Cisco Spaces: IoT Services Configuration Guide (Wireless)

First Published: 2020-08-31

Last Modified: 2022-11-03

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

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

PART I

Overview

CHAPTER 1

Overview

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

Overview of Cisco Spaces: IoT Services (Wireless)

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

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

Using IoT Services, you can perform the following management activities:

- Deploy BLE gateways on supported APs in your network.
- Claim BLE beacons that you acquired from Cisco Spaces: IoT Device Marketplace.
- Configure APs and manage floor beacons.
- You can monitor device attributes such as location, telemetry, battery status, and movement status.

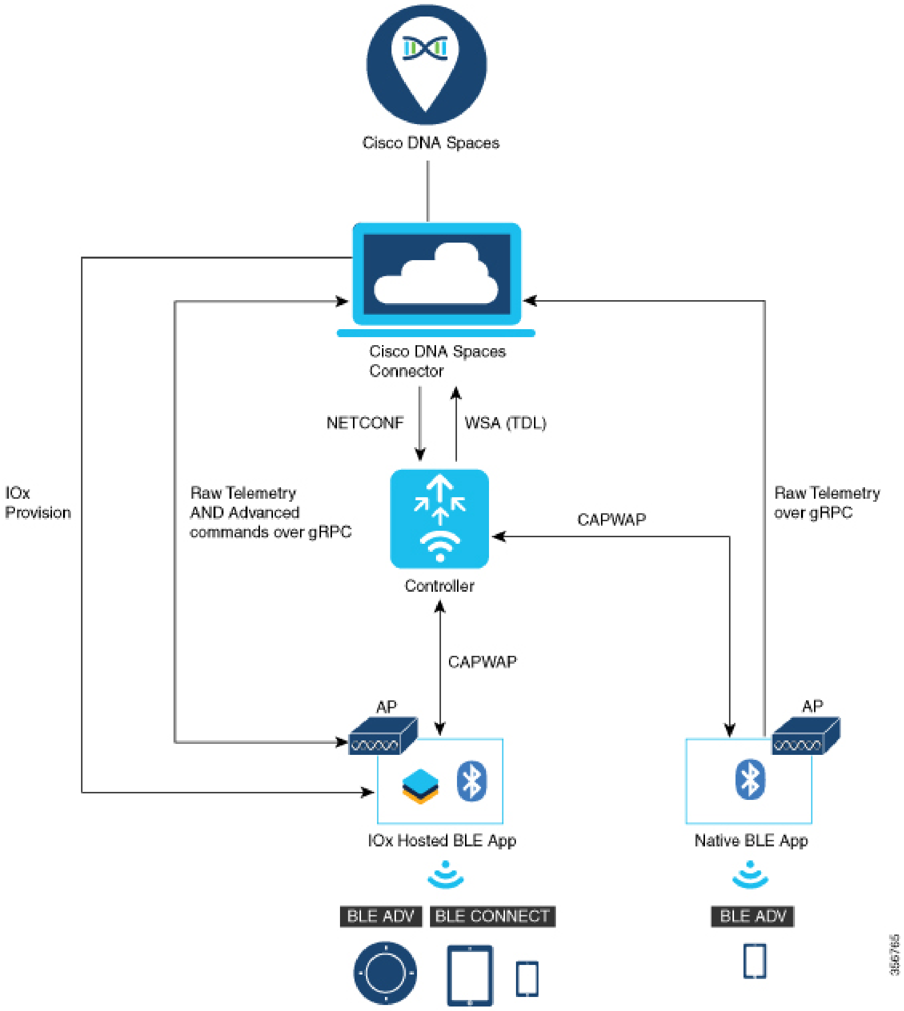
Components of Cisco Spaces: IoT Services

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

The Cisco Catalyst 9100 Series Family of Access Points acts as a gateway of communication between Cisco Spaces and the Internet of Things (IoT) devices. Cisco Spaces: IoT Services can then use a range of common

APIs to communicate with edge devices and apps. The Cisco Spaces: IoT Services collects data from devices and apps, and passes it to Cisco-partnered Device Manager websites. The Device Manager websites can leverage these edge-device signals and make the outcome specialized and targeted for each industry.

Figure 1: Components of IoT Services



Access Points

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

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

- **Base BLE Gateway**: The Base BLE gateway is a type of AP that you can configure in one of two modes. Either the **Transmit** mode or the **Scan** mode.

  In the **Transmit** 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 Cisco Spaces: Connector dashboard decodes and displays this information.

- **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 Cisco Spaces: Connector website.

  You can configure this AP in the **Scan** mode and the **Transmit** mode.

  In the **Transmit** 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 Cisco Spaces: Connector dashboard decodes and displays this information.

Cisco Catalyst 9800 Series Wireless Controllers

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

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

The 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 controller to Cisco Spaces through TDL telemetry streaming. The gRPC configuration from Cisco Spaces also goes through the controller and from there to the access point. The configuration sets up the gRPC channel between the AP and Cisco Spaces. The AP sends gRPC channel statistics to the controller where you can view the statistics.

Note

- You can have only one gRPC session between an AP and the Connector.
- Cisco Catalyst 9800 Series Wireless Controller running the Cisco IOS XE Amsterdam 17.3.x release now supports the IoT Services along with the Network Assurance solution on Cisco DNA Center.

  However, Cisco IOS XE Cupertino 17.7.x or earlier, IoT Services and Intellegent Capture (iCAP) feature are mutually exclusive. That is, if iCAP feature needs to be enabled on the device, then IoT Services cannot be deployed. Similarly, if IoT Services needs to be enabled on the device, then iCAP feature cannot be deployed.

Cisco Spaces: IoT Device Marketplace

Cisco Spaces: IoT Device Marketplace is a platform where you can discover, research, and purchase Internet of Things (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 devices are compatible with 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 Wireless Controller.

Access points connect to the Connector using the gRPC framework.

The APs establish a connection to the Connector using the gRPC protocol. gRPC protocol configures floor beacons and receive 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. The Connector can thus support many simultaneous connections.

CHAPTER 2

Prerequisites

Prerequisites of Cisco Spaces: IoT Services (Wireless)

The following prerequisites can get you started with Cisco Spaces: IoT Services.

- Install Cisco Spaces: Connector in your network.
- Install a Cisco Catalyst 9800 Series Wireless Controller with a Cisco IOS XE Amsterdam 17.3.x image.
- Deploy supported access points in your network (See Compatibility Matrix section).
- Ensure Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Cisco DNA Center.
- If the Cisco Spaces: Connector is deployed as an AWS instance using AMI, ensure that the controller and the Connector are in the same virtual private cloud (VPC). Ensure that the controller has a private IP address so that the security group of the Connector does not block the traffic allowing enabled IOT streams to function.
- Permit all TCP traffic at the VPC level so that the TDL is established without any issues.
- Before adding a Cisco Catalyst 9800 Series Wireless Controller to a Connector, run the following commands on the controller:
  - **aaa new-model**
  - **aaa authentication login default local**
  - **aaa authorization exec default local**

  These commands disable the connection services to Cisco Spaces.
- Cisco Spaces: IoT Services and Intellegent Capture (iCAP) feature can now co-exist from controller version Cisco Catalyst 9800 Series Wireless Controller Cisco IOS XE Cupertino 17.7.x release or later. For versions earlier than Cisco IOS XE Cupertino 17.7.x, disable iCAP if enabled on the controller.
- Perform NTP synchronization over controllers, Connectors, and access points (APs) in the network.
- If a USB BLE module is inserted in an AP, reboot the access point.

- NETCONF must be enabled on Cisco Catalyst 9800 Series Wireless Controller on port 830, along with permission to use NETCONF.
- The application (App) installed and running over the access pont (AP) uses the default 17.17.0.0/16 subnet. So using this subnet for other purposes can create network issues.
- IPv6 is not supported on Cisco Spaces: Connector.

Compatibility Matrix for IoT Services (Wireless)

Application Name	Support for Cisco Spaces: IoT Services
Supported Wireless controllers controller	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later • Not supported on Cisco Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Catalyst Access Points (Cisco EWC-AP)
Cisco Spaces: Connector Docker	2.0.455 and later.
Cisco Spaces: Connector OVA	2.3 and later.
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1 and later.
Cisco DNA Center (for map import)	Cisco DNA Center Release 2.1.1 and later.
Access Points for advanced BLE gateway (Wi-Fi 6)	• Cisco Aironet 9105 Series Access Points • Cisco Aironet 9115 Series Access Points • Cisco Aironet 9117 Series Access Points • Cisco Aironet 9120 Series Access Points • Cisco Aironet 9130 Series Access Points • Cisco Aironet 4800 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)
IOX Application Version	1.0.46 and above **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

Application Name	Support for Cisco Spaces: IoT Services
Kontakt firmware version	• 6.1 • Newer beacon models running version 1.1 and above

IoT Services is not supported on the following:

- Directly connected and CMX tethering Connectors.

The following table lists the compatibility of the IOX-hosted BLE App and the Native BLE App with various AP modes. This is not compatible with Cisco Embedded Wireless Controller on Catalyst Access Points (Cisco EWC-AP)

Table 1: AP Modes and Apps

AP Modes	IOX-hosted BLE App	Native BLE App
PI: Local	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported
P1: Flex	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported
P2: Fabric	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported
P3: Mesh	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported

CHAPTER 3

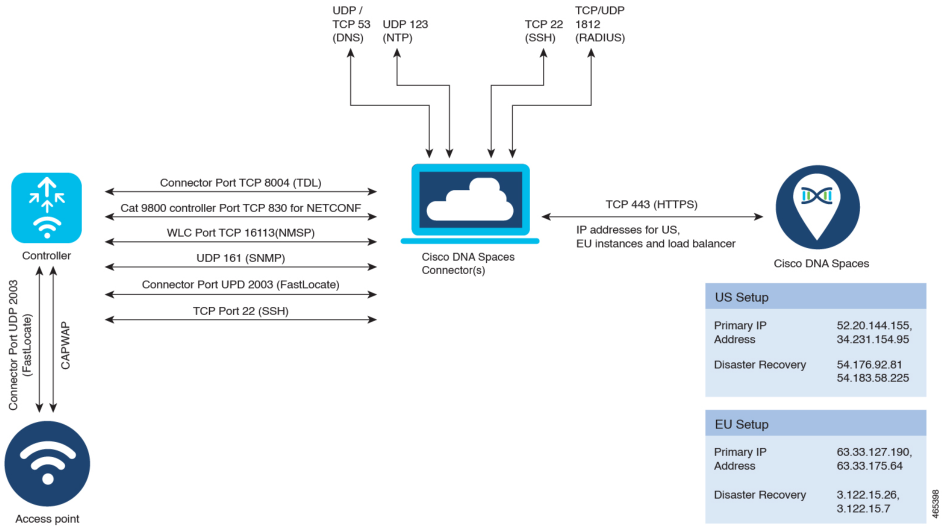
Open Ports

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.

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

Figure 2: Basic Functionality



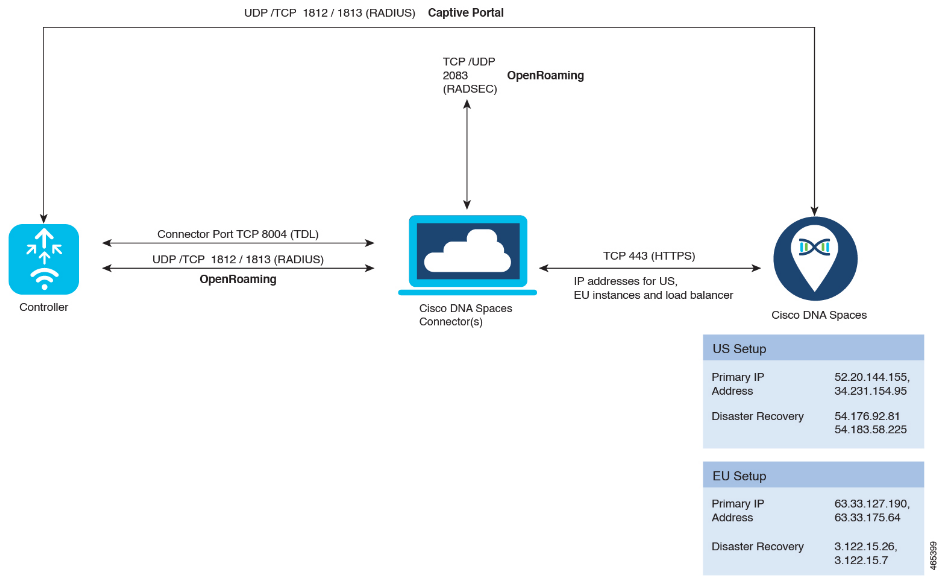
UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
Connector Port TCP 8004 (TDL)
Cat 9800 controller Port TCP 830 for NETCONF
WLC Port TCP 16113(NMSP)
UDP 161 (SNMP)
Connector Port UPD 2003 (FastLocate)
TCP Port 22 (SSH)
Controller
Connector Port UDP 2003 (FastLocate)
CAPWAP
Access point
Cisco DNA Spaces Connector(s)
TCP 443 (HTTPS)
IP addresses for US, EU instances and load balancer
Cisco DNA Spaces
465398

US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

EU Setup	
Primary IP Address	63.33.127.190, 63.33.175.64
Disaster Recovery	3.122.15.26, 3.122.15.7

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

Figure 3: Guest Onboarding

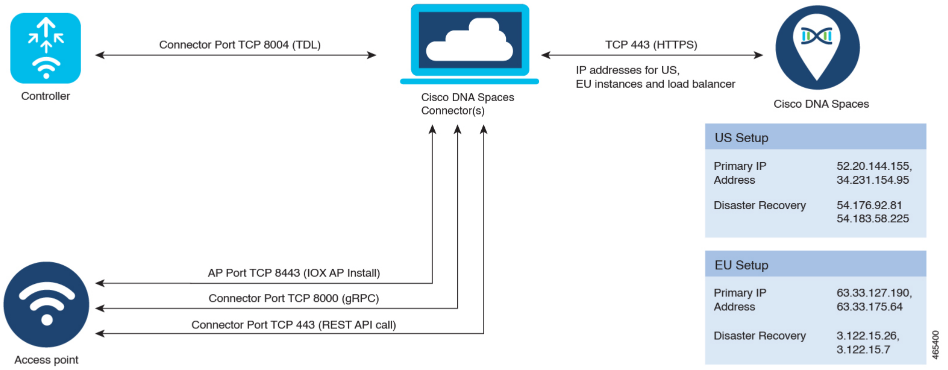


US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

EU Setup	
Primary IP Address	63.33.127.190, 63.33.175.64
Disaster Recovery	3.122.15.26, 3.122.15.7

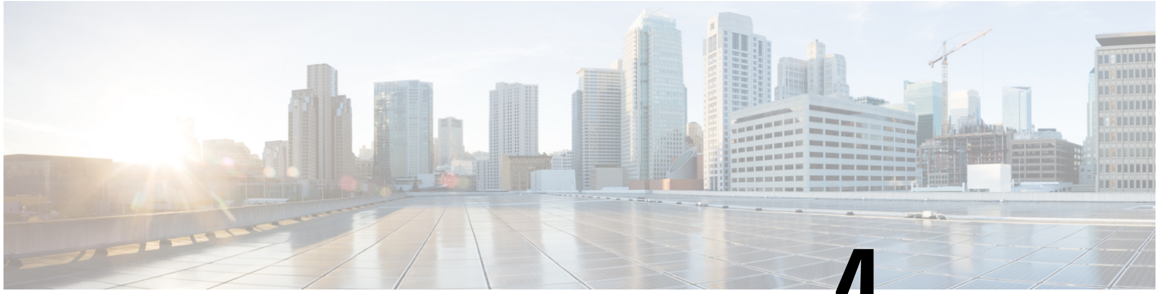
The following ports need to be opened for configuring IoT Services (wireless). To configure IoT Services (wired), see Open Ports (Wired)

Figure 4: IoT Services


Connector Port TCP 8004 (TDL)
Controller
Cisco DNA Spaces
Connector(s)
TCP 443 (HTTPS)
IP addresses for US,
EU instances and load balancer
Cisco DNA Spaces
AP Port TCP 8443 (IOX AP Install)
Connector Port TCP 8000 (gRPC)
Connector Port TCP 443 (REST API call)
Access point
465400

US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

EU Setup	
Primary IP Address	63.33.127.190, 63.33.175.64
Disaster Recovery	3.122.15.26, 3.122.15.7



CHAPTER 4

Getting Started

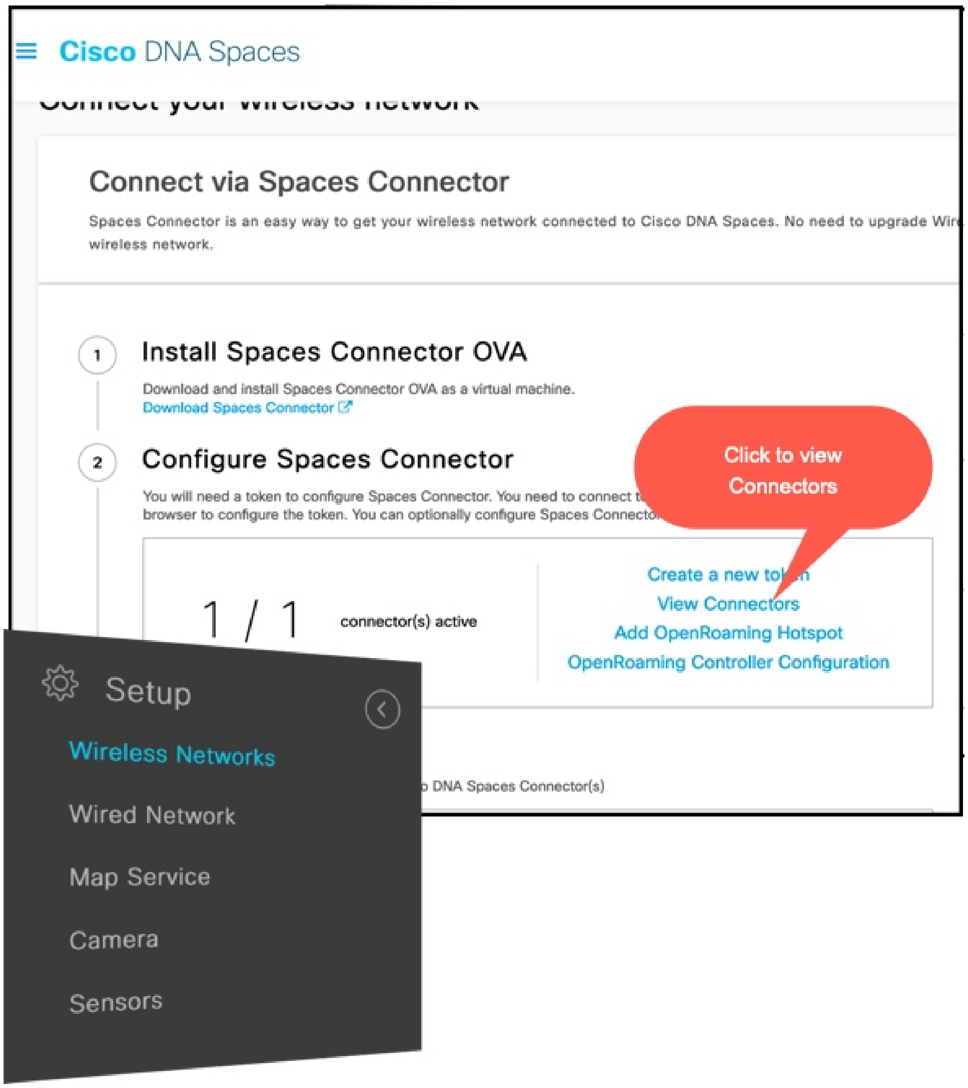
Verify Cisco Spaces: Connector is added and active

This task helps you verify if a Cisco Spaces: Connector is deployed and active. This is a necessary prerequisite for Cisco Spaces: IoT Services

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

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

Figure 5: View Connectors



Cisco DNA Spaces

Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wir
wireless network.

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect t
browser to configure the token. You can optionally configure Spaces Connecto

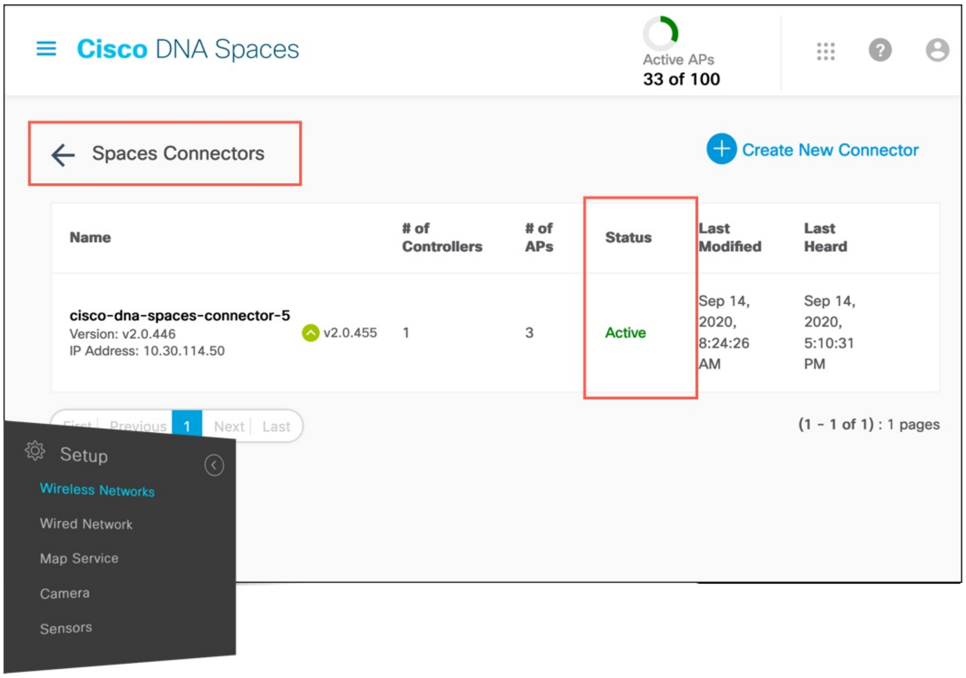
1 / 1 connector(s) active

Create a new token
View Connectors
Add OpenRoaming Hotspot
OpenRoaming Controller Configuration

DNA Spaces Connector(s)

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

Figure 6: Active Connector



Name	# of Controllers	# of APs	Status	Last Modified	Last Heard
cisco-dna-spaces-connector-5 Version: v2.0.446 IP Address: 10.30.114.50 v2.0.455	1	3	Active	Sep 14, 2020, 8:24:26 AM	Sep 14, 2020, 5:10:31 PM

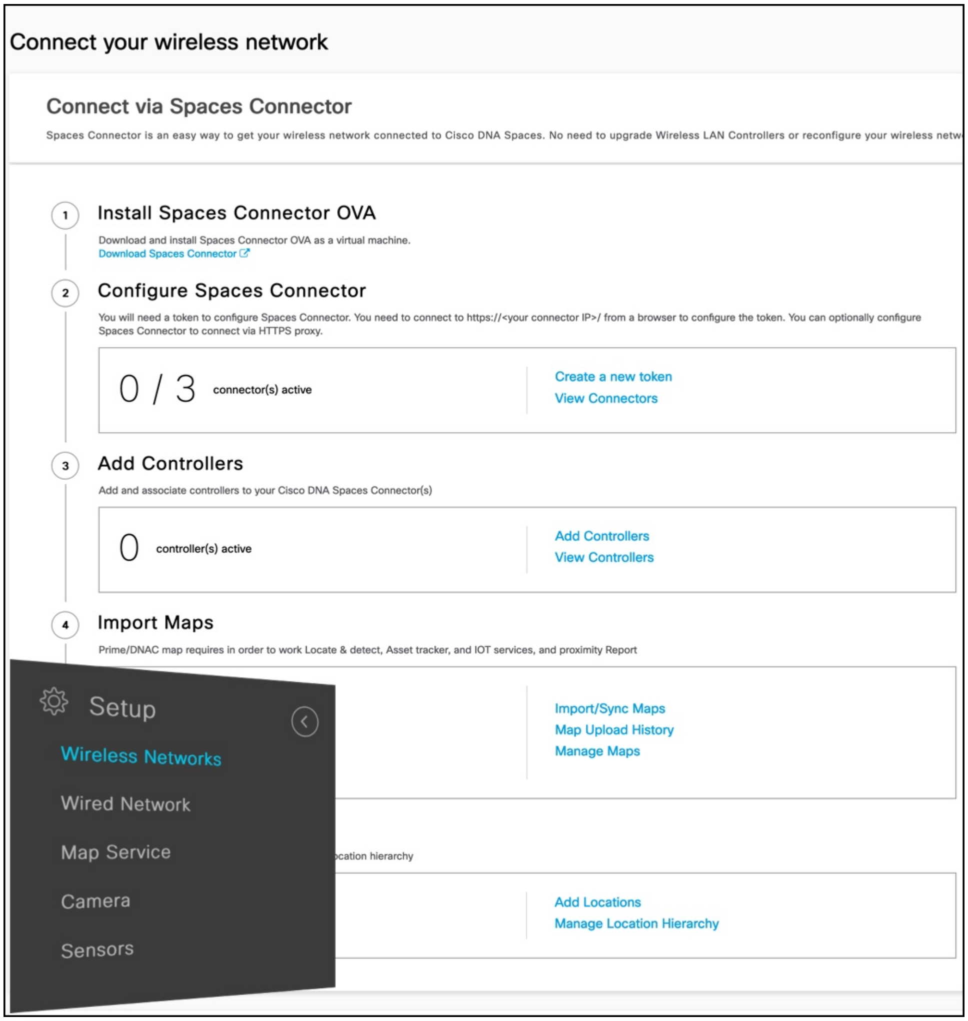
Verify Cisco Catalyst 9800 Series Wireless Controllers is added and active

This task helps you verify if a Cisco Catalyst 9800 Series Wireless Controllers is deployed and active. This is a necessary prerequisite for Cisco Spaces: IoT Services

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

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

Figure 7: View Controllers



Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless netw

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 3 connector(s) active

Create a new token
View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 controller(s) active

Add Controllers
View Controllers

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

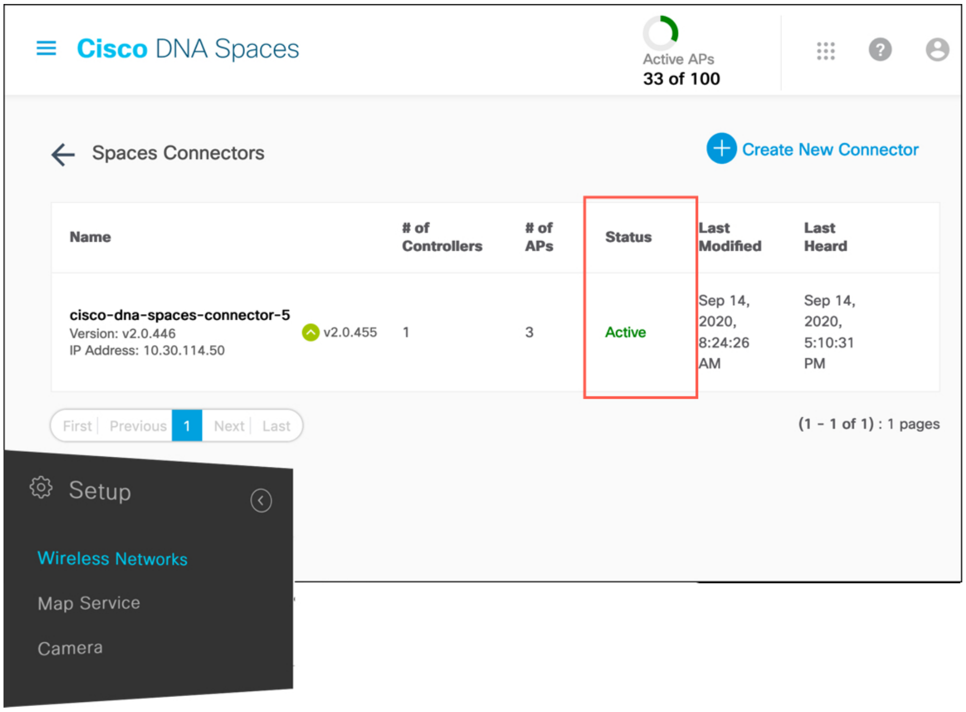
Import/Sync Maps
Map Upload History
Manage Maps

ocation hierarchy

Add Locations
Manage Location Hierarchy

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

Figure 8: Active Controller



Name	# of Controllers	# of APs	Status	Last Modified	Last Heard
cisco-dna-spaces-connector-5 Version: v2.0.446 IP Address: 10.30.114.50 v2.0.455	1	3	Active	Sep 14, 2020, 8:24:26 AM	Sep 14, 2020, 5:10:31 PM

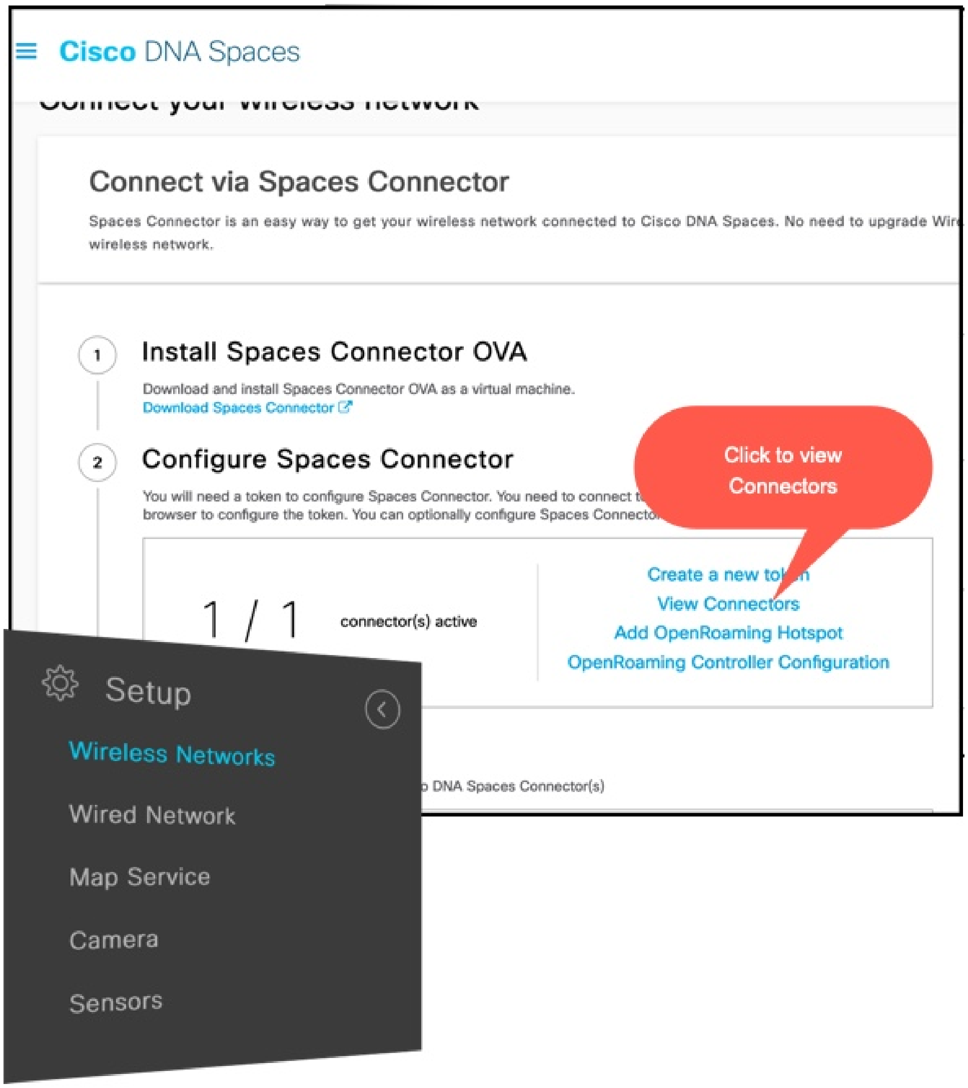
Enable IoT Manage Streams

This task helps you enable IoT streams so that your access points are visible on Cisco Spaces: IoT Services. This is a necessary step for Cisco Spaces: IoT Services

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

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

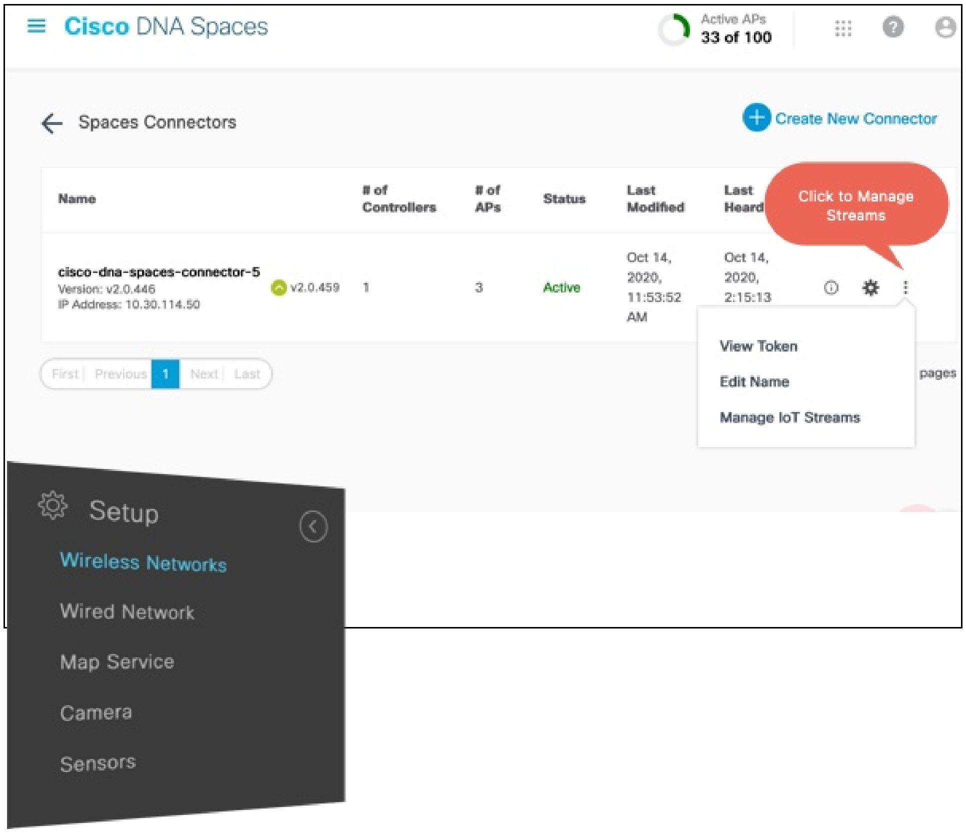
Figure 9: View Connectors



Cisco DNA Spaces
Connect your wireless network
Connect via Spaces Connector
Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wir
wireless network.
1 Install Spaces Connector OVA
Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector
2 Configure Spaces Connector
You will need a token to configure Spaces Connector. You need to connect t
browser to configure the token. You can optionally configure Spaces Connecto
1 / 1 connector(s) active
Create a new token
View Connectors
Add OpenRoaming Hotspot
OpenRoaming Controller Configuration
Click to view Connectors
DNA Spaces Connector(s)
Setup
Wireless Networks
Wired Network
Map Service
Camera
Sensors

Step 3 Click the three-dot icon of an active Connector to display a menu. Choose **Manage IoT Streams**.

Figure 10: Manage IoT Streams



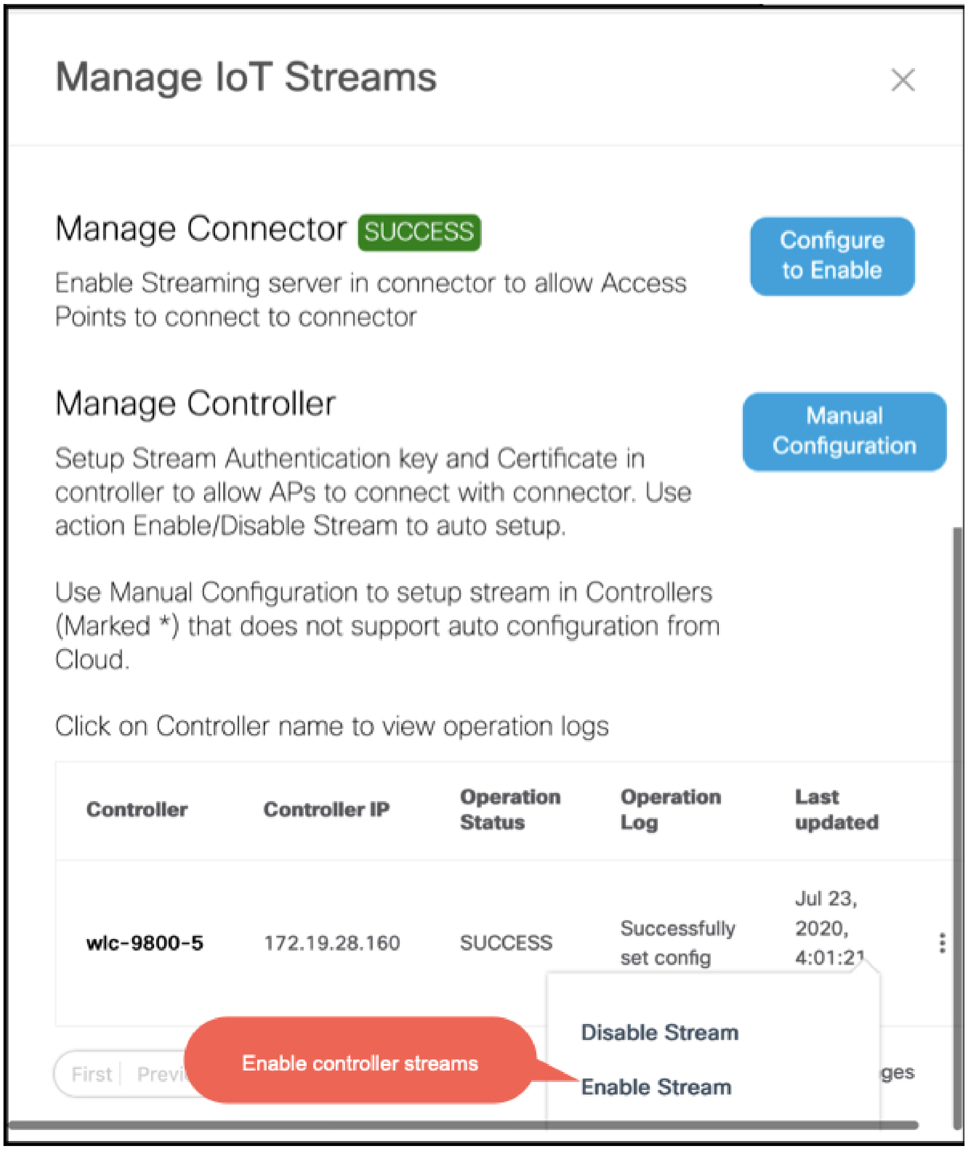
Name		# of Controllers	# of APs	Status	Last Modified	Last Heard
cisco-dna-spaces-connector-5 Version: v2.0.446 IP Address: 10.30.114.50	v2.0.459	1	3	Active	Oct 14, 2020, 11:53:52 AM	Oct 14, 2020, 2:15:13

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

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

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

Figure 11: Enabling IoT Streams for the Connector and for each associated controller



Manage IoT Streams

Manage Connector SUCCESS

Enable Streaming server in connector to allow Access Points to connect to connector

Manage Controller

Setup Stream Authentication key and Certificate in controller to allow APs to connect with connector. Use action Enable/Disable Stream to auto setup.

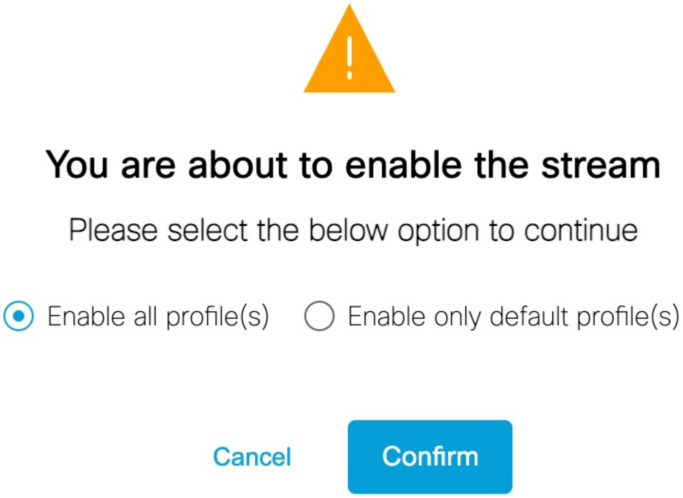
Use Manual Configuration to setup stream in Controllers (Marked *) that does not support auto configuration from Cloud.

Click on Controller name to view operation logs

Controller	Controller IP	Operation Status	Operation Log	Last updated
wlc-9800-5	172.19.28.160	SUCCESS	Successfully set config	Jul 23, 2020, 4:01:21

c) In the popup displayed, choose the AP profiles where the IoT configuration must be pushed. You can choose to push the IoT configuration to the default AP profile(s) on the controller. Or you can also choose to push the IoT configuration to all the AP join profiles on the controller.

Figure 12: Enabling IoT Streams for the Connector and for each associated controller



You are about to enable the stream

Please select the below option to continue

● Enable all profile(s) ○ Enable only default profile(s)

This step must be reconfigured if you move APs to a new AP profile.

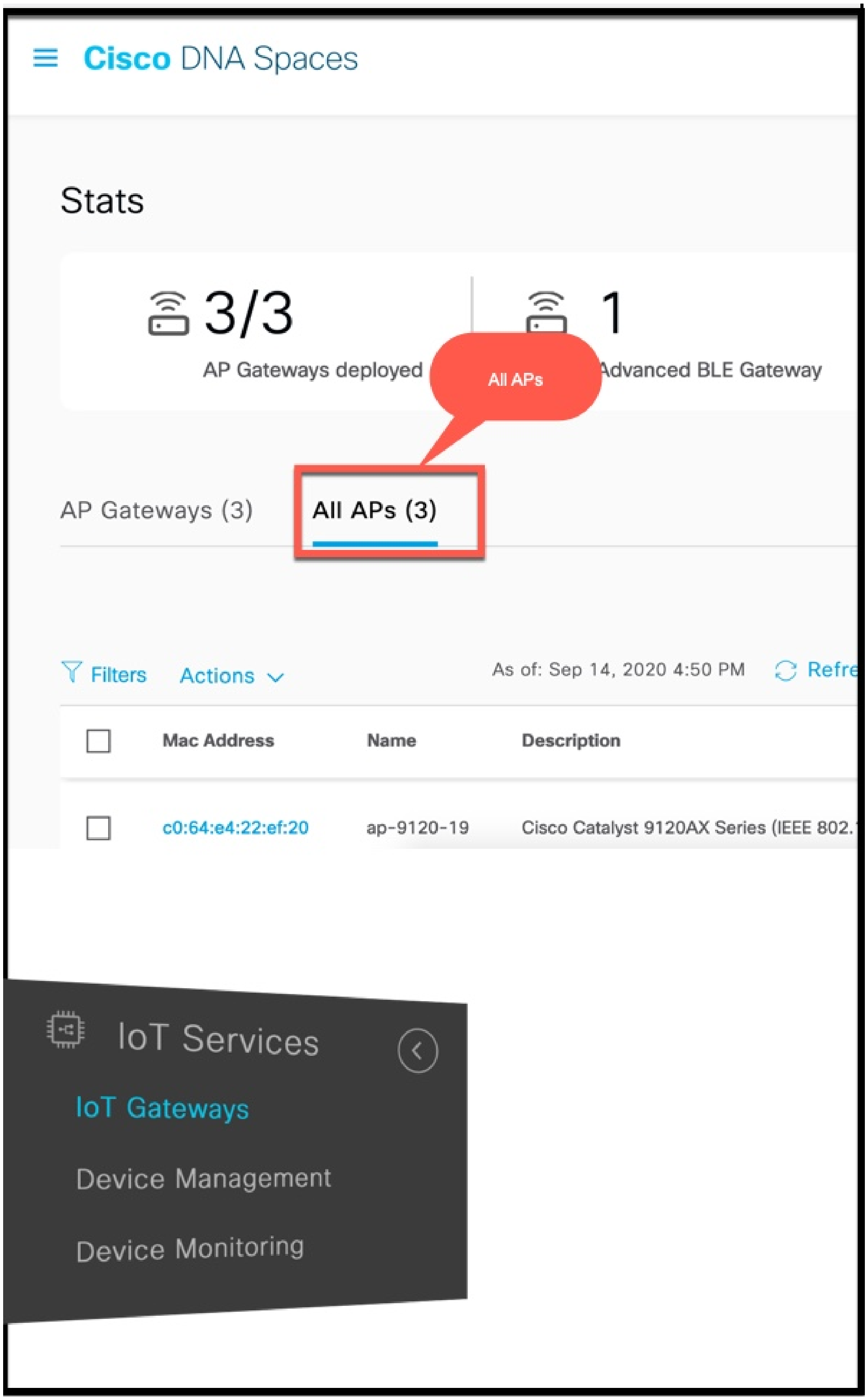
Verify Access Points

This task helps you verify whether your APs have synchronized with Cisco Spaces: IoT Services and are visible on the Cisco Spaces: IoT Services Web UI.

Step 1 From the Cisco Spaces dashboard left-navigation pane, choose **IoT Services** > **IoT Gateways** > **AP Gateway**.

Step 2 Select **All APs** tab to observe whether IoT Services has synced the APs in your network successfully and listed the APs here.

Figure 13: Verify APs



Cisco DNA Spaces

Stats

3/3 AP Gateways deployed

1 Advanced BLE Gateway

All APs

AP Gateways (3) | All APs (3)

Filters | Actions | As of: Sep 14, 2020 4:50 PM | Refre

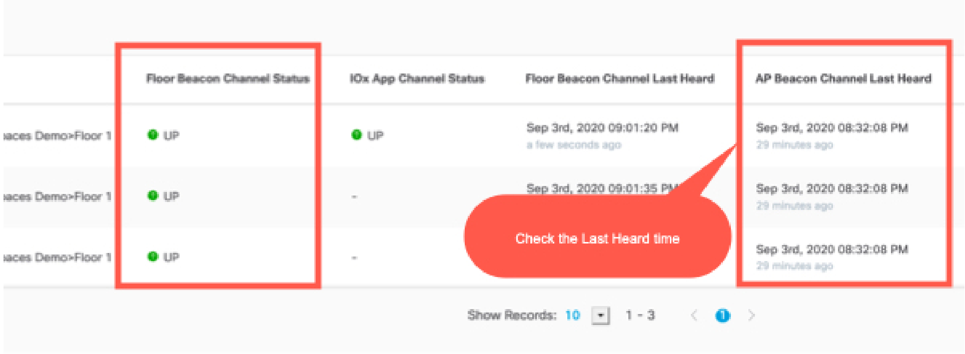
□	Mac Address	Name	Description
□	c0:64:e4:22:ef:20	ap-9120-19	Cisco Catalyst 9120AX Series (IEEE 802.1

IoT Services

- IoT Gateways
- Device Management
- Device Monitoring

Step 3 Verify whether IoT Services has synced the APs in your network successfully and listed the APs here. Observe the **Floor Beacon Channel Status** and **AP Beacon Channel Last Heard**.

Figure 14: Verify APs



	Floor Beacon Channel Status	IOx App Channel Status	Floor Beacon Channel Last Heard	AP Beacon Channel Last Heard
aces Demo>Floor 1	● UP	● UP	Sep 3rd, 2020 09:01:20 PM a few seconds ago	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	● UP	-	Sep 3rd, 2020 09:01:35 PM	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	● UP	-		Sep 3rd, 2020 08:32:08 PM 29 minutes ago

Check the Last Heard time

PART II

Configuration

CHAPTER 5

AP as a Beacon

Configuring an AP as a Beacon

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

IoT Services categorizes AP's according to their configurations as the following:

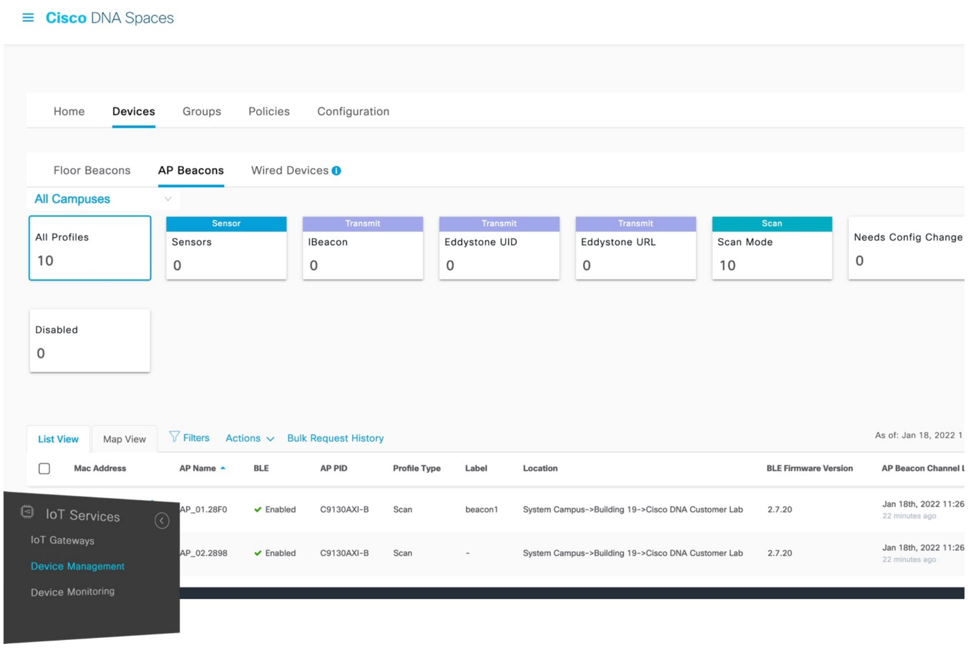
- **Disabled:** APs with BLE disabled. These APs are not scanning or transmitting.
- **Scan Mode: AP beacons** that are only scanning.
- **Transmit Mode: AP beacons** configured in one of the beacon transmit profiles.
- **Needs Config Change:** AP's that have an error in configuration. You can configure these APs in either the **Scan Mode** or the **Transmit Mode**.

You can configure an **AP Beacon** in one of the following transmit modes.

- iBeacon
- Eddystone UID
- Eddystone URL

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

Figure 15: AP Beacon-Categories



All Profiles	Sensor Sensors	Transmit IBeacon	Transmit Eddystone UID	Transmit Eddystone URL	Scan Scan Mode	Needs Config Change	Disabled
10	0	0	0	0	10	0	0

As of: Jan 18, 2022 1

Mac Address	AP Name	BLE	AP PID	Profile Type	Label	Location	BLE Firmware Version	AP Beacon Channel L
	AP_01.28F0	✓ Enabled	C9130AXI-B	Scan	beacon1	System Campus->Building 19->Cisco DNA Customer Lab	2.7.20	Jan 18th, 2022 11:26 22 minutes ago
	AP_02.2898	✓ Enabled	C9130AXI-B	Scan	-	System Campus->Building 19->Cisco DNA Customer Lab	2.7.20	Jan 18th, 2022 11:26 22 minutes ago

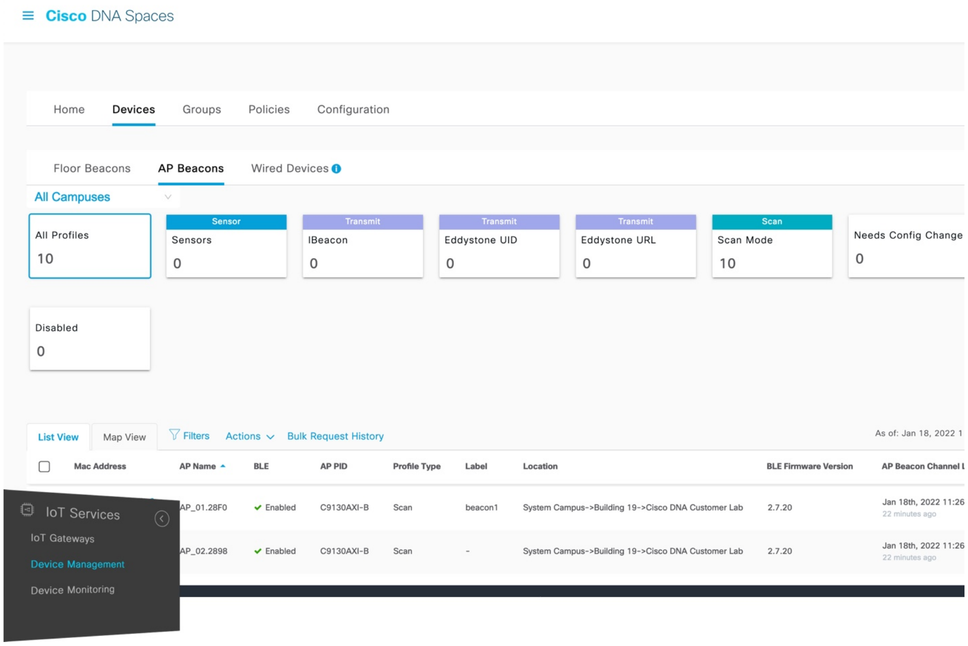
You can also enable telemetry on the AP beacon and collect sensor information.

Configure AP as a Beacon to Transmit or Scan

You can configure an AP as a beacon.

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Device Management** > **Devices** and then click **AP Beacons**. The **AP Beacon** categories page is displayed.

Figure 16: AP Beacon-Categories



All Profiles	Sensor Sensors	Transmit IBeacon	Transmit Eddystone UID	Transmit Eddystone URL	Scan Scan Mode	Needs Config Change
10	0	0	0	0	10	0

Disabled
0

As of: Jan 18, 2022 1

☐	Mac Address	AP Name ▲	BLE	AP PID	Profile Type	Label	Location	BLE Firmware Version	AP Beacon Channel l
		AP_01.28F0	✓ Enabled	C9130AXI-B	Scan	beacon1	System Campus->Building 19->Cisco DNA Customer Lab	2.7.20	Jan 18th, 2022 11:26 22 minutes ago
		AP_02.2898	✓ Enabled	C9130AXI-B	Scan	-	System Campus->Building 19->Cisco DNA Customer Lab	2.7.20	Jan 18th, 2022 11:26 22 minutes ago

Step 2 Do one of the following:

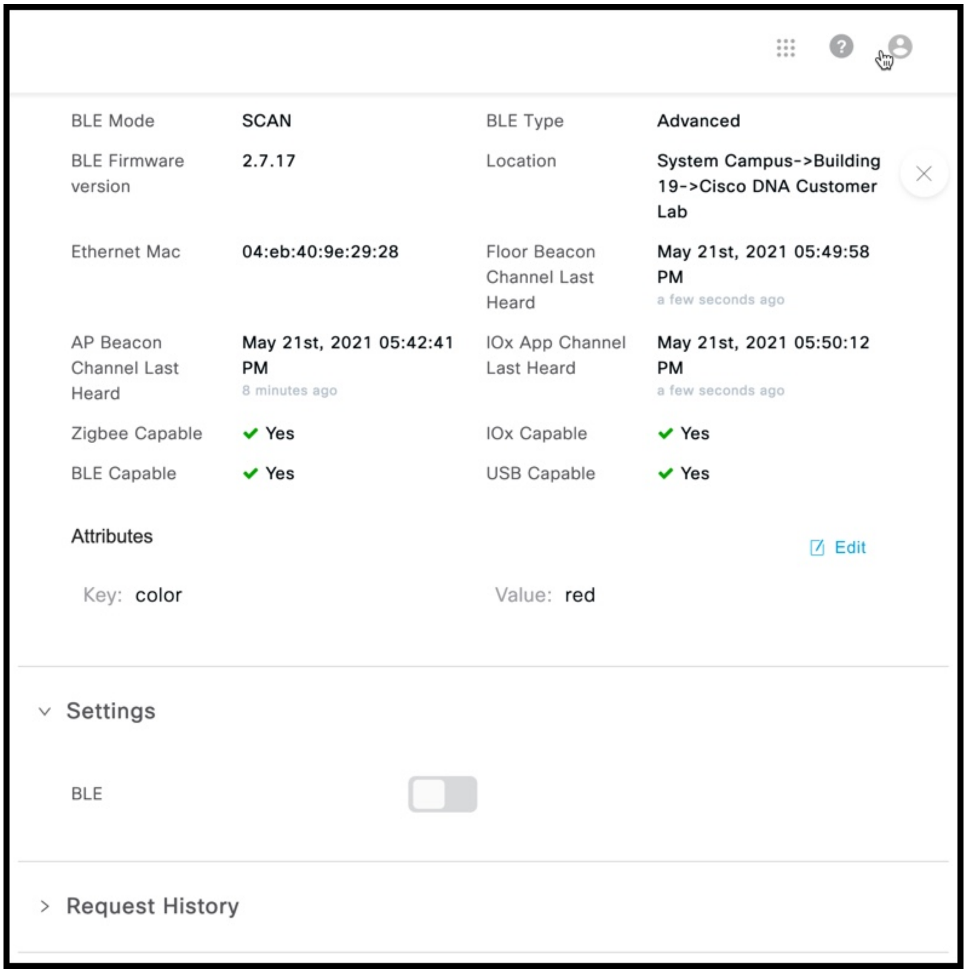
- To configure an AP in the scan mode, go to Step 3.
- To configure an AP in the transmit mode, go to Step 4.

Step 3 Click on the **Disabled** tab, if the count is greater than zero.

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

b) Under **Settings**, click **BLE**.

Figure 17: Configuring an AP as a Beacon



BLE Mode	SCAN	BLE Type	Advanced
BLE Firmware version	2.7.17	Location	System Campus->Building 19->Cisco DNA Customer Lab
Ethernet Mac	04:eb:40:9e:29:28	Floor Beacon Channel Last Heard	May 21st, 2021 05:49:58 PM a few seconds ago
AP Beacon Channel Last Heard	May 21st, 2021 05:42:41 PM 8 minutes ago	IOx App Channel Last Heard	May 21st, 2021 05:50:12 PM a few seconds ago
Zigbee Capable	✓ Yes	IOx Capable	✓ Yes
BLE Capable	✓ Yes	USB Capable	✓ Yes

Attributes

Edit

Key: color

Value: red

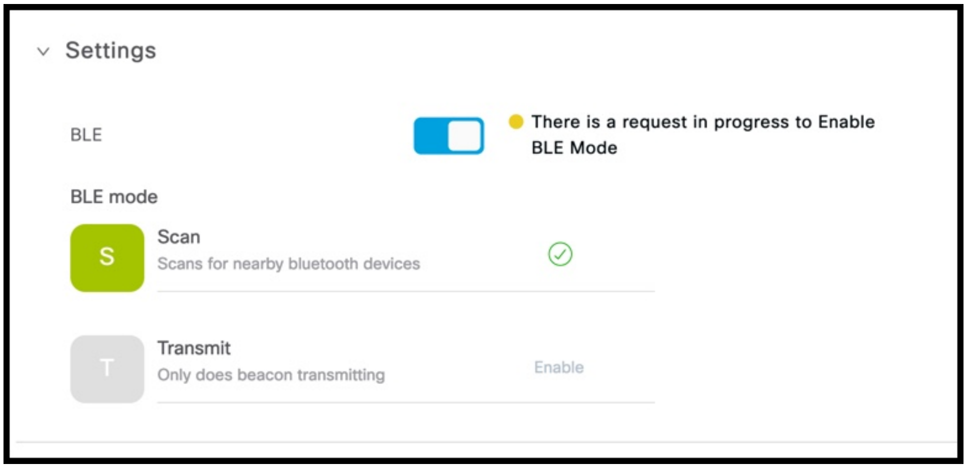
Settings

BLE

Request History

BLE is enabled and the AP is now an AP beacon in the **Scan** mode. You can observe the AP under the **Scan** category. Go to Step 6.

Figure 18: BLE Mode Enabled on AP



Settings

BLE

● There is a request in progress to Enable BLE Mode

BLE mode

S Scan
Scans for nearby bluetooth devices ✓

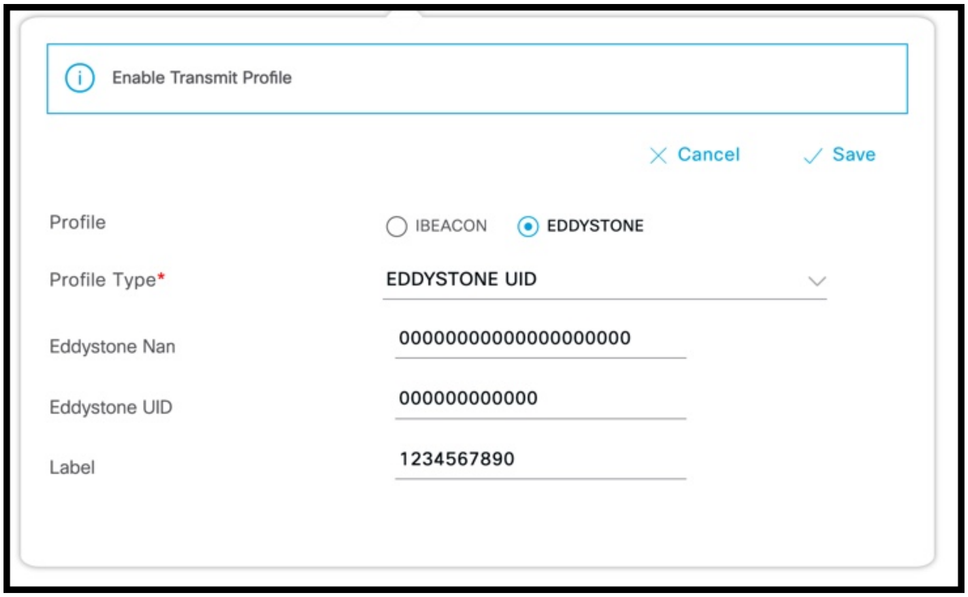
T Transmit
Only does beacon transmitting Enable

Step 4 To configure an AP Beacon in one of the transmit modes, select the MAC address of a listed AP to see further details. In the **Settings** area, you can enable **Transmit** Mode.

Step 5 In the **Enable Transmit Profile** area, you can configure this beacon. Do one of the following:

- Select **iBeacon** and choose one of the **Profile Types**, and configure the values.
- Select **EDDYSTONE** and choose one of the **Profile Types**, and configure the values.

Figure 19: Configuring an AP Beacon in Trasmit Profile



Enable Transmit Profile

Profile ○ IBEACON ● EDDYSTONE

Profile Type* EDDYSTONE UID

Eddystone Nan 00000000000000000000

Eddystone UID 000000000000

Label 1234567890

Step 6 From the **Request History** area, observe the status of the configuration change you requested. On the **AP Beacons** page, notice that the AP now has an **Out of Sync** message beside it. This message disappears once the configuration requested is complete.

CHAPTER 6

AP as a Gateway

Access Point as a BLE Gateway

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

- **Base BLE Gateway**: The Base BLE gateway is a type of AP that you can configure in one of two modes. Either the **Transmit** mode or the **Scan** mode.

  In the **Transmit** 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 Services dashboard decodes and displays this information.

- **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.

  You can configure this AP in the **Scan** mode or **Transmit** mode. In the **Transmit** 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 Services dashboard decodes and displays this information.

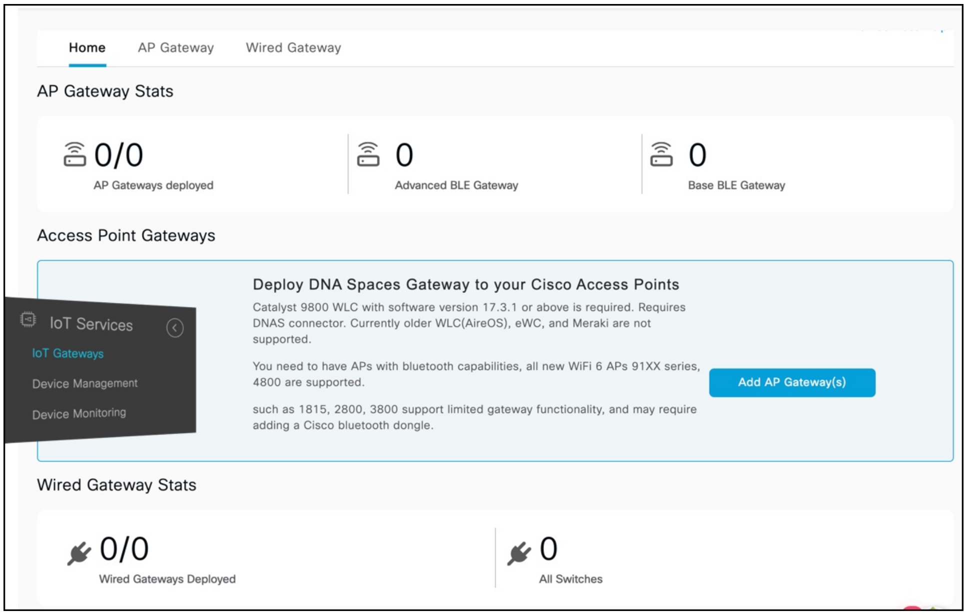
Configure an AP as a Bluetooth Low Energy (BLE) Gateway

This task enables an access point (AP) to act as a BLE gateway. For more information, see Access Point as a Gateway.

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

Step 2 Click **Add New Gateways**.

Figure 20: Adding a new Gateway: when you do not have added gateways



AP Gateway Stats

0/0 AP Gateways deployed	0 Advanced BLE Gateway	0 Base BLE Gateway

Access Point Gateways

Deploy DNA Spaces Gateway to your Cisco Access Points

Catalyst 9800 WLC with software version 17.3.1 or above is required. Requires DNAS connector. Currently older WLC(AireOS), eWC, and Meraki are not supported.

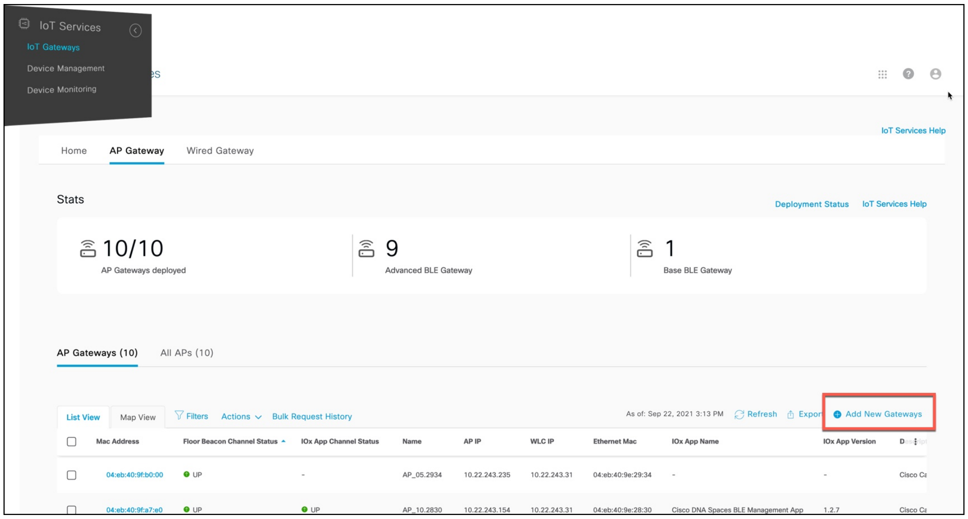
You need to have APs with bluetooth capabilities, all new WiFi 6 APs 91XX series, 4800 are supported.

such as 1815, 2800, 3800 support limited gateway functionality, and may require adding a Cisco bluetooth dongle.

Wired Gateway Stats

0/0 Wired Gateways Deployed	0 All Switches

Figure 21: Adding a new Gateway: when you have added gateways



Stats

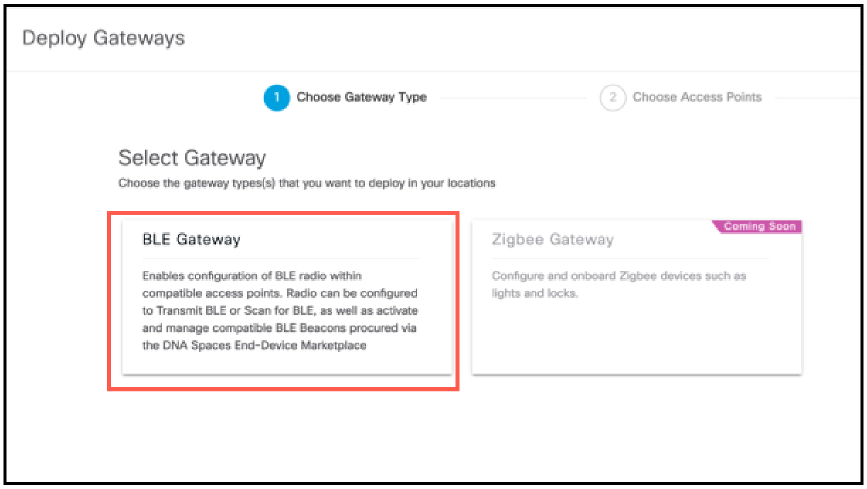
10/10 AP Gateways deployed	9 Advanced BLE Gateway	1 Base BLE Gateway

As of: Sep 22, 2021 3:13 PM

☐	Mac Address	Floor Beacon Channel Status	IOx App Channel Status	Name	AP IP	WLC IP	Ethernet Mac	IOx App Name	IOx App Version	D
☐	04:eb:40:9f:b0:00	● UP	-	AP_05.2934	10.22.243.235	10.22.243.31	04:eb:40:9e:29:34	-	-	Cisco Ca
☐	04:eb:40:9f:a7:e0	● UP	● UP	AP_10.2830	10.22.243.154	10.22.243.31	04:eb:40:9e:28:30	Cisco DNA Spaces BLE Management App	1.2.7	Cisco Ca

Step 3 In the displayed **Deploy Gateway** page, choose **BLE Gateway**.

Figure 22: Select a Gateway type



Deploy Gateways

Select Gateway

Choose the gateway types(s) that you want to deploy in your locations

BLE Gateway

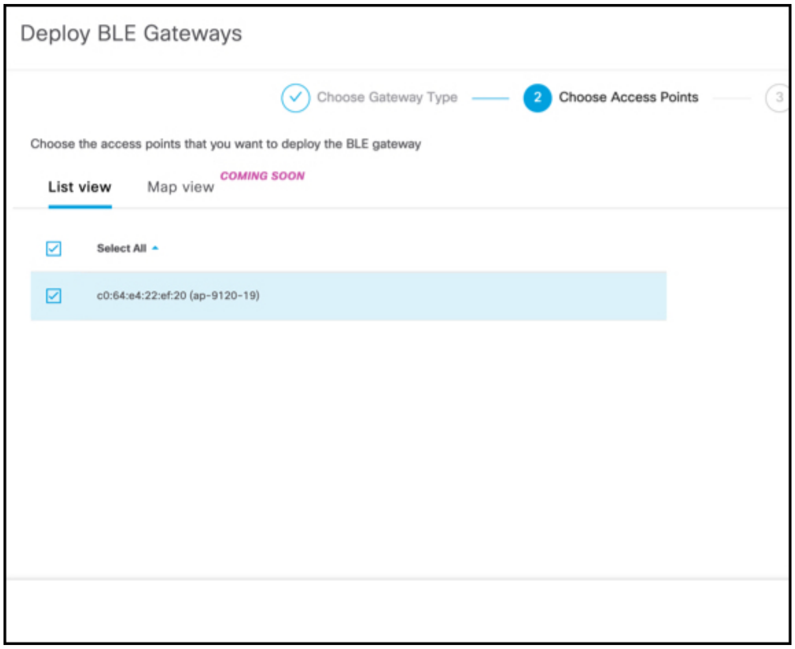
Enables configuration of BLE radio within compatible access points. Radio can be configured to Transmit BLE or Scan for BLE, as well as activate and manage compatible BLE Beacons procured via the DNA Spaces End-Device Marketplace

Zigbee Gateway

Configure and onboard Zigbee devices such as lights and locks.

Step 4 In the displayed **Deploy BLE Gateways** page, select the APs that you want to deploy as a BLE gateway. IoT Services configures a compatible AP as an advanced gateway. Otherwise, IoT Services configures the AP as a base gateway.

Figure 23: Select APs



Deploy BLE Gateways

Choose the access points that you want to deploy the BLE gateway

☑ Select All

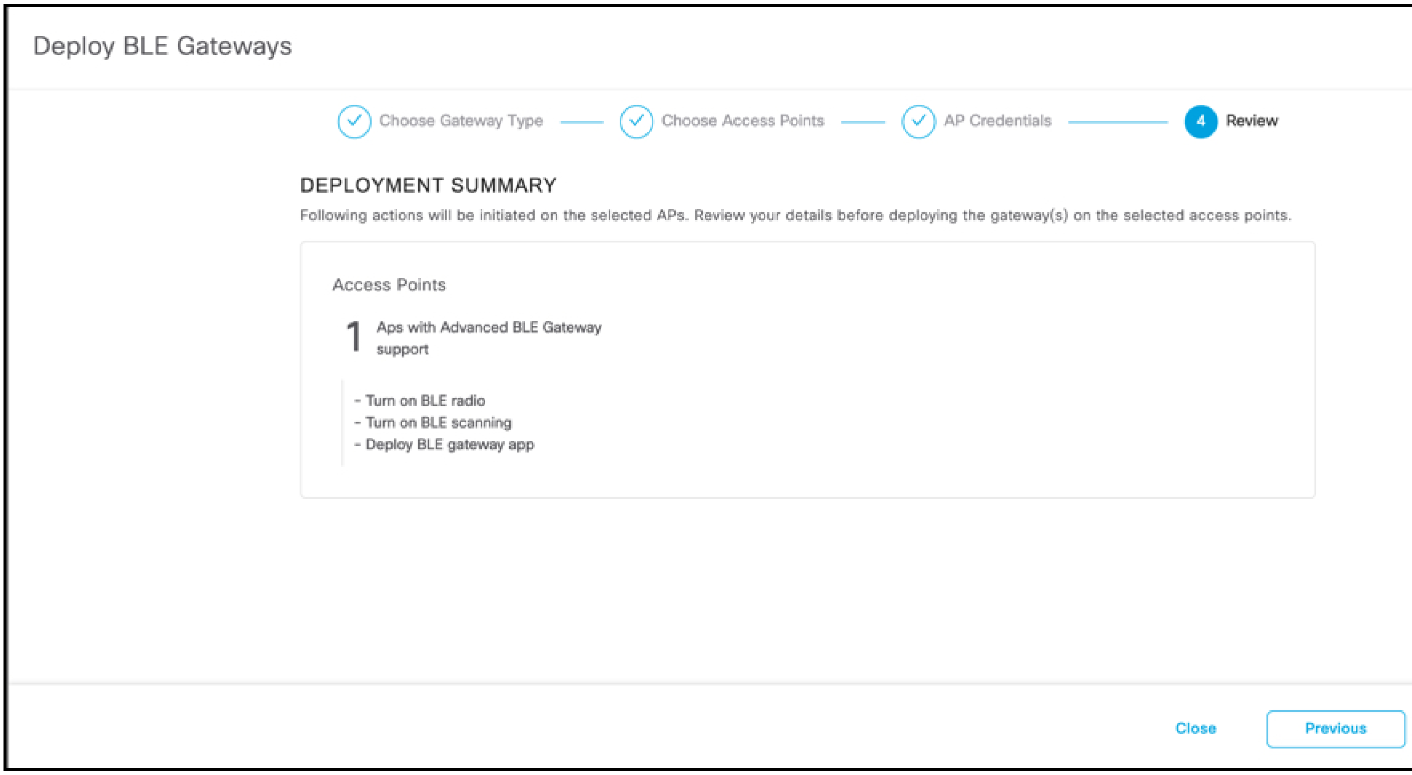
☑ c0:64:e4:22:ef:20 (ap-9120-19)

An AP enabled as an advanced gateway can scan for beacons using an installed IOx application, and can also configure these beacons.

An AP enabled as a base gateway can scan for beacons using system software but cannot configure these beacons.

Step 5 In the displayed **Deploy BLE Gateways** page, you can review the requested changes. And click **Deploy**.

Figure 24: Deploy BLE Gateways



Deploy BLE Gateways

DEPLOYMENT SUMMARY

Following actions will be initiated on the selected APs. Review your details before deploying the gateway(s) on the selected access points.

Access Points

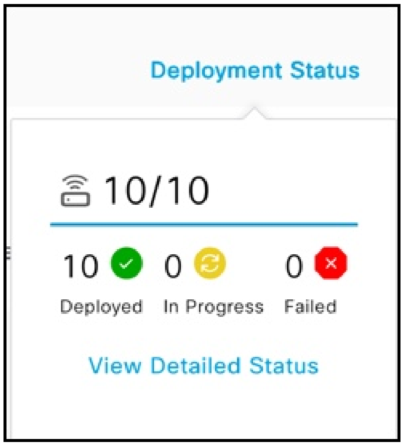
1 Aps with Advanced BLE Gateway support

- Turn on BLE radio
- Turn on BLE scanning
- Deploy BLE gateway app

Once the APs receive these change requests, the APs are queued to be deployed as BLE gateways.

You can also check the status of AP gateway deployment by clicking the **Deployment status** icon in the top-right corner of the dashboard (in the **AP Gateways** page). Here you can see the deployment status of a base or advanced gateway at a more detailed level. You can see whether the gateway is enabled, whether it is in the scan or transmit mode, whether configurations are being pushed on to the gateway, or if the gateway is capable, whether IOX is being installed. Unlike bulk history, here you can view the details of an individual AP gateway. If the gateway deployment fails, the reasons are listed here.

Figure 25: Deployment Status



Deployment Status

10/10

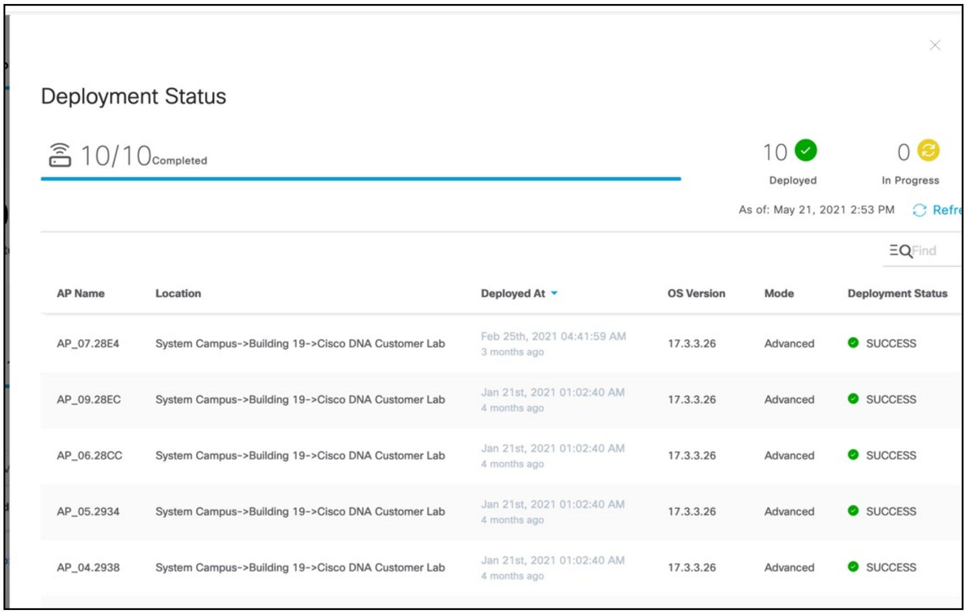
10 ✓ Deployed

0 In Progress

0 ✕ Failed

View Detailed Status

Figure 26: Deployment Status



Deployment Status

10/10 Completed

10 ✓ Deployed

0 In Progress

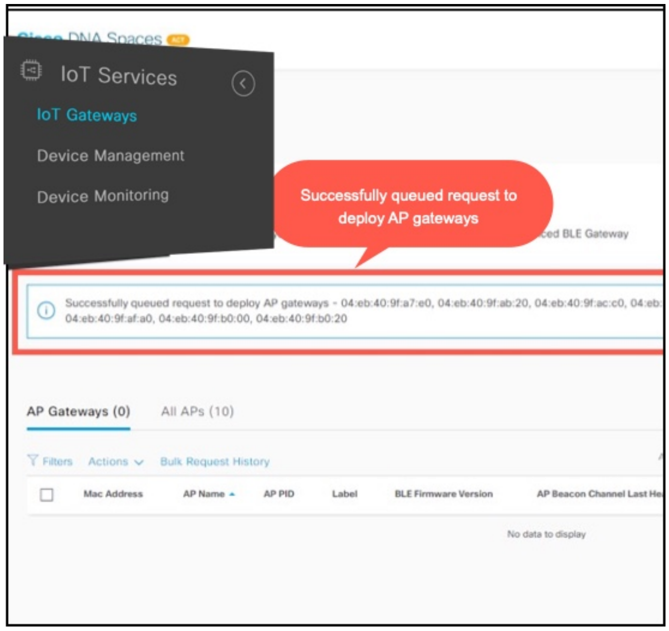
As of: May 21, 2021 2:53 PM Refre

Find

AP Name	Location	Deployed At	OS Version	Mode	Deployment Status
AP_07.28E4	System Campus->Building 19->Cisco DNA Customer Lab	Feb 25th, 2021 04:41:59 AM 3 months ago	17.3.3.26	Advanced	● SUCCESS
AP_09.28EC	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_06.28CC	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_05.2934	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_04.2938	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS

You can also observe the progress on the displayed page.

Figure 27: Progress of Deployment

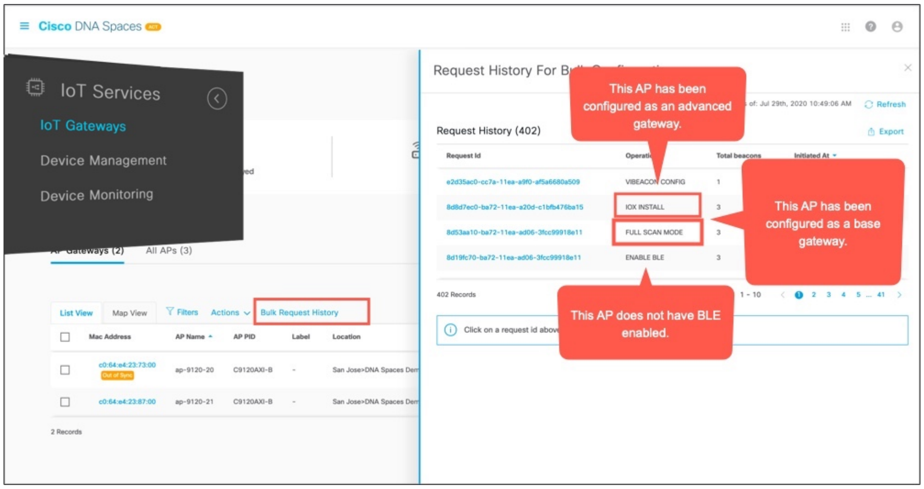


Successfully queued request to deploy AP gateways - 04:eb:40:9f:a7:e0, 04:eb:40:9f:ab:20, 04:eb:40:9f:ac:c0, 04:eb:
04:eb:40:9f:af:a0, 04:eb:40:9f:b0:00, 04:eb:40:9f:b0:20

☐	Mac Address	AP Name	AP PID	Label	BLE Firmware Version	AP Beacon Channel Last He
					No data to display	

You can also check the status of deployment by clicking **Bulk Request History**.

Figure 28: Bulk Request History



☐	Mac Address	AP Name	AP PID	Label	Location
☐	c0:64:e4:23:73:00 Out of Sync	ap-9120-20	C9120AXI-B	-	San Jose>DNA Spaces Dem
☐	c0:64:e4:23:87:00	ap-9120-21	C9120AXI-B	-	San Jose>DNA Spaces Dem

2 Records

Request History For B

of: Jul 29th, 2020 10:49:06 AM

Request History (402)

Request Id	Operati	Total beacons	Initiated At
e2d35ac0-cc7a-11ea-a9f0-af5a6680a509	VIBEACON CONFIG	1	
8d8d7ec0-ba72-11ea-a20d-c1bfb476ba15	IOX INSTALL	3	
8d53aa10-ba72-11ea-ad06-3fcc99918e11	FULL SCAN MODE	3	
8d19fc70-ba72-11ea-ad06-3fcc99918e11	ENABLE BLE	3	

402 Records 1 - 10 ‹ 1 2 3 4 5 ... 41 ›

Click on a request id above

The **Operations** column shows the status of each AP.

- IOX INSTALL: You have configured this AP as an advanced gateway.
- FULL SCAN MODE: You have configured this AP is a base gateway.
- ENABLE BLE: Enable BLE on this AP.

Install, Uninstall, or Upgrade an IOx Application on an Advanced Gateway

You can install, uninstall, or upgrade IOx applications on advanced gateways. The Cisco Spaces: BLE Management is one some application.

Before you begin

Ensure that you have configured an access point (AP) as an advanced gateway.

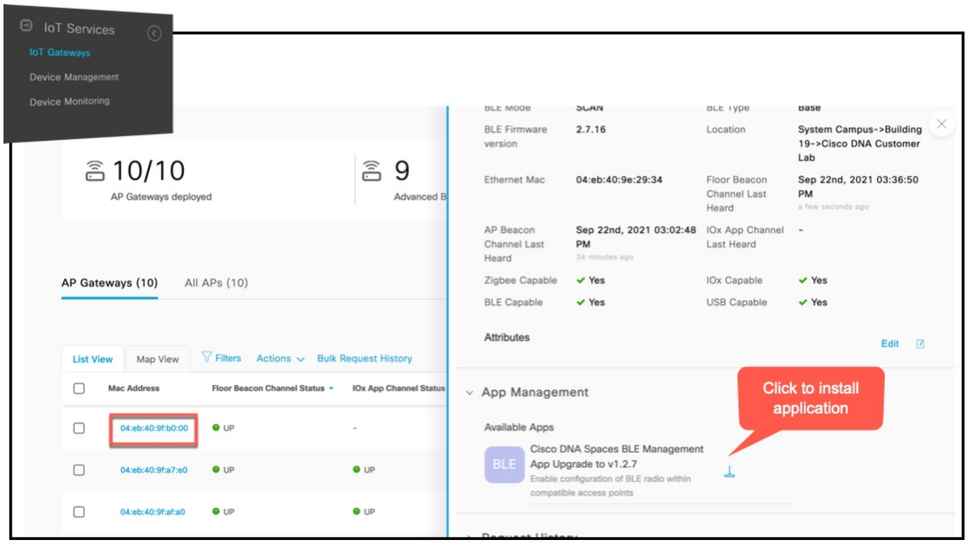
Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **IoT Gateways** > **AP Gateways** and click **All APs.**

Step 2 Click the MAC address of the AP to open the detailed **AP** page.

Step 3 In the **App Management** section, you can see the applications available for installation, uninsallation, or upgrade. Do one of the following:

- To install, click the install icon near Cisco Spaces: BLE Management.
- To uninstall, click the uninstall icon near Cisco Spaces: BLE Management.
- To upgrade, check if a version is available for upgrade near the Cisco Spaces: BLE Management and click it.
- To upload tech-support files to the Connector, click the gear icon.

Figure 29: Install Cisco Spaces: BLE Management



	Mac Address	Floor Beacon Channel Status	IOx App Channel Status
□	04:eb:40:9f:b0:00	● UP	-
□	04:eb:40:9f:a7:e0	● UP	● UP
□	04:eb:40:9f:af:a0	● UP	● UP

BLE Mode	SCAN	BLE Type	Base
BLE Firmware version	2.7.16	Location	System Campus->Building 19->Cisco DNA Customer Lab
Ethernet Mac	04:eb:40:9e:29:34	Floor Beacon Channel Last Heard	Sep 22nd, 2021 03:36:50 PM a few seconds ago
AP Beacon Channel Last Heard	Sep 22nd, 2021 03:02:48 PM 34 minutes ago	IOx App Channel Last Heard	-
Zigbee Capable	✓ Yes	IOx Capable	✓ Yes
BLE Capable	✓ Yes	USB Capable	✓ Yes

Attributes

App Management

Available Apps

Cisco DNA Spaces BLE Management
App Upgrade to v1.2.7
Enable configuration of BLE radio within compatible access points

Request History

Figure 30: Uninstall Cisco Spaces: BLE Management

After you have installed the application, a gear icon appears that allows you to upload log files to Connector. You can also download these files to assist a technical support team.

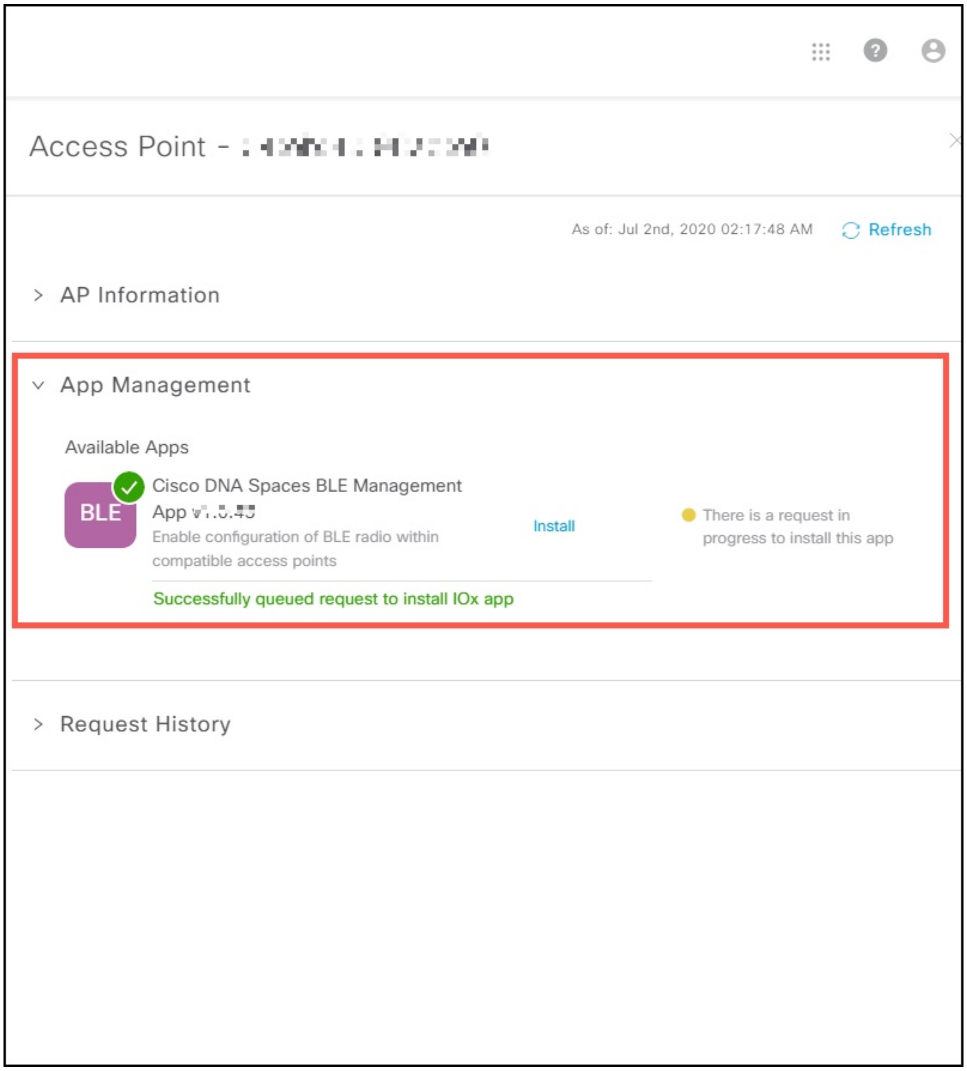
Figure 31: Technical Support Log Files

Step 4 Enter the credentials needed for authentication on the AP.

Note The authentication request to the APs includes these credentials, after which IoT Services does not retain these credentials.

The AP which is the advanced gateway receives these change requests for installations. You can observe the progress on the displayed page.

Figure 32: App Management: Progress of Installation



Access Point - [redacted]

As of: Jul 2nd, 2020 02:17:48 AM

Cisco DNA Spaces BLE Management App [redacted]

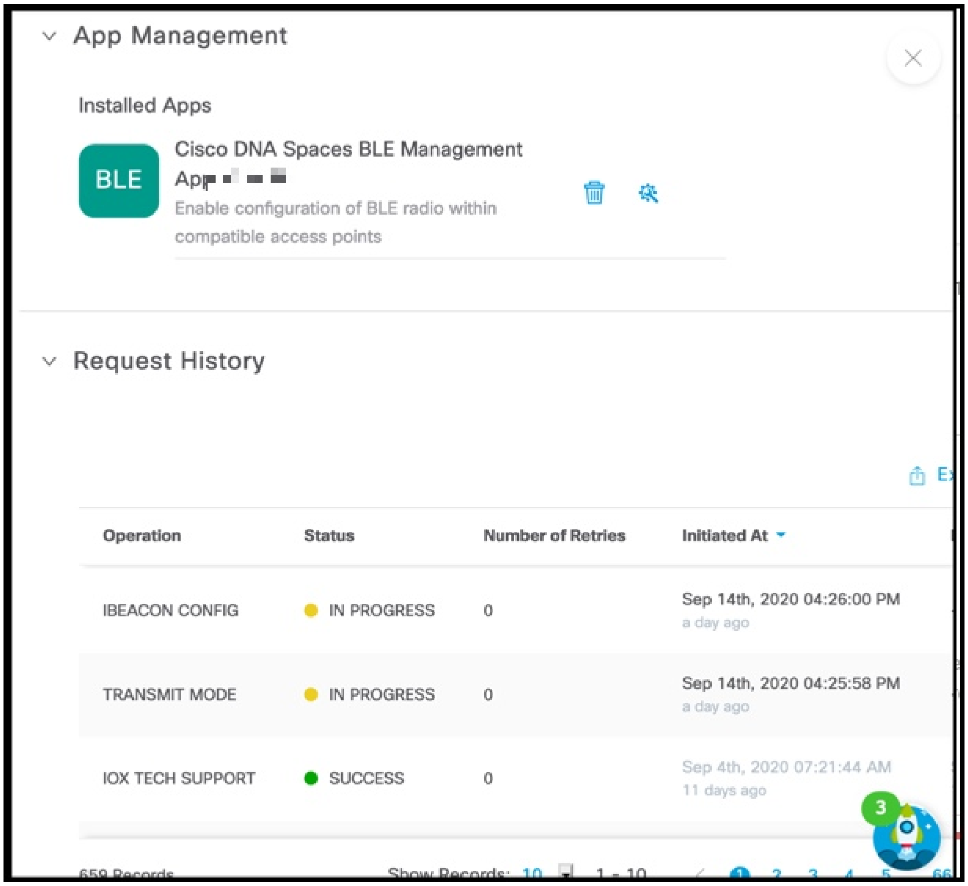
Enable configuration of BLE radio within compatible access points

● There is a request in progress to install this app

Successfully queued request to install IOx app

You can also check the status of deployment by clicking **Request History**.

Figure 33: Installation Status in the Request History Area



App Management

Installed Apps

BLE

Cisco DNA Spaces BLE Management App [redacted]

Enable configuration of BLE radio within compatible access points

Request History

Operation	Status	Number of Retries	Initiated At
IBEACON CONFIG	● IN PROGRESS	0	Sep 14th, 2020 04:26:00 PM a day ago
TRANSMIT MODE	● IN PROGRESS	0	Sep 14th, 2020 04:25:58 PM a day ago
IOX TECH SUPPORT	● SUCCESS	0	Sep 4th, 2020 07:21:44 AM 11 days ago

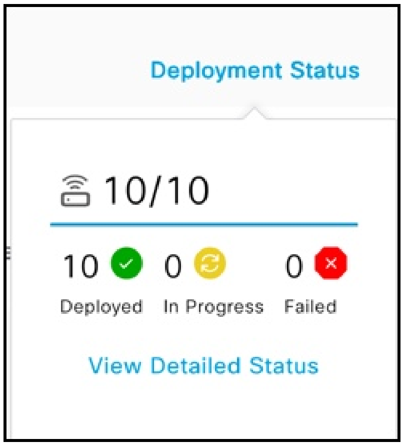
659 Records Show Records: 10 1 - 10 1 2 3 4 5 66

The **Status** column shows the status of installation on each AP.

- SUCCESS: Installation of application on the AP was a success.
- FAILURE: Installation of application on the AP was a failure.
- IN PROGRESS: Installation of application on the AP is still in progress.

You can also check the status of AP gateway deployment by clicking the **Deployment status** icon in the top-right corner of the dashboard (in the **AP Gateways** page). Here you can see the deployment status of a base or advanced gateway at a more detailed level. You can see whether the gateway is enabled, whether it is in the scan or transmit mode, whether configurations are being pushed on to the gateway, or if the gateway is capable, whether IOX is being installed. Unlike bulk history, here you can view the details of an individual AP gateway. If the gateway deployment fails, the reasons are listed here.

Figure 34: Deployment Status



Deployment Status

10/10

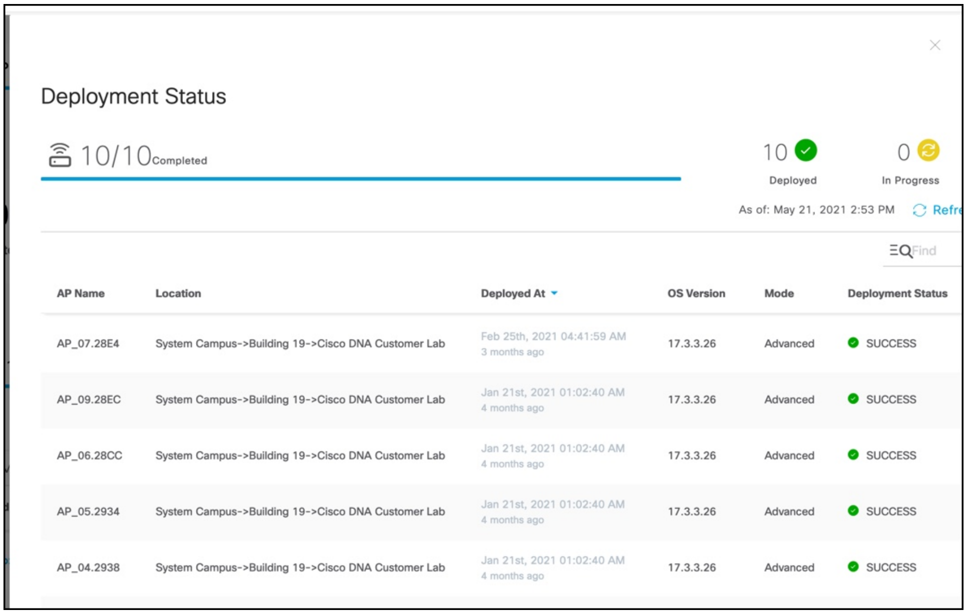
10 ✓ Deployed

0 In Progress

0 ✕ Failed

View Detailed Status

Figure 35: Deployment Status



Deployment Status

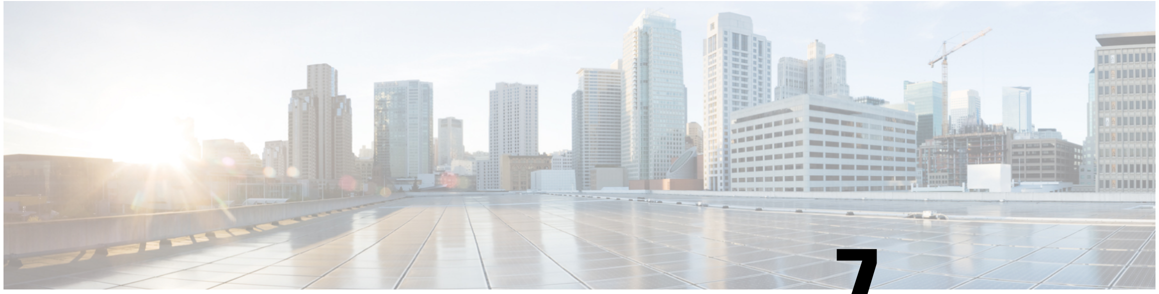
10/10Completed

10 ✓ Deployed

0 In Progress

As of: May 21, 2021 2:53 PM Refre

AP Name	Location	Deployed At	OS Version	Mode	Deployment Status
AP_07.28E4	System Campus->Building 19->Cisco DNA Customer Lab	Feb 25th, 2021 04:41:59 AM 3 months ago	17.3.3.26	Advanced	● SUCCESS
AP_09.28EC	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_06.28CC	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_05.2934	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS
AP_04.2938	System Campus->Building 19->Cisco DNA Customer Lab	Jan 21st, 2021 01:02:40 AM 4 months ago	17.3.3.26	Advanced	● SUCCESS



CHAPTER 7

Beacons and Tags

Discover Beacons

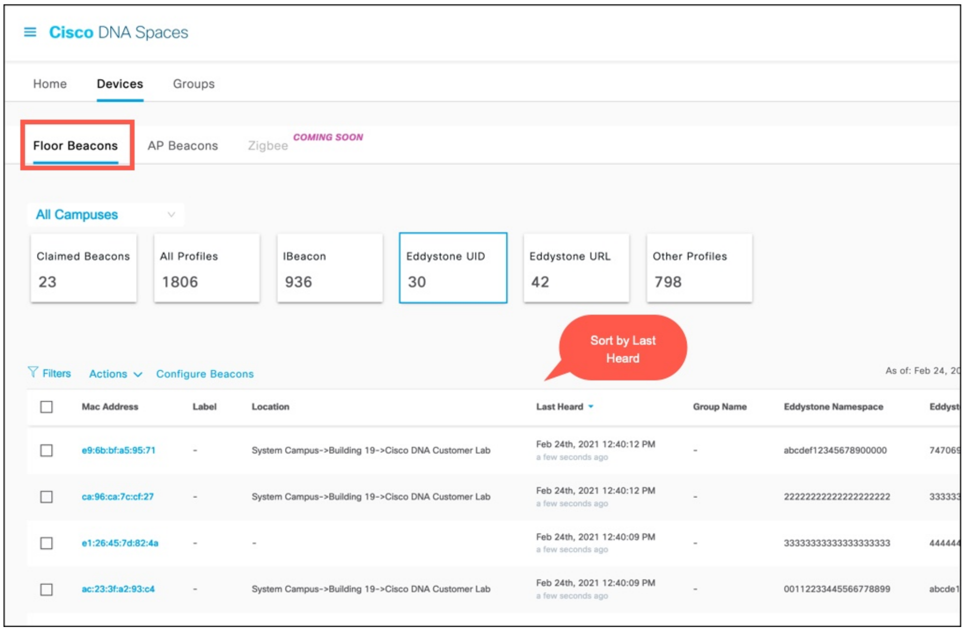
This section shows you how to view the beacons scanned by IoT Services.

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Device Management** > **Devices**.

Step 2 Click on **Floor Beacons** to view scanned beacons. Click on one of the following: **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 36: Beacon Details



≡ Cisco DNA Spaces

Home | Devices | Groups

Floor Beacons | AP Beacons | Zigbee COMING SOON

All Campuses

Claimed Beacons	All Profiles	IBeacon	Eddystone UID	Eddystone URL	Other Profiles
23	1806	936	30	42	798

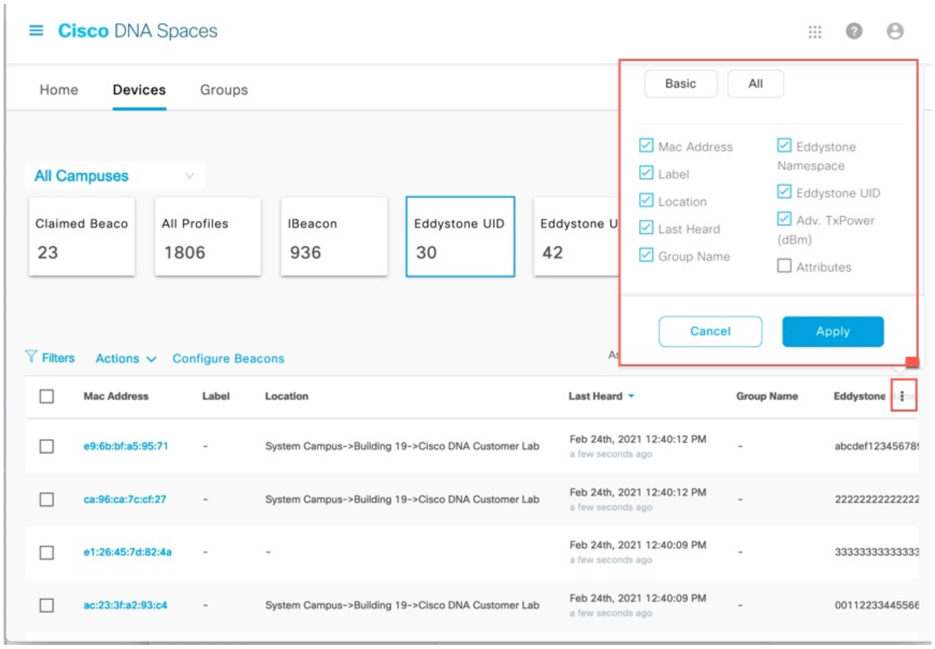
Sort by Last Heard

Filters | Actions | Configure Beacons | As of: Feb 24, 20

☐	Mac Address	Label	Location	Last Heard	Group Name	Eddystone Namespace	Eddyst
☐	e9:6b:bf:a5:95:71	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	abcdef12345678900000	74706
☐	ca:96:ca:7c:cf:27	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	22222222222222222222	33333
☐	e1:26:45:7d:82:4a	-	-	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	33333333333333333333	44444
☐	ac:23:3f:a2:93:c4	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	00112233445566778899	abcde1

Step 3 Add or delete columns using the three dots on the right.

Figure 37: Adding or Deleting Columns



≡ Cisco DNA Spaces

Home | Devices | Groups

All Campuses

Claimed Beaco	All Profiles	IBeacon	Eddystone UID	Eddystone U
23	1806	936	30	42

Basic | All

☑ Mac Address
☑ Label
☑ Location
☑ Last Heard
☑ Group Name
☑ Eddystone Namespace
☑ Eddystone UID
☑ Adv. TxPower (dBm)
☐ Attributes

Cancel | Apply

Filters | Actions | Configure Beacons

☐	Mac Address	Label	Location	Last Heard	Group Name	Eddystone ⋮
☐	e9:6b:bf:a5:95:71	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	abcdef12345678
☐	ca:96:ca:7c:cf:27	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	22222222222222
☐	e1:26:45:7d:82:4a	-	-	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	33333333333333
☐	ac:23:3f:a2:93:c4	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	00112233445566

Step 4 Click on the MAC address of the beacon to view further details.

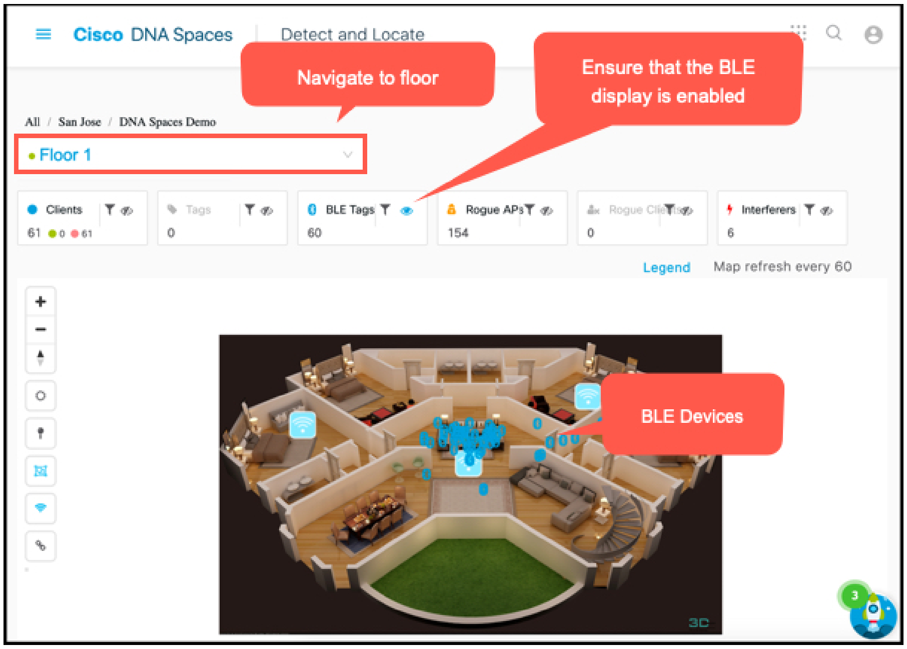
Figure 38: Beacon Details

What to do next

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

Figure 39: Cisco Spaces: Detect and Locate

Figure 40: Cisco Spaces: Detect and Locate



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

Claiming a Beacon

When you claim a beacon, your IoT Services account claims ownership of the beacon using the order ID of the beacon. If you do not claim the beacon, IoT Services may still detect the beacon. But you cannot configure or manage the beacon.

This procedure shows you how to claim a beacon scanned by IoT Services.

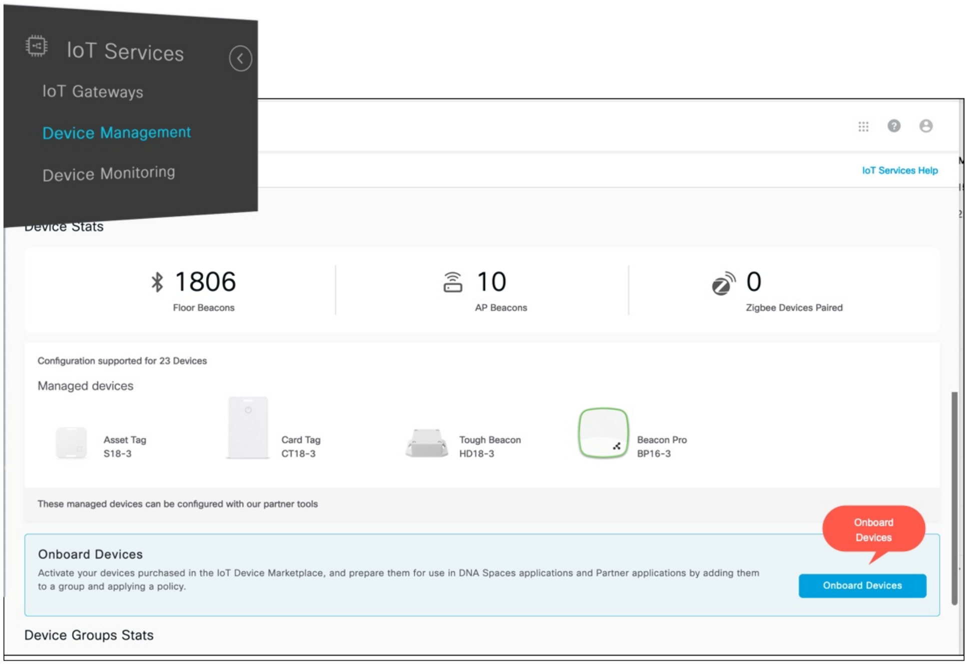
Before you begin

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.

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Device Management**.

Step 2 Click **Onboard Devices** and choose **Floor Beacons**.

Figure 41: Onboard Devices



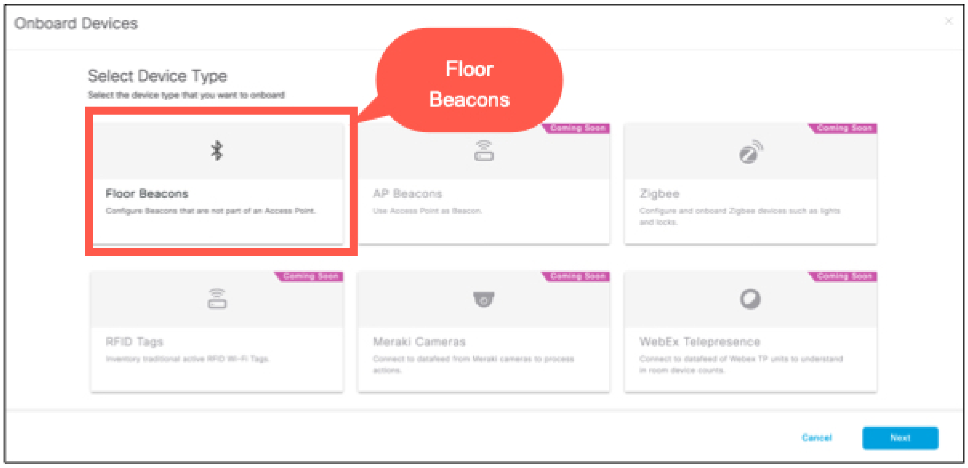
Configuration supported for 23 Devices

These managed devices can be configured with our partner tools

Onboard Devices

Activate your devices purchased in the IoT Device Marketplace, and prepare them for use in DNA Spaces applications and Partner applications by adding them to a group and applying a policy.

Figure 42: Onboard Floor Beacons



Select Device Type

Select the device type that you want to onboard

Floor Beacons

Configure Beacons that are not part of an Access Point.

AP Beacons

Use Access Point as Beacon.

Zigbee

Configure and onboard Zigbee devices such as lights and locks.

RFID Tags

Inventory traditional active RFID Wi-Fi Tags.

Meraki Cameras

Connect to datafeed from Meraki cameras to process actions.

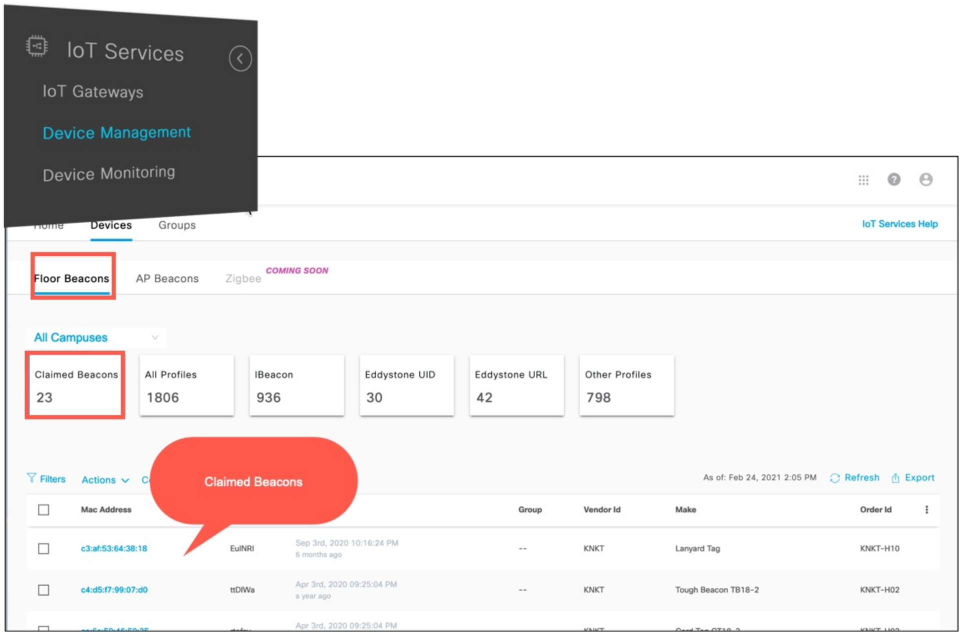
WebEx Telepresence

Connect to datafeed of Webex TP units to understand in room device counts.

Step 3 In the displayed **Claim Floor Beacons** page, enter the **Order ID** and click **Add to Inventory**.
You can see the beacon in the **IoT Services>Device Management**.

Step 4 In the IoT Services dashboard, navigate to **Device Management**. Under **Floor Beacons** > **Claimed Beacons**. Verify if the claimed beacon is displayed in this list.

Figure 43: Beacon Details



Claimed Beacons	All Profiles	IBeacon	Eddystone UID	Eddystone URL	Other Profiles
23	1806	936	30	42	798

As of: Feb 24, 2021 2:05 PM

Mac Address			Group	Vendor Id	Make	Order Id
c3:af:53:64:38:18	EuINRI	Sep 3rd, 2020 10:16:24 PM 6 months ago	--	KNKT	Lanyard Tag	KNKT-H10
c4:d5:f7:99:07:d0	ttDIWa	Apr 3rd, 2020 09:25:04 PM a year ago	--	KNKT	Tough Beacon TB18-2	KNKT-H02

What to do next

You can now configure the beacons.

Configuring a Beacon on IoT Services

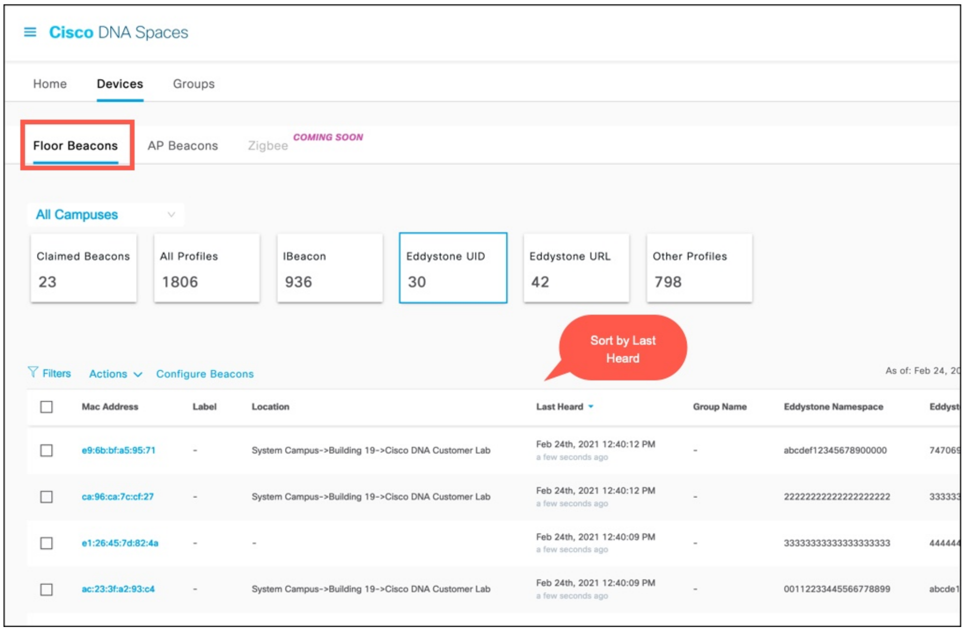
This task shows you how to view the beacons scanned by IoT Services.

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Device Management** > **Devices**.

Step 2 Click on **Floor Beacons** to view the scanned beacons.

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

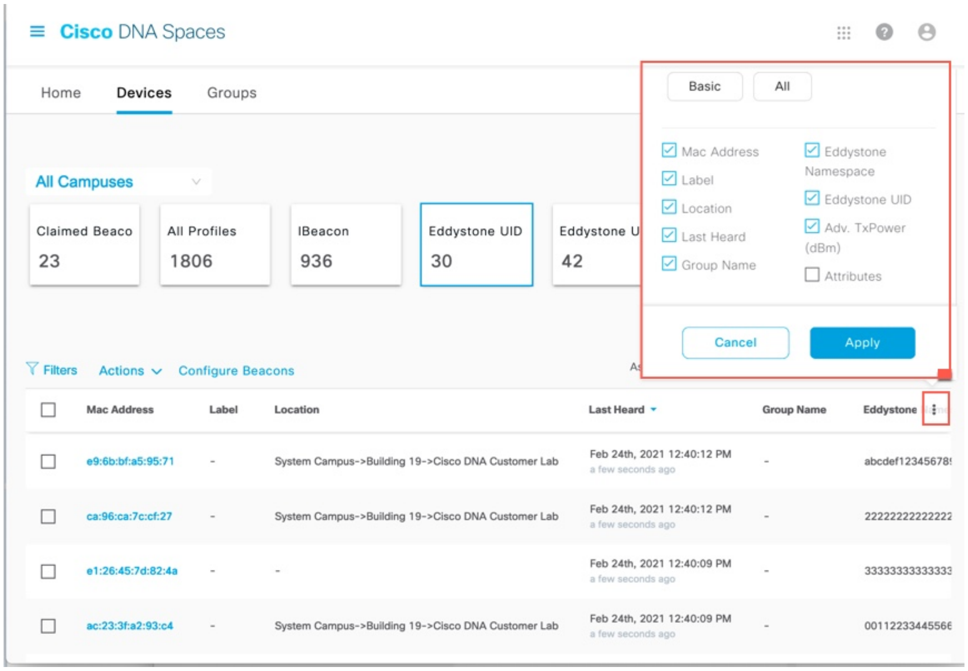
Figure 44: Beacon Details



□	Mac Address	Label	Location	Last Heard ▾	Group Name	Eddystone Namespace	Eddyst
□	e9:6b:bf:a5:95:71	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	abcdef12345678900000	747069
□	ca:96:ca:7c:cf:27	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	22222222222222222222	333333
□	e1:26:45:7d:82:4a	-	-	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	33333333333333333333	444444
□	ac:23:3f:a2:93:c4	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	00112233445566778899	abcde1

Step 3 Add or delete columns using the three dots on the right.

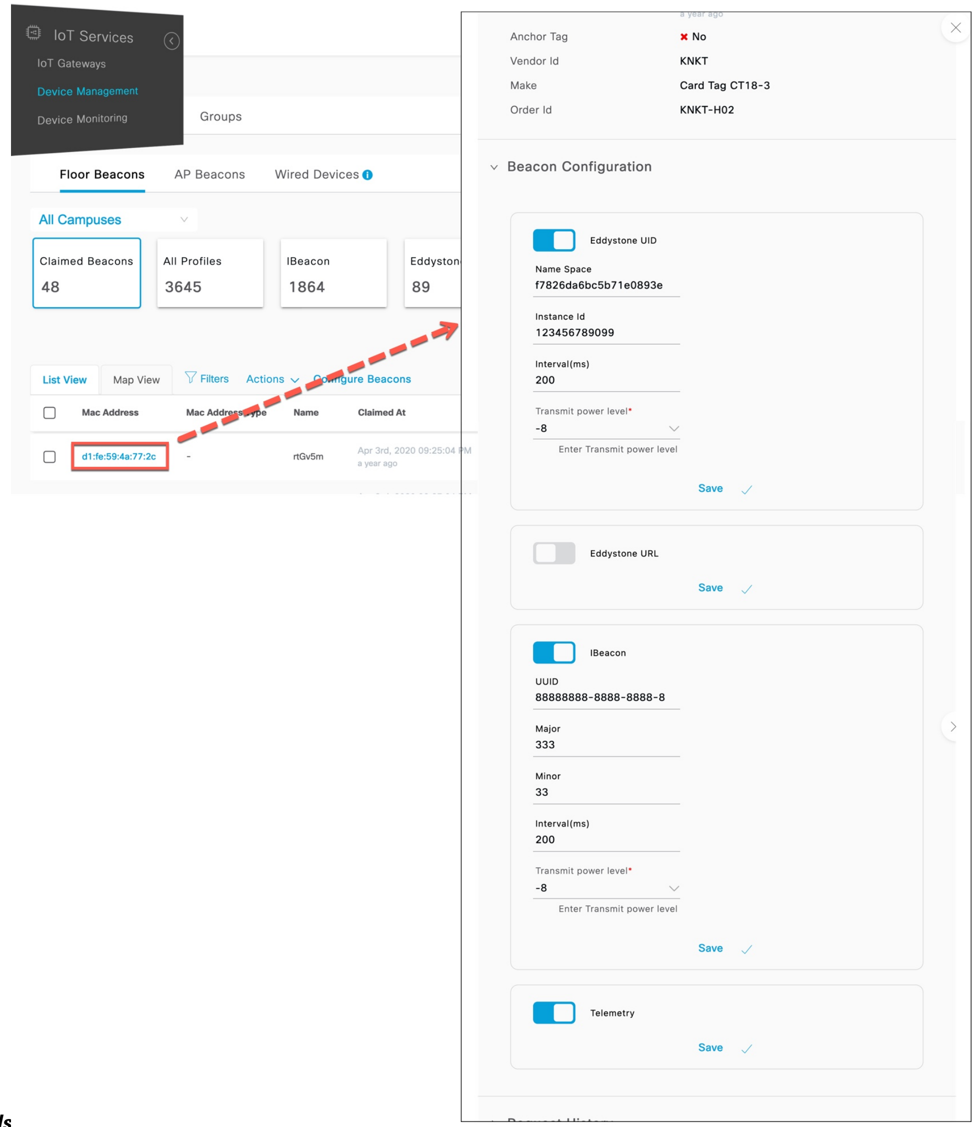
Figure 45: Adding or Deleting Columns



☑ Mac Address
☑ Label
☑ Location
☑ Last Heard
☑ Group Name
☑ Eddystone Namespace
☑ Eddystone UID
☑ Adv. TxPower (dBm)
☐ Attributes

□	Mac Address	Label	Location	Last Heard ▾	Group Name	Eddystone ⋮
□	e9:6b:bf:a5:95:71	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	abcdef12345678!
□	ca:96:ca:7c:cf:27	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 PM a few seconds ago	-	22222222222222
□	e1:26:45:7d:82:4a	-	-	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	33333333333333
□	ac:23:3f:a2:93:c4	-	System Campus->Building 19->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:09 PM a few seconds ago	-	0011223344556€

Step 4 Click on the MAC address of the beacon to view further details.



Claimed Beacons	All Profiles	IBeacon	Eddyston
48	3645	1864	89

☐	Mac Address	Mac Address Type	Name	Claimed At
☐	d1:fe:59:4a:77:2c	-	rtGv5m	Apr 3rd, 2020 09:25:04 PM a year ago

Anchor Tag	✖ No
Vendor Id	KNKT
Make	Card Tag CT18-3
Order Id	KNKT-H02

Eddystone UID

Name Space: f7826da6bc5b71e0893e

Instance Id: 123456789099

Interval(ms): 200

Transmit power level*: -8

IBeacon

UUID: 88888888-8888-8888-8

Major: 333

Minor: 33

Interval(ms): 200

Transmit power level*: -8

Figure 46: Beacon Details

Step 5 From the **Beacon Information** section, configure the device or enable telemetry.

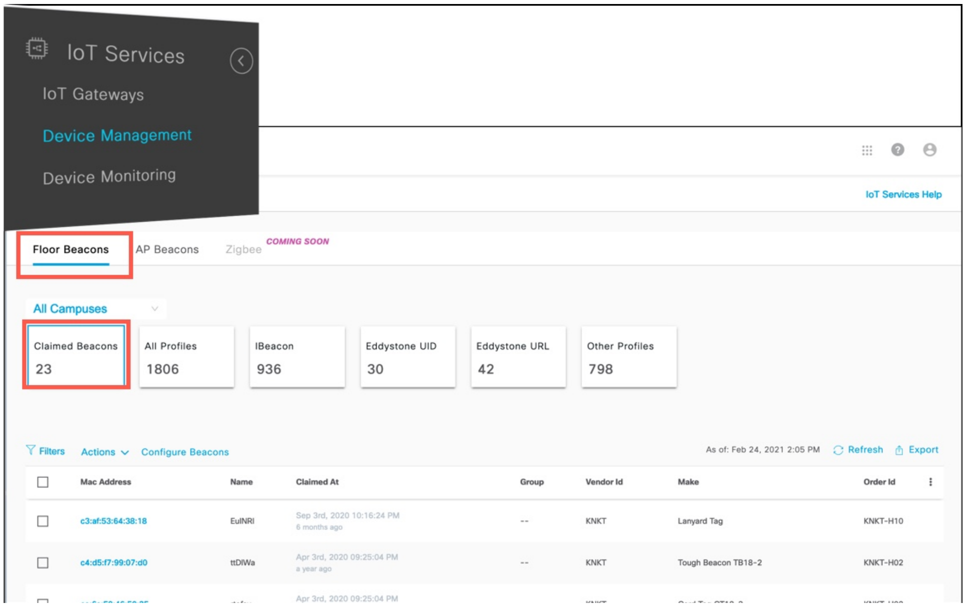
Viewing Sensor Information

Before you begin

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services** > **Device Management** > **Devices**.

Step 2 Click the **Floor Beacons** tab and click the profile. Choose the floor beacon of your choice.

Figure 47: Beacon Details



Claimed Beacons	All Profiles	IBeacon	Eddystone UID	Eddystone URL	Other Profiles
23	1806	936	30	42	798

As of: Feb 24, 2021 2:05 PM

□	Mac Address	Name	Claimed At	Group	Vendor Id	Make	Order Id
□	c3:af:53:64:38:18	EulNRI	Sep 3rd, 2020 10:16:24 PM 6 months ago	--	KNKT	Lanyard Tag	KNKT-H10
□	c4:d5:f7:99:07:d0	ttDlWa	Apr 3rd, 2020 09:25:04 PM a year ago	--	KNKT	Tough Beacon TB18-2	KNKT-H02
□			Apr 3rd, 2020 09:25:04 PM				

Step 3 Click the beacon to see further details. In the **Sensor Information** area, you can see the broadcast sensor data for the beacon.

Figure 48: Status of Configuration on IoT Services

Configuring a Location Anchor

You can configure a claimed beacon as a location anchor for wayfinding. Once a claimed floor beacon is configured as a location anchor, the **Anchor Tag** field in its details indicates the same.

Note Access Points are location anchors by default. Floor beacons must be configured as location anchors.

This task shows you how to configure a claimed floor beacon as a location anchor.

SUMMARY STEPS

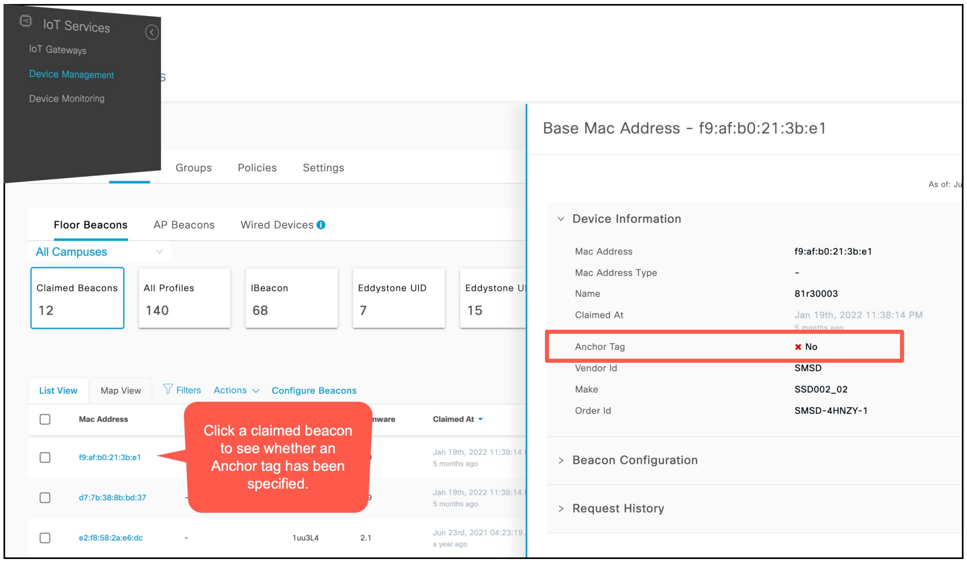
1. From the Cisco Spaces dashboard, navigate to **IoT Services > Device Management > Devices**.
2. Click the **Floor Beacons** tab and click **Claimed Beacons**. Select a floor beacon of your choice to view details. The **Anchor Tag** field indicates if the beacon has a location tag that is associated with it. Close the details page.
3. Click **Map View** and navigate to the required floor. From the list of icons in the left pane, click the **Add Anchor Tag.**
4. Click the position on the map where you want to configure the location anchor. In the **Add anchor tag** page that is displayed, choose the floor beacon by doing one of the following:
   - In the **Claimed Beacon** text field, you can type the first few letters of the floor beacon and choose the correct one from the drop-down that appears.
   - From the **Claimed Beacon** drop-down list, you can choose the floor beacon that you want to configure as a location anchor.

DETAILED STEPS

Step 1 From the Cisco Spaces dashboard, navigate to **IoT Services > Device Management > Devices**.

Step 2 Click the **Floor Beacons** tab and click **Claimed Beacons**. Select a floor beacon of your choice to view details. The **Anchor Tag** field indicates if the beacon has a location tag that is associated with it. Close the details page.

Figure 49: Anchor Tag



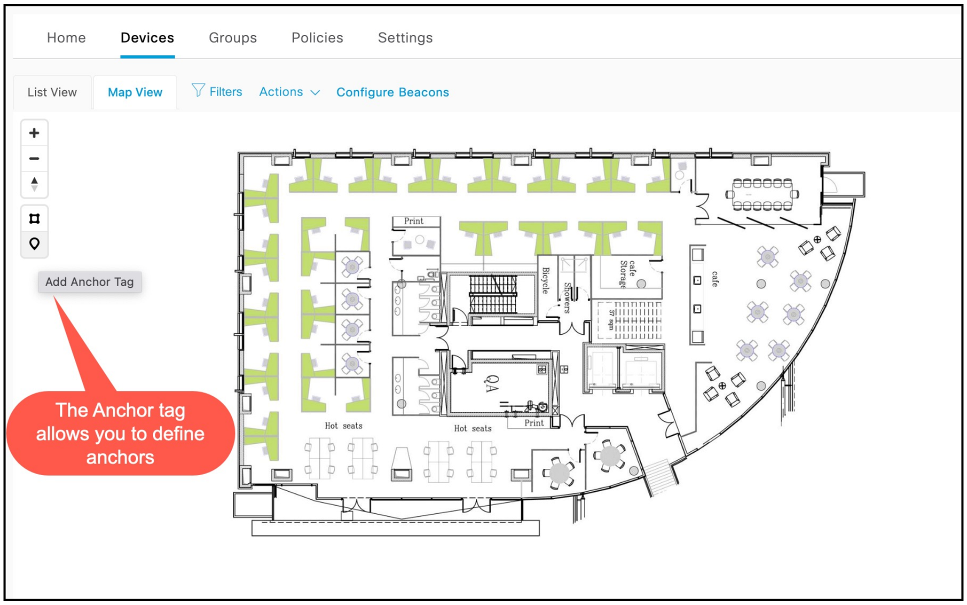
Click a claimed beacon to see whether an Anchor tag has been specified.

Base Mac Address - f9:af:b0:21:3b:e1

Mac Address	f9:af:b0:21:3b:e1
Mac Address Type	-
Name	81r30003
Claimed At	Jan 19th, 2022 11:38:14 PM 5 months ago
Anchor Tag	✖ No
Vendor Id	SMSD
Make	SSD002_02
Order Id	SMSD-4HNZY-1

Step 3 Click **Map View** and navigate to the required floor. From the list of icons in the left pane, click the **Add Anchor Tag.**

Figure 50: Adding Location Anchor in Map View

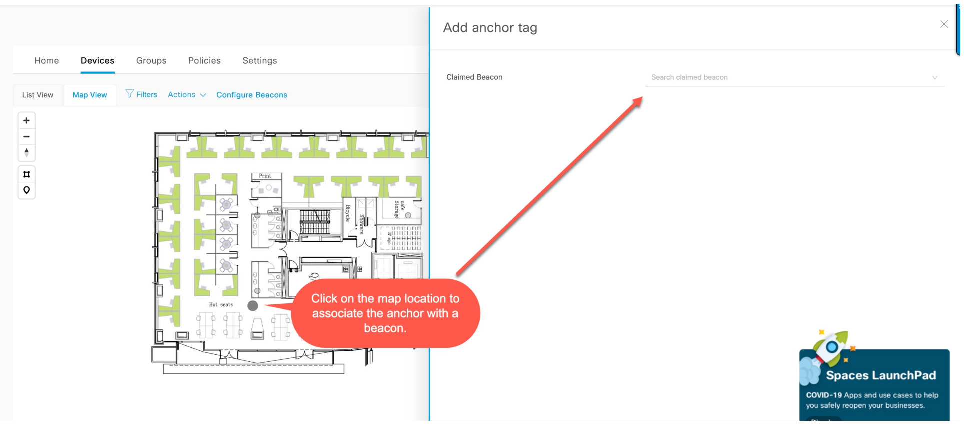


The Anchor tag allows you to define anchors

Step 4 Click the position on the map where you want to configure the location anchor. In the **Add anchor tag** page that is displayed, choose the floor beacon by doing one of the following:

- In the **Claimed Beacon** text field, you can type the first few letters of the floor beacon and choose the correct one from the drop-down that appears.
- From the **Claimed Beacon** drop-down list, you can choose the floor beacon that you want to configure as a location anchor.

Figure 51: Position Anchor Tag

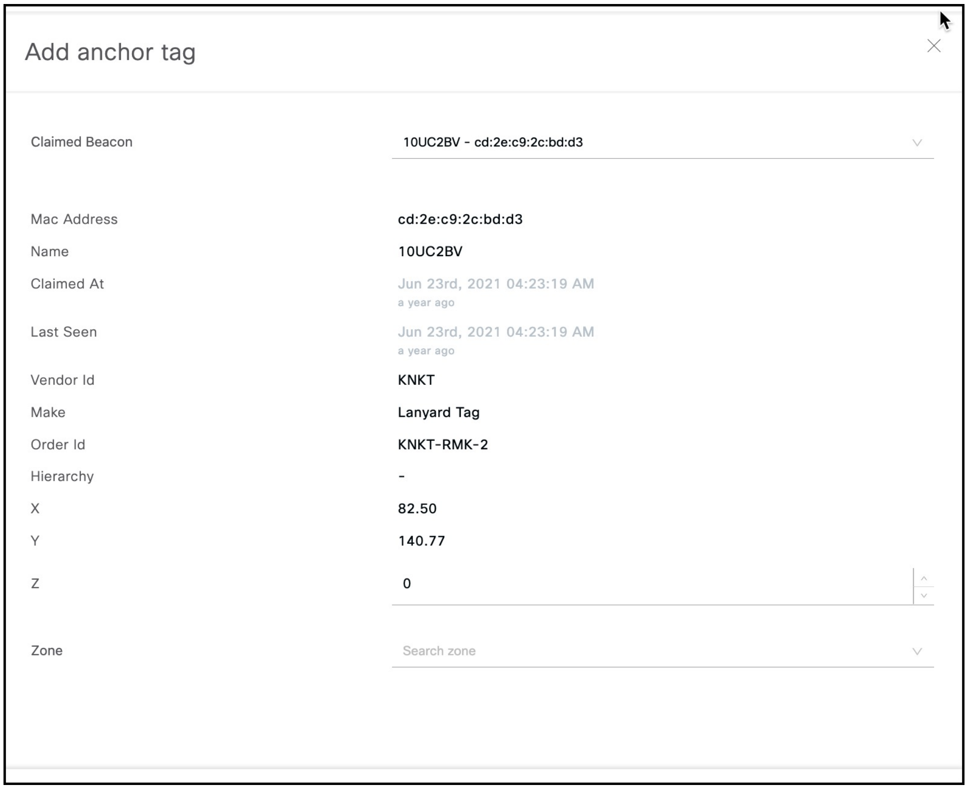


Add anchor tag

Claimed Beacon — Search claimed beacon

Click on the map location to associate the anchor with a beacon.

Figure 52: Configure Claimed Beacon as Location Anchor



Add anchor tag

Claimed Beacon	10UC2BV - cd:2e:c9:2c:bd:d3
Mac Address	cd:2e:c9:2c:bd:d3
Name	10UC2BV
Claimed At	Jun 23rd, 2021 04:23:19 AM a year ago
Last Seen	Jun 23rd, 2021 04:23:19 AM a year ago
Vendor Id	KNKT
Make	Lanyard Tag
Order Id	KNKT-RMK-2
Hierarchy	-
X	82.50
Y	140.77
Z	0
Zone	Search zone

Once you configure a location anchor, you can use Firehose events to gather location anchor information for wayfinding.

CHAPTER 8

AP as a Sensor

AP as a Sensor

You can now configure the following access points as sensors.

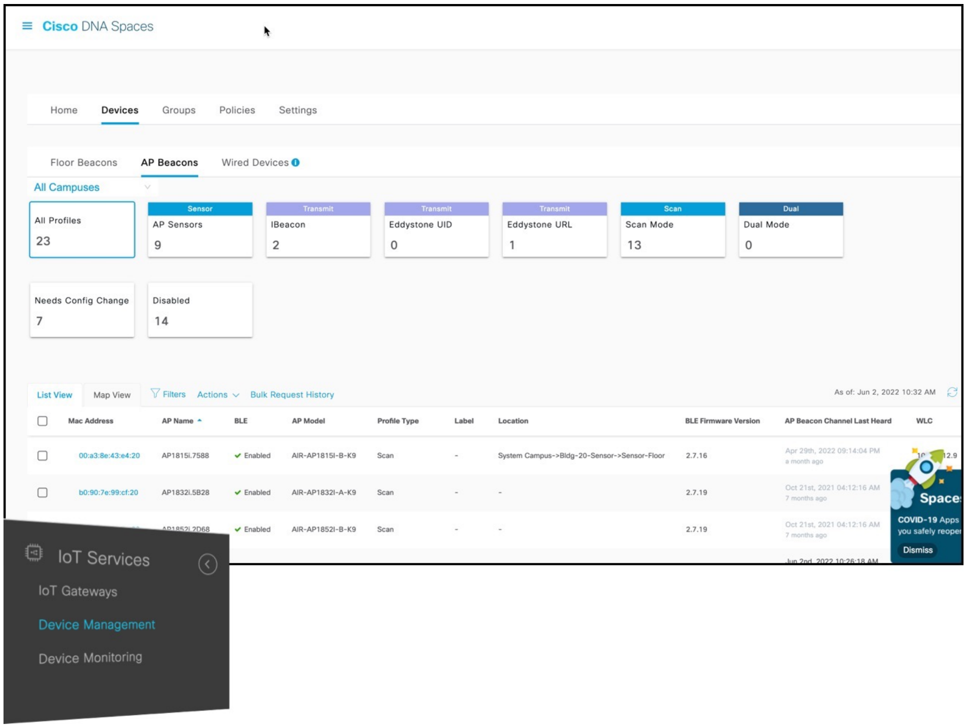
Once configured as a sensor, you can collect telemetry data using this AP. The following sensor values can be configured:

- Temperature
- Humidity
- Total volatile organic compound
- Ethanol
- Carbon Dioxide
- Indoor air quality

Enabling or Disabling an AP Sensor

Step 1 Navigate to Cisco Spaces: IoT Services > **Device Management** > **Devices** > **AP Beacons** > **Sensor**.

Figure 53: AP as a Sensor



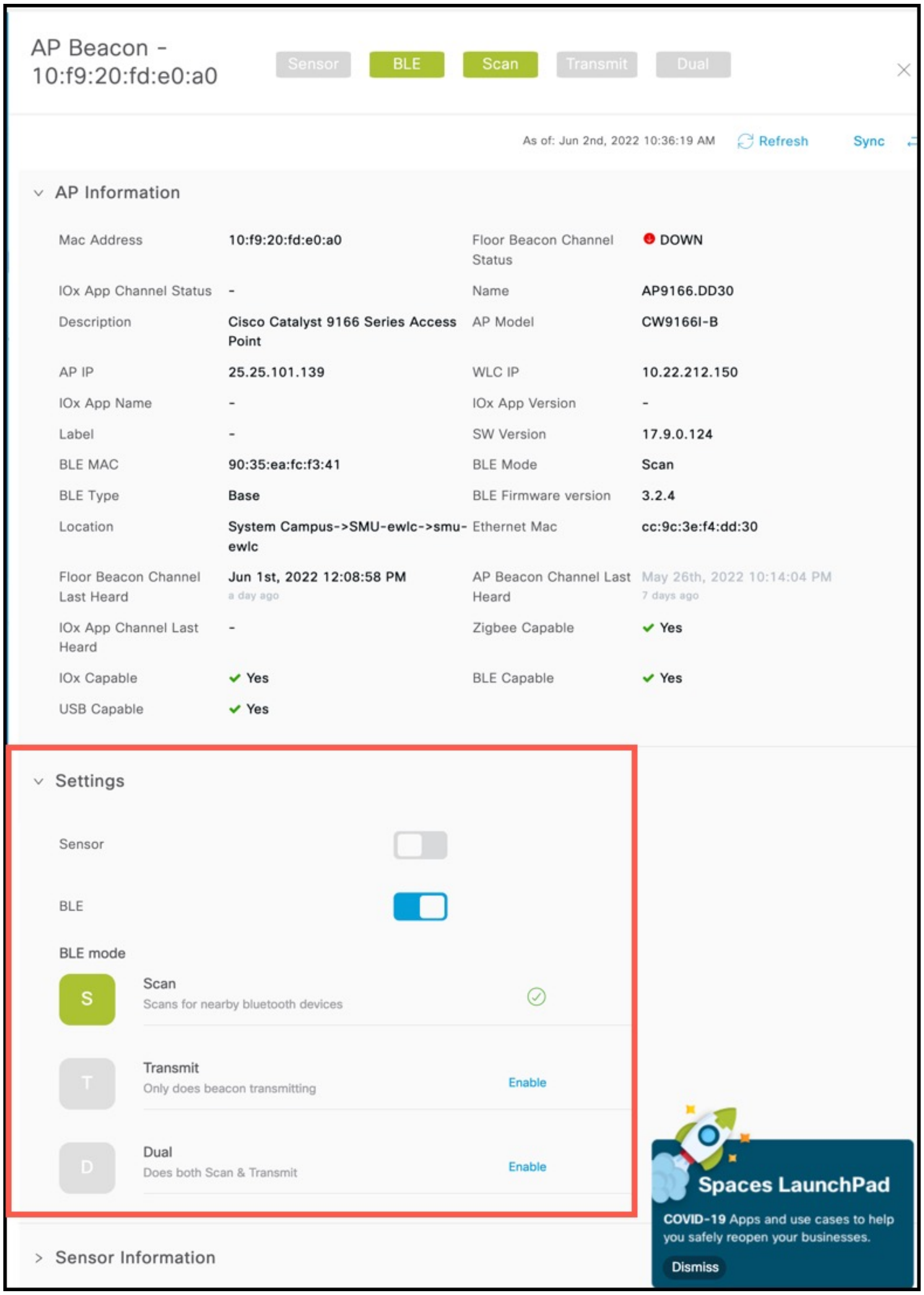
☐	Mac Address	AP Name	BLE	AP Model	Profile Type	Label	Location	BLE Firmware Version	AP Beacon Channel Last Heard	WLC
☐	00:a3:8e:43:e4:20	AP1815i.7588	✓ Enabled	AIR-AP1815I-B-K9	Scan	-	System Campus->Bldg-20-Sensor->Sensor-Floor	2.7.16	Apr 29th, 2022 09:14:04 PM a month ago	10 12.9
☐	b0:90:7e:99:cf:20	AP1832i.5B28	✓ Enabled	AIR-AP1832I-A-K9	Scan	-	-	2.7.19	Oct 21st, 2021 04:12:16 AM 7 months ago	
		AP1852i.2D68	✓ Enabled	AIR-AP1852I-B-K9	Scan	-	-	2.7.19	Oct 21st, 2021 04:12:16 AM 7 months ago	
									Jun 2nd, 2022 10:26:18 AM	

Step 2 Click the AP that you want to configure as a sensor.

The AP Beacons details page opens.

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

Figure 54: Enabling or Disabling AP as a Sensor



AP Beacon - 10:f9:20:fd:e0:a0

As of: Jun 2nd, 2022 10:36:19 AM

AP Information

Mac Address	10:f9:20:fd:e0:a0	Floor Beacon Channel Status	● DOWN
IOx App Channel Status	-	Name	AP9166.DD30
Description	Cisco Catalyst 9166 Series Access Point	AP Model	CW9166I-B
AP IP	25.25.101.139	WLC IP	10.22.212.150
IOx App Name	-	IOx App Version	-
Label	-	SW Version	17.9.0.124
BLE MAC	90:35:ea:fc:f3:41	BLE Mode	Scan
BLE Type	Base	BLE Firmware version	3.2.4
Location	System Campus->SMU-ewlc->smu-ewlc	Ethernet Mac	cc:9c:3e:f4:dd:30
Floor Beacon Channel Last Heard	Jun 1st, 2022 12:08:58 PM a day ago	AP Beacon Channel Last Heard	May 26th, 2022 10:14:04 PM 7 days ago
IOx App Channel Last Heard	-	Zigbee Capable	✓ Yes
IOx Capable	✓ Yes	BLE Capable	✓ Yes
USB Capable	✓ Yes		

Settings

Sensor

BLE

BLE mode

S Scan
Scans for nearby bluetooth devices ✓

T Transmit
Only does beacon transmitting Enable

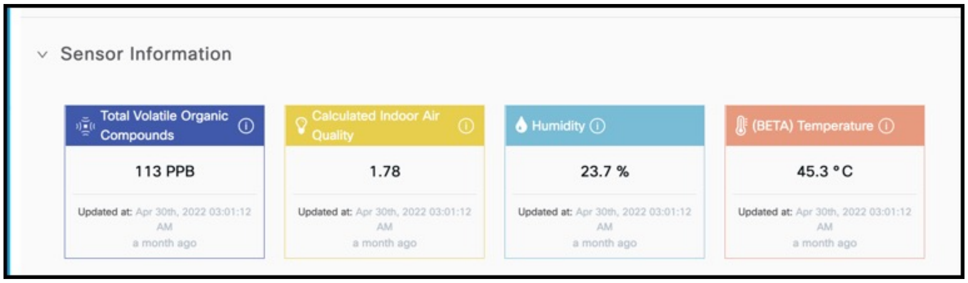
D Dual
Does both Scan & Transmit Enable

Sensor Information

Viewing Sensor Information

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

Figure 55: Viewing Sensor Information



Sensor Information

Total Volatile Organic Compounds

113 PPB

Updated at: Apr 30th, 2022 03:01:12 AM
a month ago

Calculated Indoor Air Quality

1.78

Updated at: Apr 30th, 2022 03:01:12 AM
a month ago

Humidity

23.7 %

Updated at: Apr 30th, 2022 03:01:12 AM
a month ago

(BETA) Temperature

45.3 °C

Updated at: Apr 30th, 2022 03:01:12 AM
a month ago

PART III

Device Management

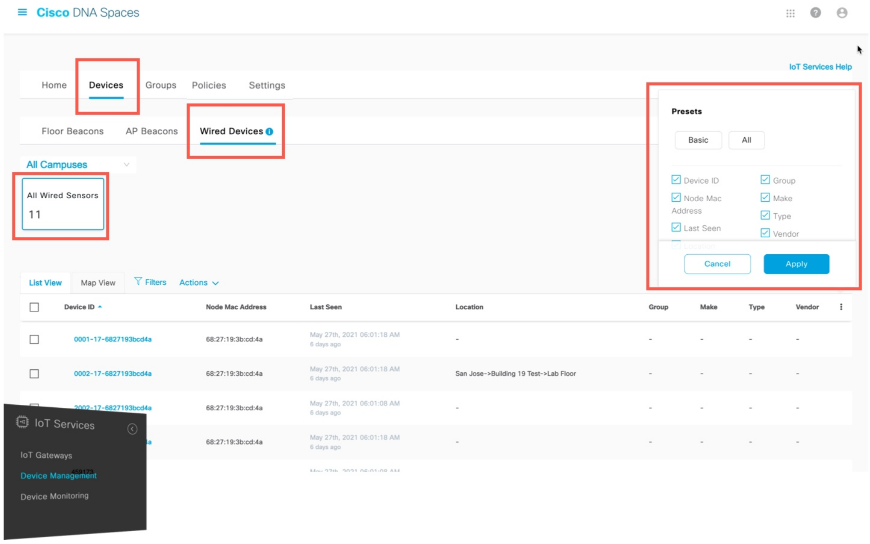
CHAPTER 9

Device Management

Dashboard View of Devices

Choose **IoT Services > Device Management > Devices** and select a device type (**Floor Beacons**, **AP Beacons**, **Wired Devices**) to view an overview of that device.

Figure 56: Dashboard View of Devices



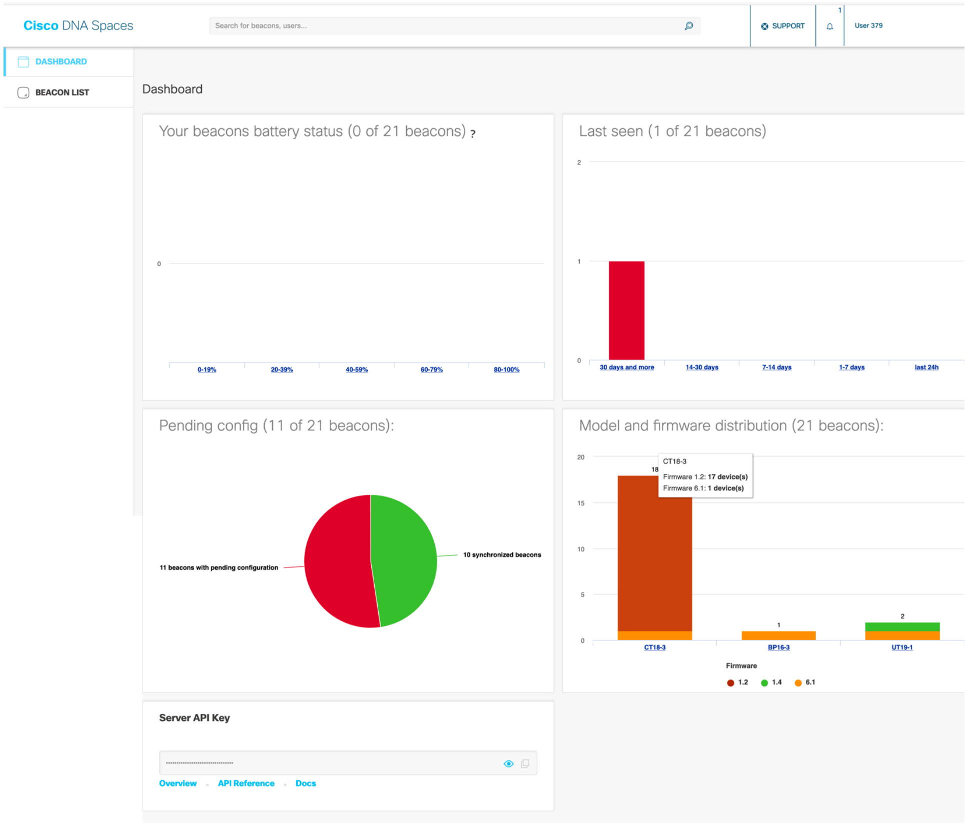
□	Device ID	Node Mac Address	Last Seen	Location	Group	Make	Type	Vendor
□	0001-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	San Jose->Building 19 Test->Lab Floor	-	-	-	-
	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 AM 6 days ago	-	-	-	-	-
	[illegible]	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-

Opening Cisco-Partnered Websites from IoT Services for Configuring AP Beacons

The Cisco-partnered website opened from **IoT Services** > **Device Management** > **Devices** > **Floor Beacons** > **Configure Beacons** is referred to as the Device Manager in this document. Kontakt.io is one such Device Manager.

The Kontakt.io Device Manager dashboard gives you a general overview of your beacon infrastructure. All beacons claimed by IoT Services are visible on the Kontakt.io 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 57: The Kontakt.io Device Manager Dashboard


Cisco DNA Spaces
Search for beacons, users...
SUPPORT
1
User 379
DASHBOARD
BEACON LIST
Dashboard
Your beacons battery status (0 of 21 beacons) ?
0
0-19%
20-39%
40-59%
60-79%
80-100%
Last seen (1 of 21 beacons)
2
1
0
30 days and more
14-30 days
7-14 days
1-7 days
last 24h
Pending config (11 of 21 beacons):
11 beacons with pending configuration
10 synchronized beacons
Model and firmware distribution (21 beacons):
20
15
10
5
0
18
1
2
CT18-3
Firmware 1.2: 17 device(s)
Firmware 6.1: 1 device(s)
CT18-3
BP16-3
UT19-1
Firmware
● 1.2
● 1.4
● 6.1
Server API Key
Overview
API Reference
Docs

Categorizing 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 by the group.

The advantages of manual groups are as follows:

- Policies are applied to groups.

- Firehose APIs can filter devices by these groups.
- In the Cisco Spaces: IoT Services dashboard, you can filter devices by groups.

Step 1 In the Cisco Spaces: IoT Services dashboard, navigate to **Device Management** > **Groups**.

Step 2 In the **Add a Group** page, enter **Group Name**, **Description**, and choose **Manual Group** and click **Next**.

Step 3 Click **Create a new group**, and provide a group name and description. Click **Next**.

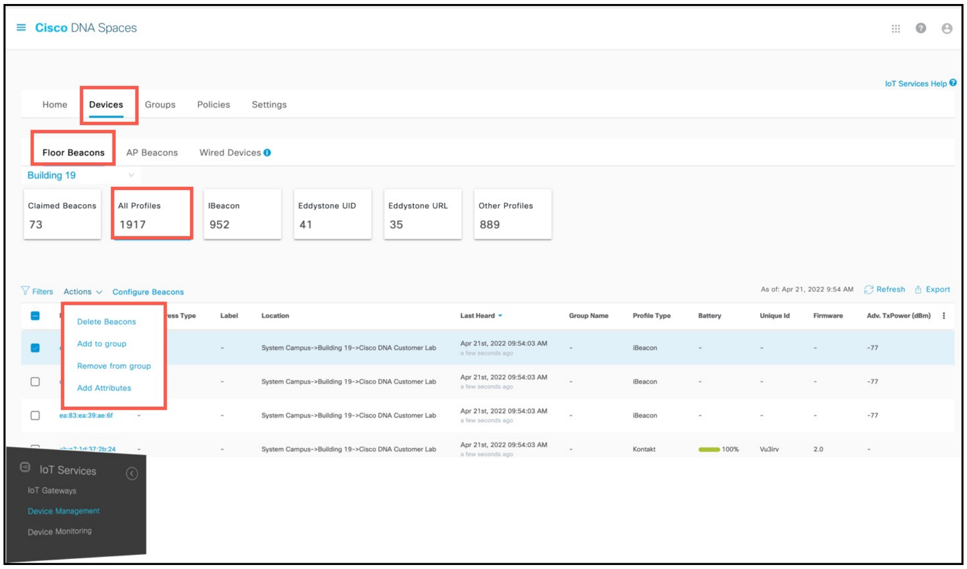
Step 4 In the **Add a group** page that is displayed, choose the type of device (Wireless or Wired), and select the devices to add to this group.

Step 5 Click **Create group**. In the **Done! You have Created a Group** page, click **Close**, or **Create another group**.

On the **Groups** tab, you can see the group that you created. Click the group to see the devices in the group. You can also edit the group from this page.

In the **Devices** > **Floor Beacons** > **All Profiles** tab, you can select devices and click **Actions** to add or remove device(s) to groups.

Figure 58: AddingDevices to a Manual Group from the Devices tab



Claimed Beacons	All Profiles	IBeacon	Eddystone UID	Eddystone URL	Other Profiles
73	1917	952	41	35	889

	ess Type	Label	Location	Last Heard	Group Name	Profile Type	Battery	Unique Id	Firmware	Adv. TxPower (dBm)
		-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
		-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
ea:83:ea:39:ae:6f	-	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
eb:e7:1d:37:2b:24	-	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	Kontakt	100%	Vu3irv	2.0	-

Categorizing Devices into Groups (Dynamic Groups)

You can configure dynamic groups using parameters like MAC prefix, vendor code, and location hierarchy (floor, building, zone, and so on). New devices are automatically added to the group based on these configured parameters.

The advantages of dynamic groups are as follows:

- 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 Services dashboard, you can filter devices by groups.

Step 1 In the Cisco Spaces: IoT Services dashboard, navigate to **Device Management** > **Groups**.

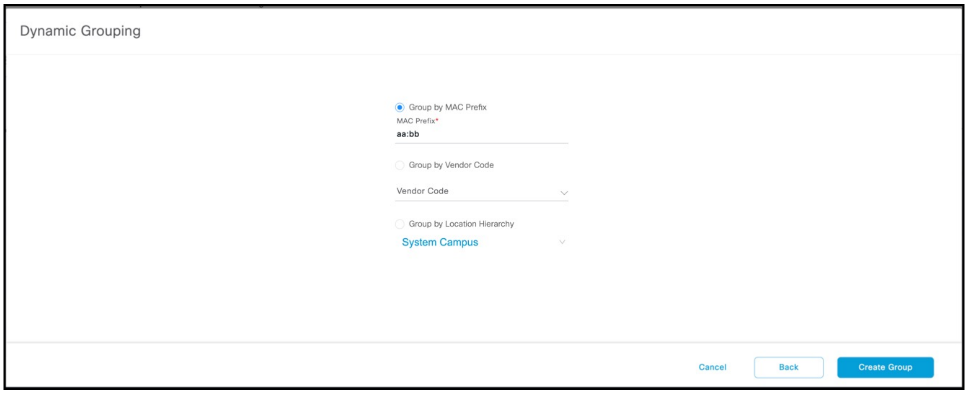
Step 2 In the **Add a Group** page, enter **Group Name**, **Description**, and choose **Dynamic Group** and click **Next.**

Step 3 Click **Create a new group**, and provide a group name and description. Click **Next**.

Step 4 In the **Dynamic Grouping** page that is displayed, configure the parameter for this group.

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

Figure 59: Group by MAC Prefix



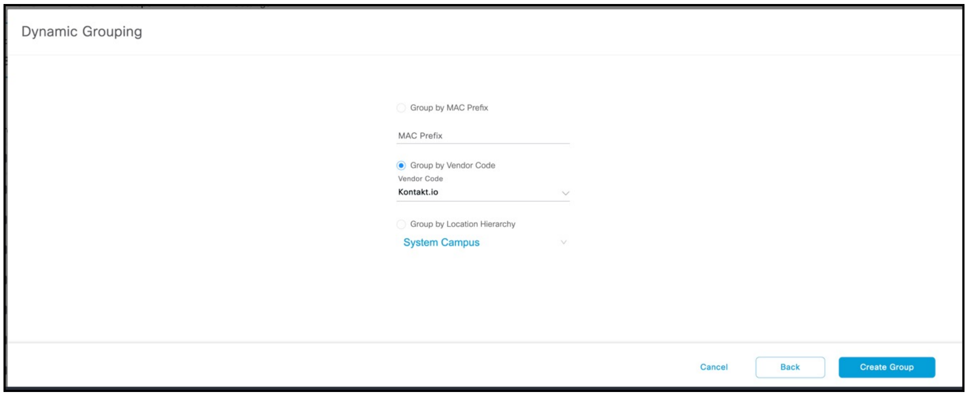
Dynamic Grouping

● Group by MAC Prefix
MAC Prefix*
aa:bb

○ Group by Vendor Code
Vendor Code

○ Group by Location Hierarchy
System Campus

Figure 60: Group by Vendor Code



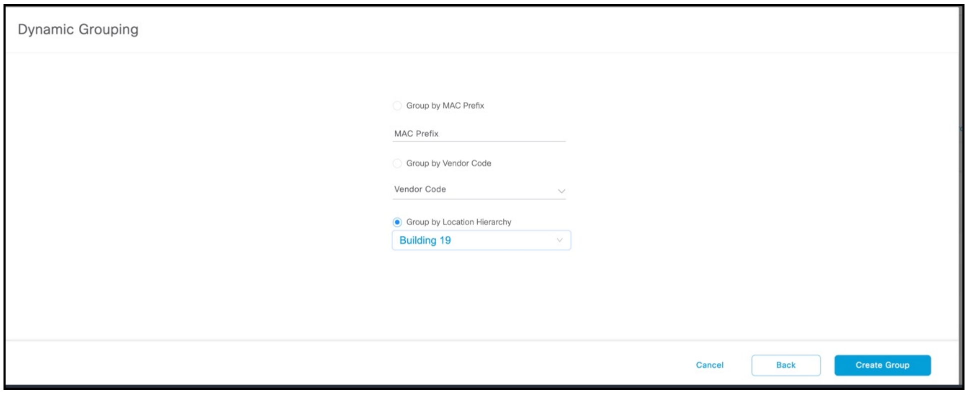
Dynamic Grouping

○ Group by MAC Prefix
MAC Prefix

● Group by Vendor Code
Vendor Code
Kontakt.io

○ Group by Location Hierarchy
System Campus

Figure 61: Group by Location Hierarchy



Dynamic Grouping

○ Group by MAC Prefix

MAC Prefix

○ Group by Vendor Code

Vendor Code

● Group by Location Hierarchy

Building 19

Step 5 Click **Create group**. In the **Done! You have Created a Group** page, click **Close**, or **Create another group**.

On the **Groups** tab, you can see the group that you created. Click the group to see the devices in the group. You can also edit the group from this page.

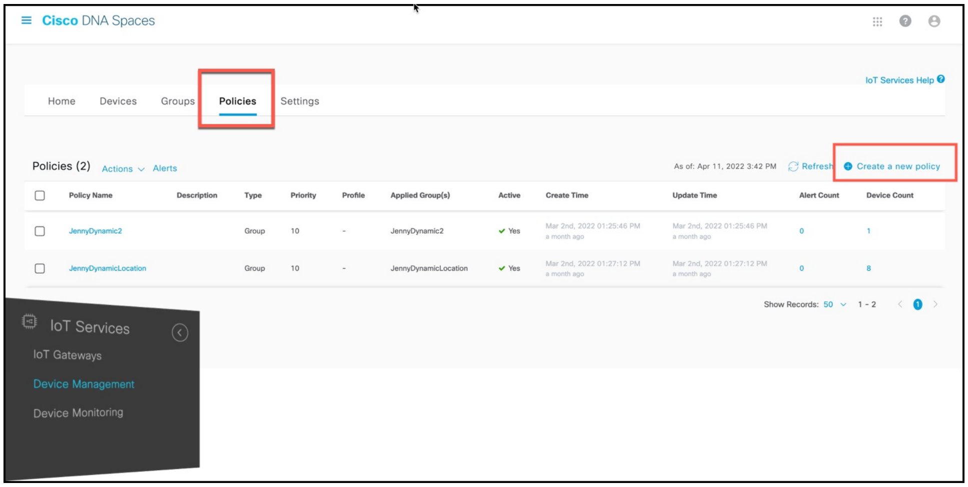
What to do next

You can delete a device by selecting the check box of the group and then selecting **Actions** > **Delete Group**.

Applying Policies to Beacons

Step 1 From the Cisco Spaces: IoT Services dashboard, click **Device Management** > **Policies** and then **Create a new policy**.

Figure 62: Creating a New Policy



Policies (2)

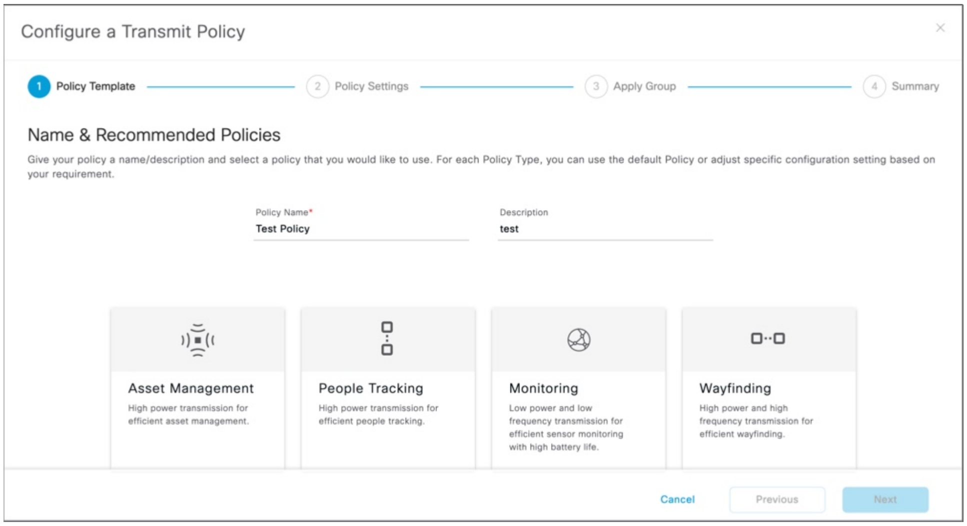
As of: Apr 11, 2022 3:42 PM

□	Policy Name	Description	Type	Priority	Profile	Applied Group(s)	Active	Create Time	Update Time	Alert Count	Device Count
□	JennyDynamic2		Group	10	-	JennyDynamic2	✓ Yes	Mar 2nd, 2022 01:25:46 PM a month ago	Mar 2nd, 2022 01:25:46 PM a month ago	0	1
□	JennyDynamicLocation		Group	10	-	JennyDynamicLocation	✓ Yes	Mar 2nd, 2022 01:27:12 PM a month ago	Mar 2nd, 2022 01:27:12 PM a month ago	0	8

Show Records: 50 1 - 2 1

Step 2 From the **Configure a Transmit Policy** page that opens, provide a policy name, a description, and choose one of the four policy types.

Figure 63: Choosing One of Four Policies



Configure a Transmit Policy

Name & Recommended Policies

Give your policy a name/description and select a policy that you would like to use. For each Policy Type, you can use the default Policy or adjust specific configuration setting based on your requirement.

Policy Name*: Test Policy

Description: test

Asset Management: High power transmission for efficient asset management.

People Tracking: High power transmission for efficient people tracking.

Monitoring: Low power and low frequency transmission for efficient sensor monitoring with high battery life.

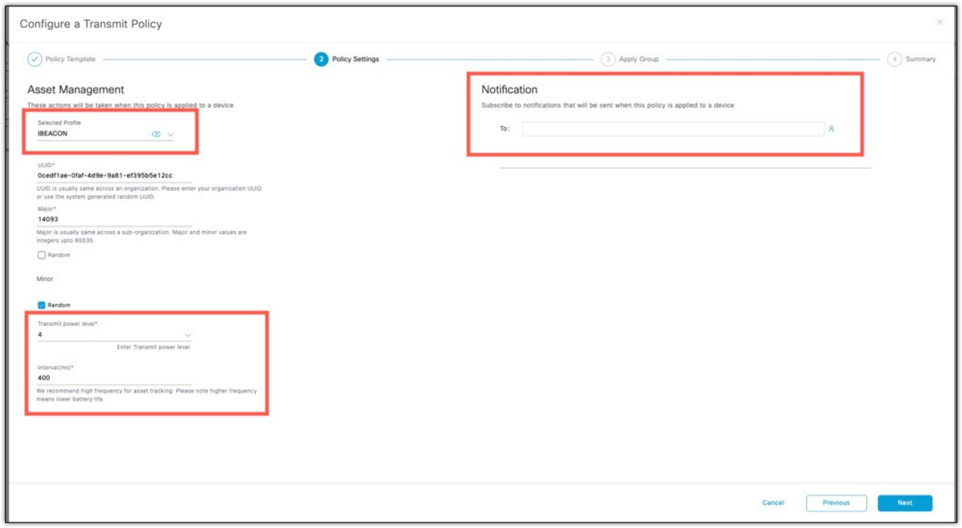
Wayfinding: High power and high frequency transmission for efficient wayfinding.

Table 2: Types of Transmit Policy

Policy Type	Transmit Power Level	Interval (ms)
Asset Management: High-Power transmission for efficient asset management	4	400
People Tracking: High-Power transmission for efficient asset management	0	300
Monitoring: Low power and low frequency transmission for efficient sensor monitoring and high battery life.	-8	2000
Wayfinding: High power and high frequence transmission for efficient wayfinding.	4	100

Step 3 From the **Configure a Transmit Policy** page that opens, enter email addresses in the **Notification** field. When this policy is applied to any device, the addresses are notified.

Figure 64: Configure a Transmit Policy



Asset Management

These actions will be taken when this policy is applied to a device

Selected Profile: IBEACON

UUID*: 0cedf1ae-0faf-4d9e-9a81-ef395b5e12cc

UUID is usually same across an organization. Please enter your organization UUID or use the system generated random UUID.

Major*: 14093

Major is usually same across a sub-organization. Major and minor values are integers upto 65535.

□ Random

Minor

☑ Random

Transmit power level*: 4

Enter Transmit power level

Interval(ms)*: 400

We recommend high frequency for asset tracking. Please note higher frequency means lower battery life.

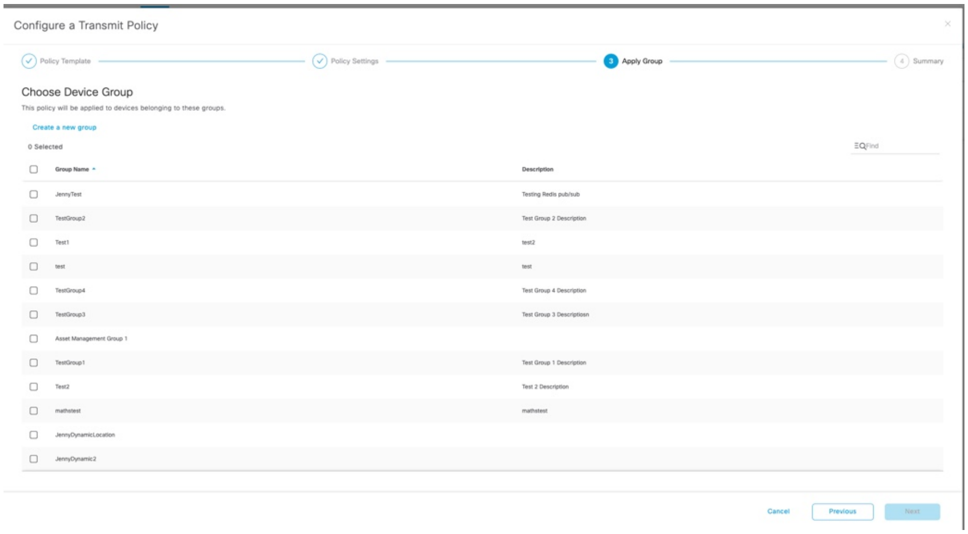
Notification

Subscribe to notifications that will be sent when this policy is applied to a device

To:

Step 4 From the **Choose Device Group** page, choose a device group. The policy is automatically applied to any device added to this device group.

Figure 65: Choosing a Device Group for Dynamic Policy Application



Choose Device Group

This policy will be applied to devices belonging to these groups.

0 Selected

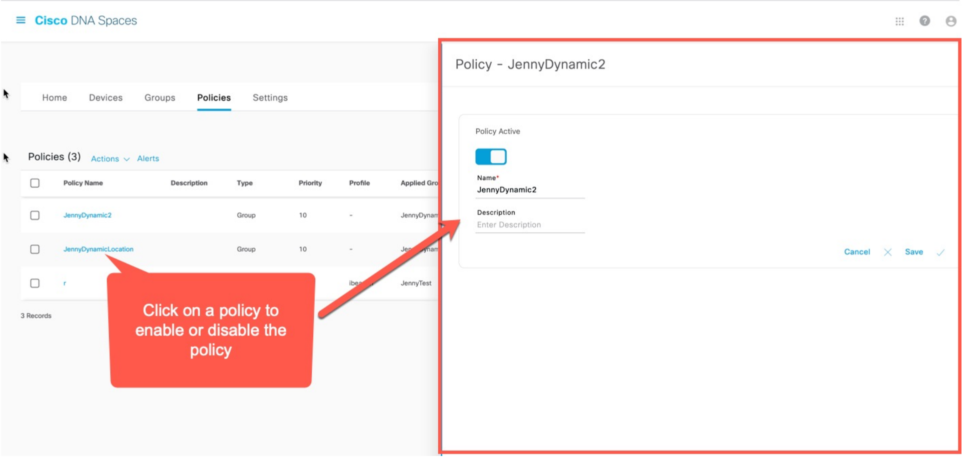
□	Group Name ▴	Description
□	JennyTest	Testing Redis pub/sub
□	TestGroup2	Test Group 2 Description
□	Test1	test2
□	test	test
□	TestGroup4	Test Group 4 Description
□	TestGroup3	Test Group 3 Descriptiosn
□	Asset Management Group 1	
□	TestGroup1	Test Group 1 Description
□	Test2	Test 2 Description
□	mathstest	mathstest
□	JennyDynamicLocation	
□	JennyDynamic2	

Step 5 Review the summary and click **Create**. Then click **Close**.

Step 6 In the **Policies** page, you can do any of the following:

- Click a policy to enable or disable the policy.
- From the **Device** column of a policy, click the value to see the list of devices on which the policy is applied.
- From the **Alert Count** column of a policy, click the value to see the list of alerts for the policy.

Figure 66: Enabling or Disabling a Policy



Cisco DNA Spaces

Home Devices Groups **Policies** Settings

Policies (3) Actions Alerts

□	Policy Name	Description	Type	Priority	Profile	Applied Gro
□	JennyDynamic2		Group	10	-	JennyDynam
□	JennyDynamicLocation		Group	10	-	JennyDynam
□	r				ibea	JennyTest

3 Records

Policy - JennyDynamic2

Policy Active

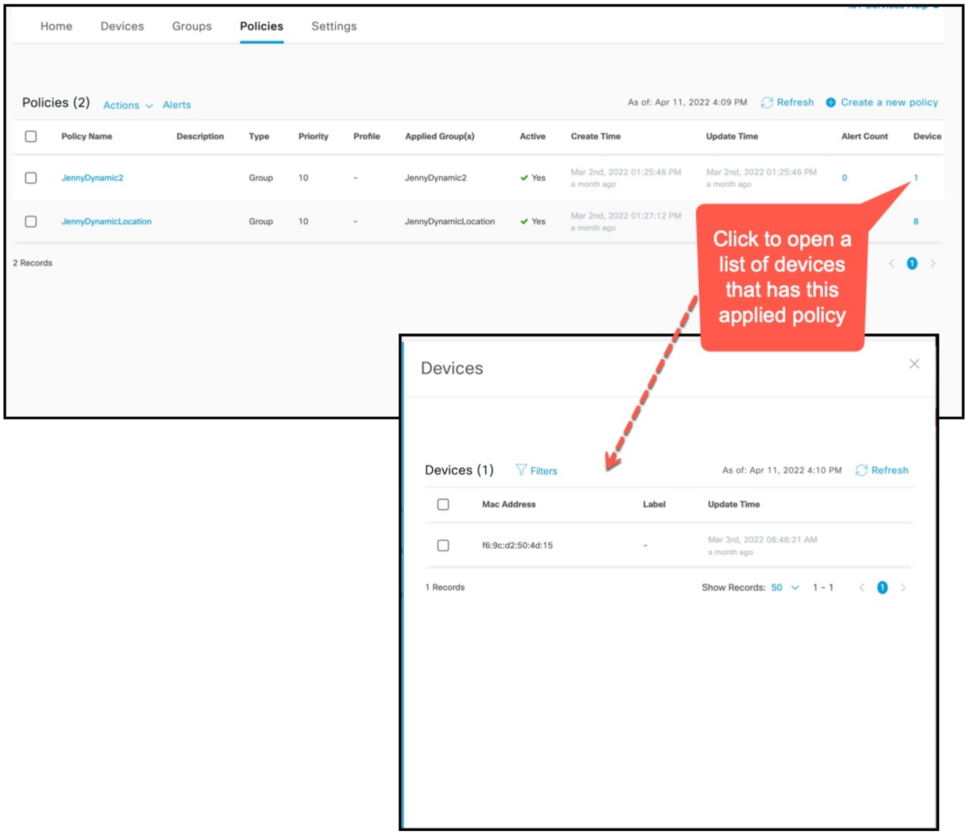
Name* JennyDynamic2

Description Enter Description

Cancel Save

Click on a policy to enable or disable the policy

Figure 67: Viewing Devices on Which a Policy Is Applied



Home Devices Groups **Policies** Settings

Policies (2) Actions Alerts As of: Apr 11, 2022 4:09 PM Refresh Create a new policy

□	Policy Name	Description	Type	Priority	Profile	Applied Group(s)	Active	Create Time	Update Time	Alert Count	Device
□	JennyDynamic2		Group	10	-	JennyDynamic2	✓ Yes	Mar 2nd, 2022 01:25:46 PM a month ago	Mar 2nd, 2022 01:25:46 PM a month ago	0	1
□	JennyDynamicLocation		Group	10	-	JennyDynamicLocation	✓ Yes	Mar 2nd, 2022 01:27:12 PM a month ago			8

2 Records

Click to open a list of devices that has this applied policy

Devices

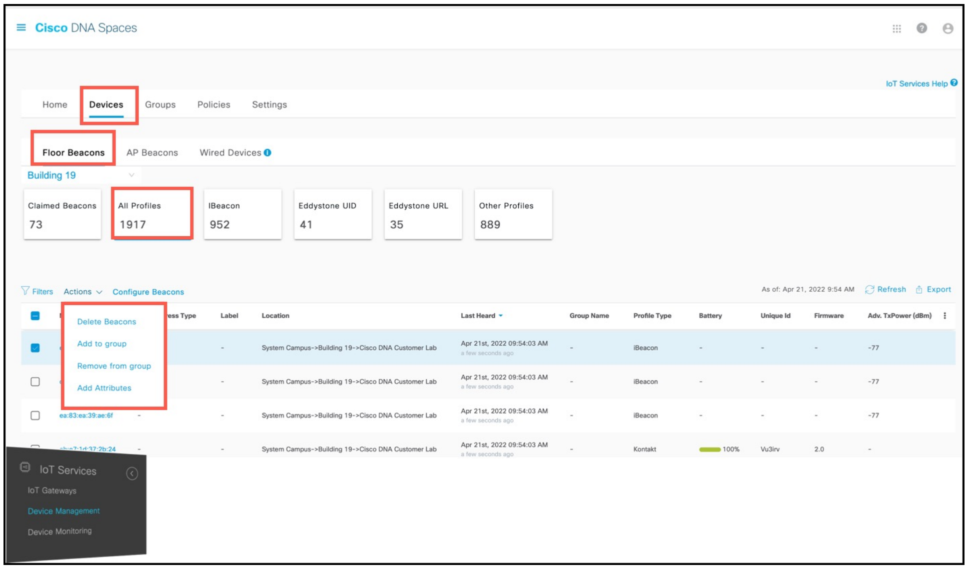
Devices (1) Filters As of: Apr 11, 2022 4:10 PM Refresh

□	Mac Address	Label	Update Time
□	f6:9c:d2:50:4d:15	-	Mar 3rd, 2022 06:48:21 AM a month ago

1 Records Show Records: 50 1 - 1

You can now apply this policy to a static or dynamic group. If the policy is applied on a static group, you can assign devices to the group, and the policy is automatically applied. To do this, navigate to the Cisco Spaces: IoT Services dashboard, click **Device Management** > **Devices** and then **Floor Beacons** > **All Profiles**. Select the devices and click **Actions** > **Add to group**.

Figure 68: Creating a New Policy



Claimed Beacons	All Profiles	IBeacon	Eddystone UID	Eddystone URL	Other Profiles
73	1917	952	41	35	889

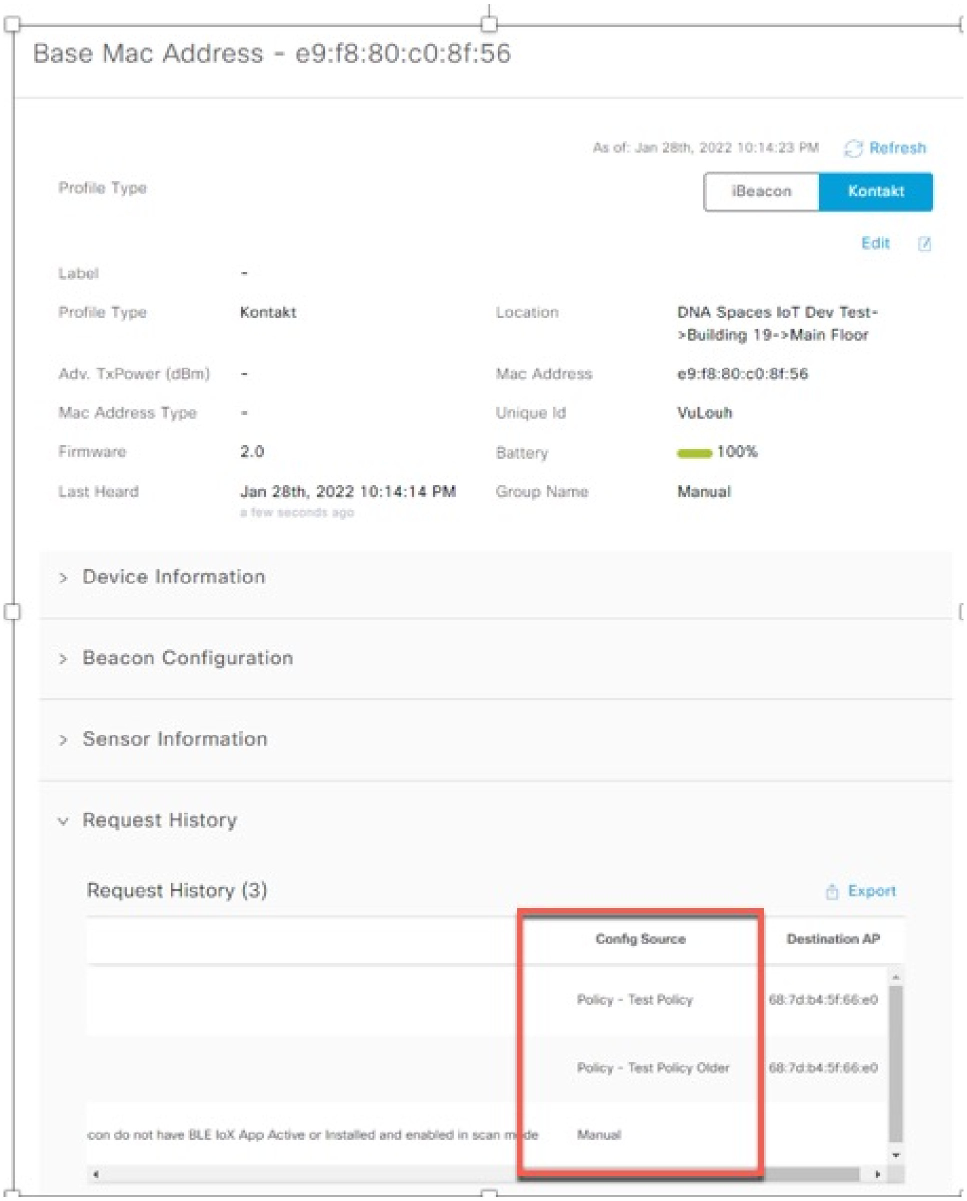
☐		ess Type	Label	Location	Last Heard	Group Name	Profile Type	Battery	Unique Id	Firmware	Adv. TxPower (dBm)
☑			-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
☐			-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
☐	ea:83:ea:39:ae:6f	-	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77
☐	ab:a7:1d:37:2b:24	-	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	Kontakt	100%	Vu3irv	2.0	-

What to do next

You can verify if a policy is applied on a device by checking the request history in the device details. In the **Request History** page, refer to the **Config Source** column.

- **Manual**: Policy change that is made by Cisco Spaces or partner dashboard.
- **<Policy Name >**: Policy has been applied dynamically to the device.

Figure 69: Config Source: Policy



Base Mac Address - e9:f8:80:c0:8f:56

As of: Jan 28th, 2022 10:14:23 PM Refresh

Profile Type: iBeacon | Kontakt

Edit

Label	-		
Profile Type	Kontakt	Location	DNA Spaces IoT Dev Test->Building 19->Main Floor
Adv. TxPower (dBm)	-	Mac Address	e9:f8:80:c0:8f:56
Mac Address Type	-	Unique Id	VuLouh
Firmware	2.0	Battery	100%
Last Heard	Jan 28th, 2022 10:14:14 PM a few seconds ago	Group Name	Manual

> Device Information

> Beacon Configuration

> Sensor Information

Request History

Request History (3) Export

	Config Source	Destination AP
	Policy - Test Policy	68:7d:b4:5f:66:e0
	Policy - Test Policy Older	68:7d:b4:5f:66:e0
con do not have BLE IoX App Active or Installed and enabled in scan mode	Manual	

Filtering Devices

While Cisco Spaces: IoT Services 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 Services dashboard using types of MAC addresses. Filtering is currently at the cloud level and not at AP-level. Once filtered, these devices do not appear in the following locations;

- Cisco Spaces: Detect and Locate
- Cisco Spaces: IoT Services

- Output of Firehose API calls

You can filter out devices based on the following MAC address types.

- **Enable Public MAC**: Allows global, fixed MAC addresses that are registered with the IEEE Registration Authority, which does not change during the device's lifetime.
- **Enable Random Static MAC**: Allows random static MAC address, which is a random number generated every time that the device boots up or a value that stays the same for the device's lifetime. However, it does not change within one power cycle of the device.
- **Enable Random Private MAC**: Allows random private MAC addresses of two types:
  - **Resolvable**: These are generated from an identity resolving key (IRK) and a random number. They can be changed often (even during the lifetime of a connection) and prevents an unknown scanning device from identifying and tracking the device. Only scanning devices that possess the IRK distributed by 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.

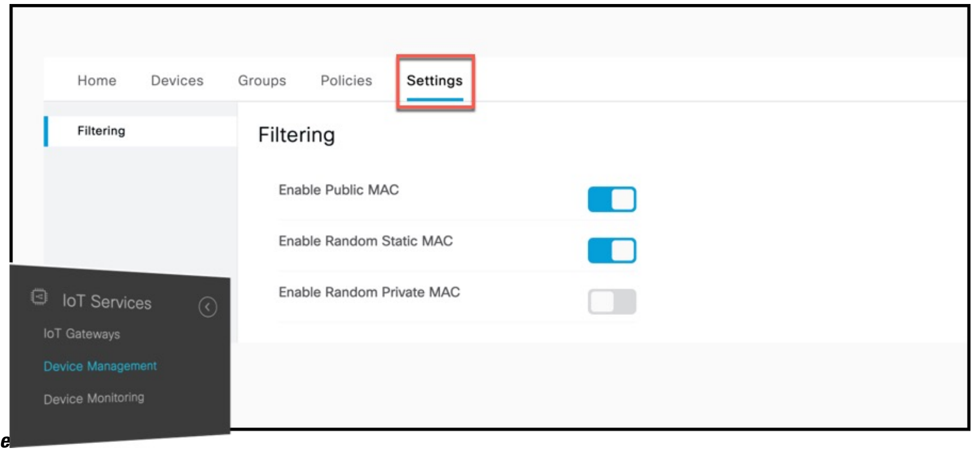
SUMMARY STEPS

1. Navigate to **Device Management** > **Settings**.

DETAILED STEPS

Navigate to **Device Management** > **Settings**.

Figure 70: Filtering Devices by MAC Address



Filtering

Enable Public MAC ●
Enable Random Static MAC ●
Enable Random Private MAC ○

Type

PART IV

Device Monitoring

CHAPTER 10

Device Monitoring

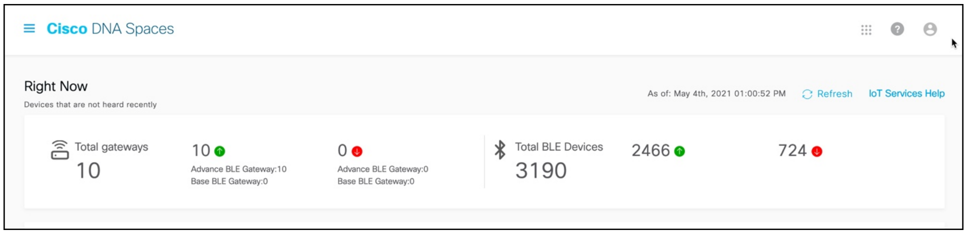
From the IoT Services > **Device Monitoring** page, you can monitor all the IoT devices and gateways, and also get a one-shot categorized view of devices according to their battery life and last heard time.

Right Now

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 dot, and the number of unreachable gateways counted under the red dot.

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 dot, and the number of unreachable devices counted under the red dot.

Figure 71: Right Now



Cisco DNA Spaces

Right Now

Devices that are not heard recently

As of: May 4th, 2021 01:00:52 PM

Refresh

IoT Services Help

Total gateways			Total BLE Devices		
10	10 ● Advance BLE Gateway:10 Base BLE Gateway:0	0 ● Advance BLE Gateway:0 Base BLE Gateway:0	3190	2466 ●	724 ●

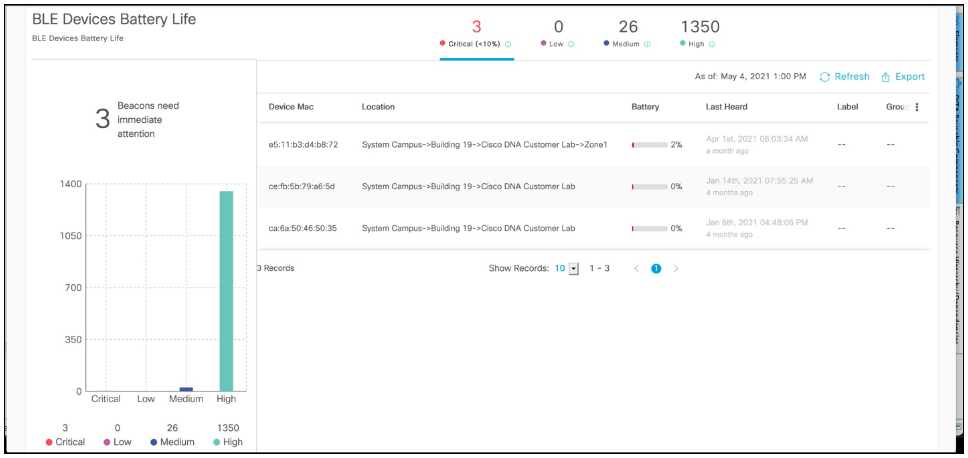
BLE Devices Battery Life

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.



BLE Devices Battery Life

BLE Devices Battery Life

3 ● Critical (<10%) | 0 ● Low | 26 ● Medium | 1350 ● High

3 Beacons need immediate attention

As of: May 4, 2021 1:00 PM

Device Mac	Location	Battery	Last Heard	Label	Group
e5:11:b3:d4:b8:72	System Campus->Building 19->Cisco DNA Customer Lab->Zone1	2%	Apr 1st, 2021 06:03:34 AM a month ago	--	--
ce:fb:5b:79:a6:5d	System Campus->Building 19->Cisco DNA Customer Lab	0%	Jan 14th, 2021 07:55:25 AM 4 months ago	--	--
ca:6a:50:46:50:35	System Campus->Building 19->Cisco DNA Customer Lab	0%	Jan 6th, 2021 04:48:06 PM 4 months ago	--	--

3 Records

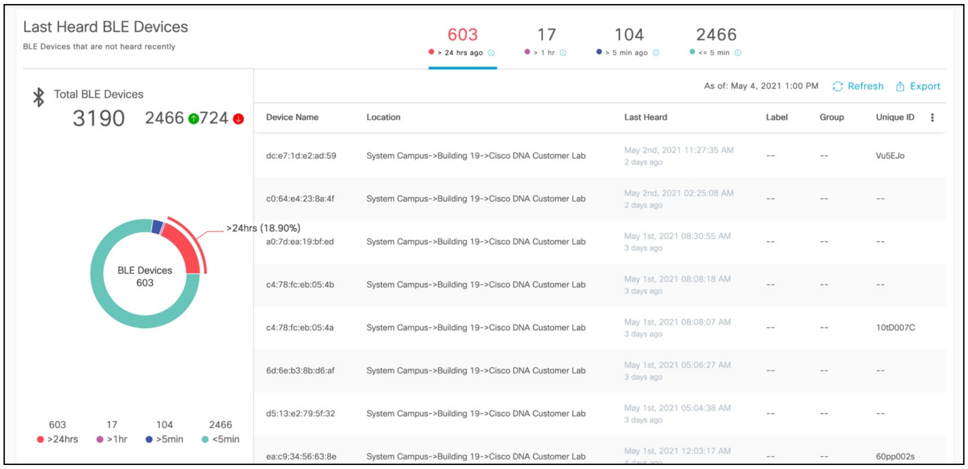
Show Records: 10 1 - 3

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 the following:

- 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 numbrs. 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

603	17	104	2466
● > 24 hrs ago	● > 1 hr	● > 5 min ago	● <= 5 min

Total BLE Devices

3190 2466 ↑ 724 ↓

As of: May 4, 2021 1:00 PM Refresh Export

Device Name	Location	Last Heard	Label	Group	Unique ID
dc:e7:1d:e2:ad:59	System Campus->Building 19->Cisco DNA Customer Lab	May 2nd, 2021 11:27:35 AM 2 days ago	--	--	Vu5EJo
c0:64:e4:23:8a:4f	System Campus->Building 19->Cisco DNA Customer Lab	May 2nd, 2021 02:25:08 AM 2 days ago	--	--	--
a0:7d:ea:19:bf:ed	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 08:30:55 AM 3 days ago	--	--	--
c4:78:fc:eb:05:4b	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 08:08:18 AM 3 days ago	--	--	--
c4:78:fc:eb:05:4a	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 08:08:07 AM 3 days ago	--	--	10tD007C
6d:6e:b3:8b:d6:af	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 05:06:27 AM 3 days ago	--	--	--
d5:13:e2:79:5f:32	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 05:04:38 AM 3 days ago	--	--	--
ea:c9:34:56:63:8e	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 12:03:17 AM 4 days ago	--	--	60pp002s

PART V

Troubleshooting

CHAPTER 11

Wireless Controller

Is BLE radio enabled on the controller?

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

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

```
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 is not shut down.

Reprovisioning IoT Services After Failover

Is there a streaming token for the gRPC connection on controller?

For the gRPC connection to work, there must be a gRPC streaming token on the controller.

Run the **show running-config | include ap cisco-dna** command on the controller.

```
controller# show running-config | include ap cisco-dna
ap cisco-dna token 0 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2MjUs
ImNpZCI6Mzc4NTc3ODI1NDI2NzIyNjUwMDAsImVwIjoiMTAuMzAuMTE0LjEwODo4MDAwIiwiaW
F0IjoxNTg1NzA2OTIxfQ.56vXfL1IGrss6TJZDQaWVarAoTWZsIhbe3tGVMEJNYk
```

The output includes the streaming token. You can compare this token with the token on the AP using the **show cloud connector key authentication** command and ensure that the two tokens match.

You can also view the encoded payload of the token by pasting the token into a decoder such as http://jwt.io/. Following is a sample payload data:

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

Is gRPC enabled in the AP Join Profile

This task shows you how to enable gRPC in the AP join profile. This is a required setting.

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
```

The command displays the default AP profile. If you want another profile, you can change it using the same command.

Verify that the profile includes the `cisco-dna grpc` command. The `cisco-dna grpc` command enables gRPC for all the access points that are using the profile.

Is gRPC up?

This task verifies if your gRPC is up and running.

Run the **show ap grpc summary** command.

This command displays the gRPC status for each AP associated with the controller.

```
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
```

Are the TDL subscriptions created and valid?

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

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

```
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?

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

The command displays the TDL subscriptions status.

```
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:
```

IoT Services has five different subscriptions ranging from122-126 which can be used as the **Subscription ID**. Check if the **Address** is the IP address of the Cisco Spaces: Connector. Also check if the **State** is **Connected**.

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

Run the command **test platform software database get ewlc_oper/ble_ltx_ap;ap_mac=mac-without-dots** command on the controller.

The command displays the current TDL values for the given AP.

```
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?

Run the command: **show telemetry internal protocol cloud-native manager** *dna-spaces-connector-ip-address* **8004 source-address** *ewlc-source-ip*.

The command displays the connection status.

```
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?

Run the **show ap ble summary** command.

This command displays the BLE AP state and mode for each AP associated with the controller.

```
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?

Run the command **show ap name** *ap-name* **grpc detail** command.

The command displays the detailed gRPC stats for an AP.

```
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
```

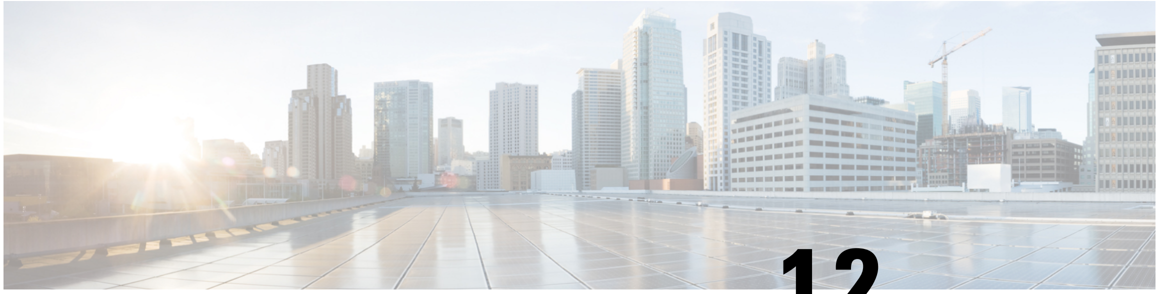
How do I view AP BLE configuration details?

Run the command **show ap name** *ap-name* **ble detail** command.

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

```
WLC# 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
```



CHAPTER 12

IoX Application

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 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
/ #
```

Topic 2.1

How can I see the logs for the IOx application?

Run the command: **tail -F /tmp/dnas_ble.log**

You can see the logs for the IOx application.

```
AP# tail -F /tmp/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?

Run the command: **tail -F /tmp/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.

Metrics Name	**Metrics Description**
Application Start Time	Local time on the AP that the application was started
Total Physical Memory	Total physical memory for the container
Physical Memory Used	Physical memory used for the container
Percent CPU Used	Percent CPU used in the container
Process Virtual Memory	Process virtual memory used
Process Physical Memory	Process physical memory used
Process CPU Used	Process CPU used
gRPC Reconnect Count	Number of times gRPC was reconnected while the application has been running
Log Rotation Count	Number of times the dnas_ble.log file has been rotated while the application has been running
Floor Beacon Scan Data Message Count	Number of scan data messages sent since the application started
Floor Beacon Config Request Count	Total number of floor beacon configuration requests since the application started
Floor Beacon Config Success Count	Number of floor beacon configuration requests that were successful
Floor Beacon Config Failure Count	Number of floor beacon configuration requests that failed

Metrics Name	Metrics Description
Profile MAC RSS Last-heard	Periodically the beacons scanned are dumped in the log with the attributes

```
AP# tail -F /data/logs/dnas_ble_metrics.log
Tue Mar 31 23:30:26 2020 [INFO]: Application Start Time: Wed May 20 02:54:05 2020
Tue Mar 31 23:30:26 2020 [INFO]: Total Physical Memory: 1920122880
Tue Mar 31 23:30:26 2020 [INFO]: Physical Memory Used: 947978240
Tue Mar 31 23:30:26 2020 [INFO]: Percent CPU Used: 2.260028
Tue Mar 31 23:30:26 2020 [INFO]: Process Virtual Memory: 74136
Tue Mar 31 23:30:26 2020 [INFO]: Process Physical Memory: 8296
Tue Mar 31 23:30:26 2020 [INFO]: Process CPU Used: 0.258247
Tue Mar 31 23:30:26 2020 [INFO]: gRPC Reconnect Count: 0
Tue Mar 31 23:30:26 2020 [INFO]: Log Rotation Count: 163
Tue Mar 31 23:30:26 2020 [INFO]: Floor Beacon Scan Data Message Count: 264757
Tue Mar 31 23:30:26 2020 [INFO]: Floor Beacon Config Request Count: 11
Tue Mar 31 23:30:26 2020 [INFO]: Floor Beacon Config Success Count: 11
Tue Mar 31 23:30:26 2020 [INFO]: Floor Beacon Config Failure Count: 0
Tue Mar 31 23:30:26 2020 [INFO]: Profile        MAC              RSSI(-dBm) Last-heard
Tue Mar 31 23:30:26 2020 [INFO]: iBeacon      18:04:ED:C4:FC:E0 100       0000D:09H:57M:36S
Tue Mar 31 23:30:26 2020 [INFO]: iBeacon      C4:0B:08:2F:EB:3D 54        0000D:00H:00M:02S
Tue Mar 31 23:30:26 2020 [INFO]: Unknown      EC:31:26:4F:48:BA 57        0000D:00H:00M:02S
Tue Mar 31 23:30:26 2020 [INFO]: Unknown      80:6F:B0:31:E0:24 97        0000D:00H:00M:00S
Tue Mar 31 23:30:26 2020 [INFO]: Eddystone URL  DE:91:06:AB:46:6D 47      0000D:00H:00M:00S
Tue Mar 31 23:30:26 2020 [INFO]: iBeacon      C2:9E:5C:21:7E:28 49        0000D:02H:16M:59S
Tue Mar 31 23:30:26 2020 [INFO]: Unknown      C3:CE:86:8A:DF:BE 47        0000D:00H:00M:02S
```

What files exist in the IOx application?

The following log files are created while running:

Log File Name	Description
/tmp/dnas_ble.log	Active log file for debug messages. Since this file is updated frequently, the file is in the tmp directory, which is a partition that can handle this I/O.
/data/logs/dnas_ble_1.log	Rotated log file for the debug messages for the application
/data/logs/dnas_ble_metrics.log	Active log file for metric messages
/data/logs/dnas_ble_metrics_1.log	Rotated log file for metric messages
/data/logs/dnas_ble_stdout.log	Standard output and standard error messages are written to the file
/data/logs/dnas_ble_last_restart.log	If the IOx application is restarted, then the /tmp/dnas_ble.log file is copied to this file. You can use this file to troubleshoot the reason for the restart
/data/logs/dnas_ble_metrics_last_restart.log	If the IOx application is restarted, then the /data/logs/dnas_ble_metrics.log file is copied to this file. You can use it to troubleshoot the reason for the restart.

The following are binary files installed specifically for the IOx application.

File Name	Description
/var/dnas_ble/dnas_ble_iox_app	IOx application binary which will scan and configure floor beacons
/var/dnas_ble/dnas_ble_iox_app_start.sh	Script to start and in the case of a failure restart the application again

CHAPTER 13

Connector

Reprovisioning IoT Services After Failover

How do I view floor beacon configuration requests and responses from the connector?

Run the command: **tail -F /opt/cmx-cloud/connector/etc/logs/server.log | grep "FLOOR BEACON CONFIG"**

This command tails the server log for just the request and response messages for floor beacon configuration.

In the request, "destinationType":"AP","apMacaddress":"AP MAC ADDRESS" indicates the destination of the request. In this example, the destination is the AP with radio MAC address: 04:eb:40:9f:af:a0.

On Cisco Catalyst 9800 Series Wireless Controller, run the command **show ap summary**. In the displayed output, you can observe the base radio MAC address and AP information.

How do I view the IOx application install logs?

Run the command: **cat /opt/cmx-cloud/connector/etc/logs/dnas_iox_app_manage.log**

Log file for IOx application management is /opt/cmx-cloud/connector/etc/logs/dnas_iox_app_manage.log

```
[cmxadmin@connector ]$ cat /opt/cmx-cloud/connector/etc/logs/dnas_iox_app_manage.log

2020-06-25 21:33:34,115 INFO [IoxApplication] Attempting to install application on:
10.22.243.144 ID: cisco_dnas_ble_iox_app Version: 1.0.44
2020-06-25 21:33:43,912 INFO [IoxApplication] Attempting to activate application on:
10.22.243.144 ID: cisco_dnas_ble_iox_app Version: 1.0.44
2020-06-25 21:33:51,043 INFO [IoxApplication] Attempting to start application on:
```

```
10.22.243.144 ID: cisco_dnas_ble_iox_app Version: 1.0.44
2020-06-25 21:33:52,840 INFO [IoxApplication] Completed install of application on:
10.22.243.144 ID: cisco_dnas_ble_iox_app Version: 1.0.44
```

How do I view the gRPC certificate on the Cisco Spaces: Connector?

Run the command: **openssl s_client -showcerts -connect <DNA Spaces Connector IP>:8000**

Look at the certificate chain and make sure the s: CN is the DNA Spaces Connector IP "s:/C=US/ST=California/L=SanJose/O=Cisco/CN=<DNA Spaces Connector IP>"

Also ensure that the i: CN is DNASpacesIntermediateCA "i:/C=US/ST=California/O=Cisco System Inc/OU=DNA Spaces/CN=DNASpacesIntermediateCA".

```
sh#  openssl s_client -showcerts -connect 10.22.243.33:8000
CONNECTED(00000003)
depth=0 C = US, ST = California, L = SanJose, O = Cisco, CN = 10.22.243.33
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = US, ST = California, L = SanJose, O = Cisco, CN = 10.22.243.33
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=SanJose/O=Cisco/CN=10.22.243.33
   i:/C=US/ST=California/O=Cisco System Inc/OU=DNA Spaces/CN=DNASpacesIntermediateCA
-----BEGIN CERTIFICATE-----
MIIEdjCCAl6gAwIBAgICEJIwDQYJKoZIhvcNAQELBQAwdDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExGTAXBgNVBAoMEENpc2NvIFN5c3RlbSBJbmMx
EzARBgNVBAsMCkROQSBTcGFjZXMxIDAeBgNVBAMMF0ROQVNwYWNlc0ludGVybWVk
aWF0ZUNBMB4XDTIwMDYyOTE5NTAyOFoXDTMwMDYyNzE5NTAyOFowWzELMAkGA1UE
BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcMB1Nhbkpvc2UxDjAM
BgNVBAoMBUNpc2NvMRUwEwYDVQQDDAwxMC4yMi4yNDMuMzMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCxrrkc/p2LdHMoGHAw8GP4zItwXSR6Olgh0UTl
BdZuyfPkOZPtrFCT7kj8q6brIsRCFF69sPTu6qAIhYVIj27iU1vUv7m1QbGYw/Fw
Q9sZ8kCoUDbkG69bRbP2dqV0G+pupQ4CWcQe/UIsrvMlV1r+kj3WSOWhw+Uq9hmT
75aGUkxWaoTMrPFeXd0/pwnPWCv7ArRc7n3/MSCL+pSCbI9AdOfNHsA2IfPLQJFy
udB2mYKAojE7FZub75x7KYrrUTQoEOi12SB2Gg3N94cDb6CSg/11d2chwoqHBCI8
Bm24jbCt0W2+AzYQG4o3s7FJ95lJGchFjL4/iq4P4RJME4VnAgMBAAGjKzApMAkG
A1UdEwQCMAAwCwYDVR0PBAQDAgXgMA8GA1UdEQQIMAaHBAoW8yEwDQYJKoZIhvcN
AQELBQADggIBAKPwQLamMTyw2qGDEidRVLBy55y3IP0KvSOWZaDPdmOx0Ah8i7Kw
zAlZFjBPZMGM2J3Ic4mIkvqIKH/pqWL3WU/Z7qKqkYdpT2rvTgzcChc9kllWwv+V
IvkN/QOhScwSEtUZO3OzjtrYxq5SLES2zUXS1KrPrCffyPP6HNnvNLv6AHzHxJCo
PZnmnjFDWoVpnI7sCr8QSYxHE2AMRrOqx/ZshTa2/fQnIC/6l8A7eKSUmJ6l2Fr3
4F7QxyZaP9RQyAs5u9PmH2K4uKrJLaKhOLzQzswM+r8+AWcqXQMHBlJUnH50rGQy
3SuppO1JXbm9eiNFBZpvcHtIGt0k8r7j/DIKwznND+aN1MZQFtU1hz0B2NH789bW
o9mI/cQQQyrRvQcCcUp25u+nyYtXjMw5Kyxuxt2RRUSKYKqiZv9iDUk4q8jkbZgX
vYOHTmEexdvUU18CumXFvGudZ+2IfTjzUXcGxLNW4DfxGaxa8MxPlNfJyA6Of5gf
sJoGG9tPFSrA+3Z5q1eVeW0yLdjJgckNXxPeI74MC4Hj3nIH+NQAr/mO1sJn1/pY
EWZWPLVaSq+pG7SOt03pJNKFhe2heCWT3SDvvvM8StZjW/x89UjN2JvogmnZ9hDh
ibYMtX8W6zuZYNIYciMJ6RcwUv7htcBrrFHZYWuShrkfUbQpdwjuMJsv
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=SanJose/O=Cisco/CN=10.22.243.33
issuer=/C=US/ST=California/O=Cisco System Inc/OU=DNA Spaces/CN=DNASpacesIntermediateCA
---
No client certificate CA names sent
Peer signing digest: SHA512
```

```
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1805 bytes and written 373 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 7BE18058D49909503C29A4EAF37B1D1BBA9B18807D7E746D2B993B441E2B12F3
    Session-ID-ctx:
    Master-Key:
0C272766509BA6E8F6DC8866E325CB756BB75D6E53BF9891EFB629EF24341D57E309627C6EA6047AA534B537DAED750B

    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 7f 0c 77 fd b3 ad fb ab-a5 79 dd bc 48 e5 47 7f   ..w......y..H.G.
    0010 - 74 0d eb c2 22 4c 5b 64-3e 20 02 b2 c5 79 f7 ff   t..."L[d> ...y..
    0020 - 4b cc cd 3d a6 73 a7 ce-35 06 24 eb c4 57 ea 8b   K..=.s..5.$..W..
    0030 - f0 45 bf 00 cb 7e da 7e-77 97 9a fe 13 c7 f1 9e   .E...~.~w.......
    0040 - 65 2c b4 40 d8 f0 d8 13-fa db 9b 84 d4 d8 93 07   e,.@............
    0050 - 0a 9c dd 16 41 d2 c9 c8-b3 6d d6 09 19 44 4a c7   ....A....m...DJ.
    0060 - d0 02 57 1f 85 db 34 63-2f aa 22 2b 02 f2 08 59   ..W...4c/."+...Y
    0070 - 8f 71 4e e3 a9 b1 98 7a-a8 db c9 f8 3b 99 1a af   .qN....z....;...
    0080 - f8 29 2f 14 8b 84 1f 90-13 06 f6 79 e3 92 81 1a   .)/........y....
    0090 - a0 2a 4e 3a e6 7f c1 77-bd a9 82 2c ac 2c ed d3   .*N:...w...,.,..

    Start Time: 1593502547
    Timeout   : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)
---
```

How do I verify that the gRPC certificate was created successfully?

Run the command: **grep GRPC_CERT_SETUP /opt/cmx-cloud/connector/etc/logs/***

In the log search for the message indicating gRPC setup completed "command":"GRPC_CERT_SETUP"

Log message displays the result status "status":"SUCCESS".

```
[cmxadmin@connector ]$ grep GRPC_CERT_SETUP /opt/cmx-cloud/connector/etc/logs/*


.
server.log:2020-06-29 12:50:29 [Thread-69159] INFO
com.cisco.cmx.command.CommandChannelHandler - Sending Command channel request
id:a7a607ce-555b-468c-a2b2-a03f6119b0fc
response:{"requestId":"a7a607ce-555b-468c-a2b2-a03f6119b0fc","message":"Successfully performed
 operation","command":"GRPC_CERT_SETUP","status":"SUCCESS"}
```

CHAPTER 14

Access Point

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 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**

```
AP# 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**

Following 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            : bfbfbfbfbfbfbfbfbfbfbfbfbf

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                 :
000001800000000000000000ecb255ad5500000000c0000000000000000000
Scan Data                :
00000000ae010000000000005446089c7f000000190000000000000004cb5
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
```

Following 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                     : 00010000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbfbf

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                 :
000001800000000000000000ecb255ad5500000000c0000000000000000000
Scan Data                :
00000000ae010000000000005446089c7f000000190000000000000004cb5
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
```

Following 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                     : 00010000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbfbf

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                 :
00000018000000000000000ecb255ad550000000c00000000000000000000
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
```

PART VI

Appendix

CHAPTER 15

Cisco Catalyst 9800 Series Wireless Controller

Disable Assurance with iCAP using Web UI (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 Assurace with Intellegent Capture (iCAP) in order to enable IoT Services. With the controller WebUI, you can issue CLI commands to disable assurance and iCAP.

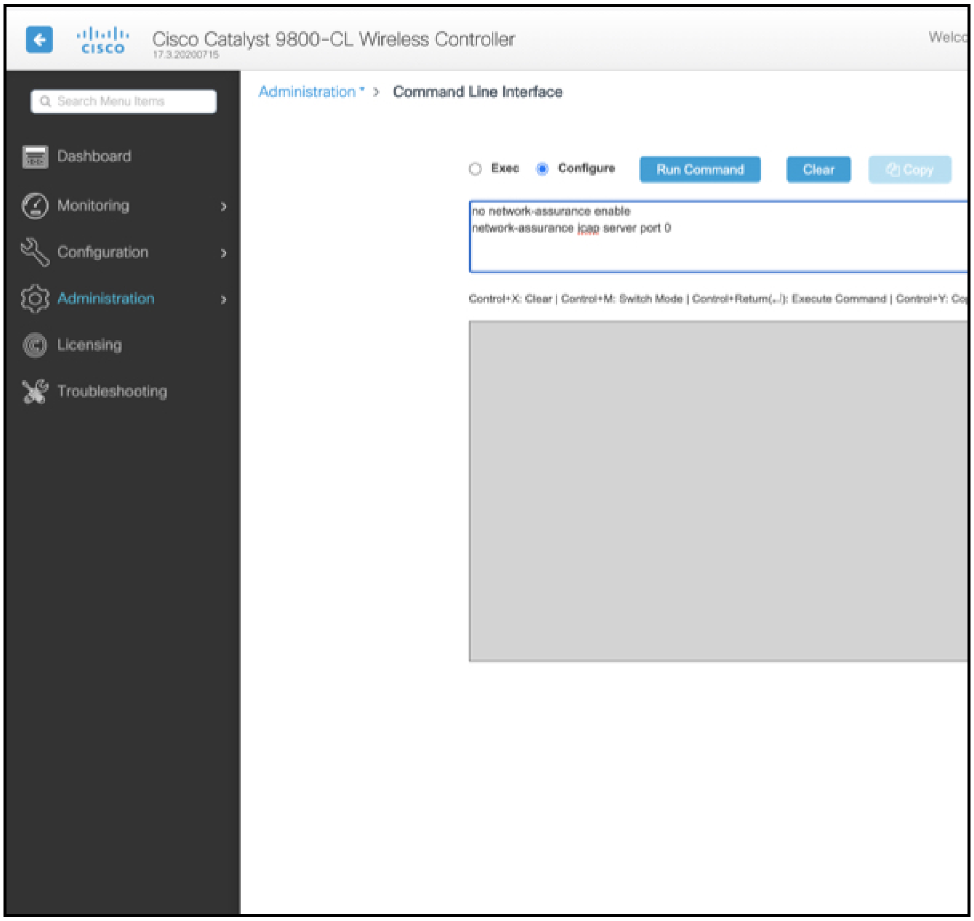
SUMMARY STEPS

1. Login to the Cisco Catalyst 9800 Series Wireless Controller Web UI 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.
2. Click **Run Command**.

DETAILED STEPS

Step 1 Login to the Cisco Catalyst 9800 Series Wireless Controller Web UI 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 72: Entering the commands to enable BLE



```
no network-assurance enable
network-assurance icap server port 0
```

Control+X: Clear | Control+M: Switch Mode | Control+Return(↵): Execute Command | Control+Y: Co

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 Cisco DNA Center (version 2.2 and above), the Cisco DNA 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

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 Cisco DNA Center (version 2.2 and above), the Cisco DNA 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 the Cisco IOS XE Amsterdam 17.3.x release now supports the IoT Services along with the Network Assurance solution on Cisco DNA Center.

IoT Services and Intellegent Capture (iCAP) can co-exist from IOS-XE image versions 17.7 or higher.

Note However, Cisco IOS XE Cupertino 17.7.x or earlier, IoT Services and Intellegent Capture (iCAP) feature are mutually exclusive. That is, if iCAP feature needs to be enabled on the device, then IoT Services cannot be deployed. Similarly, if IoT Services needs to be enabled on the device, then iCAP feature cannot be deployed.

Disable Intellegent Capture (iCAP) in order to enable IoT Services. With the controller Web UI, you can issue CLI commands to disable iCAP.

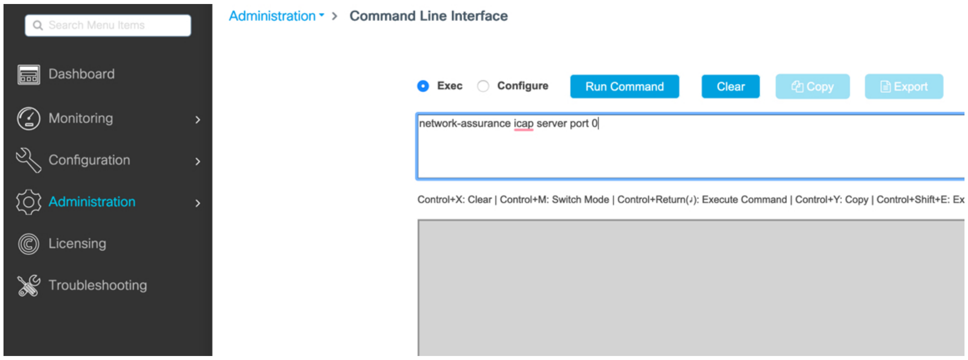
SUMMARY STEPS

1. Login 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.
2. Click **Run Command**.

DETAILED STEPS

Step 1 Login 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 73: Entering the commands to enable IoT Services



```
network-assurance icap server port 0
```

Control+X: Clear | Control+M: Switch Mode | Control+Return(↵): Execute Command | Control+Y: Copy | Control+Shift+E: Ex

Step 2 Click **Run Command**.

If the command runs successfully, you can see a success message displayed.

What to do next

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

If this controller was previously added to Cisco DNA Center (version 2.2 and above), Cisco DNA 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 controller work on Cisco Spaces.

Disable iCAP using CLI (Versions 17.3.2 or higher)

This task uses the CLI to disable Intellegent 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 the Cisco IOS XE Amsterdam 17.3.x release now supports the IoT Services along with the Network Assurance solution on Cisco DNA Center.

However, Cisco IOS XE Cupertino 17.7.x or earlier, IoT Services and Intellegent Capture (iCAP) feature are mutually exclusive. That is, if iCAP feature needs to be enabled on the device, then IoT Services cannot be deployed. Similarly, if IoT Services needs to be enabled on the device, then iCAP feature cannot be deployed.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 configure terminal

Step 2 network-assurance icap server port 0

Step 3 end

What to do next

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

If this controller was previously added to Cisco DNA Center (version 2.2 and above), Cisco DNA 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 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 Cisco DNA Center templates.

Step 1 From the Cisco DNA Center dasboard, use the template editor to create a template with the required configurration. Specify the template name, description, software type, and device type.

Step 2 Save and commit the template.

Step 3 Add the template to the respecive site.

Step 4 Select the device from the site and provision the device.

Step 5 In the Advanced Configuration select the template and apply to the device.