
☑ Timestamp
☑ Radio
☑ Network ID

MQTT topic
Empty topic will publish to broker using default topic structure.

e.g. mqtt/demo

MQTT QoS
Quality of Service(QoS) level of MQTT.

0 1 2

Publish frequency
Interval, in seconds, at which APs publish telemetry to the broker.

1 Seconds

Topic

By default, MR MQTT will publish to the following topic. However, this can be customized by adding a topic string.

The default MQTT topic is:
Meraki/v1/mr/<NetworkID>/<AP MAC>/<ble/wifi>/<Client MAC>/

For example the structure you should find with the default topic structure is the next:

![Topic Structure Diagram]

Publisher Options.

With MR MQTT solution, Meraki gives the options to choose which radio will be used to scan the network and forward the messages. The radios available are:

- Bluetooth
- Wifi

Each Radio will have its own options and at least one must be enabled in order to have a message feed to forward/publish to the broker.

⚠️ Depending on the number of clients and radios to be selected, MQTT messages can increase rapidly, be sure to add the proper Firewall rules and prepare your network for that traffic.

MQTT is lightweight but a large quantity of messages can be generated.
RSSI Publisher - Bluetooth

Bluetooth telemetry

Additional message fields
Select BLE-specific fields to populate in MQTT messages.
- Beacon type
- Raw payload
- Client UUID (iBeacon)
- Client Major value (iBeacon)
- Client Minor value (iBeacon)
- Signal power (iBeacon)

MAC address whitelist
MAC addresses of clients to publish telemetry to the broker for. Empty whitelist will publish telemetry for all clients.

UUID whitelist
UUIDs of iBeacon clients to publish telemetry to the broker for. Empty whitelist will publish telemetry for all clients.

Hysteresis

BLE Type Filter
BLE type of clients to publish telemetry to the broker for. "None" will publish telemetry for all clients.

- **Additional Message Fields** are options that can be added to the MQTT message on top of the general items that are already provided. Note that Bluetooth will only work with the iBeacon protocol for MQTT.
- **MAC Address Whitelist** allows users to only publish MQTT messages for clients with matching MAC addresses from the whitelist.
- **UUID Address Whitelist** is the same as the MAC Address Whitelist but for the UUID field. The MR will not forward any UUID that is not on the whitelist. If left blank, the MR will forward everything.
- **Hysteresis** enables an RSSI publisher to only publish messages with certain changes in RSSI value, reducing the traffic through the AP and broker.
- **BLE Type Filter** allows the user to choose the BLE beacon to be publish/forward.
  - None - Will forward all messages with no filter.
  - iBeacon - Will only forward iBeacons
- Eddystone - Will only forward Eddystone beacons.
- Unknown - Will forward all traffic that is not categorized as iBeacon or Eddystone.

⚠️ Make sure Bluetooth is enabled on Wireless > IoT radio settings. Scanning must be turned on.

**RSSI Publisher - Wi-Fi**

**WiFi telemetry**

**WiFi client type**

Client type, of which APs publish telemetry to the broker

- Visible
- Associated

**MAC address whitelist**

MAC addresses of clients to publish telemetry to the broker for. Empty whitelist will publish telemetry for all clients.


**Hysteresis**

- Disabled
- Enabled

- **WiFi client type**: Will only forward the traffic on wifi from Clients that are either Visible (every client that beacons) or Associated (only clients that are associated to the SSID broadcast by the AP).

- **MAC Address Whitelist** allows users to only publish MQTT messages for clients with matching MAC addresses from the whitelist. Wi-Fi (visible and associated) and BLE clients have their separate whitelists.

- **Hysteresis** enables the RSSI publisher to only publish messages with certain changes in RSSI value, reducing the traffic through the AP and broker.

Once all configurations are made, select **Save**.