# cisco.



### **Cisco Spaces: IoT Service Configuration Guide (Wireless)**

First Published: 2020-08-31 Last Modified: 2024-08-02

### **Americas Headquarters**

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.



### CONTENTS

Overview 7
Overview 1
Overview of Cisco Spaces: IoT Service (Wireless) 1
Components of Cisco Spaces: IoT Service 1
Compatibility Matrix for IoT Service (Wireless) 4
Prerequisites 7
Prerequisites of IoT Service (Wireless) 7
Cisco Spaces: Connector Scale and Size Guidance for IoT Service 7
Prerequisites 8
Compatibility Matrix for IoT Service (Wireless) 9
Open Ports 13
Information About Open Ports (Wireless) 13
Getting Started 15
Activate IoT Service (Wireless) 15
Configuration 21
AP as a Beacon 23
AP as a Beacon 23
iBeacon Transmit Mode 24
Configure AP as a Beacon in Scan Mode <b>24</b>
Configure AP as a Beacon in Transmit Mode 27

	Configure AP as a Beacon in Dual Mode <b>30</b>
CHAPTER 6	AP as a Gateway 33
	Access Point as a BLE Gateway <b>33</b>
	Configure an AP as a Bluetooth Low Energy (BLE) Gateway <b>33</b>
	Uninstall or Upgrade an IOx Application on an Advanced Gateway <b>36</b>
CHAPTER 7	Beacons and Tags 45
	Discover Beacons 45
	Claiming a Beacon 50
	Configuring a Beacon on IoT Service <b>52</b>
	Viewing Sensor Information 54
	Configuring a Location Anchor <b>57</b>
CHAPTER 8	AP as a Sensor 61
	AP as a Sensor 61
	Enabling or Disabling an AP Sensor 61
	Viewing Sensor Information <b>63</b>
PART III	Device Management 65
CHAPTER 9	Device Management 67
	Dashboard View of Devices 67
	Configuring Beacons 68
	Categorizing Devices into Manual Groups <b>68</b>
	Categorizing Devices into Groups (Dynamic Groups) 69
	Applying Policies to Beacons <b>71</b>
	Filtering Devices 76
PART IV	Device Monitoring 79
CHAPTER 10	Device Monitoring 81
	Right Now 81
	BLE Devices Battery Life 81

### Last Heard BLE Devices 82

PART V	Troubleshooting 85
CHAPTER 11	Troubleshooting IoT Services: Controller 87
	Reprovisioning IoT Services After Failover 87
	What settings are needed to allow access via NETCONF? 87
	The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting? <b>88</b>
	For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token? 88
	gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled? 89
	How do I verify gRPC is up? 89
	How do I verify that TDL subscriptions are created and are valid? <b>90</b>
	Are the TDL subscriptions created and valid? <b>90</b>
	What is the TDL status? 90
	How do I view the current CAPWAP values for an AP? 91
	How do I view the current TDL values for an AP? 99
	How do I get the telemetry connection status? <b>102</b>
	How do I view IOx AP state and mode? 102
	How do I view gRPC details? 103
	How do I view AP BLE configuration details? 103
	How do I view the current TDL values for AP air quality? <b>105</b>
	How do I view the current TDL values for AP temperature and humidity? <b>106</b>
CHAPTER 12	Troubleshooting IoT Services: IOx Application 107
	How do I verify the IOx application is running on the AP? <b>107</b>
	How do I debug the IOx application installation failure? <b>107</b>
	How do I verify the IoX Application AP bundle download from Cisco Spaces? 108
	How do I start an interactive shell session for the IOx application? 108
	How can I see the logs for the IOx application? <b>109</b>
	How do I monitor metrics in the IOx application? <b>109</b>
	How do I monitor BLE scans in the IoX Application? 111

	What files exist in the IOx application? <b>113</b>
CHAPTER 13	Troubleshooting IoT Services: Cisco Spaces Connector 115
	What are the metrics available on the Connector GUI for IoT Service (Wireless)? 115
	What are the log files created on the Connector for IoT Service (Wireless)? <b>116</b>
CHAPTER 14	Troubleshooting IoT Services: Access Point 117
	How do I check the gRPC connection status on the access point? <b>117</b>
	How do I check the stream token on the access point? <b>117</b>
	How do I view the gRPC server logs on the access point? <b>118</b>
	How do I view the beacons scanned by an access point running in Native Mode? 119
	How do I view the beacon broadcast setting for an access point running in Native Mode? <b>119</b>
PART VI	Appendix 123
CHAPTER 15	Cisco Catalyst 9800 Series Wireless Controller 125
	Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower) <b>125</b>
	Disable Assurance with iCAP using CLI (Versions 17.3.1 or lower) <b>126</b>
	Disable iCAP using WEBUI (Versions 17.3.2 or higher) <b>127</b>
	Disable iCAP using CLI (Versions 17.3.2 or higher) <b>128</b>
	Enable or Disable iCAP or Assurance using DNAC (Versions 17.3.2 or higher) 129



# PART

## **Overview**

- Overview, on page 1
- Prerequisites, on page 7
- Open Ports, on page 13
- Getting Started, on page 15



### **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 Service (Wireless), on page 1

### **Overview of Cisco Spaces: IoT Service (Wireless)**

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

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

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

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

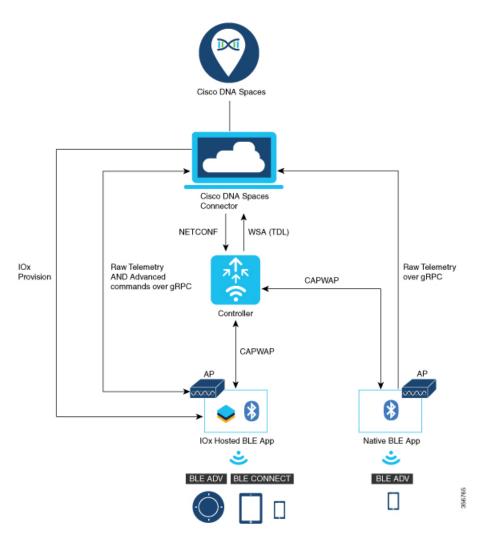
### **Components of Cisco Spaces: IoT Service**

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

The Cisco Catalyst 9100 Series Family of Access Points acts as a gateway of communication between Cisco Spaces and the IoT devices. Cisco Spaces: IoT Service can then use a range of common APIs to communicate with edge devices and apps. The Cisco Spaces: IoT Service collects data from devices and apps, and passes

it to Cisco-partnered websites that manage these devices far more extensively (referred to in this document as Device Manager websites). These Device Manager websites can use edge-device signals to enable outcomes specialized and targeted for each industry.





#### **Access Points**

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

Depending on the type of Cisco APs, you can configure an AP as one of the following types of BLE gateways:

• Base BLE Gateway: This is a type of AP that you can configure in 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, an 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: This gateway is an AP that is installed with the Cisco IOx App. Using the installed Cisco IOx App, you can configure floor beacons on the Cisco Spaces dashboard. You can also upgrade the floor beacon firmware from the Cisco Spaces dashboard.

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

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

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

Note

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

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

#### **Cisco Spaces: IoT Device Marketplace**

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

#### **Cisco Spaces: Connector**

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

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

APs connect to connector using the gRPC framework.

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

### **Compatibility Matrix for IoT Service (Wireless)**

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	Supported on Cisco Catalyst 9800 Series     Wireless Controllers, Release 17.3.1 and later
	Not supported on Cisco AireOS Wireless     Controller
	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)
	• Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA)
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
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later

Application Name	Support for Cisco Spaces: IoT Service
Access Points for advanced BLE gateway (Wi-Fi 6)	Cisco Catalyst 9105 Series Access Points
	Cisco Catalyst 9115 Series Access Points
	Cisco Catalyst 9117 Series Access Points
	Cisco Catalyst 9120 Series Access Points
	Cisco Catalyst 9130 Series Access Points
	Cisco Catalyst 9136 Series Access Points
	Cisco Catalyst 9162 Series Access Points
	Cisco Catalyst 9164 Series Access Points
	Cisco Catalyst 9166 Series Access Points
	Cisco Aironet 4800 Series Access Points
Access points for basic BLE gateway	Cisco Aironet 1815 Series Access Points
	• Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio)
	• Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later
	<b>Note</b> 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

IoT Service is not supported on the following:

• Directly connected and CMX Tethering connectors.

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

Table 1: AP Modes and App Support

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	<ul><li>11-AX: Supported</li><li>Wave2: Not supported</li></ul>	• 11-AX: Supported     • Wave2: Supported
P1: Flex	• 11-AX: Supported     • Wave2: Not supported	• 11-AX: Supported     • Wave2: Supported

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
P2: Fabric	• 11-AX: Supported	• 11-AX: Supported
	• Wave2: Not supported	• Wave2: Supported
P3: Mesh	• 11-AX: Supported	• 11-AX: Supported
	• Wave2: Not supported	• Wave2: Supported



## **Prerequisites**

• Prerequisites of IoT Service (Wireless), on page 7

## **Prerequisites of IoT Service (Wireless)**

### **Cisco Spaces: Connector Scale and Size Guidance for IoT Service**

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

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



### Note

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

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

Connector Size	Scale
Standard Connector (2vCPU, 4 GB RAM)	The Standard Connector can
	• Support up to 500 APs.
	• Send up to 25,000 outbound messages per second.
	• Process up to 1000 BLE tags or devices.

Connector Size	Scale
Advanced1 Connector (4vCPU, 8 GB RAM)	Advanced1 Connector can
	• Support up to 2500 APs
	• Send up to 120,000 outbound messages per second.
	• Process up to 10,000 BLE tags or devices.

### **Prerequisites**

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

- Install Cisco Spaces: Connector in your network.
- Install a Cisco Catalyst 9800 Series Wireless Controller with a Cisco IOS XE Amsterdam 17.3.x image.
- Deploy supported APs in your network (see the Compatibility Matrix for IoT Service (Wireless), on page 4).
- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Catalyst Center.
- If the Cisco Spaces: Connector is an Amazon Elastic Compute Cloud (EC2) Instance from Amazon Machine Images (AMI), ensure that the wireless controller and connector are in the same virtual private cloud (VPC). Ensure that the wireless controller has a private IP address so that the security group of connector does not block the traffic, allowing enabled IOT streams to function.
- Permit all the TCP traffic at the Virtual private clouds (VPC) level so that the Telemetry Data Logger (TDL) is established without any issues.
- Before adding a Cisco Catalyst 9800 Series Wireless Controller to a connector, run the following commands on the Catalyst 9800 controller in a sequence:
  - 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 Service and Intelligent Capture (iCAP) feature can now co-exist on Cisco Catalyst 9800 Series Wireless Controller Cisco IOS XE Cupertino 17.7.x release and later. For releases earlier than Cisco IOS XE Cupertino 17.7.x, disable iCAP, if already enabled on the controller.
- Perform NTP synchronization over wireless controllers, a connector, and APs in the network.
- If a USB BLE module is inserted in an AP, reboot the AP.
- NETCONF must be enabled in Cisco Catalyst 9800 Series Wireless Controller in port 830, along with permission to use NETCONF.

I

À	
Caution	The application (app) installed and running over the AP uses the default 17.17.0.0/16 subnet. So, using this subnet for other purposes might create network issues.
• []	Pv6 is not supported on Cisco Spaces: Connector.
	Fyour require two connectors installed with 3.x to work with IoT service (wireless) and function as a igh-availability pair, you must configure the connectors as Virtual IP (VIP) pair.
Acces	s Points that support IoT Service (Wireless) are as follows:
• (	isco Catalyst 9105 Series Access Points
• (	isco Catalyst 9115 Series Access Points
• (	isco Catalyst 9117 Series Access Points
• (	isco Catalyst 9120 Series Access Points
• 0	isco Catalyst 9130 Series Access Points
• 0	isco Catalyst 9136 Series Access Points
• 0	isco Catalyst 9162 Series Access Points
• 0	isco Catalyst 9164 Series Access Points
• (	isco Catalyst 9166 Series Access Points

Cisco Aironet 4800 Series Access Points

### **Compatibility Matrix for IoT Service (Wireless)**

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later
	Not supported on Cisco AireOS Wireless     Controller
	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)
	• Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA)
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

Application Name	Support for Cisco Spaces: IoT Service
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later
Access Points for advanced BLE gateway (Wi-Fi 6)	Cisco Catalyst 9105 Series Access Points
	Cisco Catalyst 9115 Series Access Points
	Cisco Catalyst 9117 Series Access Points
	Cisco Catalyst 9120 Series Access Points
	Cisco Catalyst 9130 Series Access Points
	Cisco Catalyst 9136 Series Access Points
	Cisco Catalyst 9162 Series Access Points
	Cisco Catalyst 9164 Series Access Points
	Cisco Catalyst 9166 Series Access Points
	Cisco Aironet 4800 Series Access Points
Access points for basic BLE gateway	Cisco Aironet 1815 Series Access Points
	• Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio)
	• Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later
	<b>Note</b> 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

IoT Service is not supported on the following:

• Directly connected and CMX Tethering connectors.

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

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App		
PI: Local	• 11-AX: Supported	• 11-AX: Supported		
	• Wave2: Not supported	• Wave2: Supported		

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App	
P1: Flex	• 11-AX: Supported	• 11-AX: Supported	
	• Wave2: Not supported	• Wave2: Supported	
P2: Fabric	• 11-AX: Supported	• 11-AX: Supported	
	• Wave2: Not supported	• Wave2: Supported	
P3: Mesh	• 11-AX: Supported	• 11-AX: Supported	
	• Wave2: Not supported	• Wave2: Supported	



# Open Ports

• Information About Open Ports (Wireless), on page 13

## **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

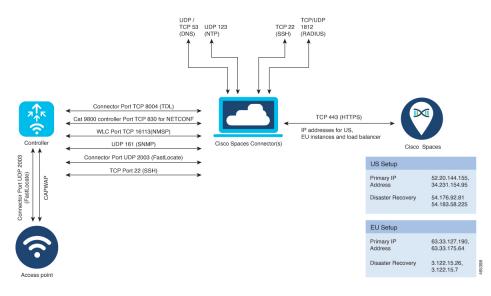


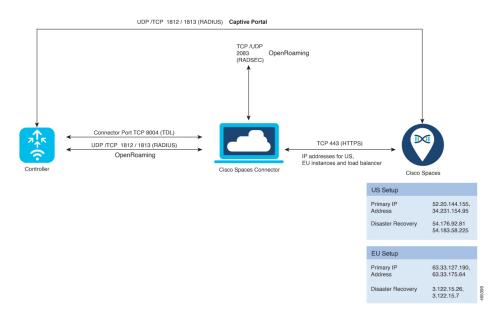
Table 4: Setups

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

Setup Type	Primary IP Address	Disaster Recovery		
EU Setup	63.33.127.190	3.122.15.26		
	63.33.175.64	3.122.15.7		
Singapore Setup (SG)	13.228.159.49	13.214.251.223		
	54.179.105.241	54.255.57.46		

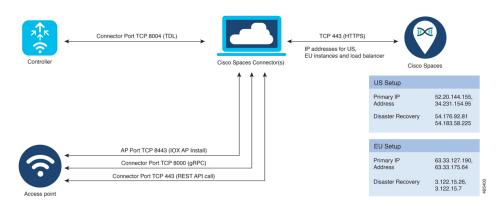
In addition to basic functionality, additional ports need to be opened for other additional functionality like guest onboarding and IoT Services.

#### Figure 3: Guest Onboarding



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





## **Getting Started**

• Activate IoT Service (Wireless), on page 15

## **Activate IoT Service (Wireless)**

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

### Before you begin

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

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



Note

- This workflow is applicable only for Connector Release 3. We recommend that you upgrade from Connector 2.x for smooth functioning of your services. If it is absolutely essential to enable IoT service (wireless) on Connector 2.x, open a support case.
- The workflow initiated by this procedure automatically checks for prerequisites necessary to complete this task.

### **Step 1** Log in to Cisco Spaces.

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

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

Figure 5: About IoT Services

About lo	T Serv	/ices									E	Activa	te loT Ser	vices
oT Service	s: Activ	vation Sta	itus			Last up	pdated: As	of Aug 30th, 2023	03:11:29 PM	Э	Troubles	shoot	View [	etailed Status
Connect	or					Controlle	ers		Gateway					
Wireless S	Services		Wired Ser	vices					Wireless 0	Bateway		Wired Gat	eway	
5	0	0	5	0	0	2	0	0	0	7	0	1	0	0
Activated	Failed	Pending	Activated	Failed	Pending	Activated	Failed	Pending	Activated	Failed	Pending	Activated	Failed	Pending

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

Figure 6: Detailed Status of Devices Activated With IoT Service (Wireless)

Connectors Controllers Wirel	ess Gateway Wired Gateway	
Wireless Services Wired Services		
5 of 5 Completed		5 O Activated Failed
Connectors	Version	Activation Status
Bhaumik-ami	V2	Deployed
bhaumik-qa-manual	V3	Deployed
connector3.1-ami-Bhaumik	V3	Deployed
Bhaumik-2-3-4-on prem	V2	Ø Deployed
Bhaumik-ami-connector-2.3.4	V2	Deployed

- Step 3 In the About IoT Services window top-right corner, click Activate IoT Services.
- **Step 4** In the Activate IoT Services window that is displayed, choose Wireless.

L

#### Figure 7: Activate IoT Service (Wireless)

Activate IoT Services		×
If you want to enable IoT services on both wireless ar	ike to activate first d wired devices, choose one option and complete the after to activate the rest.	
Wireless You must have a connector installed and added compatible APs on the connectors before you proceed with this. The gateway can be deployed all the compatible APs. Compatible devices: Catalyst 9800 series controllers and 9100 series APs	Wired Environment of the connector installed and added supported switches on the connectors before you proceed with this. The gateway can be deployed all compatible switches. You need to configure certain parameters manually. Compatible devices: Catalyst 9300 and 9400 series switches	
	Previous	Next

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

### Figure 8: List of Supported Devices

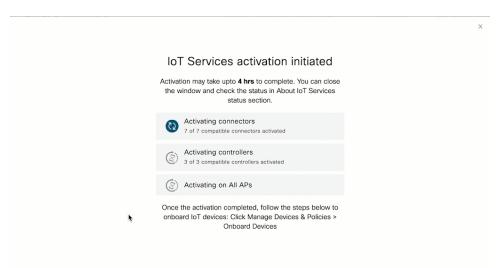
Activate IoT Services		×
	loT services will be activated on	
	7 of 9 compatible connectors Takes upto 3 hrs, 30 mins	
	2 connectors not responding, hence IoT services will not be activated on them.	
	3 of 3 compatible controllers Takes up to 30 mins	
	All Compatible APs on all locations Takes up to 10 mins/AP	
	Activating IoT services on the supported APs may take upto <b>4 hrs + 10</b> mins/AP. You can initiate the activation and check the status in the "About IoT services" page.	
	Activate	
	Activate IoT services on selected?	
	Click here for customization	

### Step 5 To activate IoT service (wireless) on all devices on your network, in the IoT services will be activated on window, click Activate.

This activation of IoT service (wireless) automates the following tasks:

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

#### Figure 9: Activate IoT Service (Wireless) on all devices



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

- a) Choose one or more connectors to activate IoT service (wireless).
- b) To activate the wireless gateway, click Activate Wireless.
- c) In the Deploy Wireless Gateway window, select the APs on which you want to activate IoT service (wireless).

#### Figure 10: Activate IoT Service (Wireless) on Preferred Devices

Activate IoT Services			×
	loT services will be a	activated on	
	5  of  8  compatible connectors	Takes upto 2 hrs, 30 mins	
	3 connectors not responding, hence IoT services w	ill not be activated on them.	
	2  of  2  compatible controllers	Takes upto 20 mins	
	All Compatible APs on all locations	Takes upto 10 mins/AP	
	Activating IoT services on the supported APs ma 10 mins/AP. You can initiate the activation and c IoT services* page.	heck the status in the "About	
	Activate	l	
	Activate IoT services on		
	Click here for customizat	ion	

Figure 11: Activate IoT Service (Wireless) on Preferred Devices

Deploy Wireless	Gatewa	ау			,
	Choose 1	he acccess points that you want to c	leploy gateway		SELECTED APs
		Select All Supported APs	Gateway Capability	Status	2/23
		RTB2-Russel-C9105	Gateway Not Supported	NA	APs
		Russell-2CF8	Advanced Gateway	Not Activated	APS
		RTB2_9115I_2	Advanced Gateway	Base Gateway Activated	1 Aps with Advanced BLE Gateway support
		RTB3-9130AXE-Marlin4-22	Advanced Gateway	Not Activated	
		RTB2-9117-2	Advanced Gateway	Not Activated	
		RTB2-9117I	Advanced Gateway	Base Gateway Activated	
		Sid-4800-1	Gateway Not Supported	NA	
		CM64-2C60	Gateway Not Supported	NA	
		RTB1-Cornwall-9130	Base Gateway	Advanced Gateway Activated	
		RTB2-9124I	Gateway Not Supported	NA	
		AP5CE1.7628.0D60	Gateway Not Supported	NA	
					Prev Next

### What to do next

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



# PART

## Configuration

- AP as a Beacon, on page 23
- AP as a Gateway, on page 33
- Beacons and Tags, on page 45
- AP as a Sensor, on page 61



### **AP** as a Beacon

- AP as a Beacon, on page 23
- iBeacon Transmit Mode, on page 24
- Configure AP as a Beacon in Scan Mode, on page 24
- Configure AP as a Beacon in Transmit Mode, on page 27
- Configure AP as a Beacon in Dual Mode, on page 30

### **AP** as a Beacon

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

IoT Service categorizes APs according to their configurations as 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. You can configure up to five iBeacons in this mode.
  - The MAC address advertised in the iBeacon payload is derived from the radio MAC address of the AP. (iBeacon MAC address).
  - The MAC address advertised in the Eddystone payload is the default MAC address of the AP's BLE chip, which is preset by the chip vendor.
- **Dual Mode:** AP beacons that are transmitting and scanning. You can configure only one iBeacon in this mode.
  - The MAC address advertised in this mode is the default MAC address of the AP's BLE chip, which is preset by the chip vendor (For both Eddystone and iBeacon single advertisement profiles)
- Needs Config Change: AP's that have an error in configuration. You can configure these APs in Scan Mode, Dual Mode, or the Transmit Mode.

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

- iBeacon
- · Eddystone UID

• Eddystone URL

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

Figure 12: Various Profiles of AP Beacons

	≡ thether Spaces													
	Dashboard	v	Home	Devices	Groups Poli-	cles	Settings							
	Home     Location Hierarchy     Integrations		All Camp All Profile 3		Sensor AP Sensors 2	IB O	Transmit		Transmit Eddystone UID D		Transmit Eddystone URL O	Scan Scan Mode 3	Dual Mode O	əl
	Monitor Admin Management IoT Services		Needs Co O	nfig Change	Disabled 3									
	💮 Setup		List View	Map View	√ Filters Actions → AP Name ●	Bulk Rec	uest History BLE	AP Model	Profile Type	Label	Location		As of: Feb 1, 20	24 8:59 PM
<ul> <li>IoT Services</li> <li>Setup</li> </ul>	About IoT Services		0	68:7dtb4:5ft66:e0 Dut of Sync	AP687D.845C.1E00	-	✓ Enabled	C9136I-B	Scan		DNA Spaces IoT Dev Test-	Building 19->Main Floor	3.2.4	Feb 1st, 202 7 minutes apr
	IoT Gateways Device Management	iow.		1c:d1:e0:65:c3:40	AP84F1.47B2.B868	-	🖌 Enabled	C9115AX0-B	Scan		DNA Spaces loT Dev Test-	Building 19->Main Floor	2.7.21	Space
	Device Monitoring	2.6		1c:d1:e0:79:8e:a0	AP84F1.47B3.31D4	-	✓ Enabled	C9115AXI-B	Scan	-	DNA Spaces IoT Dev Test-	-Building 19->Main Floor	2.7.21	COVID-19 Apps

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

### iBeacon Transmit Mode

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

Use Cisco Spaces to configure an iBeacon's payload.

Following are some terms related to iBeacons:

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

### Configure AP as a Beacon in Scan Mode

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

Step 1 In the Cisco Spaces dashboard left-navigation pane, click IoT Service > Device Management > Devices, and then click AP Beacons.

#### Figure 13: List of AP Beacons

Figure 14: Select an AP to Configure

	=	Dashboard v	Но	me Devices	Groups Pol	cles	Settings							
	~	Home Location Hierarchy Integrations Monitor	All Ca All Pro 3	mpuses	Sensors AP Sensors 2 Disabled		Transmit Beacon		Transmit dystone UID		Tratsmit Eddystone URL O	Scan Scan Mode 3	Dual Mode 0	
	8	Admin Management	0		3									
	\$	Setup		Map View	V Filters Actions ~	Bulk Re	quest History BLE	AP Model	Profile Type	Label	Location		As of: Feb 1, 202 BLE Firmware Version	4 8:59 PM
loT Services	\$	Setup About IoT Services						AP Model C9136I-B	Profile Type Scan	Label	Location DNA Spaces IoT Dev Test-	>Building 19->Main Floor		
0 IoT Services	*			Mac Address 68:7dtb4:5f:66:e0	AP Name 🔺	Label	BLE						BLE Firmware Version	AP Beaco

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

🗧 Dashboard 🗸 🗸	Home Devices Groups Policies Settings
යි Home	Floor Beacons AP Beacons Wired Sensors () Cameras () Smart PDUs ()
Location Hierarchy	All Campuses
Integrations	All Profiles AP Sensor Transmit Transmit Transmit Scan Dual AP Sensors IBeacon Eddystone UID Eddystone URL Scan Mode Dual Mode
Monitor	4         2         0         0         0         4         0
Admin Management	
IoT Services	Needs Config Chi Disabled
{Ô} Setup	
	Click to configure an AP beacon.
	List View Map View 🗸 Filters Action and Request History As of: Jan 31, 2024 8:40 AM 🔗 Refresh
	Mac Address Article Label BLE AP Model Profile Type Label Location
	et:38:76:42:addo CW9168I-8 Scan - DNA Spaces IoT Dev Test->Building 19->Main Fi

**Step 3** In the **Settings** area, click **BLE**.

Figure 15: Enable BLE

		0	Q
Home Devices Groups	Policies Settings	AP Beacon - 00:df:1d:87:6e:00 Out of Sync BLE	×
All Campuses V		Heard 2 minutes ago Heard 6 minutes ago	
All Profiles 4 All Profiles 4 AP Sensors 2 Disabled 2 List View Map View V Filters Action	0	IOx App - Zigbee Capable   Yes Channel Last Heard IOx Capable   Yer USB Capable   Yer USB Capable   Yer Click BLE to Enable BLE BLE	
Mac Address AP Name		La	
	Ar model	> Request History	
Out of Sync AP00DF.1D86.2	5A8 C9105AXW-B	-	
78:72:5d:ee:2b:80 Oit of Symc Development_A	P_3 AIR-AP4800-B-K9	·	

**Step 4** In the **BLE mode** area for the **Scan** option, click **Enable**.

#### Figure 16: Enable Scan Mode

AP Beacon - e4:38:7e:42:ad:e0	nc Sensor BLE	×
Sensor		
BLE		
<ul> <li>Before enabling BLE, you need to select BLI properly.</li> </ul>	E mode for the beacon to function	Enable Scan
BLE mode		
S Scan Scans for nearby bluetooth devices	Enable	
Transmit Only does beacon transmitting	Enable	
D Dual Does both Scan & Transmit	Enable	
> Sensor Information	•	<b>2</b>

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

**Step 5** 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.

L

#### Figure 17: Configuration Status

USB Capable	∵e0 ✓ Yes	f Sync Sensor	a Mode Connector					
Settings		Observe the status of configuration here						
Sensor Informati	on							
Request History								
				Export				
Operation	Status	Initiated At 👻	Last Updated At	Status Message				
Operation DISABLE BLE	Status • SUCCESS	Initiated At  Jan 31st, 2024 11:36:14 AM 16 minutes ago	Last Updated At Jan 31st, 2024 11:36:16 AM 16 minutes ago	Status Message				
-	/	Jan 31st, 2024 11:36:14 AM	Jan 31st, 2024 11:36:16 AM					
DISABLE BLE	success	Jan 31st, 2024 11:36:14 AM 16 minutes ago Jan 31st, 2024 11:34:05 AM	Jan 31st, 2024 11:36:16 AM 16 minutes ago Jan 31st, 2024 11:34:09 AM	Successfully ack				

## **Configure AP as a Beacon in Transmit Mode**

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

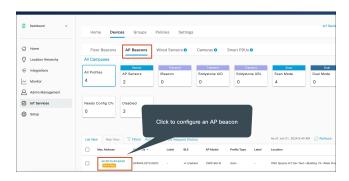
**Step 1** In the Cisco Spaces dashboard left-navigation pane, click **IoT Service > Device Management > Devices**, and then click **AP Beacons**.

Figure 18: List of AP Beacons

	<ul> <li>ethic Spaces</li> <li>Dashboard</li> <li>Home</li> <li>Location Herarchy</li> <li>Integrations</li> <li>Monitor</li> <li>Admin Management</li> </ul>	×	Hor All Car All Prof 3	npuses	Groups Pol AP Sensors 2 Disabled 3		Settings Transmit Beacon D	E	Trensmit (ddystone UID )		Transmit Eddystone URL O	Scen Scan Mode 3	Dust Mode 0	
	IoT Services		0		3	_								
	💮 Setup			Map View	∀ Filters Actions      ✓     AP Name	Bulk Re	quest History BLE	AP Model	Profile Type	Label	Location		As of: Feb 1, 202 BLE Firmware Version	4 8:59 PM
loT Services	About IoT Services		0	68:7d:b4:5f:66:e0 Out of Sync	AP587D.845C.1E00		✓ Enabled	C9136I-B	Scan		DNA Spaces loT Dev Test-	Building 19->Main Floor	3.2.4	Feb 1st, 203 7 minutes ap
{Ĝ} Setup	IoT Gateways	iow		1c;d1;e0;65;c3;40	AP84F1.4782.8868		✔ Enabled	C9115AX0-B	Scan		DNA Spaces loT Dev Test-	Building 19->Main Floor	2.7.21	9.
	Device Management	2. 		1c:d1:e0:79:8e:a0	AP84F1.47B3.31D4	-	✓ Enabled	C9115AXI-B	Scan	-	DNA Spaces IoT Day Test-	Building 19->Main Floor	2.7.21	Space

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

#### Figure 19: Select an AP to Configure



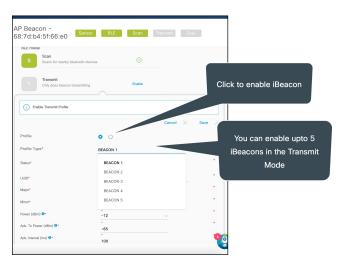
Step 3In the BLE mode area for the Transmit option, click Enable.Figure 20: Enable BLE

Hom				Settings	AP Beacon - Out of Sync Sensor BLE e4:38:7e:42:ad:e0 Scan ransmit Dual X
-	2		)	0	As of: Jan 31st, 2024 08:44:29 AM 🛛 Refresh Sync 🚅
Needs Cr		abled			> AP Information
0	2				~ Settings
List View	Map View	Filters Actions ~	Bulk Re	puest History	Sensor
• •	lac Address	AP Name +	Label	BLE	BLE
	e4:38:7e:42:ad:e0 Out of Syst	AP6849.9275.08C0	-	✓ Enabled	BLE mode
	68:7d:b4:5f:68:e0	AP687D.845C.1E00		✓ Enabled	S Scans for nearby bluetooth devices
	1e:d1:e0:65:e3:40	AP84F1.4782.8868		✓ Enabled	T Transmit Enable Only does beacon transmitting
	1c:d1:e0:79:8e:a0 Out of Sysc	AP84F1.47B3.31D4		✓ Enabled	Dual Eine 😲

**Step 4** In the **Enable Transmit Profile** area, you can configure this beacon in two modes. Do one of the following:

• Check the first checkbox to enable iBeacon. From the **Profile Type** drop-down, choose one of the beacons. Configure the remaining values for the iBeacon's payload.

Figure 21: Configuring an AP as an iBeacon



I

- **Note** APs can support up to five iBeacons in the **Transmit** mode. For more information, see iBeacon Transmit Mode, on page 24
- Select the second checkbox to enable Eddystone. Configure the values for the Eddystone payload.

Figure 22: Configure an AP Beacon as an Eddystone

	e0	Sensor BL	E		>
Before enabling B	LE, you need to select BLE	mode for the beacon to funct	ion properly.		
BLE mode Scan Scans for r	nearby bluetooth devices	Enable		to enable dystone	
T Transmit Only does	beacon transmitting	Enable	7/		
i Enable Transmit I	Profile				
			Cancel $ imes$	Save 🗸	
Profile Profile Type*	E		Cancel ×	Save 🗸	
	•	00000000000000000000000000000000000000	Cancel ×	Save 🗸	
Profile Type*		DDYSTONE UID	Cancel ×	Save 🗸	

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

**Step 5** 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.

Figure 23: Configuration Status

Settings			erve the status	
Sensor Informat	tion			-
Request History	,			
				Export
Operation	Status	Initiated At 🔻	Last Updated At	Status Messag
Operation DISABLE BLE	Status • SUCCESS	Initiated At  Jan 31st, 2024 11:36:14 AM 16 minutes ago	Last Updated At Jan 31st, 2024 11:36:16 AM 16 minutes ago	
-		Jan 31st, 2024 11:36:14 AM	Jan 31st, 2024 11:36:16 AM	Successfully ac
DISABLE BLE	SUCCESS	Jan 31st, 2024 11:36:14 AM 16 minutes ago Jan 31st, 2024 11:34:05 AM	Jan 31st, 2024 11:36:16 AM 16 minutes ago Jan 31st, 2024 11:34:09 AM	Status Messag Successfully ac Successfully ac Successfully ac

# **Configure AP as a Beacon in Dual Mode**

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

Step 1In the Cisco Spaces dashboard left-navigation pane, click IoT Service > Device Management > Devices, and then click<br/>AP Beacons.

Figure 24: List of AP Beacons

	💲 Dashboard 🗸 🗸												
	Home     Location Hierarchy     Integrations	All Car All Prot 3	npuses	Groups Poli Sensor AP Sensors 2		Settings Transmit eacon		Transmit dystone UID		Transmit Eddystone URL O	Scan Mode 3	Dual Mode 0	ıl
	Monitor	Needs	Config Change	Disabled									
	Admin Management	0		3									
	IoT Services	0		3									
		List View	Map View Mac Address	3	Bulk Req Label	uest History BLE	AP Model	Profile Type	Label	Location		As of: Feb 1, 20 BLE Firmware Version	
IoT Services	IoT Services	List View		$\overline{V}$ Filters Actions $\sim$			AP Model C9136I-B	Profile Type Scan	Label	Location DNA Spaces IoT Dev Text-I	Building 19->Main Floor		AP Be
	<ul> <li>IoT Services</li> <li>Sotup</li> </ul>		Mac Address 68:7d:b4:5f:66:e0	✓ Filters Actions ∨ AP Name *	Label	BLE						BLE Firmware Version	AP Be

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

#### Figure 25: Select an AP to Configure

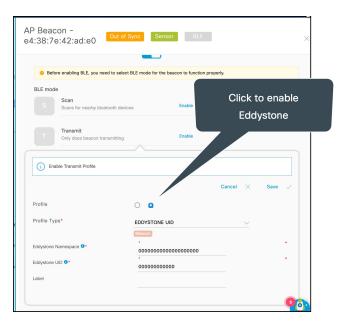
s	Dashboard ~	Home Dev	ices Groups F	Policies Setting	5			IoT Se
ŵ	Home	Floor Beacons	AP Beacons	Wired Sensors 0	Cameras 0	Smart PDUs 0		
0	Location Hierarchy	All Campuses	<u> </u>					
÷	Integrations	All Profiles	Sensor AP Sensors	Transmit	Transmit Eddystone UID	Traterrit Eddystone URL	Scan Scan Mode	Dual Mode
<u>~</u>	Monitor	4	2	0	0	0	4	0
8	Admin Management							
0	IoT Services	Needs Config Chi	Disabled					
@}	Setup	0	2	Click to config	jure an AP bea	acon		
		List New Map Vie	w V Fitters Activ	are Request His	itory		As of: Jan 31, 2024 8:40	AM 📿 Refres
		Mac Address	1	Label BLE	AP Model	Profile Type Label	Location	
		04:38:7e:42 04:01:7e:42	ad.e0 AP6849.9275.08C	0 - 🖌 En	ibled CW9166I-B	Scan -	DNA Spaces lot Dev Test	->Building 19->Main

- **Step 3** In the **BLE mode** area for the **Dual** option, click **Enable**.
- **Step 4** In the **Enable Transmit Profile** area, you can configure this beacon in two modes. Do one of the following:
  - Check the first checkbox to enable iBeacon. Configure the remaining values for the iBeacon's payload. *Figure 26: Configuring an AP as an iBeacon*

Only does beacon transr	nitting	Enable			
Dual Does both Scan & Trans	rit	Enable		Click to er	nable iBeacon
i Enable Dual Mode Profile			Cancel X Save		
Profile	0 0				ou can configure onl
Profile Type*	BEACON				
UUID*	BEACON			or	ne iBeacon in the Dua Mode
Major*	0			•	Widde
Minor*	0			•	
Power (dBm) 0*	-12				
	-65			1	
Adv. Tx Power (dBm) 0*					
Adv. Tx Power (dBm) 0* Adv. Interval (ms) 0*	100				

- **Note** APs can support only one iBeacon in the **Dual** mode. For more information, see iBeacon Transmit Mode, on page 24
- Select the second checkbox to enable Eddystone. Configure the values for the Eddystone payload.

Figure 27: Configure an AP Beacon as an Eddystone



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

**Step 5** 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.



### **AP** as a Gateway

- Access Point as a BLE Gateway, on page 33
- Configure an AP as a Bluetooth Low Energy (BLE) Gateway, on page 33
- Uninstall or Upgrade an IOx Application on an Advanced Gateway, on page 36

### 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 Bluetooth Low Energy (BLE) gateways:

- **Base BLE Gateway**: The Base BLE gateway is a type of AP that you can configure in different modes (Transmit, Scan, or Dual).
- 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 (which is now a base or advanced gateway) in **Scan** mode, **Transmit** mode, or **Dual** mode. In the **Transmit** mode or **Dual**, mode the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles.

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

### 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 Service > IoT Gateways > AP Gateway**.
- Step 2 Click Add New Gateways.
- **Step 3** In the Activate IoT Services window that is displayed, choose Wireless.

#### Figure 28: Activate IoT Service (Wireless)

Activate IoT Services			×
	What would you liil If you want to enable IoT services on both wireless and steps and come back is	d wired devices, choose one option and complete the	
	Wireless You must have a connector installed and dodd compatible APs on the connectors before you all proceed with this. The gateway can be deployed all the compatible APs. Compatible devices: Catalyst 1800 series controllers and 9100 series APs	Wired Supported switches on the connector installed and added supported switches on the connectors before you proceed with this. The gataway can be deployed all the compatible switches. You need to configure certain parameters manually. Compatible devices: Catalyst 9300 and 9400 series switches	
			Previous Next

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

#### Figure 29: List of Supported Devices

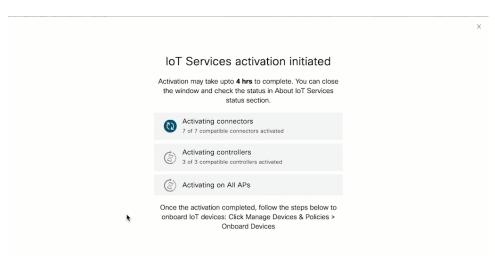
Activate IoT Services			×
	loT services will be a	activated on	
	7 of $9$ compatible connectors	Takes upto 3 hrs, 30 mins	
	2 connectors not responding, hence IoT services w	ill not be activated on them.	
	3 of $3$ compatible controllers	Takes upto 30 mins	
	All Compatible APs on all locations	Takes upto 10 mins/AP	
	Activating IoT services on the supported APs mins/AP. You can initiate the activation and cheo services" page.		
	Activate		
	Activate IoT services on		
	Click here for customization	lion	

Step 4 To activate IoT service (wireless) on all devices on your network, in the IoT services will be activated on window, click Activate.

This activation of IoT service (wireless) automates the following tasks:

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

#### Figure 30: Activate IoT Service (Wireless) on all devices



#### **Step 5** To activate IoT service (wireless) only on specific devices of your network, do the following:

- a) Choose one or more connectors to activate IoT service (wireless).
- b) To activate the wireless gateway, click Activate Wireless.
- c) In the Deploy Wireless Gateway window, select the APs on which you want to activate IoT service (wireless).

#### Figure 31: Activate IoT Service (Wireless) on Preferred Devices

Activate IoT Services	x	
	IoT services will be activated on	
	5 of 8 compatible connectors Takes upp 2 hrs, 30 mins	
	3 connectors not responding, hence IoT services will not be activated on them.	
	2 of 2 compatible controllers Takes upto 20 mins	
	All Compatible APs on all locations Takes upto 10 mins/AP	
	Activating IoT services on the supported APs may take upto 2 hrs, 50 mins + 10 mins/AP. You can initiate the activation and check the status in the "About IoT services" page.	
	Activate	
	Activate IoT services on selected?	
	Click here for customization	

Figure 32: Activate IoT Service (Wireless) on Preferred Devices

	e the acccess points that you want to	aobiol Berotrol		SELECTED APs
	Select All Supported APs	Gateway Capability	Status	2/23
2	RTB2-Russel-C9105	Gateway Not Supported	NA	APs
	Russell-2CF8	Advanced Gateway	Not Activated	AF 5
	RTB2_9115I_2	Advanced Gateway	Base Gateway Activated	1 Aps with Advanced BLE Gateway support
	RTB3-9130AXE-Marlin4-22	Advanced Gateway	Not Activated	BLE datomay support
	RTB2-9117-2	Advanced Gateway	Not Activated	
	RTB2-9117I	Advanced Gateway	Base Gateway Activated	
	Sid-4800-1	Gateway Not Supported	NA	
	CM64-2C60	Gateway Not Supported	NA	
	RTB1-Cornwall-9130	Base Gateway	Advanced Gateway Activated	
	RTB2-9124I	Gateway Not Supported	NA	
	AP5CE1.7628.0D60	Gateway Not Supported	NA	

#### What to do next

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

# Uninstall or Upgrade an IOx Application on an Advanced Gateway

You can uninstall or upgrade IOx applications on advanced gateways. The Cisco Spaces: BLE Management is one such 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 Service > 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 un-installation or upgrade. Do one of the following:
  - 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.

IoT S	ervices 🕢							
IoT Gatew	<u> </u>							
Device M	anagement							
Device M	onitoring			BLE MODE	SUAN	BLE TYPE	base	
	© 10/10			BLE Firmware version	2.7.16	Location	System Campus->Building 19->Cisco DNA Customer Lab	×
	AP Gateways deploy	red	Advanced B	Ethernet Mac	04:eb:40:9e:29:34	Floor Beacon Channel Last Heard	Sep 22nd, 2021 03:36:50 PM s few seconds ego	
				AP Beacon Channel Last Heard	Sep 22nd, 2021 03:02:48 PM 34 minutes ago	IOx App Channel Last Heard	-	
AF	Gateways (10) All	APs (10)		Zigbee Capable	✓ Yes	IOx Capable	✓ Yes	
_				BLE Capable	✓ Yes	USB Capable	✓ Yes	
	List View Map View	$\overline{V}$ Filters Actions $\checkmark$ Bulk F	equest History	Attributes			Edit 🗹	
	Mac Address	Floor Beacon Channel Status *	IOx App Channel Status	✓ App Manager	nent	100 million (100 m	k to install	
	04:eb:40:9f:b0:00	O UP		Available Apps				
	04:eb:40:9f:a7:e0	O UP	• UP	BLE App Up Enable cr	NA Spaces BLE Managemen grade to v1.2.7 onfiguration of BLE radio within ble access points	L.		
	04:eb:40:9f:af:e0	O UP	O UP	Desuest liliste			-	

#### Figure 33: Uninstall or Upgrade Cisco Spaces: BLE Management

Figure 34: Uninstall Cisco Spaces: BLE Management

A gear icon appears beside the application that allows you to upload log files to connector. You can also download these files to assist a technical support team.

Figure 35: 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 Service does not retain these credentials.

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

Figure 36: App Management: Progress of Uninstall or Upgrade

		··· 0 8
Access Point - : Home : HOLDON		>
	As of: Jul	2nd, 2020 02:17:48 AM 📿 Refresh
> AP Information		
<ul> <li>App Management</li> </ul>		
Available Apps		
Cisco DNA Spaces BLE Management App va.3.43 Enable configuration of BLE radio within compatible access points	Install	<ul> <li>There is a request in progress to install this app</li> </ul>
Successfully queued request to install IOx app		
> Request History		

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

	Installed Apps			0
	BLE Cisco DNA App = = = = Enable confi	Spaces BLE Manag guration of BLE radio w access points	<b>命</b> 森	t i
v F	Request History			
	Operation	Status	Number of Retries	Initiated At 👻
	Operation IBEACON CONFIG	Status IN PROGRESS	Number of Retries	Initiated At Sep 14th, 2020 04:26:00 PM a day ago
				Sep 14th, 2020 04:26:00 PM

Figure 37: Uninstall or Upgrade Status in the Request History Area

The Status column shows the status of Uninstall or Upgrade on each AP.

- SUCCESS: Uninstall or Upgrade of application on the AP was a success.
- FAILURE: Uninstall or Upgrade of application on the AP was a failure.
- IN PROGRESS: Uninstall or Upgrade 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, or the status of IOX installation. 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 38: Deployment Status

Deployment Status
10 🕑 0 🞯 0 😣 Deployed In Progress Failed
View Detailed Status

#### Figure 39: Deployment Status

					×
Deployme	nt Status				~
<u>â</u> 10/10	Ocompleted			10 🕑	) 🕑
			_	As of: May 21, 20	
					ΞQFind
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

Uninstall or Upgrade an IOx Application on an Advanced Gateway



# **Beacons and Tags**

- Discover Beacons, on page 45
- Claiming a Beacon, on page 50
- Configuring a Beacon on IoT Service, on page 52
- Viewing Sensor Information, on page 54
- Configuring a Location Anchor, on page 57

### **Discover Beacons**

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

- **Step 1** From the Cisco Spaces dashboard, navigate to **IoT Service > Device Management > Devices**.
- Step 2Click on Floor Beacons to view scanned beacons. Click on one of the following: All Profiles, iBeacon, Eddystone UID,<br/>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 40: Beacon Details

Cis	sco DNA Sp	aces						
Home	Devices	Groups						
Floor I	Beacons A	P Beacons	Zigbee COMING SOON					
All Ca	mpuses	×						
Claime 23	ed Beacons	All Profiles 1806	IBeacon 936	Eddystone UID 30	Eddystone URL	Other Profiles 798		
7 Filters	Actions V	Configure Beac	cons		Sort by L Heard		As o	f: Feb 24, 2
	Mac Address	Label	Location		Last Heard 👻	Group Name	Eddystone Namespace	Eddyst
	e9:6b:bf:a5:95:71	-	System Campus->Building 19	9->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 a few seconds ago	2 PM _	abcdef12345678900000	74706
	ca:96:ca:7c:cf:27	÷	System Campus->Building 15	->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:12 a few seconds ago	2 PM _	222222222222222222222222222222222222222	33333
	e1:26:45:7d:82:4	a -	-		Feb 24th, 2021 12:40:05 a few seconds ago	PM _	33333333333333333333333	44444
	ac:23:3f:a2:93:c4	-	System Campus->Building 19	9->Cisco DNA Customer Lab	Feb 24th, 2021 12:40:05 a few seconds ago	PM _	00112233445566778899	abcde1

Step 3Add or delete columns using the three dots on the right.Figure 41: Adding or Deleting Columns

Hom	Device	s Groups				Basic	All	
All C	ampuses	×.				Mac Address	Names	dystone space dystone UID
Claim 23	ed Beaco	All Profiles 1806	IBeacon 936	Eddystone UID 30	Eddystone U 42	<ul> <li>✓ Location</li> <li>✓ Last Heard</li> <li>✓ Group Name</li> </ul>	Adv (dBm)	/. TxPower
Filter	s Actions ~ Mac Address	Configure Be	acons Location		A: Last Heard	Cancel	Group Name	Apply Eddystone
Filter		Label		3->Cisco DNA Customer	Last Heard	• 021 12:40:12 PM		
Filter	Mac Address	Label	Location		Last Heard	• 021 12:40:12 PM ds ago 021 12:40:12 PM		Eddystone
Filter	Mac Address	Label 71 - 7 -	Location System Campus->Building 19		Lab Feb 24th, 2 a few secon Lab Feb 24th, 2	021 12:40:12 PM ds ago 021 12:40:12 PM ds ago 021 12:40:12 PM 021 12:40:09 PM		Eddystone

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

Figure 42: Beacon Details

#### What to do next

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

Figure 43: Cisco Spaces: Detect and Locate



#### Figure 44: 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 Service account claims ownership of the beacon using the order ID of the beacon. If you do not claim the beacon, IoT Service 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 Service.

#### 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 Service > Device Management**.
- Step 2 Click Onboard Devices and choose Floor Beacons.

#### Figure 45: Onboard Devices

IoT Services			
Device Management			Ø 😁
Device Monitoring			IoT Services Help
Device Stats			
* 1806 Floor Beacons	ap Beacons	O)	O Zigbee Devices Paired
	d Tag Tough Beacon 8-3 HD18-3	Beacon Pro BP16-3	
These managed devices can be configured with our partner Onboard Devices Activate your devices purchased in the IoT Device Marker to a group and applying a policy.		ications and Partner applications by adding t	Onboard Devices Anterno Onboard Devices
Device Groups Stats			

#### Figure 46: Onboard Floor Beacons

Select Device Type Select the device type that you want to oriboard	Floor Beacons	
*	Coming Soor	O <sup>N</sup>
Floor Beacons Configure Beacons that are not part of an Access Point.	AP Beacons Use Access Point as Beacon.	Zigbee Configure and orboard Zigbee devices such as lights and locks.
Canning Seen	Cantra Soor	
RFID Tags Inventory traditional active RFID WI-R Tags.	Meraki Cameras Connect to datafeed from Meraki cameras to process actions.	WebEx Telepresence Connect to datafreed of Webex TP units to understand in room davice 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 Service>Device Management**.
- **Step 4** In the IoT Service dashboard, navigate to **Device Management**. Under **Floor Beacons** > **Claimed Beacons**. Verify if the claimed beacon is displayed in this list.

#### Figure 47: Beacon Details

	IoT Services <sub>Gateways</sub>	$\langle$					
Dev							
Dev	vice Monitoring						Ø 😣
nome	Devices Groups						IoT Services Help
Floor B	Beacons AP Beacons	Zigbee co	MING SOON				
	d Beacons All Profiles 1806	IBeac 936		e UID Eddystone U 42	RL Other P 798	rofiles	
Ŷ Filters	Actions V C Mac Address	Claimed Bead	ions	Grou	up Vendor Id	As of: Feb 24, 2021 2: Make	OS PM 📿 Refresh 📩 Export 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
_	20150-50-45-50-35	at a face	Apr 3rd, 2020 09:25:04 PM		VALKT	Card Tax CT10, 2	KNIKT LIGO

#### What to do next

You can now configure the beacons.

# **Configuring a Beacon on IoT Service**

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

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

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

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

#### Figure 48: Beacon Details

≡ Cis	sco DNA Spac	es					
Home	Devices	Groups					
Floor E	Beacons AP I	Beacons	Zigbee comina soon				
All Ca	impuses						
Claime 23		l Profiles 806	IBeacon Eddystone 936 30	UID Eddystone URL 42	Other Profiles		
√ Filters	a Actions ✔ Co	nfigure Beac	ons	Sort by La Heard		As	of: Feb 24, 20
	Mac Address	Label	Location	Last Heard 💌	Group Name	Eddystone Namespace	Eddyst
	e9:6b:bf:a5:95:71	1	System Campus->Building 19->Cisco DNA Custom	Feb 24th, 2021 12:40:12 a few seconds ago	РМ _	abcdef12345678900000	747069
	ca:96:ca:7c:cf:27	-	System Campus->Building 19->Cisco DNA Custom	Feb 24th, 2021 12:40:12 a few seconds ago	РМ _	222222222222222222222222222222222222222	333333
	e1:26:45:7d:82:4a	<i></i>		Feb 24th, 2021 12:40:09 a few seconds ago	РМ _	333333333333333333333333	444444
	ac:23:3f:a2:93:c4	-	System Campus->Building 19->Cisco DNA Custom	Feb 24th, 2021 12:40:09 a few seconds ago	РМ _	00112233445566778899	abcde1

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

#### Figure 49: Adding or Deleting Columns

Home De	vices Groups			Basic	All	
All Campuses	Y			Mac Address	✓ Edd Names	
Claimed Beaco 23	All Profiles 1806	IBeacon Eddystone UID 936 30	Eddystone U 42	<ul> <li>✓ Location</li> <li>✓ Last Heard</li> <li>✓ Group Name</li> </ul>		. TxPower
Filters Action		acons	A:	Cancel	àroup Name	Apply Eddystone
	ress Label		Last Heard	• G		
Mac Add	ress Label 15:95:71 -	Location	Last Heard er Lab Feb 24th, 2( a few second	• 6 021 12:40:12 PM 5s ago 021 12:40:12 PM		Eddystone
Mac Add	ress Label 15:95:71 - 7c:cf:27 -	Location System Campus->Building 19->Cisco DNA Custom	Last Heard er Lab Feb 24th, 2( a few second er Lab Feb 24th, 2( a few second	O     O		Eddystone abcdef12345

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

				a year ago	
IoT Services			Anchor Tag	× No	Q
oT Gateways			Vendor Id	KNKT	
Device Management			Make	Card Tag CT18-3	
Device Monitoring Groups			Order Id	KNKT-H02	
Floor Beacons AP Beacons	Wired Devices (	0	<ul> <li>Beacon Configuration</li> </ul>	n	
All Campuses					
			Eddystone U	ID	
Claimed Beacons All Profiles	IBeacon	Eddyston	Name Space		
48 3645	1864	89	f7826da6bc5b71e089	93e	
			Instance Id		
			123456789099		
List View Map View V Filters	Actions 🗸 Coungure	Beacons	Interval(ms) 200		
Mac Address Mac Address	ype Name Cl	aimed At	Transmit power level* -8	$\sim$	
d1:fe:59:4a:77:2c -		or 3rd, 2020 09:25:04 PM	Enter Transmit pow	er level	
	ay	year ago			
				Save 🗸	
				Save 🗸	
			Eddystone U		
			Eddystone U		
			Eddystone U	JRL	
			Eddystone U	JRL	
				JRL	
			IBeacon	IRL Save 🗸	
			UUID 88888888-8888 Major	IRL Save 🗸	
			IBeacon UUID 88888888-8888-8888	IRL Save 🗸	
			UUID 88888888-8888-888 Major 333 Minor	IRL Save 🗸	
			UUID 88886888-8888-888 Major 333 Minor 33	IRL Save 🗸	
			UUD B8888888-8888-888 Major 333 Minor 33 Interval(ms)	IRL Save 🗸	
			UUID B8888888-8888-8888 Major 333 Minor 33 Interval(ms) 200	IRL Save 🗸	
			UUD B8888888-8888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level*	IRL Save 🗸	
			UUID B8888888-8888-8888 Major 333 Minor 33 Interval(ms) 200	IRL Save ✓	
			UUD B8888888-888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level* -8	IRL Save  B-8 er level	
			UUD B8888888-888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level* -8	IRL Save ✓	
			LUID B8888888-8888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level* -8 Enter Transmit power	IRL Save  B-8 er level	
			UUD B8888888-888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level* -8	IRL Save	
			LUID B8888888-8888-888 Major 333 Minor 33 Interval(ms) 200 Transmit power level* -8 Enter Transmit power	IRL Save	

#### Figure 50: 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 Service > Device Management > Devices**.
- **Step 2** Click the **Floor Beacons** tab and click the profile. Choose the floor beacon of your choice.

#### Figure 51: Beacon Details

IoT Servic loT Gateways	es 🔇					
Device Manager	nent					
Device Monitorii	ng					IoT Services Help
Floor Beacons AP B	eacons Zigbee <sup>co</sup>	MING SOON				
All Campuses Claimed Bescons 23 All 18			Eddystone URL 42	Other Profiles 798	As of: Feb 24, 2021 2:05 PM	⊖ Refresh Export
Mac Address	Name	Claimed At	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
		Apr 3rd, 2020 09:25:04 PM		MA INT	017 0710 0	VALUET LINE

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

Configuration

Figure 52: Status of Configuration on IoT Service

### **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 Service > 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**

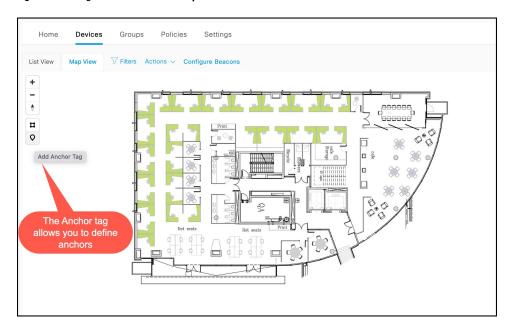
Step 1 From the Cisco Spaces dashboard, navigate to IoT Service > Device Management > Devices.

**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 53: Anchor Tag

	Dervices () vays anagement onitoring	6				Base Mac Address - f9:a	if:b0:21:3b:e1
		Groups	Policies Settin	igs			As of
Flo	or Beacons A	P Beacons	Wired Devices ()			<ul> <li>Device Information</li> </ul>	
All Can	npuses					Mac Address	f9:af:b0:21:3b:e1
Claimed	d Beacons All	Profiles	IBeacon	Eddystone L	IID Eddystone U	Mac Address Type Name	- 81r30003
12	14	0	68	7	15	Claimed At	Jan 19th, 2022 11:38:14 PM
						Anchor Tag	× No
						Vendor Id	SMSD
List Vie	W Map View	V Filters Actio	ns \vee Configure Be	acons		Make	SSD002_02
	Mac Address	Click	a claimed bea	nware	Claimed At 👻	Order Id	SMSD-4HNZY-1
0	f9:af:b0:21:3b:e1	to	see whether ar hor tag has be	n i	Jan 19th, 2022 11:38:14 I 5 months ago	> Beacon Configuration	
	d7:7b:38:8b:bd:37	-	specified.	a	Jan 19th, 2022 11:38:14 I 5 months ago	> Request History	
0	e2:f8:58:2a:e6:dc		1uu3L4	2.1	Jun 23rd, 2021 04:23:19 . a year ago		

Step 3Click Map View and navigate to the required floor. From the list of icons in the left pane, click the Add Anchor Tag.Figure 54: Adding Location Anchor in Map View



- **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 55: Position Anchor Tag

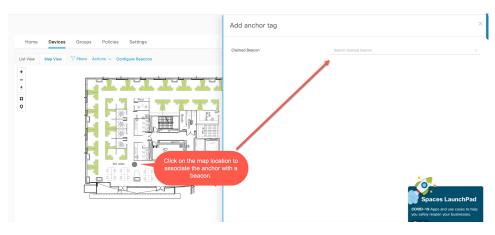


Figure 56: Configure Claimed Beacon as Location Anchor

Add anchor tag		×
Claimed Beacon	10UC2BV - cd:2e:c9:2c:bd:d3	V
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	КИКТ	
Make	Lanyard Tag	
Order Id	KNKT-RMK-2	
Hierarchy	-	
×	82.50	
Y	140.77	
Z	0	^ 
Zone	Search zone	$\vee$

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



# **AP** as a Sensor

• AP as a Sensor, on page 61

## AP as a Sensor

You can now configure the following access points as sensors:

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

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

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

### **Enabling or Disabling an AP Sensor**

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

#### Figure 57: AP as a Sensor

		olicies	Settings								
Floor Beacons	AP Beacons W	Vired Device	es 0								
All Campuses	v										
All Profiles	Sensor AP Sensors	IBe	Transmit	Trans Eddystone		Transmit Eddystone URL	Scan Scan Mode		Dual Iual Mode		
23	9	2		0			13	(			
Needs Config Change	Disabled										
7	14	s 🗸 Bulk Rei	quest History							As of: Jun 2, 20	022 10:32 A
7		s 🗸 Bulk Rei BLE	quest History AP Model	Profile Type	Label	Location		BLE Firmware Vers	ion AP Beac	As of: Jun 2, 20	
7 List View Map View	14 V Filters Actions AP Name *			Profile Type Scan	Label	Location System Campus->Bidg-20-Sensor->S	lensor-Floor	BLE Firmware Vers 2.7.16		on Channel Last Hean	
7 List View Map View Mac Address	14 V Filters Actions AP Name *	BLE	AP Model		Label -				Apr 29th a month a	2022 09:14:04 PM	
Z         List View         Map View           Mac Address         00 s3 8e:43:e4:20	14 Filters Actions AP Name • AP1815L7588	BLE	AP Model AIR-AP1815I-B-K9	Scan	Label - -			2.7.16	Apr 29th a month a Oct 21st, 7 months	on Channel Last Hear 2022 09:14:04 PM 99 2021 04:12:16 AM ago	a wu
Z         List View         Map View           Mac Address         00:a3:8e:43:e4:20           b0:90:7e:9e:f20         b0:90:7e:9e:f20	14           ✓ Fiters         Actions           AP Name •         AP1815L7588           AP1815L7588         AP1832L5028           AP1852L5028         AP1852L7068	BLE ✓ Enabled  ✓ Enabled	AP Model AIR-AP1815I-B-K9 AIR-AP1832I-A-K9	Scan	Label - - -			2.7.16 2.7.19	Apr 29th a month a Oct 21st, 7 months Oct 21st, 7 months	on Channel Last Hear 2022 09:14:04 PM 99 2021 04:12:16 AM ago	d WU
7           List View         Map View           Mac Address           00 a3 8e.43 e4.20           b0 90.7e.99.cf.20	14 V Filers Actions AP Name • AP1815L7588 AP1832L5628 *21822[7028]	BLE ✓ Enabled  ✓ Enabled	AP Model AIR-AP1815I-B-K9 AIR-AP1832I-A-K9	Scan	Label - -			2.7.16 2.7.19	Apr 29th a month a Oct 21st, 7 months Oct 21st, 7 months	on Channel Last Hean 2022 09:14:04 PM 90 2021 04:12:16 AM ago 2021 04:12:16 AM	d WU

- Step 2Click 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.

AP Beacon 10:f9:20:fd:		Sensor BLE	Scan Transmit	Dual X
			As of: Jun 2nd, 2022	2 10:36:19 AM 📿 Refresh Sync 🖨
✓ AP Information	ion			
Mac Address		10:f9:20:fd:e0:a0	Floor Beacon Channel Status	• DOWN
IOx App Channe	el 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	1	Base	BLE Firmware version	3.2.4
Location		System Campus->SMU-ewlc->smu- ewlc	Ethernet Mac	cc:9c:3e:f4:dd:30
Floor Beacon C 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 Chann Heard	el Last	-	Zigbee Capable	✓ Yes
IOx Capable		✓ Yes	BLE Capable	✓ Yes
USB Capable		✓ Yes		
S Sc Tr	ansmit	by bluetooth devices	C	
	ual bes both Scar rmation	n & Transmit	Enable	Spaces LaunchPad COVID-19 Apps and use cases to help you safely reopen your businesses. Dismiss

#### Figure 58: Enabling or Disabling AP as a Sensor

### **Viewing Sensor Information**

You can view sensor information from the Sensor Information area.

#### Figure 59: Viewing Sensor Information

Sensor Information			
$\overset{}{_{=}} \overset{\text{Total Volatile Organic}}{_{=} (i)} \overset{(i)}{_{=}}$	Quality	Humidity ()	(BETA) Temperature ①
113 PPB	1.78	23.7 %	45.3 ° C
Updated at: Apr 30th, 2022 03:01:12 AM a month ago	Updated at: Apr 30th, 2022 03:01:12 AM a month ago	Updated at: Apr 30th, 2022 03:01:12 AM a month ago	Updated at: Apr 30th, 2022 03:01:12 AM a month ago



# 

# **Device Management**

• Device Management, on page 67



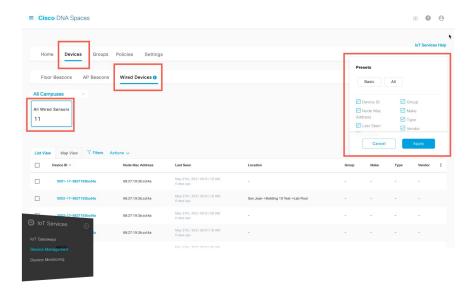
### **Device Management**

- Dashboard View of Devices, on page 67
- Configuring Beacons, on page 68
- Categorizing Devices into Manual Groups, on page 68
- Categorizing Devices into Groups (Dynamic Groups), on page 69
- Applying Policies to Beacons, on page 71
- Filtering Devices, on page 76

### **Dashboard View of Devices**

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

Figure 60: Dashboard View of Devices

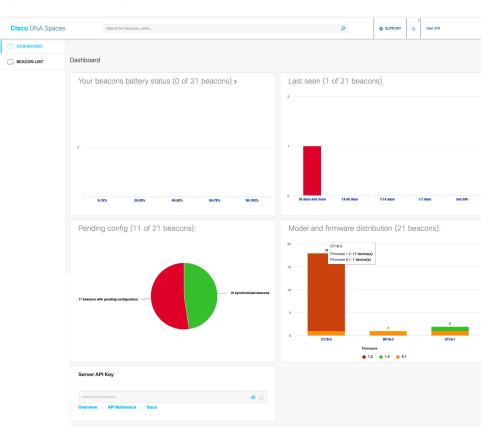


#### **Configuring Beacons**

Navigate to **IoT Service** > **Device Management** > **Devices** > **Floor Beacons** > **Configure Beacons**. The window that opens is referred to as the Device Manager in this document.

The Device Manager dashboard gives you a general overview of your beacon infrastructure. All beacons claimed by IoT Service are visible on the Device Manager dashboard. You can see actionable graphs which allow you to navigate quickly to a subset of devices. For example, beacons with 0 to 19 percent battery life, or all beacons with the same underlying firmware or model

Figure 61: The Device Manager Dashboard



### **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 Service dashboard, you can filter devices by groups.

- **Step 1** In the Cisco Spaces: IoT Service 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.

Delate Beacons     Add to group     Add to group     Second Parameter Building To Provide Table	IoT Services I
Building 19 Claimed Beacons All Profiles 1917 952 Eddystone UID Eddyston	Refresh ₼ Ei
Citizend Bascons         All Profiles         Biblio         Eddystone UBL         Other Profiles           73         1917         952         41         35         889	Refresh ⋔ Ei
7 Fitters     Actions ~ Configure Biascons     As of Arr 21, 2022 954 AM     C       Polleties Biascons     East Heard ~     Group Name     Peelline Type     Building of Group Name       Add to group     Eastern Descenario Mark from the Construction & Apr 211, 2022 954 AD     Apr 211, 2022 954 AD     C	Refresh 🔥 Er
Dutitie Descens         van Type         Label         Location         Late Haard -         Once Name         Profile Type         Eathery         Udges Id         Premiume         Address           Add to group         Add to group         Same         Add to group         Same         -	Refresh ሰ E
Delete Beacons     Add to group     Setter Common Bilders 16, Chain Tok Contract 1 A     Alf 214, 2022 0954-03 AM     Banasa     The Contract Contract 1 A	
	dv. TxPower (dBm)
Remove from group	7
Remove rom group Add Attributes System Campus-Heading 19-Cloco DMA Customer Lab AP 2110, 2022 05-54:03 AM Beacon	7
ex83xex39xex81 - System Campus->Bulding 19->Claco DNA Customer Lab Apr 21st, 2022 0754:03 AM Beacon	7
System Cempuel-Shulding 19->Disco DNA Customer Lab Apr 21a; 2022 05545040 AM - Kontakt - 100% VLDiv 2.0 -	

Figure 62: Adding Devices to a Manual Group from the Devices tab

### **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 Service dashboard, you can filter devices by groups.

- **Step 1** In the Cisco Spaces: IoT Service 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 63: Group by MAC Prefix

Dynamic Grouping				
	Group by MAC Prefix MAC Prefix axbb     Group by Vendor Code Vendor Code     Code     Group by Location Hierarchy System Campus			
		Cancel	Back	Create Group

#### Figure 64: Group by Vendor Code

Dynamic Grouping		
	Group by MAC Prefix MAC Prefix Group by Undar Code Vender Code Vender Code Contact.lo Group by Location Herarchy	
	System Campus V	Cancel Back Create Group

#### Figure 65: Group by Location Hierarchy

Dynamic Grouping		
	C Group by MAC Prefix MAC Prefix C Group by Windor Code Wendor Code Wendor Code Code C Group by Location Hierarchy Building 19 V	
		Cancel Back Create 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.

#### 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 Service dashboard, click Device Management > Policies and then Create a new policy.

 Figure 66: Creating a New Policy

Cis	co DNA Spaces										Ø 6
Но	me Devices	Groups	licies	Settings							IoT Services Help
Polici	es (2) Actions V Al								As of: Apr 11, 2022 3:42 PM		Create a new polic
U	Policy Name	Description	Туре	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
	T Services <sup>ateways</sup>	$\odot$							Show	v Records: 50 🗸	1-2 < 0

**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 67: Choosing One of Four Policies

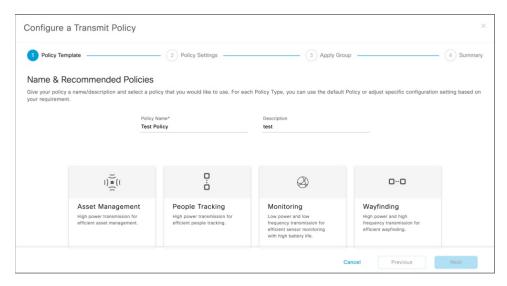


Table 5: Types of Transmit Policy

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 frequency 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 68: Configure a Transmit Policy

Policy Template	Policy Settings		Apply Group		4 Sum
sset Management		Notification			٦
ese actions will be taken when this policy is applied to a device		Subscribe to notifications	that will be sent when this policy is applied to a devi	ce	
Selected Profile IBEACON CO		To:		R	
uuo.					
Ocedf1ae-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*					
Enter Transmit power level					
29 March 1					
interval(ms)* 400					
We recommend high frequency for asset tracking. Please note higher frequency means lower battery life.					

**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 69: Choosing a Device Group for Dynamic Policy Application

Config	gure a Transmit Policy			×
Ø P	olicy Template	Policy Settings	3 Apply Group	(4) Summary
This po	bise Device Group licy will be applied to devices belonging to these groups, ate a new group			EQFind
	Group Name *		Description	
	JennyTest		Testing Redis pub/sub	
	TestGroup2		Test Group 2 Description	
	Test1		Steet	
	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	
	mathetest		mathemat	
	JennyDynamicLocation			
	JennyDynamic2			
				Cancel Previous Next

- **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 70: Enabling or Disabling a Policy

=	Cis	co DNA Space	S						:	:: G	0
								Policy - JennyDynamic2			
*	Ho	me Devices	Groups Policie	es Settings			_				
ħ	Polici	ies (3) Actions V	Alerts					Policy Active			
		Policy Name	Description	Туре	Priority	Profile	Applied Gro	Name* JennyDynamic2			
		JennyDynamic2		Group	10		JennyDynan	Description Enter Description			
		JennyDynamicLocation		Group	10	-	Jen man		Cancel $ imes$	Save	1
		9 - E				iber	JennyTest				
	3 Records		Click on a penable or dis polic	sable the							

Figure 71: Viewing Devices on Which a Policy Is Applied

	Policy Name	Description	Туре	Priority	Profile	Applied Group(s)	Active	Create Time	Update Time	Alert Count D
	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	Click to open	8
rd									list of device that has this applied polic	s 🤇 🔍 🔍
						Devices				×
						Devices (1)	√ Filters	×.	As of: Apr 11, 2022 4:10 P	M 📿 Refresh
						Mac A	ddress	Label	Update Time	
						☐ f6:9c:	d2:50:4d:15		Mar 3rd, 2022 06:48:21 AM a month ago	
						1 Records			Show Records: 50 v 1 - 1	< 0 >

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 Service dashboard, click **Device Management > Devices** and then **Floor Beacons > All Profiles**. Select the devices and click **Actions > Add to group**.

#### Figure 72: Creating a New Policy

≡ Cisc	DNA Sp	paces													0 0
Hon	ne Devi	ices Group	ps P	olicies	Settings									IoT Se	nvices Help 😡
Floo	or Beacons	AP Beaco	ins V	Vired Devic	es 0										
Building	g 19	ν.	_												
	d Beacons	All Profiles		IBeacon		Eddystone UID	Eddystone URL	Other Profiles							
73		1917		952	_	41	35	889							
<b>∀</b> Filters	Actions $\checkmark$	Configure Bea	cons									As of: Apr 2	1, 2022 9:54 AM	C Refresh	🖞 Export
•	Delete B	Beacons	ess Type	Label	Location			Last Heard 💌	Group Name	Profile Type	Battery	Unique Id	Firmware	Adv. TxPowe	r (dBm)
	Add to g	group			System C	Campus->Building 19->Cisc	o DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago		iBeacon				-77	
	Add Attr				System C	Campus->Building 19->Cisc	o DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	~	iBeacon			141	-77	
	ea:83:ea:39:ae:1	61 -		÷	System C	Campus->Building 19->Cisc	o DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77	
-	-b-s7-14-37-2b:	24 -		-	System C	Campus->Building 19->Cisc	o 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.

ase Mac Addr	ess - e9:f8:80:c0:8f	:56		
		As of	: Jan 28th, 2022 10	14:23 PM 📿 Refre
Profile Type			iBe	acon Kontakt
Label				Edit
Profile Type	Kontakt	Location		es loT Dev Test- 19->Main Floor
Adv. TxPower (dBm)	-	Mac Address	e9:f8:80:c	
Mac Address Type		Unique Id	VuLouh	
Firmware	2.0	Battery		
Last Heard	Jan 28th, 2022 10:14:14 PM a few seconds ago	Group Name	Manual	
<ul> <li>&gt; Beacon Config</li> <li>&gt; Sensor Information</li> </ul>				
<ul> <li>Request Histor</li> <li>Request Histor</li> </ul>				
noquest mator	y (0)	Confi	ig 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 k	oX App Active or Installed and enabled in s	scan m de Manual		

#### Figure 73: Config Source: Policy

### **Filtering Devices**

While Cisco Spaces: IoT Service scans all devices, you may not want to view certain devices on the dashboard. You can now filter out devices from the Cisco Spaces: IoT Service dashboard using types of MAC addresses. Filtering 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 Service

• 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 74: Filtering Devices by MAC Address
```

Home	Devices	Groups	Policies	Settings			
Filtering		Filter	ing				
		Enal	ble Public MA	٨C			
		Enal	ble Random S	Static MAC			
IoT Services IoT Gateways		Ena	ole Random F	Private MAC			
		ļ					

I



# PART **IV**

## **Device Monitoring**

• Device Monitoring, on page 81



### **Device Monitoring**

From the IoT Service > **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, on page 81
- BLE Devices Battery Life, on page 81
- Last Heard BLE Devices, on page 82

### **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 75: Right Now

■ Cisco DNA Spaces						0	Θ,
Right Now Devices that are not heard recently				As of: May 4th, 2021	01:00:52 PM 📿 Refresh 🖡	oT Service	is Help
Total gateways	10  Advance BLE Gateway:10 Base BLE Gateway:0	O e Advance BLE Gateway:0 Base BLE Gateway:0	Total BLE Devices 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			3 Critical (<10%) ①	0 • Low ③		350 High ©		
						As of: May 4, 2021 1:00 PM	C Refresh	습 Export
3 Beacons need	Device Mac	Location			Battery	Last Heard	Label	Group :
attention	e5:11:b3:d4:b8:72	System Campus->Bui	ilding 19->Cisco DNA (	Customer Lab->Zon	ne1 2%	Apr 1st, 2021 06:03:34 AM a month ago		
1400	ce:fb:5b:79:a6:5d	System Campus->Bu	ilding 19->Cisco DNA (	Customer Lab	0%	Jan 14th, 2021 07:55:25 AM 4 months ago		
1050	ca:6a:50:46:50:35	System Campus->Bu	ilding 19->Cisco DNA (	Customer Lab	0%	Jan 6th, 2021 04:48:06 PM 4 months ago		
700	3 Records		Show Re	cords: 10 💌 1	-3 < 0 >			
350								
0 Critical Low Medium High								
3 0 26 1350 • Critical • Low • Medium • High								

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

Last Heard BLE Devices BLE Devices that are not heard recently		603 17 ● > 24 hrs ago ⊙ ● > 1 hr ⊙	104 246			
* Total BLE Devices				May 4, 2021 1:00	-	fresh 🕆 Expo
3190 2466 0724 0	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 Al 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	·		
>24h	rs (18.90%) a0:7d:ea:19:bf:ed	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 08:30:55 AM 3 days ago			
BLE Devices 603	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 AN 3 days ago			
603 17 104 2466	d5:13:e2:79:5f:32	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 05:04:38 AM 3 days ago			
● >24hrs ● >1hr ● >5min ● <5min	ea:c9:34:56:63:8e	System Campus->Building 19->Cisco DNA Customer Lab	May 1st, 2021 12:03:17 AM			60pp002s



# PART V

## Troubleshooting

- Troubleshooting IoT Services: Controller, on page 87
- Troubleshooting IoT Services: IOx Application, on page 107
- Troubleshooting IoT Services: Cisco Spaces Connector, on page 115
- Troubleshooting IoT Services: Access Point, on page 117



## **Troubleshooting IoT Services: Controller**

- Reprovisioning IoT Services After Failover, on page 87
- What settings are needed to allow access via NETCONF?, on page 87
- The global configuration for BLE radio has to be enabled on Wireless Controller. How do I verify the setting?, on page 88
- For the gRPC connection to work, a streaming token is required on the Wireless Controller. How do I view the token?, on page 88
- gRPC must be enabled in the access point join profile. How do I verify the join profile has gRPC enabled?, on page 89
- How do I verify gRPC is up?, on page 89
- How do I verify that TDL subscriptions are created and are valid?, on page 90
- Are the TDL subscriptions created and valid?, on page 90
- What is the TDL status?, on page 90
- How do I view the current CAPWAP values for an AP?, on page 91
- How do I view the current TDL values for an AP?, on page 99
- How do I get the telemetry connection status?, on page 102
- How do I view IOx AP state and mode?, on page 102
- How do I view gRPC details?, on page 103
- How do I view AP BLE configuration details?, on page 103
- How do I view the current TDL values for AP air quality?, on page 105
- How do I view the current TDL values for AP temperature and humidity?, on page 106

### **Reprovisioning IoT Services After Failover**

### What settings are needed to allow access via NETCONF?

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

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

aaa new-model

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

aaa authentication login default local

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

aaa authorization exec default local

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

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

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

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

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

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

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

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

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

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

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

```
ap cisco-dna token 0 eyJhbGciOiJIUzI1NiISInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2MjUs
ImNpZCI6Mzc4NTc3ODI1NDI2NzIyNjUwMDAsImVwIjoiMTAuMzAuMTE0LjEwODo4MDAwIiwiaW
F0IjoxNTg1NzA2OTIxfQ.56vXfL1IGrss6TJZDQaWVarAoTWZsIhbe3tGVMEJNYk
```

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

ap cisco-dna token 0 <token string>

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

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

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

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

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

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

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

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

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

#### How do I verify gRPC is up?

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

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

controller# show ap grpc summary							
AP Name	AP Mac	gRPC Status					
AP 10.2830	04eb.409f.a7e0	 עף					
AP 02.2898	04eb.409f.ab20	Up					
AP 06.28CC	04eb.409f.acc0	Up					
AP_08.28E0	04eb.409f.ad60	Up					
AP_07.28E4	04eb.409f.ad80	Up					
AP_09.28EC	04eb.409f.adc0	Up					
AP_01.28F0	04eb.409f.ade0	Up					
AP_03.2928	04eb.409f.afa0	Up					
AP_05.2934	04eb.409f.b000	Up					
AP_04.2938	04eb.409f.b020	Up					

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

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

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

show telemetry ietf subscription all

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

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

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

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

### Are the TDL subscriptions created and valid?

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

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

wireless controller# show telemetry ietf subscription all Telemetry subscription brief

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

#### What is the TDL status?

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

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

```
wireless controller# show telemetry ietf subscription 125 receiver
Telemetry subscription receivers detail:
Subscription ID: 125
Address: 10.22.243.33
Port: 8004
Protocol: cloud-native
Profile:
Connection: 33
State: Connected
Explanation:
```

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

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

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

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

test platform software database get ewlc oper/capwap data; wtp mac=mac without dots

#### For example:

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

The output presents a table with various records:

- Index 0 contains the AP's MAC address, IP address, model, and other static information.
- The device\_detail.static\_info section includes the AP's model, memory type, CPU type, and memory size, among other details.
- The device\_detail.wtp\_version section includes backup software version, mini iOS version, hardware version, and the current software version that the AP is running.
- The **ap\_services** section gives details about monitor mode, DHCP server status, and sniffer interface ID.
- The tag\_info section indicates whether the AP has any misconfigured tags.
- The **external\_module\_data** section displays information about any external modules connected to the AP, including product ID and version.
- The ap state section displays administrative and operational states of the AP.
- The ap\_mode\_data section details the current mode and sub-mode of the AP.

```
wireless-controller# test platform software database get
ewlc_oper/capwap_data;wtp_mac=lcdle065c340
Table Record Index 0 = {
  [0] wtp_mac = 1CD1.E065.C340
  [1] ip_addr = 10.22.243.229
  [2] name = AP84F1.47B2.B868
  [3] device_detail.static_info.board_data.model = C9115AXI-B
  [4] device_detail.static_info.board_data.wtp_serial_num = FJC25331LCY
```

[5] device detail.static info.board data.card id = 0 [6] device\_detail.static\_info.board\_data.card\_rev = 0 [7] device detail.static info.board data.wtp enet mac = 84F1.47B2.B868 [8] device detail.static info.board data.ap sys info.mem type = DDR3 [9] device\_detail.static\_info.board\_data.ap\_sys\_info.cpu\_type = ARMv8 Processor rev 0 (v81) [10] device\_detail.static\_info.board\_data.ap\_sys\_info.mem size = 1971200 [11] device detail.static info.board data opt.antenna type = BSN INT ANT AP [12] device detail.static info.board data opt.wtp type = BSN AP STANDARD [13] device\_detail.static\_info.board\_data\_opt.remote = true [14] device\_detail.static\_info.board\_data\_opt.join\_priority = 1 [15] device detail.static info.descriptor data.max radio slots = 2 [16] device detail.static info.descriptor data.radio slots in use = 2 [17] device detail.static info.descriptor data.encryption capabilities = true [18] device\_detail.static\_info.ap\_prov.is\_universal = false [19] device\_detail.static\_info.ap\_prov.universal\_prime\_status = Unprimed [20] device\_detail.static\_info.ap\_models.model = C9115AXI-B [21] device detail.static info.ap models.ap model short = 9115AXI [22] device detail.static\_info.num\_ports = 1 [23] device detail.static info.num slots = 2 [24] device\_detail.static\_info.wtp\_type = 83 [25] device\_detail.static\_info.wtp\_model\_type = 90 [26] device detail.static info.ap capability = [ BRIDGE MODE CAPABLE, CAP THREE SPATIAL STREAMS CAPABLE, ANTENNA SELECTION RESTRICTED CAPABLE, AVC\_FNF\_CAPABLE, RXSOP THRESHOLD CAPABLE, FABRIC CAPABILITY, BARBADOS INTERNAL ANTENNA SKU CAPABLE, REMOTE LAN CAPABLE, DOT11AC 160MHZ CHANNEL WIDTH CAPABLE, AVC\_FNF\_FABRIC\_CAPABLE, AP CTS CAPABLE, AP QCA SPECTRUM\_INTELLIGENCE\_CAPABLE, FIPS CAPABLE, IS DOT1X PORT AUTH CAPABLE, AP\_TRACING\_CAPABLE, AP WPA3 CAPABLE, OFFICE EXTEND CAPABLE, ETH2 RLAN CAPABLE, AP MEWLC CAPABLE, SNIFFER MODE CAPABLE, ICAP\_PARTIAL\_PACKET\_TRACE\_CAPABLE, ICAP\_ANOMALY\_DETECTION\_CAPABLE, ICAP STATISTICS CAPABLE, ICAP FEATURE CAPABLE, AP AWIPS CAPABLE, IOX HARDWARE CAPABLE, AUX CLIENT INTERFACE CAPABLE, CLICKOS FEATURE SET, AP TRAFFIC DISTRIBUTION STATISTICS CAPABLE 1 [27] device detail.static info.remote lan.num rlan ports = 0 [28] device detail.static info.remote lan.rlan slot id = 0 [29] device\_detail.static\_info.remote\_lan.rlan\_port\_can\_be\_zero = false [30] device detail.static info.is cisco ap = true [31] device detail.static info.is mm opt = false [32] device\_detail.static\_info.ap\_image\_name = [33] device\_detail.dynamic\_info.ap\_crash\_data.ap\_crash\_file = [34] device\_detail.dynamic\_info.ap\_crash\_data.ap\_radio\_2g\_crash\_file = [35] device detail.dynamic info.ap crash data.ap radio 5g crash file =

```
[36] device detail.dynamic info.led brightness level = 8
```

```
[37] device detail.dynamic info.led state enabled = true
 [38] device detail.dynamic info.reset button state = false
 [39] device detail.dynamic info.led flash enabled = true
 [40] device detail.dynamic info.flash sec = 0
 [41] device_detail.dynamic_info.temp_info.degree = 0
 [42] device_detail.dynamic_info.temp_info.temp_status = AP TEMP STATUS NORMAL
 [43] device detail.dynamic info.temp info.heater status =
AP TEMP HEATER STATUS BOTH HEATERS OFF
 [44] device detail.wtp version.backup sw version.version = 17
 [45] device_detail.wtp_version.backup_sw_version.release = 7
 [46] device_detail.wtp_version.backup_sw_version.maint = 1
 [47] device detail.wtp version.backup sw version.build = 11
 [48] device detail.wtp version.backup sw version.stringified ver info = 17.7.1.11
 [49] device detail.wtp version.mini ios version.version = 0
 [50] device_detail.wtp_version.mini_ios_version.release =
 [51] device_detail.wtp_version.mini_ios_version.maint = 0
 [52] device_detail.wtp_version.mini_ios_version.build = 0
 [53] device detail.wtp version.mini ios version.stringified ver info =
 [54] device_detail.wtp_version.hw ver.version = 1
 [55] device detail.wtp version.hw ver.release = 0
 [56] device_detail.wtp_version.hw_ver.maint = 0
 [57] device_detail.wtp_version.hw_ver.build = 0
 [58] device detail.wtp version.hw ver.stringified ver info = 1.0.0.0
 [59] device detail.wtp version.sw ver.version = 17
 [60] device detail.wtp version.sw ver.release =
 [61] device_detail.wtp_version.sw_ver.maint = 5
 [62] device_detail.wtp_version.sw_ver.build = 43
 [63] device_detail.wtp_version.sw_ver.stringified_ver_info = 17.3.5.43
 [64] device detail.wtp version.boot ver.version = 1
 [65] device_detail.wtp_version.boot_ver.release = 1
 [66] device detail.wtp version.boot ver.maint = 2
 [67] device_detail.wtp_version.boot_ver.build = 4
 [68] device_detail.wtp_version.boot_ver.stringified_ver_info = 1.1.2.4
 [69] device_detail.wtp_version.sw_version = 17.3.5.43
 [70] ap_lag_enabled = false
 [71] ap location.floor = 0
 [72] ap location.location = default location
 [73] ap_services.monitor_mode_opt_type = ENM_MODE_TYPE_NONE
 [74] ap services.ap dhcp server.is dhcp server enabled = false
 [75] ap services.sniffer ap ifid = 0
 [76] tag_info.misconfigured_tag = APMGR_TAGS CONFIGURED
 [77] tag info.tag source = EWLC TAG SRC DEFAULT
 [78] tag info.is ap misconfigured = false
 [79] tag_info.is_policy_tag_misconfigured = false
 [80] tag_info.is_site_tag_misconfigured = false
 [81] tag_info.is_rf_tag_misconfigured = false
 [82] tag info.is flex profile misconfigured = false
 [83] tag info.is ap profile misconfigured = false
 [84] tag_info.is_rf_profile_24_misconfigured = false
 [85] tag_info.is_rf_profile_5_misconfigured = false
 [86] tag info.is ap tag registration done = true
 [87] tag_info.resolved_tag_info.resolved_policy_tag = default-policy-tag
 [88] tag info.resolved tag info.resolved site tag = default-site-tag
 [89] tag_info.resolved_tag_info.resolved_rf_tag = default-rf-tag
 [90] tag_info.policy_tag_info.policy_tag_name = default-policy-tag
 [91] tag info.site tag.site tag name = default-site-tag
 [92] tag_info.site_tag.ap_profile = default-ap-profile
 [93] tag info.site tag.flex profile = default-flex-profile
 [94] tag info.rf tag.rf tag name = default-rf-tag
 [95] tag_info.rf_tag.dot11a_rf_profile = default_rf_5gh
 [96] tag_info.rf_tag.dot11b_rf_profile = default_rf_24gh
 [97] tag info.filter info.filter name =
 [98] tunnel.preferred mode = PREFERRED MODE IPV4
 [99] tunnel.udp lite = IPV6 CAPWAP UDPLITE UNCONFIG
```

```
[100] external module data.xm data.is module present = false
 [101] external_module_data.xm_data.enable = true
 [102] external_module_data.xm_data.xm.goodness_field = [
        Ο,
        0
]
 [103] external_module_data.xm_data.xm.numeric_id = 12
 [104] external_module_data.xm_data.xm.version = [
        Ο,
        0
]
 [105] external module data.xm data.xm.product id = [
        Ο,
        0
]
 [106] external_module_data.xm_data.xm.serial_number = [
        Ο,
        0
]
 [107] external_module_data.xm_data.xm.max_power = 0
 [108] external module data.xm data.xm.eeprom size = [
```

Ο, Ο, Ο, 0 ] [109] external\_module\_data.xm\_data.xm.xm\_cookie\_version = 0 [110] external module data.xm data.xm.inventory.prod id = C9115AXI-B [111] external module data.xm data.xm.inventory.ver id = 05 [112] external\_module\_data.xm\_data.xm.inventory.serial\_num = FJC25331LCY [113] external\_module\_data.xm\_data.xm.inventory.ent\_name = C9115AX [114] external module data.xm data.xm.inventory.ent desc = Cisco Catalyst 9115AX Series (IEEE 802.11ax) Access Point [115] external module data.xm data.xm.module name = [116] external\_module\_data.xm\_data.xm.version\_string = [117] external\_module\_data.xm\_data.xm.serial\_number\_string = [118] external\_module\_data.xm\_data.xm.product\_id\_string = [119] external\_module\_data.xm\_data.xm.module\_type = [120] external module data.xm data.xm.module description = [121] external module data.xm data.xm.module capabilities = [122] external\_module\_data.xm\_data.xm.module\_state = [123] external\_module\_data.usb\_data.is\_module\_present = false [124] external module data.usb data.enable = true [125] external module data.usb data.xm.goodness field = [ Ο, 0 ] [126] external module data.usb data.xm.numeric id = 12 [127] external module data.usb data.xm.version = [ Ο, 0 1 [128] external\_module\_data.usb\_data.xm.product\_id = [ 85, 110, 107, 110, 111, 119, 110, Ο, Ο, Ο, Ο, Ο, Ο, Ο, Ο,

```
Ο,
        Ο,
        0
1
[129] external module data.usb data.xm.serial number = [
        85,
       110,
       107,
       110.
        111,
       119,
       110,
        Ο,
       Ο,
       Ο,
        0
]
 [130] external module data.usb data.xm.max power = 0
[131] external_module_data.usb_data.xm.eeprom_size = [
       Ο,
       Ο,
       Ο,
        0
]
[132] external_module_data.usb_data.xm.xm cookie version = 0
 [133] external_module_data.usb_data.xm.inventory.prod_id =
[134] external module data.usb data.xm.inventory.ver id =
[135] external module data.usb data.xm.inventory.serial num =
[136] external_module_data.usb_data.xm.inventory.ent name =
[137] external_module_data.usb_data.xm.inventory.ent_desc =
 [138] external module data.usb data.xm.module name = Unknown
[139] external_module_data.usb_data.xm.version_string = V00
[140] external module data.usb data.xm.serial number string = Unknown
 [141] external_module_data.usb_data.xm.product_id_string = Unknown
[142] external_module_data.usb_data.xm.module_type = USB Module
[143] external_module_data.usb_data.xm.module_description = Unknown
 [144] external_module_data.usb_data.xm.module_capabilities =
[145] external module data.usb data.xm.module state = Not Detected
[146] external module data.usb override = false
[147] external_module_data.is_ext_module_enabled = false
[148] external_module_data.expansion_module_extended_info.power sufficient = 0
 [149] external module data.expansion module extended info.antenna product id = [
       Ο,
        Ο,
        Ο,
        0.
        Ο,
        0,
        0,
        Ο,
        0,
        Ο,
        Ο,
       Ο,
        Ο,
        Ο,
        Ο,
        Ο,
        Ο,
        Ο,
        Ο,
```

0, 0, 0, 0,

- 0, 0,
- 0, 0,
- 0,
- Ο,
- 0, 0, 0,

0

- ]

[150] external\_module\_data.expansion\_module\_extended\_info.antenna\_serial\_number = [
 0,

```
Ο,
        0
]
 [151] external module data.expansion module extended info.antenna prod ID =
 [152] ipv6_joined = 0
 [153] wtp_ip_addr = 10.22.243.229
 [154] ap state.ap admin state = ENM ADMINSTATE ENABLED
 [155] ap_state.ap_operation_state = EWLC_ENM_AP_STATE_REG
 [156] ap mode data.home ap enabled = false
 [157] ap mode data.clear mode = false
 [158] ap_mode_data.ap_sub_mode = AP_SUB_MODE_NONE
 [159] ap_mode_data.wtp_mode = EWLC_ENM_SPAM_AP_MODE_LOCAL
 [160] ap_mode_data.ap_fabric_data.is_fabric_ap = false
 [161] ap_mode_data.ap_fabric_data.lisp_state = EWLC_ENM_LISP_QUERY_NOT_NEEDED
```

```
[162] ap time info.boot time = Fri, 05 Aug 2022 06:47:33 +0000
```

```
[163] ap time info.join time = Fri, 05 Aug 2022 06:50:13 +0000
[164] ap_time_info.join_time_taken = 159
[165] ap time info.last up time = 1
[166] country code = US
[167] ap_security_data.lsc_provision_inprogress = false
[168] ap security data.fips enabled = false
 [169] ap_security_data.wlancc_enabled = false
[170] ap security data.cert type = EWLC CERT MIC
[171] ap security data.lsc ap auth type = EWLC ENM LSC AP AUTH CAPWAP DTLS
[172] num_radio_slots = 2
[173] dart_is_connected = false
 [174] dart is connected str = Not Connected
[175] is master = false
[176] sliding window.multi window support = true
[177] sliding_window.window_size = 1
[178] ap_vlan.vlan_tag_state = VLAN_TAGGING_DISABLED
[179] ap_vlan.vlan_tag_id = 0
[180] capwap iifid = 2415919114
[181] hyperlocation data.hyperlocation method = HYPERLOCATION METHOD NONE
[182] hyperlocation data.per ap hl tlv rcvd = HYPERLOCATION AP TLV RECEIVED
[183] hyperlocation_data.cmx_ip = null
[184] cdp enable = true
 [185] cdp cache index list.buffer = [
       1,
       Ο,
       Ο,
       0
1
[186] ap_stationing_type = EWLC_ENM_INDOOR_AP
[187] int if num = 0
[188] radio key = [
       {wtp_mac : 1CD1.E065.C340, radio_slot_id : 0},
        {wtp mac : 1CD1.E065.C340, radio slot id : 1},
        {wtp_mac : 0000.0000.0000, radio_slot_id : 0},
        {wtp mac : 0000.0000.0000, radio slot id : 0}
]
[189] reboot stats.reboots = 9
[190] reboot stats.ac initiated = 4
[191] reboot_stats.link_failure = 0
[192] reboot stats.sw failure = 0
[193] reboot_stats.hw_failure = 0
[194] reboot stats.unknown failure = 0
 [195] reboot_stats.reboot_reason = AP_REBOOT_REASON_IMG_UPGRADE
[196] reboot_stats.reboot_types = AP_REBOOT_SPAM_INITIATED
[197] reboot stats.reboot type = AP REBOOT SPAM INITIATED
[198] slot type = [
       0.
       Ο,
       0.
       0
1
[199] mesh profile inuse =
 [200] mesh ap role = ENM EWLC AP ROLE MESH
[201] wtp_cfg_reval_data.wtp_revalidate = false
[202] wtp cfg reval data.pending wtp notifies = 0
[203] me internal ap = false
[204] ap_type = AP_TYPE_CAPWAP
[205] is mewlc candidate = false
 [206] is invalid master = false
[207] is callback success = false
[208] proxy info.hostname =
```

```
[209] proxy info.port = 0
[210] proxy_info.no_proxy_list =
[211] grpc enabled = true
[212] ap image size = 0
[213] ap\_cur\_bytes = 0
[214] image_size_eta = 0
[215] image size start time = Thu, 01 Jan 1970 00:00:00 +0000
[216] image size percentage = 0
[217] dual dfs capable = false
[218] mdns_group_id = 0
[219] mdns rule name =
 [220] ap keepalive state = true
[221] local dhcp = false
[222] ipv4 pool.network = 0.0.0.0
 [223] ipv4_pool.lease_time = 0
[224] ipv4 pool.netmask = 0.0.0.0
 [225] wlc image size eta = 0
[226] wlc_image_size_start_time = Thu, 01 Jan 1970 00:00:00 +0000
[227] wlc image size percentage = 0
[228] matching ewc image = false
[229] disconnect_detail.ext_disconnect_reason_capable = false
[230] disconnect_detail.disconnect_reason = UNKOWN
 [231] antenna monitor.support = false
[232] antenna monitor.enabled = false
[233] antenna monitor.rssi fail threshold = 0
[234] antenna monitor.weak rssi = 0
[235] antenna_monitor.detection_time = 0
[236] wtp_ip = 10.22.243.229
}
```

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

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

test platform software database get ewlc\_oper/ble\_ltx\_ap;ap\_mac=<mac-without-dots>

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

```
wireless controller# test platform software database get
ewlc oper/ble ltx ap;ap mac=04eb409ec3c0
```

The output presents a list of parameters, such as:

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

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

```
wireless controller# test platform software database get
ewlc_oper/ble_ltx_ap;ap_mac=04eb409ec3c0
Table Record Index 0 = \{
 [0] ap mac = 04EB.409E.C3C0
 [1] admin.state = BLE LTX ADMIN STATE ON
 [2] admin.feedback.state status = 0
 [3] admin.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [4] admin.report.valid = true
 [5] scan config.interval sec = 1
 [6] scan_config.state = BLE_LTX_SCAN STATE ON
 [7] scan config.max value = 8
 [8] scan config.window msec = 800
 [9] scan_config.filter = BLE_LTX_SCAN_FILTER_ON
 [10] scan config.feedback.interval sec status = 0
 [11] scan config.feedback.state status = 0
 [12] scan config.feedback.max value status = 0
 [13] scan config.feedback.window msec status = 0
 [14] scan config.feedback.filter status = 0
 [15] scan_config.report.last_report_time = Fri, 05 Jun 2020 07:26:18 +0000
 [16] scan config.report.valid = true
 [17] profile ibeacon.uuid = 0000000-0000-0000-0000-00000000000
 [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}
1
 [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 \overline{tlm} = 0
 [52] scan counters.regular tlm = 0
 [53] scan counters.emergency = 0
 [54] scan_counters.event_emergency = 0
 [55] scan counters.other = 0
 [56] scan_counters.report.last report time = Fri, 05 Jun 2020 07:26:18 +0000
 [57] scan counters.report.valid = true
 [58] host_data.device_name = Developme
 [59] host_data.ble_mac = 806F.B031.E024
 [60] host data.api version = 1
 [61] host data.fw version = FF020710
 [62] host data.advertise count = 0
 [63] host data.uptime dsec = 10
 [64] host data.active profile = BLE LTX PROFILE NO ADV
 [65] host data.report.last report time = Fri, 05 Jun 2020 07:26:18 +0000
 [66] host_data.report.valid = true
 [67] feature mode.feature = BLE LTX FEATURE ZIGBEE
 [68] feature mode.mode = BLE LTX MODE IOX
 [69] feature mode.report.last report time = Fri, 05 Jun 2020 07:26:19 +0000
 [70] feature mode.report.valid = true
 [71] device status.device = BLE LTX DEVICE MSM1
 [72] device status.state = BLE LTX DEVICE STATE IOX BLE MODE
 [73] device status.report.last report time = Fri, 05 Jun 2020 07:26:18 +0000
 [74] device status.report.valid = true
 [75] capability.ble = true
 [76] capability.zigbee = true
 [77] capability.thread = false
 [78] capability.usb = true
 [79] capability.report.last report time = Wed, 03 Jun 2020 08:08:20 +0000
 [80] capability.report.valid = true
}
```

### How do I get the telemetry connection status?

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

**1.** Enter the command:

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

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

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

The following is a sample output of the command. The **State** is **CNDP\_STATE\_CONNECTED** and that indicates that the connection is successfully established

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

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

### How do I view IOx AP state and mode?

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

**1.** On the wireless controller, enter the following command:

show ap ble summary

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

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

wireless-controller# show AP Name	ap ble summary BLE AP State	BLE mode
AI Name	DDE AI State	
AP 10.2830	Цр	IOx
AP 02.2898	Up	IOx
AP 06.28CC	Up	IOx
AP_08.28E0	Up	IOx
AP_07.28E4	Up	IOx
AP_09.28EC	Up	IOx
AP_01.28F0	Up	IOx
AP_03.2928	Up	IOx
AP_05.2934	Up	IOx
AP_04.2938	Up	IOx

## How do I view gRPC details?

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

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

show ap name <AP Name> grpc detail

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

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

The following is a sample output of the command:

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

gRPC cha	annel status	:	Up
Packets	transmit attempts	:	818411
Packets	transmit failures	:	2651788
Packets	receive count	:	2711
Packets	receive failures	:	0

### How do I view AP BLE configuration details?

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

show ap name <ap-name> ble detail

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

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

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

Capability report time : 06/25/2020 21:16:25 : BLE, Zigbee, USB, Capability 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 : 256 API version FW version : 2.7.16 Broadcast count : -1844445184 : 838860800 deciseconds Uptime Active profile : No Advertisement : No Advertisement : 06/25/2020 21:30:36 Scan Statistics report time 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 : Unknown Major Minor : Unknown Transmit power : Unknown Advertised transmit power : Unknown Enable : Unknown Beacon ID : 1 : Unknown UUID Major : Unknown Minor : Unknown Transmit power : Unknown Advertised transmit power : Unknown Enable : Unknown Beacon ID : 2 UUID : Unknown • Unknown Major Minor : Unknown Transmit power : Unknown Advertised transmit power : Unknown Enable : Unknown Beacon ID : 3 UUID : Unknown : Unknown Major

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

Some of the output descriptors are described below:

- 1. Mode Report Time: This timestamp, 06/25/2020 21:30:54, indicates when the AP mode was last reported.
- 2. Mode: The AP is set to an Advanced (IOx) operational mode.
- 3. Radio Mode: The radio is operating in BLE mode.
- 4. Admin State Report Time: As of 06/25/2020 21:31:14, the administrative state of the AP was last reported.
- 5. Admin State: The AP is currently Up and operational.
- 6. Interface Report Time: The interface status was last reported on 06/25/2020 21:30:58.
- 7. Interface: The interface identifier is MSM1.
- 8. Interface State: The interface is Open for connections.
- 9. Type: The AP has an Integrated interface type.
- **10.** Capability Report Time: The capabilities were last reported on 06/25/2020 21:16:25.
- 11. Capability: The AP supports BLE, Zigbee, and USB functionalities.
- 12. Host Data Report Time: This timestamp, 06/25/2020 21:31:14, shows when the host data was last reported.
- 13. Host Data: It includes the AP's name AP\_102830, its Dot15 radio MAC address 18:04:ed:c5:02:bc, API version 256, firmware version 2.7.16, and other operational details.
- 14. Scan Statistics Report Time: The scan statistics were last reported on 06/25/2020 21:30:36.
- 15. Scan Statistics: Indicates no total scan records are available.
- 16. Scan Role Report Time: The scan role was last reported on 06/25/2020 21:31:14.
- 17. Scan Role: The AP is set to enable scanning with a 1-second interval and an 800-millisecond window. The maximum value is 8 and the scan filter is enabled.

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

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

1. Run the command to retrieve the TDL values:

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

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

```
wireless controller# test platform software database get-n all ewlc oper/ap air quality
Table Record Index 0 = \{
[0] ap mac = 687D.B45E.E7C0
[1] last update = Tue, 12 Oct 2021 15:08:19 +0530
[2] \operatorname{rmox} 0 = 5.62121e+07
[3] \text{ rmox } 1 = 6.12815e+06
[4] \text{ rmox}_2 = 1.26038e+06
[5] \text{ rmox } 3 = 579564
[6] \text{ rmox } 4 = 398259
[7] \text{ rmox } 5 = 280246
[8] \text{ rmox } 6 = 201467
[9] \mod 7 = 370324
[10] \text{ rmox } 8 = 680235
[11] \text{ rmox } 9 = 1.29709e+06
[12] \text{ rmox } 10 = 3.18129e+06
[13] \text{ rmox } 11 = 1.06436e+07
[14] \text{ rmox } 12 = 6.10561e+07
[15] iaq = 1
[16] etoh = 0.0094
[17] eco2 = 400.212
[18] tvoc = 0.0178
```

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

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

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

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

test platform software database get-n all ewlc\_oper/ap\_temp

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

```
wireless controller# test platform software database get-n all ewlc_oper/ap_temp
Table Record Index 0 = {
 [0] ap_mac = 687D.B45E.E7C0
 [1] last_update = Tue, 12 Oct 2021 15:08:19 +0530
 [2] temp = 233.382
 [3] humidity = 0
 }
```

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



## **Troubleshooting IoT Services: IOx Application**

- How do I verify the IOx application is running on the AP?, on page 107
- How do I debug the IOx application installation failure?, on page 107
- How do I verify the IoX Application AP bundle download from Cisco Spaces? , on page 108
- How do I start an interactive shell session for the IOx application?, on page 108
- How can I see the logs for the IOx application?, on page 109
- How do I monitor metrics in the IOx application?, on page 109
- How do I monitor BLE scans in the IoX Application?, on page 111
- What files exist in the IOx application?, on page 113

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

Run the command: show iox applications

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

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

## How do I debug the IOx application installation failure?

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

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

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

The IoX Application installation is done from the Cisco Spaces: Connector. The AP image bundle is downloaded from Cisco Spaces to Cisco Spaces: Connector. To verify if the IoX Application was downloaded accurately, you can check the log files. See How do I debug the IOX application installation failure?, on page 107

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

spacesadmin# wget
"https://dnaspaces.io/api/edm/v1/device/iox-app/download?id=cisco\_dnas\_ble\_iox\_app&version=1.1.16"

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

Run the command: connect iox application

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

AP# connect iox application
/ #

## How can I see the logs for the IOx application?

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

Then, run the command: tail -F /data/logs/dnas\_ble.log

You can see the logs for the IOx application.

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

## How do I monitor metrics in the IOx application?

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

Run the command: tail -F /data/logs/dnas\_ble\_metrics.log

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

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

#### **Table 6: Monitor Metrics**

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

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

AP# tail -F /data/logs/dnas ble metrics.log

Wed Oct 6 17:03:49 2021 [INFO]: Application Version: 1.2.5Wed Oct 6 17:03:49 2021 [INFO]: Start Time: Fri Sep 17 15:54:11 2021 Up Time:

0019D:01H:09M:38S Wed Oct 6 17:03:49 2021 [INFO]: Total Physical Memory: 1557 MBWed Oct 6 17:03:49 2021 [INFO]: Physical Memory Free: 786 MBWed Oct 6 17:03:49 2021 [INFO]: Physical Memory Used: 770 MBWed Oct 6 17:03:49 2021 [INFO]: Total Physical Shared Memory: 170 MBWed Oct 6 17:03:49 2021 [INFO]: Total Physical Buffer Memory: 0 MBWed Oct 6 17:03:49 2021 [INFO]: Total AP Percent CPU Used: 1.934973Wed Oct 6 17:03:49 2021 [INFO]: Process Virtual Memory: 108696 kBWed Oct 6 17:03:49 2021 [INFO]: Process Physical Memory: 8828 kBWed Oct 6 17:03:49 2021 [INFO]: Process CPU Used: 0.004167Wed Oct 6 17:03:49 2021 [INFO]: gRPC Reconnect Count: 0Wed Oct 6 17:03:49 2021 [INFO]: CAPWAP Restart Count: 1Wed Oct 6 17:03:49 2021 [INFO]: Last CAPWAP Restart Time: Fri Sep 17 15:54:11 2021 Wed Oct 6 17:03:49 2021 [INFO]: BLE Device Open Count: 1Wed Oct 6 17:03:49 2021 [INFO]: Last BLE Device Open Time: Fri Sep 17 15:54:11 2021 Wed Oct 6 17:03:49 2021 [INFO]: BLE Device Close Count: 1Wed Oct 6 17:03:49 2021 [INFO]: Last BLE Device Close Time: Sat Sep 18 05:48:12 2021 Wed Oct 6 17:03:49 2021 [INFO]: Log Rotation Count: 0Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Count: 10896160 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Rate Per Second: 0.0 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Write Count: 217955 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Write Rate Per Second: 00 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Count Per Write: 50 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Scan Data Message Avg Write Time (milliseconds): 12 Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Request Count: 0Wed Oct 6 17:03:49 2021 [INFO]: Last Floor Beacon Config Request Time: None Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Success Count: 0Wed Oct 6 17:03:49 2021 [INFO]: Last Floor Beacon Config Success Time: None Wed Oct 6 17:03:49 2021 [INFO]: Floor Beacon Config Failure Count: 0Wed Oct 6 17:03:49 2021 [INFO]: Last Floor Beacon Config Failure Time: None

## How do I monitor BLE scans in the IoX Application?

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

tail -F /data/logs/dnas\_ble\_scans.log

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

### Table 7: Output Descriptions

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

#### AP# tail -F /data/logs/dnas\_ble\_scans.log

Sat Sep 18 05:44:57	2021	[INFO]:	Profile		MAC	RSSI	Count	Interval
Last-heard Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		00:00:00:00:00:0F	63	16	1S
0000D:00H:00M:01S								
Sat Sep 18 05:44:57 0000D:00H:00M:02S	2021	[INFO]:	Kontakt	Secure	F1:01:AF:4E:8A:3B	55	1	05
Sat Sep 18 05:44:57	2021	[INFO]:	Kontakt	Telem	F1:01:AF:4E:8A:3B	55	1	0 S
0000D:00H:00M:03S								
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		F1:01:AF:4E:8A:3C	56	1	05
0000D:00H:00M:01S	0.0.0.1	[ ]			<b>D1 00 15 05 DC D0</b>		1	0.7
Sat Sep 18 05:44:57 0000D:00H:00M:03S	2021	[INFO]:	iBeacon		D1:03:15:95:D6:F3	//	1	05
Sat Sep 18 05:44:57	2021	[INFO]:	Kontakt	Secure	DF:03:AB:CD:C2:DB	86	2	3S
0000D:00H:00M:01S								
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		DF:03:AB:CD:C2:DC	76	2	2S
0000D:00H:00M:02S							_	
Sat Sep 18 05:44:57	2021	[INFO]:	Unknown		18:04:ED:04:1C:5F	62	7	1S
0000D:00H:00M:01S Sat Sep 18 05:44:57	2021	[TNEO] .	Kontokt	Socuro	C3,05,7E,PD,25,D4	01	1	0S
0000D:00H:00M:04S	2021	[INFO].	NOILCARC	Decure	C3.03.7E.DD.23.D4	01	-	05
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		C3:05:7E:BD:25:D5	85	3	1S
0000D:00H:00M:01S								
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		CB:06:D8:B5:A7:97	86	1	0 S
0000D:00H:00M:03S Sat Sep 18 05:44:57	0001	[ TN DO ]	' <del>.</del>		D8:06:04:DE:80:59	0.0	1	0.0
0000D:00H:00M:04S	2021	[INFO]:	IBeacon		D8:06:04:DE:80:59	88	T	05
Sat Sep 18 05:44:57	2021	[INFO]:	Kontakt	Secure	FF:07:D0:2F:6A:AF	79	1	0S
0000D:00H:00M:02S								
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		FF:07:D0:2F:6A:B0	79	3	1S
0000D:00H:00M:01S							_	1.5
Sat Sep 18 05:44:57 0000D:00H:00M:01S	2021	[INFO]:	Unknown		36:08:36:6C:DA:E8	81	5	1S
Sat Sep 18 05:44:57	2021	[INFO]:	Kontakt	Secure	C6:09:26:9D:4D:94	73	2.	2.5
0000D:00H:00M:01S	2021	[1111 0].	nonouno	0000110	0010012010212010	, 0	-	20
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		C6:09:26:9D:4D:95	73	1	05
0000D:00H:00M:02S								
Sat Sep 18 05:44:57	2021	[INFO]:	iBeacon		C1:0A:21:02:A7:D8	77	3	1S
0000D:00H:00M:02S								

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

## What files exist in the IOx application?

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

#### **Table 8: Log Files**

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

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

#### **Table 9: Configuration Files**

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

The following are binary files installed specifically for the IOx application. All the files are located in the directory: /var/dnas\_ble

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



## **Troubleshooting IoT Services: Cisco Spaces Connector**

- What are the metrics available on the Connector GUI for IoT Service (Wireless) ?, on page 115
- What are the log files created on the Connector for IoT Service (Wireless)?, on page 116

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

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

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

#### **Table 10: Monitor Metrics**

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

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

#### Table 11: Log Files

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



## **Troubleshooting IoT Services: Access Point**

- How do I check the gRPC connection status on the access point?, on page 117
- How do I check the stream token on the access point?, on page 117
- How do I view the gRPC server logs on the access point?, on page 118
- How do I view the beacons scanned by an access point running in Native Mode?, on page 119
- How do I view the beacon broadcast setting for an access point running in Native Mode?, on page 119

## 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
                       : 10.22.243.31
Controller Ip
                     :
Stream Setup Interval
                          30
                        : 30
Keepalive Interval
Last Keepalive Rcvd On
                       : 2020-04-01 00:32:47.891433113 +0000 UTC m=+345985.338898246
Number of Dials
                          : 2
                          : 2788175
Number of Tx Pkts
                          : 11341
Number of Rx Pkts
Number of Dropped Pkts
                          : 0
                          : 11341
Number of Rx Keepalive
                          : 11341
Number of Tx Keepalive
Number of Rx Cfg Request
                          : 0
Number of Tx AP Cfg Resp
                          : 0
Number of Tx APP Cfg Resp
                          : 0
Number of Tx APP state pkts
                          : 5
Number of Tx APP data pkts : 2776829
```

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

Run the command: show cloud connector key access

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

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

Also run the command: show cloud connector key authentication.

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

## 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="2020-04-01T01:36:522" level=info msg=" Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping
for 10 seconds"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "
```

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

Run the command: show controllers ioTRadio ble 0 scan brief

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

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

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

Run the command: show controllers ioTRadio ble 0 broadcast

AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config		
Active profile	:	v-iBeacon
Profile 0 (iBeacon)		
UUID	:	000010000000000000000000000000000000000
Interval (ms)	:	100
Power (dBm)	:	-21
Advertised Power (dBm)	:	-65
Minor	:	0
Major	:	0
TxPower byte	:	bfbfbfbfbfbfbfbfbfbfbfbfbf
Profile 1 (Eddystone UID)		
Namespace (hex)	:	000000000005446089c
Instance-ID (hex)	:	7f000001f00
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
Scan Data
           :
0000000ae0100000000005446089c7f0000001900000000000004cb5
Simulator mode
           : Disabled
           Mac
Beacon-TD
                          UUID Major Minor Status
   44
                                     1
   0
   0 0
                                     0
   0 0
                                     0
Beacon-ID Transmit power(dBm) Advertised power(dBm)
            -21
                      -60
   1
   2
            -21
                      -65
   3
            -21
                      -65
   4
            -21
                       -65
   5
            -21
                       -65
```

AP# show controllers ioTRadio ble 0 broadcast

```
BLE Profile Config
```

```
_____
Active profile
              : Eddystone UID
Profile 0 (iBeacon)
             UUTD
Interval (ms)
              : 100
Power (dBm)
              : -21
Advertised Power (dBm) : -65
             : 0
Minor
Major
             : 0
TxPower byte
             : bfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
Profile 1 (Eddystone UID)
Namespace (hex) : 444444444444444444444
Instance-ID (hex)
             : 555555555555
Profile 2 (Eddystone URL)
              : http://www.
URL
Profile 3 (v-iBeacon)
v-iBeacon status
             : Chirping
Chirping interval (ms) : 100
Profile 4 (Custom Profile)
Adv Data
Scan Data
0000000ae0100000000005446089c7f0000001900000000000004cb5
Simulator mode : Disabled
Beacon-ID
             Mac
                                UUID Major Minor Status
    44
                                            1
    0
                                      0
                                    0
    0
    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 Profile 0 (iBeacon)	: Eddystone	URL			
UUID	• 0000100000	000000000000000000000000000000000000000	n		
	: 100		0		
	: -21				
Advertised Power (dBm)	: -65				
	: 0				
Major	: 0				
TxPower byte	: bfbfbfbfbf	Ebfbfbfbfbfbfbf			
Profile 1 (Eddystone UID)					
Namespace (hex)					
Instance-ID (hex)	: 555555555	555			
Profile 2 (Eddystone URL)	1				
URL	: http://www	v.cisco.com/			
Profile 3 (v-iBeacon)					
v-iBeacon status	: Chirping				
Chirping interval (ms)	: 100				
Profile 4 (Custom Profile	e)				
Adv Data	:				
000000180000000000000000		000000000000000000000000000000000000000	00		
Scan Data 00000000ae010000000000000	:	000180000000000000000	~ 5		
	: Disabled	10001900000000000000040	55		
	. Disabled	TITT	ID Major	Minor	Status
		111111111111111111111111111111111111111	2		1
2 C0:64:E4:23:7F	2E 22222222	222222222222222222222222222222222222222	22 3333		1
		000000000000000000000000000000000000000	0 00	0	0
4 C0:64:E4:23:7F	2C 00000000	000000000000000000000000000000000000000	0 00	0 0 0	0
5 C0:64:E4:23:7F	:2B 00000000	000000000000000000000000000000000000000	0 00	0	0
Beacon-ID Transmit power	(dBm) Adverti	lsed power(dBm)			
1	-21	-60			
2	-21	-65			
3	-21	-65			
4	-21	-65			
5	-21	-65			



# PART **VI**

## Appendix

• Cisco Catalyst 9800 Series Wireless Controller, on page 125



## **Cisco Catalyst 9800 Series Wireless Controller**

- Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower), on page 125
- Disable Assurance with iCAP using CLI (Versions 17.3.1 or lower), on page 126
- Disable iCAP using WEBUI (Versions 17.3.2 or higher), on page 127
- Disable iCAP using CLI (Versions 17.3.2 or higher), on page 128
- Enable or Disable iCAP or Assurance using DNAC (Versions 17.3.2 or higher), on page 129

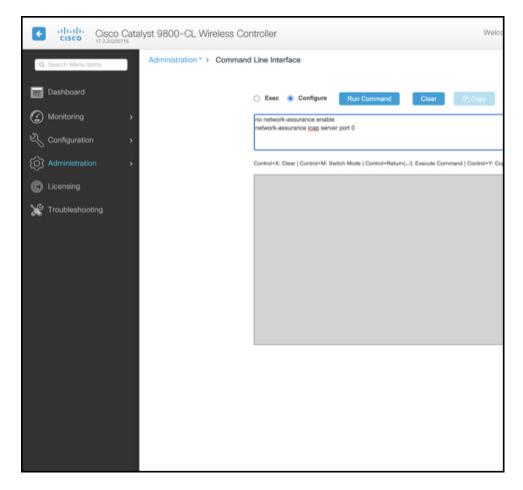
# Disable Assurance with iCAP using GUI (Versions 17.3.1 or lower)

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

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

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

#### Figure 76: Entering the commands to enable BLE



### Step 2 Click Run Command.

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

#### What to do next

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

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

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

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

### SUMMARY STEPS

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

### **DETAILED STEPS**

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

#### What to do next

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

## Disable iCAP using WEBUI (Versions 17.3.2 or higher)

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

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

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

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

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

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

#### Figure 77: Entering the commands to enable IoT Service

Q Search Menu Items	Administration • > Comman	nd Line Interface
🚃 Dashboard		Exec O Configure Run Command Clear Clopy Export
Monitoring >		network-assurance icap server port 0
Configuration		
Administration         >		Control+X: Clear   Control+M: Switch Mode   Control+Return(/): Execute Command   Control+Y: Copy   Control+Shift+E: Ex
C Licensing		
X Troubleshooting		

#### Step 2 Click Run Command.

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

#### What to do next

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

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

## Disable iCAP using CLI (Versions 17.3.2 or higher)

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

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

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

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

#### **SUMMARY STEPS**

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

### **DETAILED STEPS**

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

#### What to do next

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

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

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

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

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