Bluetooth Low Energy (BLE)

Meraki access points with an integrated Bluetooth Low Energy radio have the ability to transmit BLE Beacons, as well as to scan and locate BLE devices. Client devices like smartphones “hear” the BLE Beacon emitted by a Meraki AP, and an app on the smartphone can respond to a recognized Beacon. BLE scanning allows the Meraki AP to listen for and locate all Bluetooth Low Energy devices. The BLE scanner can hear other Beacons, BLE asset tags, and devices like fitness monitors that communicate using BLE data protocols. The Bluetooth Location API allows third party applications to provide asset tracking and analytics using battery-based bluetooth tags or wearables like fitness monitors.

Bluetooth clients

Detected devices will also be displayed in the Wireless > Monitor > Bluetooth clients page. The list of BLE clients can be viewed for several different observation time periods (two hours, one day, one week), and displays several useful pieces of information such as the AP that observed the device and, when available, the manufacturer of the device. The dashboard allows tagging the Bluetooth devices to identify individual or groups of devices.

Email alerts

Additional details about each Bluetooth device can be seen on the client details page. The name of the Bluetooth client can also be edited for easier tracking. Email alerts can be enabled to trigger when the device becomes visible by the access point and when the device is no longer visible.
Enable Bluetooth Scanning

Using the physical placement of the access points from the Map & Floorplan on the Dashboard, the Meraki cloud estimates the location of the client. The geo-location coordinates (latitude, longitude) and X,Y location data accuracy can vary based on a number of factors and should be considered a best effort estimate. AP placement, environmental conditions, and client device orientation can influence X,Y estimation; experimentation can help improve the accuracy of results or determine a maximum acceptable uncertainty for data points.

To enable BLE devices to be located, enable the BLE scanning radio on the access points. BLE Scanning is enabled in the Wireless > Bluetooth Settings page by selecting "On" in the Scanning section, as shown in Figure 3 below:

---

**BLE Scanning API**

**Bluetooth API Data Elements**

<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apMac</td>
<td>string</td>
<td>MAC address of the observing AP</td>
</tr>
<tr>
<td>Name</td>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>apTags</td>
<td>[string]</td>
<td>JSON array of all tags applied to the AP in dashboard</td>
</tr>
<tr>
<td>apFloors</td>
<td>[string]</td>
<td>JSON array of all floorplan names on which this AP appears</td>
</tr>
<tr>
<td>clientMac</td>
<td>string</td>
<td>Device MAC</td>
</tr>
<tr>
<td>seenTime</td>
<td>ISO 8601 date string</td>
<td>Observation time in UTC; example: &quot;1970-01-01T00:00:00Z&quot;</td>
</tr>
<tr>
<td>seenEpoch</td>
<td>integer</td>
<td>Observation time in seconds since the UNIX epoch</td>
</tr>
<tr>
<td>rssi</td>
<td>integer</td>
<td>Device RSSI as seen by AP</td>
</tr>
<tr>
<td>location</td>
<td>location</td>
<td>Device geolocation; null if location could not be determined</td>
</tr>
<tr>
<td>lat</td>
<td>decimal</td>
<td>Device latitude in degrees N of the equator</td>
</tr>
<tr>
<td>lng</td>
<td>decimal</td>
<td>Device longitude in degrees E of the prime meridian</td>
</tr>
<tr>
<td>unc</td>
<td>decimal</td>
<td>Uncertainty in meters</td>
</tr>
<tr>
<td>x</td>
<td>[decimal]</td>
<td>JSON array of x offsets (in meters) from lower-left corner of each floorplan</td>
</tr>
<tr>
<td>y</td>
<td>[decimal]</td>
<td>JSON array of y offsets (in meters) from lower-left corner of each floorplan</td>
</tr>
</tbody>
</table>

Enable the Scanning API with BLE Scanning, and the Location API will include both WiFi and Bluetooth devices seen by the access points in a single data feed. The event type **BluetoothDevicesSeen** is used to identify the observations from the Bluetooth radio. Below are the JSON formats used by the Location API for Bluetooth devices.

**HTTP POST body format**

```json
{
    "version":"2.0",
    "secret":<string>,
    "type":"BluetoothDevicesSeen",
    "data":<event-specific data>
}
```

**Bluetooth API Data Format**

```json
{
    "apMac": <string>,
    "apFloors": [<string>, ...],
    "apTags": [<string, ...],
    "observations": [
        {
            "location": {
                "lat": <decimal>,
                "lng": <decimal>,
                "unc": <decimal>,
                "x": [<decimal>, ...],
```
Enable Scanning API

Privacy for Scanning API

Bluetooth Beaconing

All available Cisco Meraki WiFi access points (except for MR20 and MR70) have a built-in BLE iBeacon Advertising mode. You can enable the beacon right from the Cloud-hosted dashboard and configure the UUID, Major, and Minor. Meraki’s BLE enabled access points enable customers to begin developing practical applications for BLE devices. For example, you can use the BLE beacon advertising in a mobile app to trigger notifications or determine the position of the smartphone for wayfinding. These can be broadly categorized into ‘push’ applications, where the AP informs an aware device that it is in a certain location, or ‘pull’ applications, where the AP listens for beacons and uses this information to assist with asset tracking and control through the dashboard.

Configuring Beacons

Beacons are periodic signals emitted using Bluetooth Low Energy radio technology and conforming to a specific data packet format. The data packet looks like this:

<table>
<thead>
<tr>
<th>Field</th>
<th>Access Address</th>
<th>Header</th>
<th>MAC Address</th>
<th>Beacon prefix</th>
<th>UUID</th>
<th>Major</th>
<th>Minor</th>
<th>TX Power</th>
<th>CRC</th>
</tr>
</thead>
</table>

The Preamble, Access Address, Header, MAC Address, and CRC will be set as part of the BLE radio’s frame construction. The TX Power is a calibrated indicator of the RSSI of the transmitted measured at a 1m distance; this can be used for rough estimation of proximity to the device emitting the Beacons.

UUID, Major, and Minor are fields defined by the Beacon network administrator. Typically, an organization will define a unique identifier for their habitual usage: the UUID. All Beacons deployed throughout their locations would have the same UUID.

To differentiate Beacons at different offices or store locations, and Beacons within different areas of those locations, the Major and Minor fields are used. For example, a chain restaurant might decide that all restaurants within a city will share a Major, and each restaurant within that city will have a different Minor.

Meraki APs with an integrated Bluetooth Low Energy radio can emit Beacons with following technical specifications:

- Beacon interval: 100 ms (best effort)
- Transmit power: 0 dBm
Beacon mode can be enabled under **Wireless > Configure > Bluetooth Settings** by selecting "On" beside **Advertising** in the **Beaconing** section, as shown in Figure 1 below:

**Beaconing**

Use APs as location markers. For more information, see our [documentation](#).

**Advertising**

*On* | *Off*

*Figure 4: Enabling BLE Beacon advertising*

Once advertising is enabled, the UUID, Major, and Minor fields of the Beacon frame can be set. The Major/Minor values can either be set automatically and uniquely assigned on a per-AP basis for the network, or can be assigned globally for all APs in the network. When advertising is enabled, **Unique** mode will be the default setting.

**Unique** mode will automatically assign the same major value and unique minor values to each AP in the network. If **Unique** mode is configured on a parent template network, then the networks bound to that template will assign unique major values per network, and unique minor values per AP within those networks.

Saving these settings will activate the BLE Beacon on the Meraki AP’s integrated Bluetooth Low Energy radio.

**Beaconing**

Use APs as location markers. For more information, see our [documentation](#).

**Advertising**

*On* | *Off*

**UUID**

*e.g. 8c7067da-3143-f3a6-ba94-0b0e5706b8da*

The UUID is typically used to identify your organization. You can use templates to ensure your networks have the same UUID set.

*Generate new UUID*

**Major/Minor Assignment**

*Unique* | *Non-unique*

Dashboard will automatically assign unique beacon identifiers to each AP. APs in the same network will advertise the same Major Number and distinct Minor Numbers. These identifiers won’t change once set, even if you temporarily disable beaconing.

A list of Major Numbers and Minor Numbers will appear here once your beaconing settings are saved.

*Figure 5: Setting the BLE Beacon UUID/Major/Minor*
After the unique or non-unique values have been configured, you can view the assigned values from the **Wireless > Bluetooth settings**, as shown in the above Figures 6 and 7. Additionally, these values can be retrieved via the Dashboard API as shown below:

```
curl -L -H 'X-Cisco-Meraki-API-Key: <key>' -X GET -H 'Content-Type: application/json' 'https://dashboard.meraki.com/api/v0//orkId]/devices'
```
Figure 8: API response after querying the Dashboard API to list the devices in a network

```json
[
  {
    "name": "My AP",
    "lat": 37.4180951010362,
    "lng": -122.098531723022,
    "serial": "Q2XX-XXXX-XXXX",
    "model": "MR34",
    "address": "1600 Pennsylvania Ave",
    "lanIp": "1.2.3.4",
    "tags": "recently-added",
    "networkId": "N_1234",
    "beaconIdParams": {
      "uuid": "00000000-0000-0000-0000-000000000000",
      "major": 5,
      "minor": 3
    }
  }
]
```

Note: BLE uses FHSS, hence in order to capture all BLE beacons you may require an industrial 2.4GHz wide band sniffer tuned for BLE.