

Cisco Spaces: IoT Service Configuration Guide (Wireless)

First Published: 2020-08-31

Last Modified: 2026-08-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I **About IoT Services** 9

CHAPTER 1 **Cisco Spaces: IoT Service (Wireless)** 1

Overview of Cisco Spaces: IoT Service (Wireless) 1

Components of Cisco Spaces: IoT Service 2

Compatibility Matrix for IoT Service (Wireless) 5

IoT services old Vs new UI 7

CHAPTER 2 **Prerequisites** 11

Prerequisites of IoT Service (Wireless) 11

Cisco Spaces: Connector Scale and Size Guidance for IoT Service 11

Prerequisites 12

Before activating IoT services 13

CHAPTER 3 **Getting Started** 17

Activate IoT Service (Wireless) 17

Enable IoT service on Connector2 22

Verify Cisco Spaces: Connector is Added and Active 22

Verify Cisco Catalyst 9800 Series Wireless Controllers is Added and Active 23

Configure connector for gRPC and certificate services 23

Enable BLE on AP 27

Set AP in advanced mode 28

Verify access points 29

CHAPTER 4 **Open Ports** 33

Information About Open Ports (Wireless) 33

PART II **Inventory** 35

CHAPTER 5 **Inventory** 37

Inventory 37

Configure wireless APs 38

Configure wired switches 39

Configure claimed devices 40

PART III **Manage** 45

CHAPTER 6 **Dashboard** 47

Dashboard view of devices 47

Configuring beacons 47

CHAPTER 7 **Wireless APs** 49

AP Gateways 49

Configure AP gateways 49

AP Beacons 54

iBeacon transmit mode 55

Configure AP as a beacon in scan mode 56

Configure AP as a beacon in transmit mode 58

Configure AP as a beacon in dual mode 61

AP Sensors 65

Enable or disable an AP sensor 66

View sensor information 69

CHAPTER 8 **BLE Devices** 71

Discover beacons 71

Claim a beacon 74

Configure a beacon on IoT Service 77

View sensor information 82

CHAPTER 9 **Wired** 85

Wired Gateways 85
Configure wired gateways 85
Wired Sensors 91
Configure wired sensors 91
Smart PDUs 94
Configure smart PDUs 94

PART IV Device Monitoring 99

CHAPTER 10 Monitoring 101
Right now 101
BLE devices battery life 101
Last heard BLE devices 102

PART V Settings 105

CHAPTER 11 Settings 107
Device filtering 107
Categorize devices into manual groups 108
Categorize devices into dynamic groups 109
Configure onboarding and nearby interaction settings 111

PART VI Troubleshooting 113

CHAPTER 12 Troubleshoot IoT services: controller 115
Reprovisioning IoT services after failover 115
What settings are needed to allow access via NETCONF? 115
The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting? 116
For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token? 116
gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled? 117
How do I verify gRPC is up? 117

How do I verify that TDL subscriptions are created and are valid? 118
Are the TDL subscriptions created and valid? 118
What is the TDL status? 118
How do I view the current CAPWAP values for an AP? 119
How do I view the current TDL values for an AP? 127
How do I get the telemetry connection status? 130
How do I view IOx AP state and mode? 130
How do I view gRPC details? 131
How do I view AP BLE configuration details? 131
How do I view the current TDL values for AP air quality? 133
How do I view the current TDL values for AP temperature and humidity? 134

CHAPTER 13 **Troubleshoot IoT services: IOx application** 135
How do I verify the IOx application is running on the AP? 135
How do I debug the IOx application installation failure? 135
How do I verify the IoX Application AP bundle download from Cisco Spaces? 136
How do I start an interactive shell session for the IOx application? 136
How can I see the logs for the IOx application? 137
How do I monitor metrics in the IOx application? 137
How do I monitor BLE scans in the IoX Application? 139
What files exist in the IOx application? 141

CHAPTER 14 **Troubleshoot IoT services: Cisco Spaces connector** 143
What are the metrics available on the Connector GUI for IoT Service (Wireless) ? 143
What are the log files created on the Connector for IoT Service (Wireless)? 144

CHAPTER 15 **Troubleshoot IoT services: access point** 145
How do I check the gRPC connection status on the access point? 145
How do I check the stream token on the access point? 145
How do I view the gRPC server logs on the access point? 146
How do I view the beacons scanned by an access point running in Native mode? 147
How do I view the beacon broadcast setting for an access point running in Native mode? 147

PART VII **Appendix** 151

CHAPTER 16 Cisco Catalyst 9800 Series Wireless Controller 153

Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower) 153

Disable Assurance with iCAP using CLI (Versions 17.3.1 or lower) 154

Disable iCAP using WEBUI (Versions 17.3.2 or higher) 155

Disable iCAP using CLI (Versions 17.3.2 or higher) 156

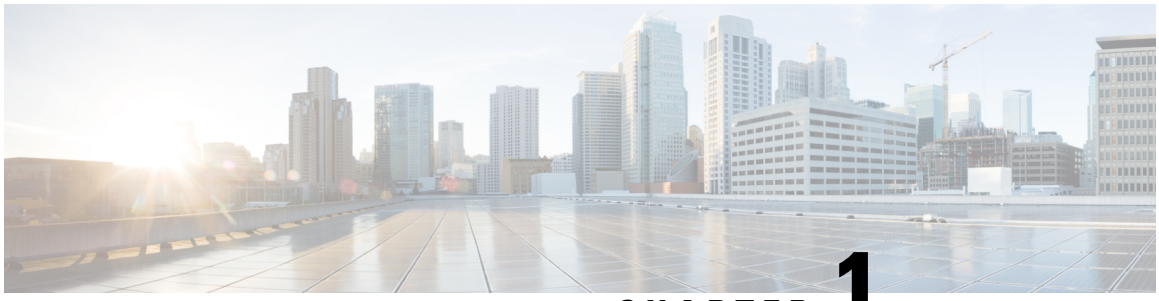
Enable or Disable iCAP or Assurance using DNAC (Versions 17.3.2 or higher) 157



PART I

About IoT Services

- **Cisco Spaces: IoT Service (Wireless)**, on page 1
- Prerequisites, on page 11
- Getting Started, on page 17
- Open Ports, on page 33



CHAPTER 1

Cisco Spaces: IoT Service (Wireless)

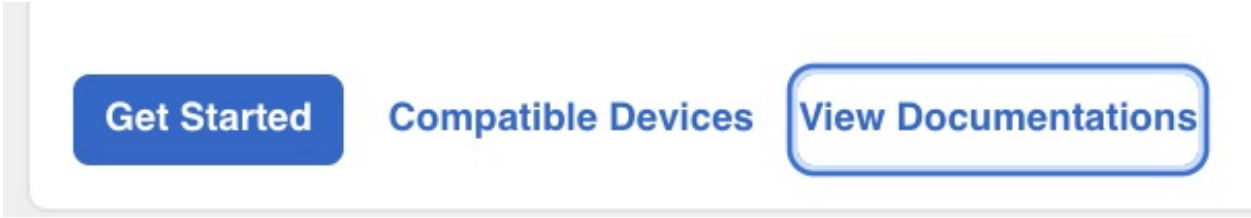
- Overview of Cisco Spaces: IoT Service (Wireless), on page 1

Overview of Cisco Spaces: IoT Service (Wireless)

Cisco Spaces: IoT Service (Wireless) is a platform service within Cisco Spaces that enables you to claim, manage, and monitor IoT devices using Cisco's wireless infrastructure. IoT Service is designed to enable management of IoT devices across vendors, form factors, and technology protocols. Bluetooth Low Energy (BLE) is the first technology available for management using IoT services.

IoT service (wireless) encompasses hardware, software, and partner components to enable the management of devices that support critical business outcomes. IoT service (wireless) uses Cisco Catalyst 9800 Series Wireless Controllers, Cisco Spaces: Connector, Cisco Wi-Fi6 access points, and Cisco Spaces. IoT service (wireless) adopts a next-generation approach to manage complexity in an enterprise environment.

Figure 1: Spaces IoT in a nutshell tab options



Click the **Get Started** button to learn more about getting started. This action redirects to the Cisco Spaces: IoT Service Configuration Guide (Wireless).

Click the **Compatible Devices** button to view the list of supported devices. This action redirects to the Cisco Spaces IoT Device Marketplace website.

Click the **View Documentation** button to see how to set up the product. This action redirects to the Cisco Spaces Setup Guide.

Using the IoT service (wireless), you can perform these IoT management activities:

- Deploy BLE gateways on supported APs in your network.
- Claim the BLE beacons that you acquired from Cisco Spaces: IoT Device Marketplace.
- Configure APs and manage floor beacons.

- Monitor device attributes such as location, telemetry, battery status, and movement status.

The section **Outcome Apps** describes these two sections:

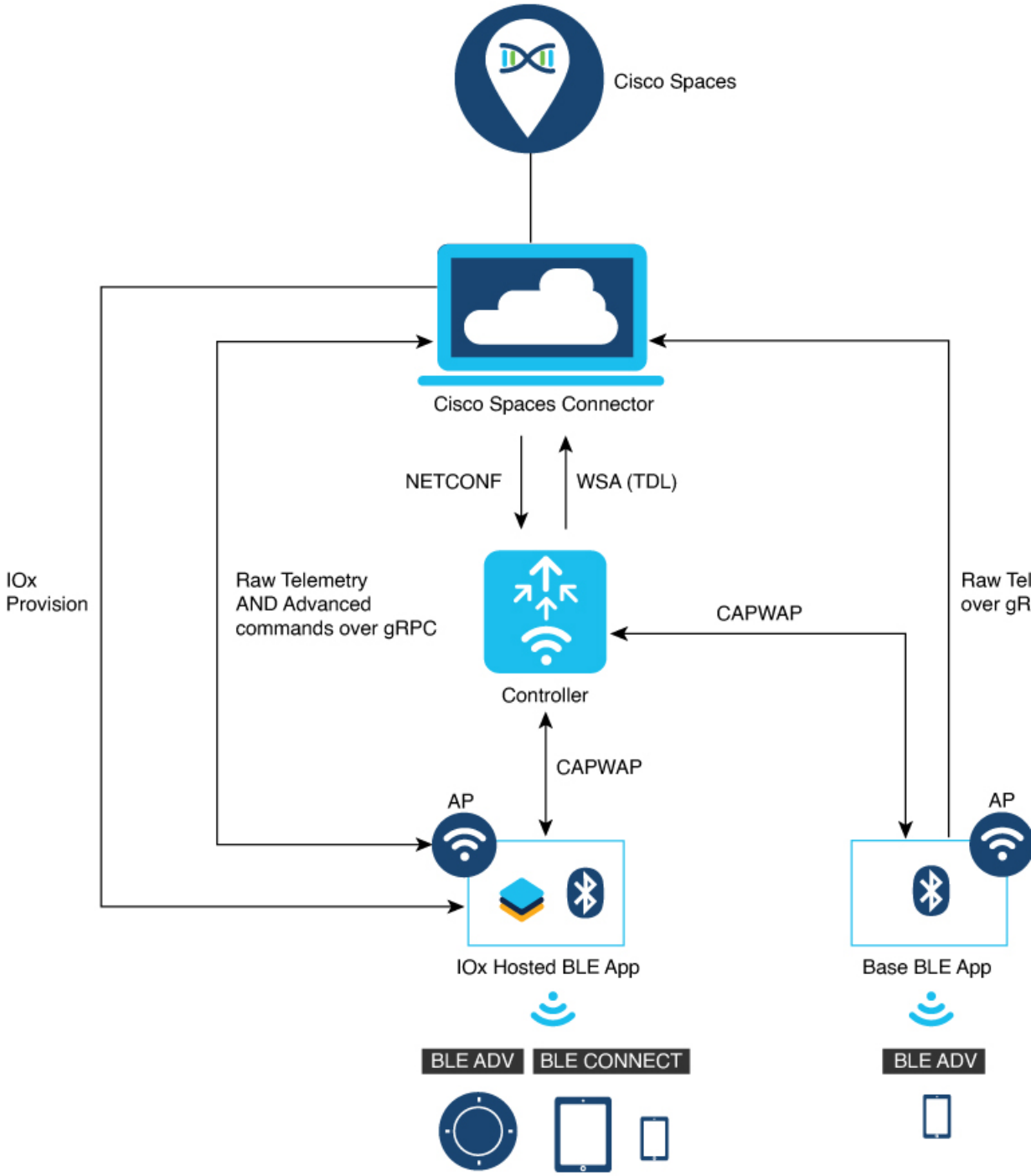
1. **Smart Workspaces**: Smart Workspaces helps you prepare your workspace for hybrid work. Click on the **Know More** button to visit the Cisco Spaces: Smart Workspaces page.
2. **Detect and Locate**: Detect and Locate simplifies IoT with eBLE technology powered by Cisco Spaces. Click on the **Know More** button to visit the Cisco Spaces: Detect and Locate page.

Components of Cisco Spaces: IoT Service

The section describes the various components that work to complete the Cisco Spaces: IoT Service solution.

The Cisco Catalyst 9100 Series Family of Access Points acts as a gateway of communication between Cisco Spaces and the IoT devices. Cisco Spaces: IoT Service can then use a range of common APIs to communicate with edge devices and apps. The Cisco Spaces: IoT Service collects data from devices and apps, and passes it to Cisco-partnered websites that manage these devices far more extensively (referred to in this document as Device Manager websites). These Device Manager websites can use edge-device signals to enable outcomes specialized and targeted for each industry.

Figure 2: Components of IoT Service



Access Points

You can configure access points as gateways in Cisco Spaces. You can find the list of supported APs in the **Compatibility Matrix** section.

Depending on your Cisco AP model, configure the AP as one of these types of BLE gateways:

- **Base BLE Gateway**: This is an AP that does not run Cisco IOx App. You can configure this AP in **Scan**, **Transmit**, or **Dual** mode.
- **Advanced BLE Gateway**: This is an AP installed with the Cisco IOx App. The Cisco IOx App brings the ability to connect, configure, and manage third-party BLE floor beacons using the Cisco Spaces dashboard. Moreover, the Cisco IOx App can be used to perform additional BLE filtering on the AP. You can configure this AP in **Scan**, **Transmit**, or **Dual** mode.

Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controller (Catalyst 9800 controller) combines RF excellence with Cisco IOS-XE benefits, and comes in physical or virtual form factor. This wireless controller is reliable and highly secure. You can manage this Catalyst 9800 controller using CLI, GUI, NETCONF, Yang, or the Catalyst Center.

The Catalyst 9800 controller is the single point for configuring and managing a wireless network and access points. The Catalyst 9800 controller configures and manages APs using the CAPWAP protocol.

The Catalyst 9800 controller receives BLE configuration from Cisco Spaces over NETCONF and passes the configuration to AP over CAPWAP. The feedback path from the AP to the wireless controller is through CAPWAP, and from the Catalyst 9800 controller to Cisco Spaces through Telemetry data logger (TDL) telemetry streaming. The gRPC configuration from Cisco Spaces also goes through the Catalyst 9800 controller, and from there to the corresponding AP. The configuration sets up the gRPC channel between the AP and Cisco Spaces. The AP sends the gRPC channel statistics to the Catalyst 9800 controller, and you can view these statistics on the Catalyst 9800 controller.



Note

- You can have only one gRPC session between an AP and connector.
- Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Amsterdam 17.3.x supports only one of the following:
  - IoT service (wireless) with Cisco Spaces.
  - Network Assurance solution on Catalyst Center using Intelligent Capture (iCAP)

IoT service (wireless) and Intelligent Capture (iCAP) can co-exist from Cisco IOS XE Cupertino 17.7.x or higher.

Cisco Spaces: IoT Device Marketplace

Cisco Spaces: IoT Device Marketplace is a platform where you can discover, research, and purchase IoT devices. IoT Device Marketplace is a part of the Cisco Spaces full-stack partner ecosystem. Each device is preconfigured to give the customer an out-of-the-box experience with sensors, tags, wearables, and more. All the devices are compatible with the applications in the App Center. Current devices in the IoT Device Marketplace leverage BLE to transmit telemetry, with plans to add other technology in the future, such as Ultra Wide Band (UWB) and Zigbee.

Cisco Spaces: Connector

Cisco Spaces: Connector allows Cisco Spaces to communicate with more than one

- Cisco AireOS Wireless Controllers, and
- Cisco Catalyst 9800 Series Wireless Controllers.

APs connect to connector using the gRPC framework.

The APs establish a connection to connector using the gRPC protocol. The gRPC protocol configures floor beacons and receives telemetry data from the floor beacons. gRPC is a bidirectional streaming service, and requires a certificate to validate the host connection and a token for authentication. Each AP creates a gRPC connection. Connector can thus support many simultaneous connections.

Compatibility Matrix for IoT Service (Wireless)

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.9.6 or 17.12.4 • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA) **Note** This support is conditional, and dependent on whether you have applied the fix described in CSCwk66790
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	3.x and later
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1 and later
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later

Application Name	Support for Cisco Spaces: IoT Service
Access Points for advanced BLE gateway (Wi-Fi 6)	• Cisco Catalyst 9105 Series Access Points • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9136 Series Access Points • Cisco Catalyst 9162 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 Series Access Points • Cisco Aironet 4800 Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points
Access points for basic BLE gateway	• Cisco Aironet 1815 Series Access Points • Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio) • Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later **Note** For Cisco Catalyst 9800 Series Wireless Controllers Cisco IOS XE Cupertino 17.7.x, ensure that the IoX Application version is upgraded to Version 1.3.x

Note IoT Service (Wireless) is not supported with a directly connected controller, CMX Tethering, and AireOS connector. The only supported configuration is the Cisco Catalyst 9800 Wireless Controller and the connector.

This table lists the compatibility of the Advanced BLE Gateway for BLE and the Base BLE Gateway App with various AP modes. This table is not applicable to Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP).

Table 1: AP Modes and app support

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	• 802.11ax: Supported • COS APs/Wave 2: Not supported	• 802.11ax: Supported • COS APs/Wave 2: Supported
P1: Flex	• 802.11ax: Supported • COS APs/Wave 2: Not supported	• 802.11ax: Supported • COS APs/Wave 2: Supported
P2: Fabric	• 802.11ax: Supported • COS APs/Wave 2: Not supported	• 802.11ax: Supported • COS APs/Wave 2: Supported
P3: Mesh	• 802.11ax: Supported • COS APs/Wave 2: Not supported	• 802.11ax: Supported • COS APs/Wave 2: Supported

IoT services old Vs new UI

Feature Parity But Moved

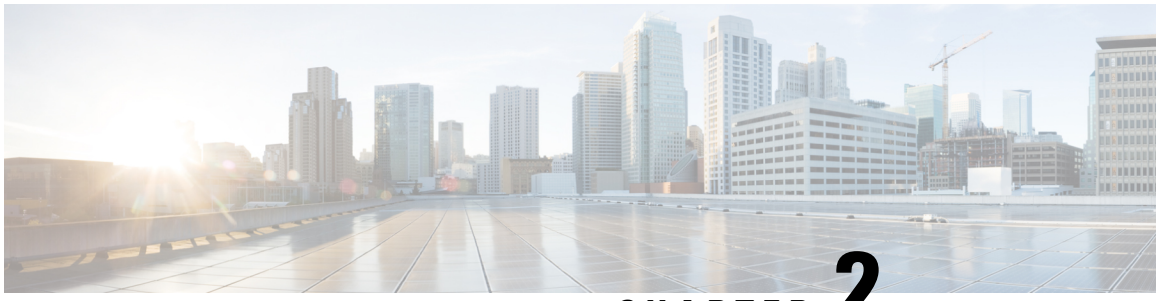
Old UI section	Old UI location	New UI location
IoT Management	Home/summary	Consolidated into **Device Management**, starting with building selection
IoT Management	AP Gateways	**Device Management → Wireless APs → AP Gateways**
IoT Management	AP inventory included within AP Gateways	**Inventory → Wireless APs**
IoT Management	Wired Gateways	**Device Management → Wired → Wired Gateways**
IoT Management	Wired switch inventory/deployment list	**Inventory → Wired**
IoT Management	AP Gateway request history	**Device Management → Wireless APs → Bulk/Operation Request History**
IoT Management	Wired Gateway request history	**Device Management → Wired → Bulk Request History**
Device Management	Home/summary	Consolidated into **Device Management**, divided into Wireless APs, BLE Devices, and Wired

Device Management	Devices → AP Beacons	**Device Management → Wireless APs → AP Beacons**
Device Management	AP Beacon sensor capability view	**Device Management → Wireless APs → AP Sensors** for non-Meraki networks
Device Management	AP Beacon scanning controls	**Device Management → Wireless APs → Activate/Stop Scanning on Network**
Device Management	Devices → Floor Beacons	**Device Management → BLE Devices**
Device Management	Floor Beacon profile views	**Device Management → BLE Devices**, using profile/KPI views
Device Management	Floor Beacons → Claimed Devices	**Inventory → Claimed Devices**
Device Management	Onboard/Claim Devices	**Inventory → Claimed Devices → Claim Devices**
Device Management	Claimed Device → Firmware Management	**Device Management → BLE Devices → Claimed Device details**
Device Management	Devices → Wired Devices	**Device Management → Wired → Wired Sensors**
Device Management	Devices → Smart PDUs	**Device Management → Wired → Smart PDUs**
Device Management	Groups	**Settings → Groups**
Device Management	Settings → Filtering	**Settings → Device Filtering**
Device Management	Different Buckets like All Profiles/AP Sensor/ Tranmist(iBeacon/eddyUid/eddyUrl)/Scan/ Dual/NeedsConfigChange/Disabl	**APbeacons/ NeedsConfigChange/Disabled**
Device Management	Actions-Manage Sensor	**Only Available in AP Sensor tab**

Deprecated / Not Provided

Old UI section	Old UI feature/location	New UI disposition
About	Standalone Network Health dashboard	**Deprecated/removed.** The `network_health` route is commented out. Per-device Network Troubleshoot remains available.
About	One-click activation when no IoT license is present	**Not provided.** Activation and configuration are license-gated; unavailable locations/actions are locked or hidden.
IoT Management / Device Management	Root/ORG/Campus-level management operations	**Deprecated.** Management is building-oriented; ROOT, ORG, and CAMPUS nodes cannot be selected for these operations.

IoT Management	Actions-Manage Sensor	Only provided in AP Sensor tab
IoT Management	Add New gateway link	Not Provided in AP Gateway tab but user can add AP gateways from about
Device Management	Policies and policy alerts	**Not provided.** Policy code exists, but the Policies tab is commented out and unreachable.
Device Management	Settings → Sensor History	**Deprecated/removed**
Device Management	Settings → Access Key	**Not provided** in the current Settings page.
Device Management	Devices → Hella Cameras	**Not provided** in active Device Management or Inventory navigation.
Device Management	Onboard through Camera	**Not provided** in the active Claim Devices choices.
Device Management	Devices → Zigbee Devices	**Not provided as a dedicated page.** Zigbee capability information may still appear for AP Gateways.
Device Management	Standalone Maps page and general list/map switching	**Deprecated.** There is no active Maps route, and the general Map View control was removed. Some device-specific embedded maps remain.



CHAPTER 2

Prerequisites

- Prerequisites of IoT Service (Wireless), on page 11

Prerequisites of IoT Service (Wireless)

Cisco Spaces: Connector Scale and Size Guidance for IoT Service

This section guides you on choosing a size for the Connector based on your scale of your deployment, such as

- number of APs in your network
- the messages that the Connector may have to send, and
- and the number of devices handled.

Note

- The table below is an approximation and assumes that only two services, namely Service manager service and IoT service (wireless), are in use. Also, every deployment is different and multiple factors impact the load on the Connector.
- Ensure that you have upgraded to the latest versions of these services to achieve the numbers mentioned in the table below.

Note We recommend that you use the **Advanced2** Connector sizing in most cases because IoT Wireless increases resource constraints.

Table 2: Cisco Spaces: Connector Scale and Size Guidance for IoT Service

Connector Size	Scale
Standard Connector (2vCPU, 4 GB RAM)	The **Standard** Connector can • Support up to 250 APs. • Send up to 25,000 outbound messages per second. • Process up to 1000 BLE tags or devices.
Advanced1 Connector (4vCPU, 8 GB RAM)	**Advanced1** Connector can • Support up to 2000 APs. • Send up to 120,000 outbound messages per second. • Process up to 20,000 BLE tags or devices.
Advanced2 Connector (8vCPU, 16 GB RAM)	**Advanced2** Connector can • Support up to 3000 APs. • Send up to 170,000 outbound messages per second. • Process up to 30,000 BLE tags or devices.

Prerequisites

These prerequisites can get you started with Cisco Spaces: IoT Service.

- Install Cisco Spaces: Connector in your network.
- Install a Cisco Catalyst 9800 Series Wireless Controller with a **Cisco IOS XE 17.12.x** or above image version.

Note There are significant improvements in Cisco Spaces: IoT Service on **Cisco IOS XE 17.9.5**. However, the minimum recommended version is **Cisco IOS XE 17.9.6** for better performance.

- Deploy supported APs in your network (refer to the Compatibility Matrix for IoT Service (Wireless) , on page 5).
- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Catalyst Center.
- If the Cisco Spaces: Connector is an Amazon Elastic Compute Cloud (EC2) Instance from Amazon Machine Images (AMI), ensure that the wireless controller and connector are in the same virtual private

cloud (VPC). Ensure that the wireless controller has a private IP address so that the security group of connector does not block the traffic, allowing enabled IOT streams to function.

- Permit all the TCP traffic at the Virtual private clouds (VPC) level so that the Telemetry Data Logger (TDL) is established without any issues.
- If location service is not added before adding a Cisco Catalyst 9800 Series Wireless Controller to a connector, run these commands on the Catalyst 9800 controller in a sequence:
  - **aaa new-model**
  - **aaa authentication login default local**
  - **aaa authorization exec default local**
- Cisco Spaces: IoT Service and Intelligent Capture (iCAP) feature can now co-exist on Cisco Catalyst 9800 Series Wireless Controller Cisco IOS XE Cupertino 17.7.x release and later. For releases earlier than Cisco IOS XE Cupertino 17.7.x, disable iCAP, if already enabled on the controller.
- Perform NTP synchronization over wireless controllers, a connector, and APs in the network.
- If a USB BLE module is inserted in an AP, reboot the AP.
- NETCONF must be enabled in Cisco Catalyst 9800 Series Wireless Controller in port 830, along with permission to use NETCONF.



Caution The application (app) installed and running over the AP uses the default 17.17.0.0/16 subnet. So, using this subnet for other purposes might create network issues.

- IPv6 is not supported on Cisco Spaces: Connector.
- If your require two connectors installed with 3.x to work with IoT service (wireless) and function as a high-availability pair, you must configure the connectors as Virtual IP (VIP) pair.

Before activating IoT services

This topic describes the prerequisites that you need before you activate IoT services:

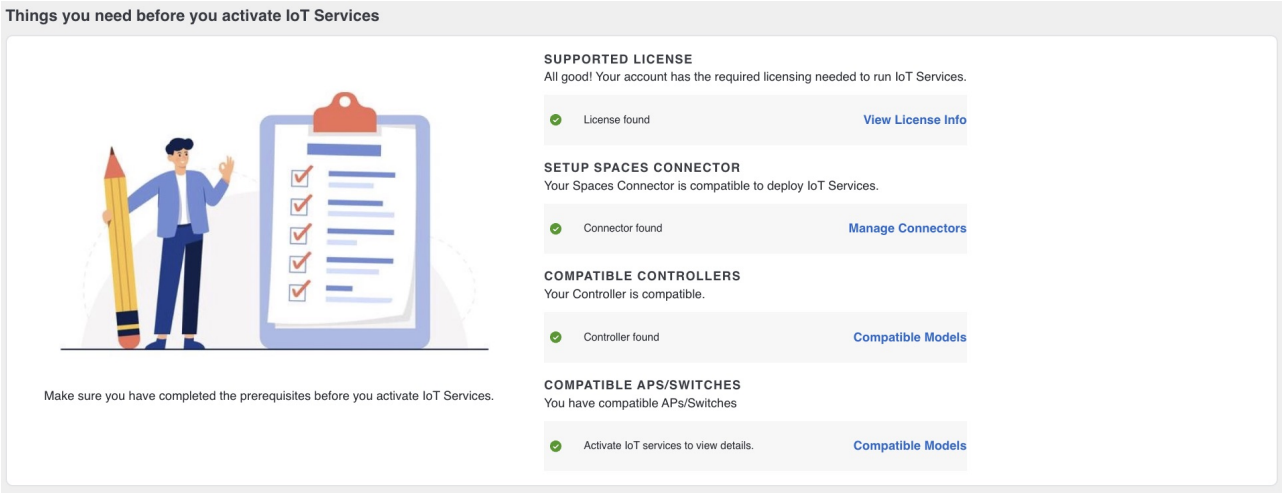
- Supported License
- Setup Spaces Connector
- Compatible Controllers
- Compatible Apps/Switches

Summary

Complete all prerequisites before activating IoT Services.

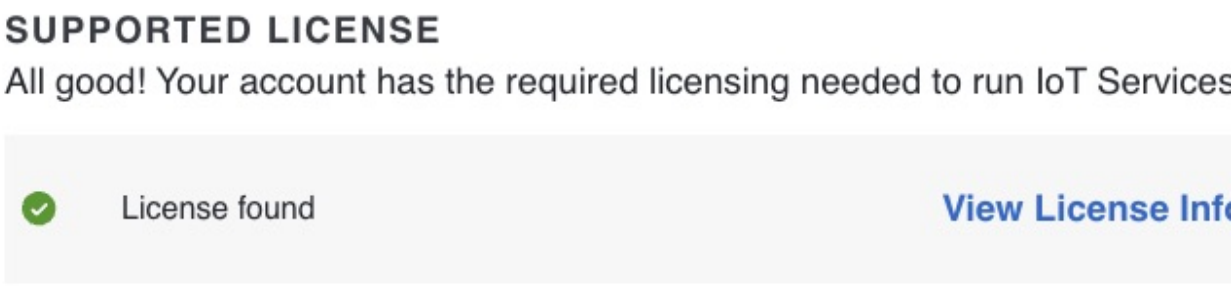
Workflow

Figure 3: Before you activate IoT Services tab



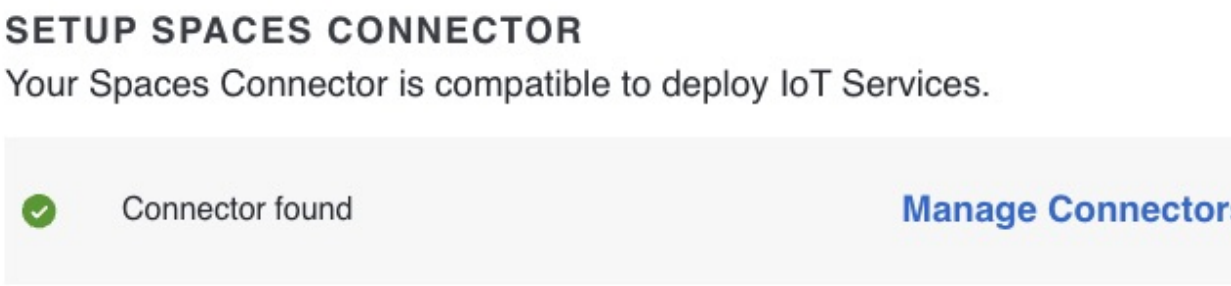
1. To confirm that the account has the required licensing for IoT Services under the **Supported License** point, click the **View License Info** button. This step redirects to the **License Info** section in the My account page.

   Figure 4: Supported License option

2. To determine if the Spaces Connector is compatible for deploying IoT Services under **Setup Spaces Connector** point, click the **Manage Connectors** button. This action redirects to the **Connectors** section in the Cisco Spaces Dashboard page.

   Figure 5: Setup Spaces Connector option

3. To verify compatibility for controllers under the **Compatible Controllers** point, click on the **Compatible Models** button. The **Compatible Models** button displays the lists of **Controllers**, **APs** and **Switches**.

Figure 6: Compatible Controllers option

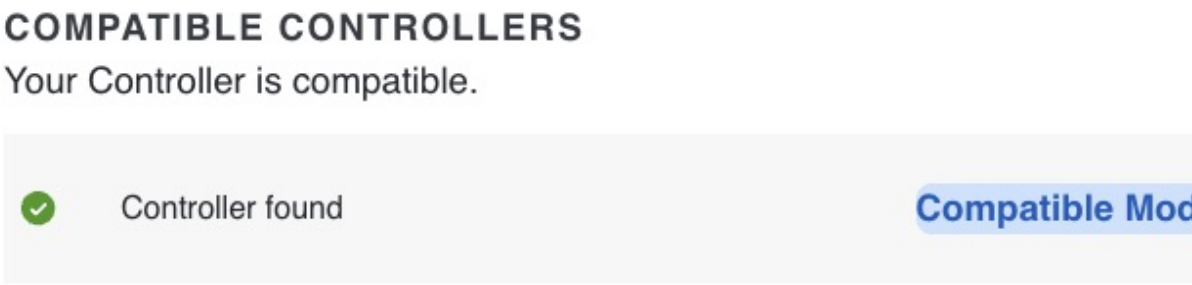
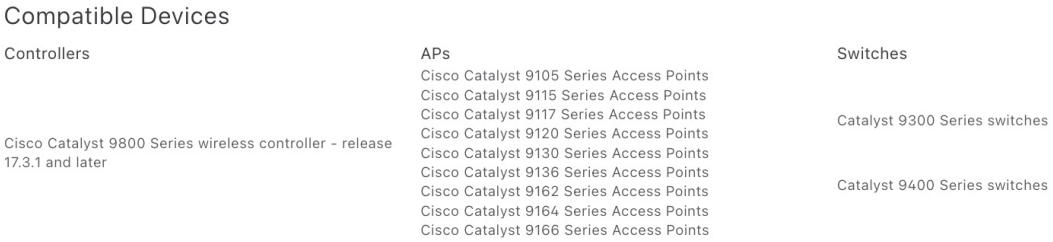
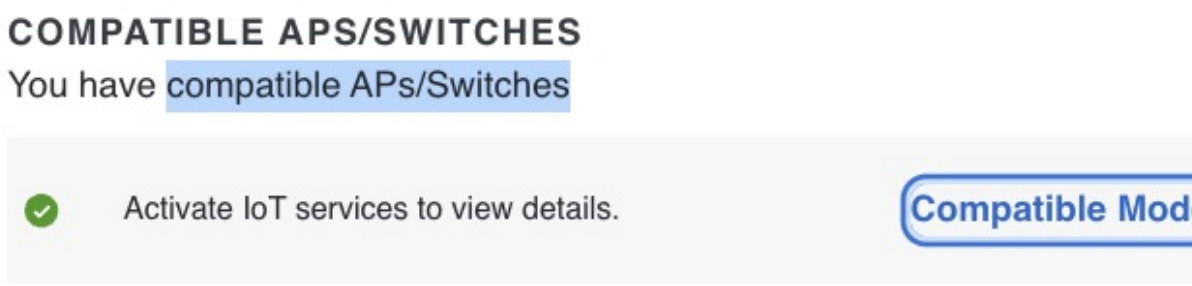


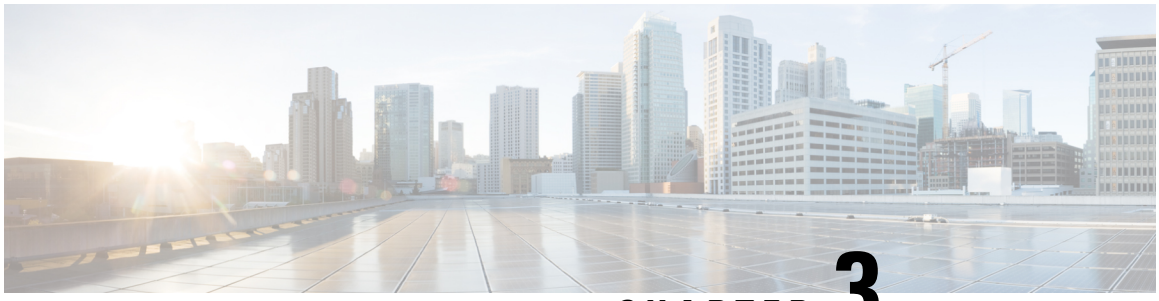
Figure 7: List of compatible devices



4. To verify compatibility for APs or Switches under **Compatible APs/Switches** point, click the **Compatible Models** button. The **Compatible Models** button displays lists of **Controllers**, **APs** and **Switches**.

Figure 8: Compatible APs/Switches option





CHAPTER 3

Getting Started

- Activate IoT Service (Wireless), on page 17
- Enable IoT service on Connector2, on page 22

Activate IoT Service (Wireless)

This task shows you how to activate IoT service (wireless) on some or all your devices, from the Cisco Spaces dashboard.

Before you begin

To activate IoT service (wireless), your network must meet the below prerequisites:

- Cisco Spaces: Connector
- Cisco Catalyst 9800 Series Wireless Controllers, installed with version 17.3.1 or higher
- Supported access points, refer to Prerequisites of IoT Service (Wireless).

Note

- This workflow is applicable only for Connector Release 3. We recommend you upgrade from Connector 2.x for smooth functioning of your services. If it is essential to enable IoT service (wireless) on Connector 2.x, refer to Enable IoT service on Connector2, on page 22.
- The workflow initiated by this procedure automatically checks for prerequisites necessary to complete this task.
- With split licensing, accounts without a full tenant-level Advantage license see a limited **About IoT Services** page. A banner directs users to activate IoT services from the **Manage** page, where activation must be done in bulk because one-click activation and the activation wizard are unavailable. The **Activate** button and **Activation Status** section are hidden, and users can view only the prerequisites. Only accounts with a full Advantage license can begin the IoT services journey from the About page.

Procedure

Step 1 Login to Cisco Spaces.

Step 2 From the left navigation pane, click **IoT Services** > **About IoT Services**.

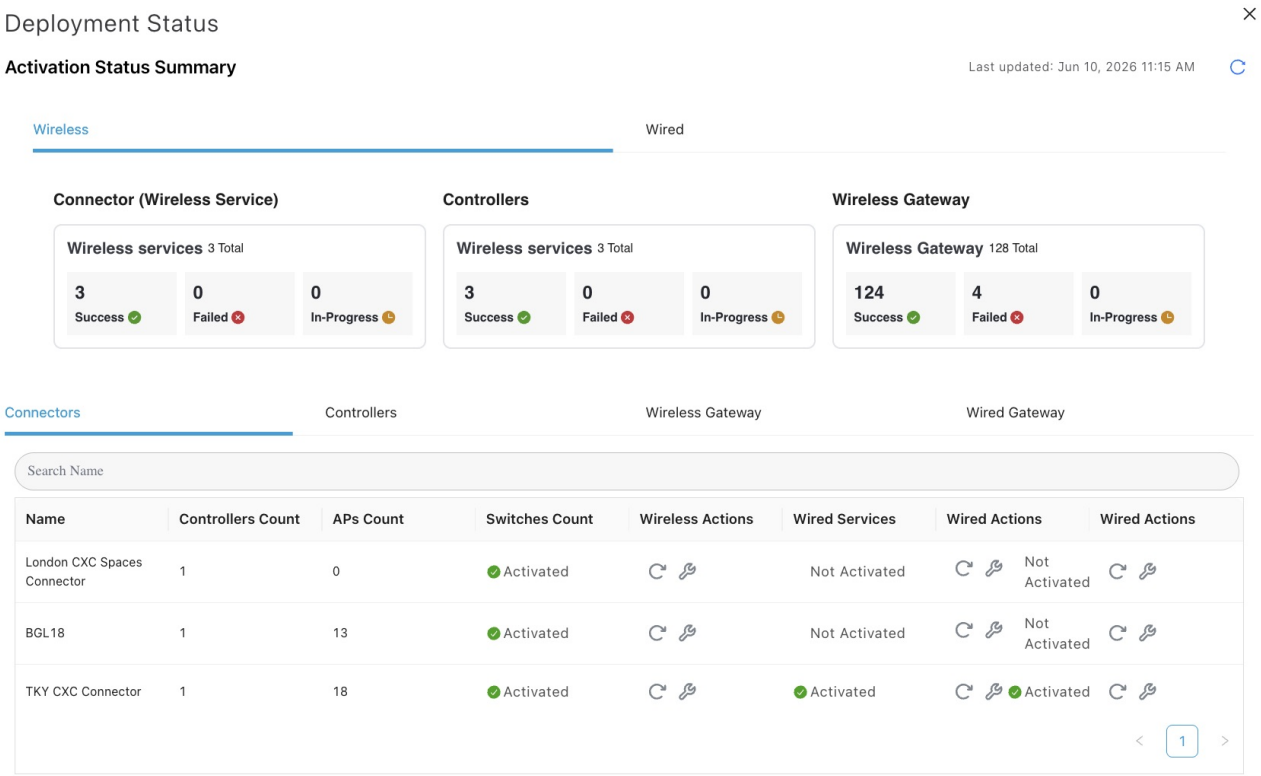
You can see the number of connectors activated with the IoT service (wireless) service. You can also see the number of APs deployed as an IoT service (wireless) gateway.

Figure 9: About IoT Services



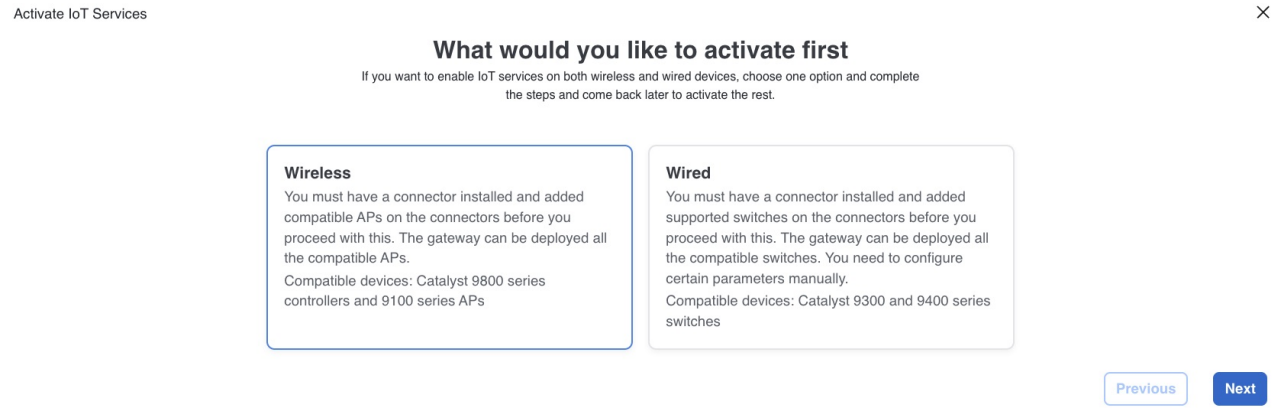
Click **View Detailed Status** to see the breakdown of the activation status of various individual devices.

Figure 10: Detailed Status of Devices Activated With IoT Service (Wireless)



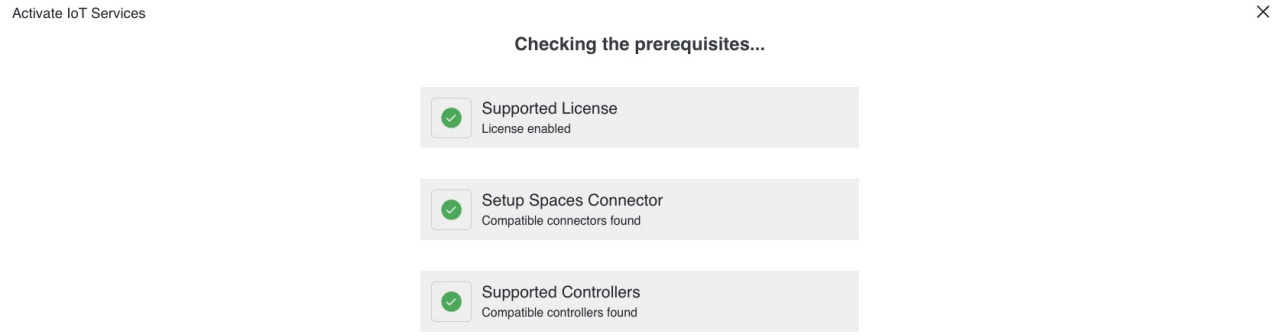
Step 3 In the **About IoT Services** window top-left corner, click **Activate** and choose **Wireless**.

Figure 11: What would you like to activate first



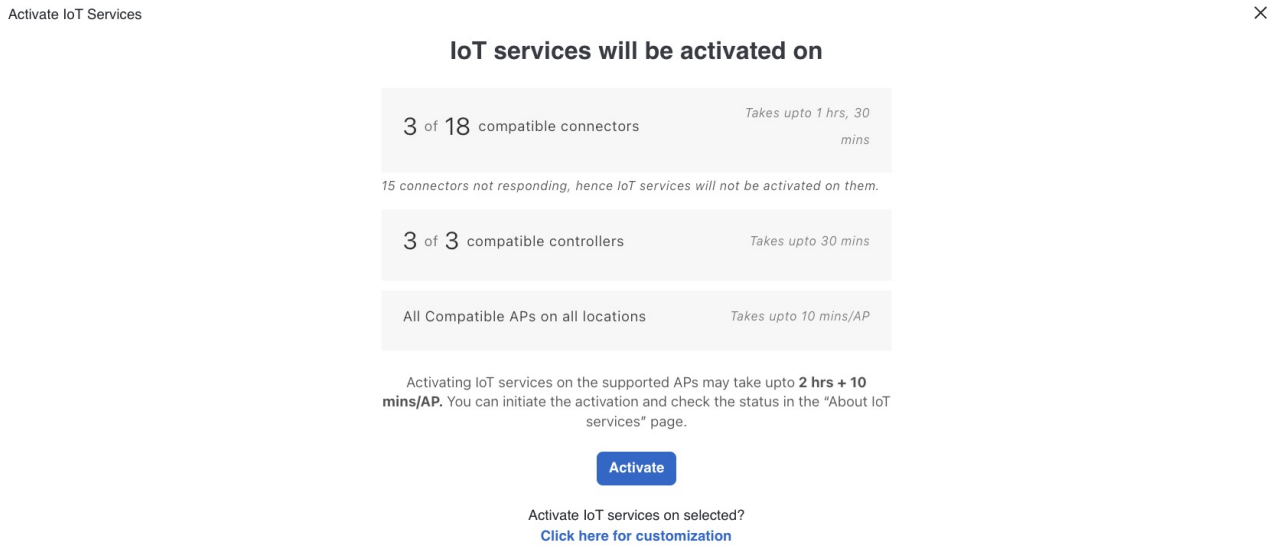
Step 4 The **Checking the prerequisites** tab appears.

Figure 12: Prerequisites check



You can see the list of all devices on which IoT service (wireless) can be activated, along with the activation time.

Figure 13: List of Supported Devices

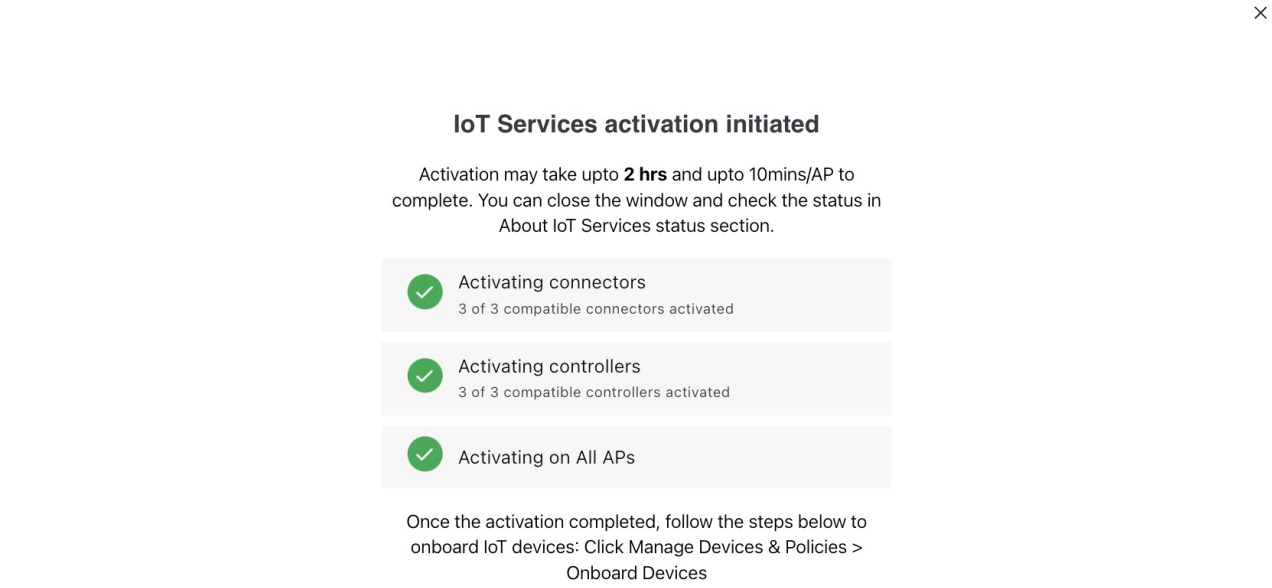


Step 5 To activate IoT service (wireless) on all devices on your network, in the **IoT services activation initiated** window, click **Activate**.

This activation of IoT service (wireless) automates these tasks:

- Enables IoT streams on the connector
- Enables the wireless controller stream
- Configures APs as a Bluetooth Low Energy (BLE) gateway (this includes turning on the BLE radio, BLE scanning, and deploying the BLE gateway app)

Figure 14:



Step 6 To activate IoT service (wireless) only on specific devices of your network, do these:

a) Choose one or more connectors to activate IoT service (wireless).

b) To activate the wireless gateway, click **Activate Wireless**.

c) In the **Deploy Wireless Gateway** window, select the APs on which you want to activate IoT service (wireless).

Figure 15: Activate IoT Service (Wireless) on Preferred Devices

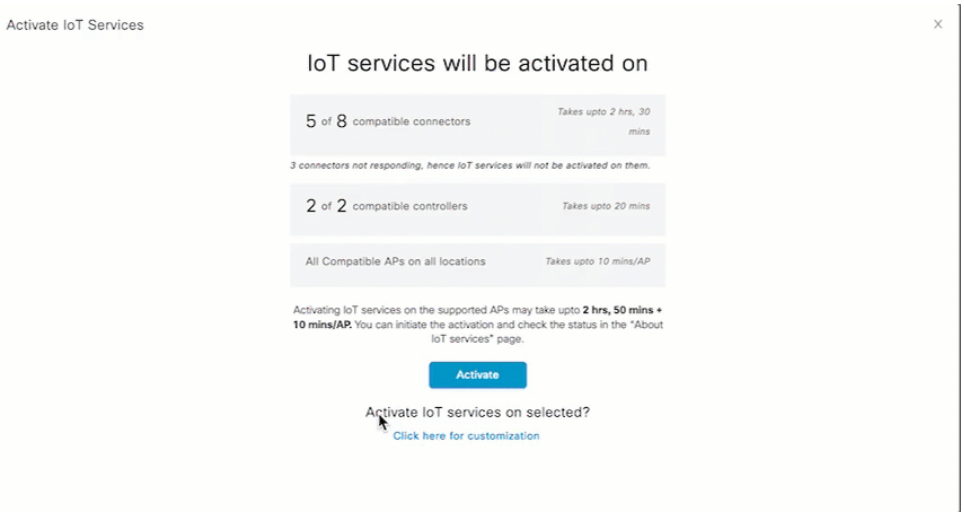
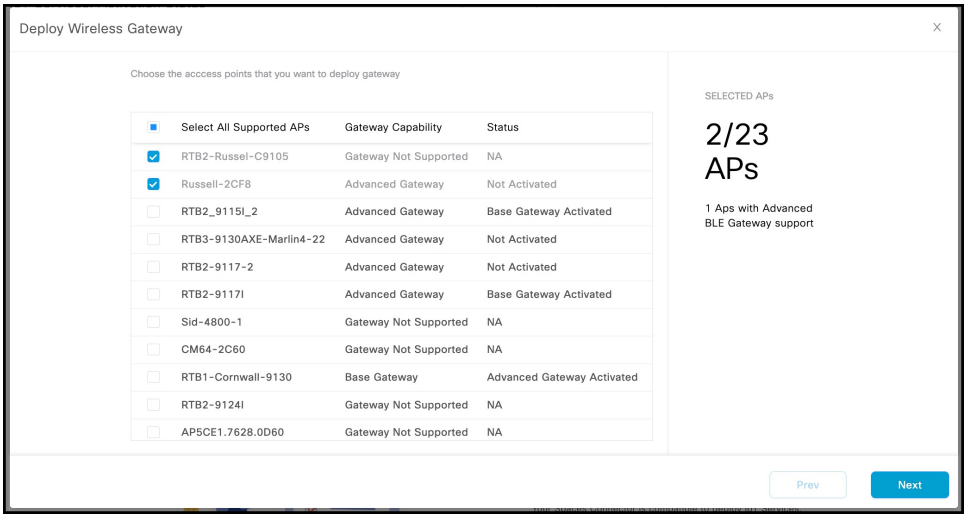


Figure 16: Activate IoT Service (Wireless) on Preferred Devices



What to do next

Once the activation completed, you can onboard the IoT Service (Wireless) devices. Click **Manage Devices & Policies** > **Onboard Devices**.

Enable IoT service on Connector2

Verify Cisco Spaces: Connector is Added and Active

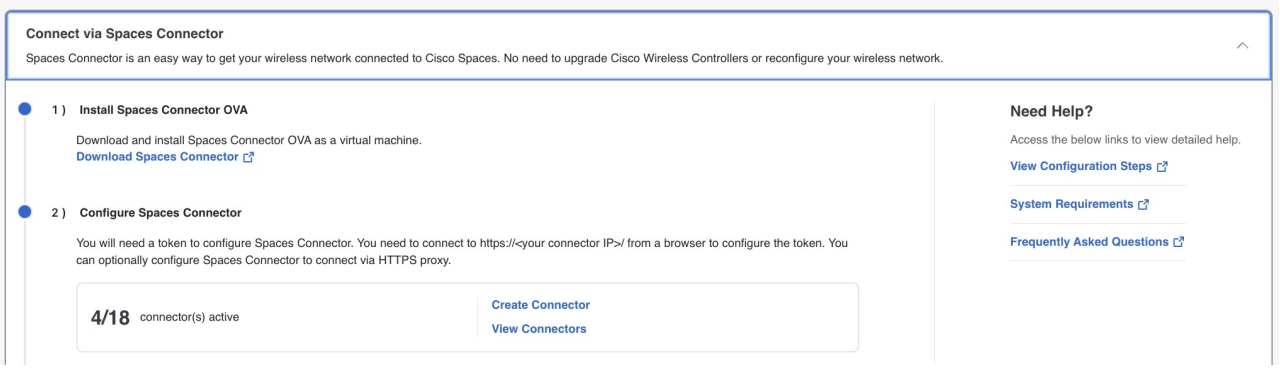
This procedure helps you verify if a Cisco Spaces: Connector is deployed and active.

Procedure

Step 1 From the Cisco Spaces dashboard left-navigation pane, choose **Setup** > **Wireless**.

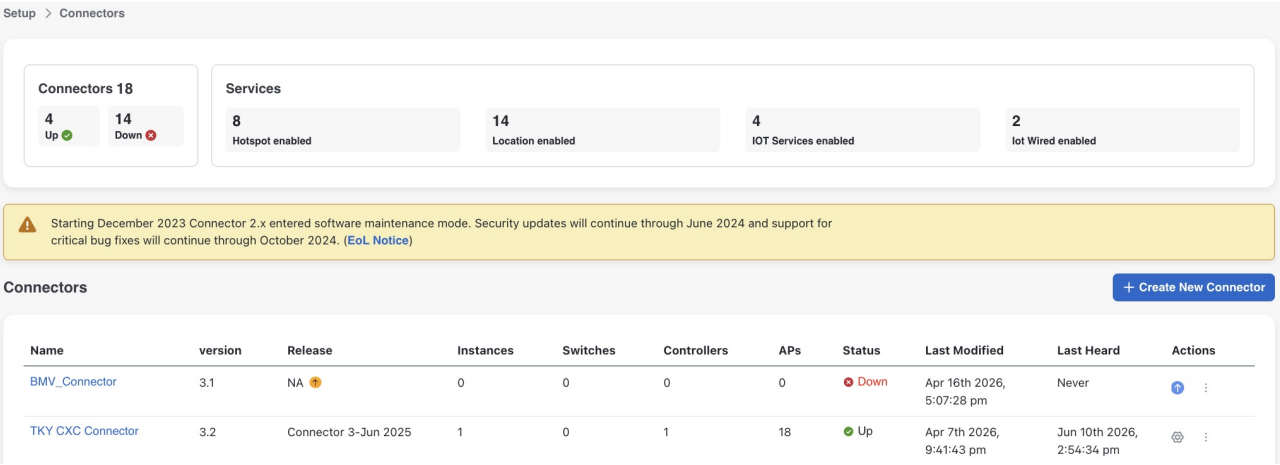
Step 2 From the **Connect via Spaces Connector** area, click **View Connectors**.

Figure 17: View Connectors



Step 3 Ensure that a connector is listed and its status is **Up**.

Figure 18: Connector Status Up



Verify Cisco Catalyst 9800 Series Wireless Controllers is Added and Active

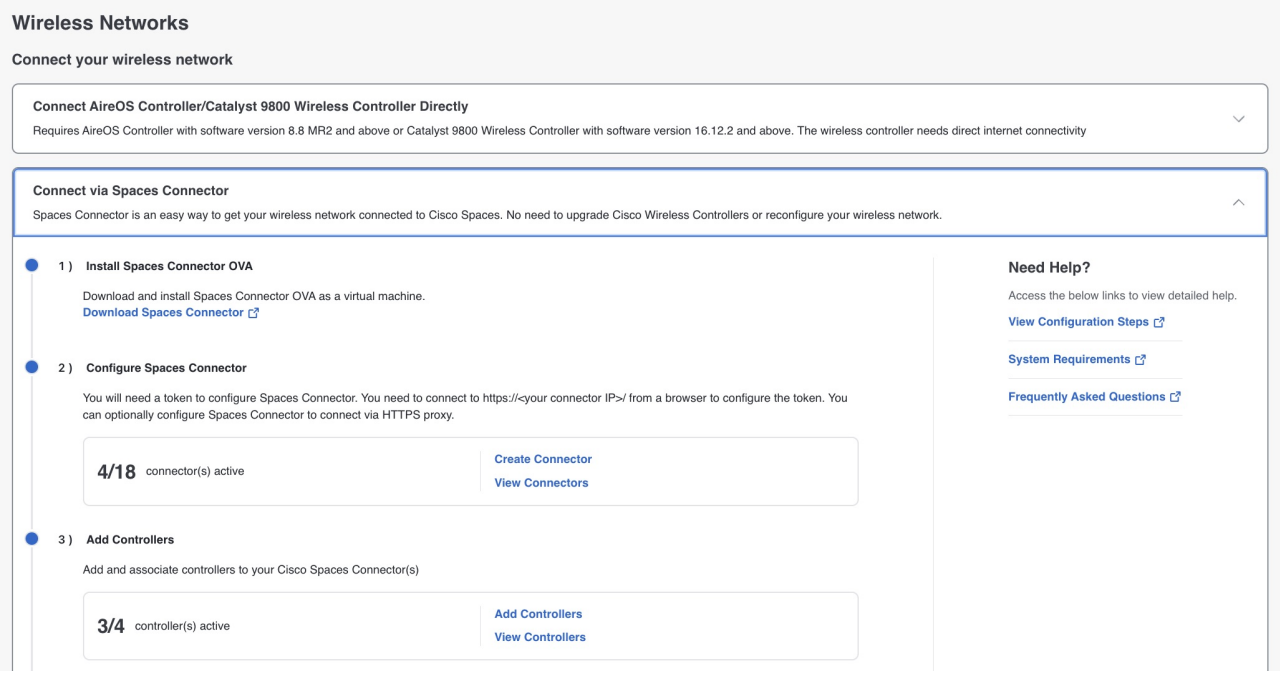
This procedure helps you verify if the Cisco Catalyst 9800 Series Wireless Controller is deployed and active.

Procedure

Step 1 From the Cisco Spaces dashboard left-navigation pane, choose **Setup** > **Wireless Networks**.

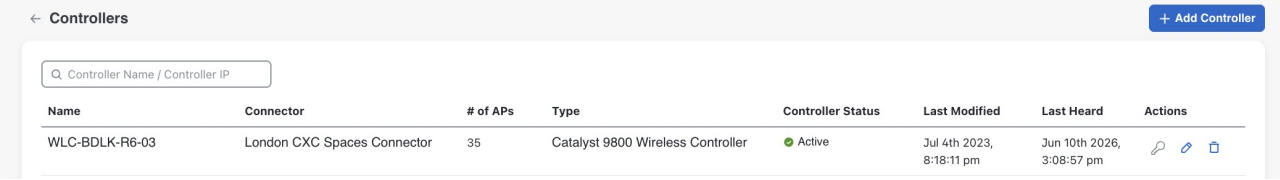
Step 2 From the **Add Controllers** area, click **View Controllers**.

Figure 19: View Controllers



Step 3 Ensure that a controller is listed here, and the corresponding status is **Active**.

Figure 20: Active Controller



Configure connector for gRPC and certificate services

This procedure enables IoT streams. This procedure ensures that your APs visible on Cisco Spaces: IoT Service. In this procedure you:

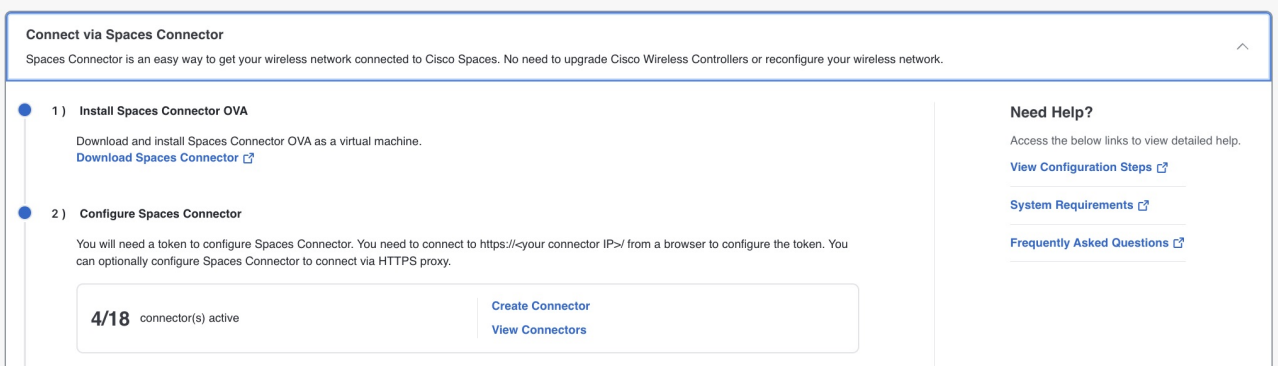
- Enable the Cisco Spaces: Connector to listen for gRPC Remote Procedure Call (gRPC) and certificate services.
- Activate these IoT streams on the wireless controller.

Procedure

Step 1 From the Cisco Spaces dashboard left-navigation pane, click **Setup** > **Wireless Networks**.

Step 2 From the **Connect via Spaces Connector** area, click **View Connectors**.

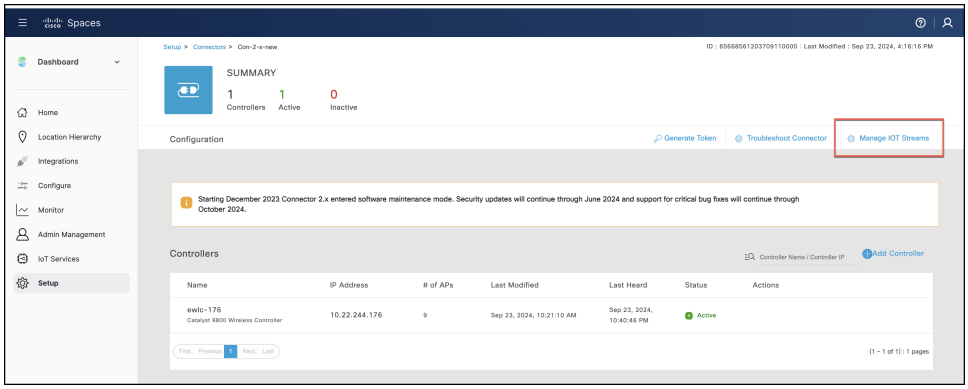
Figure 21: View Connectors



Step 3 From the list of connectors displayed, choose your connector, and then click **Manage IoT Streams**.

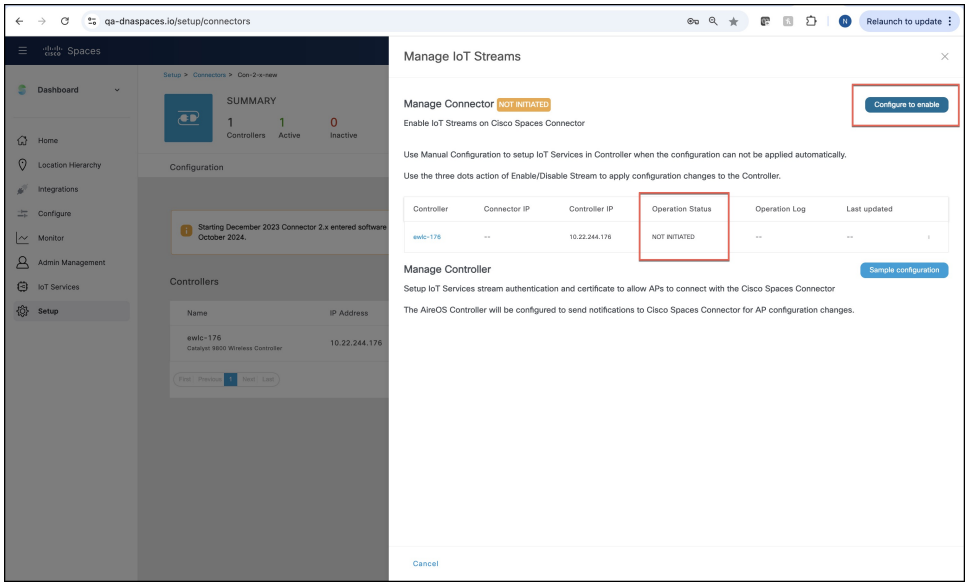
Step 4 In the **Manage IoT Streams** page that is displayed,

Figure 22: Manage IoT Streams



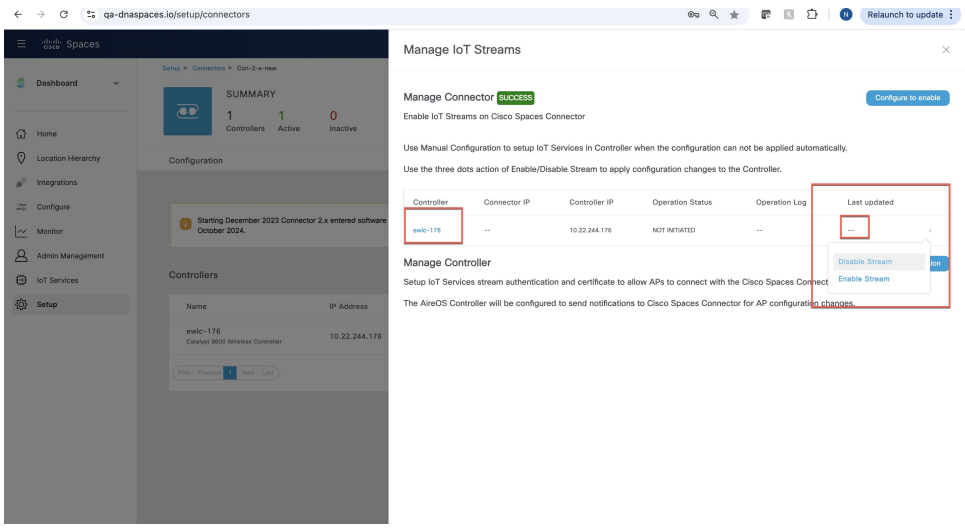
a) Click **Configure to Enable** to enable the connector stream.

Figure 23: Configure to Enable



b) For each wireless controller displayed, click the three-dot icon to display a menu. Choose **Enable Stream** to enable the wireless controller stream.

Figure 24: Enabling IoT Streams for the Connector and for each associated Wireless Controller



c) Verify if the **Operation Status** of the connector is **SUCCESS**. Click the wireless controller in the list to check for any errors.

Figure 25: Operation Status of Wireless Controller is SUCCESS

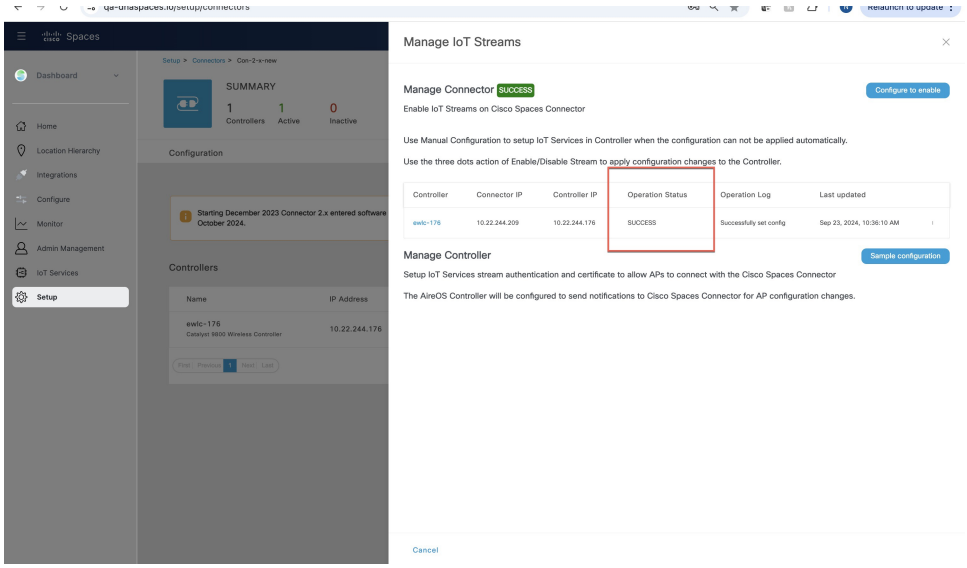
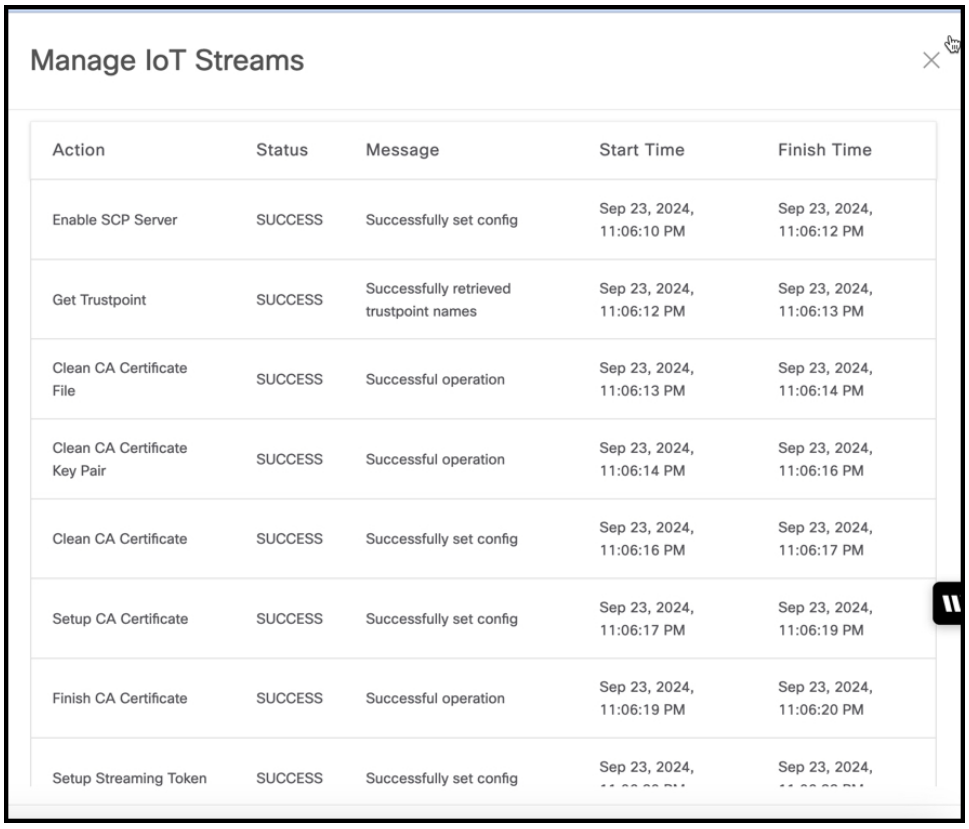


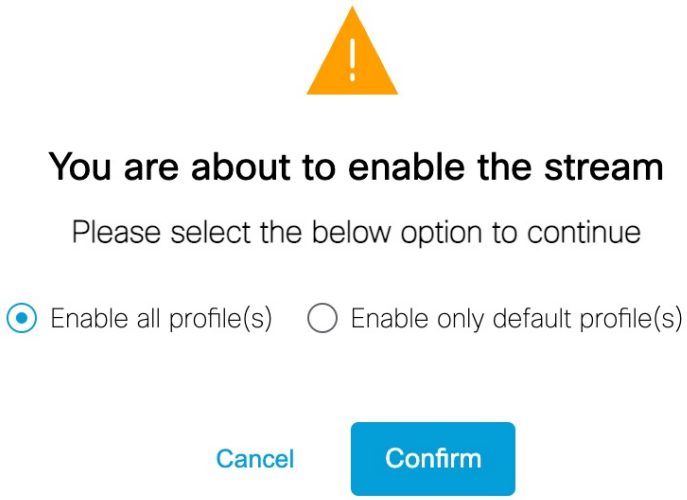
Figure 26: Check for Errors



Reconfigure this step if you move APs to a new AP profile.

d) In the displayed popup, choose the AP profiles to push the IoT configuration. You can choose to push the IoT configuration to one or more default AP profiles on the wireless controller. Or you can also choose to push the IoT configuration to all the AP join profiles on the wireless controller.

Figure 27: Enabling IoT Streams for the Connector and for Each Associated Wireless



Controller

Reconfigure this step if you move APs to a new AP profile.

Enable BLE on AP

This procedure turns on Bluetooth Low Energy (BLE) on an AP, and puts selected APs in the Admin state and in the base scan mode.

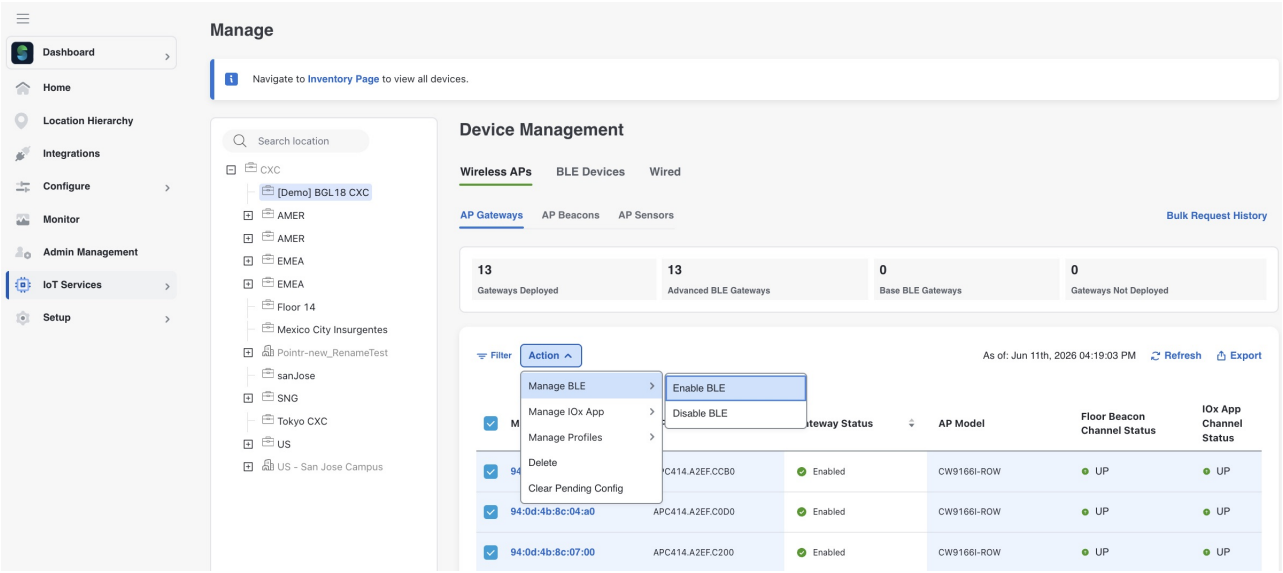
Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services** > **Manage** > **Wireless APs** > **All Gateways**.

Step 2 Check the checkboxes of specific APs, then click on the **Action** drop-down button.

Step 3 To turn on BLE Admin state and base scan mode, from the drop-down that opens, choose **Manage BLE** > **Enable BLE**.

Figure 28: Enable BLE



Set AP in advanced mode

This procedure sets an AP on the Bluetooth Low Energy (BLE) advanced mode.

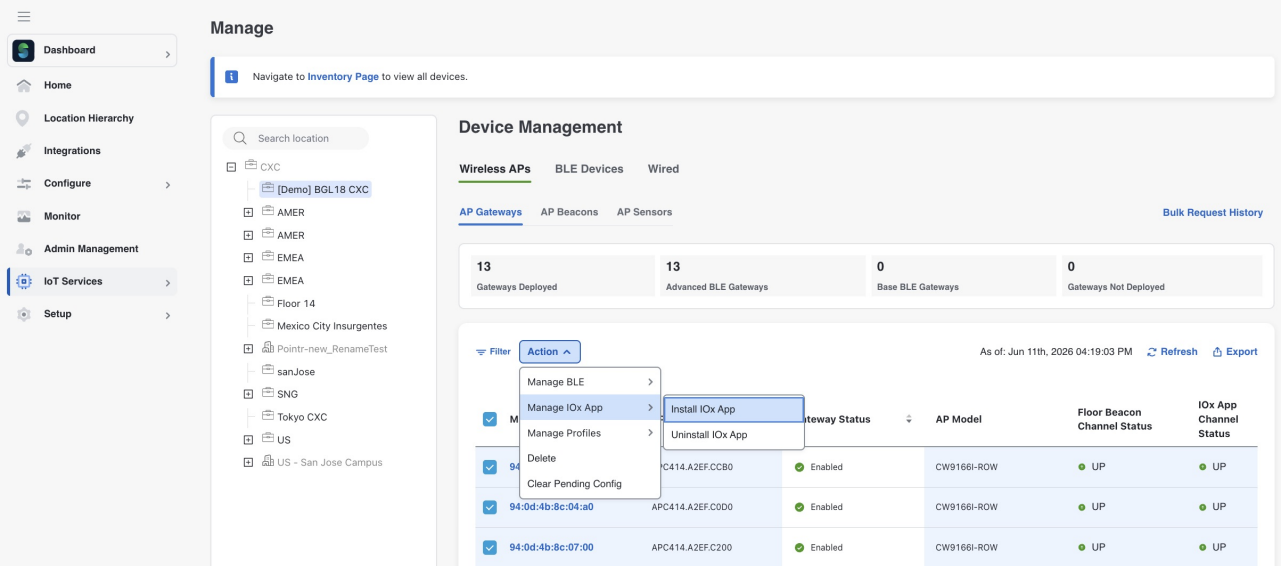
Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services** > **Manage** > **Wireless APs** > **AP Gateways**.

Step 2 Check the boxes of specific APs, and then click on the **Action** drop-down button.

Step 3 To set the AP on BLE advanced mode, from the drop-down that opens, choose **Manage IOx App** > **Install IOx App**.

Figure 29: Install IOX App



Verify access points

This procedure helps you verify if IoT service (wireless) has synchronized and listed the APs in your network on the GUI.

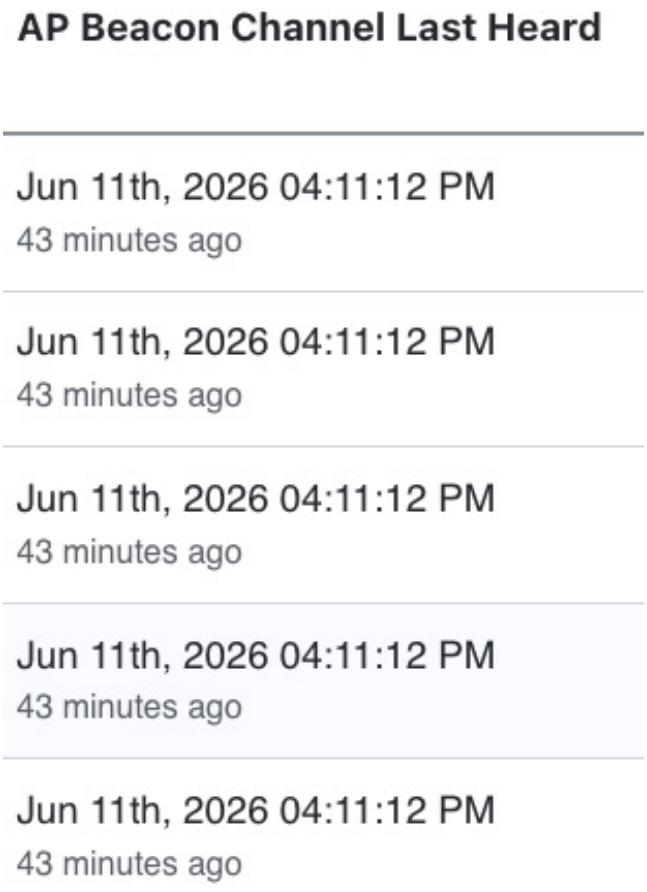
Procedure

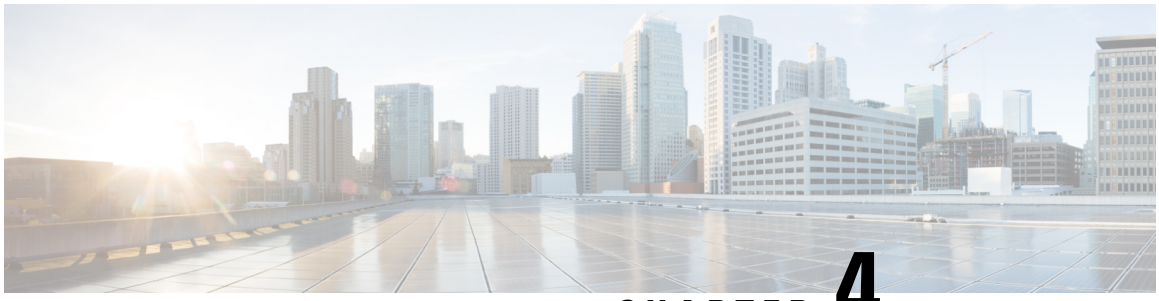
Step 1 In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services** > **Manage** > **Wireless APs** > **AP Gateways**.

Step 2 Verify if IoT service (wireless) has synchronized and listed the APs in your network. Check the **Floor Beacon Channel Status** and **AP Beacon Channel Last Heard** columns.

Figure 30: Floor Beacon Channel Status

Figure 31: AP Beacon Channel Last Heard





CHAPTER 4

Open Ports

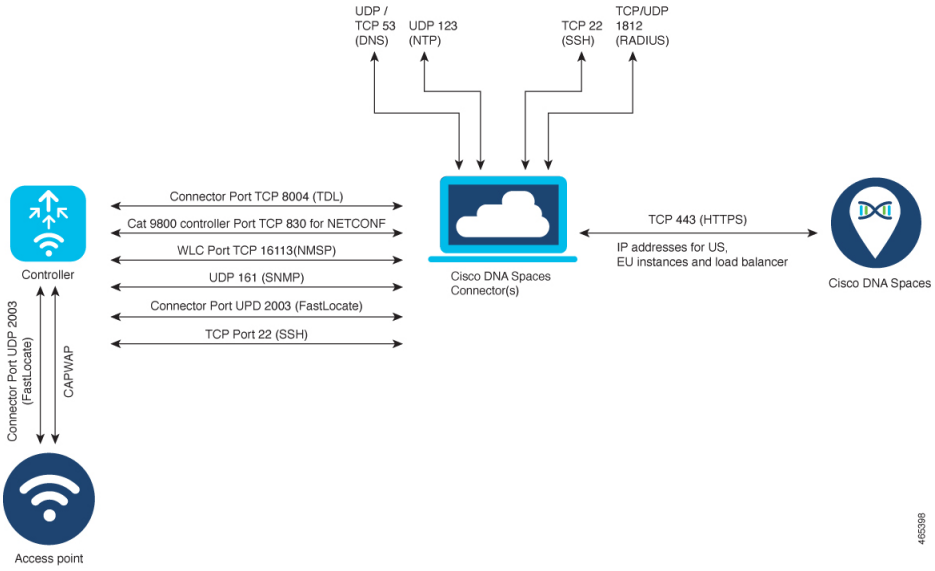
- Information About Open Ports (Wireless), on page 33

Information About Open Ports (Wireless)

This chapter lists the connector ports that need to be open for the proper functioning of various services or protocols.

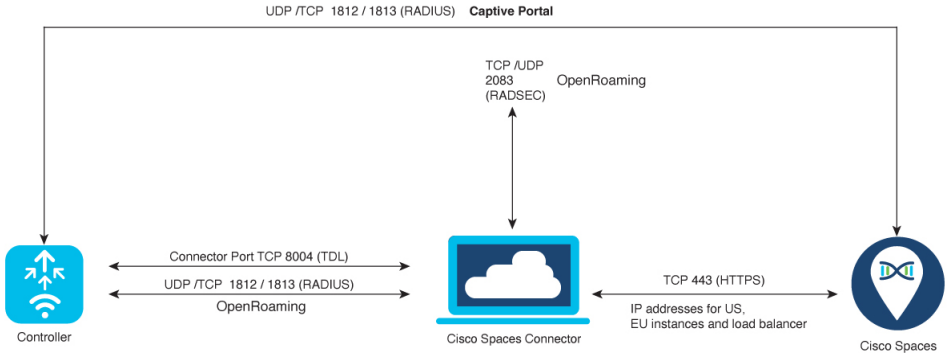
These ports need to be opened to allow for the basic functionality of Cisco Spaces.

Figure 32: Basic Functionality



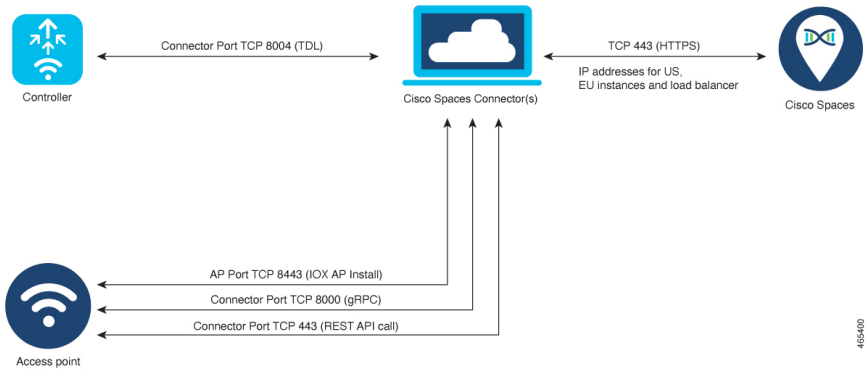
In addition to basic functionality, additional ports need to be opened for other additional functionality like guest onboarding and IoT Services.

Figure 33: Guest Onboarding



These ports need to be opened for configuring IoT Services (wireless). To configure IoT Services (wired), refer to Open Ports (Wired).

Figure 34: IoT Services

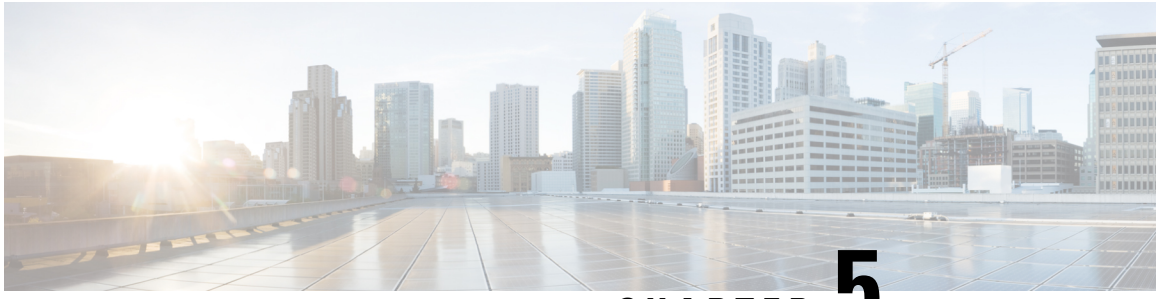




PART II

Inventory

- Inventory, on page 37



CHAPTER 5

Inventory

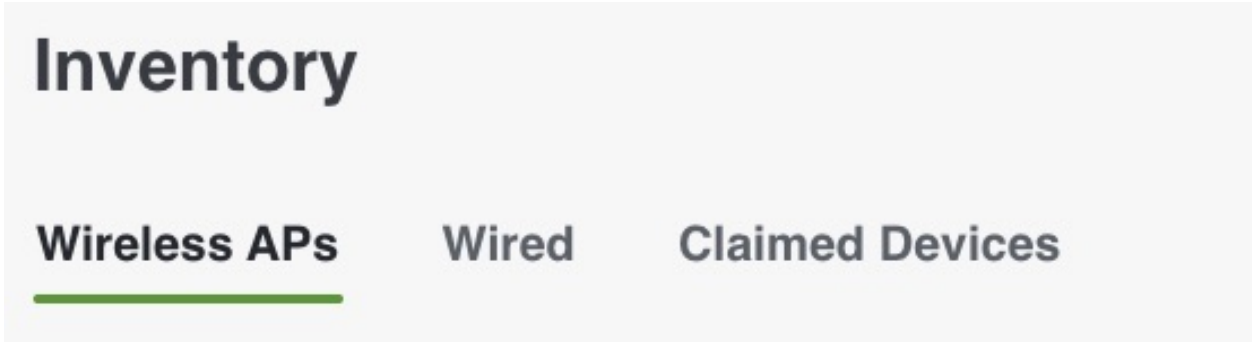
- Inventory, on page 37
- Configure wireless APs, on page 38
- Configure wired switches, on page 39
- Configure claimed devices, on page 40

Inventory

The inventory tab displays MAC addresses organized under the columns:

- Wireless Access Points
- Wired switches
- Claimed devices

Figure 35: Inventory tab



The **Inventory** tab lists every access point (AP) and switch, regardless of location. Once you map a controller to a location, the APs in that location appear under that location in the manage page. The mapping can be performed using Prime, DNAC, or Catalyst Center. After you map the APs to a floor and assign a switch to a location, they appear in the manage page under their locations.

When you add a controller and switch to a connector, and if previous IoT streams were performed on that controller or switch, the system sends the TDL subscription and retrieves data from TDL through Cisco Spaces. The inventory process has not changed. The available actions in the inventory tab are **select**, **delete**, and **export**.

If there are stale APs or switches, you can delete them from the inventory tab. No other actions can be performed on this tab.

Configure wireless APs

Use this task to customize and manage the configuration of your wireless APs, such as enabling BLE modes, monitoring installed applications, viewing request history, exporting AP information, or deleting APs.

Follow these steps to configure and manage wireless APs:

Before you begin

The **Wireless APs** tab consists of these columns: **MAC Address**, **Network Type**, **Name**, **AP ID**, **WLC ID**, **AP Model**, **Location** and **Label**.

Figure 36: Wireless APs tab



Procedure

Step 1 Select the MAC address of the AP you want to configure under the **Wireless APs** tab.

Step 2 The **AP Configuration** panel appears on the right navigation.

Step 3 In the **AP Information** panel, review these: **MAC Address**, **Network Type**, **Name**, **AP IP**, **WLC IP**, **AP Model**, **Location** and **Label**.

Step 4 In the **Settings** panel, enable **BLE** by toggling the BLE switch. To **enable** additional BLE modes, select any of these options after enabling BLE: **Scan**, **Transmit** and **Dual**.

Step 5 In the **Request History** panel, check these columns: **Operation**, **Status**, **Initiated At**, **Last Updated At**, **Status Message**, **Config Source** and **Destination AP**.

Note
Click the **Refresh** button to update all these **AP configuration** details.

Step 6 To refresh the list of wireless AP MAC addresses, click the **Refresh** button under the **Wireless APs** tab.

Step 7 To export a specific MAC address, select the desired AP under the **Wireless APs** tab and click the **Export** button. The details are downloaded as a .csv file to your local system.

Step 8 To delete the Wireless AP, check the checkbox for the desired MAC address and click on the **Action** drop down button. Click **Delete** to confirm.

Configure wired switches

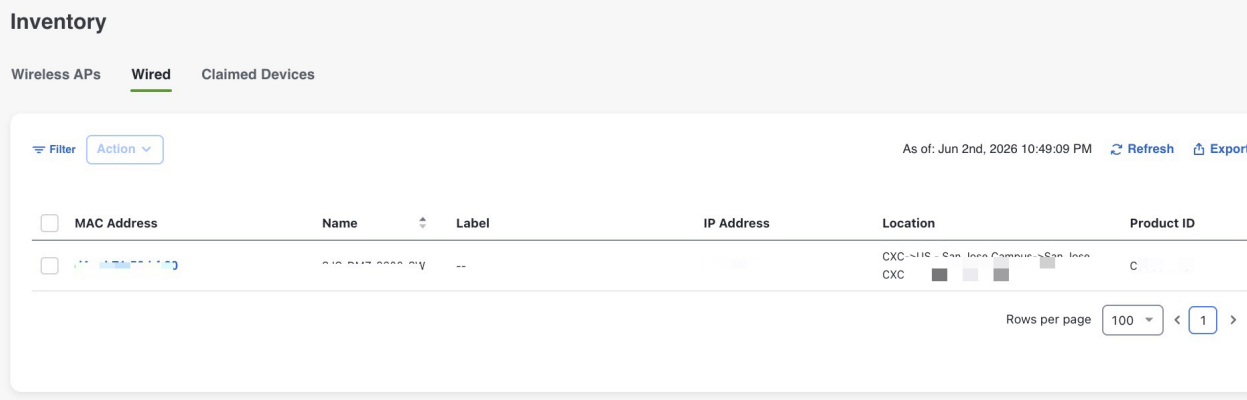
Use this task to access, configure, and maintain wired switches in your environment. This process covers viewing switch information, managing installed apps, exporting switch data, and deleting wired switches.

Follow these steps to configure and manage wired switches:

Before you begin

The **Wired** tab consists of these columns: **MAC Address**, **Name**, **Label**, **IP Address**, **Location** and **Product ID**.

Figure 37: Wired switches tab



Procedure

Step 1 Select the MAC address of the AP you want to configure under the **Wired** switches tab.

Step 2 The **Wired Gateway** panel appears on the right navigation.

Step 3 In the **Wired Information** panel, review these: **MAC Address**, **Name**, **Label**, **IP Address**, **Location** and **Product ID**.

Step 4 In the **Energy Information** panel, review these: **Device**, **Event**, **Address**, **Module**, **Module Energy**, **Module Energy Reset Time**, **Module Number**, **Module Power Budget**, **Module Power Instant**, **Module Power Peak** and **Module Type**.

a) In the **Module Details** part, review these columns: **Module Number**, **Host ID**, **Available Power**, **Chassis Number**, **Free Port**, **Max Power**, **IP Address**, **Number of Ports**, **Power Pool Index**, **Remaining Power**, **Total Consumed Power**, **Used Ports** and **Used Power**.

b) In the **Port Details** part, review these: **Interface Name**, **Device Name**, **IP Address**, **Event Time**, **Admin State**, **Max. Power Drawn**, **Operating Power**, **Operating State**, **PD Class**, **Max. Admin Power**, **Power Consumption**, **Power from PSE**, **Power to PD** and **Power Used**.

Step 5 In the **Request History** part, review these: **Operation**, **Status**, **Initiated At**, **Last Updated At**, **Status Message**, **Config Source** and **Destination AP**.

Step 6 To refresh the list of wired switch MAC addresses, click the **Refresh** button under the **Wired** tab.

Step 7 To export a specific MAC address, select the desired AP under the **Wired** tab and click the **Export** button. The details are downloaded as a .csv file to your local system.

Step 8 To delete the Wired switches, check the checkbox for the desired MAC address and click on the **Action** drop down button. Click **Delete** to confirm.

Configure claimed devices

Use this task when you need adjust device-specific parameters such as beacon configuration or telemetry, or onboard additional devices (Cisco, Meraki, or third-party) into your asset inventory.

Follow these steps to configure claimed devices:

Before you begin

The **Claimed Devices** tab consists of these columns: **MAC Address**, **Last Heard**, **Name**, **Firmware**, **Location**, **Order ID**, **Vendor ID** and **Model**.

Figure 38: Claimed devices tab



Procedure

Step 1 The **Base MAC Address** panel appears on the right navigation.

Step 2 In the **Device Information** panel, review these: **MAC Address**, **Last Heard**, **Name**, **Firmware**, **Location**, **Order ID**, **Vendor ID**, **Model** and **Label**.

Step 3 In the **Sensor Information** panel, check if the sensor data is available for that device.

Step 4 In the **Beacon Information** panel, check if the beacon data is available for that device.

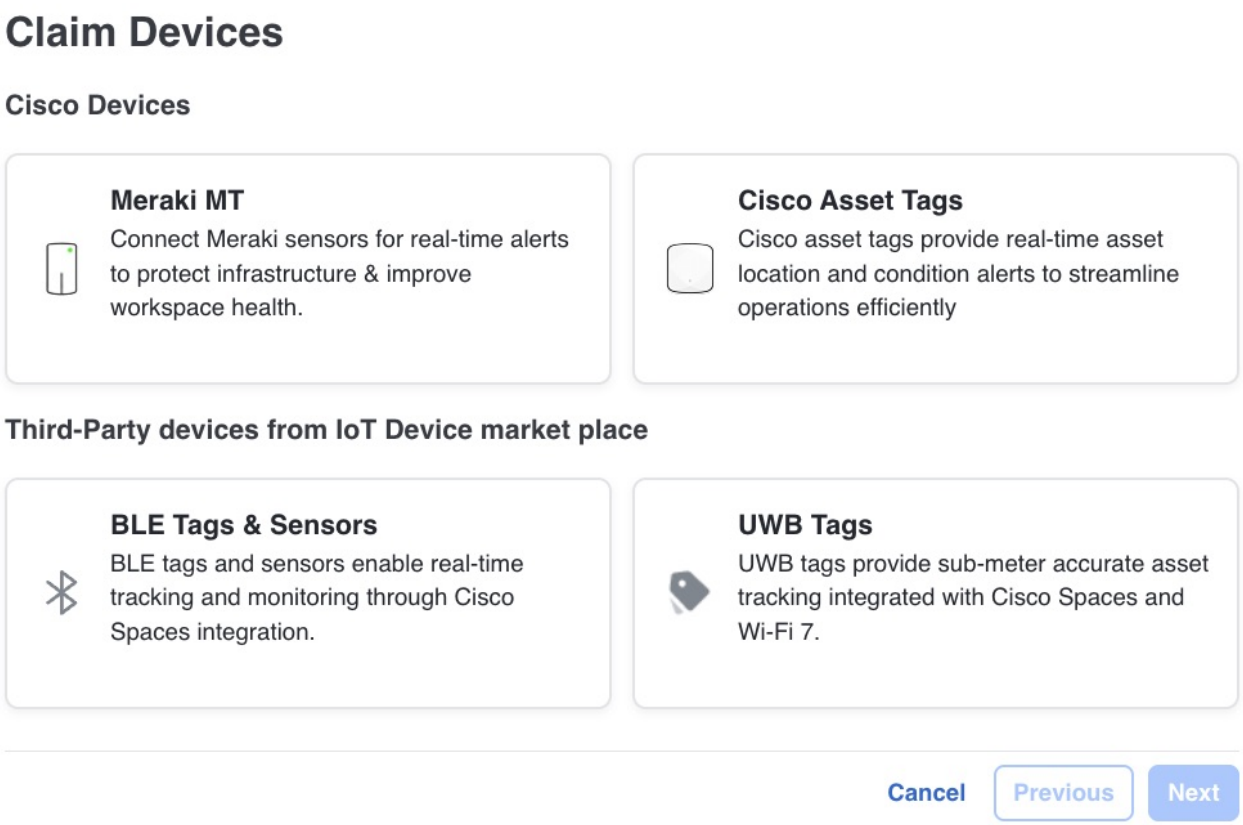
Step 5 In the **Request History** panel, review these: **Operation**, **Status**, **Initiated At**, **Last Updated At**, **Status Message**, **Config Source** and **Destination AP**.

Step 6 To refresh the list of claimed devices MAC addresses, click the **Refresh** button under the **Claimed Devices** tab.

Step 7 To export a specific MAC address, select the desired AP under the **Claimed Devices** tab and click the **Export** button. The details are downloaded as a .csv file to your local system.

Step 8 To add new claimed devices, click on the **Claim devices** button. The **Claim Devices** window appears.

Figure 39: Claim devices tab



a) **Cisco Devices**: allow **Meraki MT** and **Cisco Asset Tags**.

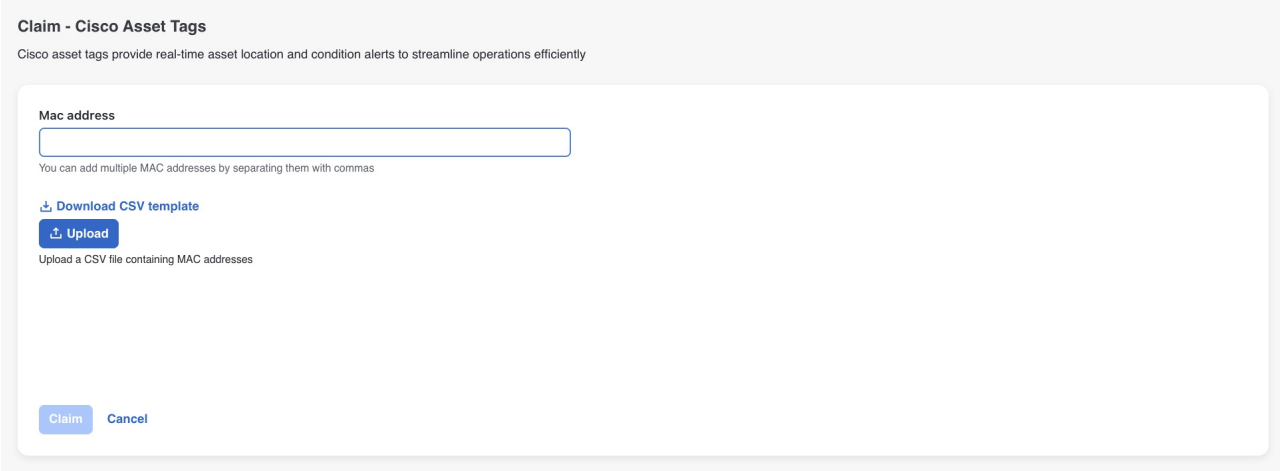
1. **Meraki MT**: Select **Meraki MT** and click **Next**. Enter the **Serial ID** and click **Next**.

   Figure 40: Serial ID tab



2. **Cisco Asset Tags**: Select **Cisco Asset Tags** and click **Next**. The **Claim - Cisco Asset Tags** page appears. You can add one or more MAC addresses in the **Mac address**. Download the CSV template by clicking on the **Download CSV template** button and re-upload a CSV file containing MAC addresses using the **Upload** button. Click **Claim to confirm**. The number of tags claimed or failed is displayed.

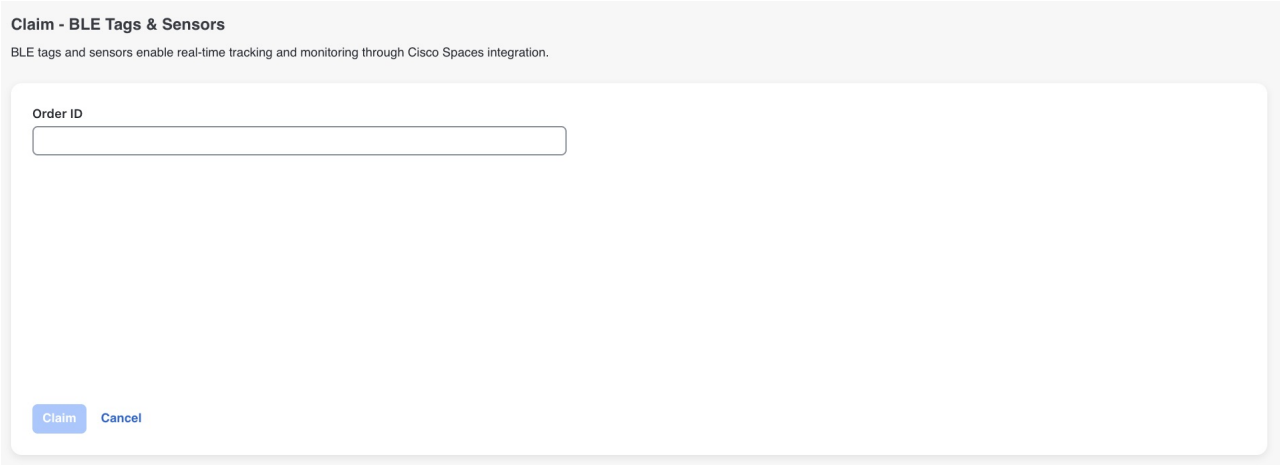
Figure 41: Claim-Cisco asset tags tab



b) **Third-Party devices from IoT Device market place**: allows third-party **BLE Tags and Sensors** and **UWB Tags**.

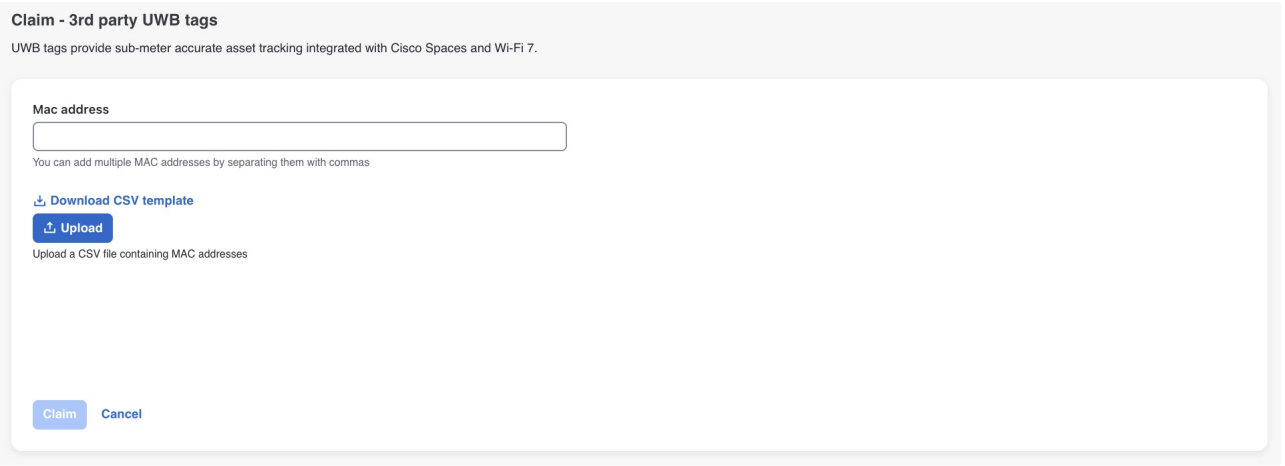
1. **BLE Tags and Sensors**: Select **BLE Tags and Sensors** and click **Next**. The **Claim - BLE Tags & Sensors** window appears. Enter the **Order ID** and click **Claim**.

Figure 42: BLE tags & sensors tab



2. **UWB Tags**: Select **UWB Tags** and click **Next**. The **Claim - 3rd party UWB tags** window appears. You can add one or more MAC addresses in the **Mac address**. Download the CSV template by clicking on the **Download CSV template** button and re-upload a CSV file containing MAC addresses using the **Upload** button. Click **Claim to confirm**. The number of tags claimed or failed is displayed.

Figure 43: 3rd party UWB tags tab

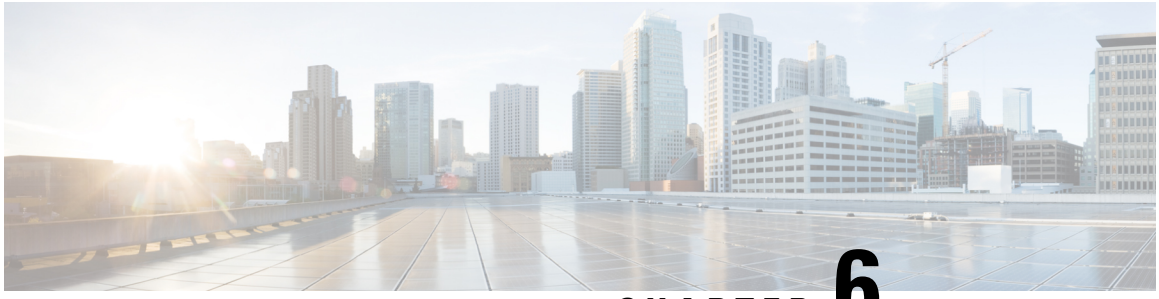




PART III

Manage

- Dashboard, on page 47
- Wireless APs, on page 49
- BLE Devices, on page 71
- Wired, on page 85



CHAPTER 6

Dashboard

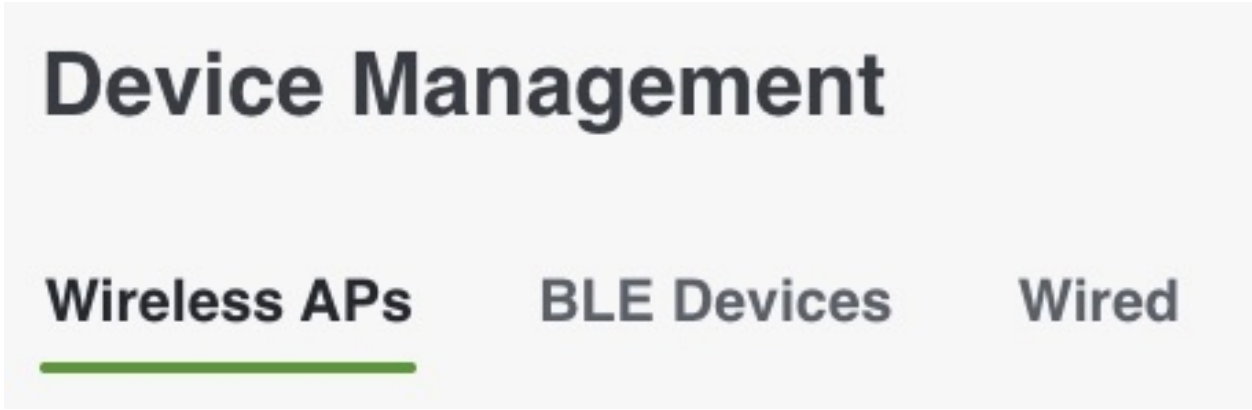
- Dashboard view of devices, on page 47
- Configuring beacons, on page 47

Dashboard view of devices

Choose **IoT Services** > **Manage** and select these device types to view an overview of that device:

- **Wireless APs**
- **BLE Devices**
- **Wired**

Figure 44: Dashboard View of Devices



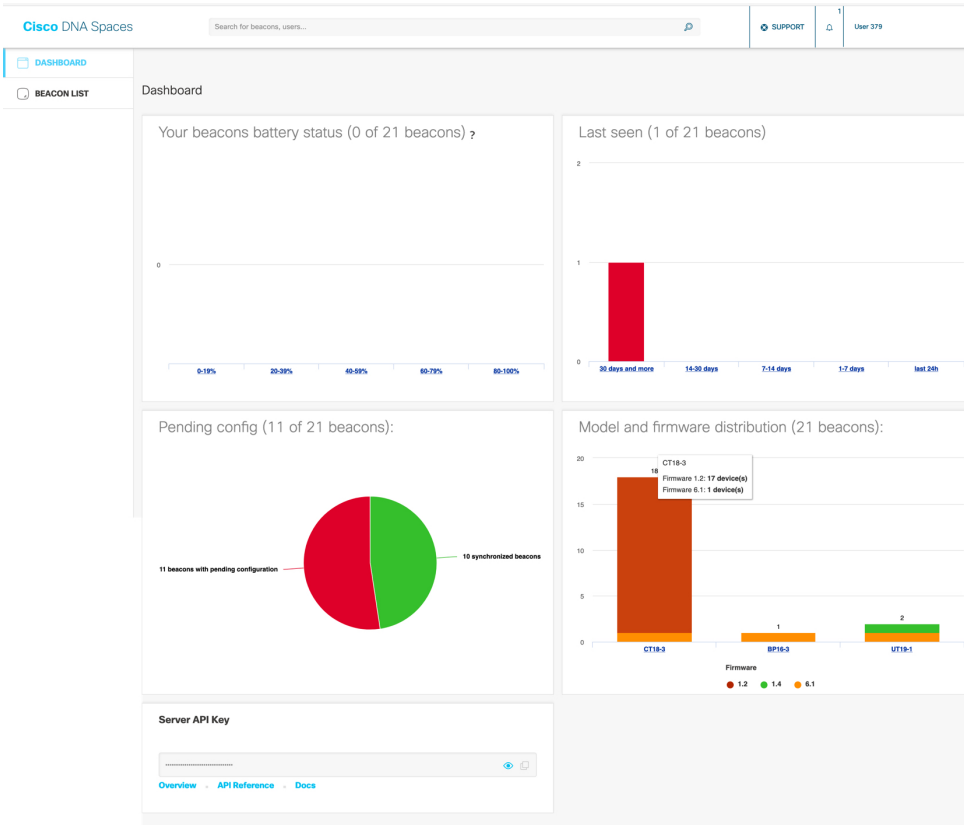
Configuring beacons

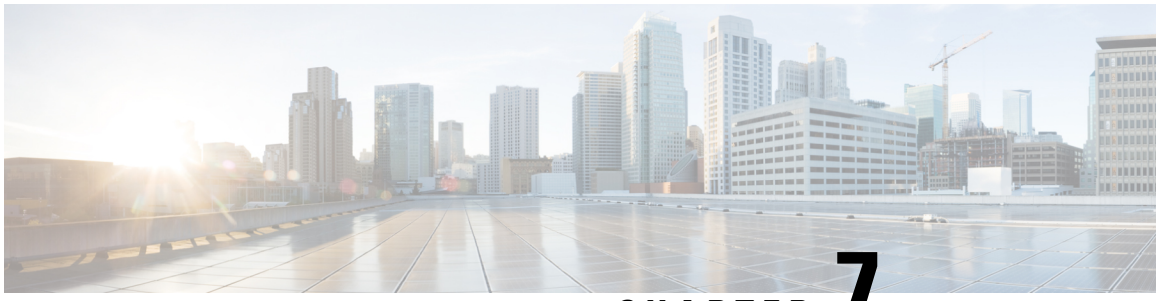
Navigate to **IoT Service** > **Manage** > **BLE devices**. Click the **MAC address** in the claim bucket and then expand **Beacon Configuration** section. Click **Advance Configuration**. After this, the model opens. Once you confirm the configuration, the process continues as designed.

The Device Manager dashboard gives you a general overview of your beacon infrastructure. All beacons claimed by IoT Service are visible on the Device Manager dashboard. You can see actionable graphs which

allow you to navigate quickly to a subset of devices. For example, beacons with 0 to 19 percent battery life, or all beacons with the same underlying firmware or model.

Figure 45: The Device Manager Dashboard





CHAPTER 7

Wireless APs

- AP Gateways, on page 49
- AP Beacons, on page 54
- AP Sensors, on page 65

AP Gateways

Depending on the type of Cisco access points (AP), you can configure an AP as one of these types of gateways:

- **Gateways deployed**: Gateways that are configured and actively deployed in your network. These gateways can connect to IoT sensors and transmit their data to the IoT Sensor Connect application.
- **Advanced BLE Gateway**: The advanced BLE gateway is an AP that is installed with an IoX Application. Using the installed IoX Application, you can configure floor beacons on the Cisco-partnered Device Manager website.
- **Base BLE Gateway**: The Base BLE gateway is a type of AP that you can configure in different modes such as Transmit, Scan, or Dual.
- **Gateways not deployed**: Gateways that are available in the application but have not yet been configured or deployed. Deploy these gateways to begin connecting and monitoring IoT sensors.

You can configure this AP which is now a base or advanced gateway in **Scan** mode, **Transmit** mode, or **Dual** mode. In the **Transmit** mode or **Dual**, mode the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles.

In the **Scan** mode, the AP can scan the vicinity for other BLE devices. Using gRPC on the AP, the AP sends the scanned data to Cisco Spaces: Connector. The AP can also receive telemetry data from floor beacons. The IoT Service dashboard decodes and displays this information.

To configure and add an AP as a BLE gateway, refer to Activate IoT services (Wireless).

Configure AP gateways

Set up and manage physical gateways on access points for IoT services, BLE functions, and application deployment.

In Cisco Spaces, configuring wireless AP gateways allows you to manage IoT services on access points, control BLE settings, deploy and maintain IOx applications, and upload diagnostic files for support.

Before you begin

Ensure that you have configured an AP as a base gateway or as an advanced gateway.

Procedure

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Manage** > **Wireless APs** > **AP Gateways**.

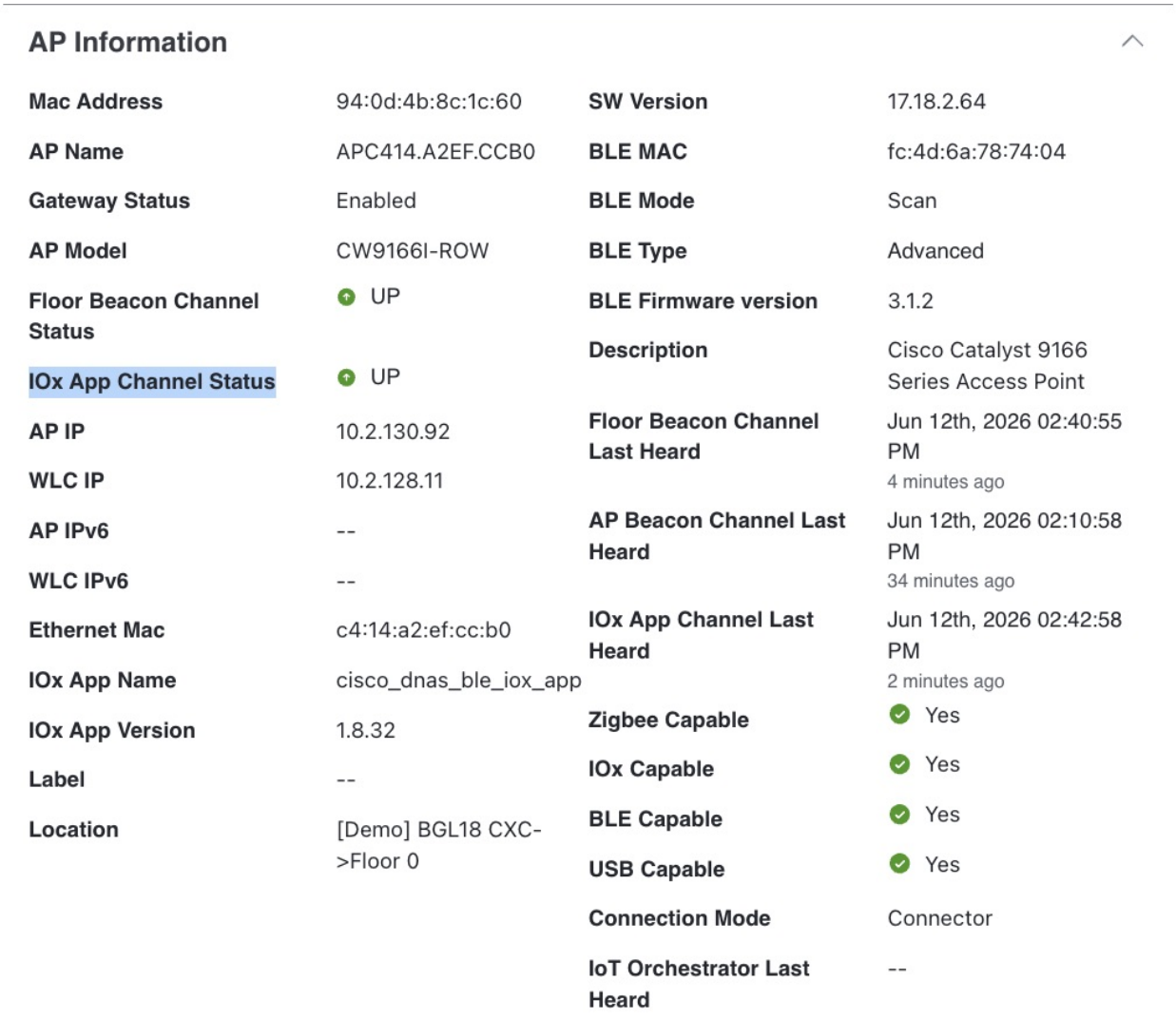
Step 2 Click the MAC address of the AP to open the detailed **AP** page. The **AP Configuration** tab appears.

Figure 46: AP Configuration tab



Step 3 Click the **AP Information** panel to view details such as **MAC Address**, **AP Name**, **Gateway Status**, **AP Status**, **Floor Beacon Channel Status**, **IOx App Channel Status** etc.

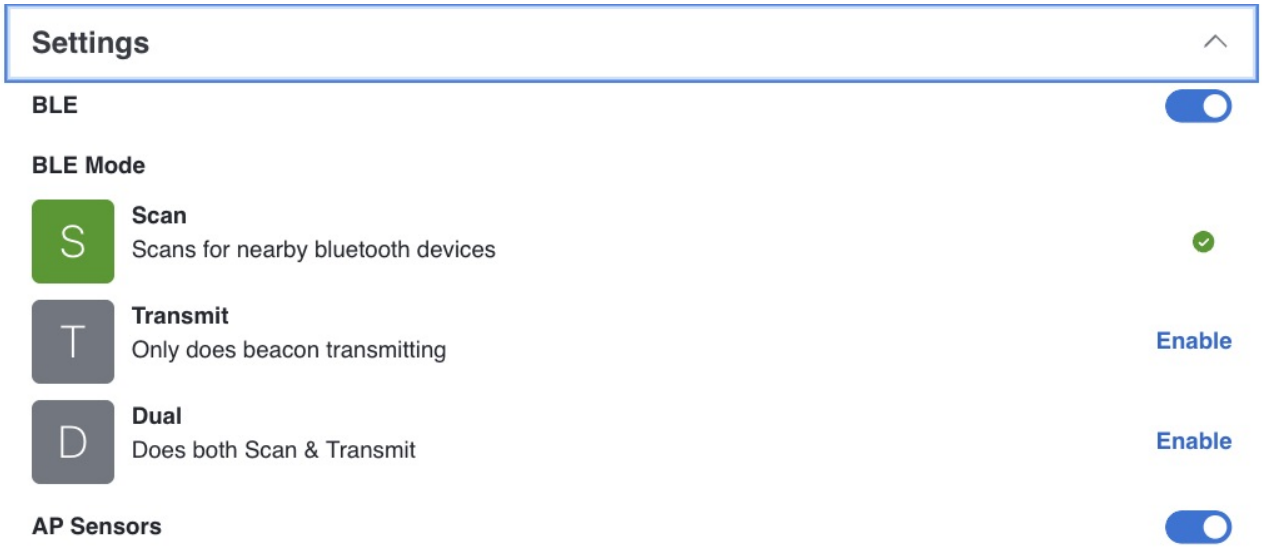
Figure 47: AP Information tab



Step 4 Click the **Settings** panel to configure the **BLE** details. Toggle the **BLE** option to turn on the different BLE modes such **Scan**, **Transmit** and **Dual**.

a) Toggle the **AP Sensors** button to turn it on.

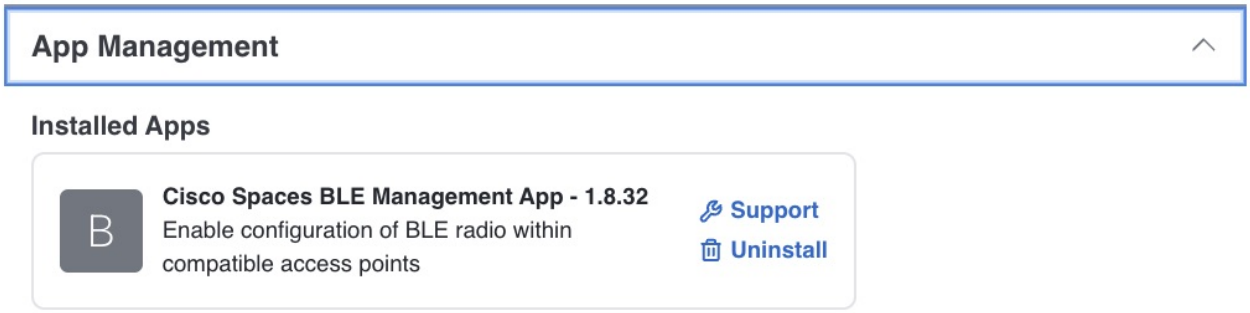
Figure 48: Settings tab



Step 5 Click the **AP Management** panel to install, uninstall or upgrade an IOx Application on a gateway. Do one of these:

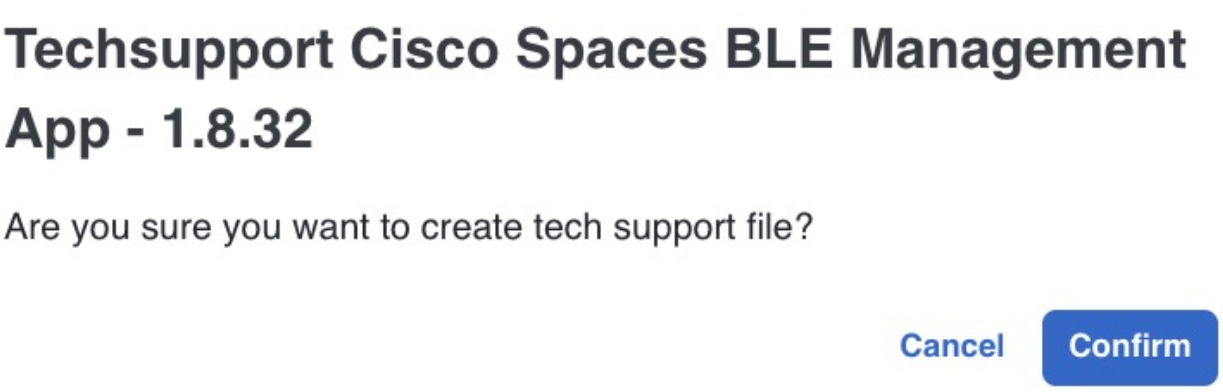
- To uninstall, click the uninstall icon near Cisco Spaces: BLE Management App.
- To upgrade, check whether an upgrade version is available near Cisco Spaces: BLE Management App and click it.
- To upload tech-support files to the connector, click the gear icon.

Figure 49: App Management tab



a) The support gear icon allows you to upload log files to connector. You can also download these files to assist a technical support team.

Figure 50: Techsupport window



b) Enter the credentials needed for authentication on the AP.

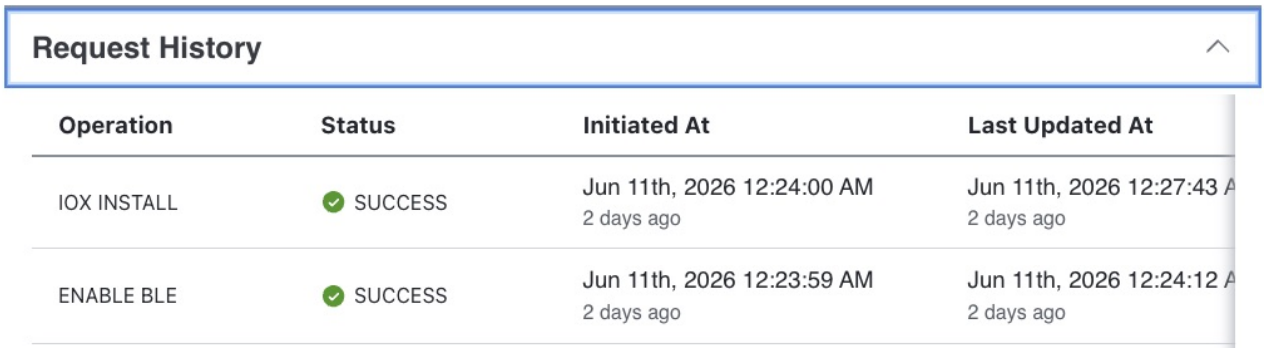
Note
The authentication request to the APs includes these credentials. After authentication, IoT Service does not retain the credentials.

The AP designated as the advanced gateway receives these change requests. You can observe the progress on the displayed page.

Step 6 Click on the **Request History** panel to check the status of deployment. The **Status** column shows the status of install, uninstall or upgrade on each AP.

a) SUCCESS: The application was uninstalled or upgraded successfully on the AP.
b) FAILURE: The application uninstall or upgrade on the AP failed.
c) IN PROGRESS: The application is currently being uninstalled or upgraded on the AP.

Figure 51: Request History tab



Step 7 Click the MAC address of the AP and click on the **Action** drop down button to **Manage BLE**, **Manage IOx app**, **Manage Profiles**, **Delete** and **Clear Pending Config**. The options for the first three choices are:

- **Manage BLE**: Enable BLE and Disable BLE
- **Manage IOx app**: Install IOx app and uninstall IOx app
- **Manage Profiles**: Scan mode, dual mode profile and sync

Step 8 Click the MAC address of the desired AP in the tab and then click the **Export** button. The details are downloaded as a .csv file to your local system.

AP Beacons

You can configure your access point (AP) to act as a beacon (AP beacons) by enabling BLE on it.

IoT Service categorizes APs according to their configurations as these:

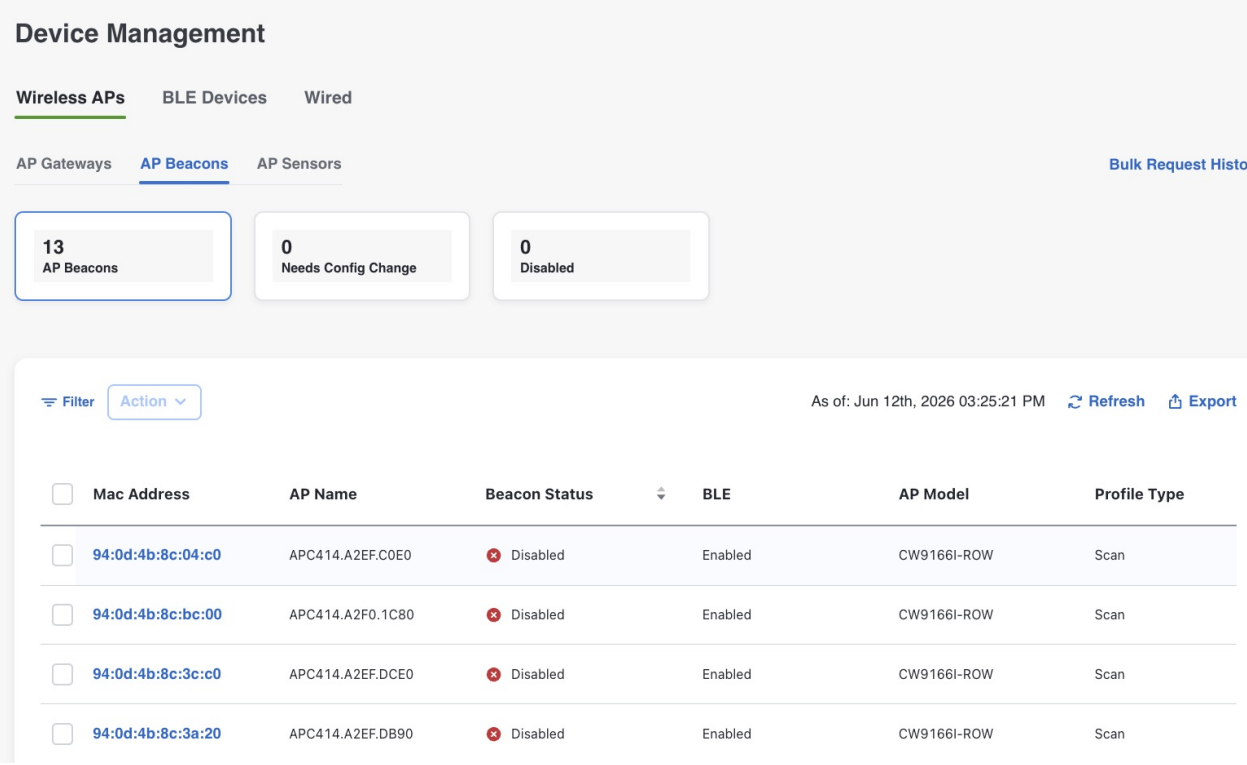
- **Disabled**: APs with BLE disabled. These APs are not scanning or transmitting.
- **Scan Mode**: AP beacons that are only scanning.
- **Transmit Mode**: AP beacons configured in one of the beacon transmit profiles. You can configure up to five iBeacons in this mode.
  - The MAC address advertised in the iBeacon payload is derived from the radio MAC address of the AP. (iBeacon MAC address).
- **Dual Mode**: AP beacons that are transmitting and scanning. You can configure only one iBeacon in this mode.
  - The MAC address advertised in this mode is the default MAC address of the AP's BLE chip, which is preset by the chip vendor (For both Eddystone and iBeacon single advertisement profiles)
- **Needs Config Change**: AP's that have an error in configuration. You can configure these APs in Scan Mode, Dual Mode, or the Transmit Mode.

You can configure an AP Beacon in one of these transmit modes.

- iBeacon

You can also see all the APs irrespective of their configurations under **All Profiles**.

Figure 52: Various Profiles of AP Beacons



You can also enable telemetry on the AP beacon and collect sensor information.

iBeacon transmit mode

A single AP can support up to five iBeacons in the transmit mode. Each iBeacon has a unique address derived from the base radio MAC address of the AP.

Use Cisco Spaces to configure an iBeacon's payload.

These are some terms related to iBeacons:

- **Transmit mode**: Mode that allows nearby devices to pick up an iBeacon's broadcasting or advertising signals.
- **Advertisement payload**: Data broadcast by an iBeacon. The advertisement payload contains information relevant to the iBeacon's purpose, such as the iBeacon's location. Use Cisco Spaces to configure this payload.
- **iBeacon MAC address**: Unique identifier of an iBeacon on the network that helps other devices recognize and differentiate one iBeacon from another. This address is part of the iBeacons' advertisement payload. The AP uses the AP's own base radio MAC address to derive this unique address. The address is derived by adding a predefined address block value to the last byte of the base radio MAC address and decrementing this value by the beacon ID.

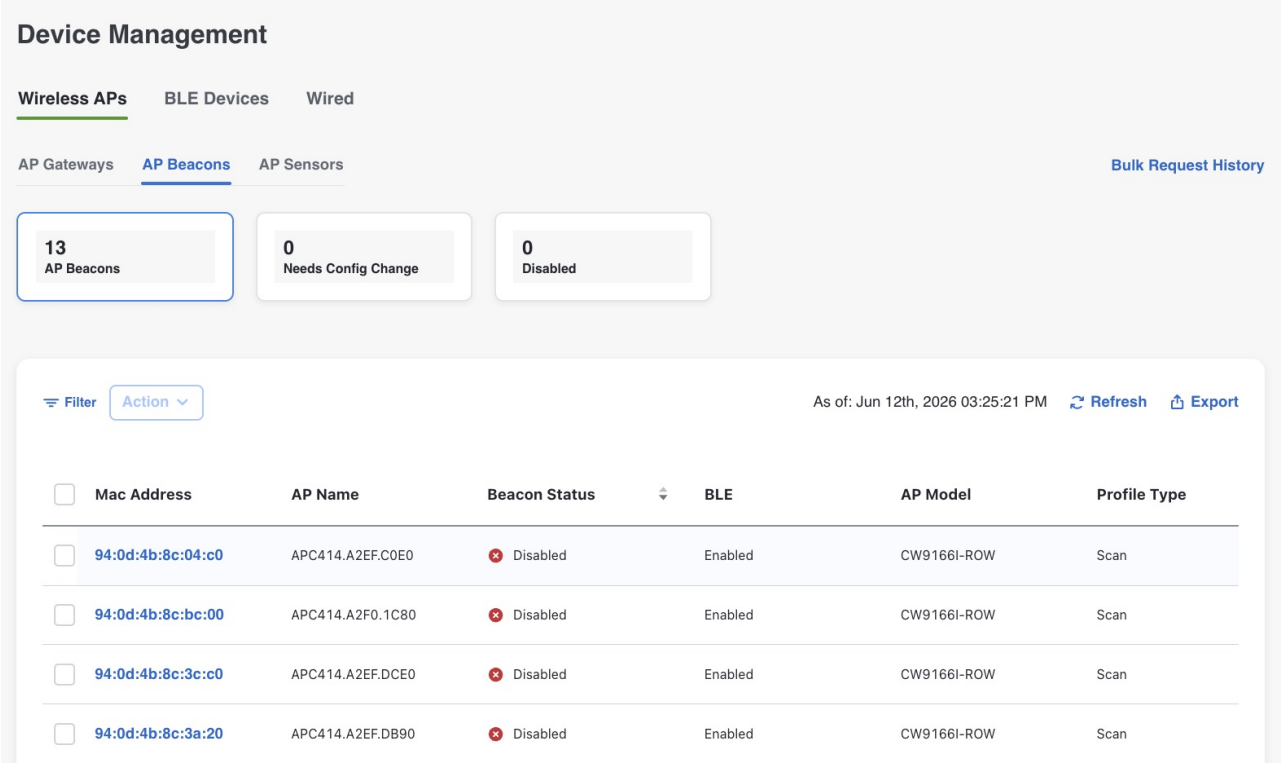
Configure AP as a beacon in scan mode

You can configure an AP as a beacon in the scan mode.

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, click **IoT Services** > **Manage** > **AP Beacons**, and then click **AP Beacons**.

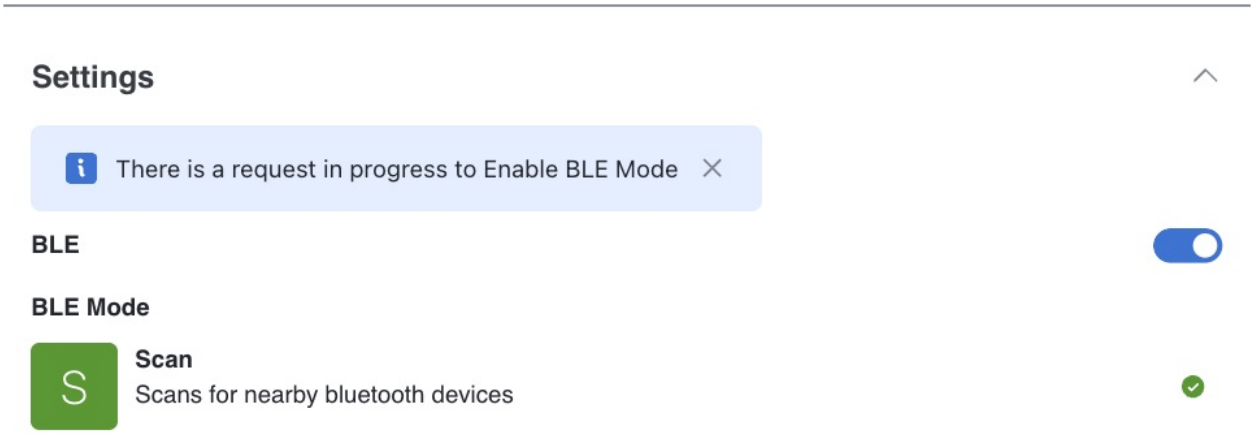
Figure 53: List of AP Beacons



Step 2 Click the **Disabled** tab, if the count is greater than zero. Click the MAC address of one of the listed APs to open a detailed view.

Step 3 Click **BLE** in the **Settings** panel.

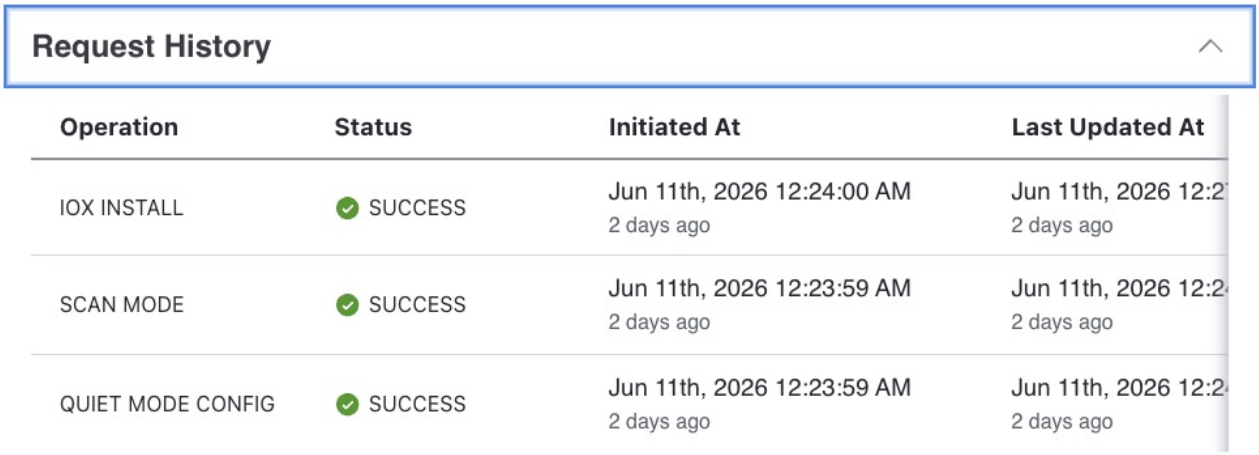
Figure 54: Enable BLE panel



AP is enabled as a beacon in **Scan** mode. You can observe the AP under the **Scan** tab.

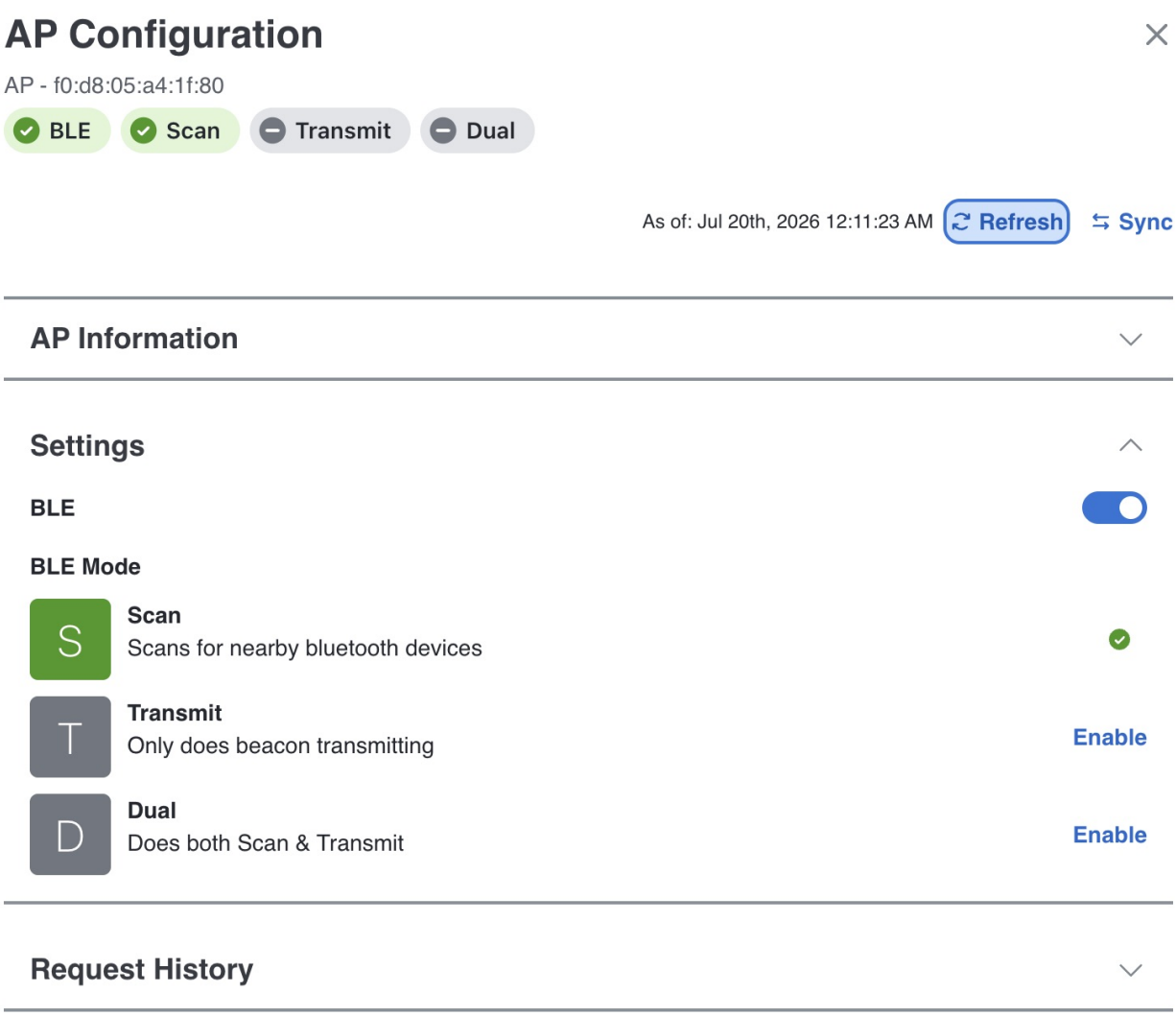
Step 4 From the **Request History** panel, observe the status of the configuration change you requested.

Figure 55: Request History panel



Step 5 Click the **Refresh** button. The settings will update and display the configuration status.

Figure 56: Configuration Status



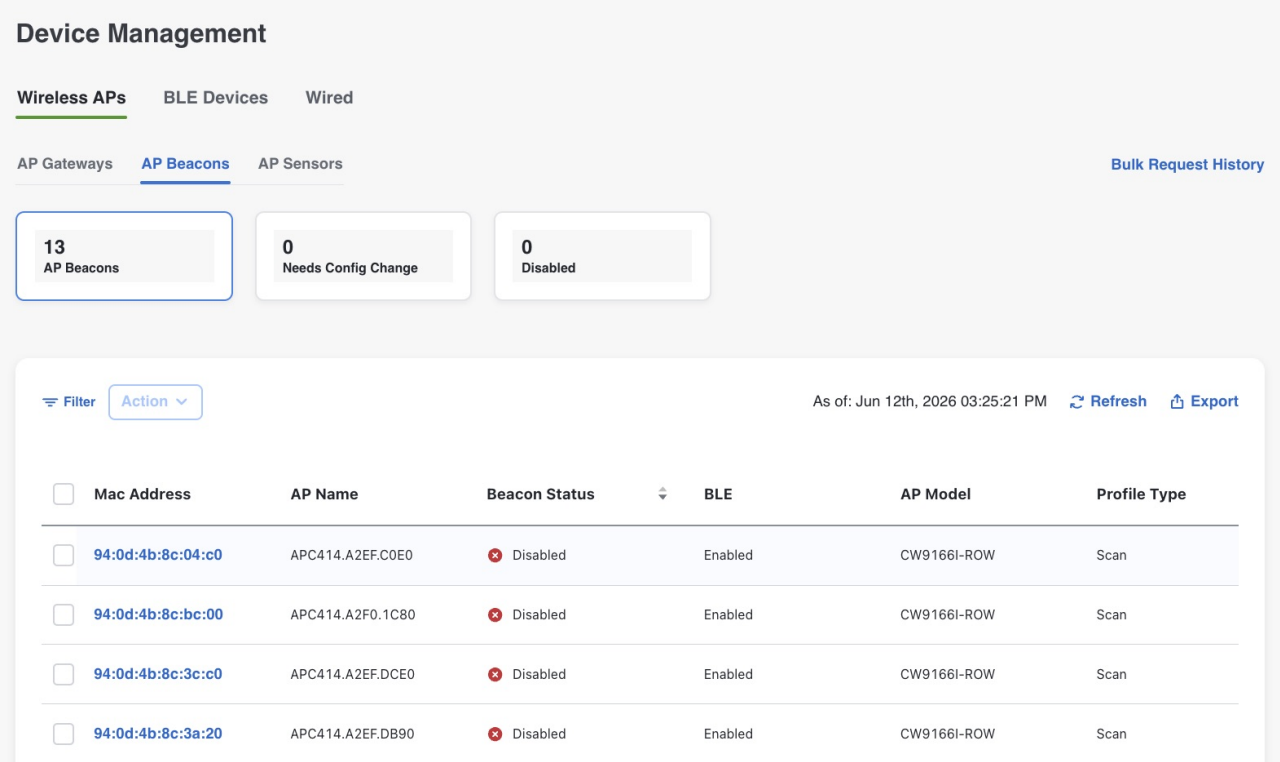
Configure AP as a beacon in transmit mode

You can configure an AP as a beacon in transmit mode.

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, click **IoT Services** > **Manage** > **AP Beacons**, and then click **AP Beacons**.

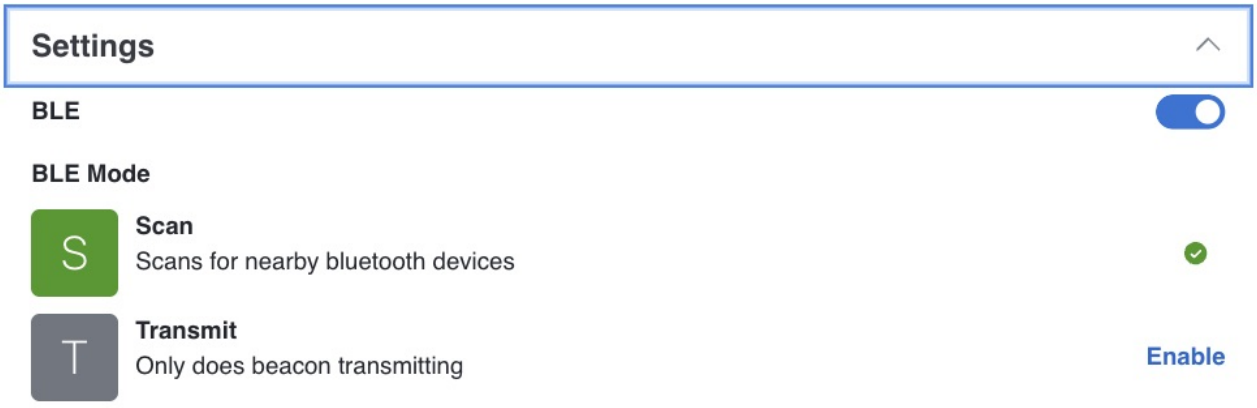
Figure 57: List of AP Beacons



Step 2 Click the MAC address of one of the listed APs to open a detailed view.

Step 3 In the **BLE mode** area under the **BLE** panel, click **Enable** for the **Transmit** option.

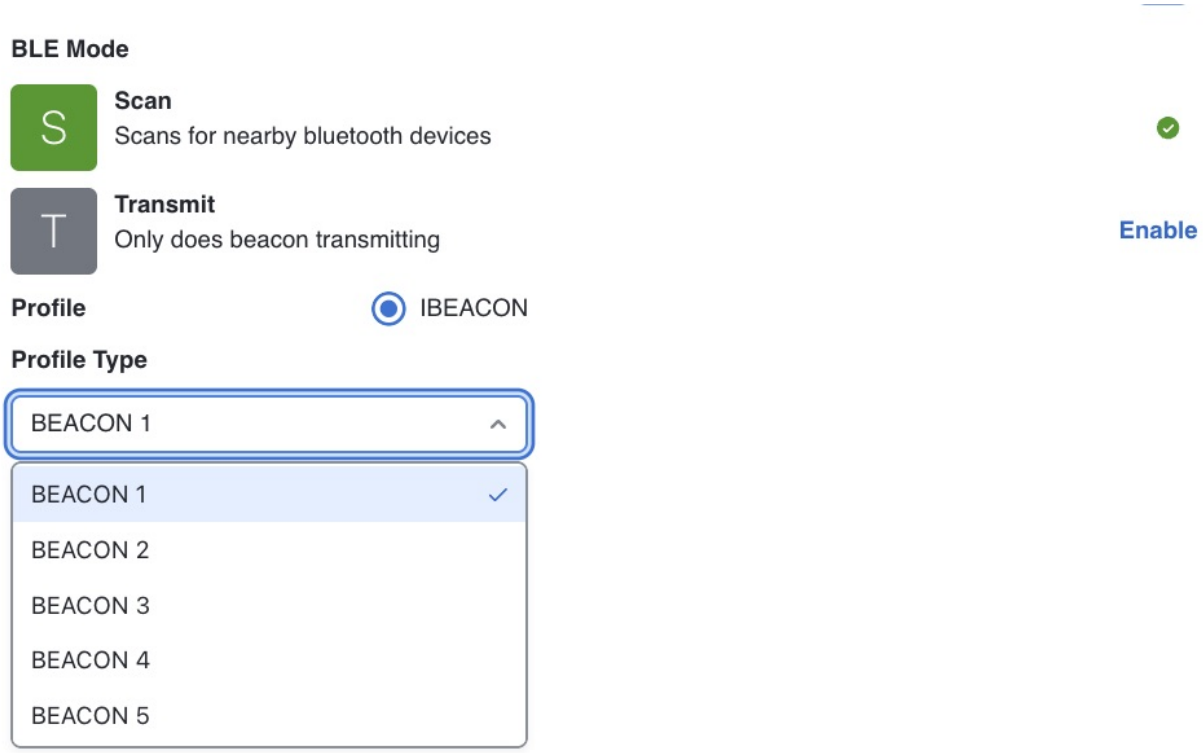
Figure 58: Enable BLE



Step 4 Configure this beacon in the **Enable Transmit Profile** area. .

- Check the checkbox to enable **iBeacon**. From the **Profile Type** drop-down, select one of the beacons.

Figure 59: Configuring an AP as an iBeacon

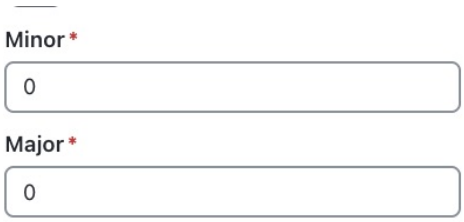


Note
APs can support up to five iBeacons in the **Transmit** mode. For more information, refer to iBeacon transmit mode, on page 55.

AP is enabled as a beacon in **Transmit** mode. You can observe the AP under the **Transmit** tab.

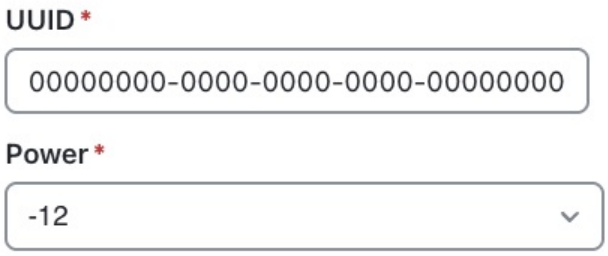
Step 5 Set the **Minor** and **Major** parameters. By default, it is zero. The valid range is between zero and 65535.

Figure 60: Minor and Major config



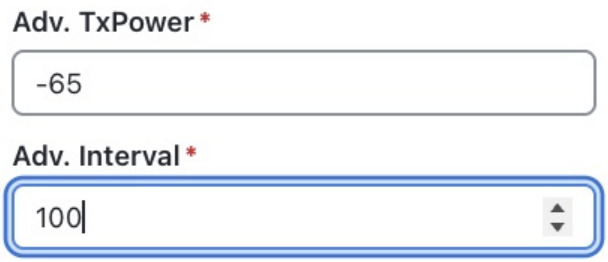
Step 6 Set the **UUID** value and select a **Power** value from the drop-down list.

Figure 61: UUID and Power config



Step 7 Set the **Adv. TxPower** and **Adv. Interval** by selecting the value.

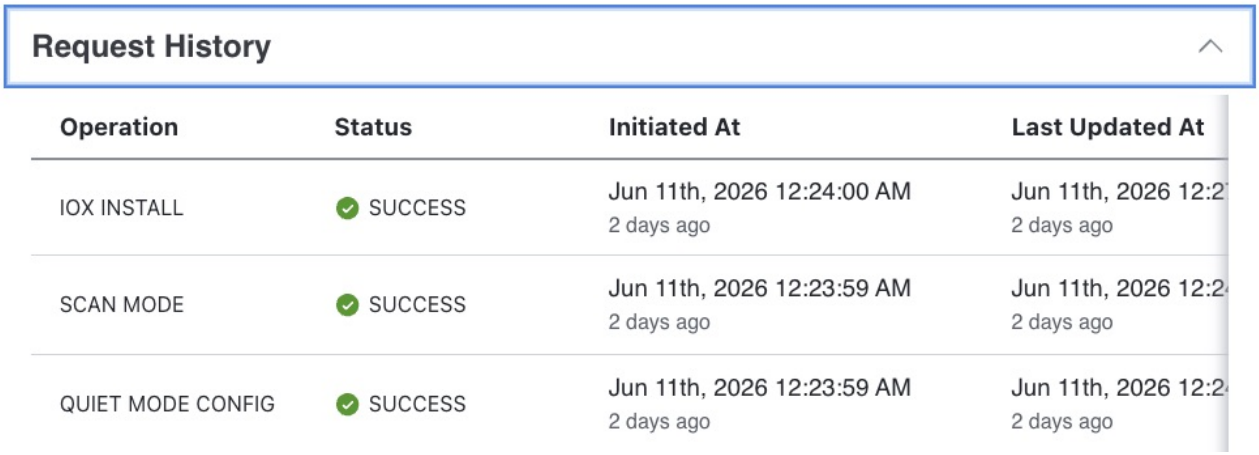
Figure 62: Adv. TxPower and Adv. Interval



Step 8 Click **Save**.

Step 9 From the **Request History** panel, observe the status of the configuration change you requested.

Figure 63: Request History panel



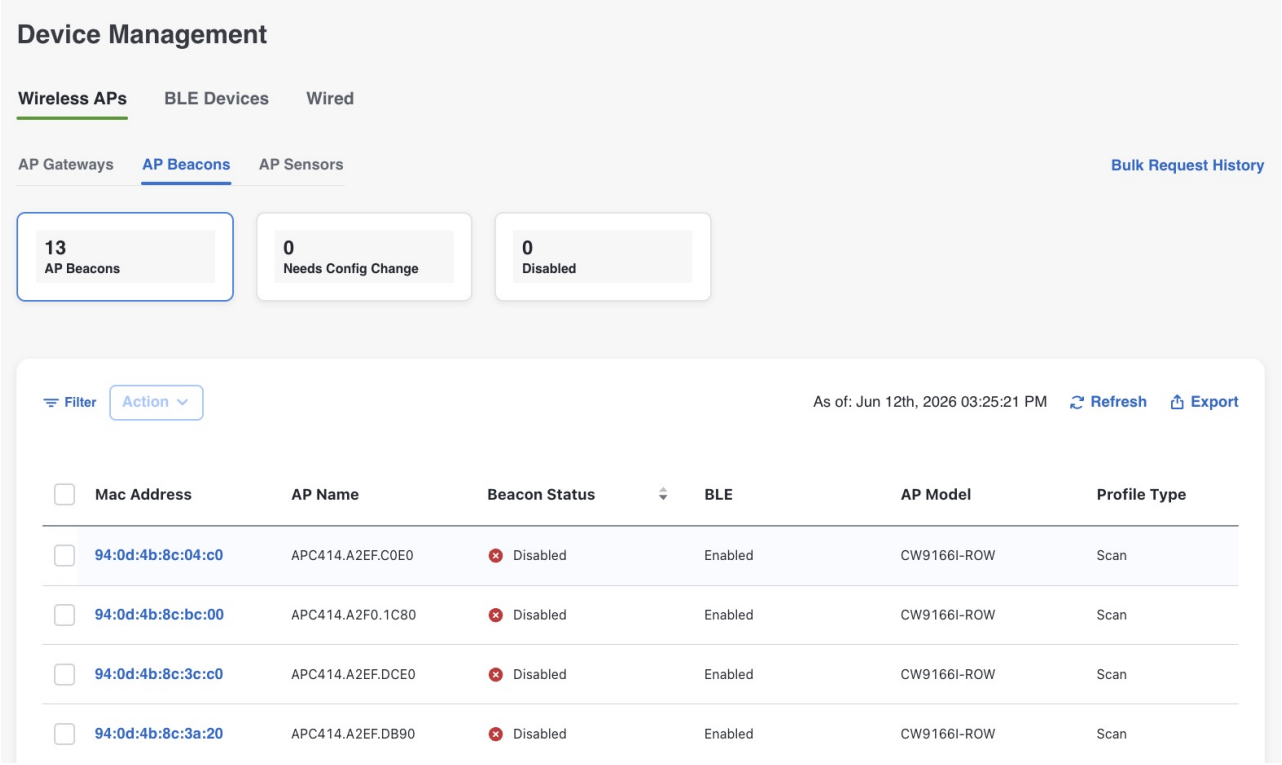
Configure AP as a beacon in dual mode

You can configure an AP as a beacon in dual mode.

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, click **IoT Services** > **Manage** > **AP Beacons**, and then click **AP Beacons**.

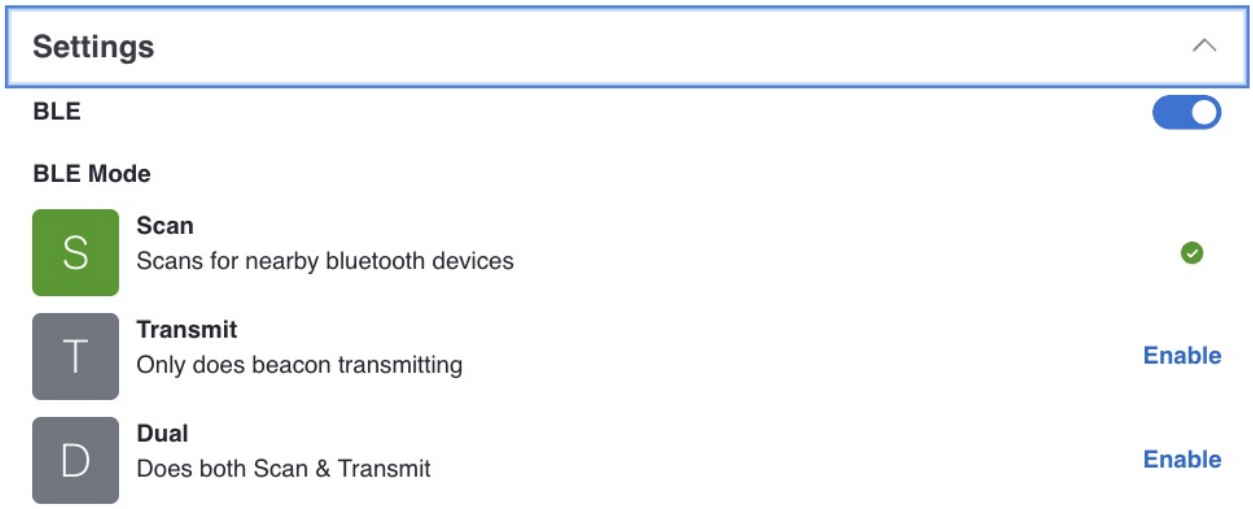
Figure 64: List of AP Beacons



Step 2 Click the MAC address of one of the listed APs to open a detailed view.

Step 3 In the **BLE mode** area under the **BLE** panel, click **Enable** for the **Dual** option.

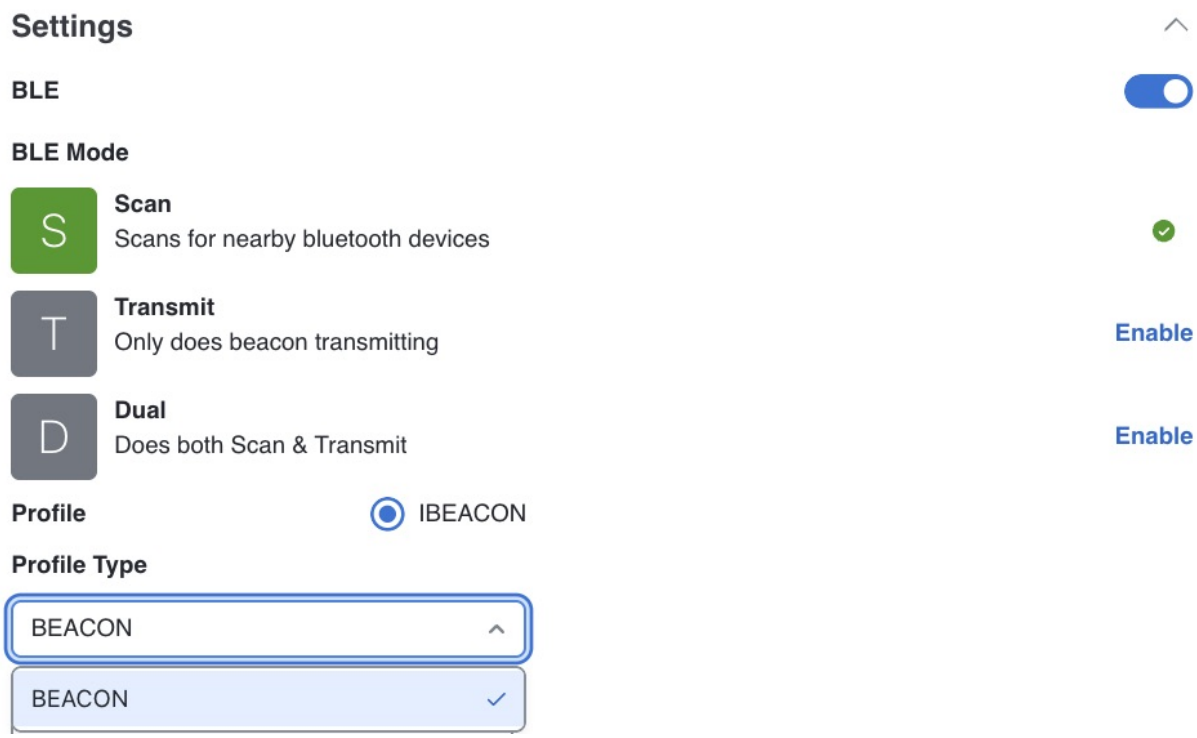
Figure 65:



Step 4 Configure this beacon in the **Enable Transmit Profile** area.

- Check the checkbox to enable iBeacon.

Figure 66: Configuring an AP as an iBeacon



Note
APs can support only one iBeacon in the **Dual** mode. For more information, refer to iBeacon transmit mode, on page 55.

AP is enabled as a beacon in **Dual** mode. You can observe the AP under the **Dual** tab.

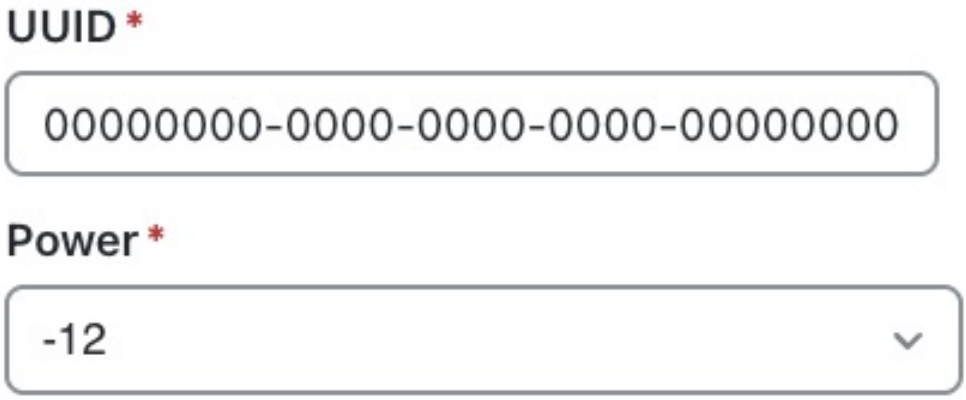
Step 5 Set the **Minor** and **Major** parameters. The valid range is between zero and 65535.

Figure 67: Minor and Major config



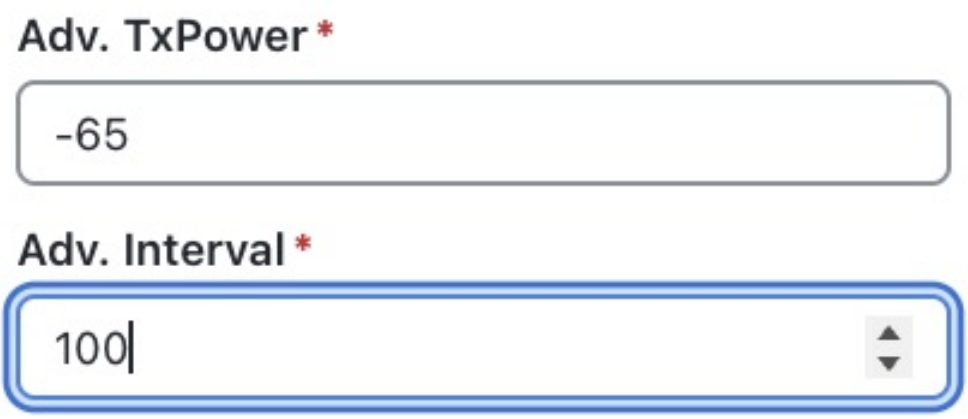
Step 6 Set the **UUID** value and select a **Power** value from the drop-down list.

Figure 68: UUID and Power config



Step 7 Set the **Adv. TxPower** and **Adv. Interval** by selecting the value.

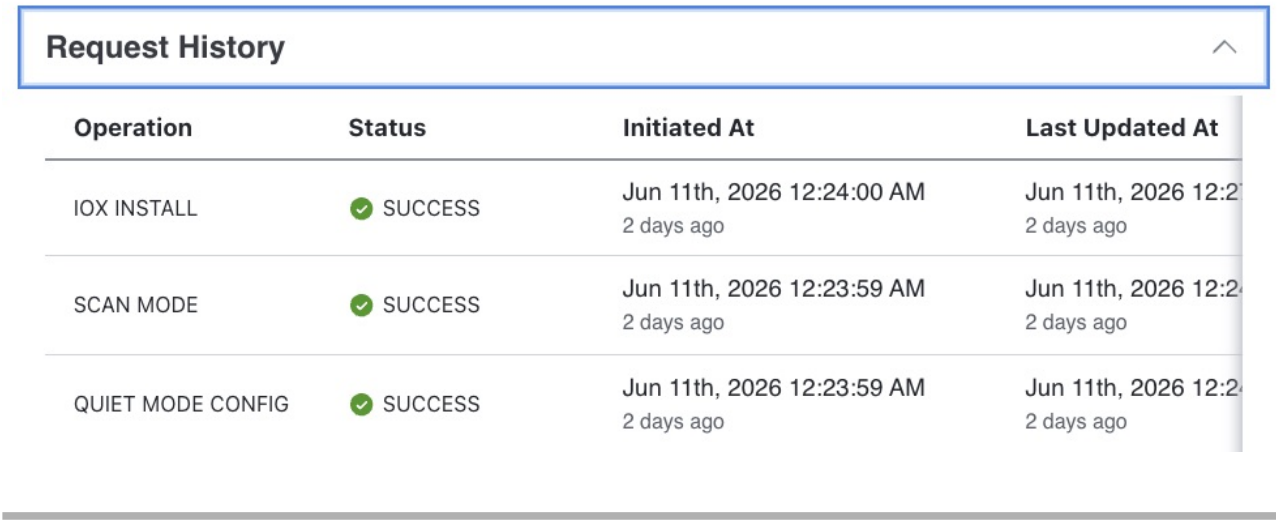
Figure 69: Adv. TxPower and Adv. Interval



Step 8 Click **Save**.

Step 9 From the **Request History** panel, observe the status of the configuration change you requested.

Figure 70: Request History panel



AP Sensors

You can now configure these access points as sensors:

- Cisco Catalyst 9136 Series Access Points
- Cisco Catalyst Wireless 9166I Series Access Points

Once configured as a sensor, you can collect telemetry data using this AP. These sensor values can be configured:

- Temperature

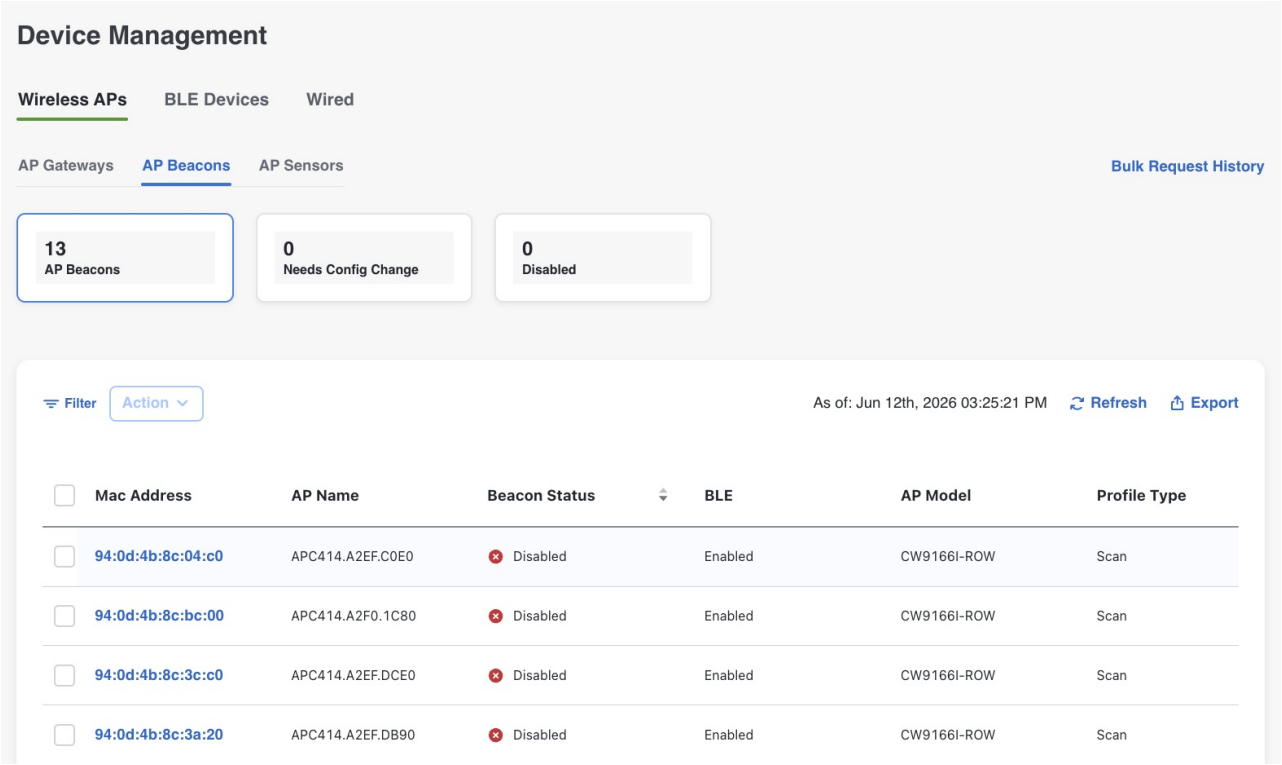
- Relative humidity
- Total volatile organic compound (TVOC), and
- Indoor air quality

Enable or disable an AP sensor

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, click **IoT Services** > **Manage** > **AP Beacons**, and then click **AP Beacons**.

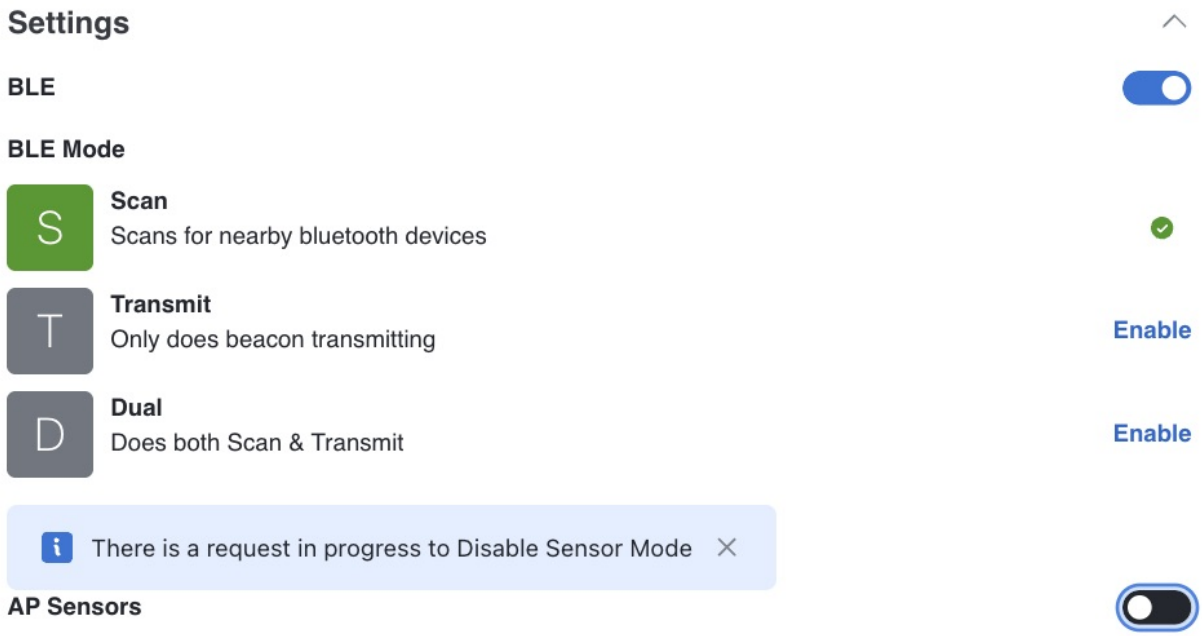
Figure 71: List of AP Beacons



Step 2 Click the AP that you want to configure as a sensor.
The AP Beacons details page opens.

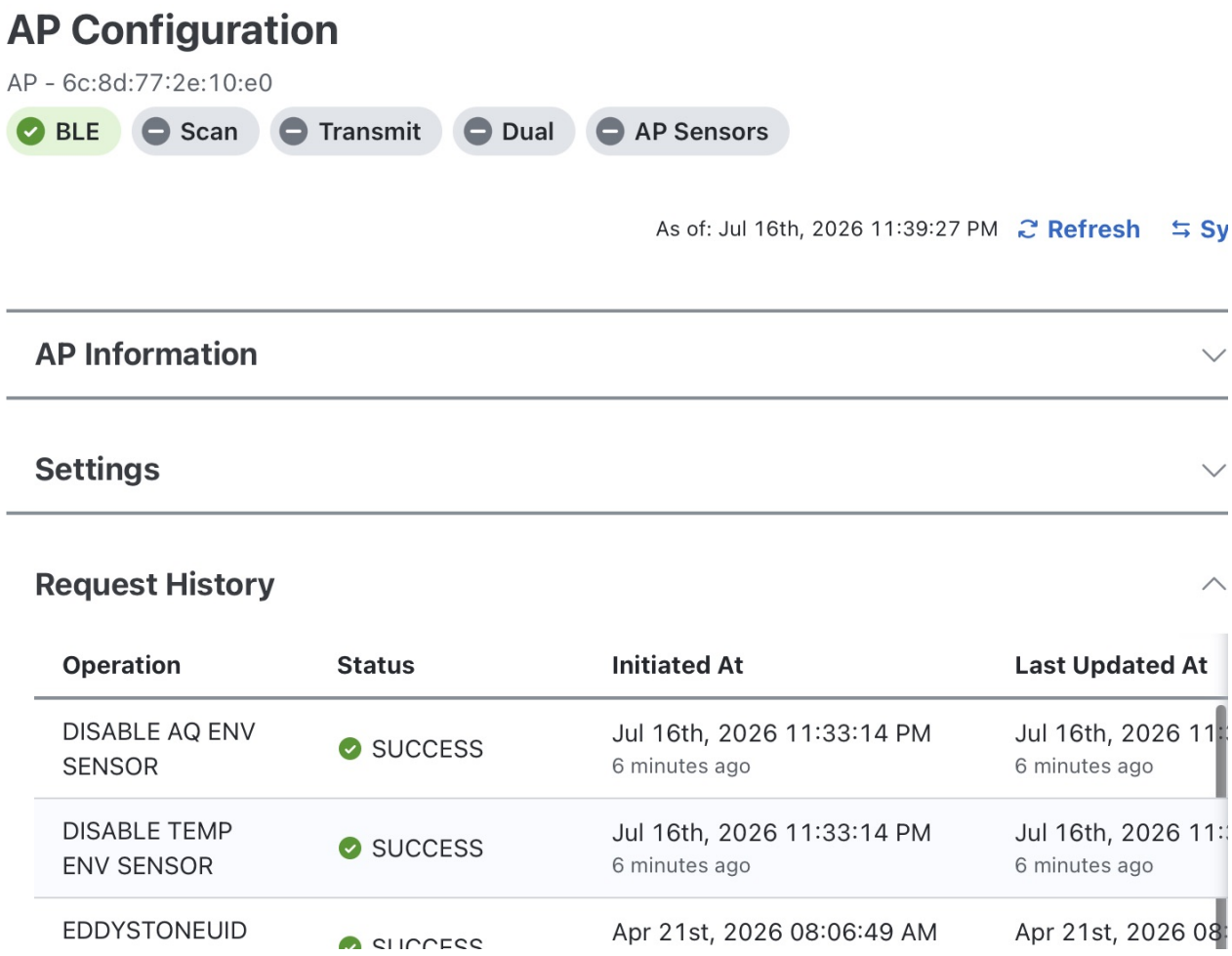
Step 3 In the **Settings** panel, toggle **Sensor** to enable or disable the AP as a sensor.

Figure 72: Enable or disable AP as a sensor



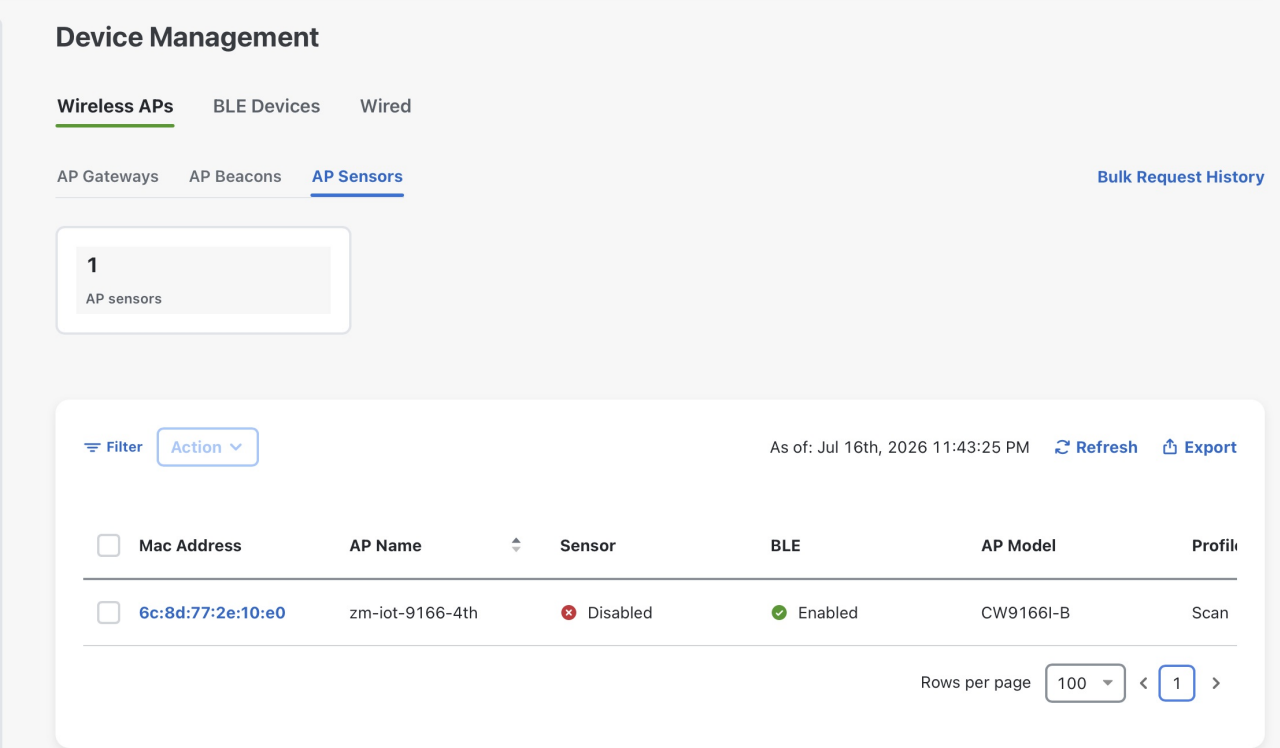
Step 4 After you enable or disable the sensor, the request history shows success for **AQ ENV SENSOR** and **TEMP ENV SENSOR**.

Figure 73: Request History tab



Step 5 The **AP sensor** tab displays whether the sensor column is enabled or disabled for each AP.

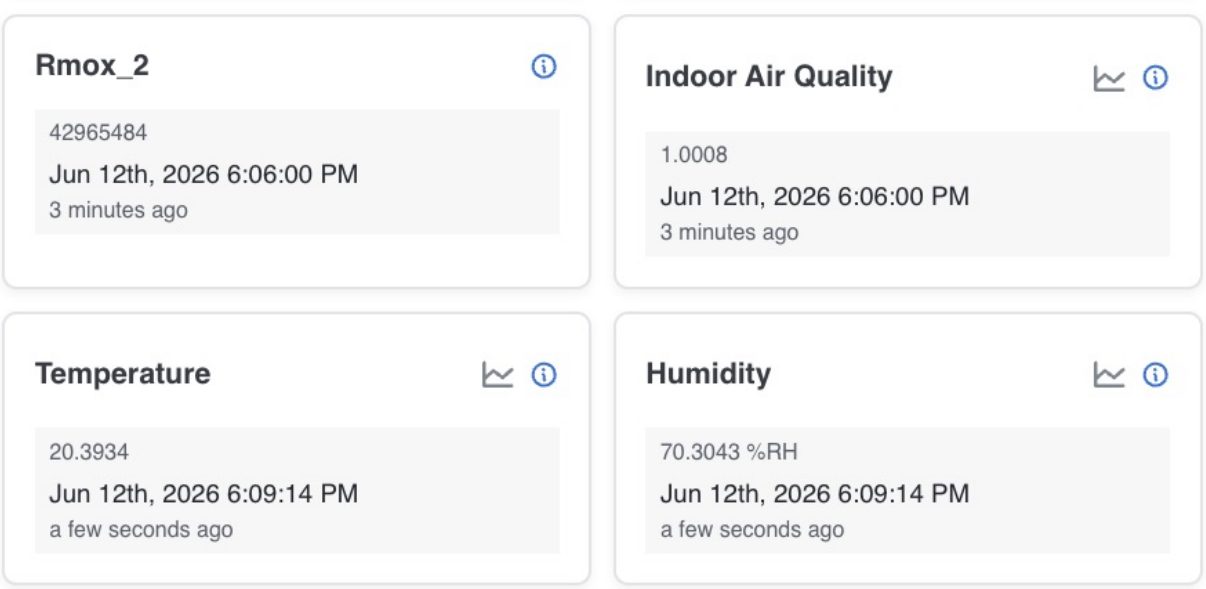
Figure 74: AP Sensor tab

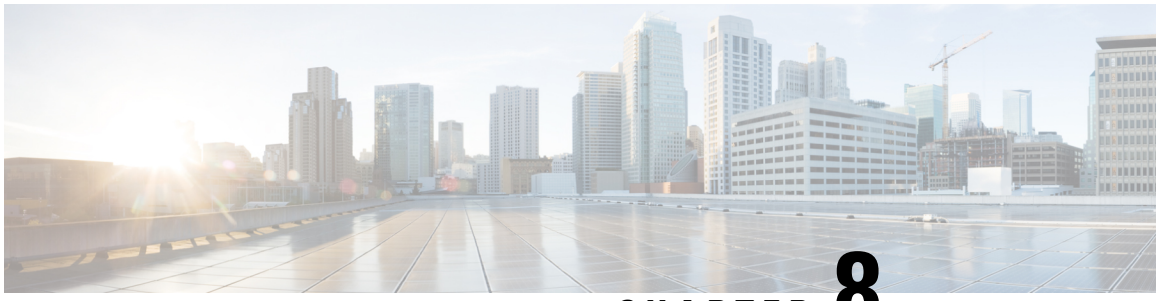


View sensor information

You can view sensor information from the **Sensor Information** area.

Figure 75: View sensor information





CHAPTER 8

BLE Devices

- Discover beacons, on page 71
- Claim a beacon, on page 74
- Configure a beacon on IoT Service, on page 77
- View sensor information, on page 82

Discover beacons

This section shows you how to view the beacons scanned by IoT Service.

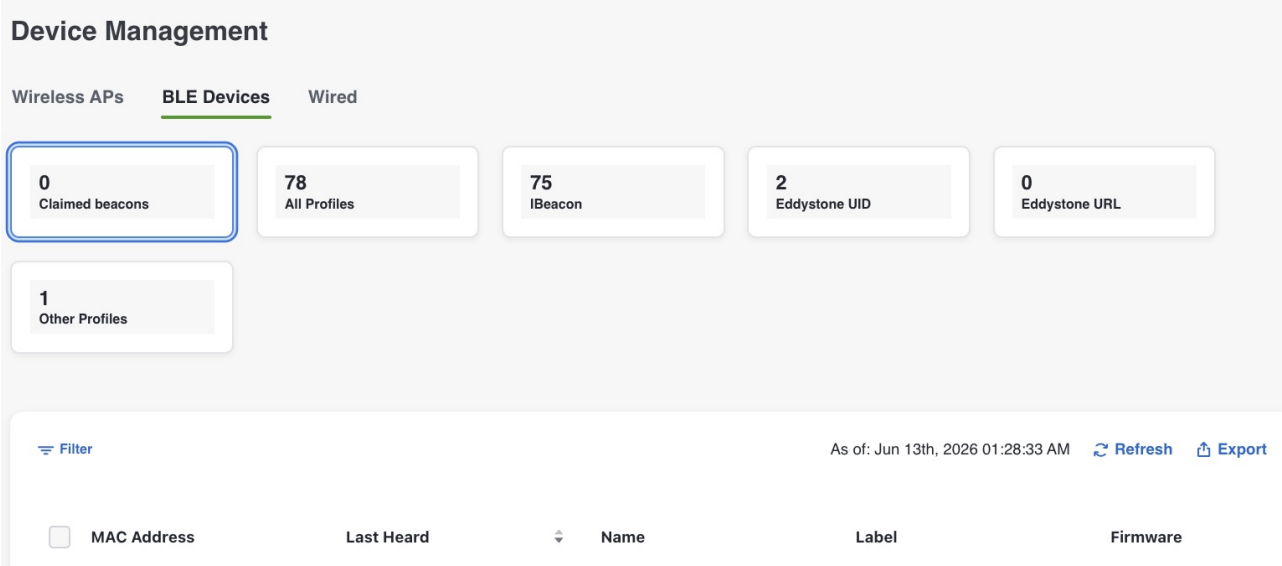
Procedure

Step 1 Navigate to **IoT Services** > **Manage** > **BLE Devices** from the Cisco Spaces dashboard.

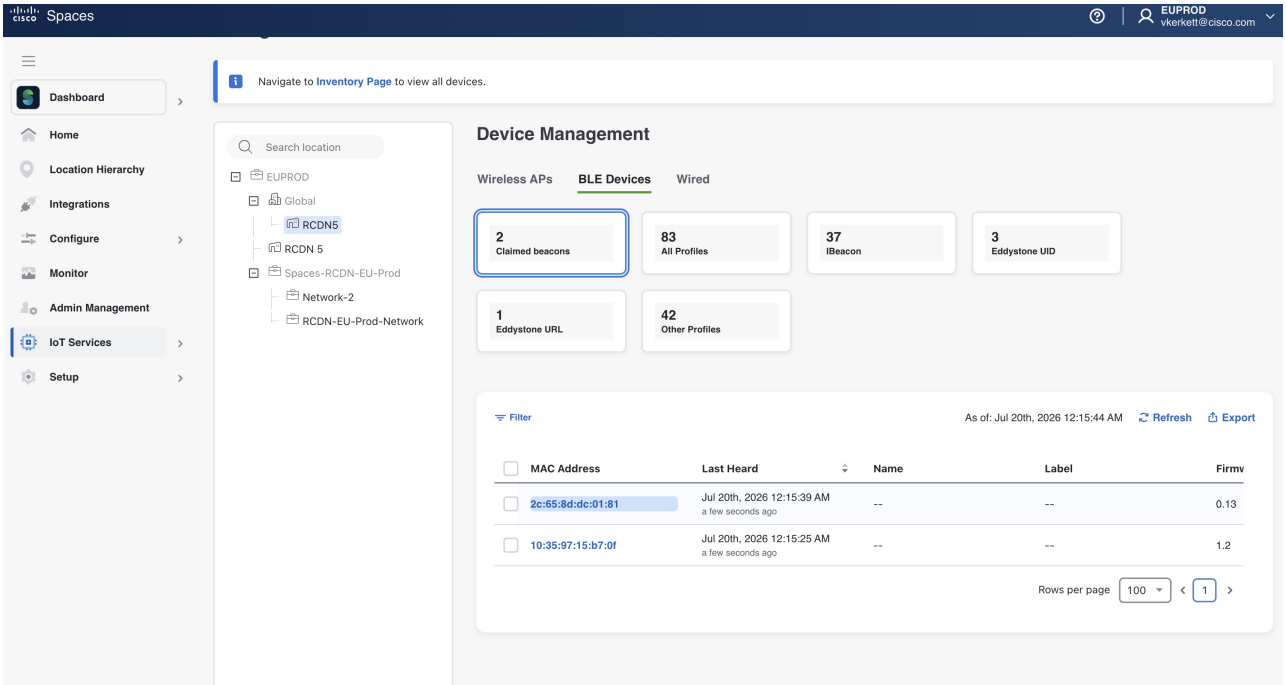
Step 2 Click on one of these: **All Profiles**, **iBeacon**, **Eddystone UID**, **Eddystone URL**, **Other Profiles**.

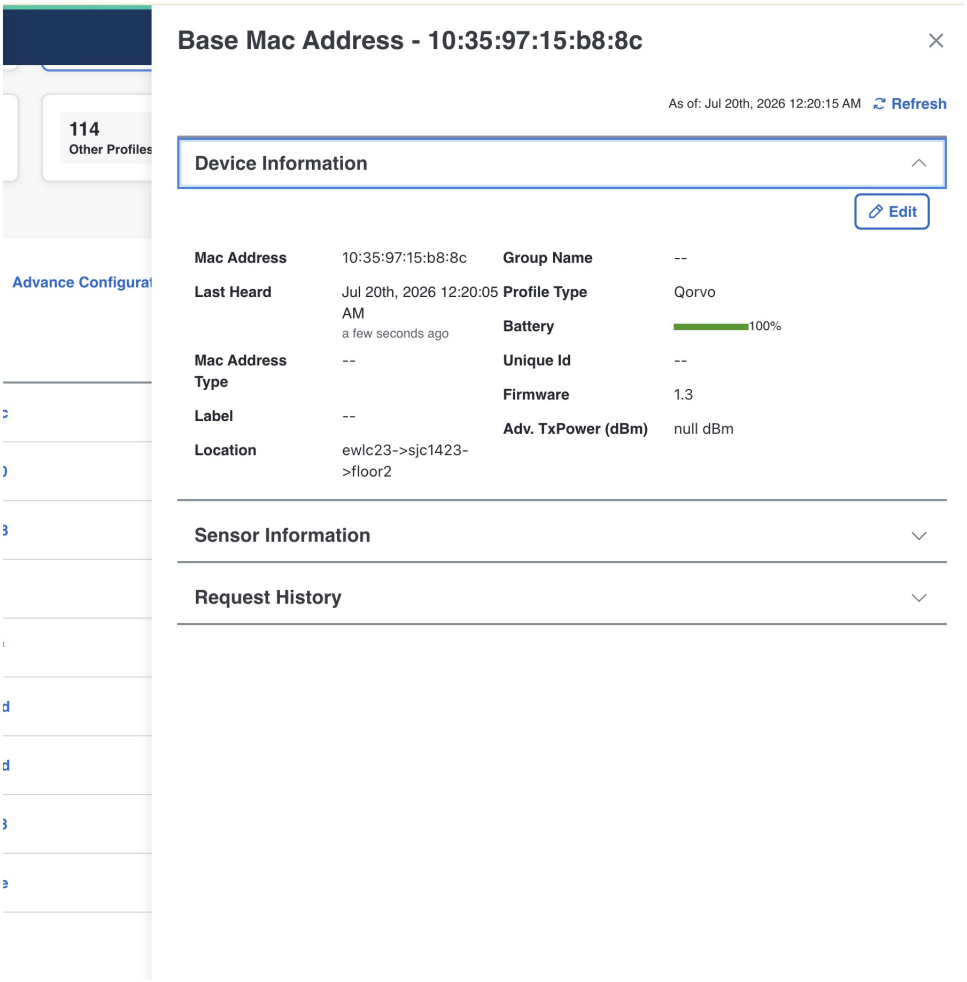
This list is sorted by **Last Heard** by default. You can sort the table by other fields by clicking the arrow beside the column header.

Figure 76: Beacon Details



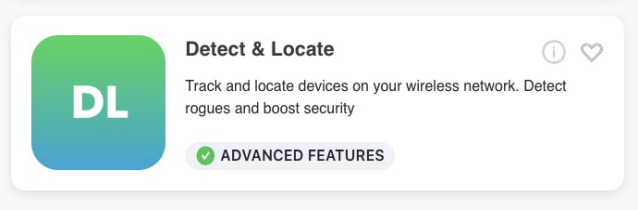
Step 3 Click on the MAC address of the beacon to view further details.

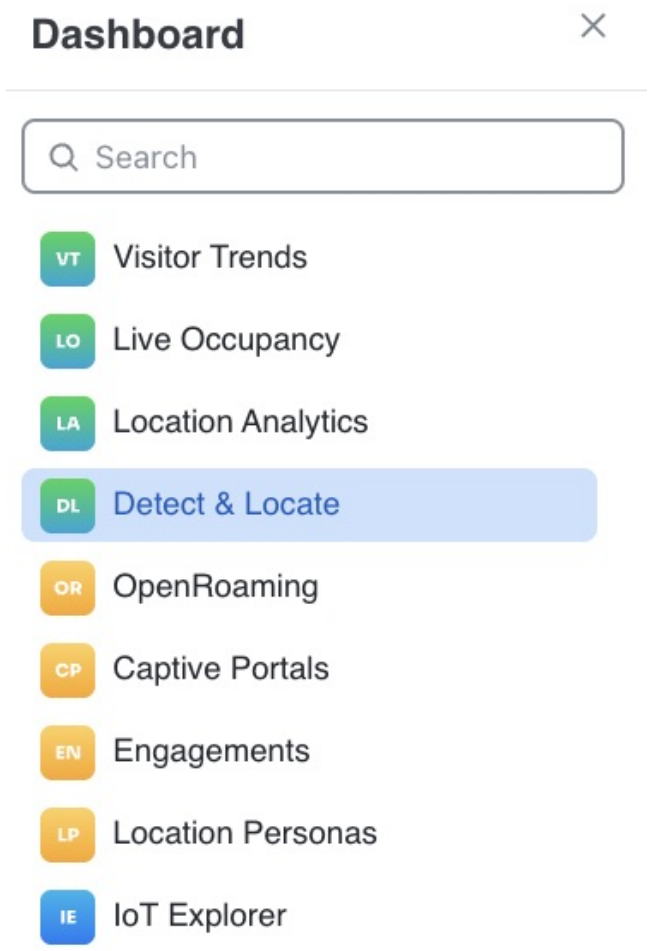




What to do next

You can view location details of the beacon on Cisco Spaces: Detect and Locate.





For more information, refer to Cisco DNA Spaces: Detect and Locate Configuration Guide.

Claim a beacon

Register a beacon device with Cisco Spaces by claiming it using its unique order ID.

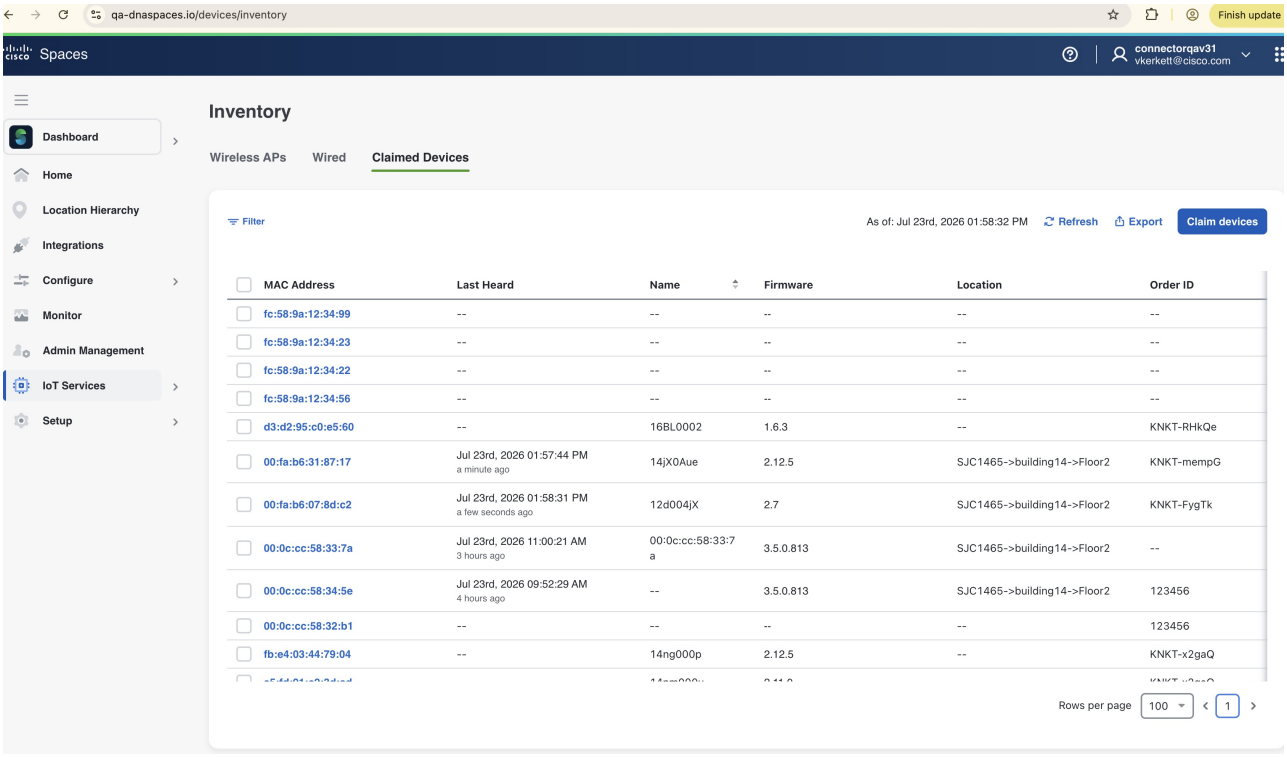
Before you begin

Keep the order ID of the beacon ready. You have received the order ID through an e-mail and physically along with the packaging of the beacon.

Procedure

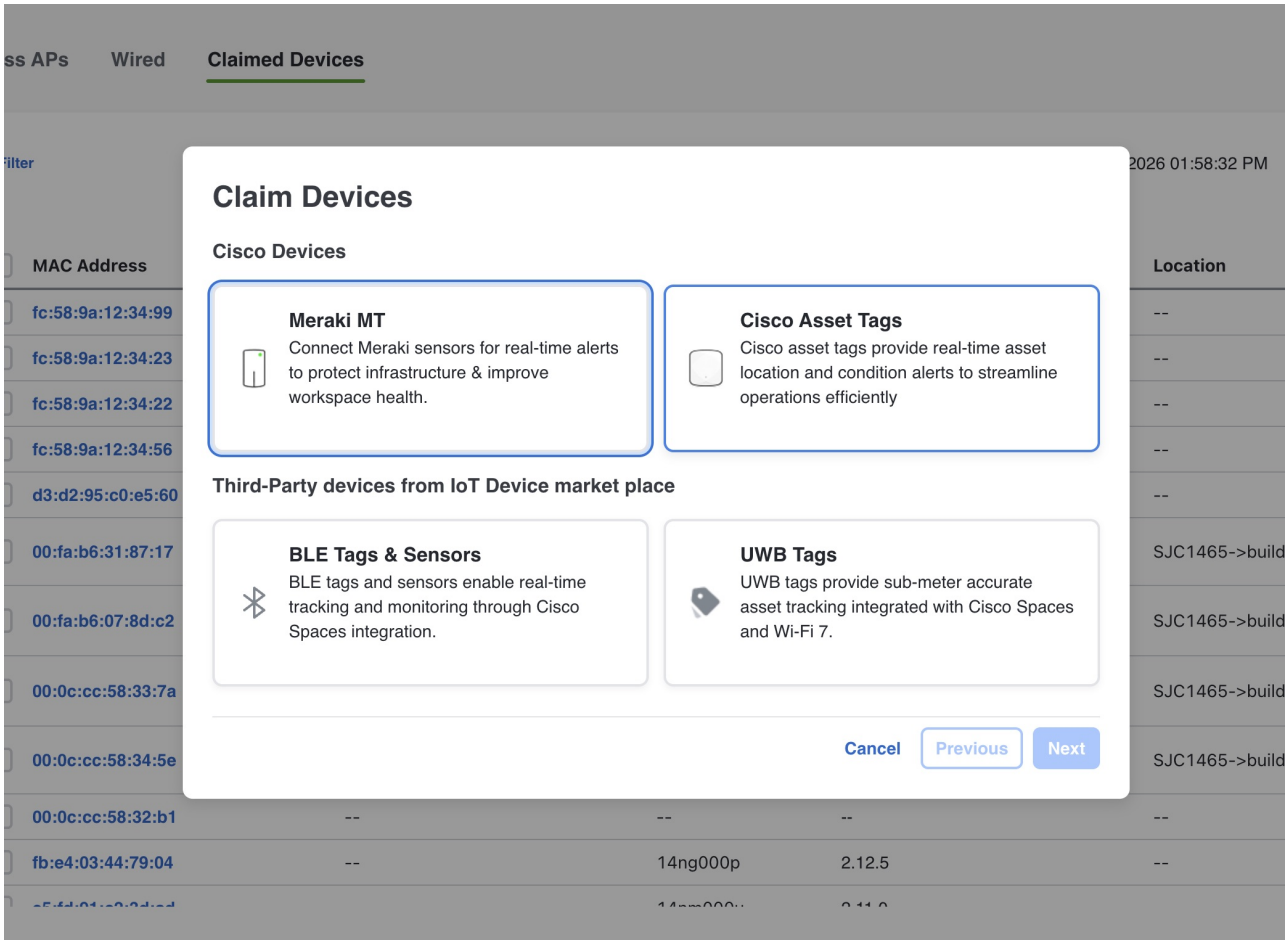
Step 1 From the Cisco Spaces dashboard, choose **IoT Services** > **Inventory** > **Claimed Devices**.

Figure 77: Claimed Devices tab



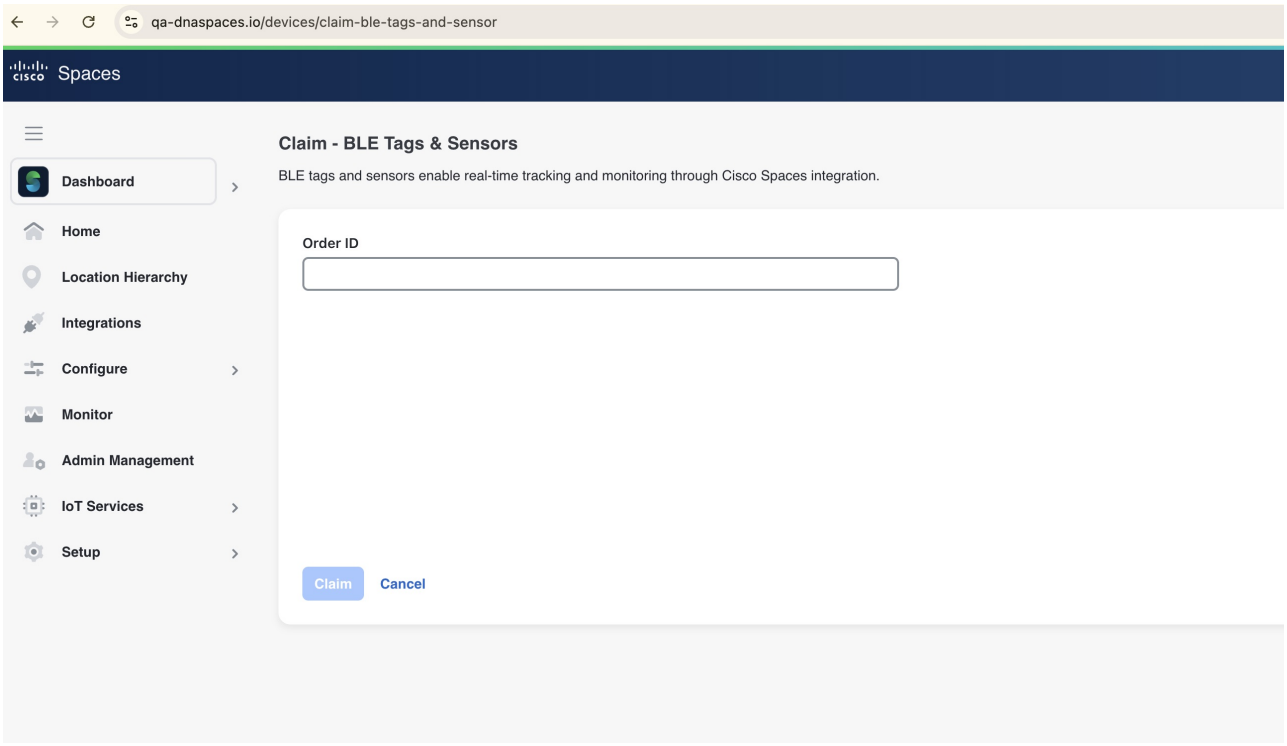
Step 2 Click **Claim devices**.

Figure 78: Claim Devices tab



Step 3 Click **BLE Tags & Sensors** within the **Third-Party devices from IoT Device market place** section. Click **Next**. The **Claim - BLE Tags & Sensors** tab is displayed.

Figure 79: Claim - BLE Tags & Sensors tab



Step 4 Enter the **Order ID**.

Step 5 Click **Claim**.

Configure a beacon on IoT Service

Configure beacon types and view their details as scanned by the IoT Service.

Procedure

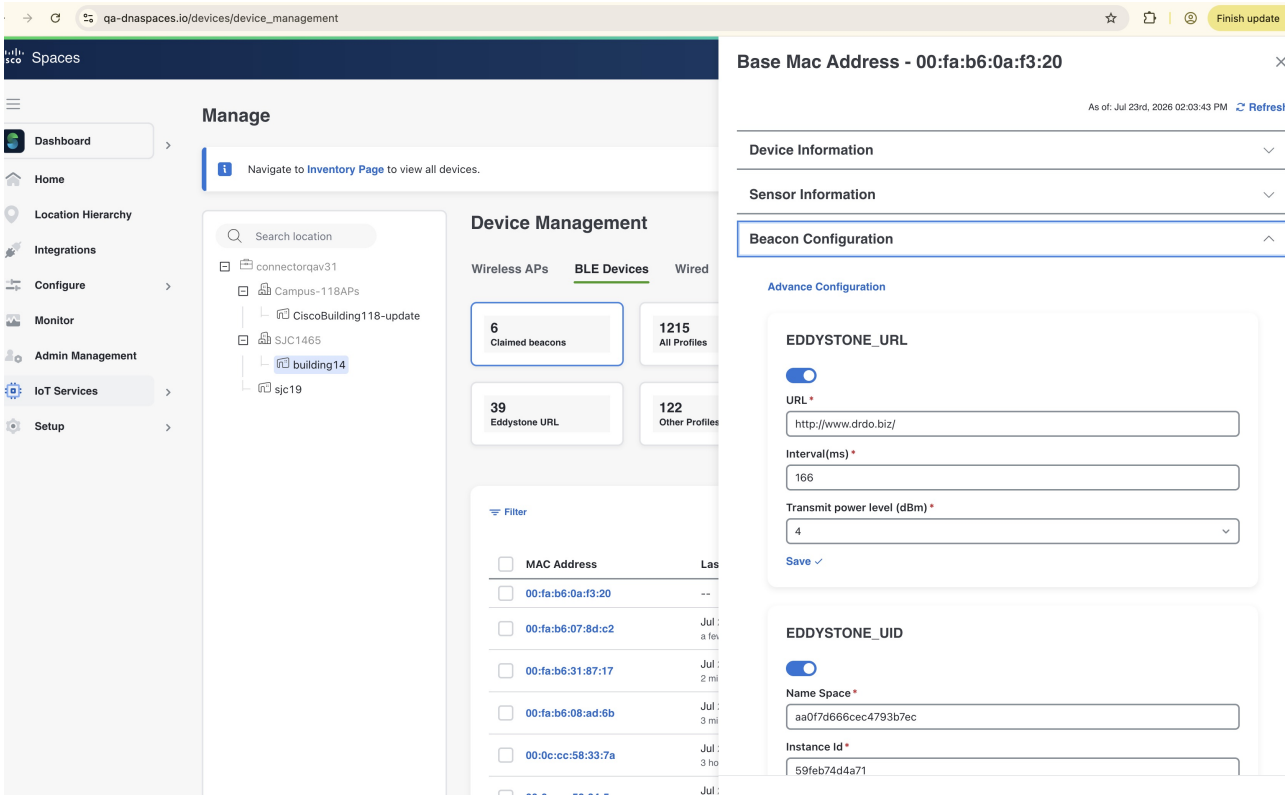
Step 1 Choose **IoT Services** > **Manage** > **BLE Devices**.

Step 2 Click on **Claimed beacons** to view the scanned beacons.

This list is sorted by **Beacon Type**.

Step 3 Click the MAC address to open the detailed **Base MAC Address** page.

Figure 80: Base MAC address tab



Step 4 In the **Beacon Configuration** area, you can see the configuration pararmeters for the beacon these:

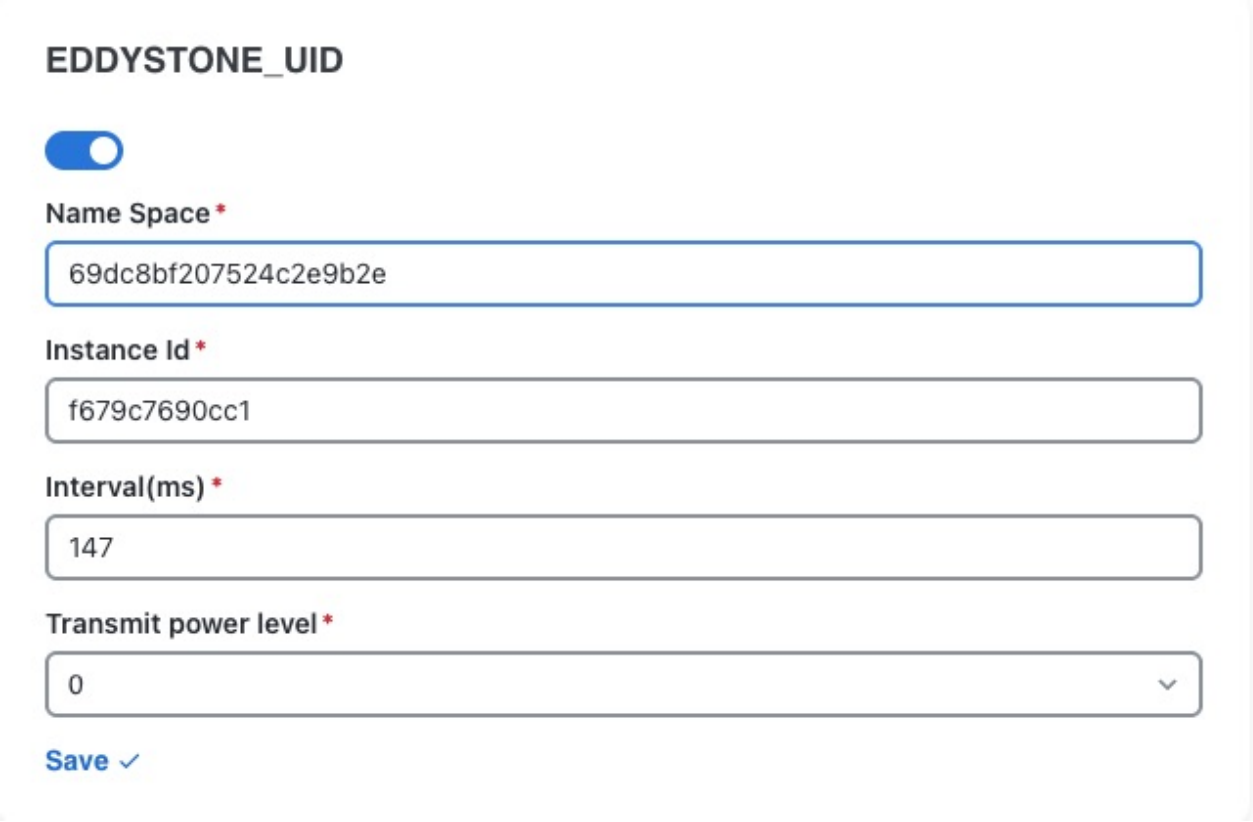
a. **EDDYSTONE_URL**: Add the URL in the **URL** section. Add a interval value in the **Interval (ms)** section. Select a transmit power level in the **Transmit power level (dBm)** from the drop-down list. Click **Save**.

Figure 81: Eddystone_URL tab



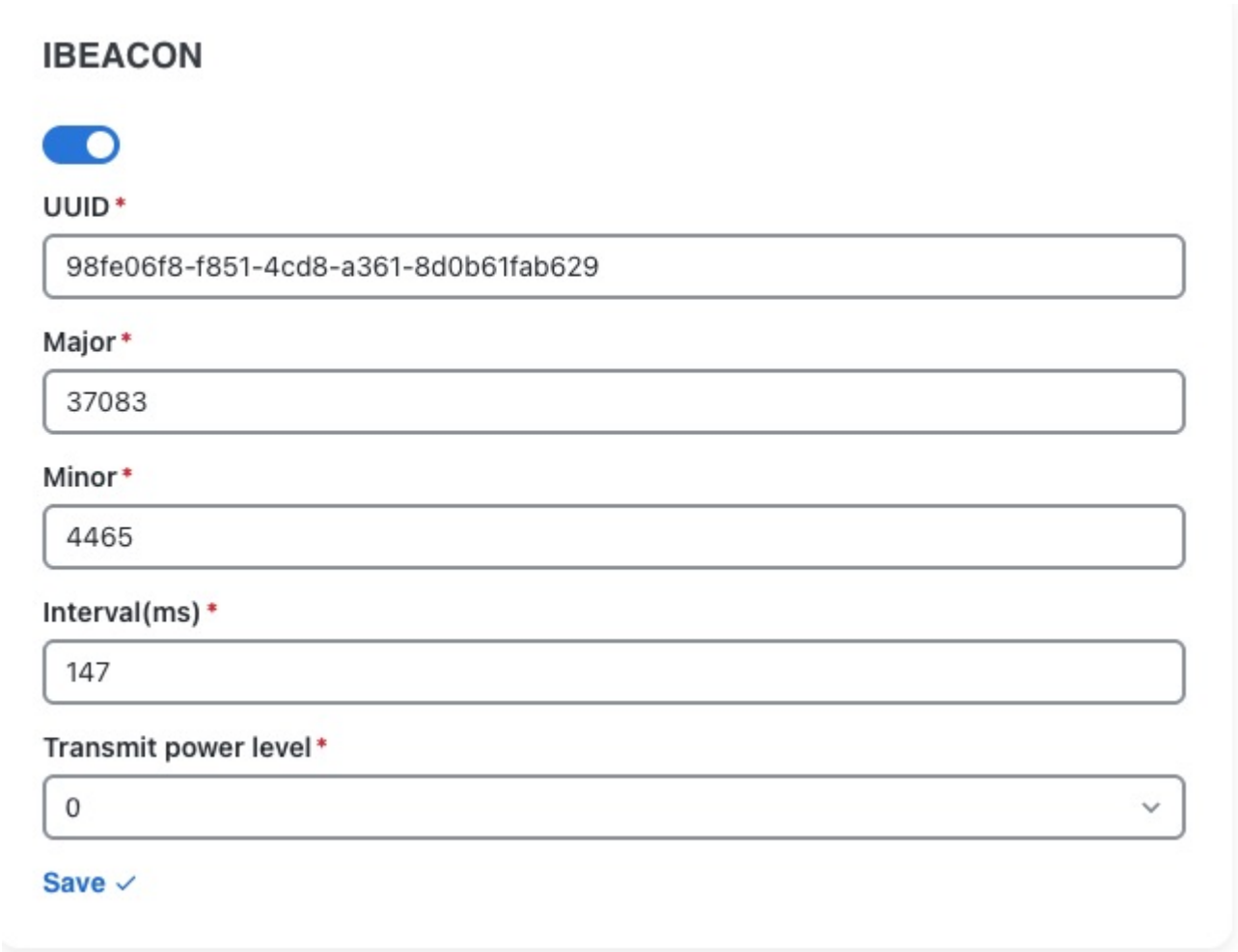
b. **EDDYSTONE_UID**: Add the name in the **Name Space** section. Add a instance ID in the **Instance Id** section. Add a interval value in the **Interval (ms)** section. Select a transmit power level in the **Transmit power level** from the drop-down list. Click **Save**.

Figure 82: Eddystone_UID tab



c. **IBEACON**: Add the UUID value in the **UUID** section. Add the major and minor values in the **Major** and **Minor** sections. Add a interval value in the **Interval (ms)** section. Select a transmit power level in the **Transmit power level** from the drop-down list. Click **Save**.

Figure 83: Ibeacon tab



d. **TELEMETRY**: Toggle the **Save** button to activate telemetry.

Figure 84: Telemetry tab



View sensor information

Allow you to view detailed sensor data for Floor Beacons that support telemetry, such as Double Tap, Movement Counter, and Precise Temperature.

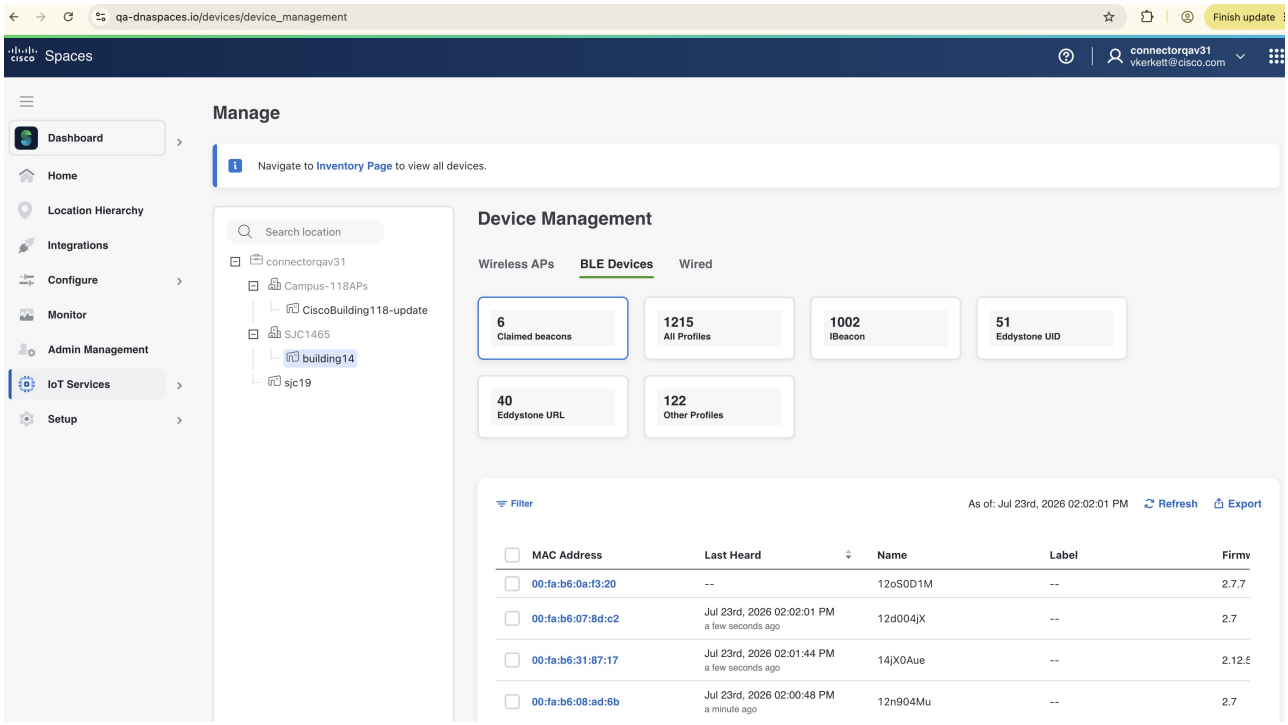
Before you begin

Sensor Information is available only for Floor Beacons where Telemetry is enabled.

Procedure

Step 1 From the Cisco Spaces dashboard, choose **IoT Services** > **Manage** > **BLE Devices**.

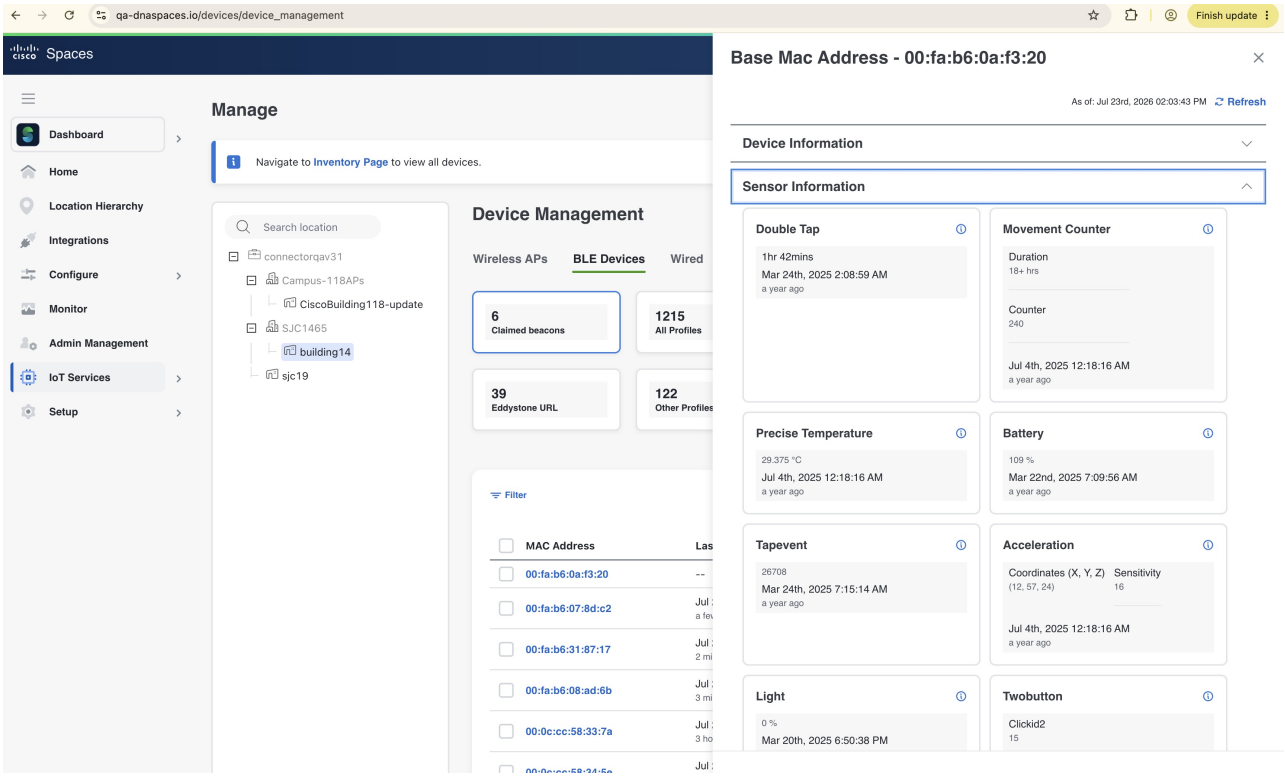
Figure 85: BLE Devices tab

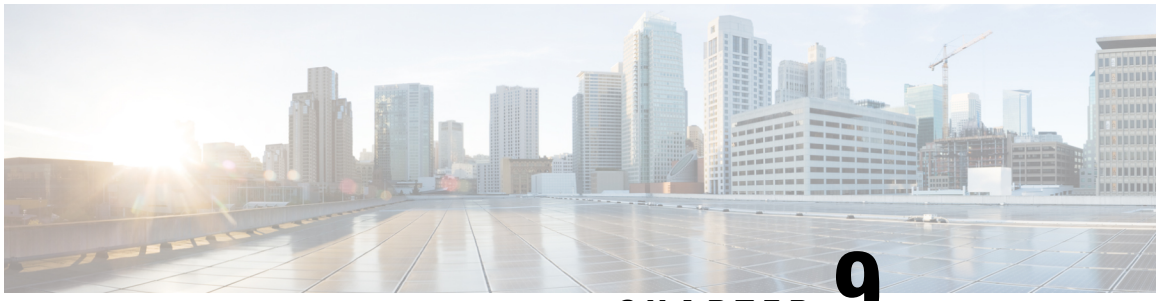


Step 2 Click **Claimed beacons.**.

Step 3 In the **Sensor Information** area, you can see the broadcast sensor data for the beacon that includes **Double Tap**, **Movement Counter**, **Precise Temperature** etc.

Figure 86: Sensor Information tab





CHAPTER 9

Wired

- Wired Gateways, on page 85
- Wired Sensors, on page 91
- Smart PDUs, on page 94

Wired Gateways

A wired gateway is a type of network device that

- installs an IOx application on Cisco Catalyst switches
- discovers and collects telemetry data from supported wired sensors, and
- transmits sensor data to Cisco Spaces: Connector for aggregation and IoT monitoring.

Configure wired gateways

Set up and maintain wired gateways using Cisco Spaces, including managing gateway applications, viewing detailed gateway information, tracking deployment history, and exporting gateway activity.

This task is used to manage IoT gateways within Cisco Spaces, enabling support for applications, monitoring device and energy information, and performing bulk operations such as installation, uninstallation, and exporting gateway history for auditing.

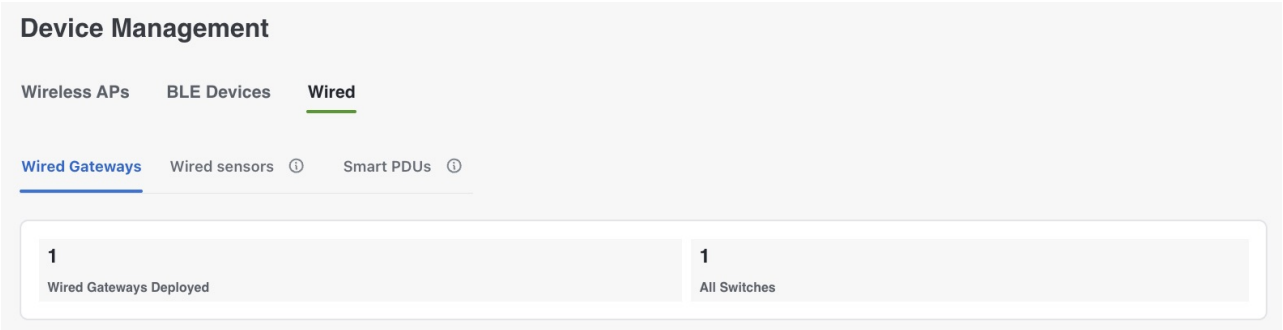
Before you begin

Verify that relevant access points (APs) are registered and available in the Wired Gateways list. Confirm you have the necessary permissions to manage IOx applications and gateway data.

Procedure

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Manage** > **Wired** > **Wired Gateways**.

Figure 87: Wired Gateways tab



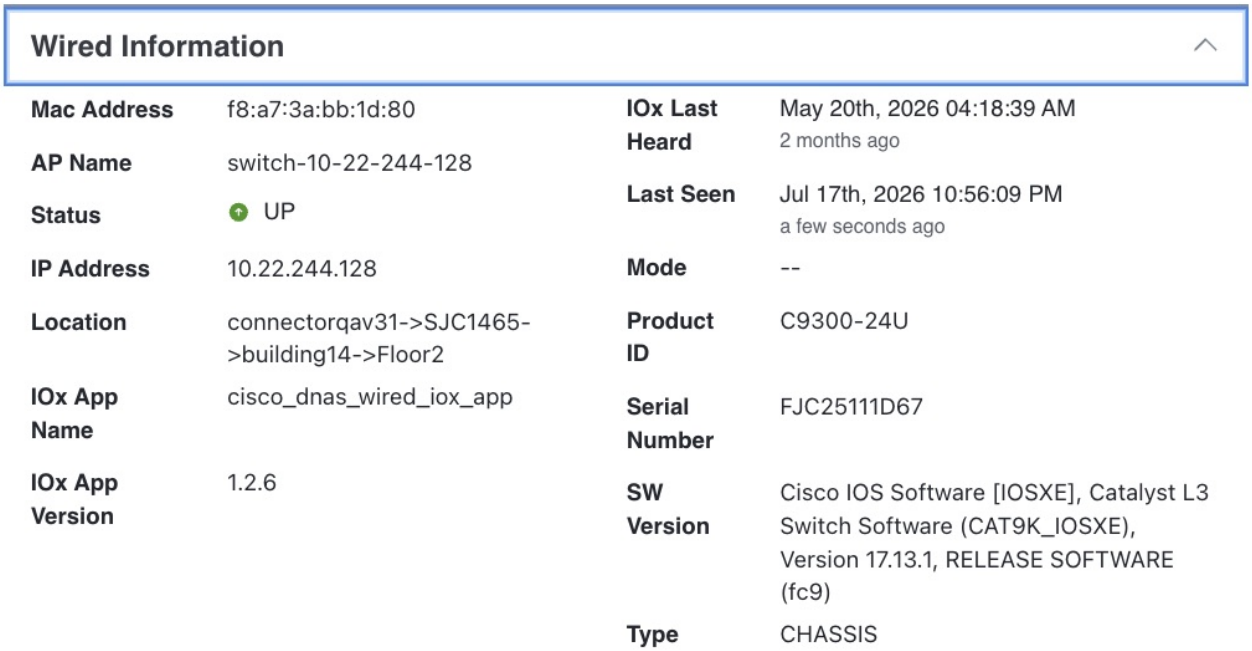
Step 2 Click the MAC address of the AP to open the detailed **Wired Gateways** page. The **Wired Gateways** tab appears.

Figure 88: Wired Gateways tab

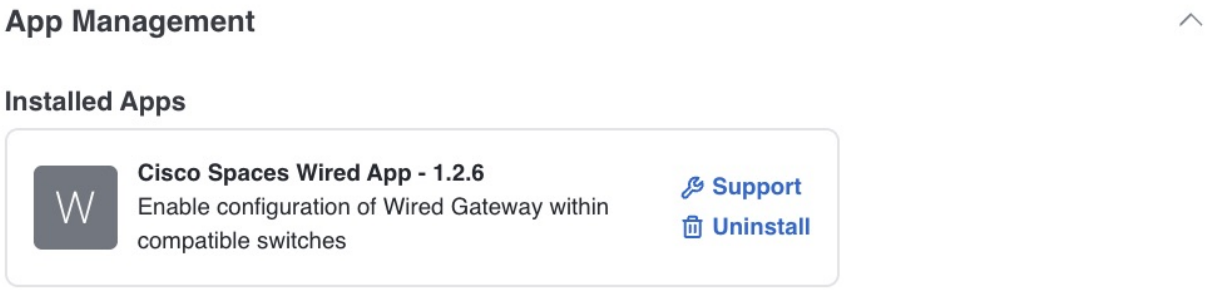


Step 3 Click the **Wired Information** panel to view details such as **MAC Address**, **AP Name**, **Status**, **IP Address**, **Location**, **IOx App Name**, **IOx App Version** etc.

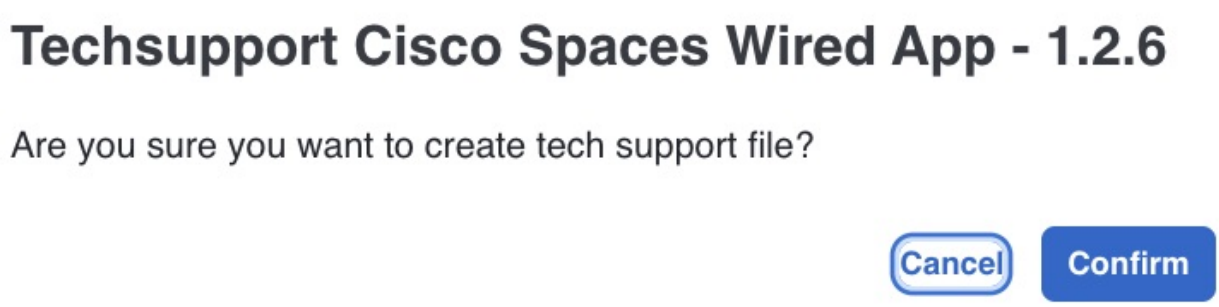
Figure 89: Wired Information tab



Step 4 Click the **App Management** panel to support or uninstall an IOx Application on a gateway. Do one of



- To support, click the **support** icon near Cisco Spaces Wired App. Click support to **confirm** or **cancel** the request.
- *Figure 90: Support icon*

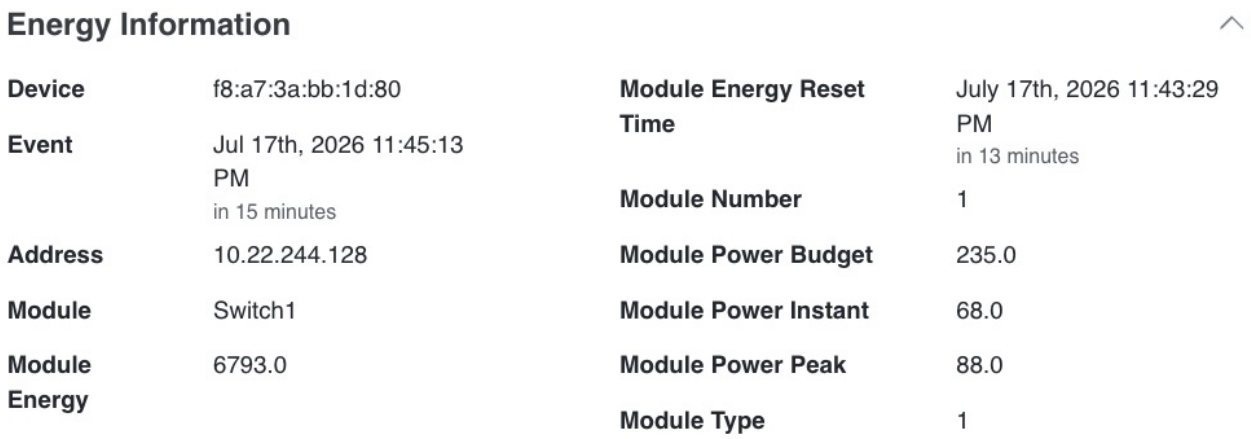


- To uninstall, click the **uninstall** icon near Cisco Spaces Wired App. Click uninstall to **confirm** or **cancel** the request.
- ***Figure 91: Uninstall icon***



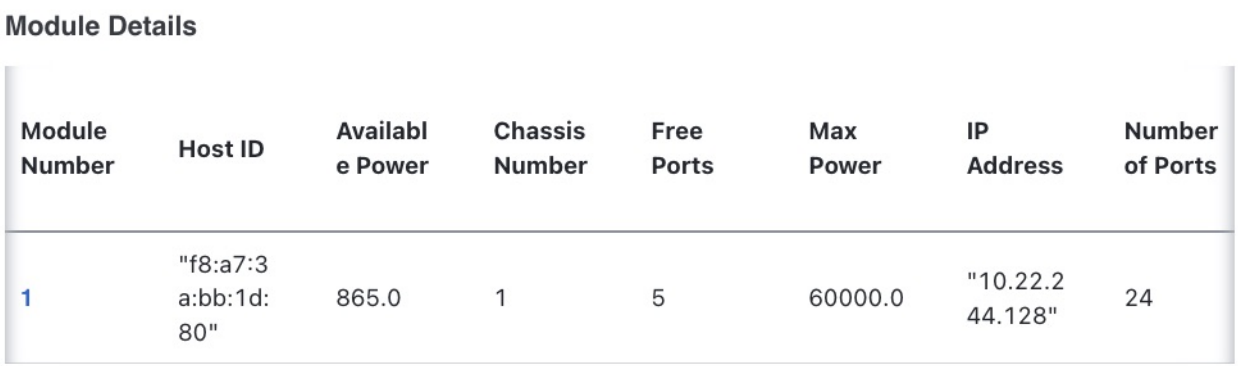
Step 5 Click the **Energy Information** panel to view details such as **Device**, **Event**, **Address**, **Module**, **Module Energy** etc.

Figure 92: Energy Information tab



a) The **Energy Information** panel also displays the **Module Details** table consisting of columns such as **Module Number**, **Host ID**, **Available Power** etc.

Figure 93: Module details tab



b) The **Energy Information** panel also displays the **Port Details** table consisting of columns such as **Interface Name**, **Device Name**, **IP Address**, **Event Time** etc.

Figure 94: Port details tab

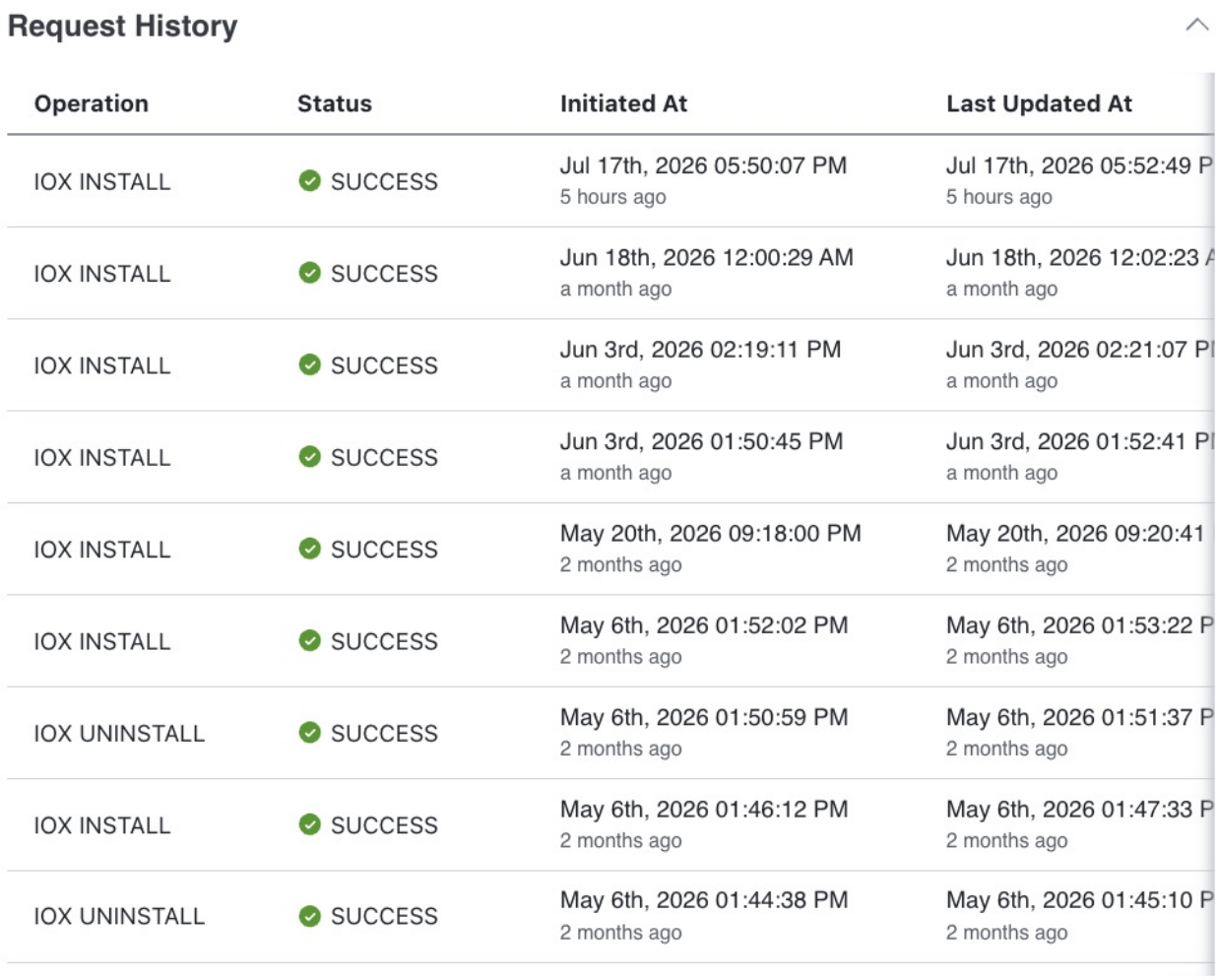
Port Details

Interface Name	Device Name	IP Address	Event Time
"GigabitEthernet1/0/22"	" CW9164I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/3"	" C9130AXI-B"	"10.22.244.128"	--
"GigabitEthernet1/0/4"	" C9136I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/5"	" CW9162I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/7"	" CW9166I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/8"	" CW9164I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/9"	" C9115AXI-B"	"10.22.244.128"	--
"GigabitEthernet1/0/12"	" C9120AXI-B"	"10.22.244.128"	--
"GigabitEthernet1/0/13"	" CW9162I-B"	"10.22.244.128"	--
"GigabitEthernet1/0/14"	" CW9166I-B"	"10.22.244.128"	--

Step 6 Click on the **Request History** panel to check the status of deployment. The **Status** column shows the status of install, uninstall or upgrade on each AP.

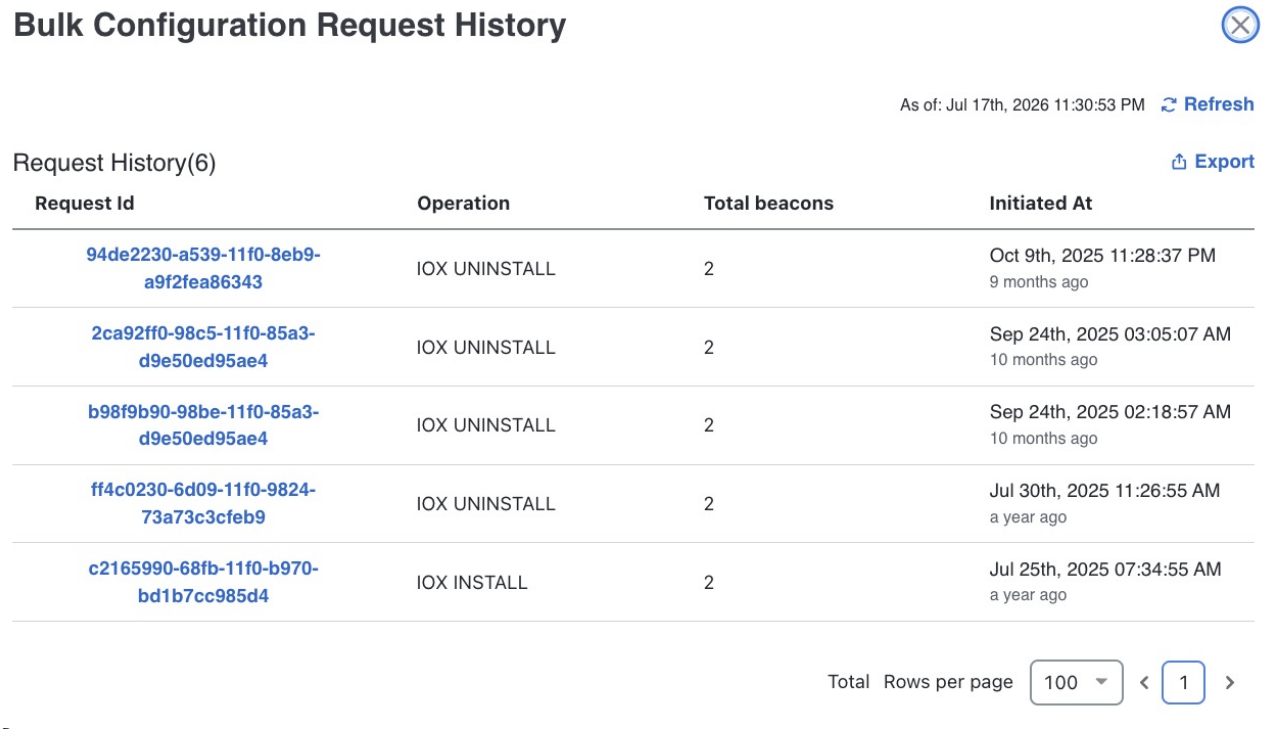
a) SUCCESS: The application was uninstalled or upgraded successfully on the AP.
b) FAILURE: The application uninstall or upgrade on the AP failed.
c) IN PROGRESS: The application is currently being uninstalled or upgraded on the AP.

Figure 95: Request History tab



Step 7 Click the MAC address of the desired AP in the tab and then click the **Bulk Request History** button to check the bulk configuration request history. Click on the **Export** button and **Refresh** button to download as a .csv file to your local

system and refresh the



Step 8 Click the MAC address of the desired AP in the tab and then click the **Action** button.

a) **Manage IOx app**: Either install or uninstall IOx app.

b) **Delete**: Delete the IOx app.

Wired Sensors

A wired sensor is an IoT device that

- connects to the network through a Cisco switch configured as a wired gateway
- collects presence and environmental telemetry such as temperature, humidity, carbon dioxide (CO_2), and air quality, and
- enables centralized monitoring and management through Cisco Spaces IoT Services, which displays sensor details, telemetry, connectivity, and location.

Configure wired sensors

Enable detailed monitoring and management of wired sensor devices connected to access points.

Wired sensors provide occupancy, environmental, and location data for spaces. Management includes editing device labels, updating sensor information, and controlling app group assignment.

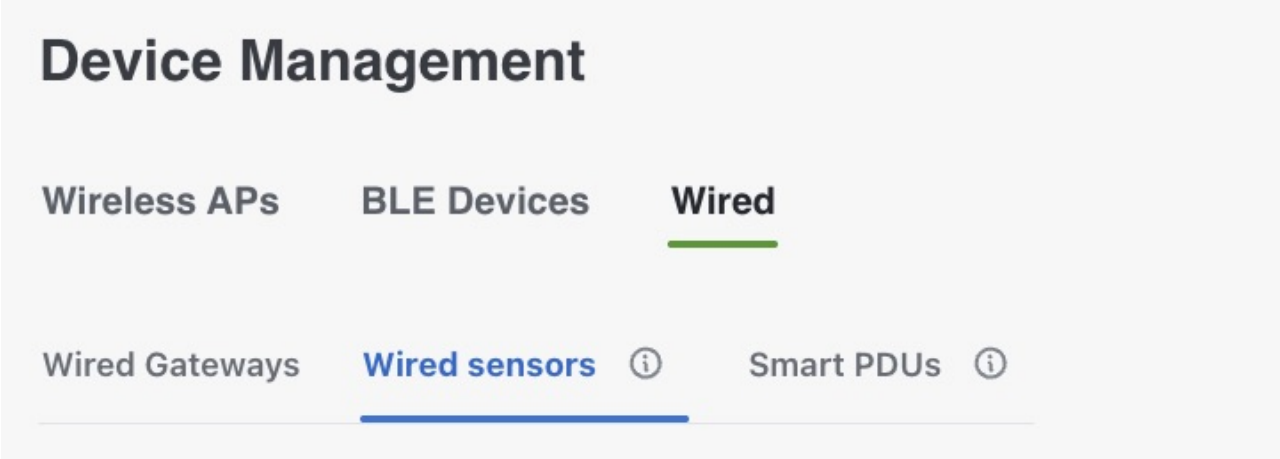
Before you begin

Verify that the APs and sensors are registered and online.

Procedure

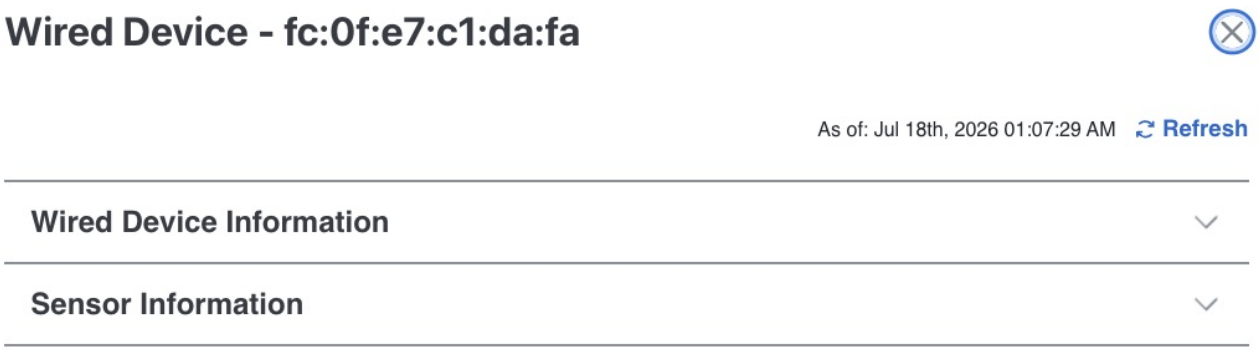
Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Manage** > **Wired** > **Wired Sensors**.

Figure 96: Wired Sensors tab



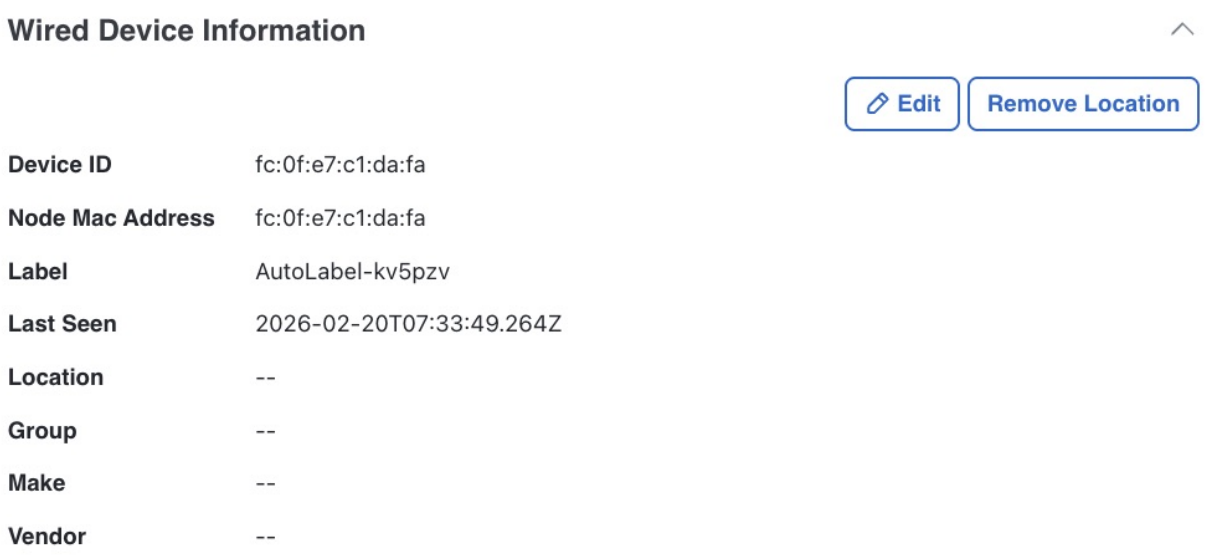
Step 2 Click the MAC address of the AP to open the detailed **Wired Device** page. The **Wired Device** tab appears.

Figure 97: Wired Device tab



Step 3 Click the **Wired Device Information** panel to view details such as **Device ID**, **Node Mac Address**, **Label**, **Last Seen**, **Location**, **Group**, **Make** and **Vendor**.

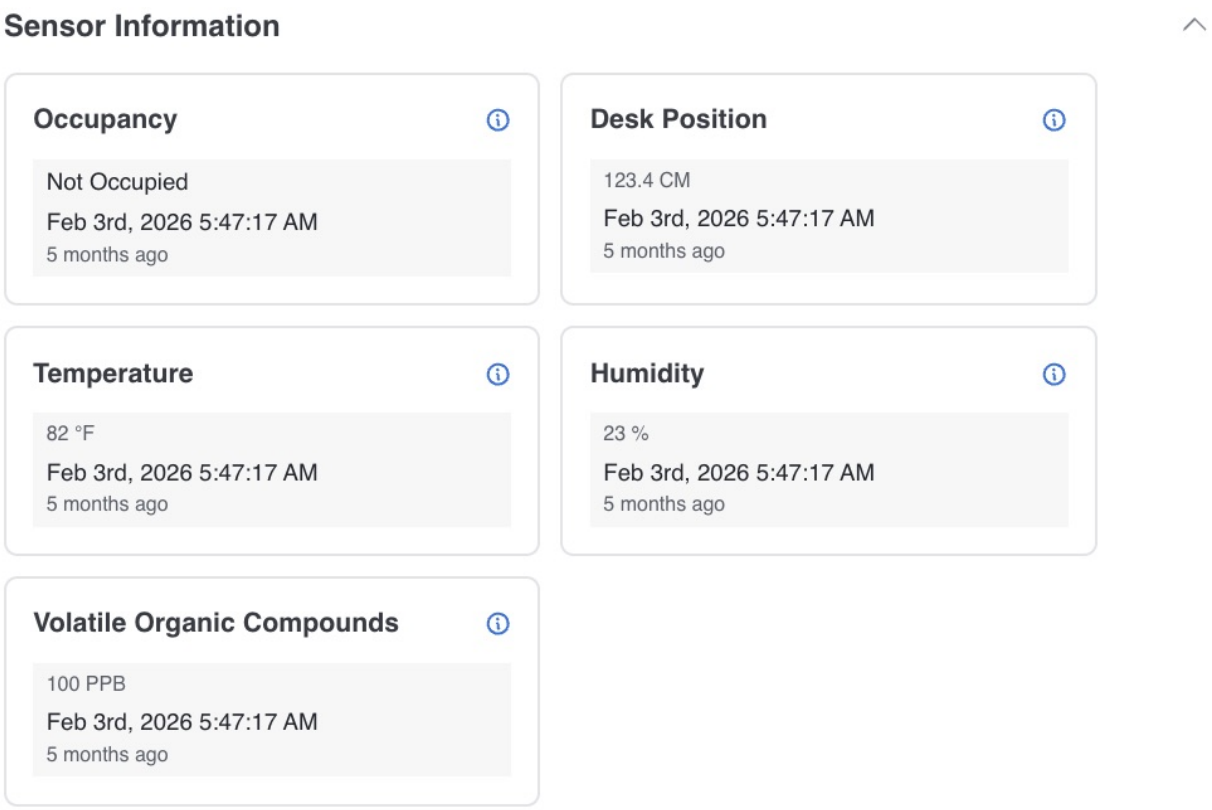
Figure 98: Wired Device Information tab



a) Click on the **Edit** button to edit the device label.
b) Click on the **Remove Location** button to remove the location.

Step 4 Click the **Sensor Information** panel to view details such as **Occupancy**, **Desk Position**, **Temperature**, **Humidity** etc.

Figure 99: Sensor Information tab



Step 5 Click the MAC address of the desired AP in the tab and then click the **Action** button.

a) **Remove from Group**: Remove the IOx app from the group.

b) **Delete**: Delete the IOx app.

Smart PDUs

A smart power distribution unit (PDU) is an energy management device that

- provides visibility into the power and energy consumption of connected infrastructure
- enables onboarding into Cisco Spaces through the Cisco Spaces: Connector using SNMP, and
- supplies operational and energy-usage data for monitoring and efficiency improvement.

Configure smart PDUs

Set up and manage smart PDUs for networked access points using Cisco Spaces IoT Services.

Use this task to configure smart PDUs including setting properties and viewing energy information through Cisco Spaces. This enables efficient power management and monitoring for connected devices.

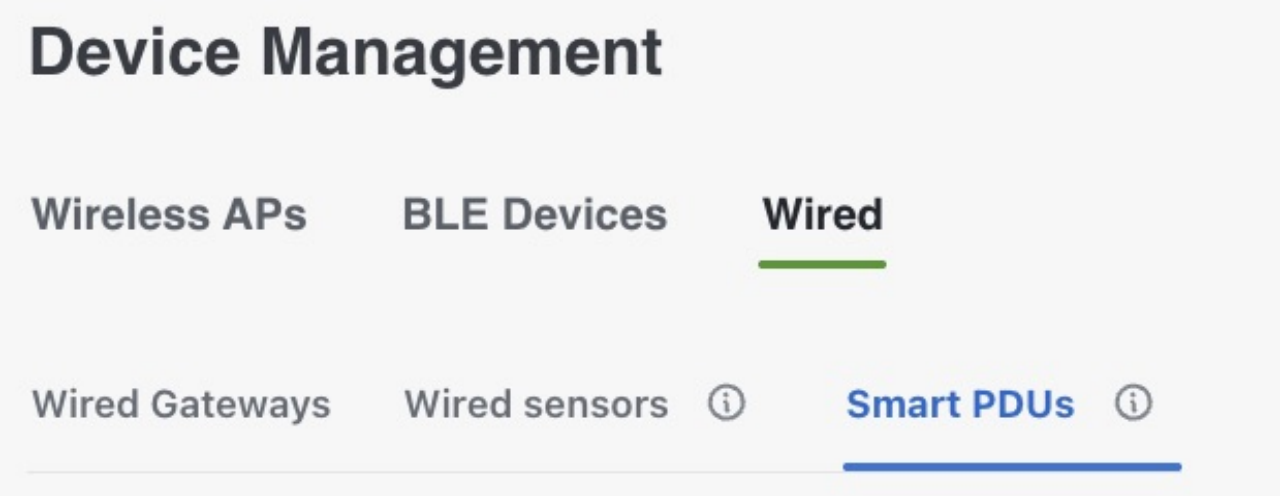
Before you begin

Know the MAC addresses of the APs you intend to manage. Have SNMP credentials and Smart PDU IP address available.

Procedure

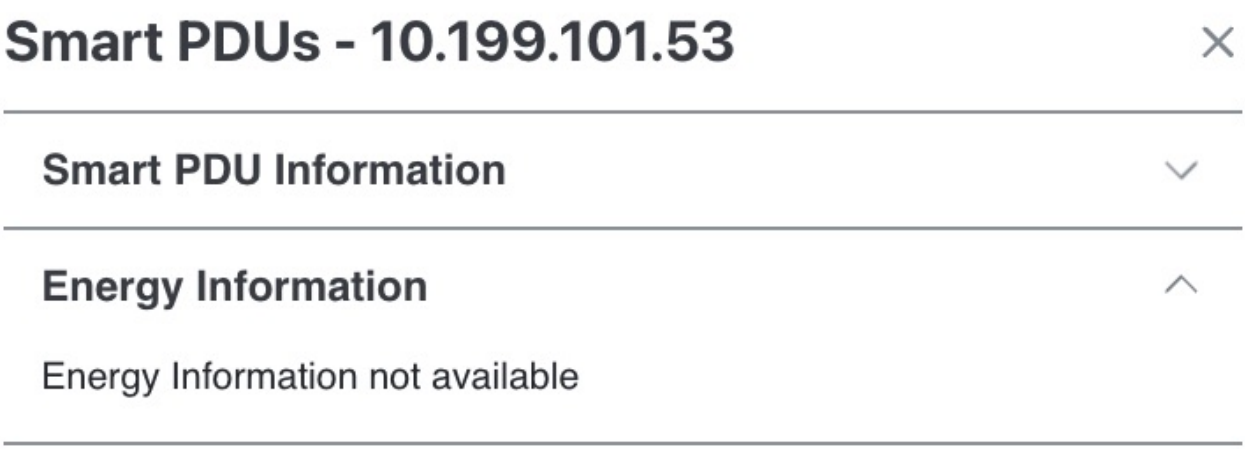
Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Manage** > **Wired** > **Smart PDUs**.

Figure 100: Smart PDUs tab



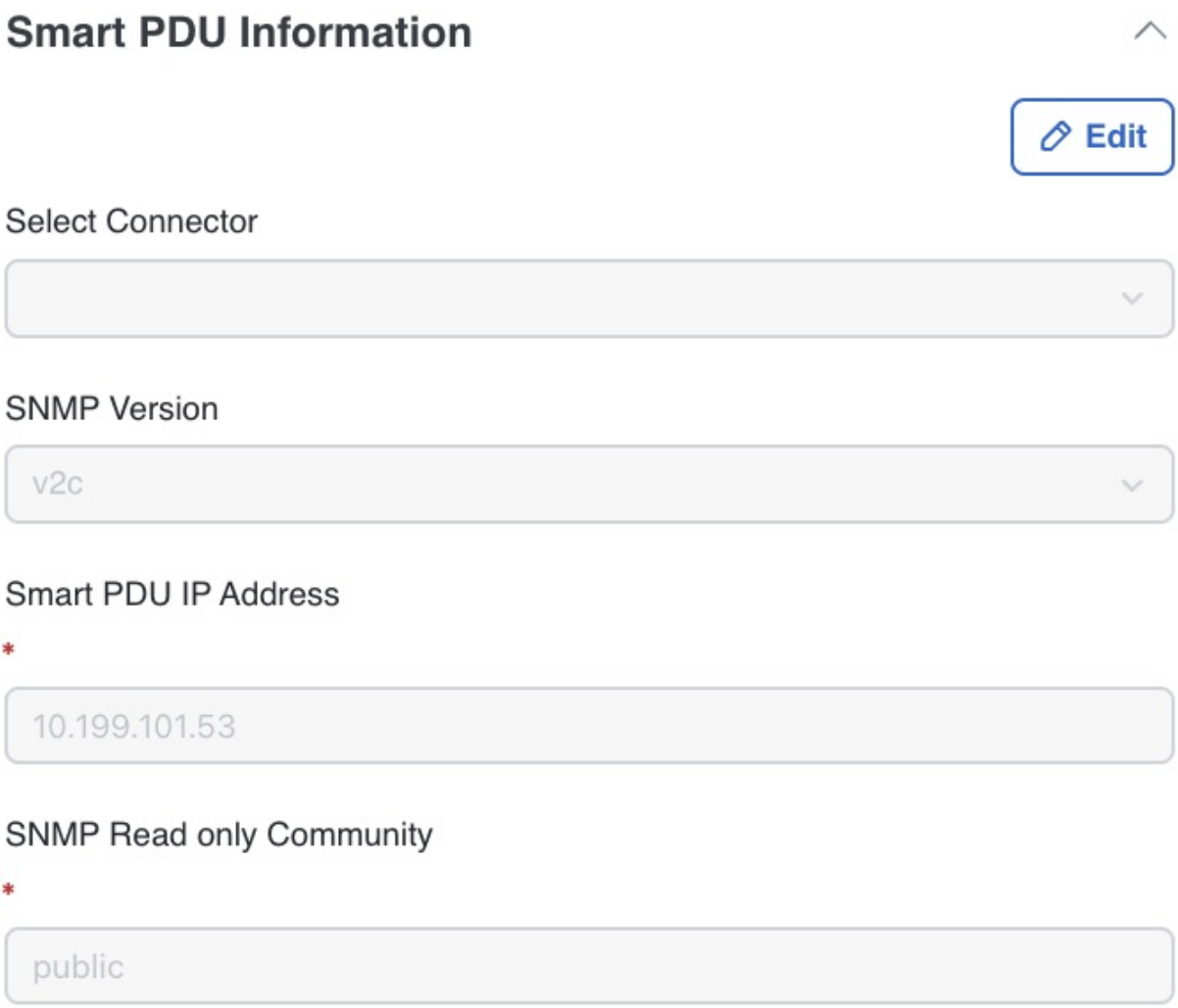
Step 2 Click the MAC address of the AP to open the detailed **Smart PDUs** page. The **Smart PDUs** tab appears.

Figure 101: Smart PDUs tab



Step 3 Click the **Smart PDUs Information** panel to view details such as **Select Connector**, **SNMP Version**, **Smart PDU IP Address** and **SNMP Read only Community**.

Figure 102: Smart PDUs Information tab



a) **Select Connector**: Select the connector from the drop-down list.
b) **SNMP Version**: Select the SNMP version from the drop-down list.
c) **Smart PDU IP Address**: Enter the smart PDU IP address.
d) **SNMP Read only Community**: Choose the SNMP read only community option.

Step 4 Click the **Energy Information** panel to view details.

Figure 103: Energy Information tab



Step 5 Click the MAC address of the desired AP in the tab and then click the **Action** button.

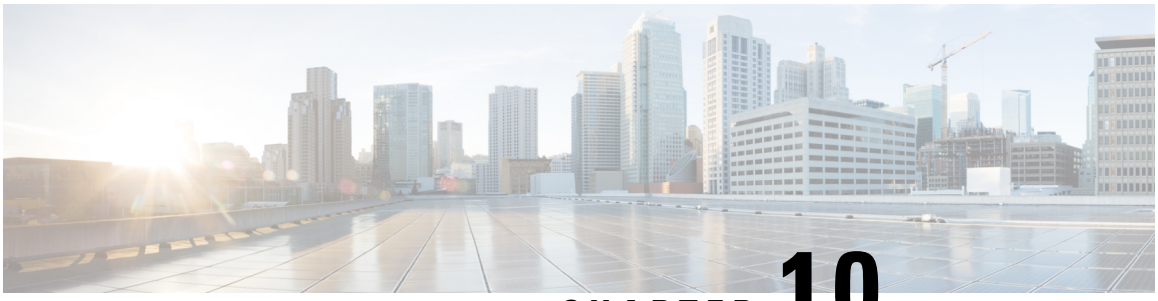
a) **Delete**: Delete the IOx app.



PART IV

Device Monitoring

- Monitoring, on page 101



CHAPTER 10

Monitoring

From the IoT Service > **Monitoring** page, you can monitor all the IoT devices and gateways, and also get a one-shot categorized view of devices according to their battery life and last heard time.

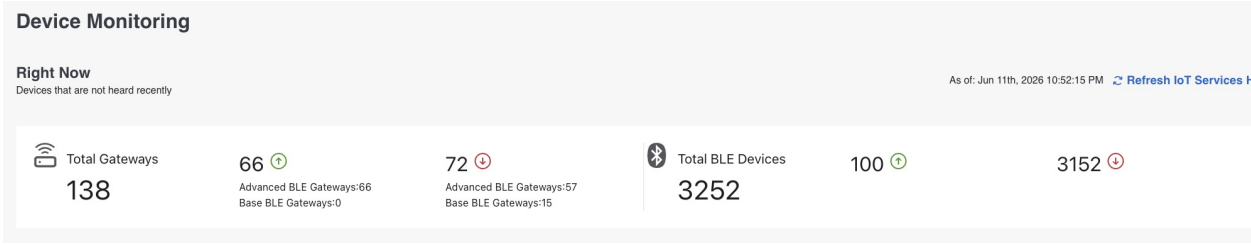
- Right now, on page 101
- BLE devices battery life, on page 101
- Last heard BLE devices, on page 102

Right now

In the **Total gateways** part of this section, you can see an overview of all gateways that are being monitored. You can also see the number of reachable gateways (base and advanced) counted under the green upward arrow, and the number of unreachable gateways counted under the red downward arrow.

In the **Total BLE Devices** part of this section, you can see an overview of all BLE devices that are being monitored. You can also see the number of reachable devices (base and advanced) counted under the green upward arrow, and the number of unreachable devices counted under the red downward arrow.

Figure 104: Right Now



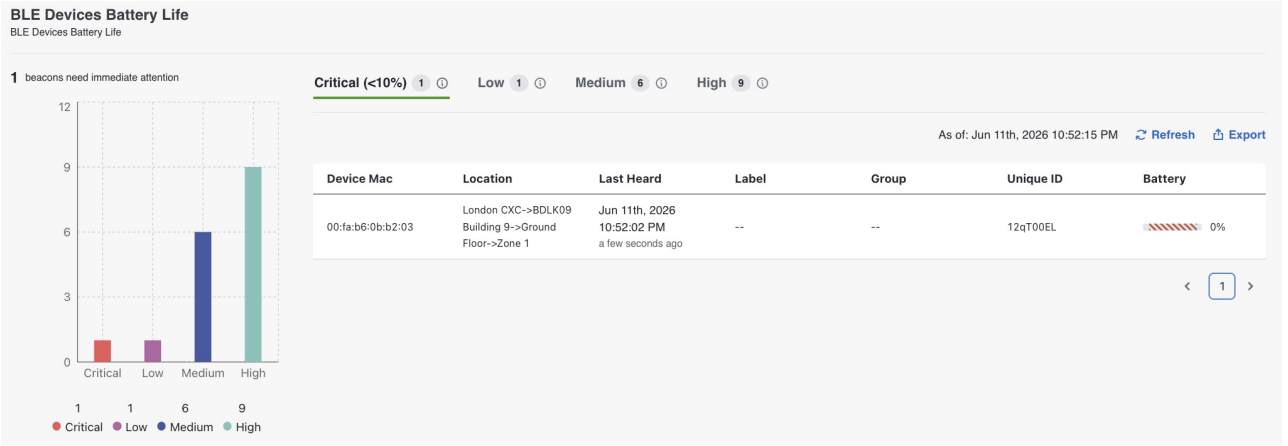
BLE devices battery life

In the section, you get an overview of only those BLE devices (beacons) that can sense their own battery life. The devices are categorized according to their current battery life as:

- Critical
- Low
- Medium

- High

On the top of this section, you can see the number of devices in each category. To the left, you can also see this information represented as a bar chart. You can click either on the category listed on the top or the corresponding bar to see a detailed list of the devices. You can also export this list as a CSV file.

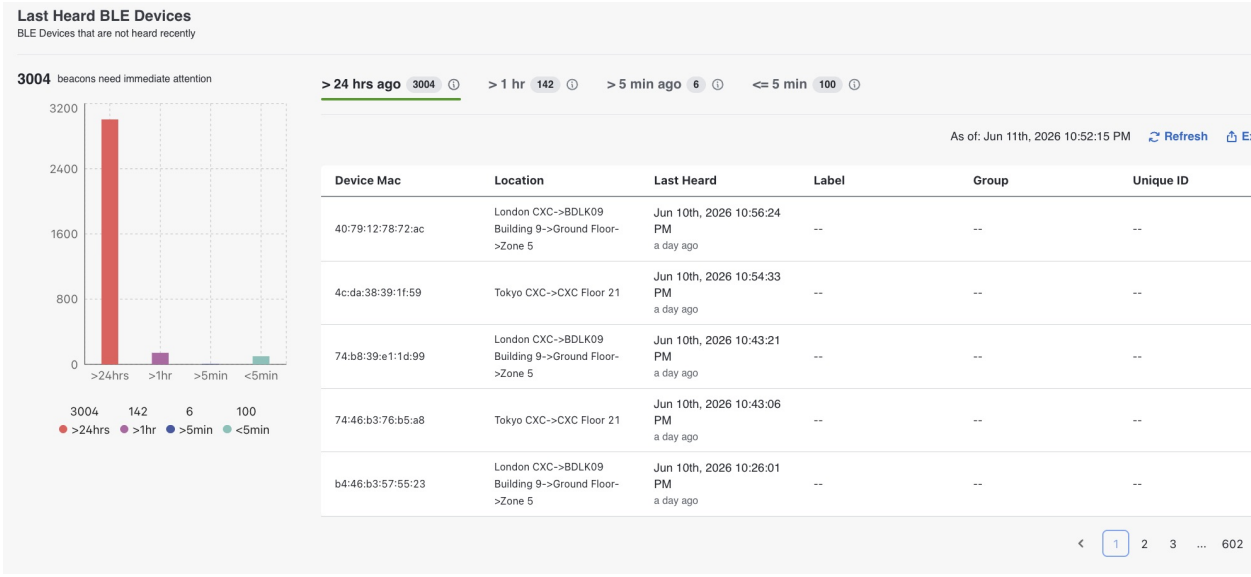


Last heard BLE devices

In the section, you get an overview of all BLE devices (beacons). The devices are categorized according to the last time they were heard as these:

- greater than 24 hrs ago
- greater than one hour ago
- greater than five minutes ago.
- less than or equal to five minutes ago

To the top of this section, you can see this information represented as numbers. To the left of this section, you can also see this information represented as a bar chart. You can click either on the number listed on the top or the corresponding bar to see a detailed list of the devices. You can also export this list as a CSV file.

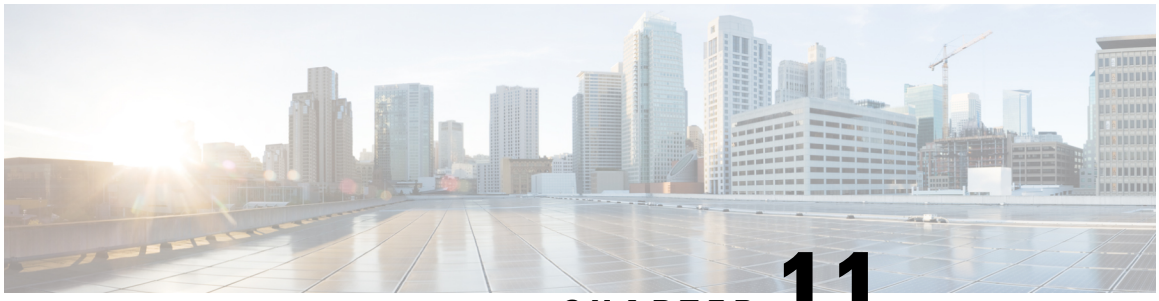

Last Heard BLE Devices
BLE Devices that are not heard recently
3004 beacons need immediate attention
3200
2400
1600
800
0
>24hrs
>1hr
>5min
<5min
3004
142
6
100
>24hrs
>1hr
>5min
<5min
> 24 hrs ago 3004
> 1 hr 142
> 5 min ago 6
<= 5 min 100
As of: Jun 11th, 2026 10:52:15 PM
Refresh
Device Mac
Location
Last Heard
Label
Group
Unique ID
40:79:12:78:72:ac
London CXC->BDLK09 Building 9->Ground Floor->Zone 5
Jun 10th, 2026 10:56:24 PM
a day ago
4c:da:38:39:1f:59
Tokyo CXC->CXC Floor 21
Jun 10th, 2026 10:54:33 PM
a day ago
74:b8:39:e1:1d:99
London CXC->BDLK09 Building 9->Ground Floor->Zone 5
Jun 10th, 2026 10:43:21 PM
a day ago
74:46:b3:76:b5:a8
Tokyo CXC->CXC Floor 21
Jun 10th, 2026 10:43:06 PM
a day ago
b4:46:b3:57:55:23
London CXC->BDLK09 Building 9->Ground Floor->Zone 5
Jun 10th, 2026 10:26:01 PM
a day ago
1
2
3
602



PART V

Settings

- Settings, on page 107



CHAPTER 11

Settings

- Device filtering, on page 107
- Categorize devices into manual groups, on page 108
- Categorize devices into dynamic groups, on page 109
- Configure onboarding and nearby interaction settings, on page 111

Device filtering

While Cisco Spaces: IoT Service scans all devices, you may not want to view certain devices on the dashboard. You can now filter out devices from the Cisco Spaces: IoT Service dashboard using types of MAC addresses. Filtering currently occurs at the cloud level, not at the AP level. Once filtered, these devices do not appear in these locations:

- Cisco Spaces: Detect and Locate
- Cisco Spaces: IoT Service
- Output of Firehose API calls

You can filter out devices based on these MAC address types:

- **Allow Public MAC**: Global, fixed MAC addresses registered with the IEEE Registration Authority that do not change during the device's lifetime. Enable the toggle to allow Public MAC.
- **Allow Random Static MAC**: Random static MAC addresses, which are random numbers generated every time the device boots up or values that stay the same for the device's lifetime. These addresses do not change within one power cycle of the device. Enable the toggle to allow Random Static MAC.
- **Allow Random Private MAC**: Random private MAC addresses of two types:
  - **Resolvable**: Generated from an identity resolving key (IRK) and a random number. These can change frequently (even during the lifetime of a connection) and prevents an unknown scanning device from identifying and tracking the device. Only scanning devices with the IRK from the beaconing device (exchanged using a private resolvable address) can resolve that address, allowing the scanning device to identify the beaconing device.
  - **Unresolvable**: A random number that can change anytime.

  Enable the toggle to allow Random Private MAC.

- **Allow MAC Prefix Configuration**: MAC Prefix configuration are new MAC prefixes that are added using the **Add** button. Enter the **New MAC prefix** and click **Save** to enable the toggle.

SUMMARY STEPS

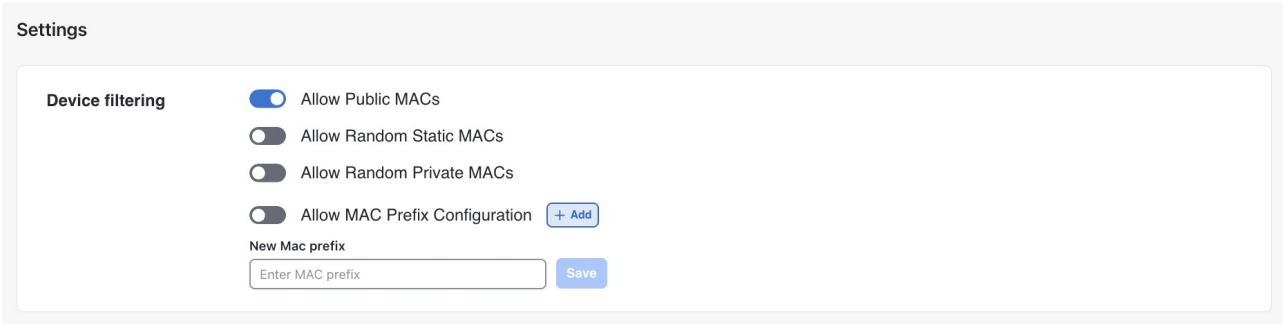
1. Navigate to **IoT Services** > **Settings** > **Device filtering**.

DETAILED STEPS

Procedure

Navigate to **IoT Services** > **Settings** > **Device filtering**.

Figure 105: Device filtering



Categorize devices into manual groups

You can create groups and assign devices to them. You can focus attention on certain devices and view only these devices by filtering them using the group.

The advantages of manual groups are:

- Policies are applied to groups.
- Firehose APIs can filter devices by these groups.
- In the Cisco Spaces: IoT Service dashboard, you can filter devices by groups.

Procedure

Step 1 In the Cisco Spaces: IoT Service dashboard, navigate to **Settings** > **Groups**.

Step 2 Click the **Create a new group** button. The **Add a Group** window appears.

Step 3 Enter the **Group Name**, **Description**, and choose **Manual Group**. Click **Next**.

Step 4 The **Add a group** page appears. Select either **Wireless Devices** or **Wired Devices** and choose the devices to add to this group.

Step 5 Click **Next**. On the **Add a Group** page, click **Done**, or **Create another group**.

On the **Groups** tab, you can view the group you created. Click the group to display its devices. To edit the group, click the **Edit** button.

To delete a device, select the group's check box, then click **Action** > **Delete** button.

Categorize devices into dynamic groups

You can configure dynamic groups using parameters such as MAC prefix, vendor code, or location hierarchy including floor, building, or zone. New devices are automatically added to the group based on these configured parameters.

The advantages of dynamic groups are:

- Policies are applied to groups. Dynamic groups automatically categorize new devices and apply policies to them.
- Firehose APIs can filter devices by these groups.
- In the Cisco Spaces: IoT Service dashboard, you can filter devices by groups.

Procedure

Step 1 In the Cisco Spaces: IoT Service dashboard, navigate to **Settings** > **Groups**.

Step 2 Click the **Create a new group** button. The **Add a Group** window appears.

Step 3 Enter the **Group Name**, **Description**, and choose **Dynamic Group**. Click **Next**.

Step 4 In the **Add a Group** page that is displayed, configure these parameters for this group.

- Group by MAC Prefix
- Group by Vendor Code
- Group by Location Hierarchy

Figure 106: Group by MAC Prefix



Figure 107: Group by Vendor Code

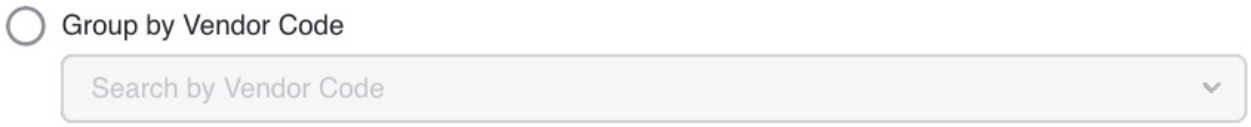


Figure 108: Group by Location Hierarchy



Step 5 Click **Next**. On the **Add a Group** page, click **Done**, or **Create another group**.

On the **Groups** tab, you can view the group you created. Click the group to display its devices. To edit the group, click the **Edit** button.

What to do next

To delete a device, select the group's check box, then click **Action** > **Delete** button.

Configure onboarding and nearby interaction settings

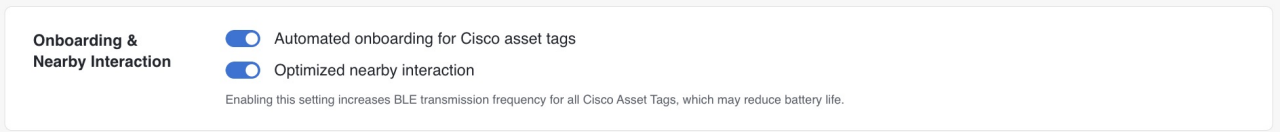
Use this procedure to optimize asset tag management and control BLE transmission rates by adjusting onboarding and interaction settings.

Procedure

Step 1 In Cisco Spaces, open the **IoT Services** settings page.

Step 2 Navigate to the **Onboarding & Nearby Interaction** section.

Figure 109: Onboarding & nearby interaction tab



Step 3 Enable or disable the **Automated onboarding for Cisco asset tags**and the **Optimized nearby interaction** toggle buttons.

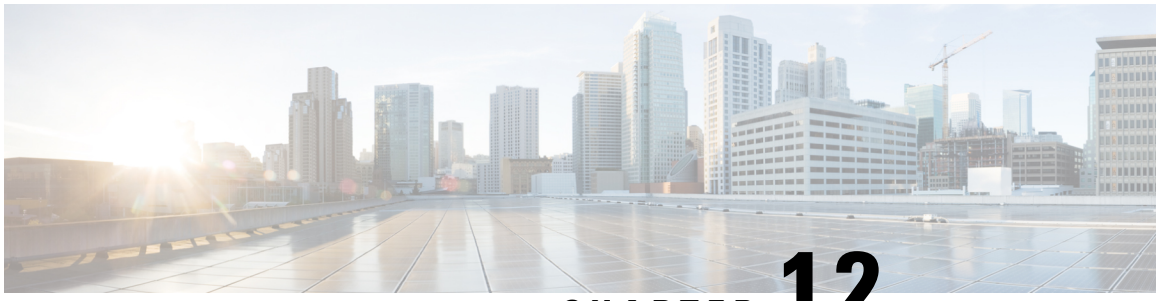
Note
Enabling these controls increases BLE transmission frequency for all Cisco Asset Tags. This higher frequency may reduce battery life.



PART VI

Troubleshooting

- Troubleshoot IoT services: controller, on page 115
- Troubleshoot IoT services: IOx application, on page 135
- Troubleshoot IoT services: Cisco Spaces connector, on page 143
- Troubleshoot IoT services: access point, on page 145



CHAPTER 12

Troubleshoot IoT services: controller

- Reprovisioning IoT services after failover, on page 115
- What settings are needed to allow access via NETCONF?, on page 115
- The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting?, on page 116
- For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token?, on page 116
- gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled?, on page 117
- How do I verify gRPC is up?, on page 117
- How do I verify that TDL subscriptions are created and are valid?, on page 118
- Are the TDL subscriptions created and valid?, on page 118
- What is the TDL status?, on page 118
- How do I view the current CAPWAP values for an AP?, on page 119
- How do I view the current TDL values for an AP?, on page 127
- How do I get the telemetry connection status?, on page 130
- How do I view IOx AP state and mode?, on page 130
- How do I view gRPC details?, on page 131
- How do I view AP BLE configuration details?, on page 131
- **How do I view the current TDL values for AP air quality?**, on page 133
- **How do I view the current TDL values for AP temperature and humidity?**, on page 134

Reprovisioning IoT services after failover

What settings are needed to allow access via NETCONF?

To enable access via the Network Configuration Protocol (NETCONF), configure these settings on your wireless controller:

1. Enable the authentication, authorization, and accounting (AAA) new model by entering this command in the global configuration mode:

   ```
   aaa new-model
   ```

2. Set the default AAA authentication for login to the local user database with the command:

```
aaa authentication login default local
```

3. Specify the default AAA authorization for exec (shell access) to use the local user database by using the command:

```
aaa authorization exec default local
```

Enter these commands in the global configuration mode of your wireless controller:

```
wireless controller# configure terminal
wireless controller(config)# aaa new-model
wireless controller(config)# aaa authentication login default local
wireless controller(config)# aaa authorization exec default local
```

After executing these commands, your wireless controller should be properly configured to allow access through NETCONF using the local user database for authentication and authorization.

The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting?

This task shows you how to verify if you have enabled BLE radio on the wireless controller at a global configuration level. This is a necessary setting.

Run the command: **show running-config | include ap dot15**

```
wireless controller# show running-config | include ap dot15
no ap dot15 shutdown
```

Verify if the output is `no ap dot15 shutdown`. This output indicates that the dot15 BLE radios are not shut down.

For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token?

To establish a functioning gRPC connection, a gRPC streaming token must be present on the wireless controller. To verify the token, execute the **show running-config | include ap cisco-dna** command on the wireless controller

```
wireless-controller# show running-config | include ap cisco-dna

ap cisco-dna token 0 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2MjUs
ImNpZCI6Mzc4NTc3ODI1NDI2NzIyNjUwMDAsImVwIjoiMTAuMzAuMTE0LjEwODo4MDAwIiwiaW
F0IjoxNTg1NzA2OTIxfQ.56vXfL1IGrss6TJZDQaWVarAoTWZsIhbe3tGVMEJNYk
```

The resulting output will display the gRPC streaming token. For example:

```
ap cisco-dna token 0 <token_string>
```

Ensure that this token corresponds with the token configured on the access point (AP). You can check the AP's token by running the **show cloud connector key authentication** command.

Additionally, to examine the encoded information contained in the token, you can input the token into a JWT decoder like the one found at http://jwt.io/. Here is an example of the kind of payload data you might see:

```
PAYLOAD:DATA
{
  "tid": 1625,
  "cid": 37857782542672265000,
  "ep": "10.30.114.108:8000",
  "iat": 1585706921
}
```

gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled?

This procedure demonstrates how to enable gRPC in the AP join profile, a necessary configuration.

To view the active settings, run the **show running-config | begin ap profile default-ap-profile** command.

```
controller# show running-config | begin ap profile default-ap-profileap profile
default-ap-profile
 apphost
 cisco-dna grpc
 description "default ap profile"
 mgmtuser username admin password 0 Cisco123! secret 0 Cisco123!
 ssh
trapflags ap crash
trapflags ap noradiocards
trapflags ap register
netconf-yang
end
```

This output reveals the configuration for the default AP profile. Should you require a different profile, apply the command accordingly, replacing **`default-ap-profile`** with the desired profile name.

Ensure the configuration includes the line `cisco-dna grpc`. This line confirms that gRPC is enabled for all access points utilizing this profile.

How do I verify gRPC is up?

To verify whether gRPC is operational, execute the **show ap grpc summary** command.

This command displays the gRPC connection status for each AP connected to the wireless controller, as shown in the example below:

```
controller# show ap grpc summary
AP Name                          AP Mac               gRPC Status
-----------------------------------------------------------------------------------
AP_10.2830                       04eb.409f.a7e0       Up
AP_02.2898                       04eb.409f.ab20       Up
AP_06.28CC                       04eb.409f.acc0       Up
AP_08.28E0                       04eb.409f.ad60       Up
AP_07.28E4                       04eb.409f.ad80       Up
AP_09.28EC                       04eb.409f.adc0       Up
AP_01.28F0                       04eb.409f.ade0       Up
AP_03.2928                       04eb.409f.afa0       Up
AP_05.2934                       04eb.409f.b000       Up
AP_04.2938                       04eb.409f.b020       Up
```

Each AP's name, MAC address, and gRPC status are listed. A status of `Up` indicates that gRPC is active and running for that AP.

.

How do I verify that TDL subscriptions are created and are valid?

1. To initiate the process of viewing all current telemetry subscriptions and to check their types and validity statuses, input the command below:

   ```
   show telemetry ietf subscription all
   ```

2. After executing the command, the wireless controller present a summarized output of the telemetry subscriptions. Enterprise Data Management (EDM) configures six distinct subscriptions, which you can identify by their numbers ranging from 122 to 127.

   Here is a sample of what the command's output might look like:

   ```
   wireless controller# show telemetry ietf subscription all
   Telemetry subscription brief
   ID     Type          State    Filter type
   ----------------------------------------
   122    Configured    Valid    tdl-uri
   123    Configured    Valid    tdl-uri
   124    Configured    Valid    tdl-uri
   125    Configured    Valid    transform-name
   126    Configured    Valid    transform-name
   ```

The output enumerates each subscription's unique ID, its configuration status, the validity of the state, and the applied filter type.

Are the TDL subscriptions created and valid?

Run the command **show telemetry ietf subscription all** command on the wireless controller.

The command displays the subscriptions, the subscription type, and if a subscription is valid. IoT Service creates five different subscriptions 122-126.

```
wireless controller# show telemetry ietf subscription all
  Telemetry subscription brief

  ID               Type        State       Filter type
  ------------------------------------------------------
  122              Configured  Valid       tdl-uri
  123              Configured  Valid       tdl-uri
  124              Configured  Valid       tdl-uri
  125              Configured  Valid       transform-name
  126              Configured  Valid       transform-name
```

What is the TDL status?

Execute the **show telemetry ietf subscription ID receiver** command on the wireless controller.

The command presents the status of Telemetry Description Language (TDL) subscriptions.

```
wireless controller# show telemetry ietf subscription 125 receiver
Telemetry subscription receivers detail:

  Subscription ID: 125
  Address: 10.22.243.33
  Port: 8004
  Protocol: cloud-native
  Profile:
  Connection: 33
  State: Connected
  Explanation:
```

The IoT Service manages five distinct subscriptions, with IDs from 122 to 126. For each subscription:

- Verify that the **Address** matches the IP address of the Cisco Spaces: Connector.
- Confirm that the **State** is **Connected**.

.

How do I view the current CAPWAP values for an AP?

1. Enter the command without any dots in the MAC address of the AP:

   ```
   test platform software database get ewlc_oper/capwap_data;wtp_mac=mac_without_dots
   ```

For example:

```
wireless controller# test platform software database get
ewlc_oper/capwap_data;wtp_mac=1cd1e065c340
```

The output presents a table with various records:

- Index zero contains the AP's MAC address, IP address, model, and other static information.
- The **device_detail.static_info** section includes the AP's model, memory type, CPU type, and memory size, among other details.
- The **device_detail.wtp_version section** includes backup software version, mini iOS version, hardware version, and the current software version that the AP is running.
- The **ap_services** section gives details about monitor mode, DHCP server status, and sniffer interface ID.
- The **tag_info** section indicates whether the AP has any misconfigured tags.
- The **external_module_data** section displays information about any external modules connected to the AP, including product ID and version.
- The **ap_state** section displays administrative and operational states of the AP.
- The **ap_mode_data** section details the current mode and sub-mode of the AP.

```
wireless-controller# test platform software database get
ewlc_oper/capwap_data;wtp_mac=1cd1e065c340
Table Record Index 0 = {
 [0] wtp_mac = 1CD1.E065.C340
 [1] ip_addr = 10.22.243.229
 [2] name = AP84F1.47B2.B868
 [3] device_detail.static_info.board_data.model = C9115AXI-B
 [4] device_detail.static_info.board_data.wtp_serial_num = FJC25331LCY
```

```
 [5] device_detail.static_info.board_data.card_id = 0
 [6] device_detail.static_info.board_data.card_rev = 0
 [7] device_detail.static_info.board_data.wtp_enet_mac = 84F1.47B2.B868
 [8] device_detail.static_info.board_data.ap_sys_info.mem_type = DDR3
 [9] device_detail.static_info.board_data.ap_sys_info.cpu_type =  ARMv8 Processor rev 0
(v8l)
 [10] device_detail.static_info.board_data.ap_sys_info.mem_size = 1971200
 [11] device_detail.static_info.board_data_opt.antenna_type = BSN_INT_ANT_AP
 [12] device_detail.static_info.board_data_opt.wtp_type = BSN_AP_STANDARD
 [13] device_detail.static_info.board_data_opt.remote = true
 [14] device_detail.static_info.board_data_opt.join_priority = 1
 [15] device_detail.static_info.descriptor_data.max_radio_slots = 2
 [16] device_detail.static_info.descriptor_data.radio_slots_in_use = 2
 [17] device_detail.static_info.descriptor_data.encryption_capabilities = true
 [18] device_detail.static_info.ap_prov.is_universal = false
 [19] device_detail.static_info.ap_prov.universal_prime_status = Unprimed
 [20] device_detail.static_info.ap_models.model = C9115AXI-B
 [21] device_detail.static_info.ap_models.ap_model_short = 9115AXI
 [22] device_detail.static_info.num_ports = 1
 [23] device_detail.static_info.num_slots = 2
 [24] device_detail.static_info.wtp_type = 83
 [25] device_detail.static_info.wtp_model_type = 90
 [26] device_detail.static_info.ap_capability = [
        BRIDGE_MODE_CAPABLE,
        CAP_THREE_SPATIAL_STREAMS_CAPABLE,
        ANTENNA_SELECTION_RESTRICTED_CAPABLE,
        AVC_FNF_CAPABLE,
        RXSOP_THRESHOLD_CAPABLE,
        FABRIC_CAPABILITY,
        BARBADOS_INTERNAL_ANTENNA_SKU_CAPABLE,
        REMOTE_LAN_CAPABLE,
        DOT11AC_160MHZ_CHANNEL_WIDTH_CAPABLE,
        AVC_FNF_FABRIC_CAPABLE,
        AP_CTS_CAPABLE,
        AP_QCA_SPECTRUM_INTELLIGENCE_CAPABLE,
        FIPS_CAPABLE,
        IS_DOT1X_PORT_AUTH_CAPABLE,
        AP_TRACING_CAPABLE,
        AP_WPA3_CAPABLE,
        OFFICE_EXTEND_CAPABLE,
        ETH2_RLAN_CAPABLE,
        AP_MEWLC_CAPABLE,
        SNIFFER_MODE_CAPABLE,
        ICAP_PARTIAL_PACKET_TRACE_CAPABLE,
        ICAP_ANOMALY_DETECTION_CAPABLE,
        ICAP_STATISTICS_CAPABLE,
        ICAP_FEATURE_CAPABLE,
        AP_AWIPS_CAPABLE,
        IOX_HARDWARE_CAPABLE,
        AUX_CLIENT_INTERFACE_CAPABLE,
        CLICKOS_FEATURE_SET,
        AP_TRAFFIC_DISTRIBUTION_STATISTICS_CAPABLE
]

 [27] device_detail.static_info.remote_lan.num_rlan_ports = 0
 [28] device_detail.static_info.remote_lan.rlan_slot_id = 0
 [29] device_detail.static_info.remote_lan.rlan_port_can_be_zero = false
 [30] device_detail.static_info.is_cisco_ap = true
 [31] device_detail.static_info.is_mm_opt = false
 [32] device_detail.static_info.ap_image_name =
 [33] device_detail.dynamic_info.ap_crash_data.ap_crash_file =
 [34] device_detail.dynamic_info.ap_crash_data.ap_radio_2g_crash_file =
 [35] device_detail.dynamic_info.ap_crash_data.ap_radio_5g_crash_file =
 [36] device_detail.dynamic_info.led_brightness_level = 8
```

```
 [37] device_detail.dynamic_info.led_state_enabled = true
 [38] device_detail.dynamic_info.reset_button_state = false
 [39] device_detail.dynamic_info.led_flash_enabled = true
 [40] device_detail.dynamic_info.flash_sec = 0
 [41] device_detail.dynamic_info.temp_info.degree = 0
 [42] device_detail.dynamic_info.temp_info.temp_status = AP_TEMP_STATUS_NORMAL
 [43] device_detail.dynamic_info.temp_info.heater_status =
AP_TEMP_HEATER_STATUS_BOTH_HEATERS_OFF
 [44] device_detail.wtp_version.backup_sw_version.version = 17
 [45] device_detail.wtp_version.backup_sw_version.release = 7
 [46] device_detail.wtp_version.backup_sw_version.maint = 1
 [47] device_detail.wtp_version.backup_sw_version.build = 11
 [48] device_detail.wtp_version.backup_sw_version.stringified_ver_info = 17.7.1.11
 [49] device_detail.wtp_version.mini_ios_version.version = 0
 [50] device_detail.wtp_version.mini_ios_version.release = 0
 [51] device_detail.wtp_version.mini_ios_version.maint = 0
 [52] device_detail.wtp_version.mini_ios_version.build = 0
 [53] device_detail.wtp_version.mini_ios_version.stringified_ver_info =
 [54] device_detail.wtp_version.hw_ver.version = 1
 [55] device_detail.wtp_version.hw_ver.release = 0
 [56] device_detail.wtp_version.hw_ver.maint = 0
 [57] device_detail.wtp_version.hw_ver.build = 0
 [58] device_detail.wtp_version.hw_ver.stringified_ver_info = 1.0.0.0
 [59] device_detail.wtp_version.sw_ver.version = 17
 [60] device_detail.wtp_version.sw_ver.release = 3
 [61] device_detail.wtp_version.sw_ver.maint = 5
 [62] device_detail.wtp_version.sw_ver.build = 43
 [63] device_detail.wtp_version.sw_ver.stringified_ver_info = 17.3.5.43
 [64] device_detail.wtp_version.boot_ver.version = 1
 [65] device_detail.wtp_version.boot_ver.release = 1
 [66] device_detail.wtp_version.boot_ver.maint = 2
 [67] device_detail.wtp_version.boot_ver.build = 4
 [68] device_detail.wtp_version.boot_ver.stringified_ver_info = 1.1.2.4
 [69] device_detail.wtp_version.sw_version = 17.3.5.43
 [70] ap_lag_enabled = false
 [71] ap_location.floor = 0
 [72] ap_location.location = default location
 [73] ap_services.monitor_mode_opt_type = ENM_MODE_TYPE_NONE
 [74] ap_services.ap_dhcp_server.is_dhcp_server_enabled = false
 [75] ap_services.sniffer_ap_ifid = 0
 [76] tag_info.misconfigured_tag = APMGR_TAGS_CONFIGURED
 [77] tag_info.tag_source = EWLC_TAG_SRC_DEFAULT
 [78] tag_info.is_ap_misconfigured = false
 [79] tag_info.is_policy_tag_misconfigured = false
 [80] tag_info.is_site_tag_misconfigured = false
 [81] tag_info.is_rf_tag_misconfigured = false
 [82] tag_info.is_flex_profile_misconfigured = false
 [83] tag_info.is_ap_profile_misconfigured = false
 [84] tag_info.is_rf_profile_24_misconfigured = false
 [85] tag_info.is_rf_profile_5_misconfigured = false
 [86] tag_info.is_ap_tag_registration_done = true
 [87] tag_info.resolved_tag_info.resolved_policy_tag = default-policy-tag
 [88] tag_info.resolved_tag_info.resolved_site_tag = default-site-tag
 [89] tag_info.resolved_tag_info.resolved_rf_tag = default-rf-tag
 [90] tag_info.policy_tag_info.policy_tag_name = default-policy-tag
 [91] tag_info.site_tag.site_tag_name = default-site-tag
 [92] tag_info.site_tag.ap_profile = default-ap-profile
 [93] tag_info.site_tag.flex_profile = default-flex-profile
 [94] tag_info.rf_tag.rf_tag_name = default-rf-tag
 [95] tag_info.rf_tag.dot11a_rf_profile = default_rf_5gh
 [96] tag_info.rf_tag.dot11b_rf_profile = default_rf_24gh
 [97] tag_info.filter_info.filter_name =
 [98] tunnel.preferred_mode = PREFERRED_MODE_IPV4
 [99] tunnel.udp_lite = IPV6_CAPWAP_UDPLITE_UNCONFIG
```

```
 [100] external_module_data.xm_data.is_module_present = false
 [101] external_module_data.xm_data.enable = true
 [102] external_module_data.xm_data.xm.goodness_field = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [103] external_module_data.xm_data.xm.numeric_id = 12
 [104] external_module_data.xm_data.xm.version = [
        0,
        0
]

 [105] external_module_data.xm_data.xm.product_id = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [106] external_module_data.xm_data.xm.serial_number = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [107] external_module_data.xm_data.xm.max_power = 0
 [108] external_module_data.xm_data.xm.eeprom_size = [
```

```
        0,
        0,
        0,
        0
]

 [109] external_module_data.xm_data.xm.xm_cookie_version = 0
 [110] external_module_data.xm_data.xm.inventory.prod_id = C9115AXI-B
 [111] external_module_data.xm_data.xm.inventory.ver_id = 05
 [112] external_module_data.xm_data.xm.inventory.serial_num = FJC25331LCY
 [113] external_module_data.xm_data.xm.inventory.ent_name = C9115AX
 [114] external_module_data.xm_data.xm.inventory.ent_desc = Cisco Catalyst 9115AX Series
(IEEE 802.11ax) Access Point
 [115] external_module_data.xm_data.xm.module_name =
 [116] external_module_data.xm_data.xm.version_string =
 [117] external_module_data.xm_data.xm.serial_number_string =
 [118] external_module_data.xm_data.xm.product_id_string =
 [119] external_module_data.xm_data.xm.module_type =
 [120] external_module_data.xm_data.xm.module_description =
 [121] external_module_data.xm_data.xm.module_capabilities =
 [122] external_module_data.xm_data.xm.module_state =
 [123] external_module_data.usb_data.is_module_present = false
 [124] external_module_data.usb_data.enable = true
 [125] external_module_data.usb_data.xm.goodness_field = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [126] external_module_data.usb_data.xm.numeric_id = 12
 [127] external_module_data.usb_data.xm.version = [
        0,
        0
]

 [128] external_module_data.usb_data.xm.product_id = [
        85,
        110,
        107,
        110,
        111,
        119,
        110,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
```

```
        0,
        0,
        0
]

 [129] external_module_data.usb_data.xm.serial_number = [
        85,
        110,
        107,
        110,
        111,
        119,
        110,
        0,
        0,
        0,
        0
]

 [130] external_module_data.usb_data.xm.max_power = 0
 [131] external_module_data.usb_data.xm.eeprom_size = [
        0,
        0,
        0,
        0
]

 [132] external_module_data.usb_data.xm.xm_cookie_version = 0
 [133] external_module_data.usb_data.xm.inventory.prod_id =
 [134] external_module_data.usb_data.xm.inventory.ver_id =
 [135] external_module_data.usb_data.xm.inventory.serial_num =
 [136] external_module_data.usb_data.xm.inventory.ent_name =
 [137] external_module_data.usb_data.xm.inventory.ent_desc =
 [138] external_module_data.usb_data.xm.module_name = Unknown
 [139] external_module_data.usb_data.xm.version_string = V00
 [140] external_module_data.usb_data.xm.serial_number_string = Unknown
 [141] external_module_data.usb_data.xm.product_id_string = Unknown
 [142] external_module_data.usb_data.xm.module_type = USB Module
 [143] external_module_data.usb_data.xm.module_description = Unknown
 [144] external_module_data.usb_data.xm.module_capabilities =
 [145] external_module_data.usb_data.xm.module_state = Not Detected
 [146] external_module_data.usb_override = false
 [147] external_module_data.is_ext_module_enabled = false
 [148] external_module_data.expansion_module_extended_info.power_sufficient = 0
 [149] external_module_data.expansion_module_extended_info.antenna_product_id = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
```

```
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [150] external_module_data.expansion_module_extended_info.antenna_serial_number = [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0
]

 [151] external_module_data.expansion_module_extended_info.antenna_prod_ID =
 [152] ipv6_joined = 0
 [153] wtp_ip_addr = 10.22.243.229
 [154] ap_state.ap_admin_state = ENM_ADMINSTATE_ENABLED
 [155] ap_state.ap_operation_state = EWLC_ENM_AP_STATE_REG
 [156] ap_mode_data.home_ap_enabled = false
 [157] ap_mode_data.clear_mode = false
 [158] ap_mode_data.ap_sub_mode = AP_SUB_MODE_NONE
 [159] ap_mode_data.wtp_mode = EWLC_ENM_SPAM_AP_MODE_LOCAL
 [160] ap_mode_data.ap_fabric_data.is_fabric_ap = false
 [161] ap_mode_data.ap_fabric_data.lisp_state = EWLC_ENM_LISP_QUERY_NOT_NEEDED
 [162] ap_time_info.boot_time = Fri, 05 Aug 2022 06:47:33 +0000
```

```
 [163] ap_time_info.join_time = Fri, 05 Aug 2022 06:50:13 +0000
 [164] ap_time_info.join_time_taken = 159
 [165] ap_time_info.last_up_time = 1
 [166] country_code = US
 [167] ap_security_data.lsc_provision_inprogress = false
 [168] ap_security_data.fips_enabled = false
 [169] ap_security_data.wlancc_enabled = false
 [170] ap_security_data.cert_type = EWLC_CERT_MIC
 [171] ap_security_data.lsc_ap_auth_type = EWLC_ENM_LSC_AP_AUTH_CAPWAP_DTLS
 [172] num_radio_slots = 2
 [173] dart_is_connected = false
 [174] dart_is_connected_str = Not Connected
 [175] is_master = false
 [176] sliding_window.multi_window_support = true
 [177] sliding_window.window_size = 1
 [178] ap_vlan.vlan_tag_state = VLAN_TAGGING_DISABLED
 [179] ap_vlan.vlan_tag_id = 0
 [180] capwap_iifid = 2415919114
 [181] hyperlocation_data.hyperlocation_method = HYPERLOCATION_METHOD_NONE
 [182] hyperlocation_data.per_ap_hl_tlv_rcvd = HYPERLOCATION_AP_TLV_RECEIVED
 [183] hyperlocation_data.cmx_ip = null
 [184] cdp_enable = true
 [185] cdp_cache_index_list.buffer = [
        1,
        0,
        0,
        0
]

 [186] ap_stationing_type = EWLC_ENM_INDOOR_AP
 [187] int_if_num = 0
 [188] radio_key = [
        {wtp_mac : 1CD1.E065.C340, radio_slot_id : 0},
        {wtp_mac : 1CD1.E065.C340, radio_slot_id : 1},
        {wtp_mac : 0000.0000.0000, radio_slot_id : 0},
        {wtp_mac : 0000.0000.0000, radio_slot_id : 0}
]

 [189] reboot_stats.reboots = 9
 [190] reboot_stats.ac_initiated = 4
 [191] reboot_stats.link_failure = 0
 [192] reboot_stats.sw_failure = 0
 [193] reboot_stats.hw_failure = 0
 [194] reboot_stats.unknown_failure = 0
 [195] reboot_stats.reboot_reason = AP_REBOOT_REASON_IMG_UPGRADE
 [196] reboot_stats.reboot_types = AP_REBOOT_SPAM_INITIATED
 [197] reboot_stats.reboot_type = AP_REBOOT_SPAM_INITIATED
 [198] slot_type = [
        0,
        0,
        0,
        0
]

 [199] mesh_profile_inuse =
 [200] mesh_ap_role = ENM_EWLC_AP_ROLE_MESH
 [201] wtp_cfg_reval_data.wtp_revalidate = false
 [202] wtp_cfg_reval_data.pending_wtp_notifies = 0
 [203] me_internal_ap = false
 [204] ap_type = AP_TYPE_CAPWAP
 [205] is_mewlc_candidate = false
 [206] is_invalid_master = false
 [207] is_callback_success = false
 [208] proxy_info.hostname =
```

```
 [209] proxy_info.port = 0
 [210] proxy_info.no_proxy_list =
 [211] grpc_enabled = true
 [212] ap_image_size = 0
 [213] ap_cur_bytes = 0
 [214] image_size_eta = 0
 [215] image_size_start_time = Thu, 01 Jan 1970 00:00:00 +0000
 [216] image_size_percentage = 0
 [217] dual_dfs_capable = false
 [218] mdns_group_id = 0
 [219] mdns_rule_name =
 [220] ap_keepalive_state = true
 [221] local_dhcp = false
 [222] ipv4_pool.network = 0.0.0.0
 [223] ipv4_pool.lease_time = 0
 [224] ipv4_pool.netmask = 0.0.0.0
 [225] wlc_image_size_eta = 0
 [226] wlc_image_size_start_time = Thu, 01 Jan 1970 00:00:00 +0000
 [227] wlc_image_size_percentage = 0
 [228] matching_ewc_image = false
 [229] disconnect_detail.ext_disconnect_reason_capable = false
 [230] disconnect_detail.disconnect_reason = UNKOWN
 [231] antenna_monitor.support = false
 [232] antenna_monitor.enabled = false
 [233] antenna_monitor.rssi_fail_threshold = 0
 [234] antenna_monitor.weak_rssi = 0
 [235] antenna_monitor.detection_time = 0
 [236] wtp_ip = 10.22.243.229
}
```

How do I view the current TDL values for an AP?

1. Execute the command on the wireless controller to retrieve the current configuration for an AP:

   ```
   test platform software database get ewlc_oper/ble_ltx_ap;ap_mac=<mac-without-dots>
   ```

   Replace <*mac-without-dots*> with the actual MAC address of the AP, removing any periods. For example:

   ```
   wireless controller# test platform software database get
   ewlc_oper/ble_ltx_ap;ap_mac=04eb409ec3c0
   ```

The output presents a list of parameters, such as:

- The AP's MAC address, without any delimiters.
- The administrative state of the AP.
- Details of the scan configuration, including intervals and states.
- Settings for the iBeacon and Eddystone profiles.
- Information on viBeacons profiles.
- Statistics on the types of scans performed.
- Host device data, such as the name and BLE MAC address.
- Current feature modes and the operational status of the device.
- Capabilities of the device, including support for technologies like BLE and Zigbee.

Each parameter provides details including the last report time and the validity of the status.

```
wireless controller# test platform software database get
ewlc_oper/ble_ltx_ap;ap_mac=04eb409ec3c0
Table Record Index 0 = {
 [0] ap_mac = 04EB.409E.C3C0
 [1] admin.state = BLE_LTX_ADMIN_STATE_ON
 [2] admin.feedback.state_status = 0
 [3] admin.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [4] admin.report.valid = true
 [5] scan_config.interval_sec = 1
 [6] scan_config.state = BLE_LTX_SCAN_STATE_ON
 [7] scan_config.max_value = 8
 [8] scan_config.window_msec = 800
 [9] scan_config.filter = BLE_LTX_SCAN_FILTER_ON
 [10] scan_config.feedback.interval_sec_status = 0
 [11] scan_config.feedback.state_status = 0
 [12] scan_config.feedback.max_value_status = 0
 [13] scan_config.feedback.window_msec_status = 0
 [14] scan_config.feedback.filter_status = 0
 [15] scan_config.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [16] scan_config.report.valid = true
 [17] profile_ibeacon.uuid = 00000000-0000-0000-0000-000000000000
 [18] profile_ibeacon.major = 0
 [19] profile_ibeacon.minor = 0
 [20] profile_ibeacon.tx_power = 0
 [21] profile_ibeacon.frequency_msec = 0
 [22] profile_ibeacon.adv_tx_power = 65
 [23] profile_ibeacon.feedback.uuid_status = 0
 [24] profile_ibeacon.feedback.major_status = 0
 [25] profile_ibeacon.feedback.minor_status = 0
 [26] profile_ibeacon.feedback.tx_power_status = 0
 [27] profile_ibeacon.feedback.frequency_msec_status = 0
 [28] profile_ibeacon.feedback.adv_tx_power_status = 0
 [29] profile_ibeacon.report.last_report_time = Fri, 05 Jun 2020 02:18:30 +0000
 [30] profile_ibeacon.report.valid = true
 [31] profile_eddy_url.url =
 [32] profile_eddy_url.feedback.url_status = 0
 [33] profile_eddy_url.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [34] profile_eddy_url.report.valid = false
 [35] profile_eddy_uid.namespace =
 [36] profile_eddy_uid.instance_id =
 [37] profile_eddy_uid.feedback.namespace_status = 0
 [38] profile_eddy_uid.feedback.instance_id_status = 0
 [39] profile_eddy_uid.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [40] profile_eddy_uid.report.valid = false
 [41] profile_vibeacons.common.interval_msec = 0
 [42] profile_vibeacons.common.feedback.interval_msec_status = 0
 [43] profile_vibeacons.common.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [44] profile_vibeacons.common.report.valid = false
 [45] profile_vibeacons.vibeacons = [
        {beacon_id : 0, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 1, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
```

```
report.valid : false},
        {beacon_id : 2, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 3, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false},
        {beacon_id : 4, uuid : , tx_power : 0, major : 0, minor : 0, adv_tx_power : 0,
status : BLE_LTX_VIBEACON_OFF,
feedback.beacon_id_status : 0, feedback.uuid_status : 0, feedback.tx_power_status : 0,
feedback.major_status : 0,
feedback.minor_status : 0, feedback.status_status : 0, feedback.adv_tx_power_status : 0,
report.last_report_time : Thu, 01 Jan 1970 00:00:00 +0000,
report.valid : false}
]

 [46] profile_vibeacons.report.last_report_time = Thu, 01 Jan 1970 00:00:00 +0000
 [47] profile_vibeacons.report.valid = false
 [48] scan_counters.total = 0
 [49] scan_counters.dna_ltx = 0
 [50] scan_counters.system_tlm = 0
 [51] scan_counters.event_tlm = 0
 [52] scan_counters.regular_tlm = 0
 [53] scan_counters.emergency = 0
 [54] scan_counters.event_emergency = 0
 [55] scan_counters.other = 0
 [56] scan_counters.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [57] scan_counters.report.valid = true
 [58] host_data.device_name = Developme
 [59] host_data.ble_mac = 806F.B031.E024
 [60] host_data.api_version = 1
 [61] host_data.fw_version = FF020710
 [62] host_data.advertise_count = 0
 [63] host_data.uptime_dsec = 10
 [64] host_data.active_profile = BLE_LTX_PROFILE_NO_ADV
 [65] host_data.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [66] host_data.report.valid = true
 [67] feature_mode.feature = BLE_LTX_FEATURE_ZIGBEE
 [68] feature_mode.mode = BLE_LTX_MODE_IOX
 [69] feature_mode.report.last_report_time = Fri, 05 Jun 2020 07:26:19 +0000
 [70] feature_mode.report.valid = true
 [71] device_status.device = BLE_LTX_DEVICE_MSM1
 [72] device_status.state = BLE_LTX_DEVICE_STATE_IOX_BLE_MODE
 [73] device_status.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [74] device_status.report.valid = true
 [75] capability.ble = true
 [76] capability.zigbee = true
 [77] capability.thread = false
 [78] capability.usb = true
 [79] capability.report.last_report_time = Wed, 03 Jun 2020 08:08:20 +0000
 [80] capability.report.valid = true
}
```

How do I get the telemetry connection status?

This procedure shows you how to check the telemetry connection status.

1. Enter the command:

   ```
   show telemetry internal protocol cloud-native manager <connector-ip-address> 8004
   source-address <source-IP-address>
   ```

   Replace <*connector-ip-address*> with the IP address of the connector and <*source-IP-address*> with the source IP address of your wireless controller.

2. In the output displayed, look for the **State** field to determine the telemetry connection status.

The following is a sample output of the command. The **State** is **CNDP_STATE_CONNECTED** and that indicates that the connection is successfully established

```
wireless controller# show telemetry internal protocol cloud-native manager 10.22.243.53
8004 source-address 10.22.243.52
Telemetry protocol manager stats:

Con str               : 10.22.243.53:8004:0:10.22.243.52
Sockfd                : 97
Protocol              : cloud-native
State                 : CNDP_STATE_CONNECTED
Table id              : 0
Wait Mask             :
Connection Retries    : 0
Send Retries          : 0
Pending events        : 0
Session requests      : 1
Session replies       : 1
Source ip             : 10.22.243.52
Bytes Sent            : 1121093
Msgs Sent             : 17613
Msgs Received         : 0
Creation time:        : Wed Jun  3 23:16:22:830
Last connected time:  : Wed Jun  3 23:16:22:892
Last disconnect time: :
Last error:           :
Connection flaps:     : 0
Last flap Reason:     :
Keep Alive Timeouts:  : 0
Last Transport Error  : No Error
```

How do I view IOx AP state and mode?

To view the Bluetooth Low Energy (BLE) state and mode for each AP connected to the wireless controller, you can perform these steps:

1. On the wireless controller, enter this command:

   ```
   show ap ble summary
   ```

The following example shows how to view the BLE state and mode for each AP.

This output provides a summary of each AP's BLE status, indicating whether it is active (**Up**) and the current BLE mode, which is **IOx** for all APs in this example.

```
wireless-controller# show ap ble summary
AP Name                          BLE AP State          BLE mode
-----------------------------------------------------------------
AP_10.2830                       Up                    IOx
AP_02.2898                       Up                    IOx
AP_06.28CC                       Up                    IOx
AP_08.28E0                       Up                    IOx
AP_07.28E4                       Up                    IOx
AP_09.28EC                       Up                    IOx
AP_01.28F0                       Up                    IOx
AP_03.2928                       Up                    IOx
AP_05.2934                       Up                    IOx
AP_04.2938                       Up                    IOx
```

How do I view gRPC details?

To view detailed gRPC (gRPC Remote Procedure Calls) statistics for a specific Access Point (AP), follow these steps:

1. Run this command after replacing the <*AP Name*>:

   ```
   show ap name <AP Name> grpc detail
   ```

2. The output provides detailed gRPC statistics for the specified AP.

   In this output, the **gRPC channel status** indicates whether the connection is active (**Up**). The output also shows various packet statistics such as transmit attempts, transmit failures, packets received, and receive failures.

   The following is a sample output of the command:

   ```
   wireless-controller# show ap name ap-name grpc detail

   gRPC channel status        : Up
   Packets transmit attempts  : 818411
   Packets transmit failures  : 2651788
   Packets receive count      : 2711
   Packets receive failures   : 0
   ```

How do I view AP BLE configuration details?

To understand the Bluetooth Low Energy (BLE) configuration details for an AP, you can examine the output provided by your wireless controller. Run this command, and replace <*ap-name*>.

```
show ap name <ap-name> ble detail
```

The command displays the detailed BLE configuration settings for an AP.

```
wireless-controller# show ap name ap-name grpc detail

Mode report time          : 06/25/2020 21:30:54
Mode                      : Advanced (IOx)
Radio mode                : BLE
Admin state report time   : 06/25/2020 21:31:14
Admin state               : Up
Interface report time     : 06/25/2020 21:30:58
Interface                 : MSM1
Interface state           : Open
Type                      : Integrated
```

```
Capability report time    : 06/25/2020 21:16:25
Capability                : BLE, Zigbee, USB,
Host data report time     : 06/25/2020 21:31:14
Host data
  Device name                 : AP_102830
  Dot15 Radio MAC             : 18:04:ed:c5:02:bc
  API version                 : 256
  FW version                  : 2.7.16
  Broadcast count             : -1844445184
  Uptime                      : 838860800 deciseconds
  Active profile              : No Advertisement
Scan Statistics report time    : 06/25/2020 21:30:36
Scan statistics
  Total scan records          : 0
Scan role report time  : 06/25/2020 21:31:14
Scan role
  Scan state                  : Enable
  Scan interval               : 1 seconds
  Scan window                 : 800 milliseconds
  Scan max value              : 8
  Scan filter                 : Enable
Broadcaster role
  Current profile type: iBeacon
  Last report time            : N/A
    UUID                      : Unknown
    Major                     : Unknown
    Minor                     : Unknown
    Transmit power            : Unknown
    Frequency                 : Unknown
    Advertised transmit power : Unknown
  Current profile type: Eddystone URL
  Last report time            : 06/25/2020 21:27:50
    URL                       : http://dnaspaces.io/edm
  Current profile type: Eddystone UID
  Last report time            : N/A
    Namespace                 : Unknown
    Instance id               : Unknown
  Current profile type: viBeacon
  Last report time            : N/A
    Interval                  : Unknown
    Beacon ID                 : 0
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 1
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 2
      UUID                      : Unknown
      Major                     : Unknown
      Minor                     : Unknown
      Transmit power            : Unknown
      Advertised transmit power : Unknown
      Enable                    : Unknown
    Beacon ID                 : 3
      UUID                      : Unknown
      Major                     : Unknown
```

```
    Minor                      : Unknown
    Transmit power             : Unknown
    Advertised transmit power  : Unknown
    Enable                     : Unknown
  Beacon ID                 : 4
    UUID                       : Unknown
    Major                      : Unknown
    Minor                      : Unknown
    Transmit power             : Unknown
    Advertised transmit power  : Unknown
    Enable                     : Unknown
```

Some of the output descriptors are described below:

1. **Mode Report Time:** This timestamp, **06/25/2020 21:30:54**, indicates when the AP mode was last reported.
2. **Mode:** The AP is set to an **Advanced (IOx)** operational mode.
3. **Radio Mode:** The radio is operating in **BLE** mode.
4. **Admin State Report Time:** As of **06/25/2020 21:31:14**, the administrative state of the AP was last reported.
5. **Admin State:** The AP is currently **Up** and operational.
6. **Interface Report Time:** The interface status was last reported on **06/25/2020 21:30:58**.
7. **Interface:** The interface identifier is **MSM1**.
8. **Interface State:** The interface is **Open** for connections.
9. **Type:** The AP has an **Integrated** interface type.
10. **Capability Report Time:** The capabilities were last reported on **06/25/2020 21:16:25**.
11. **Capability:** The AP supports **BLE**, **Zigbee**, and **USB** functionalities.
12. **Host Data Report Time:** This timestamp, **06/25/2020 21:31:14**, shows when the host data was last reported.
13. **Host Data:** It includes the AP's name **AP_102830**, its Dot15 radio MAC address **18:04:ed:c5:02:bc**, API version **256**, firmware version **2.7.16**, and other operational details.
14. **Scan Statistics Report Time:** The scan statistics were last reported on **06/25/2020 21:30:36**.
15. **Scan Statistics:** Indicates no total scan records are available.
16. **Scan Role Report Time:** The scan role was last reported on **06/25/2020 21:31:14**.
17. **Scan Role:** The AP is set to enable scanning with a **1-second** interval and an **800-millisecond** window. The maximum value is **8** and the scan filter is enabled.

How do I view the current TDL values for AP air quality?

To view the current Total Dissolved Load (TDL) values for AP air quality, perform these steps:

1. Run the command to retrieve the TDL values:

```
test platform software database get-n all ewlc_oper/ap_air_quality
```

2. The command displays the current TDL values for all APs with air quality sensors. For example:

```
wireless controller# test platform software database get-n all ewlc_oper/ap_air_quality
Table Record Index 0 = {
[0] ap_mac = 687D.B45E.E7C0
[1] last_update = Tue, 12 Oct 2021 15:08:19 +0530
[2] rmox_0 = 5.62121e+07
[3] rmox_1 = 6.12815e+06
[4] rmox_2 = 1.26038e+06
[5] rmox_3 = 579564
[6] rmox_4 = 398259
[7] rmox_5 = 280246
[8] rmox_6 = 201467
[9] rmox_7 = 370324
[10] rmox_8 = 680235
[11] rmox_9 = 1.29709e+06
[12] rmox_10 = 3.18129e+06
[13] rmox_11 = 1.06436e+07
[14] rmox_12 = 6.10561e+07
[15] iaq = 1
[16] etoh = 0.0094
[17] eco2 = 400.212
[18] tvoc = 0.0178
}
```

In this example, the output provides the air quality data for an AP, including the MAC address, last update time, various rmox values, indoor air quality (iaq), ethanol (etoh), equivalent carbon dioxide (eco2), and total volatile organic compounds (tvoc).

How do I view the current TDL values for AP temperature and humidity?

To view the current Total Dissolved Load (TDL) values for AP temperature and humidity, please follow these steps:

1. Execute the command to fetch the TDL values for temperature and humidity:

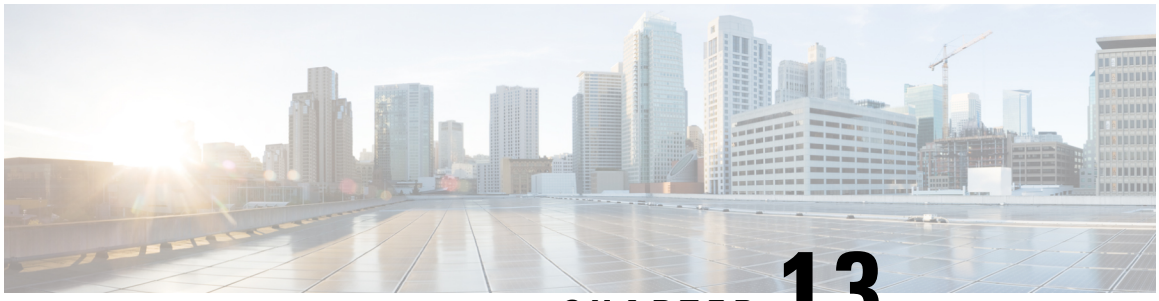
```
test platform software database get-n all ewlc_oper/ap_temp
```

2. This command shows the TDL values for all APs equipped with temperature and humidity sensors. For example:

```
wireless controller# test platform software database get-n all ewlc_oper/ap_temp

Table Record Index 0 = {
[0] ap_mac = 687D.B45E.E7C0
[1] last_update = Tue, 12 Oct 2021 15:08:19 +0530
[2] temp = 233.382
[3] humidity = 0
}
```

In this example, the output lists the temperature and humidity values, along with the MAC address of the AP and the last update timestamp.



CHAPTER 13

Troubleshoot IoT services: IOx application

- How do I verify the IOx application is running on the AP?, on page 135
- **How do I debug the IOx application installation failure?**, on page 135
- How do I verify the IoX Application AP bundle download from Cisco Spaces? , on page 136
- How do I start an interactive shell session for the IOx application?, on page 136
- How can I see the logs for the IOx application?, on page 137
- How do I monitor metrics in the IOx application?, on page 137
- **How do I monitor BLE scans in the IoX Application?**, on page 139
- What files exist in the IOx application?, on page 141

How do I verify the IOx application is running on the AP?

Run the command: **show iox applications**

App State should be *RUNNING* to indicate if it is running.

```
AP# show iox applications
Total Number of Apps : 1
--------------------------
App Name                      : cisco_dnas_ble_iox_app
   App Ip                     : 192.168.11.2
   App State                  : RUNNING
   App Token                  : 02fb3e98-ac02-4356-95ba-c43e8a1f4217
   App Protocol               : ble
   App Grpc Connection        : Up
   Rx Pkts From App           : 3878345
   Tx Pkts To App             : 6460
   Tx Pkts To Wlc             : 0
   Tx Data Pkts To DNASpaces  : 3866864
   Tx Cfg Resp To DNASpaces   : 1
   Rx KeepAlive from App      : 11480
   Dropped Pkts               : 0
   App keepAlive Received On  : Mar 24 05:56:49
```

How do I debug the IOx application installation failure?

1. Ensure that the Network Time Protocol (NTP) server is synchronized with the Wireless Controller and APs in use.

2. Cisco Spaces: Connector installs the IoX Application. Download the AP image bundle from Cisco Spaces to Connector. Next, use the Cisco Application Framework (CAF) to install the image and launch the application from Cisco Spaces, primarily utilizing the ioxclient tool. For more information, refer What is ioxclient?.
3. To examine the logs, you can either upload them to the Cisco Spaces or log into Cisco Spaces: Connector using SSH.
4. Observe these critical logs:
   - `/opt/spaces-connector/runtime/logs/iot-services/server.log` : Records the initiation and completion of requests. It indicates when the main installation begins and the parameters it uses.
   - `/opt/spaces-connector/runtime/logs/iot-services/dnas_iox_app_manage.log`: Provides detailed information on the installation process.
5. To monitor the logs in real-time, do these:
   - As a spacesadmin user, run the command, `tail -F /opt/spaces-connector/runtime/logs/iot-services/server.log`.
   - As a spacesadmin user, run the command, `tail -F /opt/spaces-connector/runtime/logs/iot-services/dnas_iox_app_manage.log`.

How do I verify the IoX Application AP bundle download from Cisco Spaces?

The IoX Application installation is done from the Cisco Spaces: Connector. The AP image bundle is downloaded from Cisco Spaces to Cisco Spaces: Connector. To verify if the IoX Application was downloaded accurately, you can check the log files. Refer to How do I debug the IOx application installation failure?, on page 135

If the logs suggest a problem with the download, you can attempt to manually download the image. To manually download the image, log into Cisco Spaces: Connector via SSH. As a **spacesadmin** user, use the **wget** command:

```
spacesadmin# wget
"https://dnaspaces.io/api/edm/v1/device/iox-app/download?id=cisco_dnas_ble_iox_app&version=1.1.16"
```

How do I start an interactive shell session for the IOx application?

Run the command: **connect iox application**

This starts a shell which is running inside the IOx application container.

```
AP# connect iox application
/ #
```

How can I see the logs for the IOx application?

First, start an interactive shell using the **show iox application** command.

Then, run the command: **tail -F /data/logs/dnas_ble.log**

You can see the logs for the IOx application.

```
AP# tail -F /data/logs/dnas_ble.log
Tue Mar 24 06:55:21 2020 [INFO]: Starting DNA Spaces BLE IOx Application
Tue Mar 24 06:55:21 2020 [INFO]: Auth token file contents:
db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Setting gRPC endpoint to: 1.1.7.101:57777
Tue Mar 24 06:55:21 2020 [INFO]: Auth with token: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Attempt to connect to DNAS Channel
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run metrics
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run Channel Keepalive
Tue Mar 24 06:55:21 2020 [INFO]: Initialize DNAS Reader Channel
Tue Mar 24 06:55:21 2020 [INFO]: Start listener for messages
Tue Mar 24 06:55:21 2020 [INFO]: Running BLE scan thread
```

How do I monitor metrics in the IOx application?

First, start an interactive shell using the **show iox application** command.

Run the command: **tail -F /data/logs/dnas_ble_metrics.log**

This command begins watching the log file for IOx application metrics. Metrics are updated every 30 seconds in the log file.

Table 3: Monitor Metrics

Metrics Name	Metrics Description
Application Version	The version number of the IOx application that is currently in use.
Start Time	The timestamp of when the application was initialized on the AP.
Up Time	The total time the application has been running since it was last started.
Total Physical Memory	The total RAM allocated to the application's container.
Physical Memory Free	The amount of RAM that remains unused in the application's container.
Physical Memory Used	The amount of RAM that is currently being used by the application's container.
Total Physical Shared Memory	The amount of memory shared amongst processes or containers.
Total Physical Buffer Memory	The memory dedicated to buffering, which aids in optimizing I/O operations.
Total AP Percent CPU Used	The percentage of the AP's CPU that is consumed by the application's container.

Metrics Name	Metrics Description
Process Virtual Memory	The virtual memory used by the application's process.
Process Physical Memory	The amount of physical RAM occupied by the application's process.
Process CPU Used	The CPU usage of the application's process.
gRPC Reconnect Count	The number of times a gRPC (remote procedure call) connection has been reestablished.
CAPWAP Restart Count	The number of restarts of the Control And Provisioning of Wireless Access Points (CAPWAP) protocol connection.
Last CAPWAP Restart Time	The timestamp marking the most recent CAPWAP connection restart.
BLE Device Open Count	The number of instances a Bluetooth Low Energy (BLE) device connection has been established.
Last BLE Device Open Time	The timestamp indicating the last occasion a BLE device was connected.
BLE Device Close Count	A count of disconnections of a BLE device.
Last BLE Device Close Time	The timestamp of the most recent closure of a BLE device connection.
Log Rotation Count	The frequency with which the log file (`dnas_ble.log`) has been archived and a new log started.
Floor Beacon Scan Data Message Count	The total count of BLE scan data messages since the application began.
Floor Beacon Scan Data Message Rate Per Second	The average creation rate of BLE scan data messages per second.
Floor Beacon Scan Data Write Count	The total number of BLE scan data packets transmitted since the start of the application.
Floor Beacon Scan Data Write Rate Per Second	The transmission rate of BLE scan data packets per second.
Floor Beacon Scan Data Message Count Per Write	The average count of BLE scan data messages included in each write operation.
Floor Beacon Scan Data Message Avg Write Time	The average duration it takes to write a BLE scan data packet.
Floor Beacon Config Request Count	The total number of floor beacon configuration requests since the application started.
Last Floor Beacon Config Request Time	The timestamp of the most recent request for floor beacon configuration.
Floor Beacon Config Success Count	The total number of successful floor beacon configuration requests.

Metrics Name	Metrics Description
Last Floor Beacon Config Success Time	The timestamp indicating the completion of the most recent successful floor beacon configuration.
Floor Beacon Config Failure Count	The count of floor beacon configuration requests that did not succeed.
Last Floor Beacon Config Failure Time	The timestamp of the last unsuccessful floor beacon configuration request.

```
AP# tail -F /data/logs/dnas_ble_metrics.log
Wed Oct 6 17:03:49 2021 [INFO]: Application Version: 1.2.5Wed Oct  6 17:03:49 2021 [INFO]:
 Start Time: Fri Sep 17 15:54:11 2021 Up Time:
        0019D:01H:09M:38S
Wed Oct 6 17:03:49 2021 [INFO]: Total Physical Memory: 1557 MBWed Oct 6 17:03:49 2021 [INFO]:
 Physical Memory Free: 786 MBWed Oct 6 17:03:49 2021 [INFO]: Physical Memory Used: 770 MBWed
 Oct 6 17:03:49 2021 [INFO]: Total Physical Shared Memory: 170 MBWed Oct 6 17:03:49 2021
[INFO]: Total Physical Buffer Memory: 0 MBWed Oct 6 17:03:49 2021 [INFO]: Total AP Percent
 CPU Used: 1.934973Wed Oct 6 17:03:49 2021 [INFO]: Process Virtual Memory: 108696 kBWed Oct
 6 17:03:49 2021 [INFO]: Process Physical Memory: 8828 kBWed Oct 6 17:03:49 2021 [INFO]:
Process CPU Used: 0.004167Wed Oct 6 17:03:49 2021 [INFO]: gRPC Reconnect Count: 0Wed Oct 6
 17:03:49 2021 [INFO]: CAPWAP Restart Count: 1Wed Oct  6 17:03:49 2021 [INFO]: Last CAPWAP
 Restart Time: Fri Sep 17 15:54:11
       2021
Wed Oct 6 17:03:49 2021 [INFO]: BLE Device Open Count: 1Wed Oct  6 17:03:49 2021 [INFO]:
Last BLE Device Open Time: Fri Sep 17 15:54:11
        2021
Wed Oct 6 17:03:49 2021 [INFO]: BLE Device Close Count: 1Wed Oct  6 17:03:49 2021 [INFO]:
Last BLE Device Close Time: Sat Sep 18 05:48:12
        2021
Wed Oct 6 17:03:49 2021 [INFO]: Log Rotation Count: 0Wed Oct  6 17:03:49 2021 [INFO]: Floor
 Beacon Scan Data Message Count:
       10896160
Wed Oct  6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Rate Per Second:
       00
Wed Oct  6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Write Count:
       217955
Wed Oct  6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Write Rate Per Second:
       00
Wed Oct  6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Count Per Write:
       50
Wed Oct  6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Avg Write Time
         (milliseconds): 12
Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Request Count: 0Wed Oct  6 17:03:49
2021 [INFO]: Last Floor Beacon Config Request Time:
       None
Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Success Count: 0Wed Oct  6 17:03:49
2021 [INFO]: Last Floor Beacon Config Success Time:
       None
Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Failure Count: 0Wed Oct  6 17:03:49
2021 [INFO]: Last Floor Beacon Config Failure Time:
    None
```

How do I monitor BLE scans in the IoX Application?

1. To monitor the IoX Application scan log file in real-time, execute this command:

   ```
   tail -F /data/logs/dnas_ble_scans.log
   ```

2. This command will continuously display the log file's output as it updates with new scan information.
3. The IoX Application scans update every 5 minutes, but they may occur more frequently if the scan table becomes full.

Table 4: Output Descriptions

Field	Description
Profile	Beacon profile such as iBeacon, Eddystone URL, Eddystone UID, or Unknown.
MAC	MAC address of the beacon scanned.
RSSI	Last Received Signal Strength Indicator (RSSI) of the beacon detected.
Count	Number of times the beacon was heard since the last scan values were dumped.
Interval	Average interval between detections of the beacon.
Last-heard	Time elapsed since the beacon was last detected based on the latest scan values.

```
AP# tail -F /data/logs/dnas_ble_scans.log

Sat Sep 18 05:44:57 2021 [INFO]: Profile        MAC               RSSI  Count  Interval
Last-heard
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        00:00:00:00:00:0F 63    16           1S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure F1:01:AF:4E:8A:3B 55    1            0S
0000D:00H:00M:02S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Telem  F1:01:AF:4E:8A:3B 55    1            0S
0000D:00H:00M:03S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        F1:01:AF:4E:8A:3C 56    1            0S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        D1:03:15:95:D6:F3 77    1            0S
0000D:00H:00M:03S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure DF:03:AB:CD:C2:DB 86    2            3S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        DF:03:AB:CD:C2:DC 76    2            2S
0000D:00H:00M:02S
Sat Sep 18 05:44:57 2021 [INFO]: Unknown        18:04:ED:04:1C:5F 62    7            1S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure C3:05:7E:BD:25:D4 81    1            0S
0000D:00H:00M:04S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        C3:05:7E:BD:25:D5 85    3            1S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        CB:06:D8:B5:A7:97 86    1            0S
0000D:00H:00M:03S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        D8:06:04:DE:80:59 88    1            0S
0000D:00H:00M:04S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure FF:07:D0:2F:6A:AF 79    1            0S
0000D:00H:00M:02S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        FF:07:D0:2F:6A:B0 79    3            1S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: Unknown        36:08:36:6C:DA:E8 81    5            1S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure C6:09:26:9D:4D:94 73    2            2S
0000D:00H:00M:01S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        C6:09:26:9D:4D:95 73    1            0S
0000D:00H:00M:02S
Sat Sep 18 05:44:57 2021 [INFO]: iBeacon        C1:0A:21:02:A7:D8 77    3            1S
0000D:00H:00M:02S
```

```
Sat Sep 18 05:44:57 2021 [INFO]: Kontakt Secure FD:0C:9B:17:A2:22 88    1           0S
0000D:00H:00M:03S
```

What files exist in the IOx application?

The following log files are generated when the application is running and are located in the directory **/data/logs**

Table 5: Log Files

Log File Name	Description
dnas_ble_scans.log	Active log file recording data on BLE devices scanned by the application.
dnas_ble.log	Active log file for debug messages, located in the temporary directory due to its high write frequency and to utilize the partition's I/O capabilities.
dnas_ble_metrics.log	Active log file that records metric messages related to the IOx application's performance and operations.
dnas_ble_last_restart.log	When the IOx application restarts, the current dnas_ble.log file is copied to this file to help troubleshoot the cause of the restart.
dnas_ble_metrics_last_restart.log	When the IOx application restarts, dnas_ble_metrics.log is copied to this file to aid in diagnosing the reasons for the restart based on the metrics recorded before it occurred.
dnas_ble_scans_last_restart.log	When the IOx application restarts, dnas_ble_scans.log is copied to this file to aid in diagnosing the reasons for the restart based on BLE scanning activity recorded prior to the restart.
dnas_ble_scans_1.log	A rotated log file for BLE device scans. It is part of the log file management system that helps control file size by archiving older entries.
dnas_ble_metrics_1.log	Rotated log file containing historical metric messages, also part of the log rotation strategy.
dnas_ble_1.log	Rotated log file that includes debug messages for the application, ensuring older logs are archived for size management.
dnas_ble_stdout.log	Log file capturing the standard output and error streams of the IOx application, which is useful for reviewing the application's console output and any error messages.

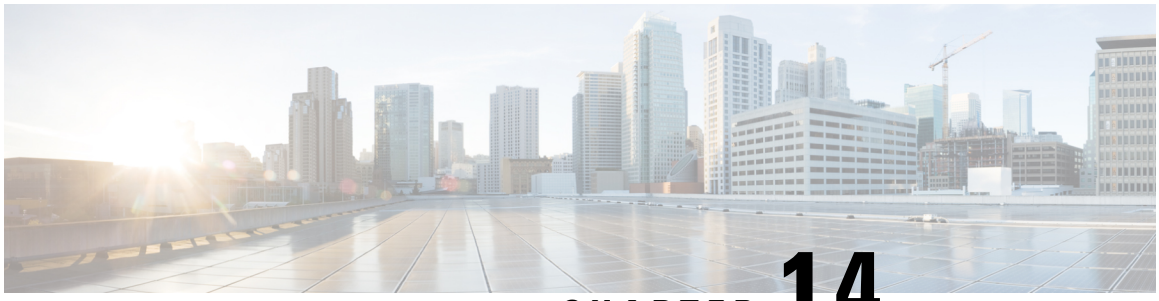
This configuration files are generated when the application is running and are located in the directory **/data/logs**

Table 6: Configuration Files

Configuration File Name	Description
dnas_ble_config.json	Configuration settings for the BLE radio; these settings are used to reload the last configuration upon restart.

This are binary files installed specifically for the IOx application. All the files are located in the directory: **/var/dnas_ble**

File Name	Description
/dnas_ble_iox_app	IOx application binary used to scan and configure floor beacons.
dnas_ble_iox_app_start.sh	Script to start the application and restart it in case of failure.



CHAPTER 14

Troubleshoot IoT services: Cisco Spaces connector

- What are the metrics available on the Connector GUI for IoT Service (Wireless) ?, on page 143
- **What are the log files created on the Connector for IoT Service (Wireless)?**, on page 144

What are the metrics available on the Connector GUI for IoT Service (Wireless) ?

You can monitor these metrics on the connector GUI for the tile for IoT Service (Wireless).

Table 7: Monitor Metrics

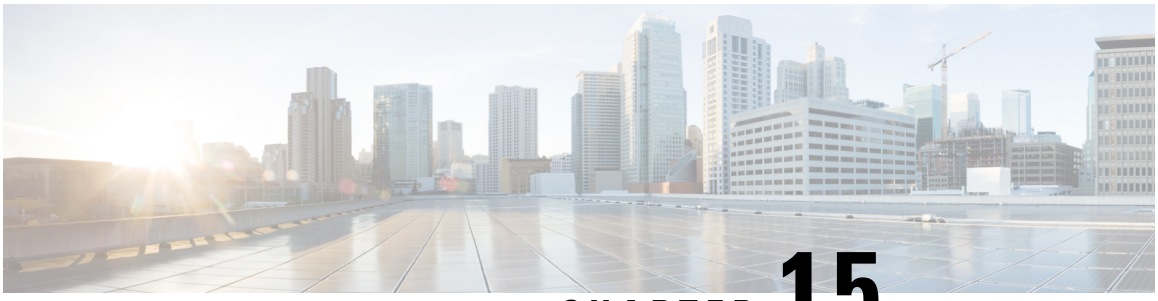
Metrics Name	Metrics Description
Mac Address	MAC address of the IoT Service (Wireless) on the connector
IP Address	IP address of the IoT Service (Wireless) on the connector
Log Level	Logging level set for the IoT Service (Wireless)
Incoming gRPC rate	The number of gRPC Remote Procedure Calls (gRPC) events the connector receives each second.
Incoming TDL rate	The number of TDL (Telemetry Definition Language) events the connector receives each second.
Incoming TDL failed rate	The number of TDL events per second that fail to be processed by the connector.
Last five minutes Incoming gRPC rate	The average rate of incoming gRPC events for the past five minutes.
Last five minutes TDL rate	The average rate of incoming TDL events for the past five minutes.
Last five minutes TDL failed rate	The average rate of incoming TDL events that failed in the last five minutes.
Active gRPC connection count	The current count of active gRPC connections to the connector.

What are the log files created on the Connector for IoT Service (Wireless)?

These log files are located in the directory /opt/spaces-connector/runtime/logs/iot-services/.

Table 8: Log Files

Log File Name	Description
apgrpcchannel.log	Active log file recording data on BLE devices scanned by the application.
apgrpcchannel.log	This log file records the connection status of the Access Point's gRPC (gRPC Remote Procedure Calls) channel.
boot.log	This log file contains boot information such as CPU and memory details.
control-channel.log	This log file monitors the status of the control channel connection.
dnas_iox_app_manage.log	This log file pertains to the management of the IoX Application environment, including installation, uninstallation, and technical support actions.
filter.log	This log file is related to the filter configuration activities.
heartbeat.log	This log file captures heartbeat messages sent to the service manager.
highavailability.log	This log file details the status of high availability features.
metrics.log	This log file contains metric data formatted in JavaScript Object Notation (JSON).
netconf-service/server.log	This log file records operations related to Network Configuration Protocol (NETCONF).
nginx-access.log	This log file captures access records for NGINX.
nginx-error.log	This log file documents error messages related to NGINX.
server.log	This log file includes general messages and information.
status.log	This log file provides updates on the status of the system or service.



CHAPTER 15

Troubleshoot IoT services: access point

- How do I check the gRPC connection status on the access point?, on page 145
- How do I check the stream token on the access point?, on page 145
- How do I view the gRPC server logs on the access point?, on page 146
- How do I view the beacons scanned by an access point running in Native mode?, on page 147
- How do I view the beacon broadcast setting for an access point running in Native mode?, on page 147

How do I check the gRPC connection status on the access point?

Run the command: **show cloud connector connection detail**

This command returns information about the connection. ***Connection State*** should be READY. ***Connection Url*** should be the IP address of the Cisco Spaces: Connector on port 8000. ***Certificate Available*** should be true. ***Controller Ip*** should be the controller the AP is associated with.

```
AP# show cloud connector connection detail
Connection State           : READY
Connection Url             :  10.22.243.33:8000
Certificate Available      :  true
Controller Ip              :  10.22.243.31
Stream Setup Interval      :  30
Keepalive Interval         :  30
Last Keepalive Rcvd On     :  2020-04-01 00:32:47.891433113 +0000 UTC m=+345985.338898246
Number of Dials               :  2
Number of Tx Pkts             :  2788175
Number of Rx Pkts             :  11341
Number of Dropped Pkts        :  0
Number of Rx Keepalive        :  11341
Number of Tx Keepalive        :  11341
Number of Rx Cfg Request      :  0
Number of Tx AP Cfg Resp      :  0
Number of Tx APP Cfg Resp     :  0
Number of Tx APP state pkts   :  5
Number of Tx APP data pkts    :  2776829
```

How do I check the stream token on the access point?

Run the command: **show cloud connector key access**

This command returns information about the stream token. ***Token Valid*** should be Yes. The ***Last Success on*** time should be more recent than the ***Last Failure on*** time. If there are failures, the ***Last Failure reason*** field details the reason for the failure.

```
AP# show cloud connector key access
Token Valid : Yes
Token Stats :
        Number of Attempts  : 44
        Number of Failures  : 27
        Last Failure on     : 2020-03-28 02:02:15.649556818 +0000 UTC m=+5753.097022576
        Last Failure reason : curl: SSL connect error
        Last Success on     : 2020-04-01 00:48:37.313511596 +0000 UTC m=+346934.760976625
        Expiration time     : 2020-04-02 00:48:37 +0000 UTC
Connection Retry Interval : 30
```

Also run the command: **show cloud connector key authentication**.

This command returns the authentication token used initially to set up the connection. ***Token Valid*** should be Yes. ***Token Endpoint*** should be the IP address of the Cisco Spaces connector on port 8000. ***Token Content*** should be the token set on the wireless controller using this configuration command: **ap cisco-dna token 0** *token-content*.

```
AP# show cloud connector key authentication
Token Valid    : Yes
Token Endpoint : 10.22.243.33:8000
Token Content  :
----------------------------------------
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
0aWQiOjEwMTM3LCJjaWQiOjExNTM5MzM4MDQ5NDM
3MzM2MDAwLCJlcCI6IjEwLjIyLjI0My4zMzo4MDA
wIiwiaWF0IjoxNTg1MzYwNzk5fQ.tj0LQDzXorHz
30Q_ffRWWY6Ege3xyF_tgQOmVFBkG3k
----------------------------------------
```

How do I view the gRPC server logs on the access point?

Run the command: **show grpc server log**

```
AP# show grpc server log
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces conn url 10.22.243.33:8000"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] launching token request cycle"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02
 01:36:52 +0000 UTC"
time="2020-04-01T01:36:52Z" level=info msg=" Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping
for 10 seconds"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX  routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "
```

How do I view the beacons scanned by an access point running in Native mode?

Run the command: **show controllers ioTRadio ble 0 scan brief**

```
<access-point># show controllers ioTRadio ble 0 scan brief

      Profile               MAC  RSSI(-dBm)  RSSI@1meter(-dBm)        Last-heard
      Unknown 3C:1D:AF:62:EC:EC          88                 0 0000D:00H:00M:01S
      iBeacon 18:04:ED:04:1C:5F          86                65 0000D:00H:00M:01S
      Unknown 18:04:ED:04:1C:5F          78                65 0000D:00H:00M:01S
      Unknown 04:45:E5:28:8E:E7          85                65 0000D:00H:00M:01S
      Unknown 2D:97:FA:0F:92:9A          91                65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          68                65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          45               256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          45               256 0000D:00H:00M:01S
              04:EE:03:53:6A:3A          72               N/A 0000D:00H:00M:01S
      Unknown 04:EE:03:53:6A:3A          72                65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          67                65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          60               256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          60               256 0000D:00H:00M:01S
Eddystone URL 04:EE:03:53:6A:3A          72               N/A 0000D:00H:00M:01S
```

How do I view the beacon broadcast setting for an access point running in Native mode?

Run the command: **show controllers ioTRadio ble 0 broadcast**

This is an example of two *iBeacons* configured in the v-iBeacon profile. Beacon 1 has ***UUID***: 11111111-1111-1111-1111-111111111111 ***Major***: 22222***Minor***: 33 ***Transmit Power***: -21 and ***Advertisement Power***: -60 ***Interval***: 100. Beacon 1 has ***UUID***: 22222222-2222-2222-2222-222222222222 ***Major***: 3333 ***Minor***: 44 ***Transmit Power***: -21 and ***Advertisement Power***: -65 ***Interval***: 100.

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
------------------
Active profile           : v-iBeacon
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 0000000000005446089c
Instance-ID (hex)        : 7f0000001f00

Profile 2 (Eddystone URL)
URL                      : http://www.
```

```
Profile 3 (v-iBeacon)
v-iBeacon status         : Chirping
Chirping interval (ms)   : 100
Profile 4 (Custom Profile)
Adv Data                 :
0000001800000000000000ecb255ad550000000c0000000000000000000000
Scan Data                :
00000000ae0100000000000005446089c7f000000190000000000000004cb5
Simulator mode           : Disabled
Beacon-ID               Mac                                UUID Major Minor Status
        1 C0:64:E4:23:7F:2F 11111111111111111111111111111111 22222    33      1
        2 C0:64:E4:23:7F:2E 22222222222222222222222222222222 33333    44      1
        3 C0:64:E4:23:7F:2D 00000000000000000000000000000000     0     0      0
        4 C0:64:E4:23:7F:2C 00000000000000000000000000000000     0     0      0
        5 C0:64:E4:23:7F:2B 00000000000000000000000000000000     0     0      0

Beacon-ID Transmit power(dBm) Advertised power(dBm)
        1                -21                   -60
        2                -21                   -65
        3                -21                   -65
        4                -21                   -65
        5                -21                   -65
```

This is an example of *Eddystone UID* profile. Beacon has ***Namespace***: 44444444444444444444 ***Instance-ID***: 555555555555 ***Transmit Power***: -21and ***Advertisement Power***: -65 ***Interval***: 100.

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
------------------
Active profile           : Eddystone UID
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 44444444444444444444
Instance-ID (hex)        : 555555555555

Profile 2 (Eddystone URL)
URL                      : http://www.

Profile 3 (v-iBeacon)
v-iBeacon status         : Chirping
Chirping interval (ms)   : 100
Profile 4 (Custom Profile)
Adv Data                 :
0000001800000000000000ecb255ad550000000c0000000000000000000000
Scan Data                :
00000000ae0100000000000005446089c7f000000190000000000000004cb5
Simulator mode           : Disabled
Beacon-ID               Mac                                UUID Major Minor Status
        1 C0:64:E4:23:7F:2F 11111111111111111111111111111111 22222    33      1
        2 C0:64:E4:23:7F:2E 22222222222222222222222222222222  3333    44      1
        3 C0:64:E4:23:7F:2D 00000000000000000000000000000000     0     0      0
        4 C0:64:E4:23:7F:2C 00000000000000000000000000000000     0     0      0
        5 C0:64:E4:23:7F:2B 00000000000000000000000000000000     0     0      0
```

```
Beacon-ID Transmit power(dBm) Advertised power(dBm)
        1                -21                   -60
        2                -21                   -65
        3                -21                   -65
        4                -21                   -65
        5                -21                   -65
```

This is an example of *Eddystone URL* profile. Beacon has ***URL***: http://www.cisco.com/ ***Transmit Power***: -21 and ***Advertisement Power***: -65 ***Interval***: 100.

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
------------------
Active profile           : Eddystone URL
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 44444444444444444444
Instance-ID (hex)        : 555555555555

Profile 2 (Eddystone URL)
URL                      : http://www.cisco.com/

Profile 3 (v-iBeacon)
v-iBeacon status         : Chirping
Chirping interval (ms)   : 100
Profile 4 (Custom Profile)
Adv Data                 :
0000001800000000000000ecb255ad550000000c00000000000000000000
Scan Data                :
00000000ae01000000000000005446089c7f000000190000000000000004cb5
Simulator mode           : Disabled
Beacon-ID              Mac                                 UUID Major Minor Status
        1 C0:64:E4:23:7F:2F 11111111111111111111111111111111 22222    33      1
        2 C0:64:E4:23:7F:2E 22222222222222222222222222222222  3333    44      1
        3 C0:64:E4:23:7F:2D 00000000000000000000000000000000     0     0      0
        4 C0:64:E4:23:7F:2C 00000000000000000000000000000000     0     0      0
        5 C0:64:E4:23:7F:2B 00000000000000000000000000000000     0     0      0

Beacon-ID Transmit power(dBm) Advertised power(dBm)
        1                -21                   -60
        2                -21                   -65
        3                -21                   -65
        4                -21                   -65
        5                -21                   -65
```

How do I view the beacon broadcast setting for an access point running in Native mode?



PART VII

Appendix

- Cisco Catalyst 9800 Series Wireless Controller, on page 153



CHAPTER 16

Cisco Catalyst 9800 Series Wireless Controller

- Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower), on page 153
- Disable Assurance with iCAP using CLI (Versions 17.3.1 or lower), on page 154
- Disable iCAP using WEBUI (Versions 17.3.2 or higher), on page 155
- Disable iCAP using CLI (Versions 17.3.2 or higher), on page 156
- Enable or Disable iCAP or Assurance using DNAC (Versions 17.3.2 or higher), on page 157

Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower)

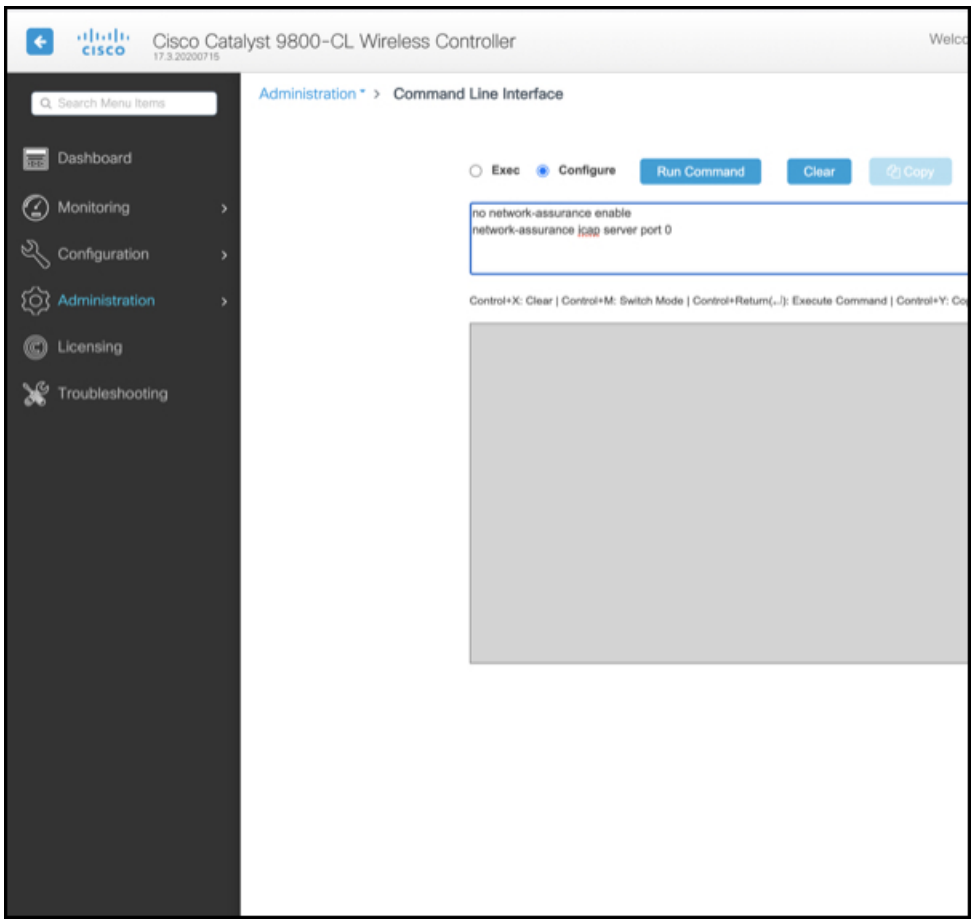
This task is applicable only for Cisco Catalyst 9800 Series Wireless Controller versions 17.3.1 or lower.

Disable Assurance with Intelligent Capture (iCAP) in order to enable IoT Service. With the wireless controller WebUI, you can issue CLI commands to disable assurance and iCAP.

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Series Wireless Controller GUI and navigate to **Administration > Command Line Interface.** Click Configure and enter the **no network-assurance enable** command and the **network-assurance icap server port 0** command.

Figure 110: Entering the commands to enable BLE



Step 2 Click **Run Command**.
If the command runs successfully, you can see a success message displayed.

What to do next

Assurance and iCAP are now disabled. You can add this Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces. If the Cisco Catalyst 9800 Series Wireless Controller was previously added to Catalyst Center (version 2.2 and above), the Catalyst Center can automatically categorize this device as a noncompliant device. No further action is thus required to make the Cisco Catalyst 9800 Series Wireless Controller work on Cisco Spaces.

Disable Assurance with iCAP using CLI (Versions 17.3.1 or lower)

This task is applicable only for Cisco Catalyst 9800 Series Wireless Controller versions 17.3.1 or lower.

This task uses the CLI to disable assurance including internet Content Adaptation Protocol (iCAP). Login to the Cisco Catalyst 9800 Series Wireless Controller CLI and enter the following commands.

SUMMARY STEPS

1. configure terminal
2. no network-assurance enable
3. network-assurance icap server port 0
4. end

DETAILED STEPS

Procedure

Step 1 configure terminal

Step 2 no network-assurance enable

Step 3 network-assurance icap server port 0

Step 4 end

What to do next

Assurance and iCAP are now disabled. You can add this Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces. If the Cisco Catalyst 9800 Series Wireless Controller was previously added to Catalyst Center (version 2.2 and above), the Catalyst Center can automatically categorize this device as a noncompliant device. No further action is thus required to make the Cisco Catalyst 9800 Series Wireless Controller work on Cisco Spaces.

Disable iCAP using WEBUI (Versions 17.3.2 or higher)

This task is applicable only for Cisco Catalyst 9800 Series Wireless Controller versions 17.3.2 or higher.

Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Amsterdam 17.3.x supports only one of the following:

- IoT service (wireless) with Cisco Spaces.
- Network Assurance solution on Catalyst Center using Intelligent Capture (iCAP)

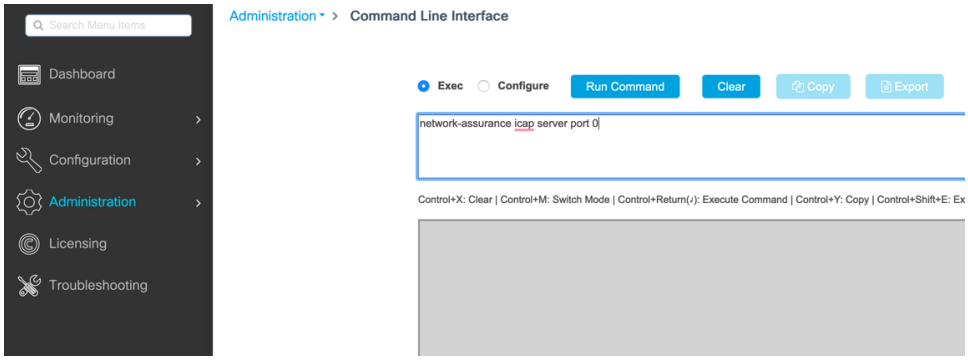
IoT service (wireless) and Intelligent Capture (iCAP) can co-exist from Cisco IOS XE Cupertino 17.7.x or higher.

Disable Intelligent Capture (iCAP) in order to enable IoT service (wireless). With the wireless controller GUI, you can issue CLI commands to disable iCAP.

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Series Wireless Controller WebUI and navigate to **Administration > Command Line Interface.** Click Configure and enter the **network-assurance icap server port 0** command.

Figure 111: Entering the commands to enable IoT Service



Step 2 Click **Run Command**.
If the command runs successfully, you can see a success message displayed.

What to do next

Intelligent Capture (iCAP) feature is now disabled. You can now add this Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces

If this wireless controller was previously added to Catalyst Center (version 2.2 and above), Catalyst Center now categorizes this device as a noncompliant device allowing Cisco Spaces to push the necessary configurations to the device. No further action is thus required to make the wireless controller work on Cisco Spaces.

Disable iCAP using CLI (Versions 17.3.2 or higher)

This task uses the CLI to disable Intelligent Capture (iCAP). Login to the Cisco Catalyst 9800 Series Wireless Controller CLI and enter the following commands.

This task is applicable only for Cisco Catalyst 9800 Series Wireless Controller versions 17.3.2 or higher.

Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Amsterdam 17.3.x supports only one of the following:

- IoT service (wireless) with Cisco Spaces.
- Network Assurance solution on Catalyst Center using Intelligent Capture (iCAP)

SUMMARY STEPS

1. configure terminal

2. network-assurance icap server port 0
3. end

DETAILED STEPS

Procedure

Step 1 configure terminal
Step 2 network-assurance icap server port 0
Step 3 end

What to do next

Intelligent Capture (iCAP) feature is now disabled. You can now add this Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces

If this wireless controller was previously added to Catalyst Center (version 2.2 and above), Catalyst Center now categorizes this device as a noncompliant device allowing Cisco Spaces to push the necessary configurations to the device. No further action is thus required to make the wireless controller work on Cisco Spaces.

Enable or Disable iCAP or Assurance using DNAC (Versions 17.3.2 or higher)

This task shows you how you can disable or enable the network-assurance or iCAP feature using the Catalyst Center templates.

Procedure

Step 1 From the Catalyst Center dashboard, use the template editor to create a template with the required configuration. Specify the template name, description, software type, and device type.
Step 2 Save and commit the template.
Step 3 Add the template to the respective site.
Step 4 Select the device from the site and provision the device.
Step 5 In **Advanced Configuration**, select the template and apply to the device.