



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

The screenshot displays the Cisco DNA Spaces IoT Services dashboard. The main navigation bar includes 'Home', 'Devices', 'Groups', 'Policies', and 'Settings'. The 'Devices' tab is active, and the 'Wired Devices' sub-tab is selected. A dropdown menu shows 'All Campuses' with 'All Wired Sensors' (11) selected. A table lists device details, and a 'Presets' panel on the right allows for filtering by 'Basic' or 'All' with checkboxes for various attributes like Device ID, Node Mac Address, Last Seen, Group, Make, Type, and Vendor.

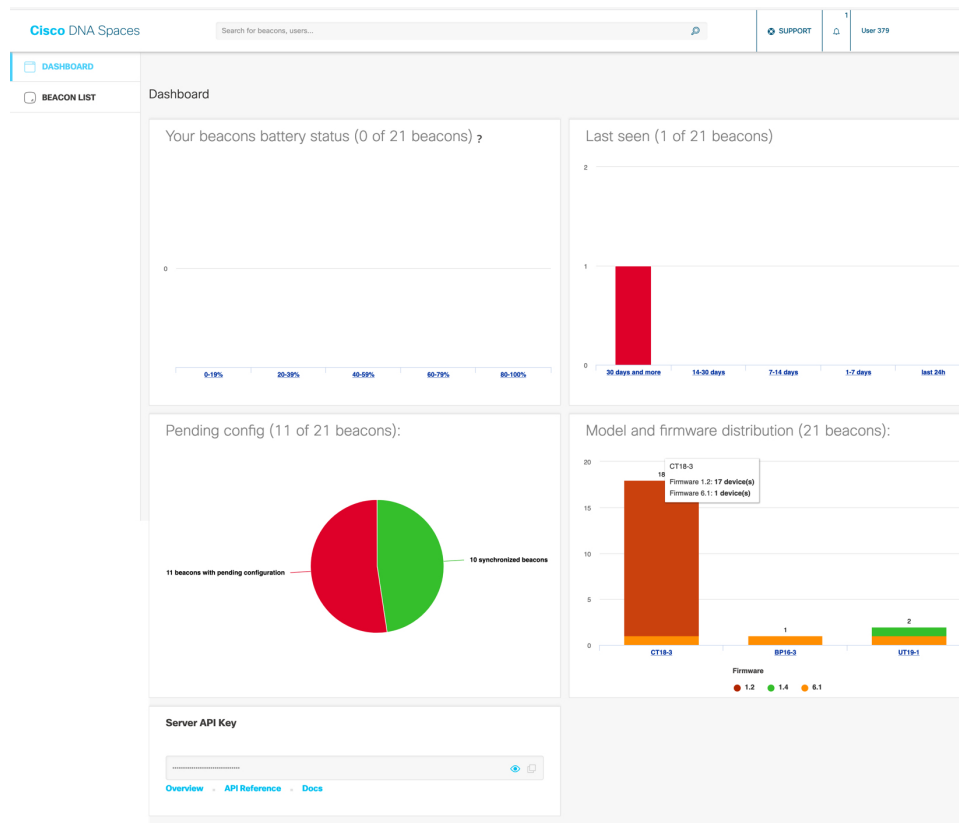
Device ID	Node Mac Address	Last Seen	Location	Group	Make	Type	Vendor
0001-17-6827193bcd4a	68:27:19:3b:cd4a	May 27th, 2021 08:01:18 AM 6 days ago	-	-	-	-	-
0002-17-6827193bcd4a	68:27:19:3b:cd4a	May 27th, 2021 06:01:18 AM 6 days ago	San Jose -> Building 19 Test -> Lab Floor	-	-	-	-
0003-17-6827193bcd4a	68:27:19:3b:cd4a	May 27th, 2021 06:01:08 AM 6 days ago	-	-	-	-	-
0004-17-6827193bcd4a	68:27:19:3b:cd4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-

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:

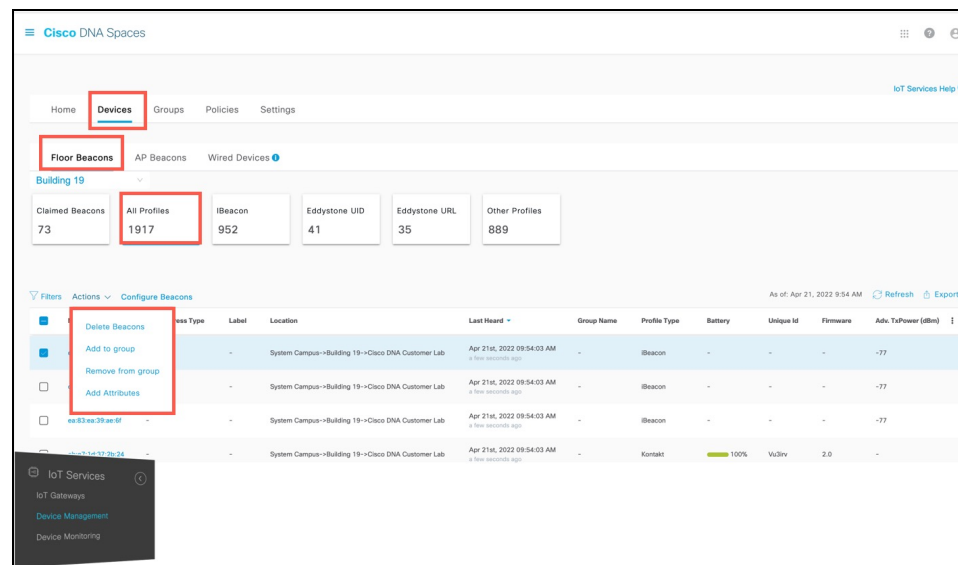
- Policies are applied to groups.
- Firehose APIs can filter devices by these groups.
- In the Cisco Spaces: IoT Service dashboard, you can filter devices by groups.

- 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.

Figure 3: Adding Devices to a Manual Group from the Devices tab



Categorizing Devices into Groups (Dynamic Groups)

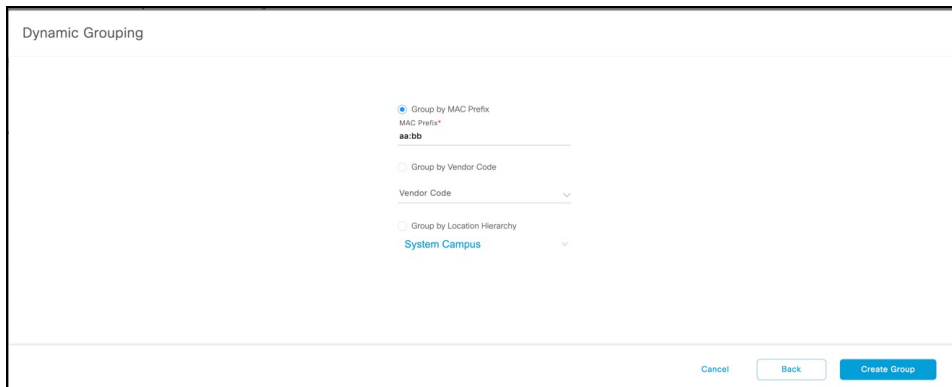
You can configure dynamic groups using parameters like MAC prefix, vendor code, and location hierarchy (floor, building, zone, and so on). New devices are automatically added to the group based on these configured parameters.

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.

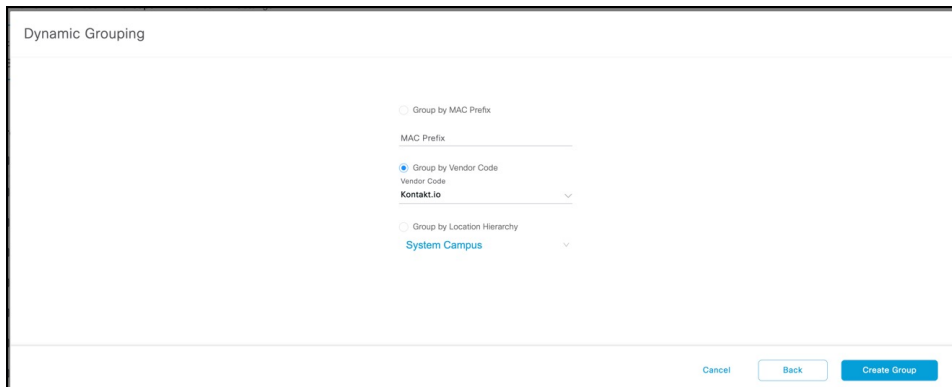
- Step 1** In the Cisco Spaces: IoT Service dashboard, navigate to **Device Management > Groups**.
- Step 2** In the **Add a Group** page, enter **Group Name**, **Description**, and choose **Dynamic Group** and click **Next**.
- Step 3** Click **Create a new group**, and provide a group name and description. 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



The screenshot shows the 'Dynamic Grouping' configuration page. The 'Group by MAC Prefix' option is selected with a radio button. Below it, the 'MAC Prefix' field contains the value 'aa:bb'. The 'Group by Vendor Code' and 'Group by Location Hierarchy' options are unselected. The 'Vendor Code' dropdown menu is open, showing 'System Campus' as the selected item. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Create Group'.

Figure 5: Group by Vendor Code



The screenshot shows the 'Dynamic Grouping' configuration page. The 'Group by Vendor Code' option is selected with a radio button. Below it, the 'Vendor Code' field contains the value 'Kontakt.io'. The 'Group by MAC Prefix' and 'Group by Location Hierarchy' options are unselected. The 'System Campus' dropdown menu is open, showing 'System Campus' as the selected item. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Create Group'.

Figure 6: Group by Location Hierarchy

Dynamic Grouping

Group by MAC Prefix
 MAC Prefix: _____
 Group by Vendor Code
 Vendor Code: _____
 Group by Location Hierarchy
 Building 19

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 7: Creating a New Policy

Cisco DNA Spaces

Home Devices Groups **Policies** Settings IoT Services Help

Policies (2) Actions Alerts As of: Apr 11, 2022 3:42 PM Refresh Create a new policy

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

Show Records: 50 1 - 2

IoT Services
IoT Gateways
Device Management
Device Monitoring

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

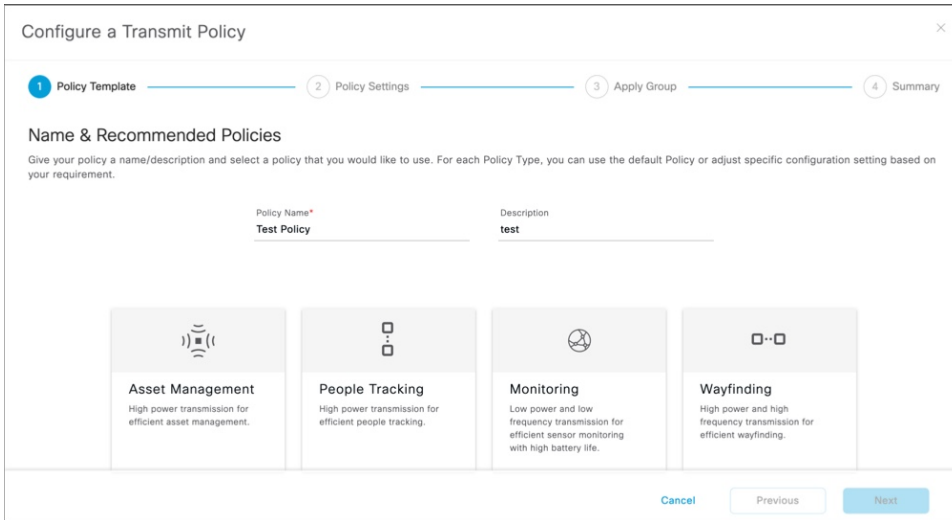
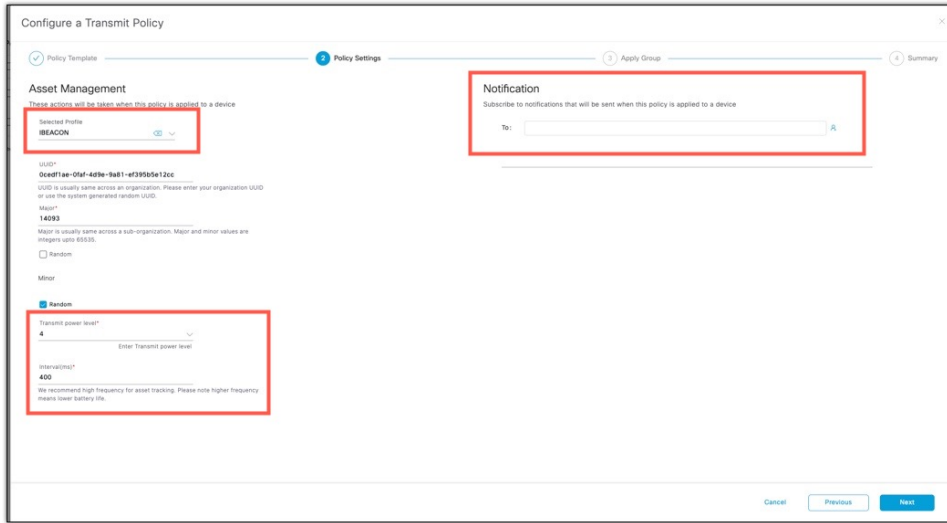


Table 1: Types of Transmit Policy

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

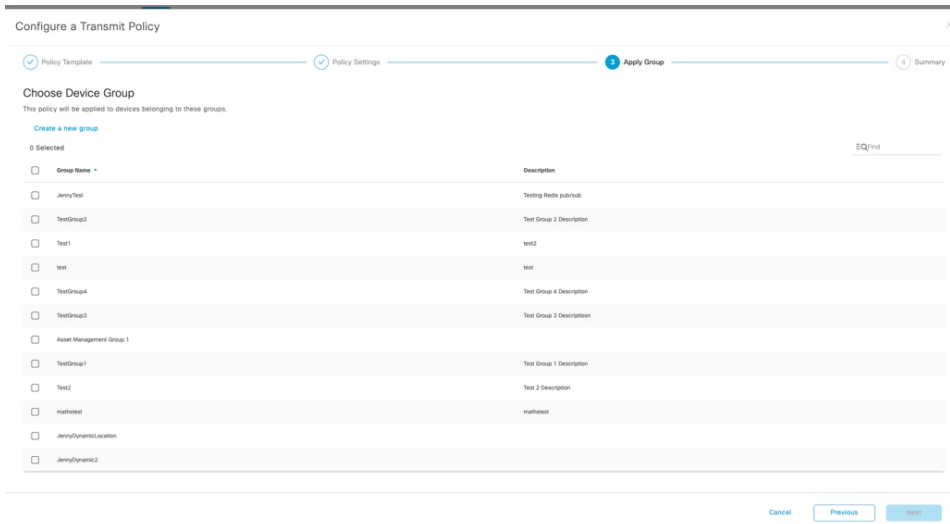
Step 3 From the **Configure a Transmit Policy** page that opens, enter email addresses in the **Notification** field. When this policy is applied to any device, the addresses are notified.

Figure 9: Configure a Transmit Policy



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



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

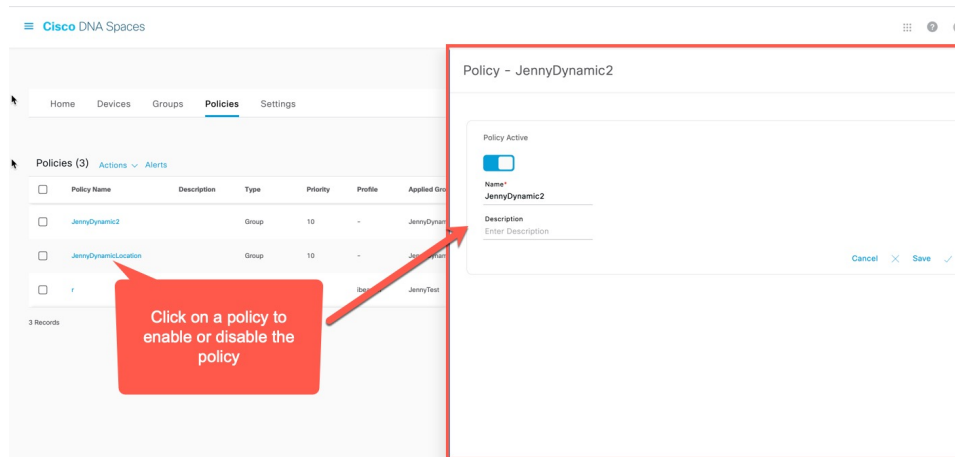
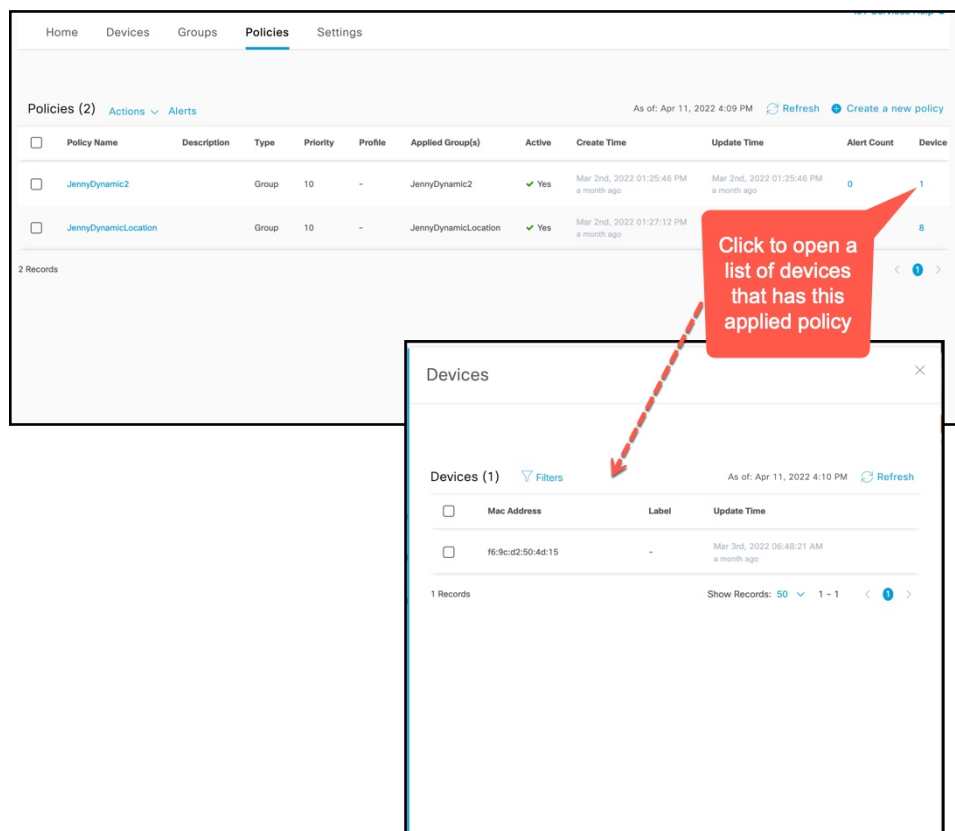


Figure 12: Viewing Devices on Which a Policy Is Applied



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

The screenshot shows the Cisco DNA Spaces interface. The 'Devices' tab is active, and 'Floor Beacons' is selected. A summary card shows 'All Profiles' with a count of 1917. Below, a table lists beacon profiles. A context menu is open over the table with the following options:

- Delete Beacons
- Add to group
- Remove from group
- Add Attributes

Profile Type	Label	Location	Last Heard	Group Name	Profile Type	Battery	Unique Id	Firmware	Adm. TxPower (dBm)
iBeacon	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM 8 hrs seconds ago	-	iBeacon	-	-	-	-77
iBeacon	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM 8 hrs seconds ago	-	iBeacon	-	-	-	-77
iBeacon	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM 8 hrs seconds ago	-	iBeacon	-	-	-	-77
Kontakt	-	System Campus->Building 19->Cisco DNA Customer Lab	Apr 21st, 2022 09:54:03 AM 8 hrs seconds ago	-	Kontakt	100%	Vu3rv	2.0	-

What to do next

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

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

Figure 14: Config Source: Policy

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

As of: Jan 28th, 2022 10:14:23 PM [Refresh](#)

Profile Type: iBeacon **Kontakt** [Edit](#) [🔗](#)

Label: -

Profile Type: **Kontakt** Location: DNA Spaces IoT Dev Test->Building 19->Main Floor

Adv. TxPower (dBm): - Mac Address: e9:f8:80:c0:8f:56

Mac Address Type: - Unique Id: VuLouh

Firmware: 2.0 Battery: 100%

Last Heard: Jan 28th, 2022 10:14:14 PM a few seconds ago Group Name: Manual

> Device Information

> Beacon Configuration

> Sensor Information

▼ Request History

Request History (3) [Export](#)

Config Source	Destination AP
Policy - Test Policy	68:7d:b4:5f:66:e0
Policy - Test Policy Older	68:7d:b4:5f:66:e0
Manual	

can do not have BLE ioX App Active or Installed and enabled in scan mode

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 15: Filtering Devices by MAC Address

