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

safectory GmbH

1 Preamble

1.1 Terms of use

Subject to technical modification without notice.

Errors and omissions excepted.

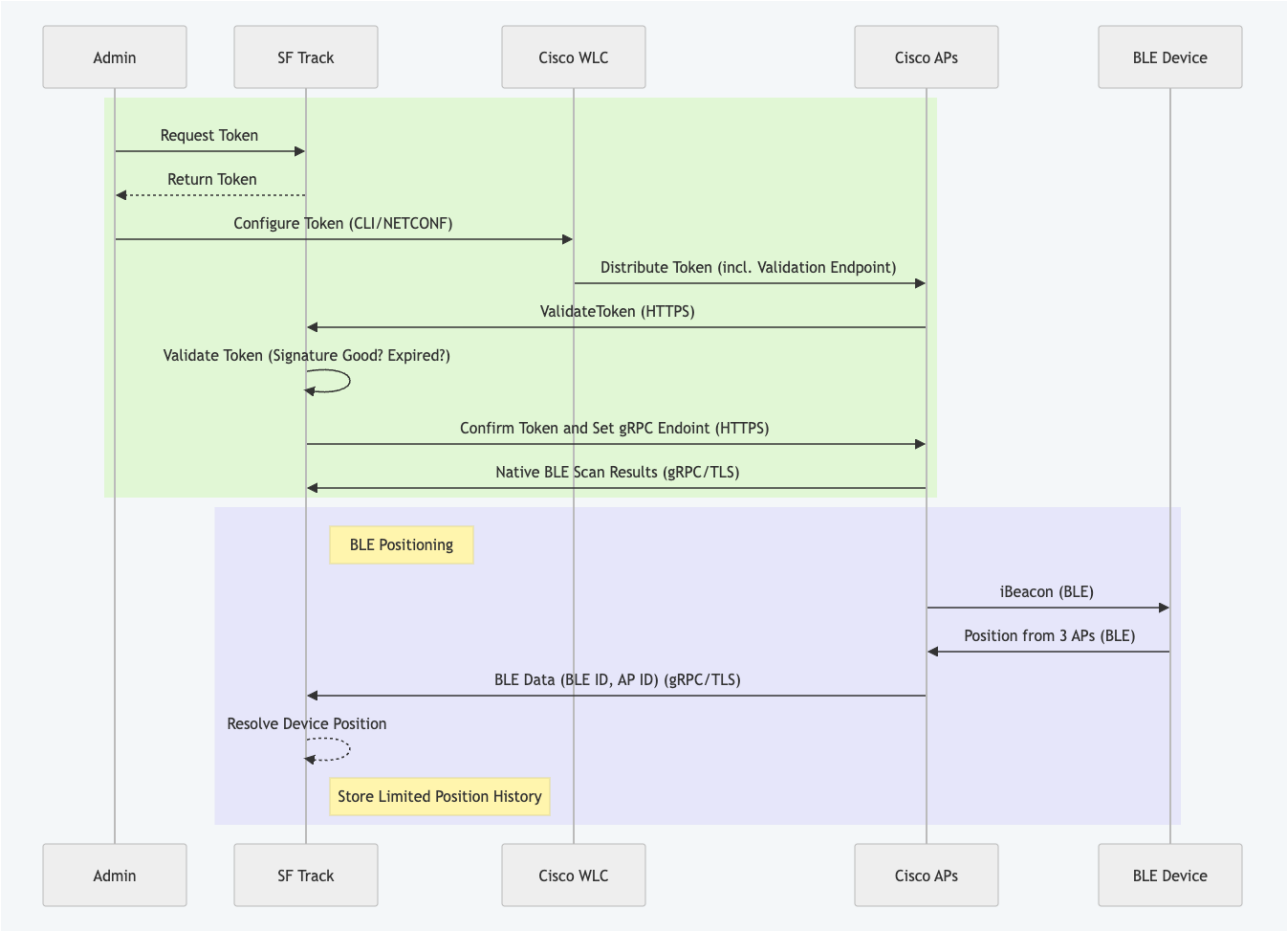
For further information regarding legal and proprietary statements, please go to our GENERAL TERMS AND CONDITIONS at https://safectory.com/gtc/.

1.2 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 1.17.3+
  - SF backend versions approved: 1.17.+
  - Minimal gRPC version: 1.11.0

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).

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 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`

3.4 Set Up Track

- Make sure that `gateway.jwt.secretKey` is set in `/opt/prodtrac/config/credentials.xml`, otherwise generate a new key via `openssl rand 256 | openssl enc -A -base64`
- Add/adjust those backend config options to/in `/opt/prodtrac/config/custom.xml` (make sure to replace `TRACK_ADDRESS` with the IP address or hostname; `server.{cert,pkcs8}` are the files generated in Set Up Certificate + PKCS#8 Key, whose paths need to be adjusted in the backend config):

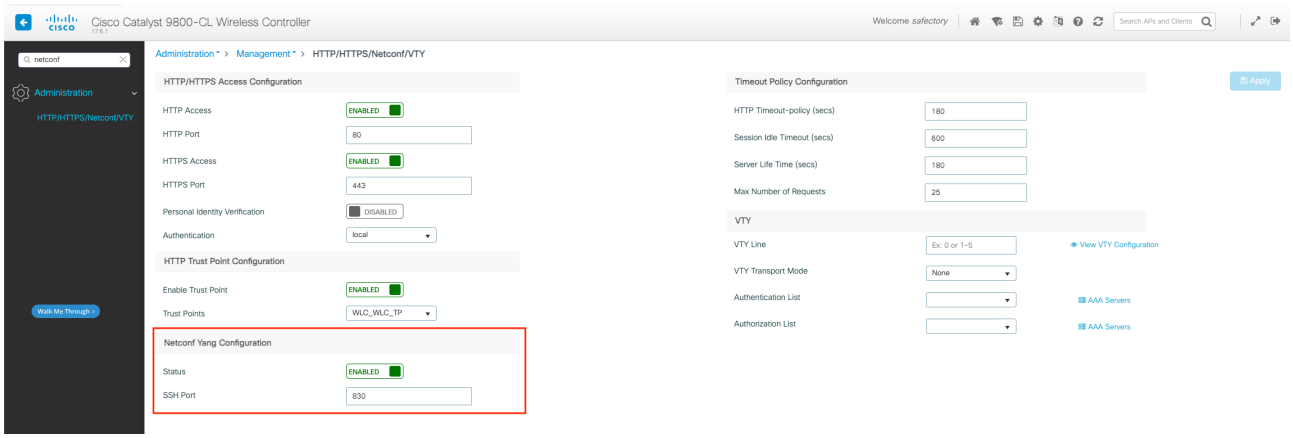
```
<entry key='gateway.jwt.grpcRetryIntervalSec'>120</entry>
<entry key='gateway.grpc.streaming.port'>57501</entry>
<entry key='gateway.grpc.autoAddDevicesAndBeacons.enable'>true</entry>

<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>
```

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>
```

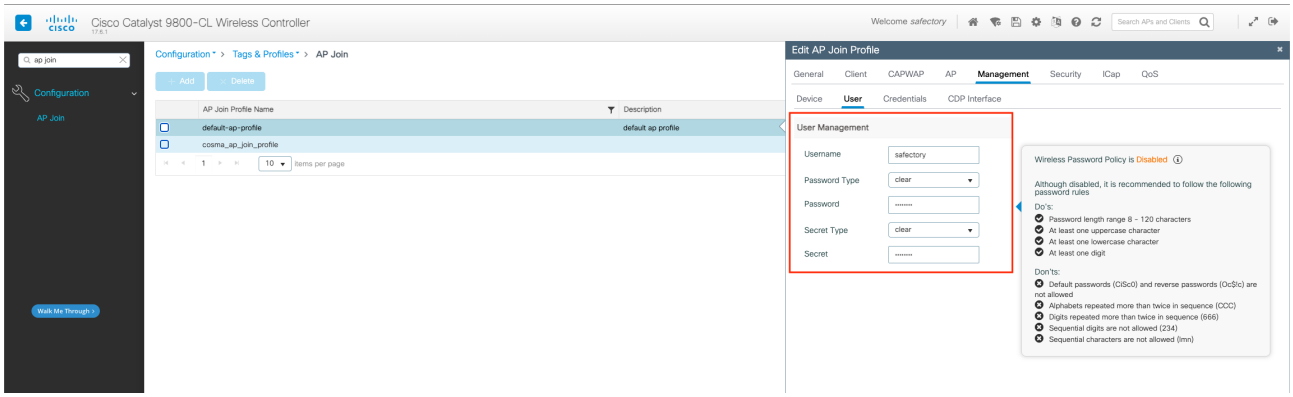
Check that the output contains the following modules (usually found within the `<capability>` tags):

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

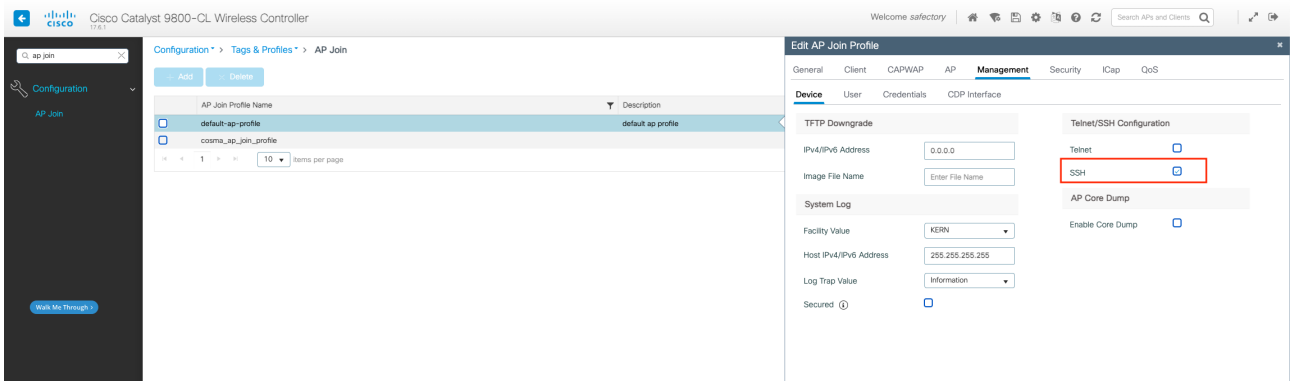
3.5.3 Enable SSH Access via Web UI on WLC and APs

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 Setting up a NETCONF Client (Example: Cisco YANG Suite)

A NETCONF client is required to interact with Cisco IOS XE to enable features such as BLE scanning or beaconing and to distribute a Java Web Token (JWT) for successful authentication and communication between access points and the Track service.

While this guide demonstrates using **Cisco YANG Suite** [https://developer.cisco.com/yangsuite/] (a web-based NETCONF client), you may use alternative NETCONF clients such as the `netconf-client` Python library or other compatible tools.

The Track service will generate XML elements that are executed as RPCs via your chosen NETCONF client.

The following procedures were tested on Ubuntu 20.04.2 LTS.

Install YANG Suite (Debian-based distribution assumed) Please ensure that you have a machine with direct WLC access, then install the suite as described on following resources:

- https://developer.cisco.com/docs/yangsuite/#!welcome-to-cisco-yang-suite/docker-based-installation
- https://github.com/CiscoDevNet/yangsuite

For the next steps, a successful installation is assumed, which allows you to log in to the YANG Suite web frontend.

Configure YANG Suite Navigate (left menu bar) to **Setup** > **Device profiles** > Set up new device by

- giving it a name (e.g., `WLC`)
- entering the WLC's IP address (e.g., `172.27.0.121`)
- entering credentials (e.g., `safectory` / `secretpassword`)
- selecting **Skip SSH key validation for this device** in device settings
- making sure that the correct type is selected for NETCONF (i.e., `Cisco IOS XE`)
- testing the config and confirming (green) checkmarks for NETCONF and "Ping" when hitting the **Check connectivity** button

Running an RPC via NETCONF / YANG Suite An XML RPC can be executed by

1) navigating (left menu bar in YANG Suite) to **Protocols** > **NETCONF**
2) selecting a device (e.g., `WLC`)
3) pasting one or more XML elements into the text field on the right and hitting **Run RPC(s)**

Note:

- It is **neither** necessary to select a **YANG Set** nor any **Module(s)** nor a **NETCONF Operation** to successfully execute RPCs (because the XML elements contain all information needed to execute them).
- Loading modules etc. is only required if you want to display the **YANG Tree**, which can be useful to generate custom XML RPCs via YANG Suite (**Build RPC** button).

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.

You can perform this step manually as part of the bulk configuration via NETCONF (Method A) or via CLI (Method B).

Method A: NETCONF (Batched, recommended)

The setting is included in the bulk NETCONF configuration described in Section Enable BLE Radio (Scanning). If you choose that method, you can skip repetitive manual AP setup steps.

Method B: Manual CLI (Per AP)

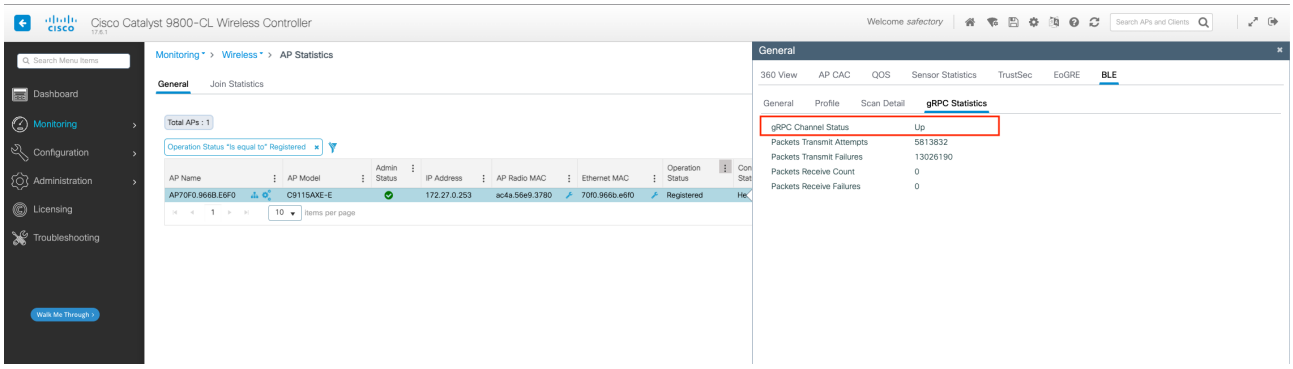
The following steps can be done via CLI per AP:

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:

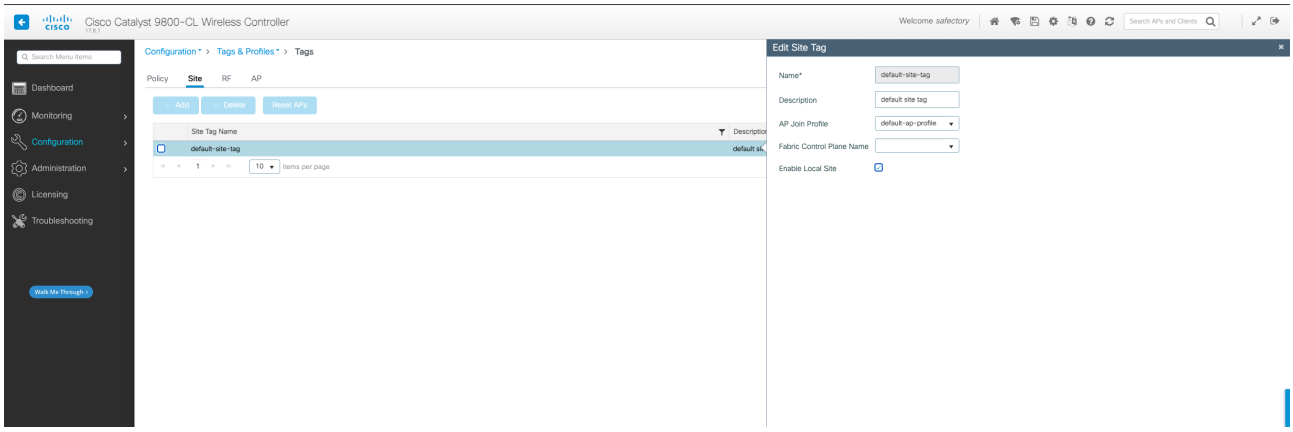
1) Log in via SSH
2) Type `configure terminal`
3) Type `ap profile <ap-profile-name>` (replace `<ap-profile-name>` appropriately)
4) Type `cisco-dna grpc`
5) Verify **gRPC Channel Status** is **Up** via web UI
   - Navigate to **Monitoring** > **Wireless** > **AP Statistics**
   - Select an AP
   - Switch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

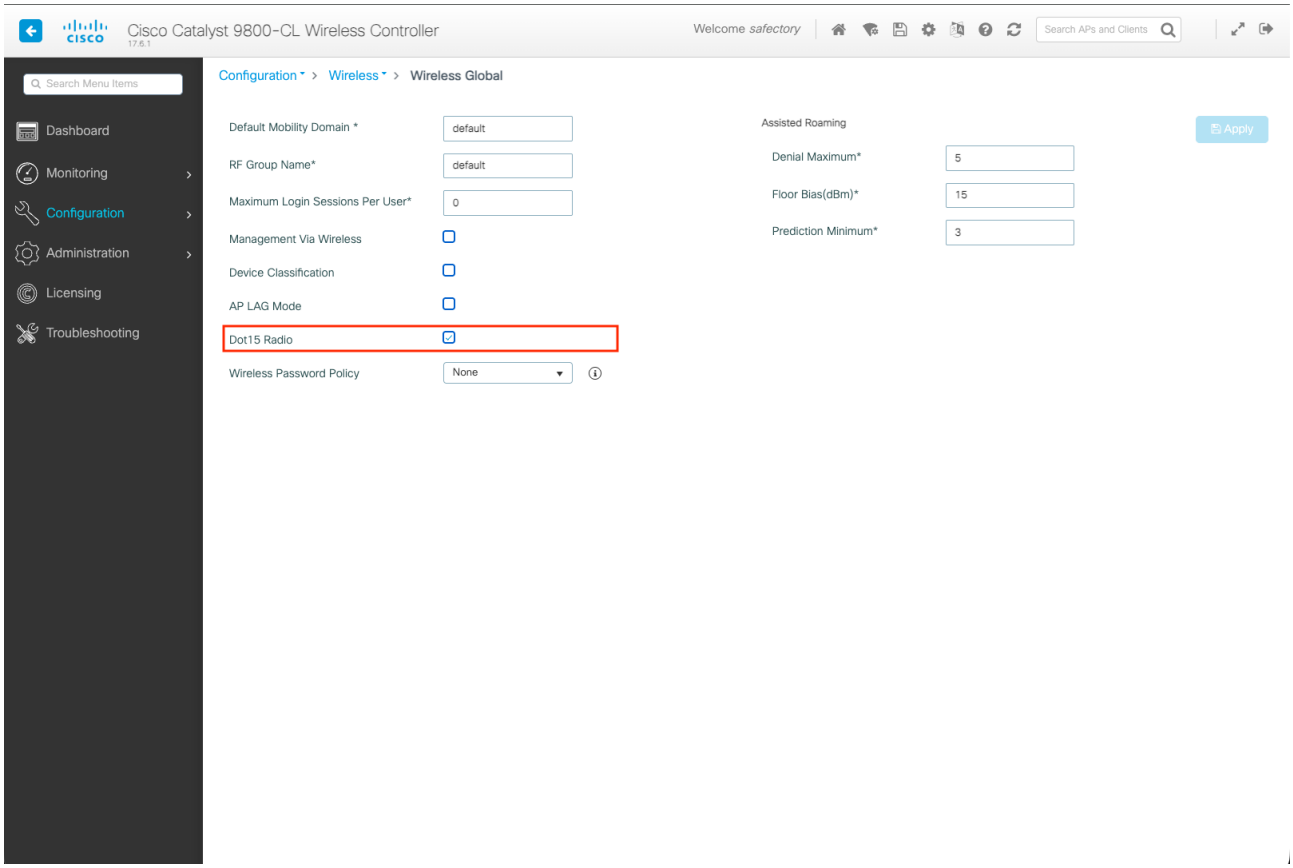


3.5.8 Enable BLE Radio (Scanning)

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 You can enable BLE scanning via NETCONF (Method A) or Manual CLI (Method B).

Method A: NETCONF (Batched)

To enable BLE scanning (and other features) via NETCONF, get output from Track service and execute as follows.

- 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 NETCONF RPC via YANG suite (w/o `<CONFIGURATION>` start and end tag), see paragraph **Running an RPC via NETCONF / YANG Suite**

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 B: Manual CLI (Per AP)

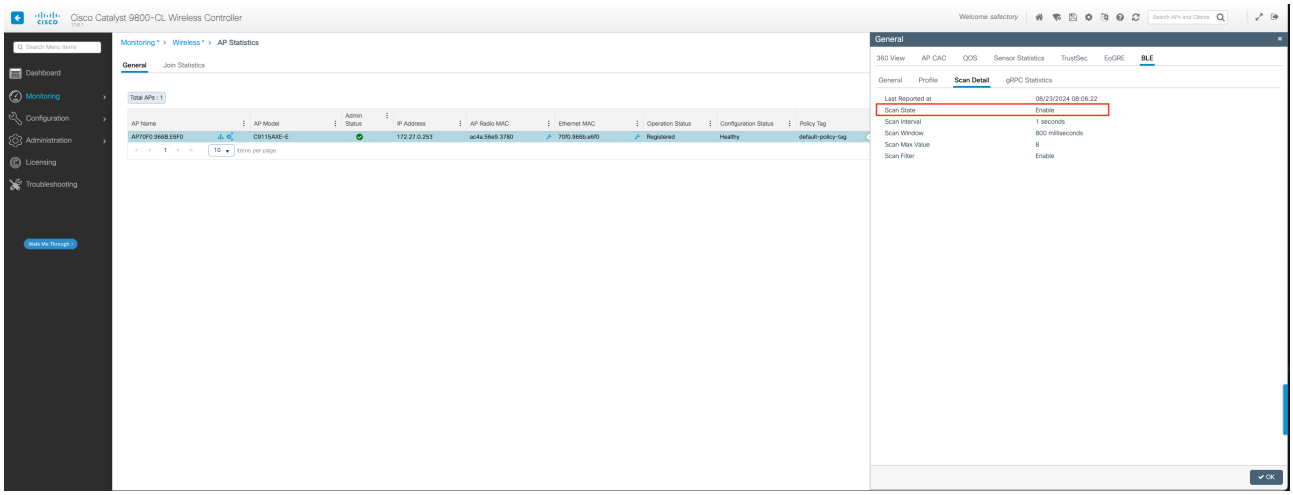
To enable BLE scanning manually, use the following command (substitute `<ap-name>` with your AP's name):

```
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):



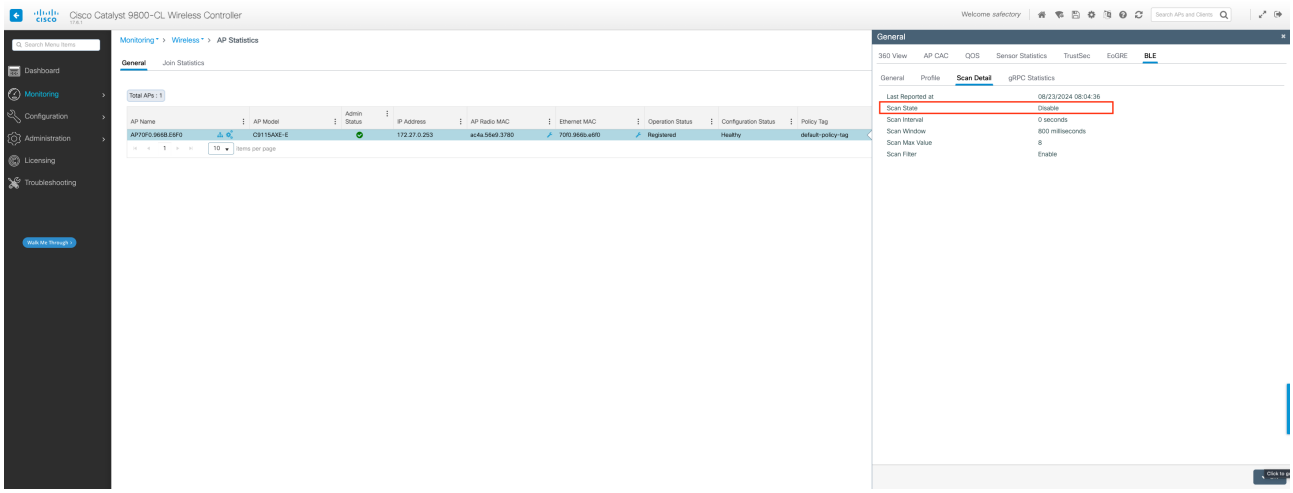
To disable it:

```
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 is required to authenticate the APs against the Track backend (via gRPC) and authorizes them to upload scanning data.

To distribute a new token (JWT), get output from Track service and execute via CLI as follows:

- **Generate JWT**: https://TRACK_ADDRESS/api/streaming/token/generate → returned value from key `streamAccessKey` needs to be inserted for `<token>` in next step (w/o 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`)

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 NETCONF (Method A) or Manual CLI (Method B).

4.1 Method A: NETCONF (Batched)

This setting is included in the bulk NETCONF configuration described in Section Enable BLE Scanning (Method B).

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):

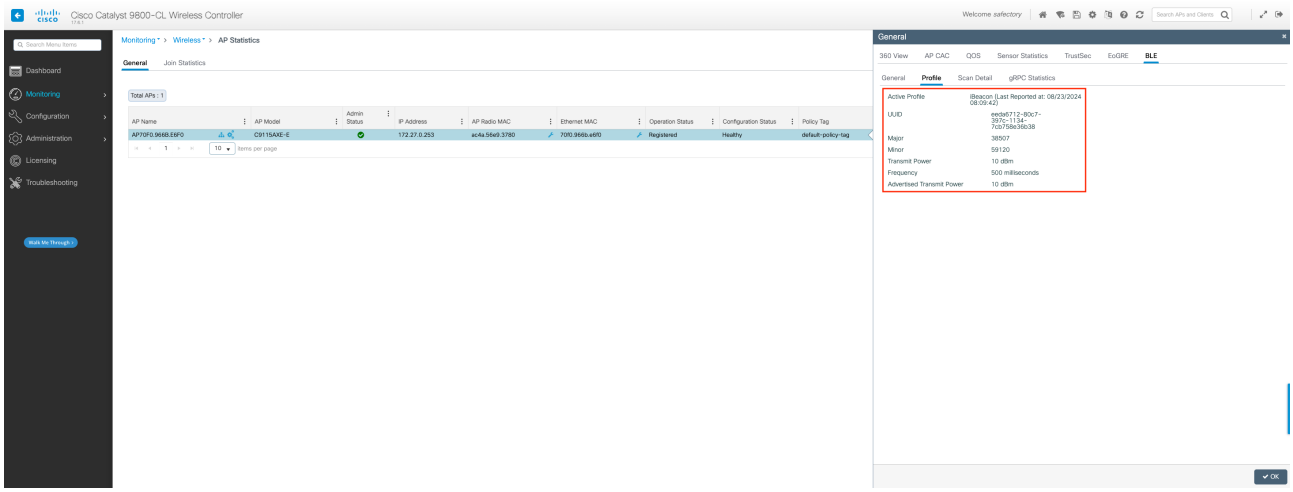
```
ap name <ap-name> ble ibeacon uuid <uuid>
      major <major> minor <minor> tx_power <tx_power>
      frequency <frequency> advertised_tx_power <advertised_tx_power>
```

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:

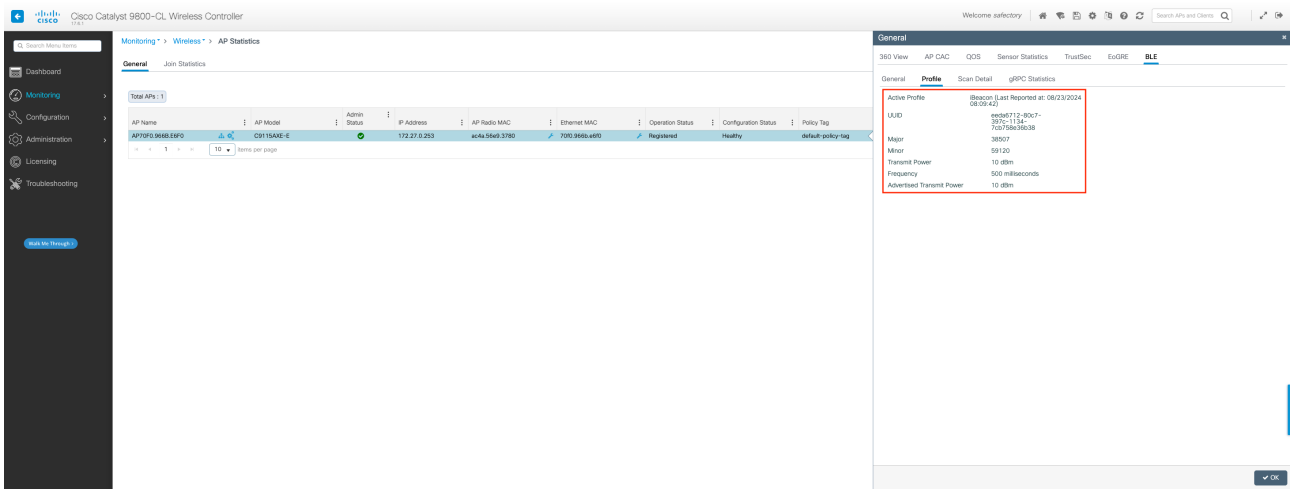


To disable it: `ap name <ap-name> ble no-advertisement`

Example:

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

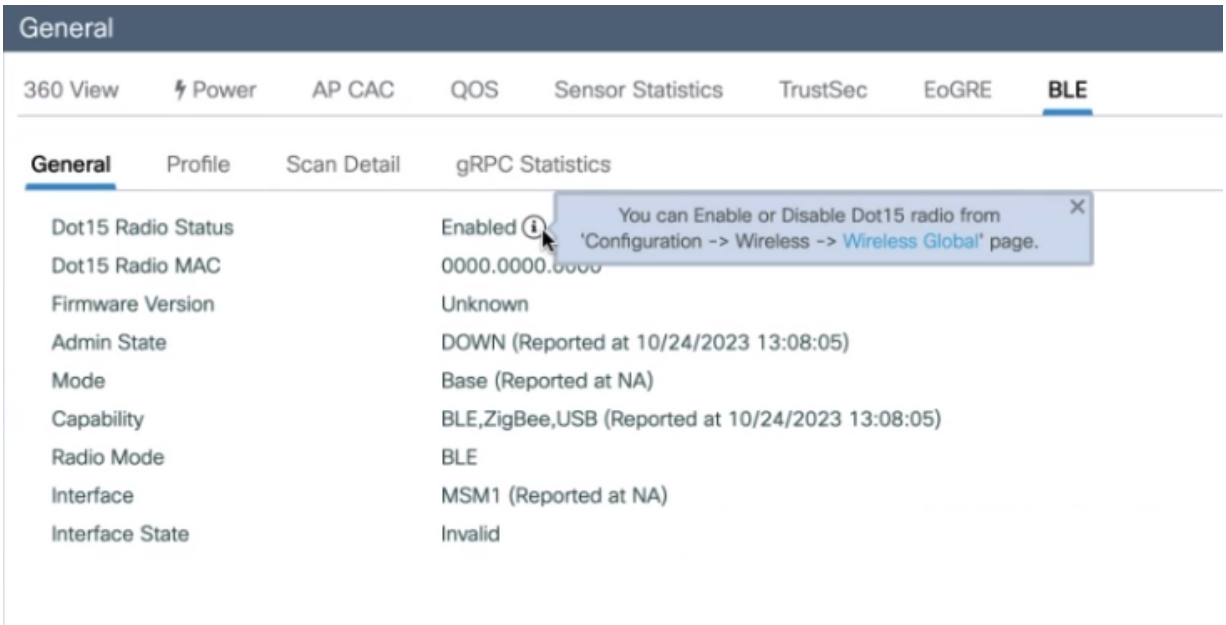
Result:

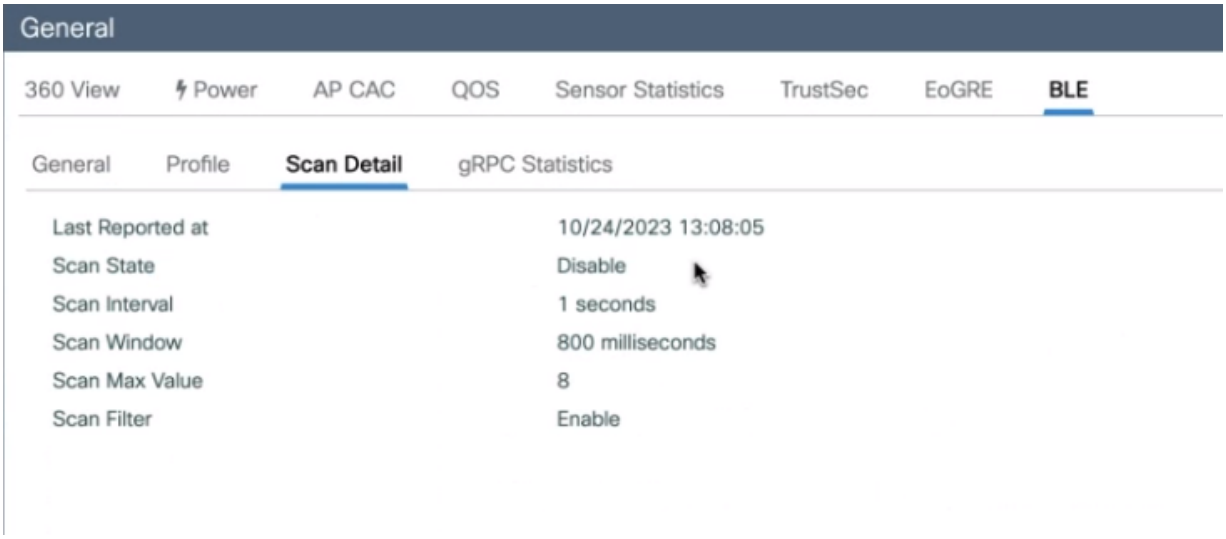


5 Troubleshooting

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`
2. Bad request (400) when trying to launch YANG Suite
   - Possible solution: When running it locally only, use IP address instead of a hostname for YANG Nginx webserver
3. 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>
```

4. 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.*`)

6 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