Safectory Track – Configuration Guide for Aruba Access Points

safectory GmbH

1 Preamble

1.1 Copyright

1.2 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.

1.3 Warranty

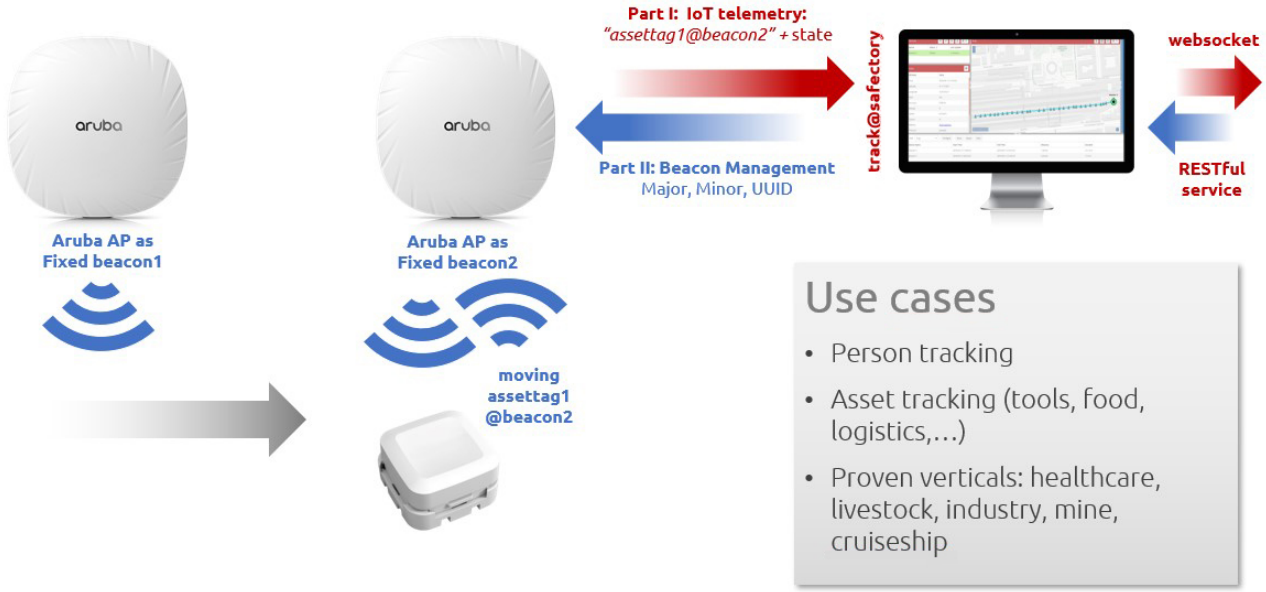
The Product Warranty and Software License and Warranty and other information are available in our GENERAL TERMS AND CONDITIONS at https://safectory.com/gtc?lang=en.

2 Introduction and Prerequisites

safectory's BLE hardware for tracking assets and tracing contacts.

Northbound / Upstream (covered in Part I): the access point forwards data created between tags and beacons to the server backend, a service called "safectory Track".

Beacon Management (covered in Part II): Data requested from the backend by the access point allows convenient and central management of the integrated AP beacon (APB).



To set up Aruba access points to be used with safectory products (asset tags, beacons, mobile SDK, Track backend), use the following manual.

2.1 Certified Product Summary

Type	Description
Manufacturer:	Aruba Networks: www.arubanetworks.com
Certified products:	all BLE-enabled access points (e.g., Aruba 36x, 32x, 515 (tested))
	Aruba Virtual Controller,
	Aruba Mobility Master Controller (e.g., ArubaMM-HW-5k, 8.11.0.1 SSR; ArubaMM-VA, 8.12.0.5 SSR)
Aruba software versions approved:	8.9.+ (8.6.+ for Beacon Management)
SF backend versions approved:	1.16.+

CLI documentation for Aruba Instant can be found in this document. Aruba controller CLI for ArubaOS will become available in the next version of this document added here.

2.2 Track-On-Premise (ToP) Server Requirements

For detailed server requirements when deploying Track-on-Premise, please refer to the ToP Server Requirements PDF.

2.3 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.

2.4 Configuring Preferred DNS to Reach *.safectory.com

The Aruba wireless controller should have DNS configured:

- **For Track-On-Premise (ToP)**: To resolve the FQDN of your ToP installation
- **For Cloud Track installations**: To reach `*.safectory.com` servers

2.5 Request or Create an Authorized User

This user is required for authentication between the Aruba APs/controller and the backend. BLE data sent from the Aruba APs/controller to the Track backend will be attributed to this user (i.e., the data is submitted **on behalf of** this user).

- Request or create a Track user with email `mysecret@authkey.safectory.com`
- Set a secret password, (e.g. `mysecret`)
- Make sure the user has a group in Track that can at least access (read/write) beacons and devices.

2.6 Add the CA Certificate(s) to the Virtual Controller

One or more CA certificates are required on the controller when connecting to the Track backend server. The Aruba Instant APs need to trust the certificate chain presented by Track.

2.6.1 Using Safectory-Hosted Instance (track.safectory.com)

If you are using the Safectory-hosted instance at track.safectory.com, follow these steps to add the **ISRG Root X1** certificate to the virtual controller:

- Download the ISRG Root X1 certificate from http://track.safectory.com/isrgrootx1.pem.

- Navigate to **Maintenance** > **Certificates** on your virtual controller.
- Click on **Upload New Certificate**.
  - Browse for the certificate file `isrgrootx1.pem` and upload it.
  - Certificate name: **ISRGRootX1**
  - Certificate type: **TrustedCA**
  - Certificate format: **X509 (`.pem`, `.cer`, or `.crt`)**
  - Click **Upload Certificate**.

Alternatively, this can be done via CLI:

```
Aruba_AP Name#
crypto pki-import format pem cert-type TrustedCA http://track.safectory.com/isrgrootx1.pem
↪  certname ISRGRootX1
```

The CA cert checksums for reference are:

```
SHA1:   CA BD 2A 79 A1 07 6A 31 F2 1D 25 36 35 CB 03 9D 43 29 A5 E8
MD5:    0C D2 F9 E0 DA 17 73 E9 ED 86 4D A5 E3 70 E7 4E
```

2.6.2 Using Track-on-Premise with Own Certificate

If you are using Track-on-Premise with a certificate issued by your IT department:

- **Check if the required CA certificate is already installed on the controller.**
  In many environments, the necessary root or intermediate CA certificates are already configured for other purposes, such as corporate Wi-Fi authentication. If the CA certificate is already present, no further action is required.
- **Obtain the necessary CA certificate(s)** from your IT department.
  This may be:
  - The root CA certificate
  - Any intermediate CA certificates required to complete the chain
- **Upload the certificate(s)** through the Aruba Instant Web UI:
  - Navigate to **Maintenance** > **Certificates**.
  - Click on **Upload New Certificate**.
  - Browse for each certificate file and upload it as:
    - Certificate type: **TrustedCA**
    - Certificate format: **X509 (`.pem`, `.cer`, or `.crt`)**
  - Click **Upload Certificate**.

Alternatively, if the certificate file is accessible via an HTTP/HTTPS URL, you can use the CLI command:

```
Aruba_AP Name#
crypto pki-import format pem cert-type TrustedCA
↪  http://your-custom-certificate-url/custom-ca-cert.pem certname CustomCA
```

> **Note:** Replace `http://your-custom-certificate-url/custom-ca-cert.pem` with the actual URL provided. If no URL is available, use the Web UI upload instead.

If you have any questions or encounter issues, please contact your IT administrator or Safectory support for assistance.

3 Part I: IoT Telemetry Setup for Track Service

3.1 Configure transportProfile

To send BLE data received by the Aruba AP to the Track server, you need to configure an Aruba IoT WebSocket connection. In the Aruba documentation, this is referred to as a **Northbound BLE Telemetry / Data Forwarding transportProfile**.

You need to know the hostname/URL of your Track instance. In this example, we will use `track.safectory.com`, please adjust accordingly.

- In the Aruba config, go to **Configuration** > **Services** > **IoT**
- Add a **transportProfile** and select Type **Telemetry Websocket**, name it "Safectory-Asset-Telemetry" (e.g.)
- Server-URL: can be left blank; URL will be set automatically during authentication
- Authentication – two options:
  1) User/password-based authentication (supported by all Track version >= 1.16)
     - Method: check **User ID /password**
     - Authentication URL (example): `https://track.safectory.com/api/session`
       - Protocol `https` (or `http`) and endpoint `/api/session` are mandatory
       - **When not using HTTPS** (i.e., HTTP),
         - then please explicitly specify port `6555` (default `web.port`, defined in `/opt/prodtrac/custom.xml`) in the authentication URL (example: `http://track.internal:6555/api/session`)
         - and make sure the port is open (firewall)
     - Server URL: can be left blank
     - Username / password: `mysecret@authkey.safectory.com` / `mysecret`
  2) Token-based authentication (supported with Track version 1.25+)
     - Method: check **Token**
     - Server URL (example): `ws://track.safectory.com/api/socket`
       - Protocol `ws` and endpoint `/api/socket` are mandatory (note: the Aruba frontend may complain about `ws://` but saving should work nonetheless)
       - **When not using HTTPS** (i.e., HTTP),
         - then please explicitly specify port `6555` (default `web.port`, defined in `/opt/prodtrac/custom.xml`) in the server URL (example: `ws://track.internal:6555/api/socket`)
         - and make sure the port is open (firewall)
     - Access Token: enter token as defined in Track's `credentials.xml` (for details, see Track admin manual, Section **Token-Based Authentication**)
- Choose a reporting interval according to your desired latency and bandwidth budget
- In **Transport service**, check **BLE Data** (enabling **BLE Telemetry** is not necessary for receiving BLE data)
- In **BLE Data** section, check **Per Frame Filtering**
- Add a **Company Identifier** Filter and set it to `0A35` to filter and enable BLE data for safectory devices
- *Optional*: Add a second **Company Identifier** filter and set it to `000d` to filter and enable BLE data using this manufacturer code
- The same can be done with CLI commands, as exemplarily described in Section Aruba Instant

3.1.1 Aruba Instant

Example for user/password-based authentication:

```
Aruba_AP Name#

configure terminal
iot transportProfile Safectory-Asset-Telemetry
authenticationURL https://track.safectory.com/api/session
authentication-mode password
username mysecret@authkey.safectory.com
password mysecret
endpointType telemetry-websocket
bleDataForwarding
perFrameFiltering
companyIdentifierFilter 0a35,000d
exit
exit
commit apply
```

Note: `endpointURL` will be managed automatically by the `authenticationURL` response.

3.2 Enable IoT Radio Profile

Before BLE data can be forwarded, an IoT radio profile must be created and activated. The profile must be set to `scanning` mode (if you also need beaconing (cf. part II), then select `both`).

- **CLI**: Use the `iot radio-profile` and `iot use-radio-profile` commands as shown in the IoT Radio Profile section.
- **Web UI (Mobility Conductor)**: Navigate to **Configuration → IoT → IoT Radios** to create the profile, then assign it to the appropriate AP groups under **Configuration → AP Groups → IoT** tab.

For detailed steps, refer to the IoT Radio Profile section.

3.3 Monitor Operation with CLI Commands

Once the **Transport Profile** is activated, its operation can also be checked using some CLI commands.

Note:
The exact syntax and availability of CLI commands may vary depending on your **ArubaOS** version and AP/controller model. Some commands shown in this manual may not be present or may output slightly different information on your system. Always consult the official Aruba documentation that matches your deployment version (e.g., available on the HPE Aruba Networking Documentation Portal).

3.3.1 Connection Status

Field `TransportContext` shows the connection status (`Connection Established` is expected here if everything is working correctly):

```
hostname #show ble_relay iot-profile
---------------------------------Profile[safectory-iot-profile]--------------------------------

Identifier                              : 1709920737
serverURL                               : ws://10.42.13.37:6555/api/socket
serverType                              : Telemetry Websocket
deviceClassFilter                       : None
reportingInterval                       : 600 second
authentication-mode                     : none
accessToken                             : axvjxvz92392413akbc923
rssiReporting                           : Average
environment                             : office
bleDataForwarding                       : TRUE
perFrameFiltering                       : TRUE
companyIdentifierFilter                 : 000D,0A35
include_ap_group                        : OFFICE
Server Connection State
-----------------------------
TransportContext                        : Connection Established
Last Data Update                        : 2024-03-08 09:57:18
Last Send Time                          : 2024-03-08 09:57:34
TransType                               : Websocket
```

3.3.2 Message Statistics

```
hostname# show ap debug ble-relay tag-report

-------------------------Profile[Safectory-Asset-Telemetry]-------------------------

Incoming Tag messages                   : 23
```

```
Tag messages processed                  : 20
Tag messages dropped                    : 3
Tag messages WS queue success           : 20
Tag messages WS queue unavailable       : 0
Tag messages WS not connected           : 0
Tag messages WS sent                    : 20
Heartbeat messages WS sent              : 18
...
```

When safectory BLE devices are present in the range of the AP, the message counter should increase.

3.3.3 Show Profile Information

To output the complete setup, run this command:

```
show iot transportProfile Safectory-Asset-Telemetry

Name                        :Safectory-Asset-Telemetry
EndpointType                :telemetry-websocket
TransportInterval           :10
Username                    :mysecret@authkey.safectory.com
Password                    :*****
AuthenticationURL           :https://track.safectory.com/api/session
Authentication-mode         :password
companyIdentifierFilter     :000d,0a35
bleDataForwarding           :TRUE
perFrameFiltering           :TRUE

<only relevant parameters shown in this manual>
```

In **SF Track**, devices with the exact same name as your Aruba APs will be created and will appear online (green).

4 Part II: Setup Access Point as Location Beacon (iBeacon)

This functionality is given and validated for ArubaOS versions 8.9.0.2, 8.10.0.{3,9,13,15,17,20,21} (LSR), 8.11.2.0 (SSR), 8.12.0.4 (SSR), and 8.12.0.5 (SSR), and 8.13.1.1 (LSR).

This step is useful (but optional) if you want to use the integrated AP Beacons as location beacon in areas where SF beacons are not mounted (yet).

To set up one or more Aruba access points to transmit iBeacon advertisements, the safectory Track server provides an **Aruba Beacon Management Console** that can be used to manage all beacon aspects in a central place.

To connect to a Track server, you need to know its hostname/URL. In this example we will use `track.safectory.com`, please adjust accordingly.

4.1 Beacon Management

To configure multiple Aruba APs with iBeacon function to be active within Track, follow these steps:

- Enable the IoT radio profile in `beaconing` mode (if you also need scanning (cf. part I), then select `both`). Create the profile via CLI (`iot radio-profile`) or through the Mobility Conductor UI (**Configuration → IoT → IoT Radios**), then assign it to the appropriate AP groups. See the IoT Radio Profile section for detailed steps.
- Edit the group where the authorized users (`mysecret@authkey.safectory.com`) are members, add the attribute `aruba_next_sync`, and set it to e.g. `20` in order to make all APs poll every 20 sec.

- You may want to use a slower interval after a setup phase is complete. The Aruba default is 10 minutes.

Alternative way to configure an Aruba AP's iBeacon config individually via a CLI command, here giving the AP with BLE MAC address `24:7D:4D:C0:44:DF` the UUID-major-minor triplet `f32b1e749a7051689e93085ef2cd40db-12-6`:

```
ap ble-configure cfg-ble-mac 24:7d:4d:c0:44:df major 12 minor 6 uuid
 ↪  f32b1e74-9a70-5168-9e93-085ef2cd40db slot 0 interval 100
```

Note:

- One way to determine the BLE MAC address is via CLI command `show ap debug ble-database` (this shows a table with column `BLE MAC`).
- The above command was confirmed working with Aruba OS 8.11.2.0 SSR. Earlier and future version may have a different syntax.
- The beaconing interval (`interval 100` in the example) does not seem to have any effect (on Aruba OS 8.11.2.0 SSR) and stays at 100 ms independent of the actually submitted value.

4.1.1 Aruba Web UI

- In the Aruba config, go to **Configuration** > **Services** > **IoT**
- Add a **transportProfile** and select type `Meridian-Beacon-Management`, name it "Safectory-Beacon-Management" (e.g.)
  - As Server URL add `https://track.safectory.com/api/beacons/arubaBmc`
  - Access token: `mysecret`
- The same can be done with CLI commands, as exemplarily described in Section Aruba Instant

4.1.2 Aruba Instant

```
Aruba_AP Name#

crypto pki-import format pem cert-type TrustedCA http://track.safectory.com/isrgrootx1.pem
 ↪  certname ISRGRootX1

configure terminal
iot transportProfile Safectory-Beacon-Management
endpointURL "https://track.safectory.com/api/beacons/arubaBmc"
endpointToken mysecret
payloadContent managed-beacons
exit
iot useTransportProfile Safectory-Beacon-Management
exit
commit apply
```

The above commands will configure the profile and start an update right away. When adding via the WebUI it may take up to 10 minutes before the update.

- Beacons with the exact same name as your Aruba APs will be created in Track (if they don't exist).
- Use a group attribute `ibeacon_uuid` with the value of the desired uuid to set a new project-specific uuid for all beacons.
- Changes to the beacons `uuid/major/minor` and attributes `txpower` will be transferred to the APs upon update.
- Be aware that the AP may start advertising new changes with a delay of up to several minutes (~10 min).
- CLI command `ble-init-action send-update Safectory-Beacon-Management` can trigger an immediate update.

Beacon management is supported on ArubaOS 8.6.+.

See e.g. https://www.arubanetworks.com/techdocs/CLI-Bank/Content/aos8/sh-ap-dbg-ble-cn.htm for more details.

5 IoT Radio Profile

Beginning from Aruba Operating System Software 8.6.0.0 you need to configure and activate an IoT Radio Profile to assure receiving or sending BLE signals.

There are 3 different modes:

- `scanning`: only scan for BLE signals and forward to configured service
- `beaconing`: only send beacon advertisements
- `Both`: scan for BLE signals and forward to configured service + send beacon advertisements

Example Configuration:

```
(host) (config) #
iot radio-profile ap-ble
radio-mode ble
exit
iot use-radio-profile ap-ble
commit apply
```

```
cc:d0:83:c7:0f:6c# show iot radio-profile

IoT Radio Profile List
----------------------
Name    References  Instance  Mode
----    ----------  --------  ----
ap-ble  1           internal  ble
------------
Total:1
(host) [mynode] #show iot radio-profile ap-ble

Name                :ap-ble
Reference           :1
Instance            :internal
Mode                :ble
BLE Opmode          :scanning beaconing
BLE Console         :
BLE TxPower         :0
Zigbee Mode         :coordinator
Zigbee Channel(s)   :auto
```

5.0.1 Mobility Conductor UI Configuration

When using Aruba Mobility Conductor (or Mobility Master), you can create and assign IoT Radio Profiles through the web interface:

1. **Create IoT Radio Profile**:
   - Navigate to **Configuration → IoT → IoT Radios**
   - Click **Add** to create a new profile
   - Configure the profile with the desired mode (`scanning`, `beaconing`, or `Both`)
   - Save the profile with a descriptive name (e.g., `safectory-iot-radio`)
2. **Assign to AP Groups**:
   - Navigate to **Configuration → AP Groups**
   - Select the target AP group

- Go to the **IoT** tab within the AP group configuration
- Under **IoT Radio Profile**, select the previously created profile (e.g., `safectory-iot-radio`)
- Save the configuration

The changes will propagate to the affected access points. For CLI‑based deployments, use the commands shown above.

> **Note:** The exact menu labels and navigation path may vary slightly between different ArubaOS versions and controller models (Mobility Conductor, Mobility Master, or Virtual Controller). Consult your Aruba documentation if the described UI elements do not match your environment.

See https://www.arubanetworks.com/techdocs/CLI-Bank/Content/aos8/ap-ble-conf.htm for reference.

6 Legal Statements

Please be aware that the above configuration should only be applied if you are not using, or in the future planning to use, Aruba Meridian location products.

Safectory as developer of the integration solution notifies you that

- Safectory determines the suitability of Aruba Beacon Management Protocol to configure Aruba BLE beacons to integrate them with safectory BLE products and solutions.
- Safectory is fully responsible for the integration of the location solutions in Aruba products and its technical troubleshooting, or field sales support.

7 Revision History

Version	Date	Description
0.2	10/2021	Initial Release
0.3	11/2021	Harmonized information
0.4	02/2022	Added new ArubaOS version number 8.9.0.1
0.5	03/2022	Added new ArubaOS version number 8.9.0.2
0.6	11/2023	Added new ArubaOS version numbers 8.10.0.3 (LSR), 8.10.0.9 (LSR), 8.11.2.0 (SSR)
0.7	05/2024	Added instructions for token-based authentication
0.8	09/2024	Added CLI command for AP iBeacon control
0.9	03/2025	Added new tested version numbers 8.10.0.13 (LSR), 8.10.0.15 (LSR), 8.12.0.4 (SSR)
1.0	05/2025	Revise document structure
1.1	07/2025	Added new version number 8.10.0.17 (LSR)
1.2	07/2025	Added more details about CA certificates
1.3	08/2025	Added hints about HTTP vs. backend port and IoT connection check
1.4	12/2025	Added new tested version numbers 8.10.0.20 (LSR), 8.13.1.1 (LSR)
1.5	01/2026	Added new tested version number 8.10.0.21 (LSR)
1.6	03/2026	Added more details on IoT radio, Track user, and Aruba versions