Safectory Track – Configuration Guide for Cisco (gRPC-Based) Access Points

safectory GmbH

1 Preamble 2
- 1.1 Revision history . . . 2
- 1.2 Terms of use . . . 2
- 1.3 Warranty . . . 2

2 Introduction and Prerequisites 3
- 2.1 Certified Product and Software Summary . . . 3
- 2.2 Track-On-Premise (ToP) Server Requirements . . . 3
- 2.3 Configuring Clock/NTP Services . . . 4
- 2.4 Configuring Preferred DNS . . . 4
- 2.5 Request or Create an Authorized User . . . 4

3 Part I: HTTPS and gRPC Setup for Track Service 4
- 3.1 Set Up Certificate + PKCS#8 Key . . . 4
- 3.2 Set Up Firewall . . . 5
- 3.3 Set Up Routing on the ToP Host . . . 5
- 3.4 Set Up Nginx (Track On-Premise (ToP) Installation) . . . 5
- 3.5 Set Up WLC (and Access Points) . . . 6
  - 3.5.1 Enable NETCONF via Web UI on WLC . . . 6
  - 3.5.2 Verify NETCONF Capabilities . . . 6
  - 3.5.3 Enable SSH Access via Web UI on WLC and APs . . . 6
  - 3.5.4 Using an optional external NETCONF client . . . 7
  - 3.5.5 Adding a Trust Point and Certificate to the (v)WLC (Enrollment) . . . 7
  - 3.5.6 Enable BLE Admin State . . . 9
  - 3.5.7 Enable gRPC in AP Join Profile . . . 9
  - 3.5.8 Enable BLE Radio (Scanning) . . . 10
  - 3.5.9 Distribute JSON Web Token (JWT) . . . 12
  - 3.5.10 Set up gRPC Endpoints . . . 13
- 3.6 Set Up Track . . . 13
  - 3.6.1 Configure the Track backend . . . 13

4 Part II: Setup Access Point as Location Beacon (iBeacon) 15
- 4.1 Method A: Manual NETCONF (Batched) . . . 15
- 4.2 Method B: Manual CLI (Per AP) . . . 15

5 Troubleshooting 16

1 Preamble

This guide describes how to integrate Cisco Catalyst access points and wireless LAN controllers with Safectory Track for BLE data transmission, beacon tracking, and optional iBeacon advertising. It covers certificate, firewall, routing, WLC, access point, gRPC, and backend NETCONF automation setup. The backend NETCONF binding is the preferred method for routine token renewal, BLE state recovery, and AP inventory synchronization.

1.1 Revision history

Version	Date	Description
0.1	12/2023	Initial version
0.2	04/2024	Revised version
0.3	05/2025	Revised version
0.4	02/2026	Revised version
0.5	11/2026	Revised version

1.2 Terms of use

Subject to technical modification without notice.

Errors and omissions excepted.

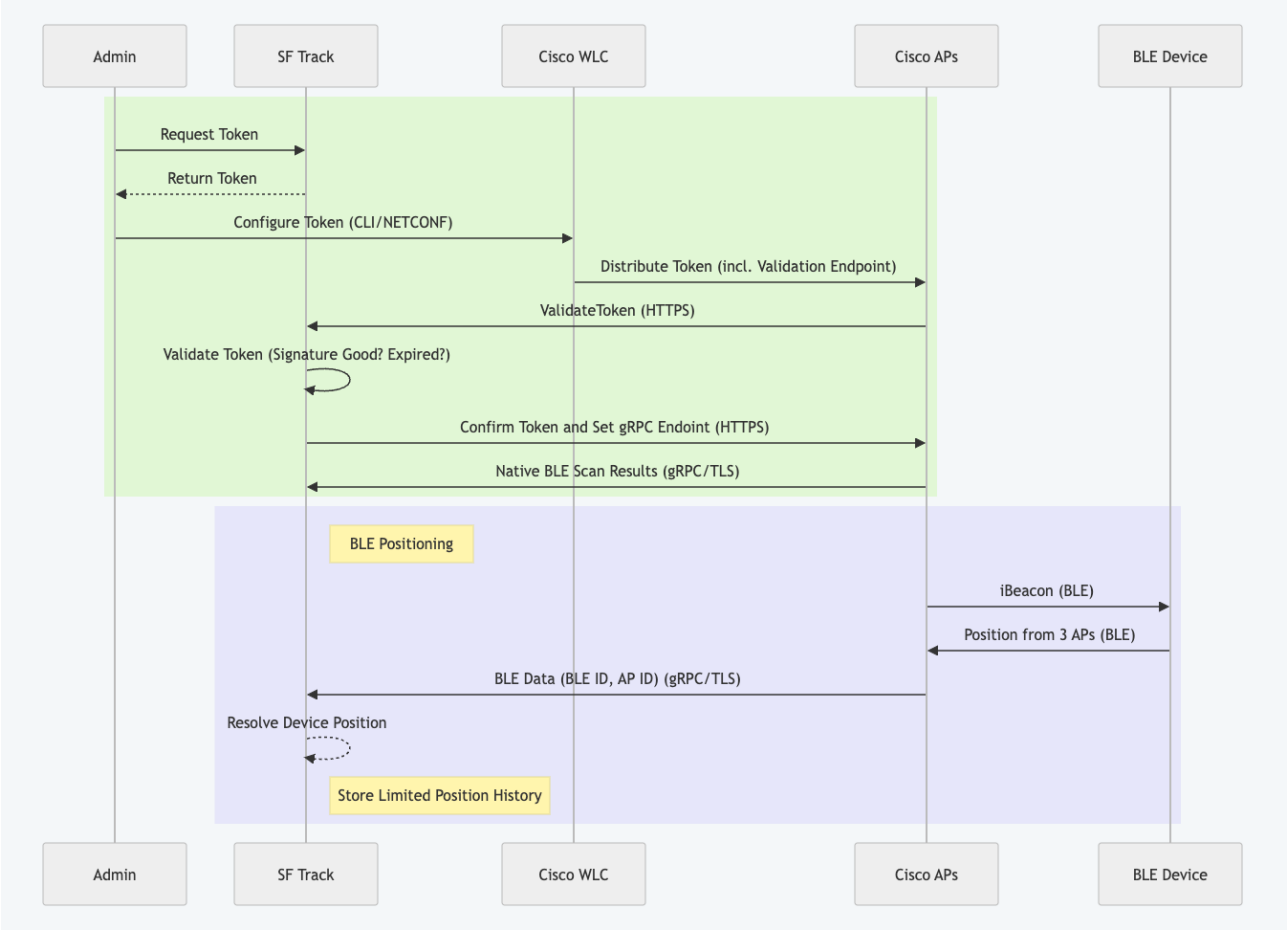
For further information regarding legal and proprietary statements, please go to our GENERAL TERMS AND CONDITIONS at https://safectory.com/gtc/.

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/.

2 Introduction and Prerequisites

To set up Cisco access points to be used with safectory's BLE products (asset tags, beacons, mobile SDK, Track backend) for tracking assets and tracings contacts, use the following manual. Overview diagram:



2.1 Certified Product and Software Summary

- Certified products:
  - all BLE-enabled access points (e.g., Cisco Catalyst 9105AX Series-W / 9115AXI-E / 9115AXE-E / 9120AXI-E (tested))
  - (v)WLCs: Cisco Catalyst 9800 Series Wireless Controller (tested: 9800-L, 9800-80) / Cisco Catalyst 9800-CL Wireless Controller
- Certified software:
  - Cisco software versions approved (WLC): Cisco IOS XE 17.3.1, 17.6.1, 17.9.3, 17.15.5
  - SF backend versions approved: 1.17.x+
  - Minimal gRPC version tested: 1.11.0

Only the versions listed above have been tested. Newer Cisco firmware versions may require additional development effort and incur additional costs.

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 please make sure that all the nodes are synchronized with the same reference server and time.

2.4 Configuring Preferred DNS

The 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 to generate the JSON Web Token (JWT) used for authentication. BLE data sent from the Cisco 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.

3 Part I: HTTPS and gRPC Setup for Track Service

In order to make all communication channels work, the following changes are necessary (all described in the upcoming subsections):

- HTTPS and gRPC certificate creation
- Nginx configuration and firewall adjustments
- Track backend config adjustments
- WLC config adjustments
- Certificate enrollment (WLC)
- Enabling BLE admin state
- Enabling gRPC in AP Join Profile (WLC)
- Enabling BLE radio(s) for scanning (WLC)
- Enabling gRPC endpoint(s) in the Track backend
- Distributing JSON Web Token (JWT)

Info: Once HTTPS connections between the backend and Cisco APs work, in SF Track, devices (+ associated beacons) with the exact same name as your Cisco APs will be automatically created and shown online/green.

3.1 Set Up Certificate + PKCS#8 Key

The following steps describe generation of a self-signed certificate. If there is already a certificate available, then you may skip to step 5 (PKCS#8 generation).

SSL/TLS certificates expire. On-site IT staff must be aware of the expiration date and maintain a process for periodically renewing the certificate. This process includes creating or obtaining a renewed certificate, enrolling it on the WLC, importing it into Nginx on the ToP instance, converting the private key to PKCS#8, and importing the certificate and key into the backend on the ToP instance.

1) Suggestion: Use the same certificate for both HTTPS (→ Nginx config) and gRPC
2) Determine the IP address of Track Service Host
3) Generate a file named `ssl.conf` with following content; adjust the IP address `xxx.xxx.xxx.xxx` to the one determined in the previous step. The file is assumed to be in the same directory as the other files generated in the next steps:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
countryName                 = DE
countryName_default         = CA
stateOrProvinceName         = Bayern
stateOrProvinceName_default = Bayern
localityName                = Bamberg
localityName_default        = Bamberg
organizationName            = safectory
organizationName_default    = safectory
commonName                  = xxx.xxx.xxx.xxx
commonName_max              = 64
commonName_default          = xxx.xxx.xxx.xxx

[v3_req]
subjectAltName = @alt_names

[alt_names]
IP.1 = xxx.xxx.xxx.xxx
```

4) Generate basic key file (`server.key`) and certificate (`server.cert`):

```
openssl genrsa -out myca.key 2048
openssl genrsa -out server.key 2048
openssl req -x509 -new -nodes -key myca.key -sha256 -days 365 -out myca.cert
openssl req -out server.csr -key server.key -new -config ssl.conf
openssl x509 -req -in server.csr -CA myca.cert -CAkey myca.key -CAcreateserial -out
↪  server.cert -days 365 -extensions v3_req -extfile ./ssl.conf
```

5) Generate `server.pkcs8` from `server.key` (**without** password)

```
$ openssl pkcs8 -topk8 -inform PEM -outform PEM -nocrypt -in server.key -out server.pkcs8
```

6) Adjust Nginx config to use newly generated key pair, see next subsection (requires to generate PEM: `openssl x509 -inform PEM -in server.cert > server.cert.pem`)

3.2 Set Up Firewall

Ensure that TCP ports 57501 (gRPC) and 443 (HTTPS) are open from WLC/APs towards the Track Service Host (track.safectory.com or ToP Host)

3.3 Set Up Routing on the ToP Host

Make sure that the routing configuration on the Debian or Ubuntu ToP host allows bidirectional communication with the WLCs and APs. This is especially important when the APs or WLCs and the ToP host are located in different networks. Configure the required routes and gateways on the ToP host and verify them before testing the connection.

Use `ip route` and `ip route get <WLC_OR_AP_ADDRESS>` to check the active routing configuration. When troubleshooting the connection, capture traffic on the ToP host with `tcpdump`. Seeing only TCP `SYN` packets without the corresponding replies can indicate that the routing configuration is incomplete or incorrect.

3.4 Set Up Nginx (Track On-Premise (ToP) Installation)

Check config towards `streaming` endpoint definition and paths of SSL certificate/key:

1. Open `/etc/nginx/sites-enabled/001-trac-ssl`

2. Update paths of `ssl_certificate` and `ssl_certificate_key` (to the ones of `server.cert.pem` and `server.key`, respectively)
3. If not defined yet, add:

```
    location /streaming {
        proxy_pass          http://backend-track/api/streaming;
        proxy_set_header    X-Real-IP       $remote_addr;
        proxy_set_header    X-Forwarded-For $remote_addr;
        proxy_set_header    Host            $host;

    }
```

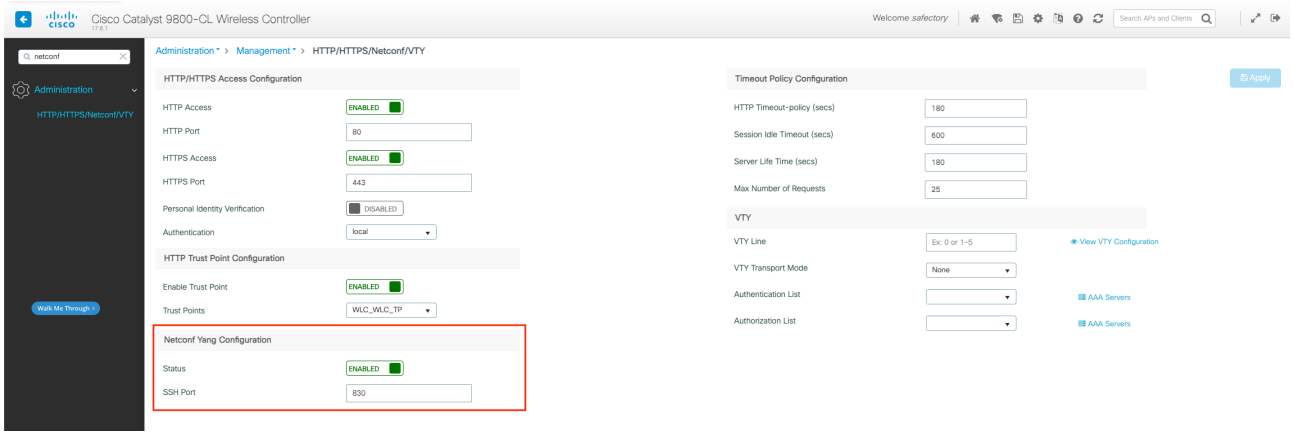
4. Verify changed config via `nginx -t` (outputs like `syntax is ok` and `test is successful` are expected)
5. When there were no errors, reload or restart Nginx: `systemctl restart nginx`

3.5 Set Up WLC (and Access Points)

3.5.1 Enable NETCONF via Web UI on WLC

Navigate to **Administration** > **Management** > **HTTP/HTTPS/Netconf/VTY**:

- Enable **Netconf Yang Configuration**
- SSH Port: 830



3.5.2 Verify NETCONF Capabilities

To ensure your WLC supports the necessary BLE management features, you can verify the advertised capabilities by connecting to the NETCONF port (830).

Run the following command:

```
ssh -p 830 <USER>@<WLC_ADDRESS>
```

Check that the output contains the following modules (usually found within the `<capability>` tags):

```
Cisco-IOS-XE-wireless-ble-ltx-oper
Cisco-IOS-XE-wireless-ble-mgmt-cmd-rpc
Cisco-IOS-XE-wireless-ble-mgmt-oper
```

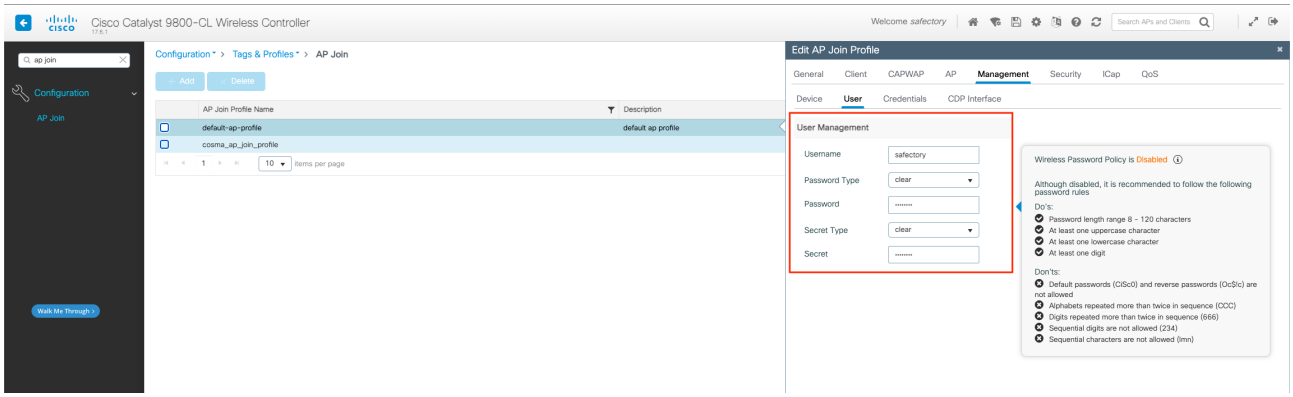
3.5.3 Enable SSH Access via Web UI on WLC and APs

1) Navigate to **Administration** > **Command Line Interface**:
   - Switch to **Configure** mode

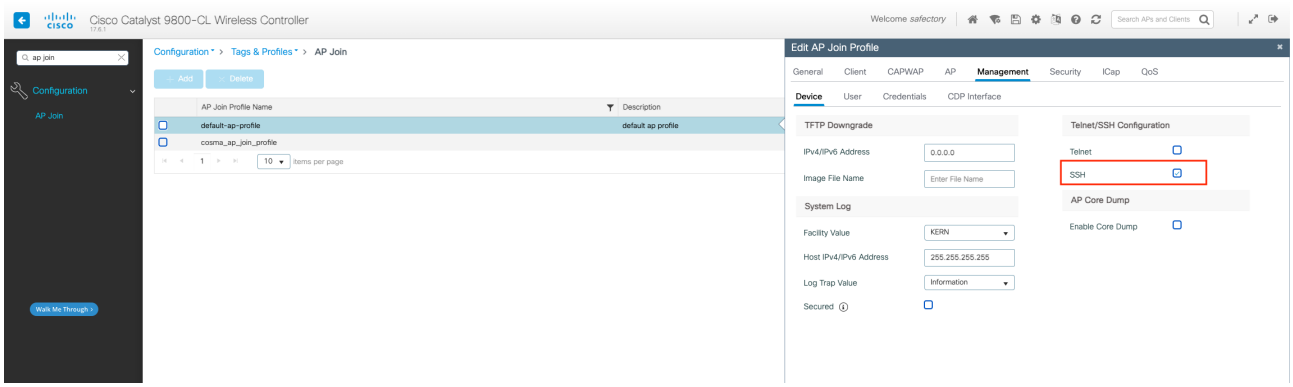
- Paste and execute (**Run Command** button) following commands:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
```

2) Navigate to **Configuration** > **Tags & Profiles** > **AP Join** > Select (default) AP profile
   - Add new user (**Management** > **User** tab)



   - Enable SSH (**Management** > **Device** tab)



3.5.4 Using an optional external NETCONF client

The direct NETCONF binding in the Track backend is the preferred method for routine token renewal, BLE state recovery, and AP inventory synchronization. An external NETCONF client is optional and is intended for manual troubleshooting, custom RPCs, iBeacon configuration, or installations where the backend binding is not used.

The Track service generates XML elements that can be executed as RPCs by any compatible NETCONF client. The client must have network access to the WLC's NETCONF port, usually TCP port 830.

Running an RPC via an external NETCONF client

1. Connect the NETCONF client to the WLC using the WLC address, port, and credentials.
2. Request the required XML elements from the Track service, for example through `/api/netconf`.
3. Submit the XML elements as an RPC through the NETCONF client.

Do not add a `<CONFIGURATION>` wrapper unless the selected client specifically requires one.

3.5.5 Adding a Trust Point and Certificate to the (v)WLC (Enrollment)

A trust point and the certificate can be enrolled via CLI.

If you are using two certificates (one for Nginx/HTTPS and one for gRPC), it is required to enroll both certificates as described for one certificate in the following to the (v)WLC. This is necessary to allow communication with

the ToP backend endpoint `/api/streaming/validate` (HTTPS) and to allow gRPC connections from the AP(s) to the gRPC endpoint (see Section Set up gRPC Endpoints) that is configured for the respective AP device (e.g., via TrackUI = frontend for Track / Track-on-Premise).

1) Connect to the (v)WLC via SSH/CLI
2) Optional: To remove an already existing trust point (`trackca` in the example):

```
WLC#configure t
WLC(config)#no crypto pki trustpoint trackca
% Removing an enrolled trustpoint will destroy all certificates
 received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.
```

3) Prepare new trust point via following commands; the name of the trust point (`trackca` in the example below) can be chosen freely:

```
Enter configuration commands, one per line.  End with CNTL/Z.
WLC#configure t
WLC(config)#crypto pki trustpoint trackca
WLC(ca-trustpoint)#enrollment terminal
WLC(ca-trustpoint)#chain-validation stop
WLC(ca-trustpoint)#revocation-check  none
WLC(ca-trustpoint)#exit
```

Note: The above commands `revocation-check none` and `chain-validation stop` are strictly required when using the self-managed certificate authority described in this guide, as the WLC cannot check an online Certificate Revocation List (CRL).

If you are using a certificate issued by your organization's **Enterprise CA** and the WLC has network access to the CRL/OCSP responders, you should omit these lines to ensure proper validation.

4) Add the actual certificate to the trust point; it simply can be pasted after entering the following command on the first line:

```
WLC(config)#crypto pki authenticate trackca

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIULzxZ3O1WImFajJohxbCGsisQgYQwDQYJKoZIhvcNAQEL
[...]
QsPnyIyBA2/916aW4ugc4AgMiQ==
-----END CERTIFICATE-----

Trustpoint 'trackca' is a subordinate CA and holds a non self signed cert
Trustpoint 'trackca' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: 4BE72F95 6DF15BA8 A29F8118 A54626A1
      Fingerprint SHA1: 7121A37A D9381935 D43FBA7D BFD27574 3B566D01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

5) Optional: To verify/view the certificate afterwards:

```
WLC#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2F3C59DCED5622615A8C9A21C5B086B22B108184
  Certificate Usage: General Purpose
  Issuer:
    o=Safectory
    l=Bamberg
    st=Bayern
    c=DE
  Subject:
    cn=172.27.0.55
    o=safectory
    l=Bamberg
    st=Bayern
    c=CA
[...]
```

3.5.6 Enable BLE Admin State

Enabling the **BLE Admin State** effectively powers on the BLE radio subsystem on the access point. This is a mandatory prerequisite for any BLE-based functionality.

The Track backend can perform this step automatically when NETCONF automation is enabled. This backend binding is the recommended method because it can also recover stale APs after the initial setup.

Method A: Backend NETCONF automation (recommended)

Enable `gateway.netconf.auto.enable` and `gateway.netconf.auto.adminState.enable` as described in Configure NETCONF automation. The backend then performs periodic or stale-triggered BLE admin-state OFF-to-ON resets.

Method B: Manual NETCONF via an external client

The setting can be included in the manual NETCONF configuration described in Section Enable BLE Radio (Scanning). Use this method only when backend NETCONF automation is unavailable or for troubleshooting.

Method C: Manual CLI (Per AP)

The following steps can be done via CLI per AP:

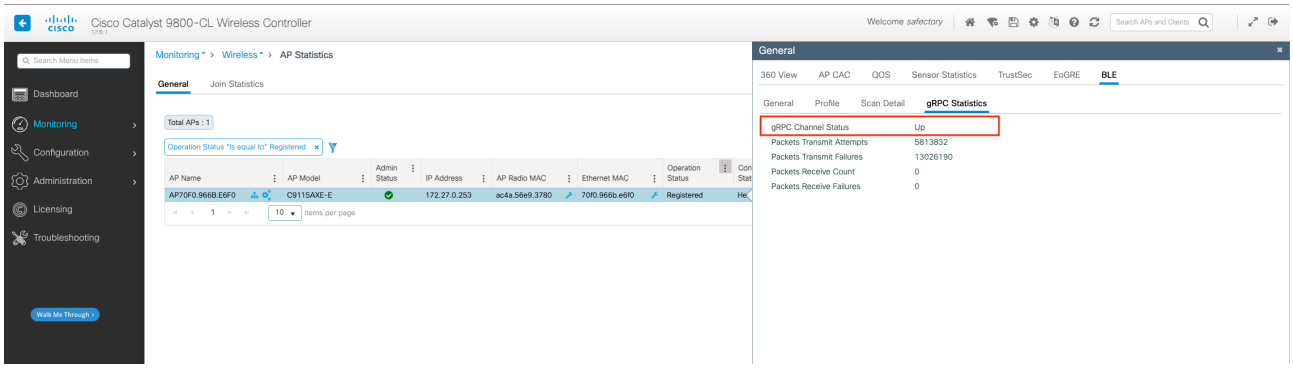
1) Log in via SSH
2) Type `configure terminal`
3) Type `ap name <ap-name> ble admin enable` (replace `<ap-name>` appropriately)

3.5.7 Enable gRPC in AP Join Profile

The following steps need to be done via CLI:

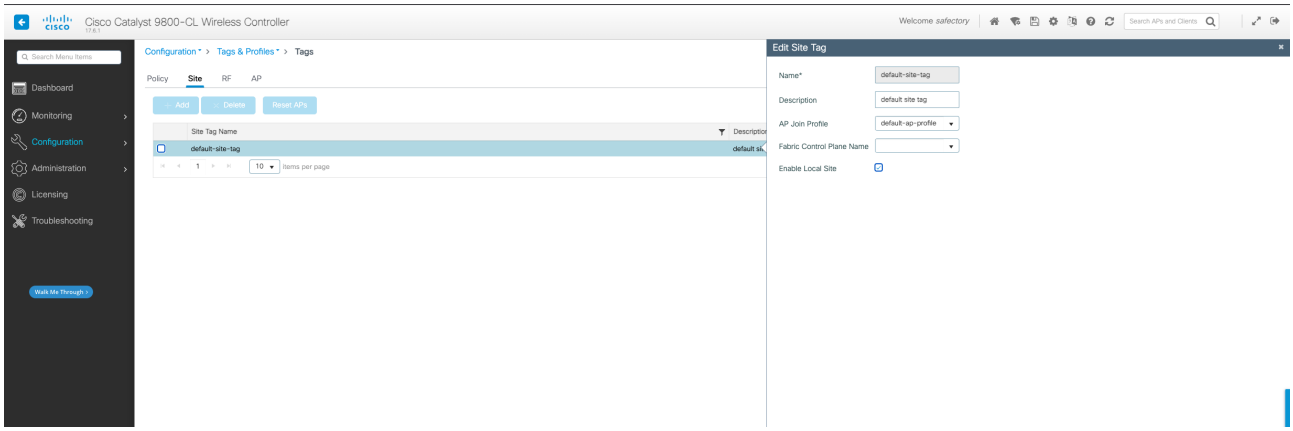
1) Log in via SSH
2) Type `configure terminal`
3) Type `ap profile <ap-profile-name>` (replace `<ap-profile-name>` appropriately)
4) Type `cisco-dna grpc`
5) Verify **gRPC Channel Status** is **Up** via web UI
   - Navigate to **Monitoring** > **Wireless** > **AP Statistics**
   - Select an AP
   - Switch to **BLE** tab (on the right-hand side)
   - Switch to **gRPC Statistics** tab

Steps 1–4 are also described in more detail on https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-5/config-guide/b_wl_17_5_cg/m_ble_management_in_the_controller.html.



Notes:

- It may be necessary to create an **AP Join Profile** in the first place, which can be done at **Configuration** > **Tags & Profiles** > **AP Join**.
- Furthermore, it may also be necessary to create a **Site Tag** that needs to be associated with the **AP Join Profile** at **Configuration** > **Tags & Profiles** > **Tags** > select **Site** tab:



3.5.8 Enable BLE Radio (Scanning)

The Track backend has a generator at `/api/netconf` to generate NETCONF XML entries for different tasks/settings. Track also has a function to generate signed JSON Web Tokens (JWTs) that can be used as an authorized user with device-write permissions by requesting `https://<TRACK_ADDRESS>/api/streaming/token/generate`.

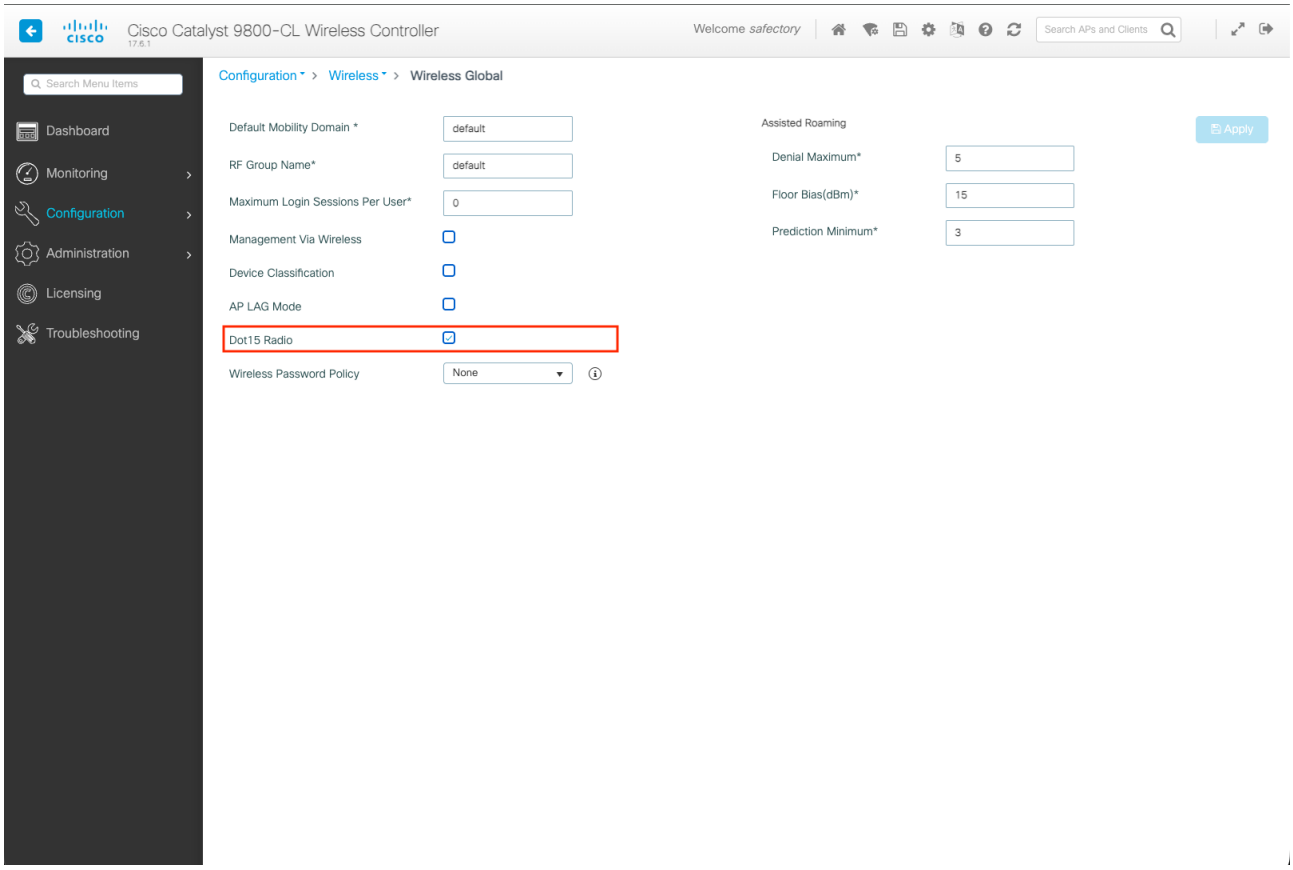
Globally Enable Radio via WebUI You can verify that the BLE radio is globally enabled via the Web UI:

1. Navigate to **Configuration** > **Wireless** > **Wireless Global** or access via https://WLC_ADDRESS/webui/#/wirelessglobal.
2. Ensure that **Dot15 Radio** (or **Dual Band (802.15.4)** on some versions) is **Enabled**.

Enable BLE Scanning The Track backend can enable and recover BLE scanning through its direct NETCONF binding. This backend automation is the recommended method for new installations.

Method A: Backend NETCONF automation (recommended)

Enable `gateway.netconf.auto.enable` and `gateway.netconf.auto.scanState.enable` as described in Configure NETCONF automation. The backend then performs periodic or stale-triggered BLE scan-state OFF-to-ON resets.



Method B: Manual NETCONF via an external client

To enable BLE scanning manually via NETCONF, get output from the Track service and execute it with an external NETCONF client. Use this method only when backend NETCONF automation is unavailable or for troubleshooting.

- TrackUI: Have at least one (AP) device with attribute `generate_grpc_netconf` set to `true`
- Get output for NETCONF (for all APs). **Critical RPCs for scanning are `ble-scan-req` and `ble-mgt-admin-req`**: https://TRACK_ADDRESS/api/netconf?configsEnabled=ble-scan-req&configsEnabled=ble-ibeacon-req&configsEnabled=ble-mgt-admin-req&configsEnabled=ap-dna-global-config
- Submit the NETCONF RPC with the external NETCONF client.

Important note on AP identifiers for NETCONF: Identifying the AP correctly in the NETCONF XML is critical for the configuration to take effect:

- **Requirement**: You must use either the **Radio MAC address** or the **AP Name**. The Ethernet (Base) MAC address will **not** work.
- **Verification**: Check the MAC address in the XML generated by the `/api/netconf` endpoint. If it matches the AP's **Ethernet (Base) MAC**, it must be replaced with the **Radio MAC**.
- **Format**: When using the `<mac-addr>` tag, the address must be in the format `aa:bb:cc:dd:ee:ff` (all lowercase with colons). The Cisco-style `aaaa.bbbb.cccc` format will fail.
- **Alternative**: You can manually replace the `<mac-addr>...</mac-addr>` tag in the generated XML with `<ap-name>YOUR_AP_NAME</ap-name>`.
- **Finding Identifiers**: You can find the Radio MAC and AP Name in the WLC Web UI under **Configuration** > **Wireless** > **Access Points** > [Select AP] > **General** or **Inventory** tab.

Method C: Manual CLI (legacy, per AP)

On Cisco IOS XE 17.15.3 and newer, scan state can no longer be enabled or disabled via CLI. Use the backend NETCONF automation or manual NETCONF method instead.

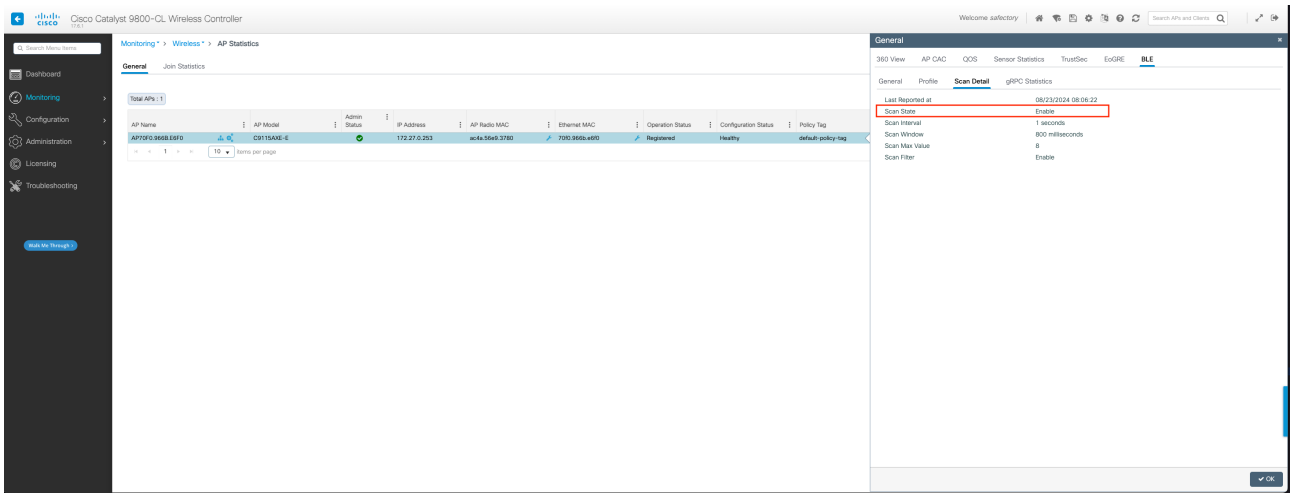
To enable BLE scanning manually on older IOS XE versions, use the following command (substitute `<ap-name>` with your AP's name):

```
ap name <ap-name> ble interval 1 window 0 max_value 8 filter disable state enable
```

Example:

```
WLC#ap name AP70F0.966B.E6F0 ble interval 1 window 0 max_value 8 filter disable state enable
```

Result (Enabled):



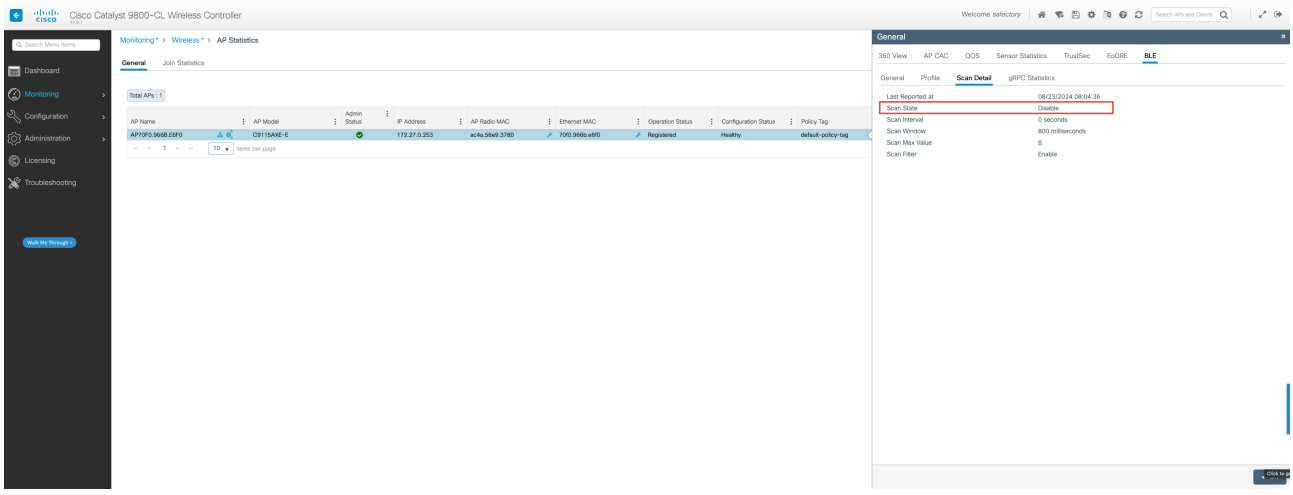
To disable it:

```
ap name <ap-name> ble interval 0 window 0 max_value 1 filter disable state disable
```

Example:

```
WLC#ap name AP70F0.966B.E6F0 ble interval 0 window 0 max_value 1 filter disable state disable
```

Result (Disabled):



3.5.9 Distribute JSON Web Token (JWT)

The JWT authenticates the APs against the Track backend through gRPC and authorizes them to upload scanning data. The Track backend can refresh and distribute the token through its direct NETCONF binding.

Method A: Backend NETCONF automation (recommended)

Enable `gateway.netconf.auto.enable` and `gateway.netconf.auto.tokenRenew.enable` as described in Configure NETCONF automation. The backend uses the configured Track user and WLC connection definitions to perform periodic token updates.

Method B: Manual CLI via WLC (fallback)

To distribute a new token manually, get output from the Track service and execute the following commands:

- **Generate JWT**: https://TRACK_ADDRESS/api/streaming/token/generate returns a value under `streamAccessKey`, which must be inserted as `<token>` in the next step without quotes.
- **Distribute JWT via WLC**: Type `configure terminal`, followed by `ap cisco-dna token 0 <token>`.

  Example:

```
WLC#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
WLC(config)# ap cisco-dna token 0 eyJhbGciOiJI[...]
WLC(config)# exit
WLC#
```

Tip: To verify if a token is valid or not, you can run the following commands via CLI on an AP (requires privileged EXEC mode):

1. Type `enable` (you may be prompted for the password again).
2. Type `show cloud connector key authentication`.

3.5.10 Set up gRPC Endpoints

To make an AP talk with the ToP backend, it is required to specify the address and port for gRPC connections:

- TrackUI: Add `grpcEndpoint` attribute to generated AP devices via TrackUI (value: `<TRACK_ADDRESS>:57501`)

3.6 Set Up Track

The Track backend can connect directly to the WLC through NETCONF. This direct backend connection is the preferred method for token refresh, BLE state recovery, and AP inventory synchronization. An external NETCONF client is only needed for manual troubleshooting, custom RPCs, or installations where the backend binding is not used.

Restart the Track backend after changing the certificate, private key, or any backend configuration.

3.6.1 Configure the Track backend

Configure gRPC and JWT settings Make sure that `gateway.jwt.secretKey` is set. It is configured in `/opt/prodtrac/config/credentials.xml`. If it is not set, generate a new key with:

```
openssl rand 256 | openssl enc -A -base64
```

Add or adjust the following options in `/opt/prodtrac/config/custom.xml`, replacing `TRACK_ADDRESS` with the IP address or hostname of the Track Service Host.

```
<entry key='gateway.jwt.grpcRetryIntervalSec'>120</entry>
<entry key='gateway.grpc.streaming.port'>57501</entry>
<entry key='gateway.grpc.autoAddDevicesAndBeacons.enable'>true</entry>
<entry key='gateway.jwt.tokenValidateEndpoint'>TRACK_ADDRESS:443</entry>
<entry key='gateway.jwt.grpcEndpointInvalid'>TRACK_ADDRESS:9</entry>
<entry key='gateway.grpc.server.cert'>/path/to/server.cert</entry>
<entry key='gateway.grpc.server.key'>/path/to/server.pkcs8</entry>
```

Configure NETCONF automation For detailed backend configuration possibilities, refer to the Track Administration Manual, section **Third-Party Gateways: gRPC- and JWT-Related Backend Configuration Options**. If you have not received a copy of the Track Administration Manual yet, please contact Safectory support.

Configure the WLC connection definitions and automation user-email mappings. They are stored in `/opt/prodtrac/config/credentials.xml`. Add the following entries for each WLC, using increasing indexes starting at `0`.

```
<entry key='gateway.netconf.auto.tokenRenew.userEmail'>TRACK_USER_EMAIL</entry>
<entry key='gateway.netconf.auto.apSync.userEmail'>TRACK_USER_EMAIL</entry>
<entry key='gateway.netconf.wlc.0.id'>wlc-1</entry>
<entry key='gateway.netconf.wlc.0.host'>WLC_HOST</entry>
<entry key='gateway.netconf.wlc.0.port'>830</entry>
<entry key='gateway.netconf.wlc.0.user'>WLC_USER</entry>
<entry key='gateway.netconf.wlc.0.password'>WLC_PASSWORD</entry>
```

The NETCONF automation user must be a Track user with the permissions required by the enabled jobs. A separate user created through the WLC frontend may be used for the NETCONF connection.

For new installations, add the following recommended settings to `/opt/prodtrac/config/custom.xml`:

```
<entry key='gateway.netconf.auto.enable'>true</entry>
<entry key='gateway.netconf.auto.tokenRenew.enable'>true</entry>
<entry key='gateway.netconf.auto.adminState.enable'>true</entry>
<entry key='gateway.netconf.auto.scanState.enable'>true</entry>
<entry key='gateway.netconf.auto.apSync.enable'>true</entry>
<entry key='gateway.netconf.auto.scheduler.intervalSec'>30</entry>
<entry key='gateway.netconf.auto.tokenRenew.intervalHours'>1</entry>
<entry key='gateway.netconf.auto.adminState.intervalHours'>0.0</entry>
<entry key='gateway.netconf.auto.scanState.intervalHours'>0.0</entry>
<entry key='gateway.netconf.auto.adminState.onStaleOnline.enable'>true</entry>
<entry key='gateway.netconf.auto.scanState.onStaleOnline.enable'>true</entry>
<entry key='gateway.netconf.auto.adminState.onStaleOnline.thresholdHours'>0.5</entry>
<entry key='gateway.netconf.auto.scanState.onStaleOnline.thresholdHours'>0.5</entry>
<entry key='gateway.netconf.auto.apSync.intervalHours'>24.0</entry>
```

Configure reliability and recovery The master switch and each individual job switch must be enabled for a job to run. Newer Cisco firmware can leave APs disconnected from BLE uploads even while the JWT remains valid. Periodic token renewal and BLE admin-state or scan-state resets can help APs recover, reconnect, and resume BLE transmission.

BLE messages are forwarded in batches and APs may reconnect periodically, so a few messages can occasionally be missed during reconnection. The setup provides robust positioning for typical use, but additional measures may be required for absolutely uninterrupted tracking. Configure the MEMS duration long enough to filter very short transients so that tamper-safe alarm capture remains consistent across reconnects. Events appear in Track after the connection is re-established, with a short delay sometimes possible before all recent events are shown. Site-specific tuning or additional infrastructure may be needed in particularly challenging environments.

For general beacon reachability and battery-level monitoring, a one-hour tolerance has proven reliable when AP-to-beacon connectivity is stable. Ensure stable AP-to-beacon connectivity by repositioning beacons or adding access points when necessary. The following settings are enabled by default and support beacon tracking and rate limiting:

```
<entry key="gateway.grpc.beaconTracker.enable">true</entry>
<entry key="gateway.grpc.rateLimit.beacons.enable">true</entry>
<entry key="gateway.grpc.rateLimit.buttons.enable">true</entry>
<entry key="gateway.grpc.rateLimit.beacons.maxdiff.sec">60</entry>
<entry key="gateway.grpc.rateLimit.buttons.maxdiff.sec">5</entry>
```

Using the beacon-tracker functionality is recommended to help avoid exceeding such deadlines.

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

This functionality is given and validated for Cisco IOS XE (17.3.1 + 17.6.1 + 17.9.3).

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).

You can enable iBeacon advertising via manual NETCONF (Method A) or Manual CLI (Method B). The backend NETCONF automation currently covers token renewal, BLE admin-state recovery, BLE scan-state recovery, and AP inventory synchronization, but not iBeacon advertising.

4.1 Method A: Manual NETCONF (Batched)

This setting is included in the manual NETCONF configuration described in Section Enable BLE Scanning (Method B). The backend NETCONF automation does not currently configure iBeacon advertising.

Note on NETCONF Configuration: If you want to adjust the access points' triplets (i.e., UUID, major, and minor), you need to adjust them in the **Beacon** window in TrackUI, re-generate the XMLs via `/api/netconf` endpoint, and then execute the RPCs.

4.2 Method B: Manual CLI (Per AP)

To enable iBeacon advertising manually, use the following command structure (must be entered as a single line):

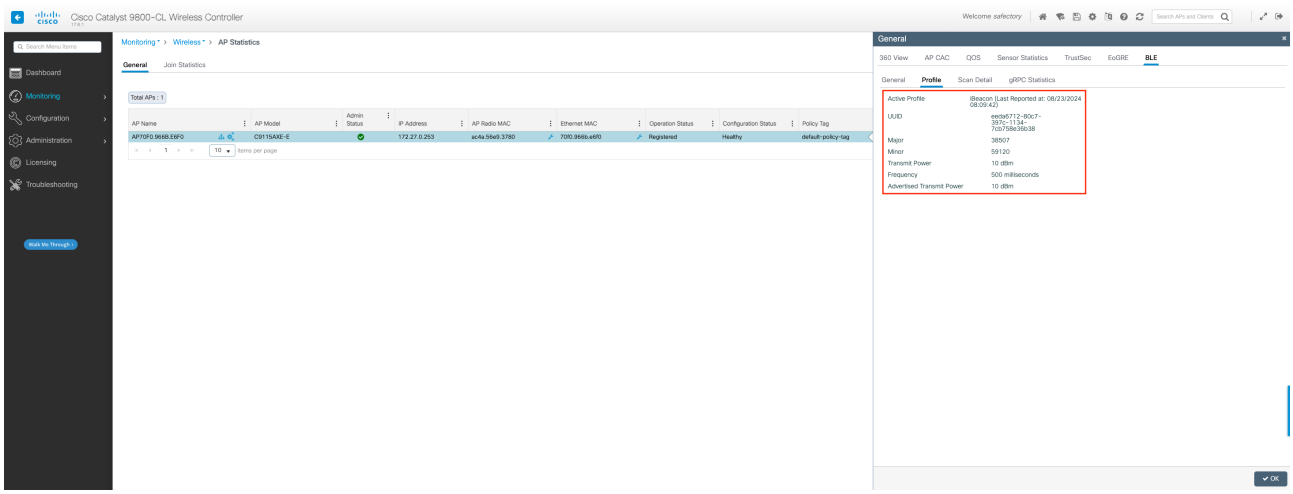
```
ap name <ap-name> ble ibeacon uuid <uuid>
      major <major> minor <minor> tx_power <tx_power>
      frequency <frequency> advertised_tx_power <advertised_tx_power>
```

Example:

```
WLC#ap name AP70F0.966B.E6F0 ble ibeacon
      uuid eeda6712-80c7-397c-1134-7cb758e36b38
      major 38507 minor 59120 tx_power 10
      frequency 500 advertised_tx_power 10
```

Note: The command is displayed across multiple lines for readability. It must be entered as a single line.

Result:

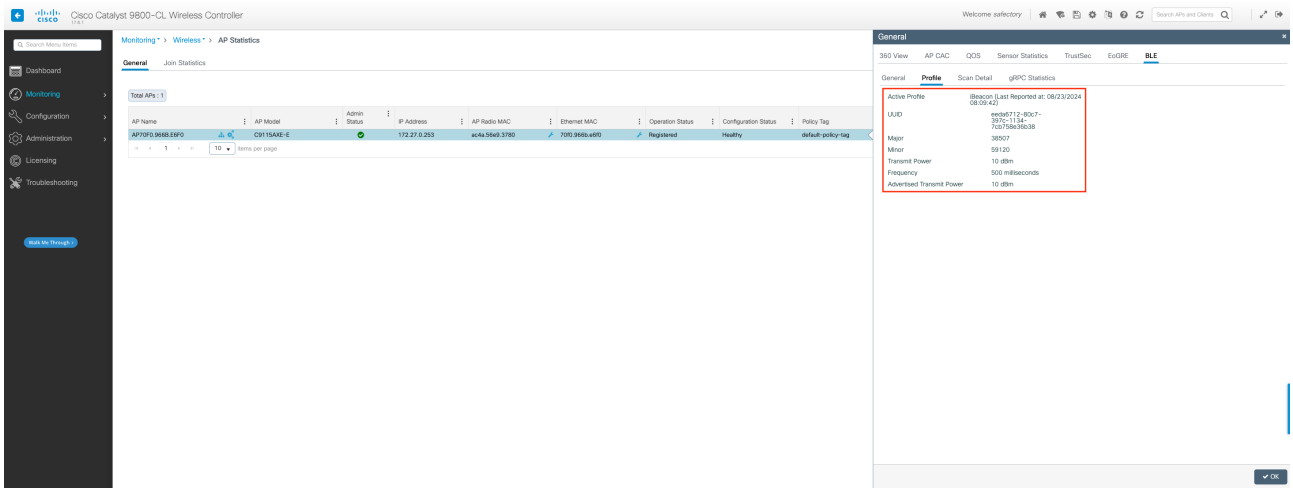


To disable it: `ap name <ap-name> ble no-advertisement`

Example:

```
WLC#ap name AP70F0.966B.E6F0 ble no-advertisement
```

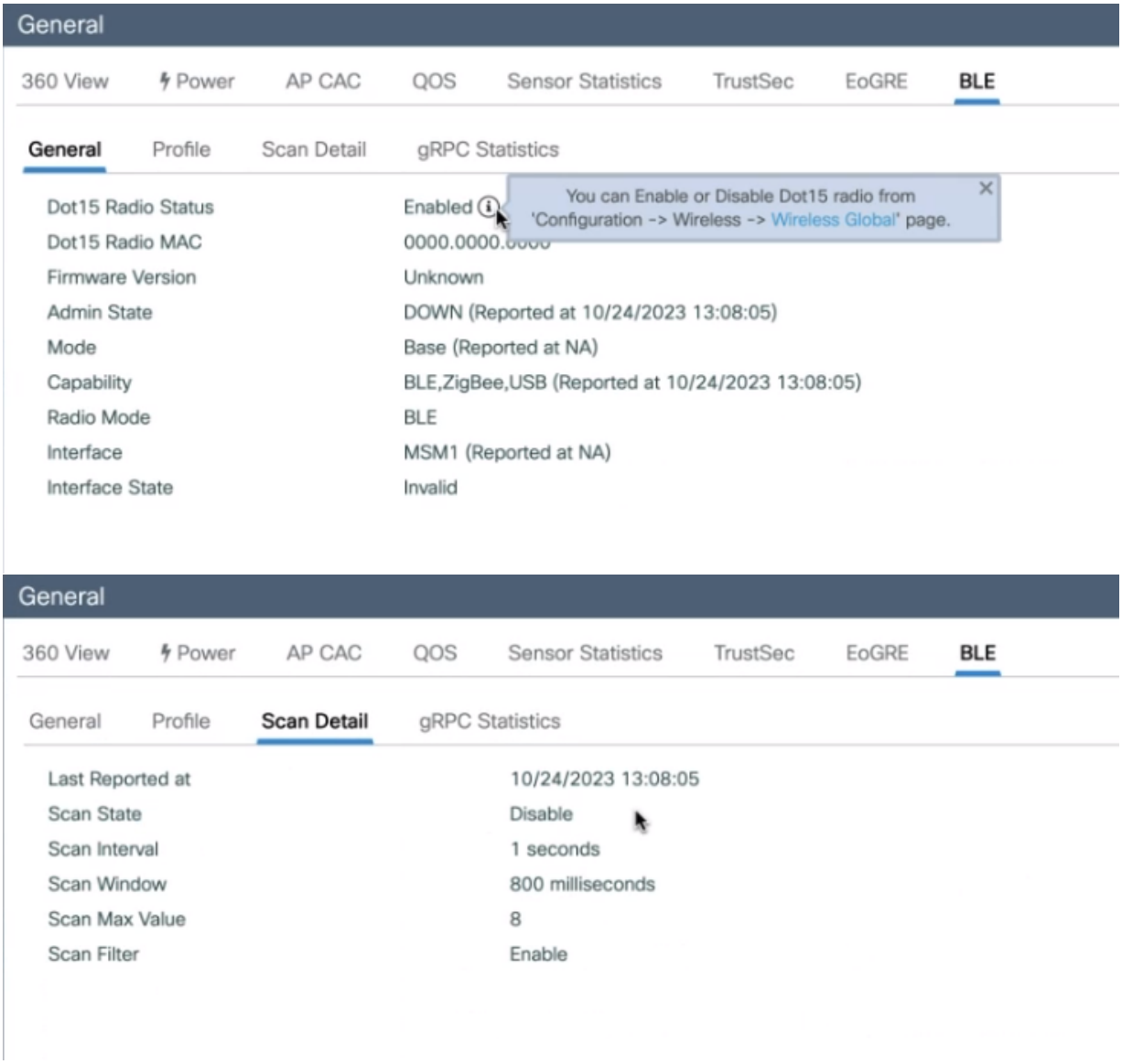
Result:



5 Troubleshooting

The following troubleshooting section may help to solve various error situations. Note that there is also an official Cisco troubleshooting guide available at https://www.cisco.com/c/en/us/td/docs/wireless/spaces/iot-services-wireless/b_iot_services/m-trb-wlc.html, which contains further hints.

1. When in doubt that the token was accepted by the WLC:
   - Check output of following CLI commands on WLC whether the token was actually set: `show configuration | include token` and `show running-config | include dna`
   - Check output of following CLI command on one of the APs whether they received the `dnas-config` config and if the token was updated (this may also show if there is a problem with the certificate): `enable` (requires to enter SSH password one more time), followed by `show grpc server log`
   - For additional gRPC diagnostics on an AP, use `show grpc collector-config` and `show grpc connection`.
   - On some IOS XE versions, `show grpc server log` may not return the expected output. In that case, try `show grpc log` instead.
   - If a token set on the WLC appears to be stuck and cannot be replaced, reboot the affected APs and try again. This appears to be a Cisco WLC firmware bug.
2. It 1) is not possible to adjust BLE filtering (function seems to be non-functional) and/or 2) scan state is disabled and BLE radio is enabled but shows an invalid MAC address and unknown firmware version:



Suggestion: Make sure that the admin state is included in the NETCONFIG RPCs with `ble-admin-state-on` (requires `&configsEnabled=ble-mgt-admin-req` to be part of the endpoint address, cf. Enable BLE Radio (Scanning)), example:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <ble-mgt-admin-req xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ble-mgmt-cmd-rpc">
    <state>ble-admin-state-on</state>
    <ap-name>AP70F0.966B.E6F0</ap-name>
  </ble-mgt-admin-req>
</rpc>
```

3. gRPC server (of Track service) does not start up
   - Make sure that permissions and ownerships for certificate and private key are correct
   - Make sure that file paths to the certificate and private key are correct (backend config + Nginx)
   - Make sure that the key file is passwordless
   - Check backend log files for any related error messages (log files of interest: `application.*`, `grpc.*`, `bledataparser.*`)