

Device Management

- Dashboard View of Devices, on page 1
- Configuring Beacons, on page 2
- Categorizing Devices into Manual Groups, on page 2
- Categorizing Devices into Groups (Dynamic Groups), on page 3
- Applying Policies to Beacons, on page 5
- Filtering Devices, on page 10

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 1: Dashboard View of Devices

Home Devices Groups				IOT Service			
Floor Beacons AP Beacons II Campuses	Wired Devices ()		Pre	Basic Device ID Node Mac dress Last Seen Location Cancel		iroup fake ype endor Apply	
Device ID *	Node Mac Address	Last Seen	Location	Group	Make	Туре	Vendor
0001-17-6827193bcd4a	68:27:19:3b:od:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-			
0001-17-6827193bcd4a	68:27:19:3b:od:4a 68:27:19:3b:od:4a	May 27th, 2021 Ob:01:18 AM 6 days ago May 27th, 2021 Ob:01:18 AM 6 days ago	- San Jose->Building 19 Test->Lab Floor		-		
0001-17-6827193bod4a 0002-17-6827193bod4a	68:27:19:3b:od:4a 68:27:19:3b:od:4a 68:27:19:3b:od:4a	May 27th, 2021 08:01:18 AM 6 days ago May 27th, 2021 06:01:18 AM 6 days ago May 27th, 2021 06:01:08 AM 6 days ago	- San Jose->Building 19 Test->Lab Floor -	-	•	•	-

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 2: 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.

devices to add

Procedure

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 c 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.

Clsco DNA Spaces
If or Clsco DNA Space Clsco DNA Clscowere List Area Space Clsco DNA Space Clsco DNA Clasterer List Area Space Space Clsco DNA Clasterer List Area Space Space Clsco DNA Clasterer List Area Space Space Area Area Area Area

Figure 3: 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.

Procedure

- **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 4: Group by MAC Prefix

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

Figure 5: Group by Vendor Code

Dynamic Grouping		
	Croup by MAC Prefix MAC Prefix Coup by Vendor Code Vendor Code Vendor Code Kontakt.io Croup by Location Hierarchy System Campus V	
		Cancel Back Create Group

Figure 6: Group by Location Hierarchy

Dynamic Grouping	
Group by M	1.G Prefix
MAC Prefix Group by Ve Vendor Code	ndur Code
Group by Lo Building 19	cation Hierarchy
	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

Procedure

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

 Figure 7: Creating a New Policy



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 8: Choosing One of Four Policies

Configure	a Transmit Policy				×
1 Policy Ten	nplate	2 Policy Settings	3 Apply Grou	ip	4 Summary
Name & R	Recommended Policies				
Give your policy your requirement	a name/description and select a poli nt.	cy that you would like to use. For eac	h Policy Type, you can use the default P	Policy or adjust specific configuration	setting based on
	Policy N Test Po	ame* Nicy	Description test		
))≡((0	Ø	00	
	Asset Management High power transmission for efficient asset management.	People Tracking High power transmission for efficient people tracking.	Monitoring Low power and low frequency transmission for efficient sensor monitoring with high battery life.	Wayfinding High power and high frequency transmission for efficient wayfinding.	
			C	ancel Previous	Next

Table 1: 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 9: Configure a Transmit Policy

Policy Template	Policy Settings		(3) Apply Group			4 Summary
Asset Management		Notification				
ese actions will be taken when this policy is applied to a device		Subscribe to notifications the	hat will be sent when this policy is applied to a de	rice		
Selected Profile IBEACON C V		To:			я	
uuo*						
0cedf1ae-0faf-4d9e-9a81-ef395b5e12cc						
UUID is usually same across an organization. Please enter your organization UUID or use the system generated random UUID.						
Major* 14093						
Major is usually same across a sub-organization. Major and minor values are integers upto 65535.						
Random						
Minor						
👩 Random						
Transmit power level*						
A V						
Citer mananic power reven						
Interval(ims)*						
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 10: Choosing a Device Group for Dynamic Policy Application

Config	gure a Transmit Policy			×
Ø Pi	plicy Template	Policy Settings	3 Apply Group	(4) Summary
Choo This pol Creat	use Device Group key wil be applied to devices belonging to these groups. In new group seted			EQ/ind
	Group Name *		Description	
	Jerny Test		Testing Redis pub/sub	
	TestGroup2		Test Group 2 Description	
	Test1		test2	
	test		test	
	TestGroup4		Test Group 4 Description	
	TestGroup3		Test Group 3 Descriptiosn	
	Asset Management Group 1			
	TestGroup1		Test Group 1 Description	
	Test2		Test 2 Description	
	mathdest		mathatest	
	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 11: Enabling or Disabling a Policy

-	E Cis	co DNA Spaces	1								0	θ
								Policy - JennyDynamic2				
۲	Но	me Devices	Groups Policie	s Settings								
*	Polici	es (3) Actions ~	Alerts					Policy Active				
		Policy Name	Description	Туре	Priority	Profile	Applied Gro	Name* JennyDynamic2				
		JennyDynamic2		Group	10	-	JennyDynam	Description Enter Description				
		JannyDynamicLocation		Group	10		Jen man		Cancel	×s	ave	
		1 - E				iber	JennyTest					
	3 Records		Click on a p enable or dis polic	policy to sable the y								

Figure 12: Viewing Devices on Which a Policy Is Applied

		.,,,,,,	· nonty	FIGHE	Abbuen en onbras	Active	Greate fille		Alert Count	De
	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	a	8
rds								list of device that has this applied polic	s <	0
					Devices					×
					Devices (1)	√ Filters		As of: Apr 11, 2022 4:10 P	M 📿 Refresh	1
					Mac.	Address	Label	Update Time		
					☐ f6:9c	:d2:50:4d:15	-	Mar 3rd, 2022 06:48:21 AM a month ago		
					1 Records			Show Records: 50 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 13: Creating a New Policy

≡ Ciso	DNA Sp	oaces													0	Θ
Hor	Home Devices Groups Policies Settings													IoT Se	arvices I	telp 😡
Flor	or Beacons	AP Beaco	ons \	Wired Devic	es 0											
Claimed 73	g 19 d Beacons	All Profiles		IBeacon 952		Eddystone UID 41	Eddystone URL 35	Other Profiles 889								
∀ Filters	Actions ~	Configure Bea	icons									As of: Apr 2	1, 2022 9:54 AM	C Refresh	ð Ei	port
	Delete B	leacons	ess Type	Label	Location			Last Heard 👻	Group Name	Profile Type	Battery	Unique Id	Firmware	Adv. TxPowe	ar (dBm)	1
•	Add to g	group			System Ca	ampus->Building 19->Cis	co DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago		iBeacon				-77		
	Add Attr	ibutes			System Ci	ampus->Building 19->Cis	co DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	~	iBeacon			-	-77		
	ea:83:ea:39:ae:1	61 -		-	System Ca	ampus->Building 19->Cis	co DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago	-	iBeacon	-	-	-	-77		
	-h-a7-14-37-2b:	24 -			System Ca	ampus->Building 19->Cis	co DNA Customer Lab	Apr 21st, 2022 09:54:03 AM a few seconds ago		Kontakt	100%	Vu3irv	2.0	-		
loT Gate Device I Device I	Services tways Management Monitoring	٢														

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	DNA Spaces IoT Dev Test- >Building 19->Main Floor	
Adv. TxPower (dBm)	-	Mac Address	e9:f8:80:c0:8f:56	
Mac Address Type		Unique Id	VuLouh	
Firmware	2.0	Battery	100%	
Last Heard	Jan 28th, 2022 10:14:14 PM	Group Name	Manual	
> Beacon Config	Juration			
 V Request Histor 	y			
Request Histor	y (3)	_		Export
		Confi	g Source	Destination AP
		Policy -	Test Policy	68:7d:b4:5f:66:e0
		Policy -	Test Policy Older	68:7d:54:5f:66:e0
con do not have BLE k	X App Active or Installed and enabled in t	scan m de Manual		

Figure 14: 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

Procedure

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

Figure 15: Filtering Devices by MAC Address

Home Devices	Groups Policies Settings
Filtering	Filtering
	Enable Public MAC
	Enable Random Static MAC
IoT Services <i>○</i>	Enable Random Private MAC

I

Device Management