Revised: November 11, 2024

Migrate Connector 2.x to Connector 3 from Cisco Spaces Dashboard

Why Migrate Connector 2.x to Connector 3

Here are the reasons why you must consider migrating from Connector 2.x to Connector 3:

Table 1: Why Migrate to Connector 3

Improvement	Description
Improved Architecture:	• Uses a service-oriented architecture to create a modular Connector. • Each service is an independent module featuring lifecycle management, business logic, data channels, as well as command-line and user interfaces. • Simplifies management and development of services both in cloud environments and within the connector itself.
Enhanced Features:	Offers a comprehensive suite of advanced functionalities.
High Availability:	• Supports Virtual IP-based high availability configurations. • Facilitates seamless IoT and Cisco FastLocate operations with automated failover mechanisms.
Advanced Troubleshooting:	Provides detailed, step-by-step troubleshooting tools to quickly identify and resolve connectivity issues.
Improved Monitoring:	• Delivers extensive metrics on system and service performance, including CPU usage, memory, connectivity, and traffic. • Enables monitoring through the Cisco Spaces dashboard for real-time insights.
Efficient Upgrades:	Enables streamlined and uninterrupted upgrades, including service updates and security patches, all managed through the Cisco Spaces dashboard.

Features Support in Connector 2.x and Connector 3

Table 2: Connector 3 vs Connector 2.x Feature Matrix

Features	Connector 2.x	Connector 3
Location service	YES	YES
IoT Service (Wireless) and IoT Service (Wired)	YES	YES
OpenRoaming	YES	YES

Features	Connector 2.x	Connector 3
Cisco Spaces Apps	YES	YES
Cisco FastLocate	YES	YES
IPv4	YES	YES
IPv6	**NO**	YES
AMI support	YES	YES
Azure support	**NO**	YES
Hyper-V support	YES	YES
Local Firehose Service	YES	YES
External AAA support	YES	YES
Partner App Integration OR App Support	YES	YES
Dual Interface	YES	YES
High Availability	YES	YES
Advanced High Availability (IoT HA)	**NO**	YES

Before You Begin

Download and configure Connector Release 3. Refer to the Configuration section of the Cisco Spaces: Connector Configuration Guide. Refer to the release note to find the latest installation. Release Notes for Cisco Spaces: Connector

Once you install the Connector 3 instance, ensure that the services relevant to your specific use case are enabled, ACTIVE, and updated to the latest version.

Table 3: Services to Install

Service	Instructions
IoT Service (Wired)	Configure IoT Service (Wired)
IoT Service (Wireless)	Configure IoT Service (Wireless)
Hotspot Service	Configure Hotspot Service, on page 22
Local Firehose Service	Configure Local Firehose Service, on page 23

Note

Make sure that the x86-64-v2 CPU is available for Enterprise Linux 9. Also, ensure that the x86-64-v2 CPU supports the following flags: SSE3, SSE4_1, SSE4_2, and SSSE3.

Migrate and Verify

Migrate Connector 2.x to Connector 3 from Cisco Spaces Dashboard

This procedure shows you how to migrate your existing Cisco Spaces: Connector 2.x configurations to Connector 3, from the Cisco Spaces dashboard.

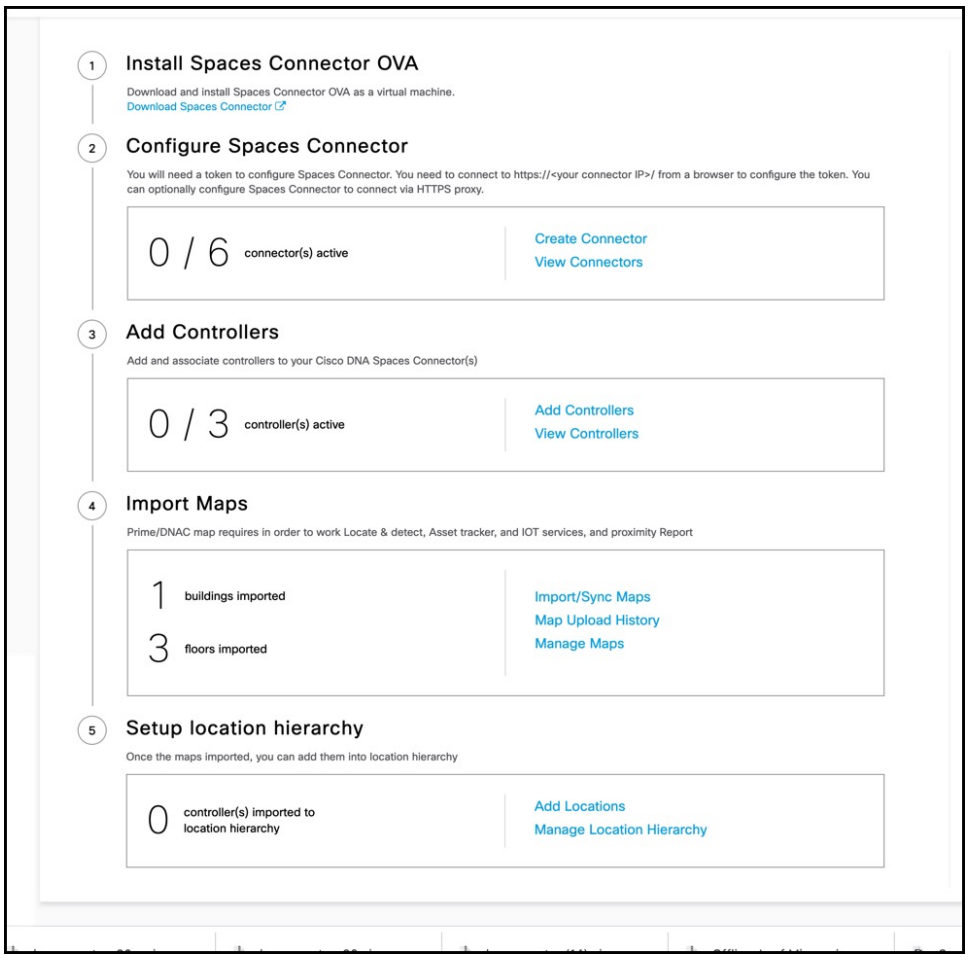
Step 1 Log in to **Cisco Spaces**.

Note The Cisco Spaces URL is region-dependent.

Step 2 In the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.

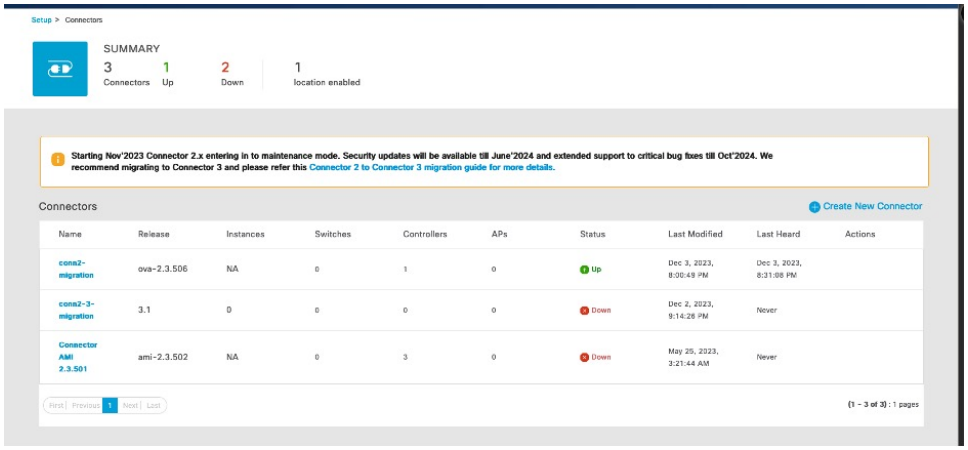
Step 3 From the **2. Configure the Spaces Connector** area, click **View Connectors**.

Figure 1: View Connectors



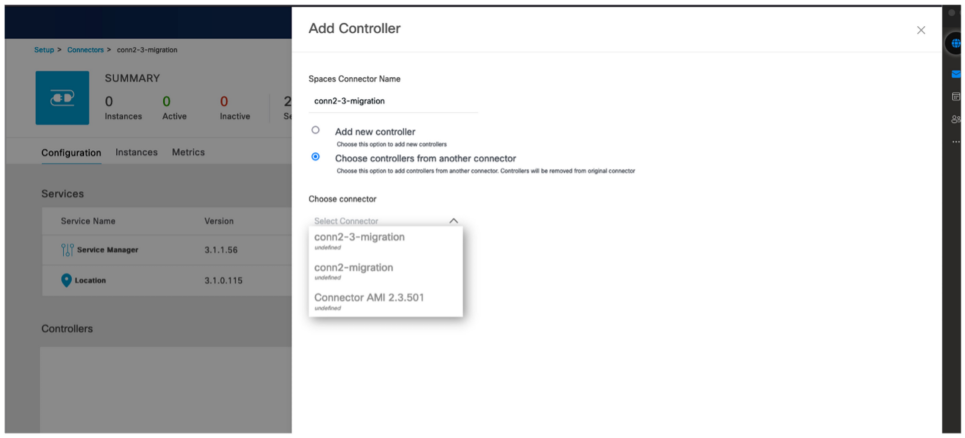
Step 4 From the list of connectors displayed, click the connector 3 you installed. Click **Add Controller**.

Figure 2: Choose Connector 3



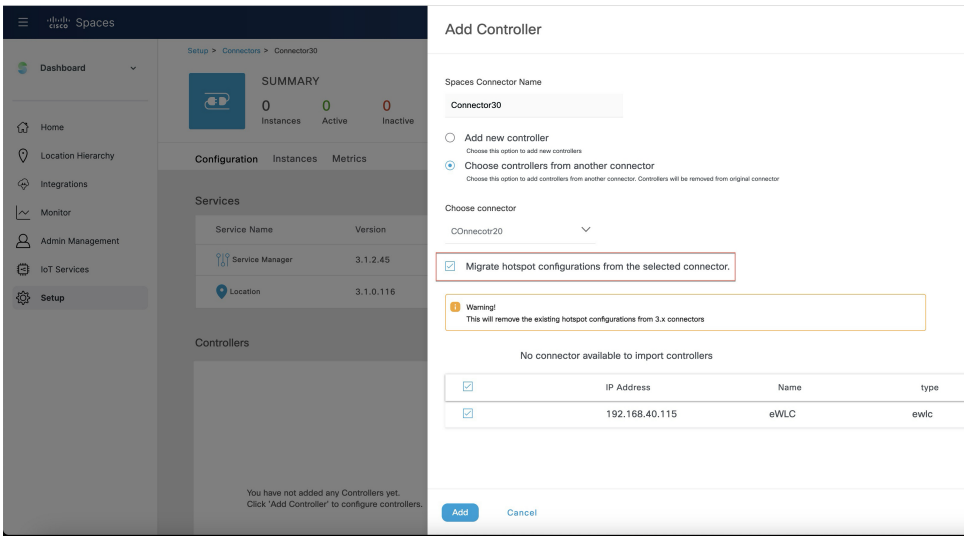
Step 5 From the **Add Controller** tab of this specific connector, click **Choose controllers from another connector**. From the **Choose connector** drop-down list displayed, choose the connector 2.x that you want to migrate configurations from.

Figure 3: Move Wireless Controllers from Connector 2.x



Step 6 To migrate hotspot configurations from the connector 2.x, check the **Migrate hotspot configurations from the selected connector** check box.

Figure 4: Migrate Hotspot Configurations from Connector 2.x



Note

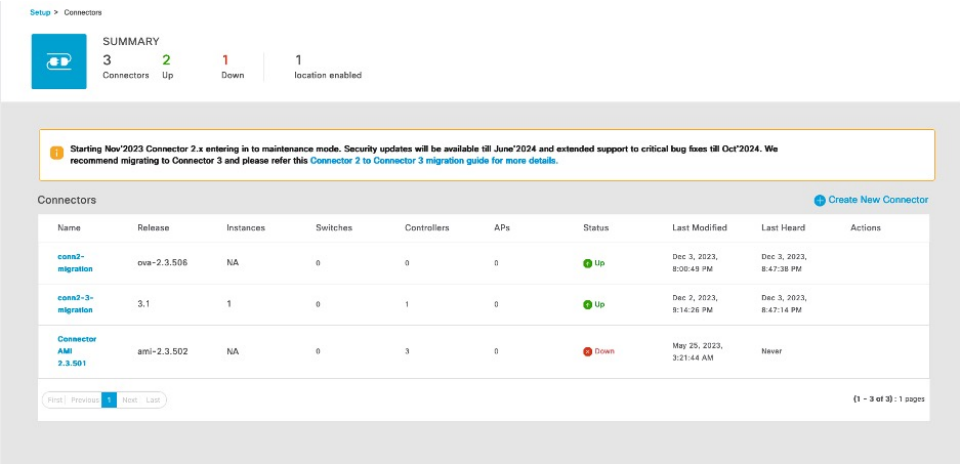
The following points are related to the migration of Hotspot Service:

- Cisco Spaces sets up and enables the same hotspot configuration on the new Connector 3 instance as on the Connector 2.x.
- Cisco Spaces does not automatically route traffic from the wireless controller to the Connector 3 onstance.
- Users must manually update their wireless controller configurations to direct traffic to the Connector 3 instance.To migrate the wireless controller configuration to the Connector3 Instance, see Configure Cisco AireOS or Cisco Catalyst Network, on page 25.
- After setting up and confirming the new configuration, users must remove any references to Connector 2 to disable the previous Hotspot or OpenRoaming setup.
- Any existing hotspot settings on Connector 3 are overwritten when migrating from Connector 2.x to Connector 3.

Verify the Migration Status of Connector 3

In the **Setup > Connector** window, observe the status of migration. Wait for the value of the **Status** cell of the Connector 3 to change from **Down** to **Up**.

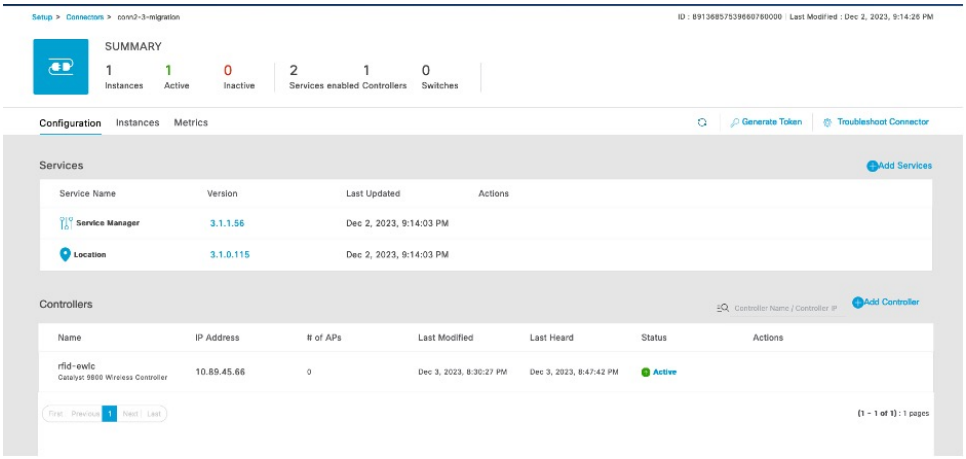
Figure 5: Observe Status of Connector 3



Verify Wireless Controllers, APs, and Location Service

Verify if the wireless controller is in **Active** state. Then, verify if the number of APs is the same as the Connector 2.x. This automatically verifies the Location service as well.

Figure 6: Status of Wireless Controller



Note

The time it takes for the controller to reach an ACTIVE state may differ based on the number of services chosen and the size of the deployment; however, we recommend that you wait a few minutes for this process to be completed.

Verify IoT Service (Wireless)

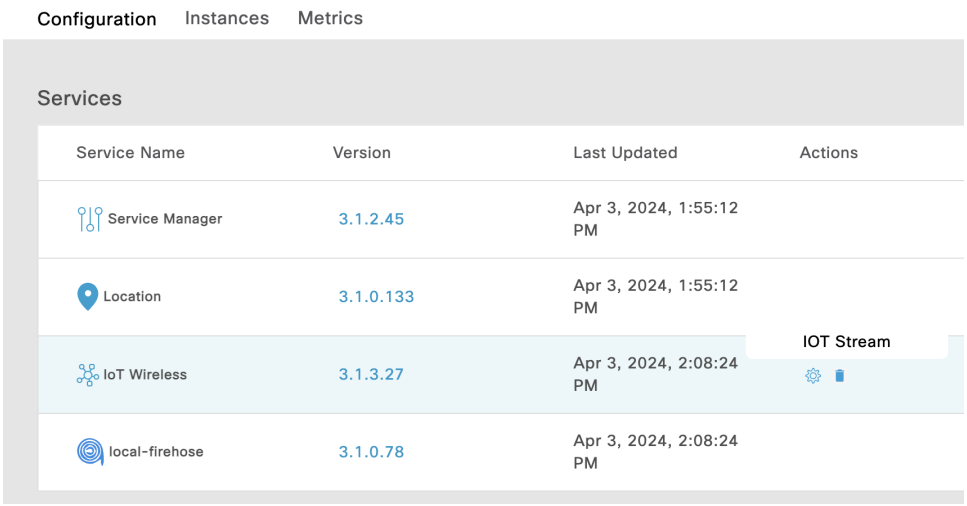
If you had enabled the IoT service (wireless) for your use case, verify if the service is migrated.

Step 1 In the Cisco Spaces dashboard, choose **Setup > Wireless Networks** > **2. Configure the Spaces Connector** area > **View Connectors**.

Step 2 From the list of Connectors displayed, choose the newly migrated connector 3.

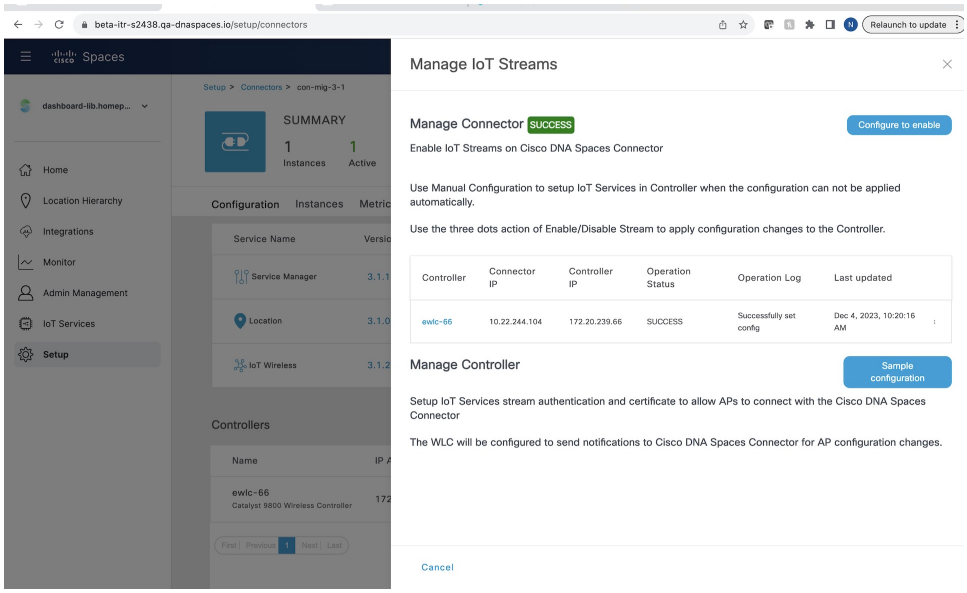
Step 3 From the list of services, click the gear icon on the **IoT Wireless** row and from the pop-up menu, choose **IoT Stream**.

Figure 7: Choose IoT Stream



Step 4 In the **Manage IoT Streams** window, check the **Operation Log** and ensure that the status is **Successfully set config**.

Figure 8: Status of IoT Service (Wireless)



Verify Hotspot Service

If you had enabled the Hotspot service for your use case, verify if the service is migrated.

Step 1 In the Cisco Spaces dashboard, choose **OpenRoaming**. In the **OpenRoaming** left-navigation pane, choose **Setup.**

Step 2 In the **Hotspot-enabled Connectors** area, choose **Cisco Wireless Controllers**.

Step 3 Verify if the new Connector 3 instance is in the ACTIVE state.

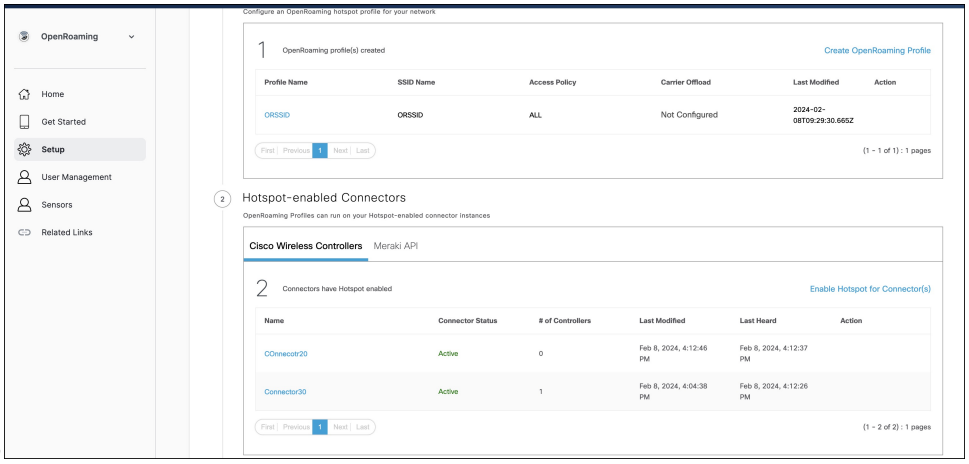


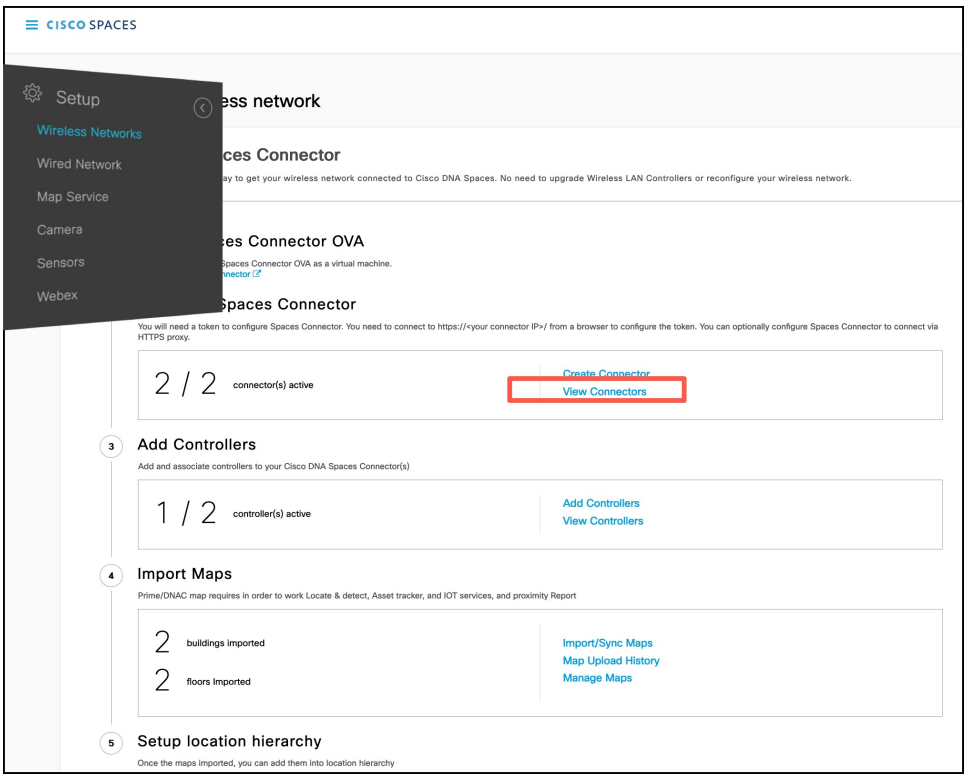
Figure 9: Status of Hotspot Service

Configure Local Firehose

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

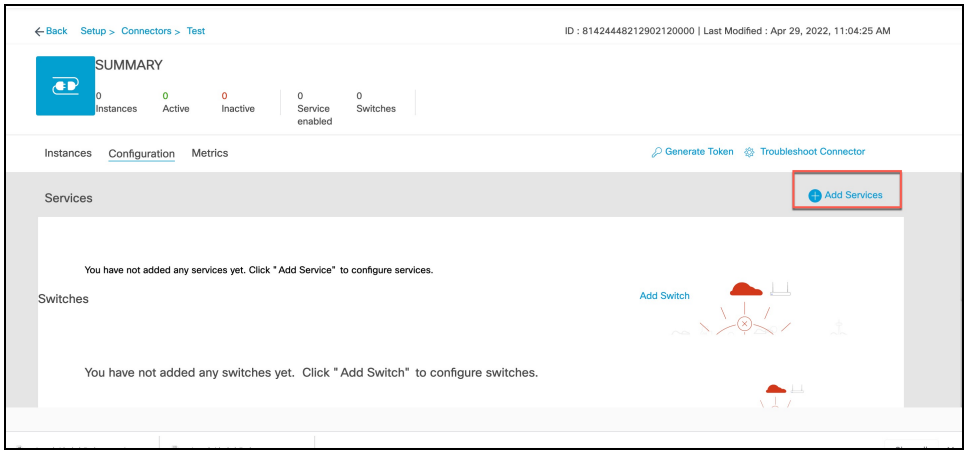
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 10: View Connectors



Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 11: Add Service



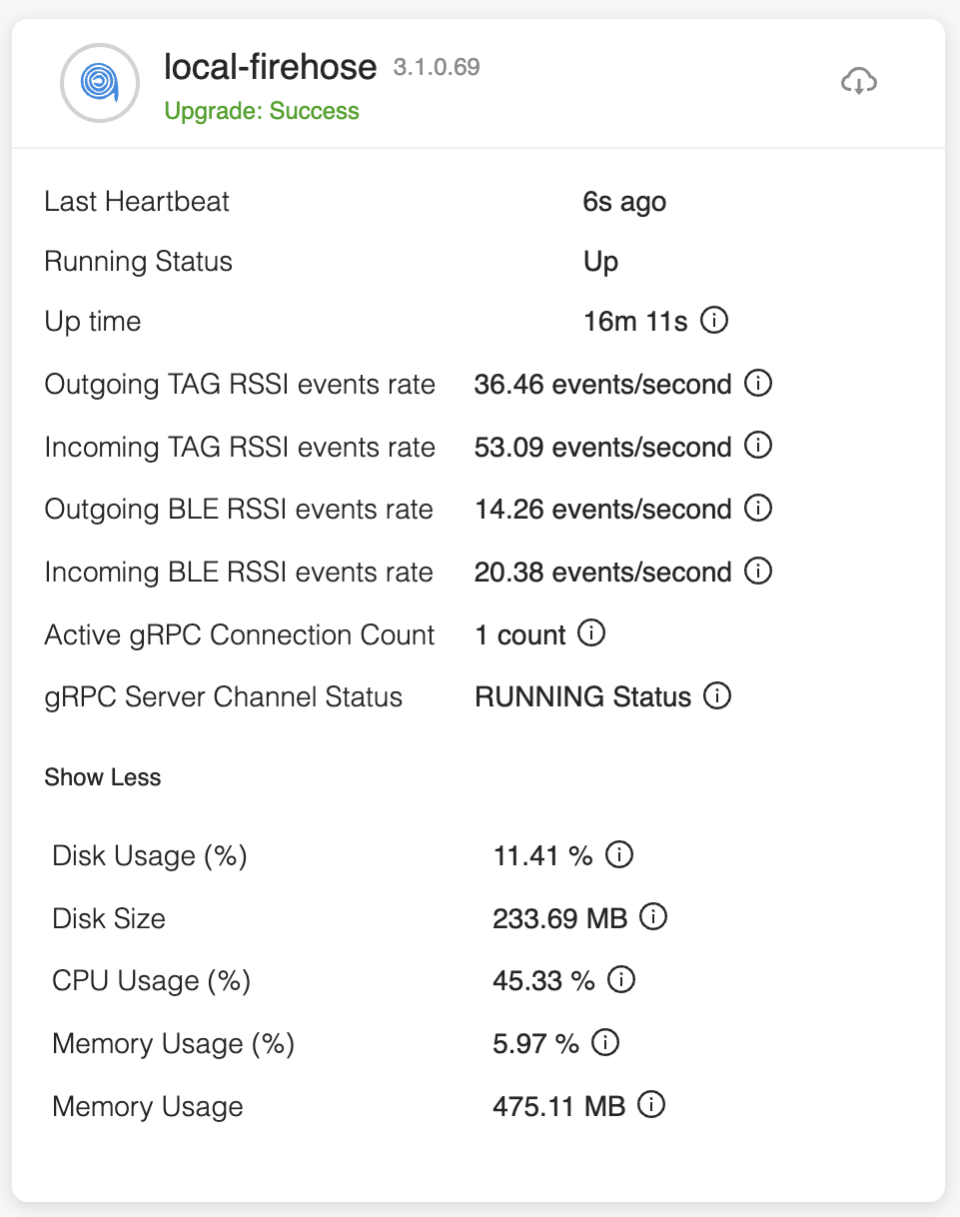
Step 4 In the **Add Service** window that is displayed, choose **local-firehose** and click **Add**.

Note To receive events such as Device_RSSI for Received Signal Strength Indicator (RSSI)-based tags and Device_BLE events for Bluetooth Low Energy (BLE) tags, ensure that **location** and **iot-services** services are also added.

You can see that the number of services enabled has increased.

Step 5 Login to the Connector GUI. Scroll downwards to the **local-firehose** tile. Verify if the running status is **Up**.

Figure 12: local-firehose



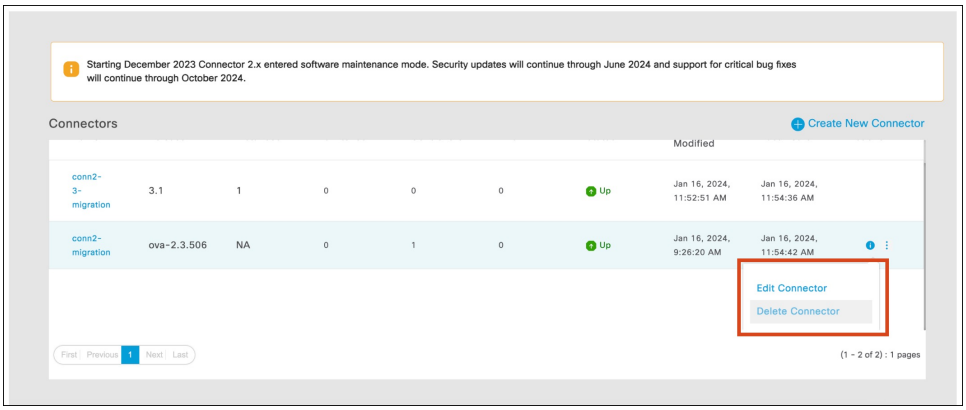
What's next

- Stanley customers using the Aeroscout Location Engine (ALE) should update the IP address of the Connector 2.x instance to the IP address of the Connector 3 instance.
- All other customers must update their applications with the new Connector 3 instance IP address.
- If the Connector3 is configured in High Availability VIP mode, both the primary and secondary Connector 3 instance IPs must be utilized in the ALE.
- The API key for the local firehose remains unchanged and is the same as the one generated for Connector 2.

Last Steps

Once migrations is completed, and verified, remove Connector 2.x instances from the Cisco Spaces dashboard.

Figure 13: Delete Connector 2.x Instance



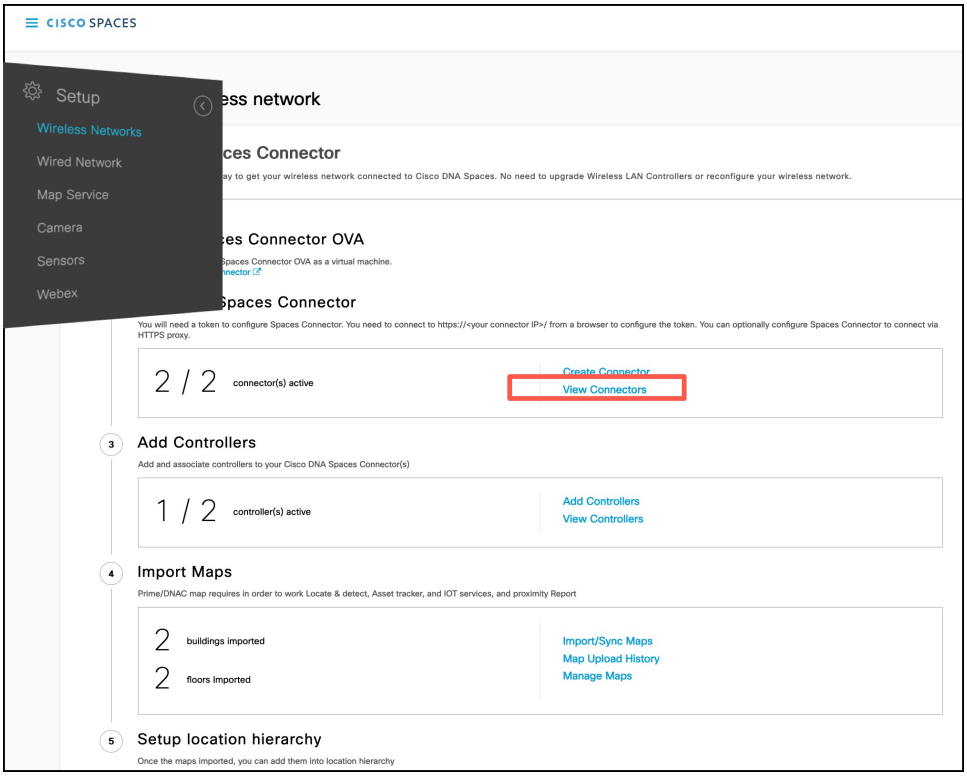
For Your Reference

Configure IoT Service (Wireless)

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

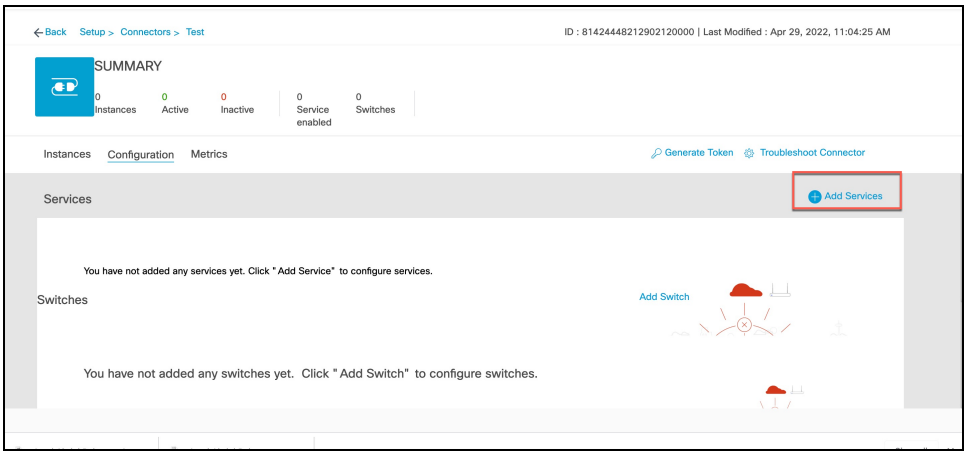
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 14: View Connectors



Step 3 In the connector details window that is displayed, click **Add Services**.

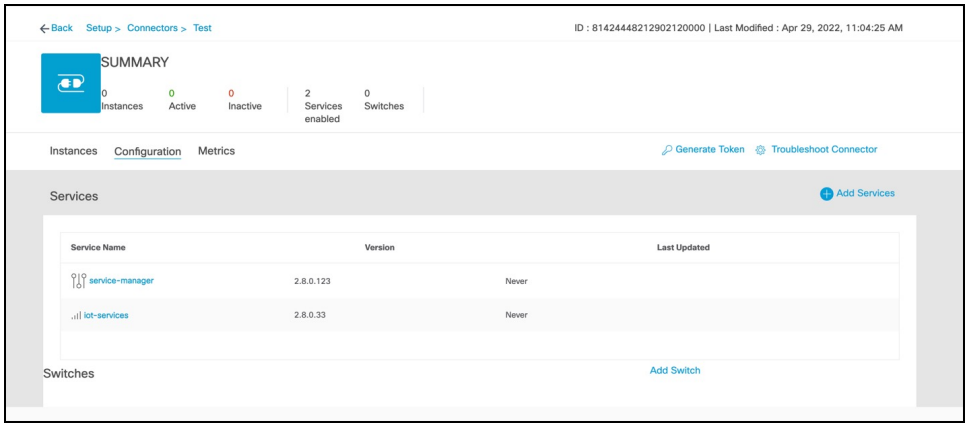
Figure 15: Add Services



Step 4 In the **Add Services** window that is displayed, choose **IoT Wireless** and click **Add**.

Note **service-manager** is chosen by default.

Figure 16: Connector Details



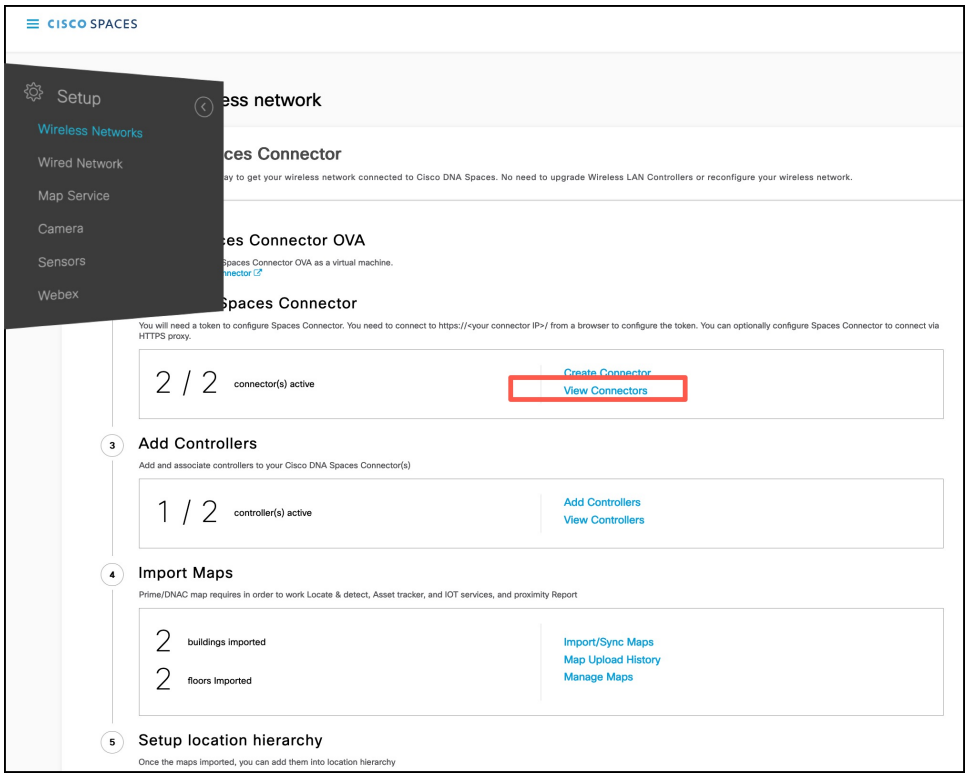
In the **Connector Details** window, you can see that the number of services that are enabled has increased.

Configure IoT Service (Wired)

Step 1 From the Cisco Spaces dashboard left-navigation pane, click **Setup** and choose **Wired Networks**.

Step 2 From the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 17: View Connectors

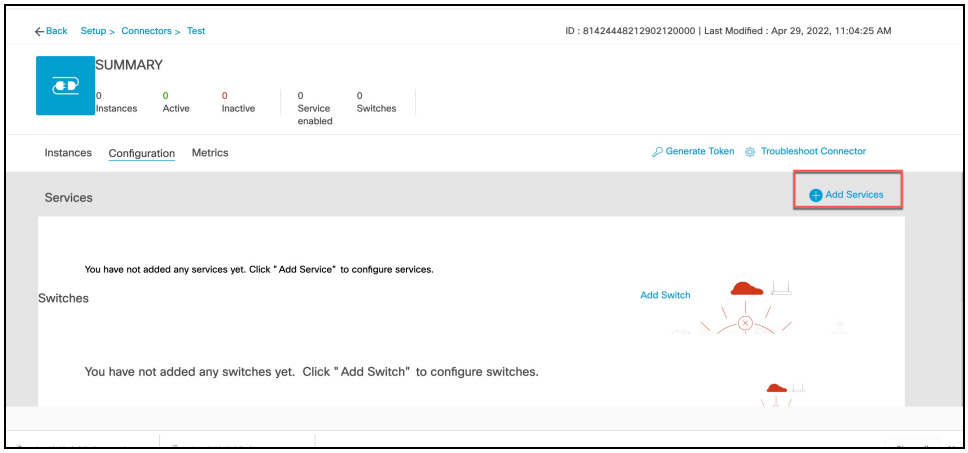


Step 3 Click a connector 3 of your choice.

Note You can use the same connector that you used for Cisco Spaces: IoT Service (Wireless).

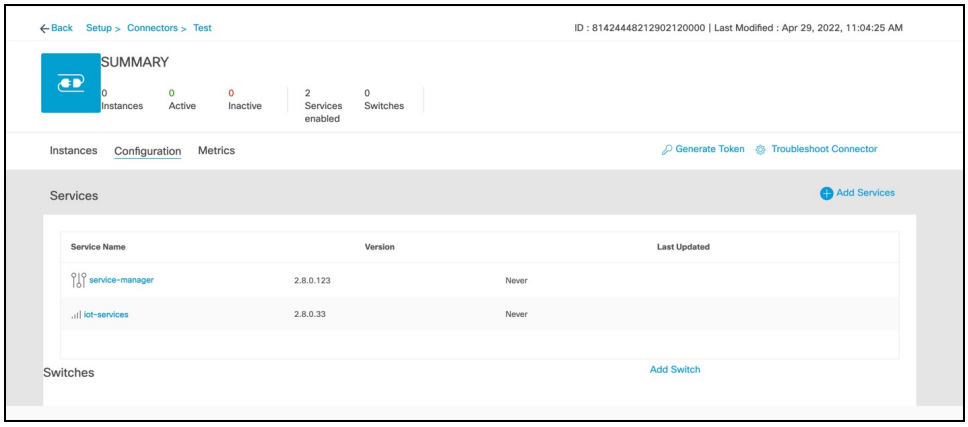
Step 4 In the connector details window that is displayed, click **Add Services**.

Figure 18: Add Services



Step 5 In the **Add Service** window that is displayed, choose **IoT Wired** and click **Add**.

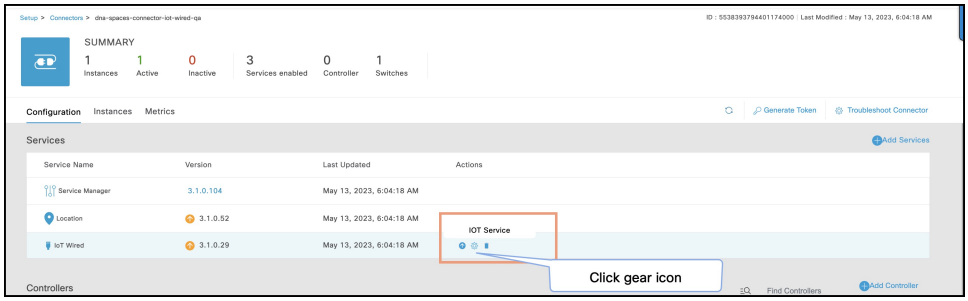
Figure 19: Adding a Service



In the **Connector Details** window, you can see that the **IoT Wired** service has been added.

Step 6 Click the gear icon near the **IoT Wired** row.

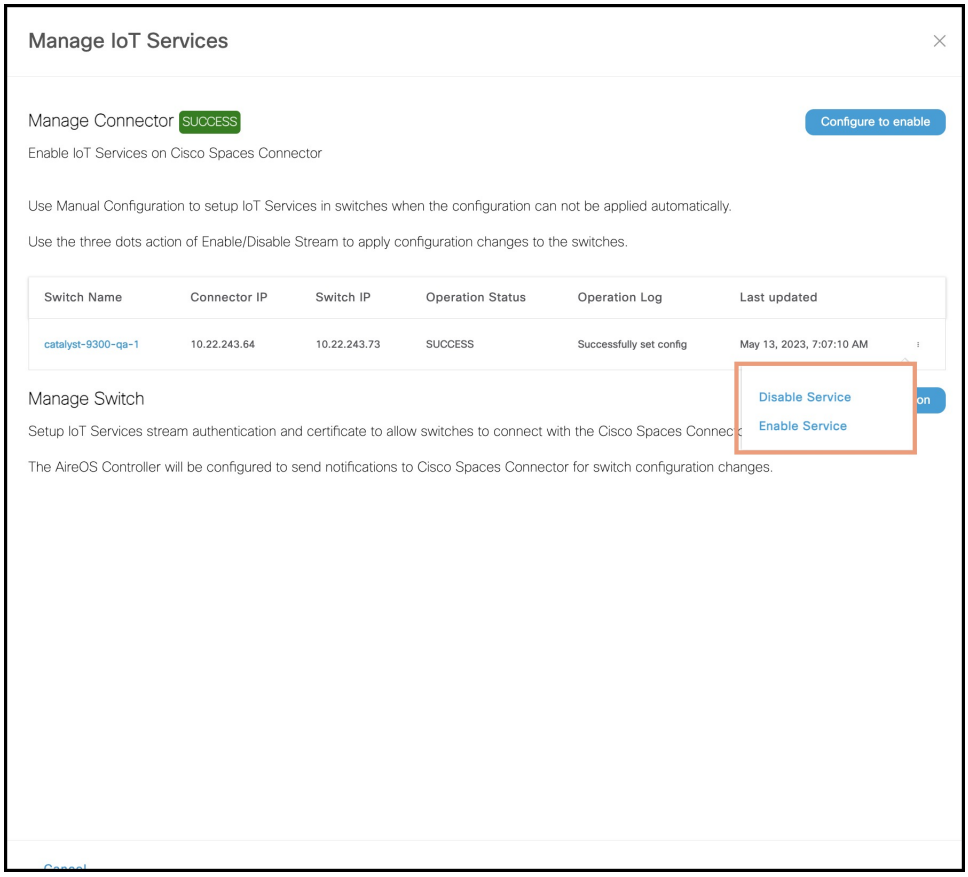
Figure 20: Gear Icon of IoT Wired



Step 7 (Optional) In the **Manage IoT Streams** window that is displayed, check if the connector is not already enabled, and if it is not, click **Configure to Enable**.

Step 8 From the list of switches, click the vertical three-dot icon adjacent to the switch and select **Enable Service**.

Figure 21: Enable Service



Note If you are using the same connector for both wired and wireless IoT services, the connector is already enabled.

Step 9 Enter the SPAN VLAN and the Cisco IOx App details.

- **Destination SPAN VLAN**: The VLAN used to send Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.
- **Destination SPAN VLAN IP address**: This is the Switched Virtual Interface (SVI) or the IP address of the destination VLAN that can be used to route traffic. If you are using an existing VLAN, you can provide the same IP address. We recommend that you create a new VLAN so that you can keep the ERSPAN traffic local without impacting the existing configuration. Note that this VLAN is used only within the switch for the SPAN traffic.
- **Source SPAN VLAN list:** List of VLANs to which the wired devices are connected. The traffic on these VLANs are monitored. If the wired devices are connected to multiple VLANs, enter the VLANs separated by a comma.
- **Monitor SPAN origin IP address**: This is the source IP address of the monitor session. This can be from the SPAN VLAN. This can also be the same as the destination VLAN IP address.
- **IoX application Span IP Address**
- **Application Cisco Spaces Connector VLAN**: This is the VLAN on which the connector is reachable (for management or data). You can configure the Cisco IOx App's second interface to use this VLAN to send traffic to the connector. This VLAN can be the same as the wired PoE node VLAN. The connector must be permitted to accept communications from the Cisco IOx application.
- **DHCP**: When enabled, DHCP allocates an IP address from the **Application DNA Spaces Connector VLAN** to the Cisco IOx App's second interface.
- **IoX application IP address**: This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the Connector. This is not required if you select DHCP.
- **IoX application netmask**: This is the IP subnet mask that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.
- **IoX application gateway address**: This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.

Figure 22: Configure Switch

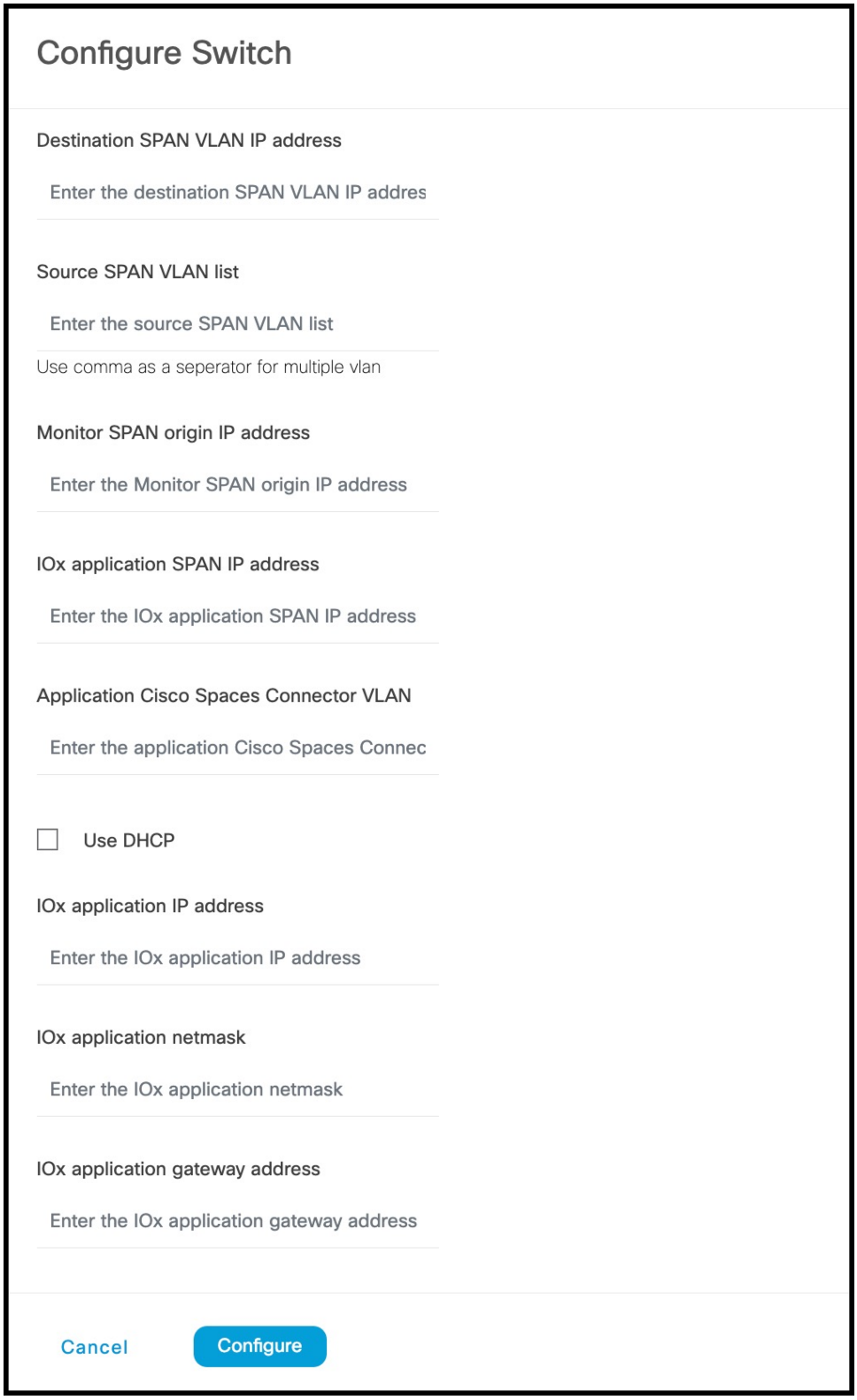


Figure 23: Configure Switch

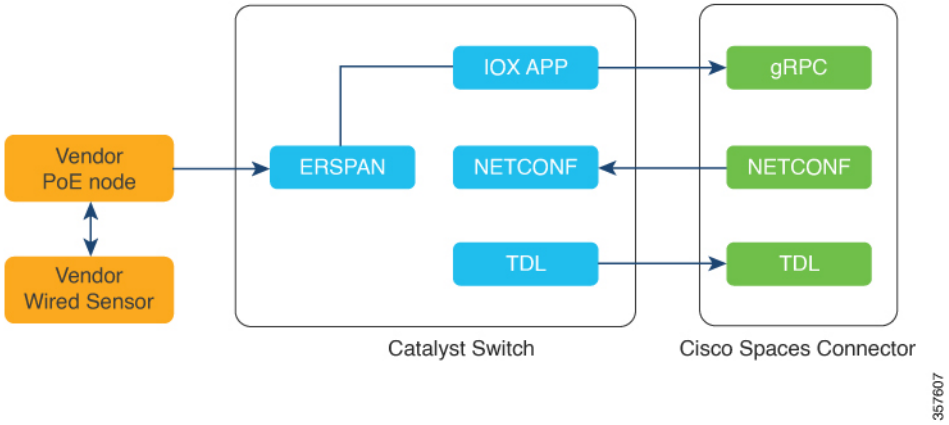
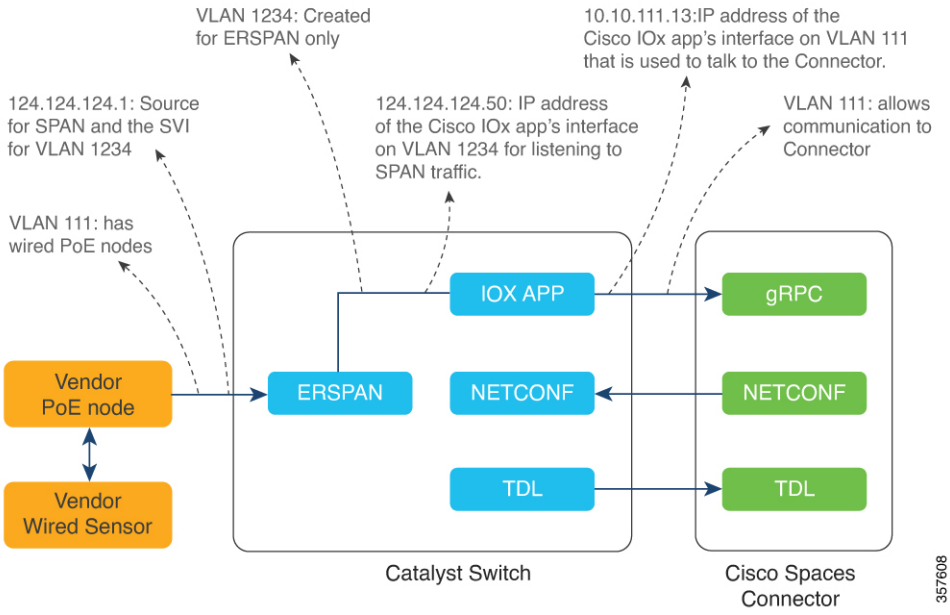


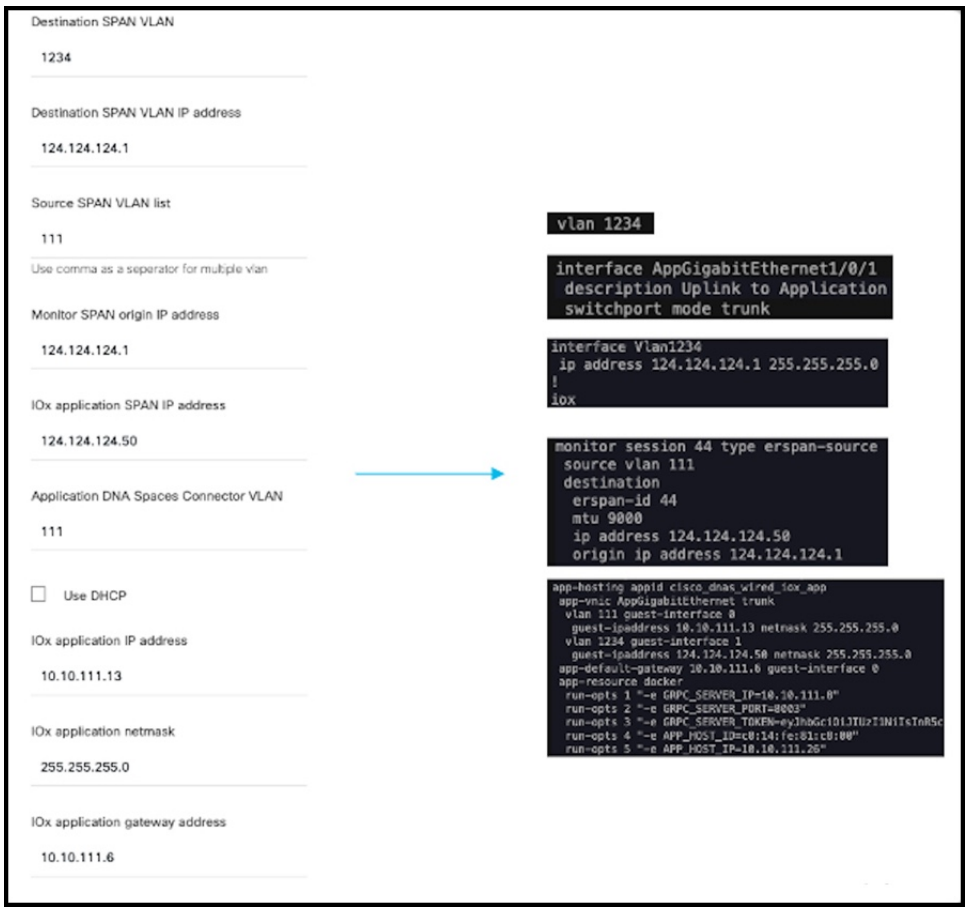
Figure 24: Sample Configuration



Step 10 Click **Configure**.

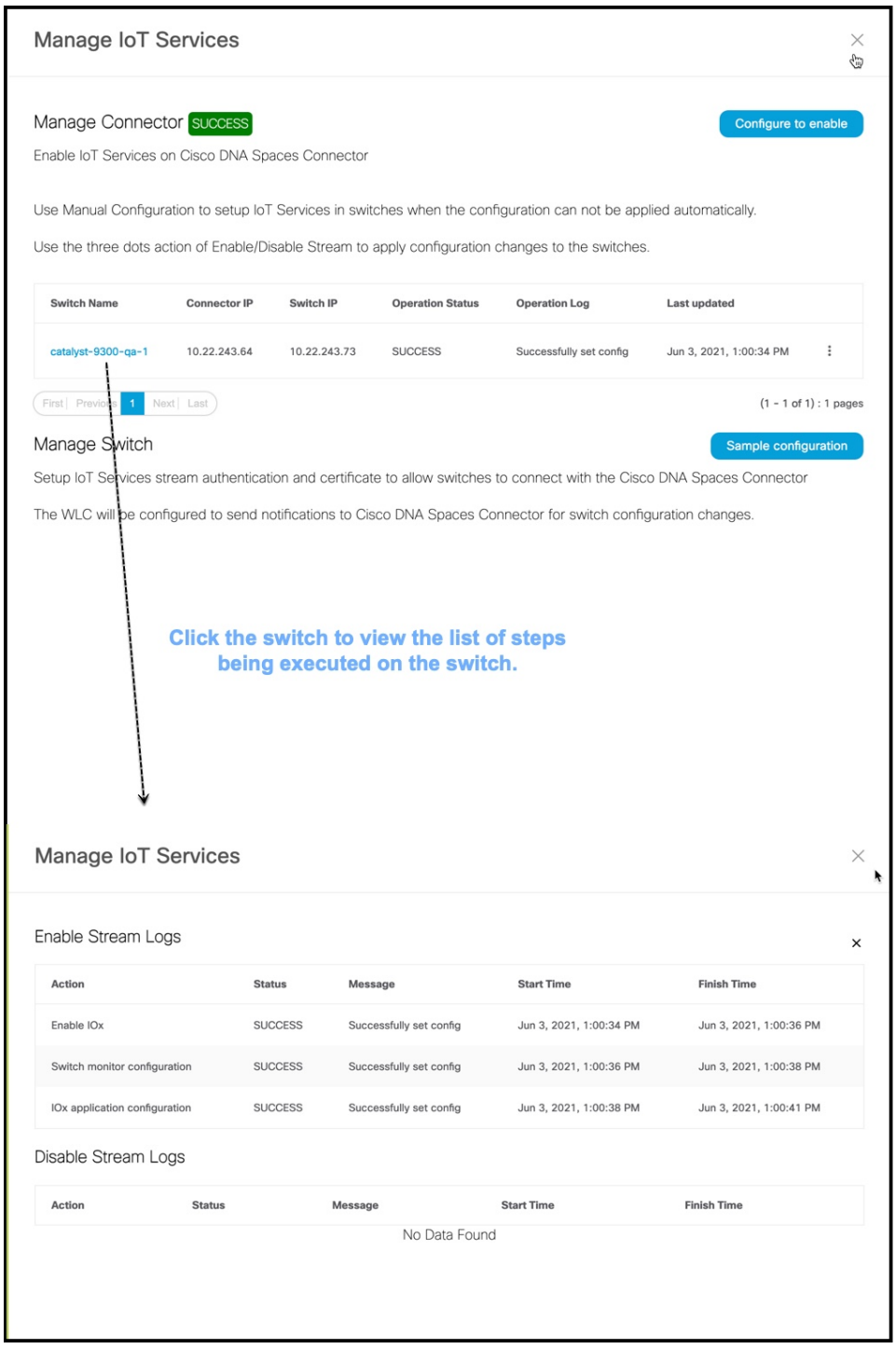
The configurations are deployed on the switch. The following diagram shows the corresponding CLI commands you can use in place of the GUI configuration.

Figure 25: GUI-Command Line Mapping



Step 11 In the **Manage IoT Services** window that you are taken to, you can click on a name of the switch to see the list of steps executed on that switch.

Figure 26: Manage IoT Services

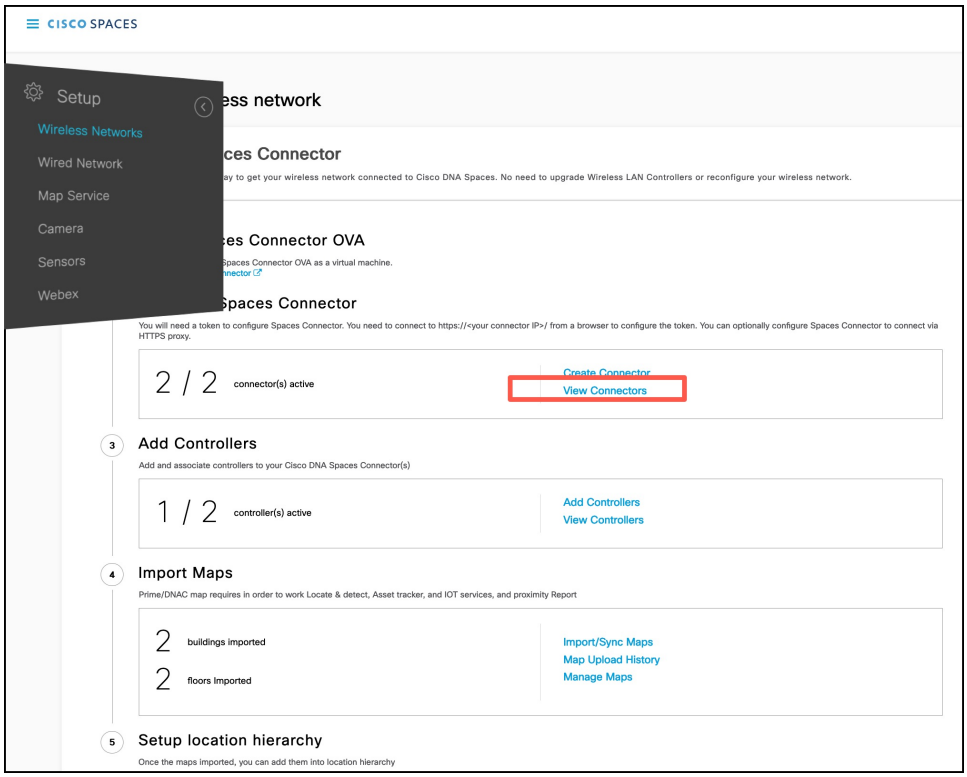


Configure Hotspot Service

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

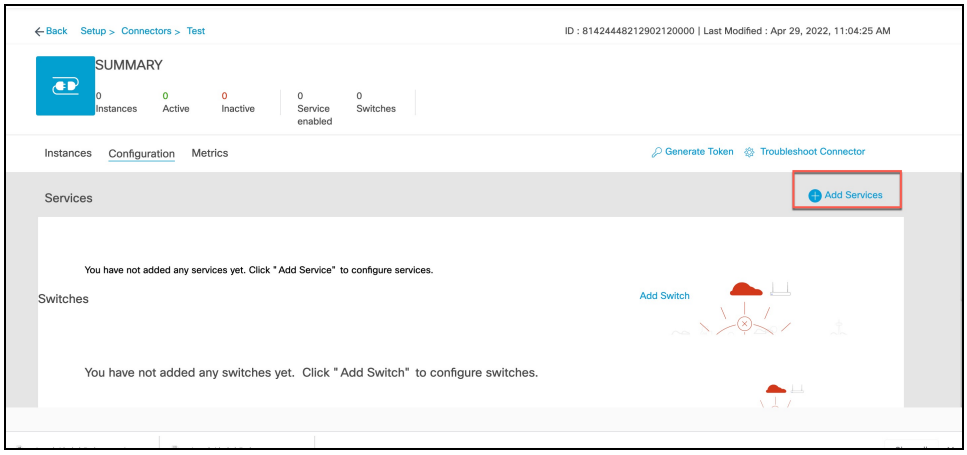
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 27: View Connectors



Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 28: Add Service



Step 4 In the **Add Service** window that is displayed, choose **hotspot** and click **Add**.

service-manager is added by default.

Note

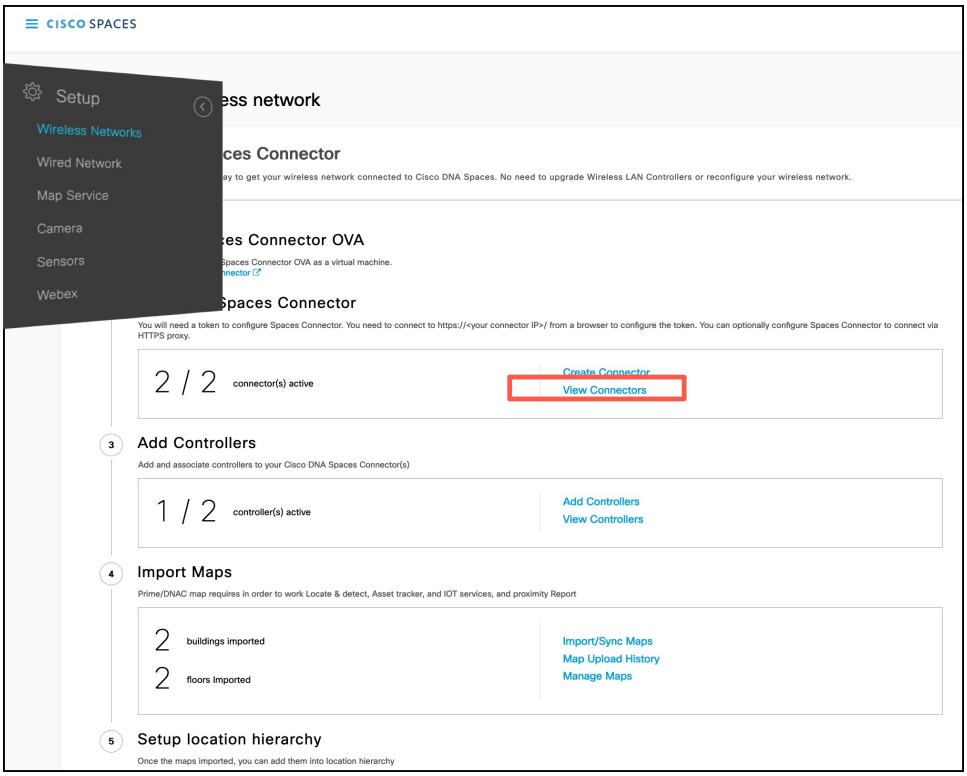
In the **Connector Details** window, you can see that the number of services enabled has increased.

Configure Local Firehose Service

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

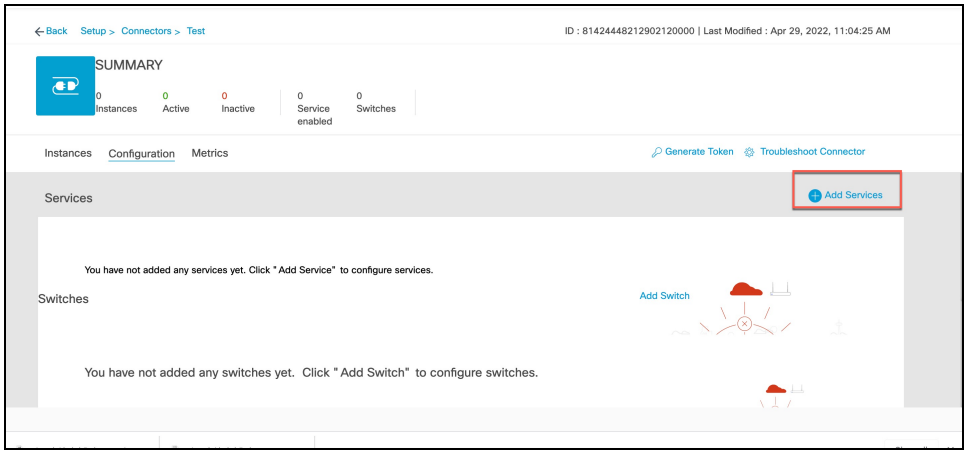
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 29: View Connectors



Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 30: Add Service



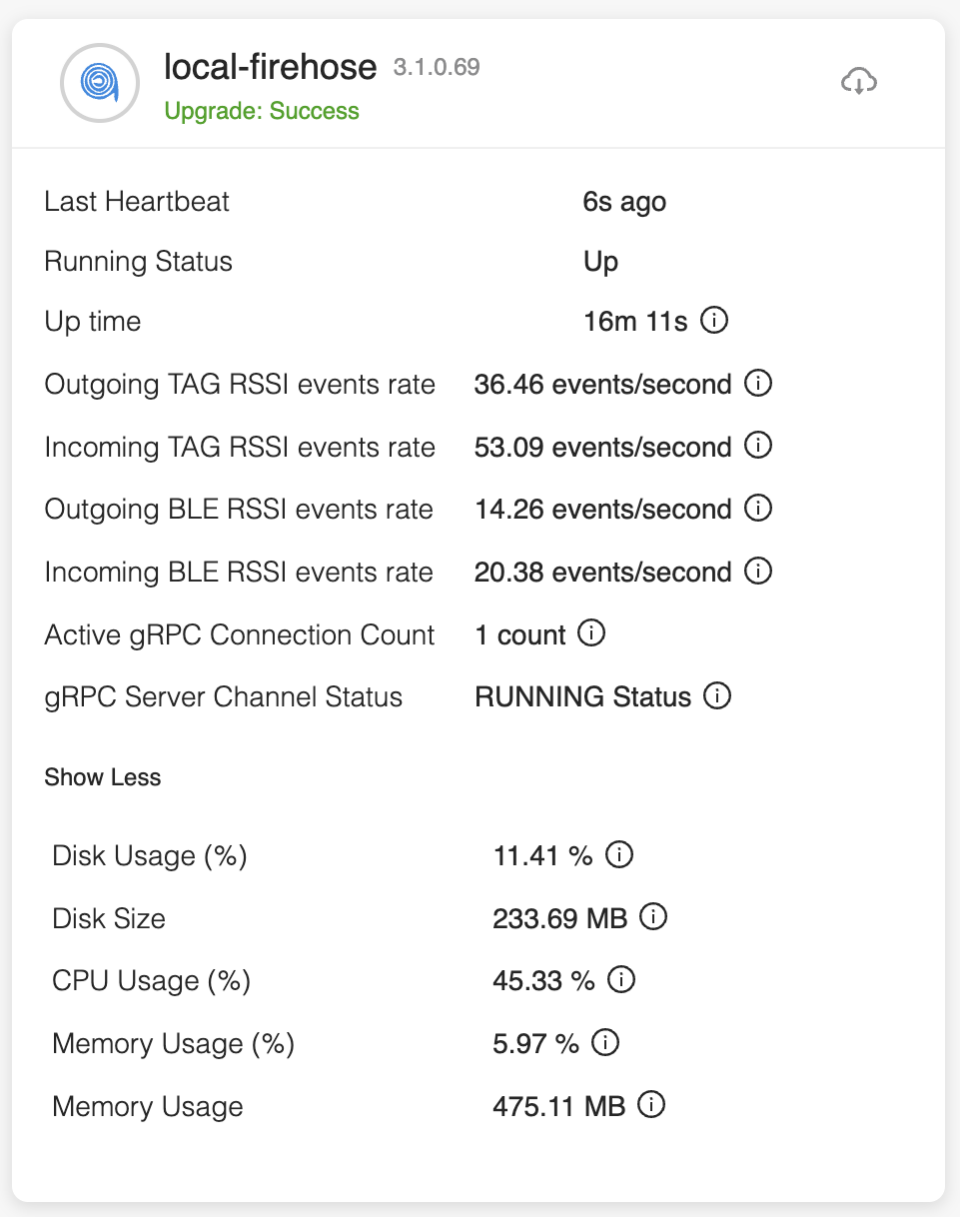
Step 4 In the **Add Service** window that is displayed, choose **local-firehose** and click **Add**.

Note To receive events such as Device_RSSI for Received Signal Strength Indicator (RSSI)-based tags and Device_BLE events for Bluetooth Low Energy (BLE) tags, ensure that **location** and **iot-services** services are also added.

You can see that the number of services enabled has increased.

Step 5 Login to the Connector GUI. Scroll downwards to the **local-firehose** tile. Verify if the running status is **Up**.

Figure 31: local-firehose



Configure Cisco AireOS or Cisco Catalyst Network

Before you configure the Cisco AireOS or Cisco Catalyst wireless network, you must configure the SSID and AAA policy.

Step 1 In the **OpenRoaming** window, click **Set Up OpenRoaming** or choose > **Setup**.

The **OpenRoaming Setup** page is displayed.

Note If you have completed the OpenRoaming Profile configuration, click **Continue OR Setup** in the configuration wizard to proceed.

In the **Network configuration** section, under the **AireOS/Catalyst controllers** tab, a list of all the Cisco AireOS and Cisco Catalyst series controllers appears with details such as the Controller status and associated Connectors.

Step 2 Under **Network configuration** > **AireOS/Catalyst controllers**, in the **Action** column, click the settings icon corresponding to the controller you want to configure.

The **Configure Controller** window is displayed.

Step 3 Under **Generate Configuration**, select the OpenRoaming profile from the drop-down list.

If a non-default policy profile or policy tag is used, you must copy only the Access Network Query Protocol (ANQP) server settings and apply it to the wireless policy profile. Ensure that the policy tag uses the WLAN configured for OpenRoaming, and is mapped to the configured wireless policy profile.

Step 4 Paste the selected OpenRoaming profile configuration in the Cisco AireOS or Catalyst controller CLI.

Note Only CLI-based configuration is supported.

Step 5 Click **Continue**.
A **Controller configured with profile successfully** message is displayed.

Step 6 Choose the controller type between **AireOS** and **Catalyst 9800**.

Step 7 In the **WLAN ID** field, enter a WLAN ID if your existing network is based on a Cisco AireOS Controller. Specify the WLAN name if it is based on a Cisco Catalyst Controller.

Step 8 Click **Close**.
The **OpenRoaming Setup** window is displayed.