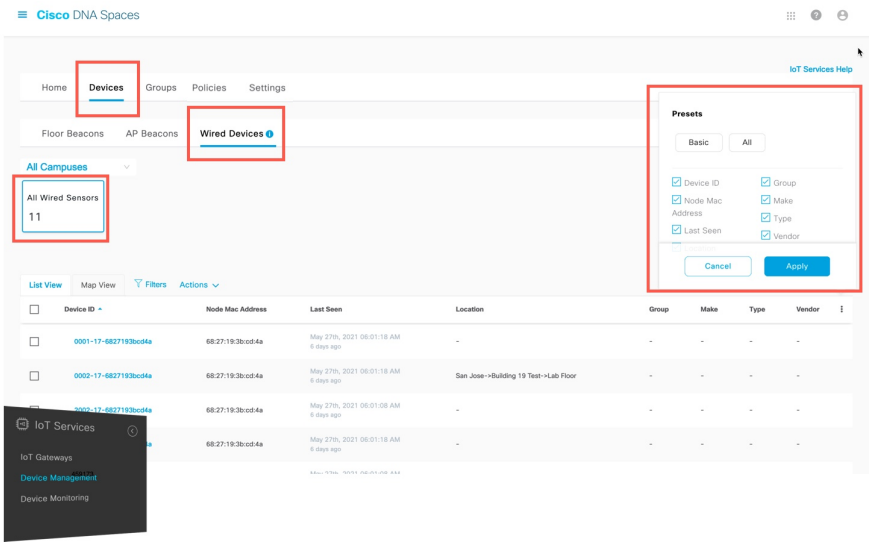
Device Management

- 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

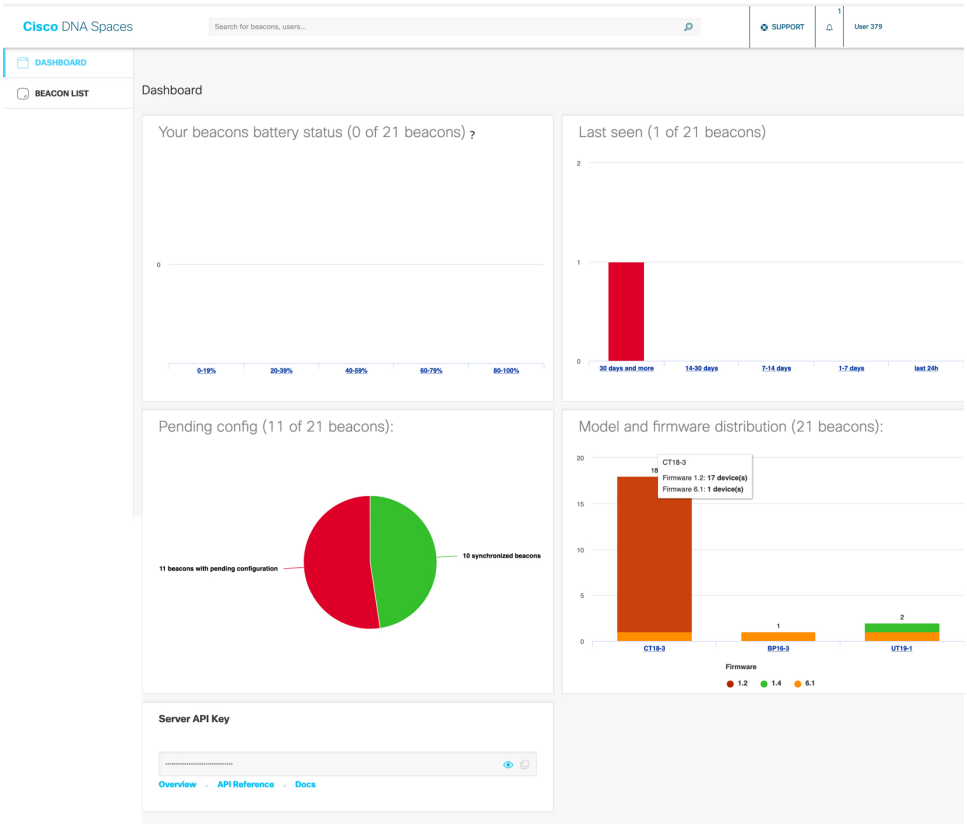


Configuring Beacons

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**.

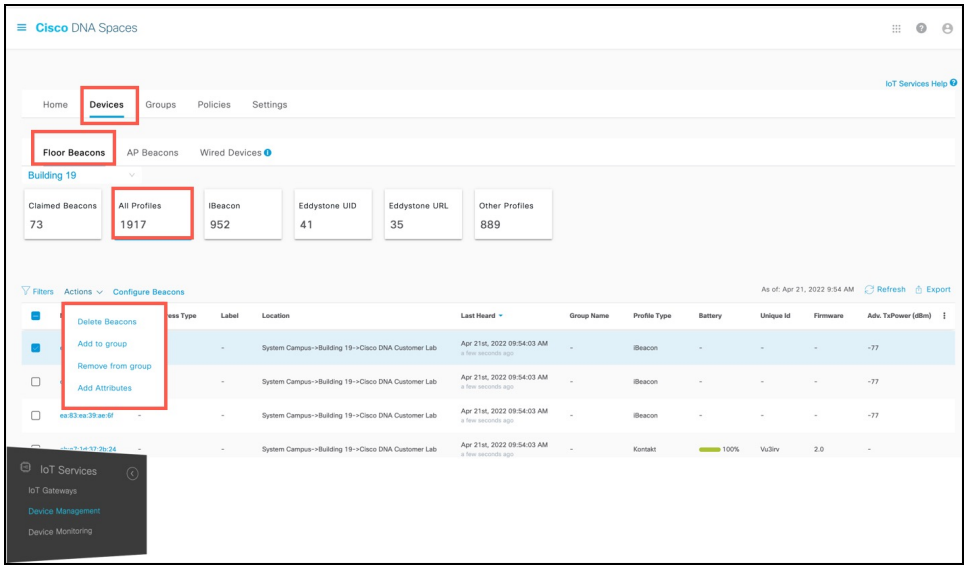
Step 4 In the **Add a group** page that is displayed, choose the type of device (Wireless or Wired), and select the devices to add to this group.

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

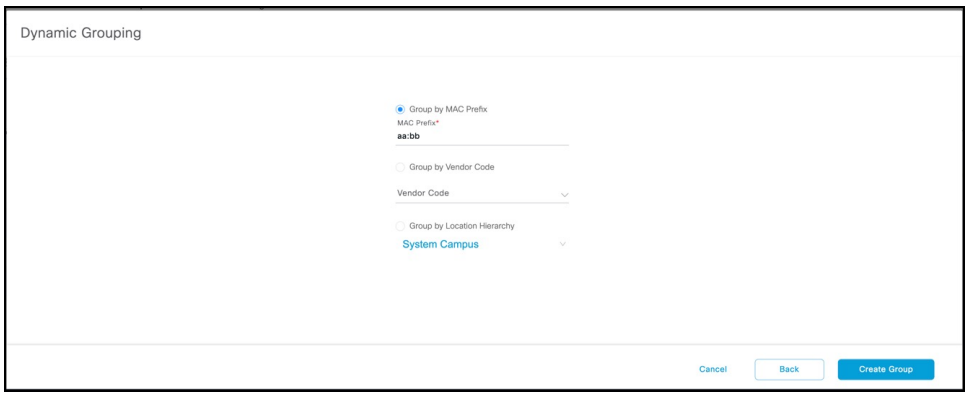


Figure 5: Group by Vendor Code

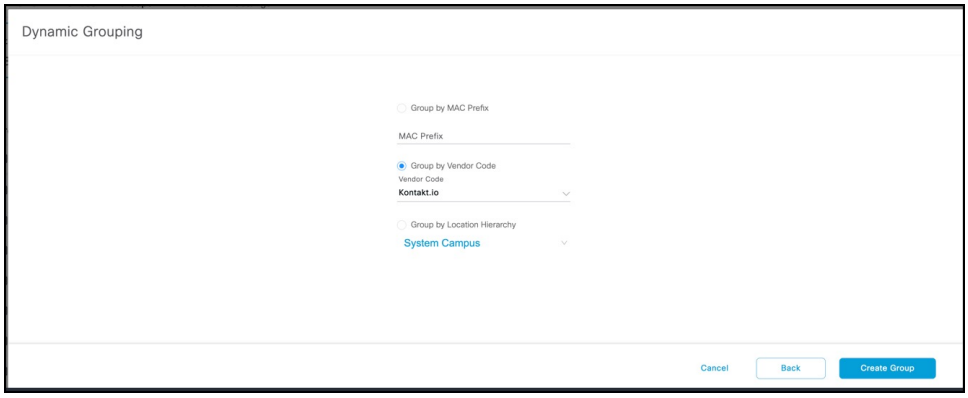


Figure 6: Group by Location Hierarchy

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.

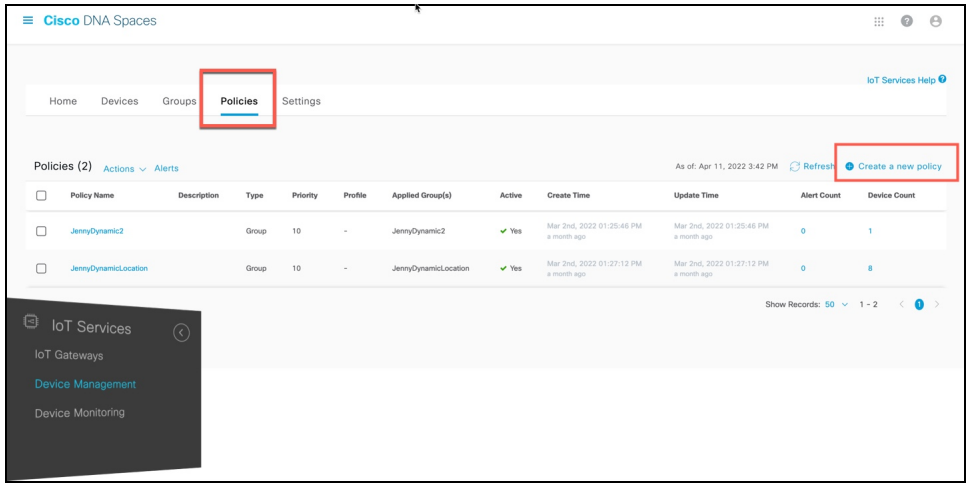
What to do next

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



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

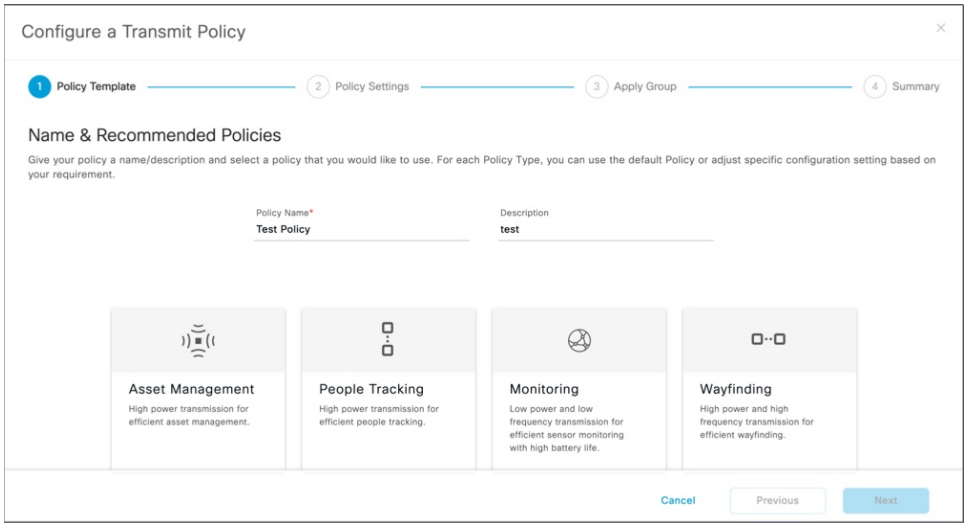
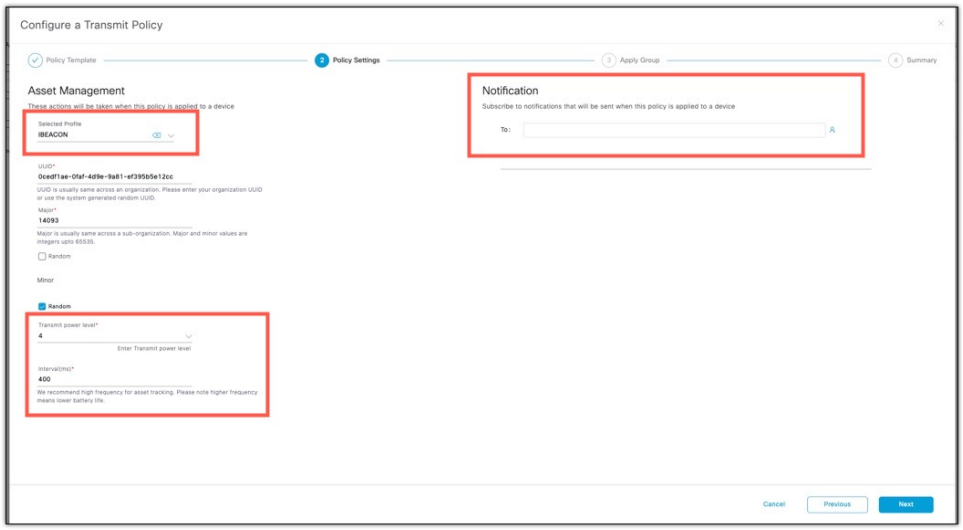


Table 1: Types of Transmit Policy

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

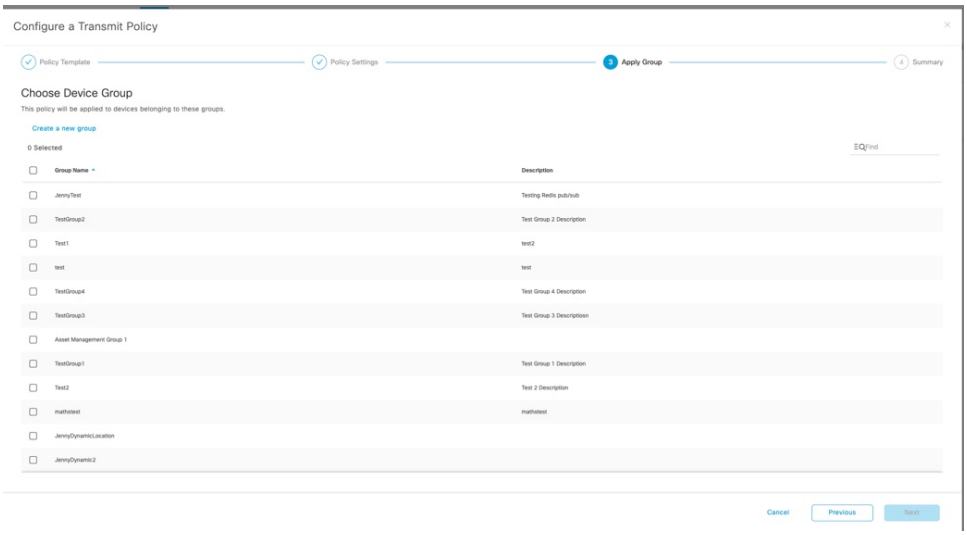
Step 3 From the **Configure a Transmit Policy** page that opens, enter email addresses in the **Notification** field. When this policy is applied to any device, the addresses are notified.

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

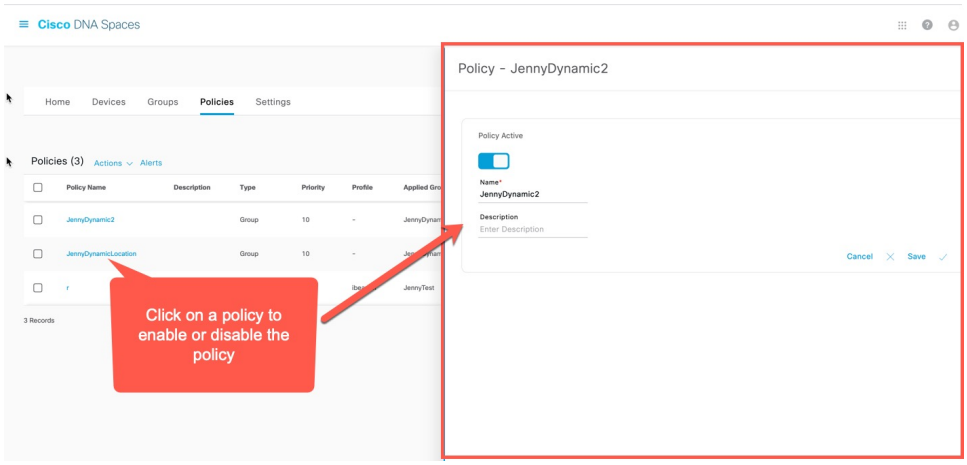
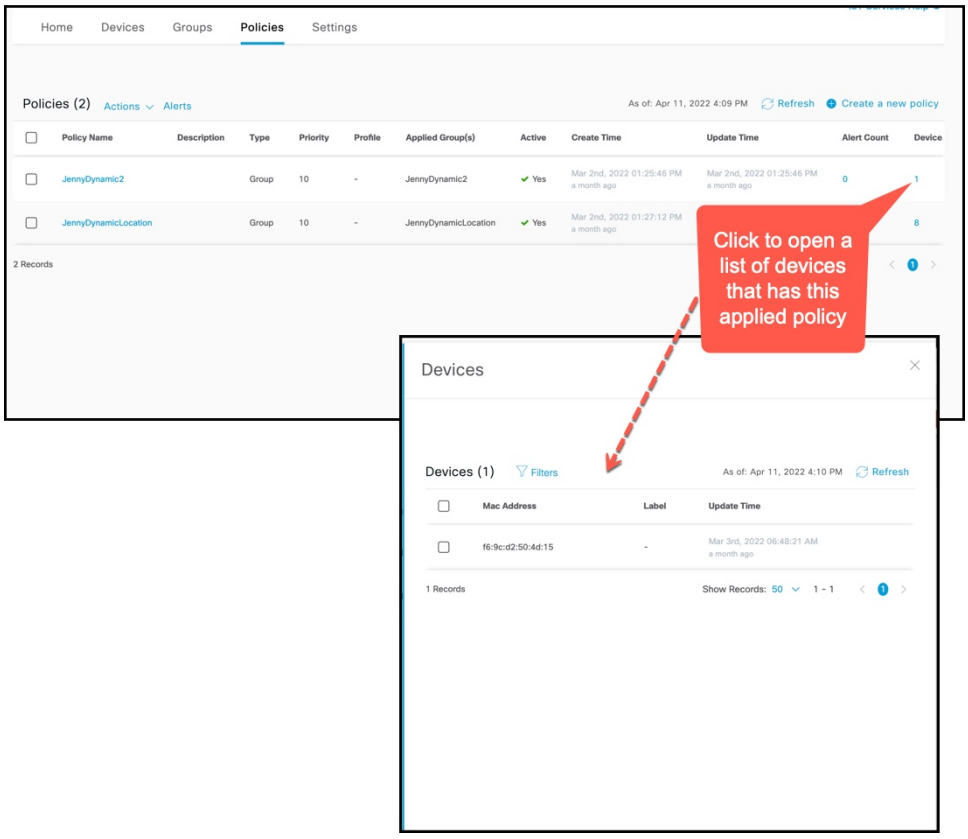
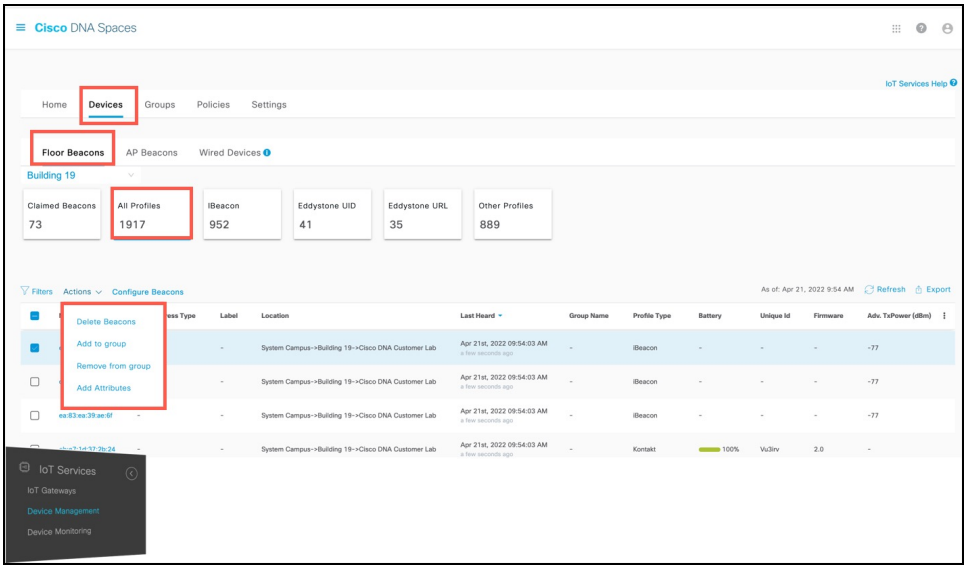


Figure 12: Viewing Devices on Which a Policy Is Applied



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

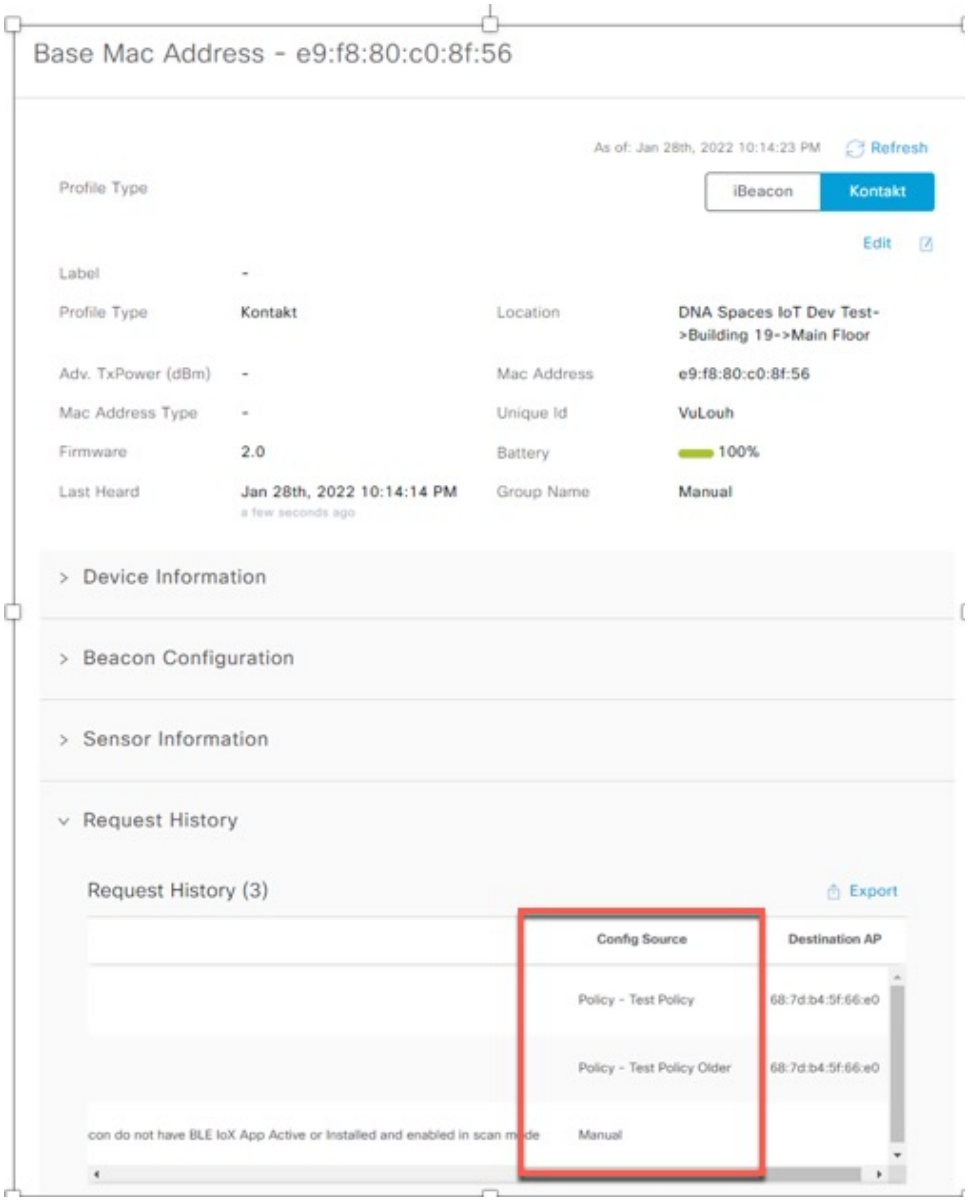


What to do next

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



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.

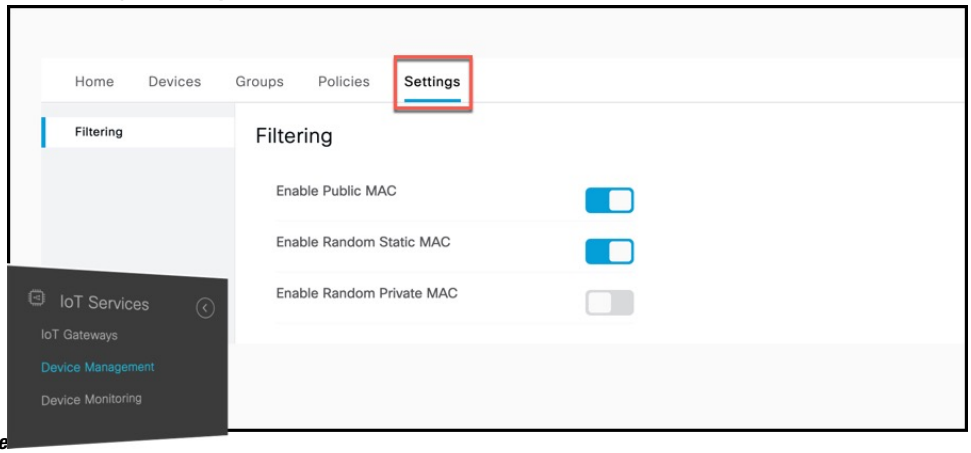
SUMMARY STEPS

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

DETAILED STEPS

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

Figure 15: Filtering Devices by MAC Address



Type