Safectory Track – Configuration Guide for Extreme Networks Access Points

safectory GmbH

1 Preamble **2**
1.1 Copyright . . . 2
1.2 Revision History . . . 2
1.3 Terms of Use . . . 2
1.4 Warranty . . . 2

2 Introduction **3**
2.1 Certified Product and Software Summary . . . 3
2.2 Configuring Clock/NTP Services . . . 3

3 IoT Telemetry Setup for Track Service (Non-Controller Variant) **4**
3.1 Configure Track Backend for TCP Packets . . . 4
3.2 Configure BLE Service in Network Policy . . . 4
3.3 Optional per-device BLE Service override . . . 5

4 IoT Telemetry Setup for Track Service (Controller Variant) **6**
4.1 Configure Track Backend for UDP Packets . . . 6
4.2 Configure IoT Profile . . . 7

1 Preamble

This guide describes how to integrate Extreme Networks access points and cloud or controller-based deployments with Safectory Track for BLE telemetry and beacon data transmission. It covers IoT profile, network, access point, controller, and backend configuration for the supported Extreme Networks variants.

1.1 Copyright

© Safectory GmbH - any unauthorized use without written permission prohibited.

1.2 Revision History

Version	Date	Description
0.1	01/2025	Initial version
0.2	03/2025	ExtremeCloud IQ non-controller configuration
0.3	04/2026	Revised ExtremeCloud IQ Pilot section

1.3 Terms of Use

Subject to technical modification without notice.

Errors and omissions excepted.

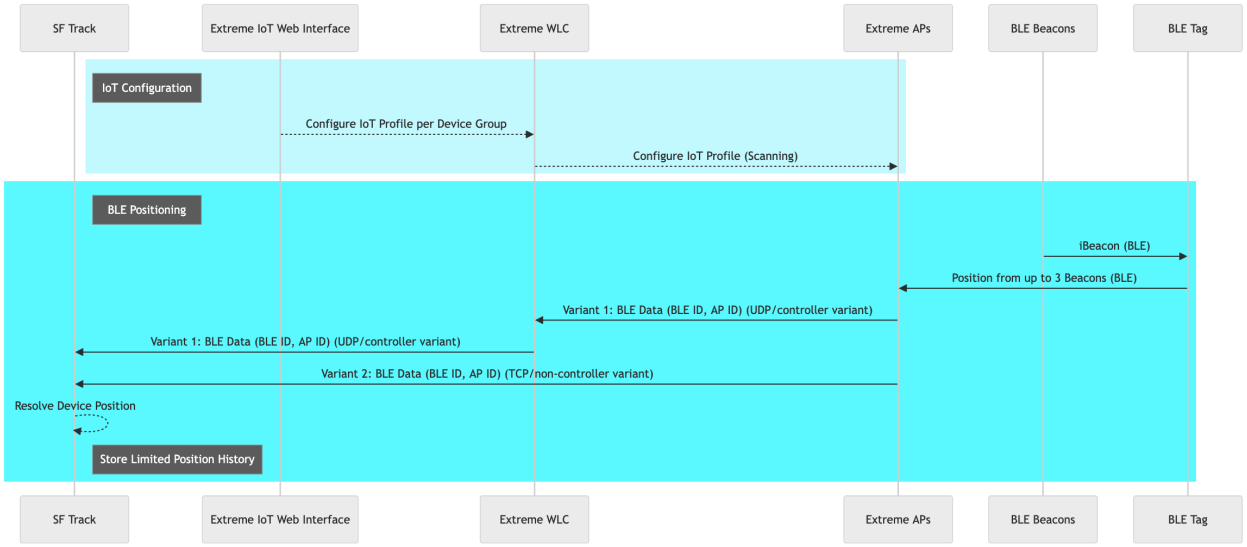
For further information regarding legal and proprietary statements, please go to our GENERAL TERMS AND CONDITIONS at https://safectory.com/gtc?lang=en.

1.4 Warranty

The Product Warranty and Software License and Warranty and other information are available in our GENERAL TERMS AND CONDITIONS at https://safectory.com/gtc?lang=en.

2 Introduction

To set up an IoT telemetry profile for Extreme Networks access points to be used with safectory products (asset tags, beacons, mobile SDK, Track backend), use the following manual. The access points will be configured to forward data created between tags and beacons to the server backend, a service called “safectory Track”. Overview diagram:



Note:

- Only one scanning or one beaconing profile can be active at once; thus, simultaneous scanning and beaconing is not possible.
- This guide assumes that the access points to be used already have an established setup of sites and device groups.
- As communication between the WLC and the backend occurs via unencrypted UDP messages, administrators are expected to implement adequate security measures to safeguard this traffic from unauthorized third parties.

2.1 Certified Product and Software Summary

- Certified products
  - all BLE-enabled access points (e.g., AP305C-WR, AP3000)
- Certified software
  - **Controller variant (ExtremeCloud IQ Controller)**:
    - Extreme Networks software versions approved (WLC): ExtremeCloud IQ Controller 10.09.01.0037
    - Extreme Networks software versions approved (AP): 10.9.1.0-038R
    - ExtremeCloud IQ Controller needs to support IoT profile setting **Generic BLE Scan**
  - **Non-controller variant (ExtremeCloud IQ Pilot)**:
    - ExtremeCloud IQ Pilot: build version 25.6.4-4
    - XIQ driver version: 10.8.5.0
  - SF backend versions approved: 1.27.+

2.2 Configuring Clock/NTP Services

Time synchronization is an essential part of managing beacons and tracking asset in your network, so make sure that all the nodes are synchronized with the same reference server and time.

3 IoT Telemetry Setup for Track Service (Non-Controller Variant)

This variant may apply if you are using ExtremeIQ Cloud (Pilot) and are not using a controller. In this case, a **BLE Service** can be configured that only allows to send HTTP (TCP) packets to a specific URL.

3.1 Configure Track Backend for TCP Packets

The ExtremeCloud IQ-managed APs will send data via HTTP (TCP) directly to the backend. The port can be freely chosen within the regular port range. The default port configured in the backend is `6979`.

- Ensure no **firewall rule** is blocking the TCP port
- Enable the Extreme Networks **backend module** and configure your desired **TCP port** in the backend configuration (`custom.xml`):

```
<entry key="gateway.extremeNetworks.enable">true</entry>
<entry key="gateway.extremeNetworks.tcp.port">6979</entry>
<entry key="gateway.extremeNetworks.tcp.endpoint">extreme</entry> <!-- With
↪  http://track.safectory.com as web.url, the default endpoint would be
↪  http://track.safectory.com/extreme -->
```

- Ensure a **Track user** exists in a **group with appropriate permissions** for device/beacon writes to the desired tags and beacons (`credentials.xml`); set this user's email address with the following backend config option:

```
<entry key="gateway.extremeNetworks.trackUserEmail">## TRACKUI_USER ##</entry>
```

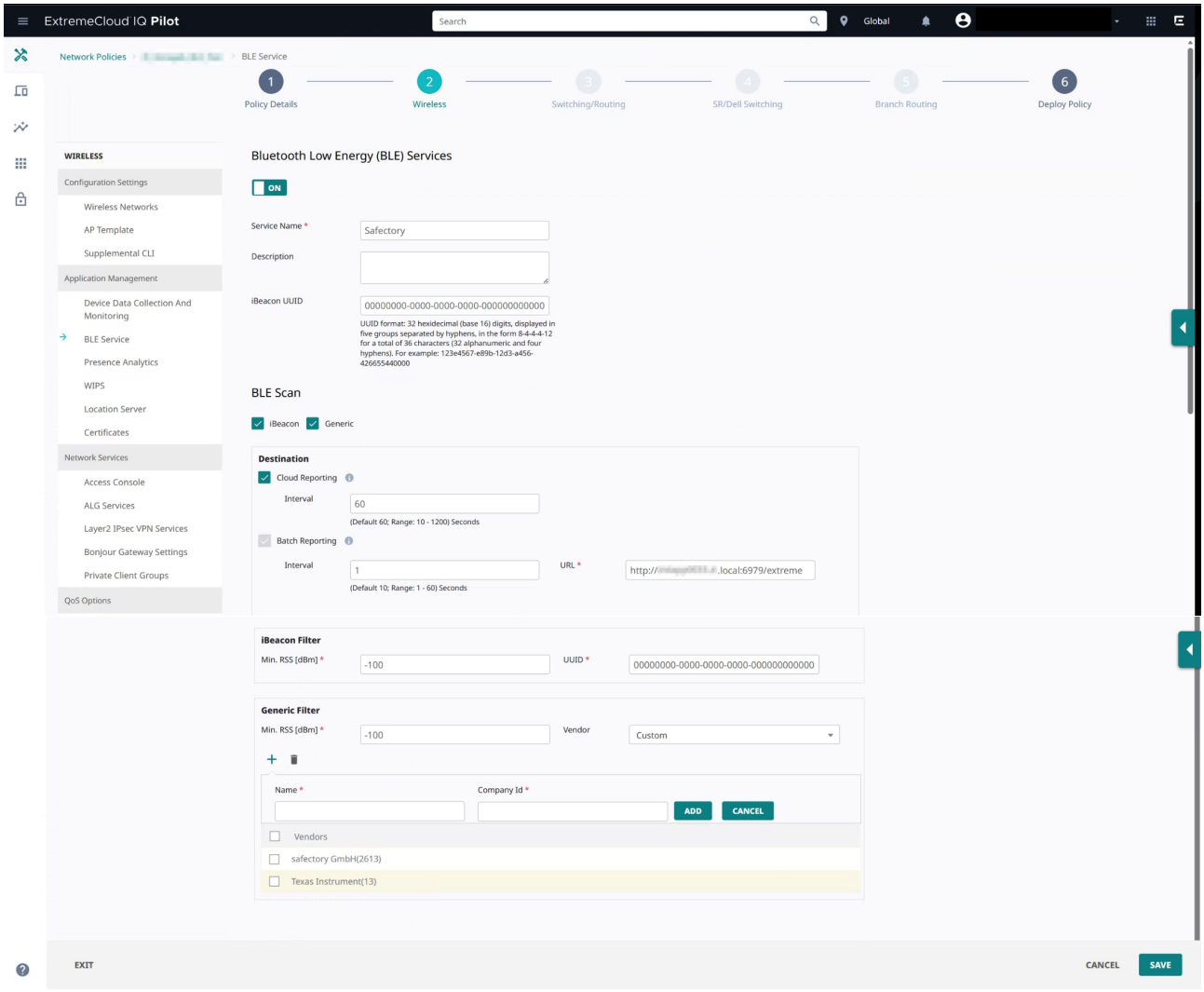
3.2 Configure BLE Service in Network Policy

First, define the BLE service profile in the Network Policy. This controls which BLE frames are scanned and how they are reported to the Track backend.

- Navigate to **Configure** → **Network Policies** → select the relevant policy → **Wireless** → **Application Management** → **BLE Service**
  - Toggle **BLE Service** to **ON**
  - Enter a **Service Name**
  - (Optional) Enter an **iBeacon UUID** if you also want to use the APs as iBeacon transmitters
- In section **BLE Scan**
  - Enable **iBeacon**
  - Enable **Generic**
- In section **Destination**
  - Enable **Cloud Reporting**
    - **Interval:** `60`
  - Enable **Batch Reporting**
    - **Interval:** `1`
    - **URL:** `http://<TOP_ADDRESS>:6979/extreme` (e.g., `http://top.safectory.de:6979/extreme`)
    - Note: Please make sure the port specified in the URL matches with the port specified in the Track backend config (cf. Configure Track Backend for TCP Packets)
  - Enable **Remove Duplicates** (switch = **ON**)
- In section **iBeacon Filter**:
  - **Min. RSS [dBm]**: `-100`
  - **UUID**: tags/beacons of one ToP instance usually share the same UUID, which can be entered here. For initial bring-up, you can leave this field empty (or use a less restrictive setting) to verify that data is flowing; once setup is confirmed working, you can narrow the filter to the specific UUID of your ToP instance.
- In section **Generic Filter**:
  - **Min. RSS [dBm]**: `-100`
  - **Vendor**: `Custom`
  - Add the following vendor-company-id pairs:

- Pair 1:
  - **Name**: `safectory GmbH`
  - **Company Id**: `2613`
- Pair 2:
  - **Name**: `Texas Instruments Inc.`
  - **Company Id**: `13`
- Pair 3:
  - **Name**: `iBeacons`
  - **Company Id**: `76`

Example BLE service configuration in Network Policy:



3.3 Optional per-device BLE Service override

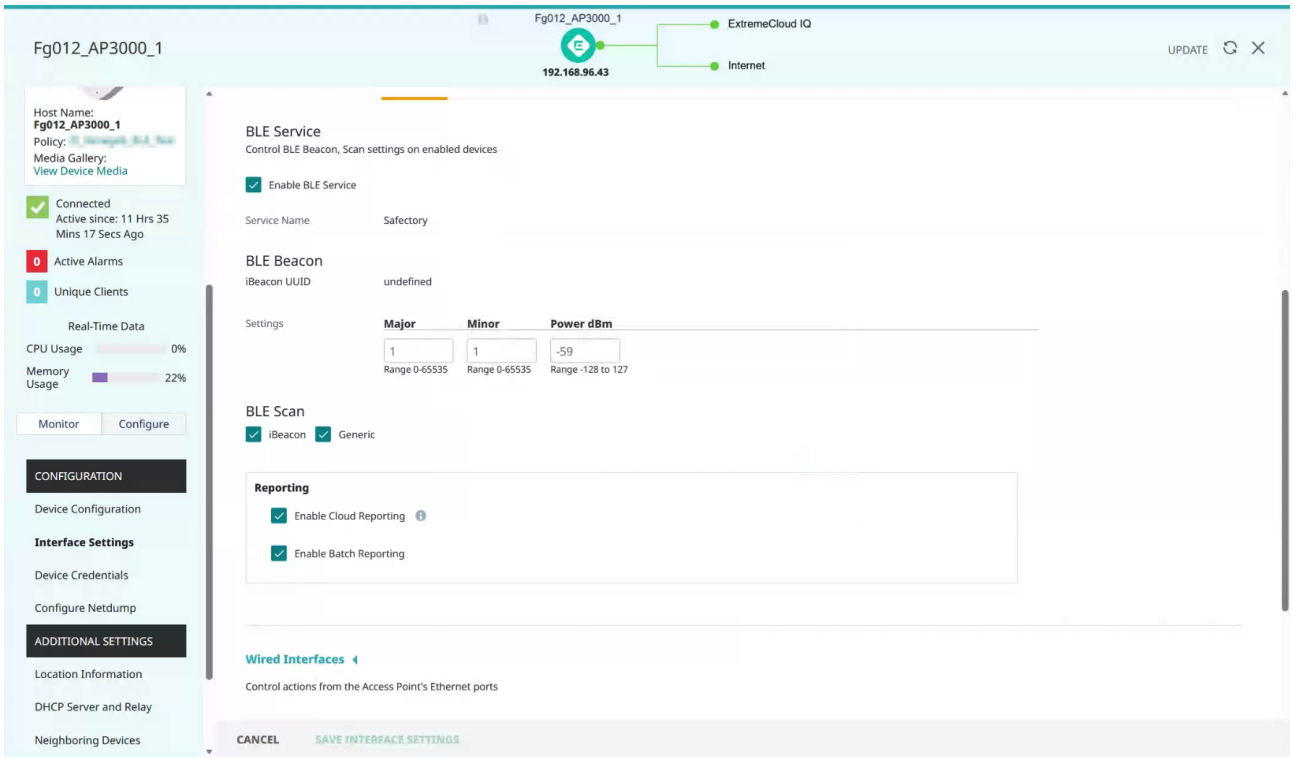
After defining the BLE service in the Network Policy and applying that policy to your BLE-capable access points, you can optionally review or override BLE settings per device (AP).

- Navigate to **Manage → Devices**, select the relevant BLE-capable access point, and open its configuration.
- Go to the **BLE Service** section:
  - Enable **BLE Service** (checkbox) if it is not already enabled.
  - Select the BLE service profile that was created in the Network Policy.
- Optionally, you can configure the **BLE Beacon** section (iBeacon UUID, Major, Minor, Power [dBm]) if you want the AP to act as an iBeacon transmitter. This is not required for the Track BLE scanning setup.
- The **BLE Scan** and **Reporting** options in the device view mirror the Network Policy BLE service settings. In typical Track setups, you keep them aligned with the Network Policy and only change them per device

for troubleshooting or exceptional cases.

- The AP device MAC address displayed in the ExtremeCloud IQ Pilot GUI for this BLE service is the **management MAC address** of the AP; you will see this MAC address in the Track backend when data is received.

Example per-device BLE service override configuration:



4 IoT Telemetry Setup for Track Service (Controller Variant)

This variant may apply if you are using ExtremeIQ Cloud Controller. In this case, an IoT profile can be configured that only allows to send UDP packets to a specific IP address.

4.1 Configure Track Backend for UDP Packets

The Extreme Networks WLC will send data via UDP to the backend. The port can be freely chosen within the regular port range. The default port configured in the backend is `6978`.

- Ensure no **firewall rule** is blocking the UDP port
- Enable the Extreme Networks **backend module** and configure your desired **UDP port** in the backend configuration (`custom.xml`):

```
<entry key="gateway.extremeNetworks.enable">true</entry>
<entry key="gateway.extremeNetworks.udp.port">6978</entry>
```

- Ensure a **Track user** exists in a **group with appropriate permissions** for device/beacon writes to the desired tags and beacons (`credentials.xml`); set this user's email address with the following backend config option:

```
<entry key="gateway.extremeNetworks.trackUserEmail">## TRACKUI_USER ##</entry>
```

4.2 Configure IoT Profile

To send BLE data received by the Extreme Networks AP to the Track server, you need to configure an IoT profile with the “Generic Scan” application (also see official documentation).

For the configuration of the IoT profile, it is mandatory to use the IP address of the Track instance. In the example below, we are using `172.27.0.122`, please adjust accordingly.

An IoT profile for scanning can be configured **per device group** as follows via WLC frontend:

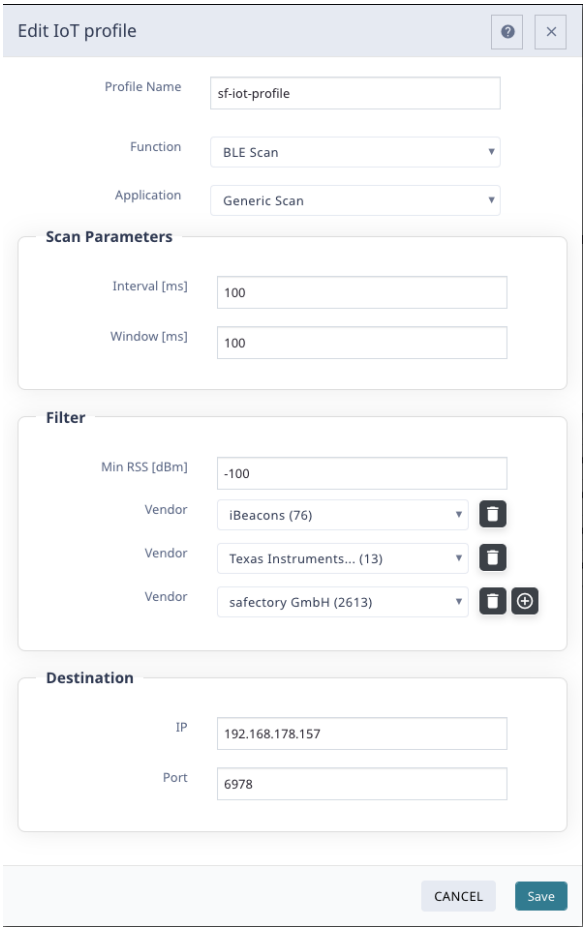
- In the frontend, navigate as follows:
  - Go to **Sites**
  - Select specific site
  - Configure site (gear symbol at the top)
  - Select specific device group, which should open the **Edit Device Group” dialog
- Either edit the default **Profile** (e.g., named `AP305C-default`) or create a new one (**Plus** button), then hit the **Edit** button
- Switch to tab **IOT** and create a new **IoT Profile** (**Plus** button)
- Fill following settings
  - **Profile Name**: can be freely chosen
  - **Function**: `BLE Scan`
  - **Application**: `Generic Scan`
  - **Scan Parameters**:
    - **Interval [ms]**: 100
    - **Window [ms]**: 100
  - **Min RSS [dBm]**: -100
  - **Vendor**:
    - Choose **Custom** and enter:
      - **Name**: `safectory GmbH`
      - **Company Id**: `2613`
    - Hit **Plus** button to get a second name-id pair, and enter:
      - **Name**: `Texas Instruments Inc.`
      - **Company Id**: `13`
    - Hit **Plus** button to get a third name-id pair, and enter:
      - **Name**: `iBeacons`
      - **Company Id**: `76`
  - **Destination**:
    - **IP**: enter Track instance’s IP address
    - **Port**: enter specified port in Track config (cf. Configure Track Backend for UDP Packets)
  - Hit **Save** button
- Hit **Save** button in **Edit Profile** dialog

Example configuration:

Alternatively, if you prefer to configure via CLI, then the sections **`iot`**, **`site`**, and **`profile`** are of particular interest. A **`site`** is associated with device groups, which contain the access points. The device groups are associated with one AP-specific **`profile`**. Each AP-specific profile is associated with one **`iot`** profile.

The following example CLI outputs shall just give an idea (for more details, please refer to the official CLI documentation by checking the output of the `help` command):

- **`iot`** section showing the settings of our IoT profile:




```
XIQC.extremenetworks.com# iot
XIQC.extremenetworks.com:iot# show

iot name                  iot ID

sf-iot-profile            1
XIQC.extremenetworks.com:iot# sf-iot-profile show
iot Name: sf-iot-profile
iot UUID: f24bbd75-00bd-45e1-9250-f1b34af91917
IoT Application: generic-scan
...
IoT scan_dest_port: 6978
IoT scan_interval: 100
IoT scan_min_rss: -100
IoT scan_window: 100
IoT scan_src_port: 0
iot ibeacon_uuid: 00000000-0000-0000-0000-000000000000
iot scan_dest_ip: 192.168.178.157
iot scan_src_ip: 0.0.0.0
iot eddystone_url:
IoT measured_rssi: 0
...
Company Name  Company Id:
Texas Instruments   13
iBeacons    76
safectory GmbH  2613
```

- **`site`** section showing that site **`sf`** is associated with device group **`sf-device-group`**, which in turn is

associated with **sf-custom-ap305c-profile**:

```
XIQC.extremenetworks.com# site
XIQC.extremenetworks.com:site:sf#
XIQC.extremenetworks.com:site:sf#device-group
XIQC.extremenetworks.com:site:sf:device-group# show
sf-device-group
```

```
XIQC.extremenetworks.com:site:sf:device-group:sf-device-group# profile-uuid
XIQC.extremenetworks.com:site:sf:device-group:sf-device-group# show
Device Group Name: sf
id: 1
device_group_uuid: 525f7fe2-3297-4684-b50c-873c54e88297
profile id: 30
profile_name: sf-custom-ap305c-profile
profile_uuid: 790c8efe-e119-42c8-a1e5-37fb73c5560b
smart rf id: 1
smartrf_name: Default Smart RF
smartrf_uuid: bd9d7042-f0c7-11e7-8c3f-9a214cf093ae
apsn: "03052104121404  "
```

- **profile** section showing that above **sf-custom-ap305c-profile** is associated with the IoT profile from above with UUID **f24bbd75-00bd-45e1-9250-f1b34af91917**:

```
XIQC.extremenetworks.com:profile# show

profile name              AP platform  profile ID

....
sf-custom-ap305c-profile  AP305C       30
```

```
XIQC.extremenetworks.com:profile:sf-custom-ap305c-profile# show
...
IoT Profile UUID: f24bbd75-00bd-45e1-9250-f1b34af91917
...
```