Cisco Spaces: OpenRoaming Configuration Guide

First Published: 2021-12-14

Last Modified: 2022-11-21

CHAPTER 1

Overview of OpenRoaming

> ✎
>
> **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.

Prior to the introduction of OpenRoaming, many mobile device users preferred to stay connected to their personal cellular network because it was more convenient and provided a more secure internet connection. Their internet usage was dependent on their cellular coverage and mobile data plan.

OpenRoaming enables secure, seamless, and automatic network connectivity by eliminating tedious Wi-Fi guest onboarding processes and the risk of connecting to rogue SSIDs. This is especially helpful for a mobile device user trying to access the internet because OpenRoaming removes the need to choose between multiple SSIDs, or enter insecure, shared credentials on poorly designed captive portals. With OpenRoaming, user mobility is enhanced by enabling users to connect to the guest network by signing in using a trusted identity provider.

Figure 1: OpenRoaming Federation
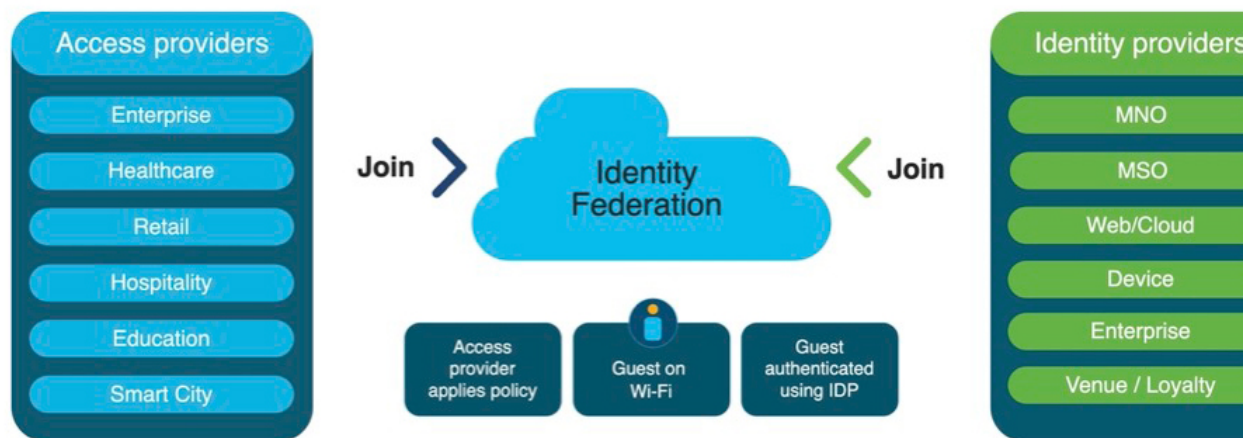
The OpenRoaming Federation consists of access providers and identity providers. Access providers provide the wireless networks that customers will automatically connect to. Access providers include retailers, airports,

hotels, large enterprises, and public venues. Identity providers allow users to access the network after verifying if they are valid customers. Identity providers include service providers (based on SIM card validity), device and cloud providers (such as Google and Apple), and internet Wi-Fi providers.

OpenRoaming leverages Hotspot 2.0 and enables guest users to roam freely across Wi-Fi and cellular networks. The Wi-Fi connection is secured using industry-standard Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3) protocols and encrypted authentication.

As a retail or other public-access location operator, you can accelerate your guest Wi-Fi attach rate, with the click of a button. The amount of data you can gather about the usage of your physical space can be leveraged with Cisco Spaces, which help you better understand and identify your consumers' behavior patterns. This leads to an improved and engaged experience for your customers at your location while delivering your business outcomes.

This chapter contains the following sections:

Benefits of OpenRoaming

- Simplified Wi-Fi guest access for your customers on site

- Increased Wi-Fi attach rate

- Improved customer onboarding with seamless and secure Wi-Fi connection

- Easy sign-up and network configuration for OpenRoaming through your Cisco Spaces account

- Access to insights and analytics on visitors and customers

- Improved engagement with your customers through Wi-Fi, Cisco Spaces, and your loyalty app

- Reduced operational expenses because of traffic offload from cellular to Wi-Fi networks

Prerequisites for OpenRoaming

To use OpenRoaming through Cisco Spaces, your network must meet the following prerequisites:

- You need an active Cisco Spaces account.

- You need a Cisco wireless network. Both controller-based (Cisco AireOS or Cisco Catalyst wireless controller) and cloud-based (Cisco Meraki) networks are supported.

- You need to add the wireless network to your Cisco Spaces account.

  - For controller-based architecture, the Cisco Spaces Connector must be used. For information on downloading and configuring a Cisco Spaces Connector, see the *Cisco Spaces Connector Configuration Guide*.

  - For Cisco Meraki networks, you need to add the Cisco Meraki account to your Cisco Spaces account.

Configure OpenRoaming

Before you begin

Before proceeding with configuring OpenRoaming for your wireless network, ensure that your network meets the prerequisites described in Prerequisites for OpenRoaming, on page 2. To set up OpenRoaming in Cisco Spaces, click the **OpenRoaming** tile on the Cisco Spaces dashboard. The **OpenRoaming** dashboard is displayed.

Figure 2: Cisco Spaces Dashboard: OpenRoaming Tile
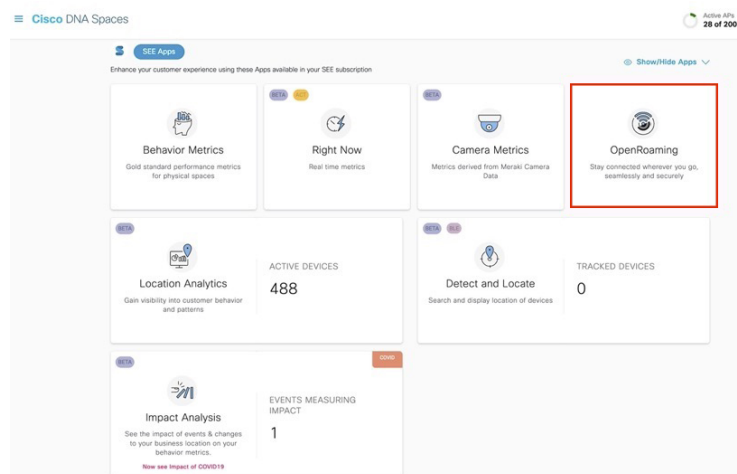
Note   If you have configured OpenRoaming earlier, you will see your OpenRoaming reports in the **OpenRoaming** home page. To view a list of available sample reports, click the **See Sample Dashboard** link provided in the OpenRoaming home page.

To configure OpenRoaming, perform the following tasks:

Step 1   Create an OpenRoaming Profile.

Step 2   Enable a Hotspot on the Cisco Spaces Connector.

Step 3   Configure Network Controller.

Step 4   Test Your OpenRoaming Network.

This chapter contains the following sections:

Create an OpenRoaming Profile

An OpenRoaming profile contains information about the network SSID and specifies which user identities are allowed to access the guest network. You can also configure carrier offload in the OpenRoaming profile. To create an OpenRoaming profile, perform the following tasks:

SUMMARY STEPS

1. Choose an access policy.
2. Configure an SSID.
3. (Optional) Configure carrier offload.
4. Review and confirm the OpenRoaming profile configuration.

DETAILED STEPS

Step 1   Choose an access policy.

a) In the **OpenRoaming** window, click **Set Up OpenRoaming** or ☰ > **Setup**.
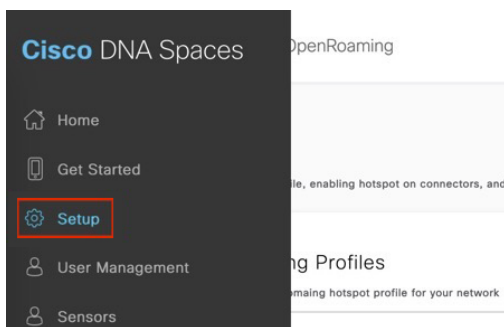
Note   If this is the first time that you are setting up OpenRoaming, when you click ☰ > **Setup**, a **Terms and Conditions** dialog box is displayed. Click **I Agree** to proceed.

The **OpenRoaming Setup** window is displayed.

b) In the **OpenRoaming Profiles** section, click **Create OpenRoaming Profile**.

The **Create an OpenRoaming Profile** configuration wizard is displayed.

c) Click **Proceed**.

d) Under **Access Policy**, specify who can access your OpenRoaming network.

The options available are:

- **Accept all authenticated users**: This is the default option.

- **Accept only users who provide their identity**: An example of an accepted identity is a real identity, such as an email ID.

- **Accept users with specified identity types**: Choose the desired identity types from the list that is displayed. Enable the **Require real identity** knob if you want users to enter their real identities.

  The identity types chosen here is displayed adjacent to their real or anonymous identity settings, in a table next to this list.

- **Accept only your users**: If you choose this option, you will need to be added as an identity provider.

e) Under **Preferred Credentials**, choose the desired option from those listed below by clicking the corresponding radio button:

- **I do not have preferred credentials**

  Note   If you have selected **Accept only your users** in the **Access Policy** section, this option will be disabled.

- **I have preferred credentials, which I want to use**: If you choose this option, you must select a domain from the list of domains that are displayed or click **Add a Custom Domain**.

f) Click **Next**.

The **SSID Details** window is displayed.

Step 2   Configure an SSID.

a) In the **SSID Details** section, enter the SSID name in the corresponding field. This is the SSID that will be broadcast for OpenRoaming.

  Note   If the name that you enter is an existing SSID, ensure that the SSID name is an exact match of what is in the network.

b) (Optional) In the **Advanced** section, you can choose among the following options by clicking the corresponding radio button:

- **Default Status**: Choose between **Enable** or **Disable** by clicking the corresponding radio button. The default option is **Enable**.

- **Fast Transition (802.11r)**: Choose between **Adaptive**, **Enable** or **Disable** by clicking the corresponding radio button. The default option is **Adaptive**.

The **Create an OpenRoaming Profile** configuration wizard is displayed.

c) Click **Next**.

The **Carrier Offload** window is displayed.

Step 3   (Optional) Configure carrier offload.

You can leverage your Wi-Fi network to provide voice and data services to mobile carrier subscribers on your Wi-Fi network. This configuration is optional.

Before you configure carrier offload, ensure that the following prerequisites are in place:

- You must have an existing relationship with a mobile carrier or service provider.

- You must have configured the settlement provider with the mobile carrier or service provider.

a) Use the **Allow Carrier Offload** knob to enable the **Carrier Offload** settings.

A table listing the various carriers, along with their corresponding details such as the **Offloading Partner**, **Static Routing**, **Realms**, and **MNC/MCC** settings, is displayed.

b) Based on your existing relationships with various carriers, you can either select from the carriers that are available in the table or click **Add Custom Carrier** to add carriers of your choice.

Note   If you have not configured a carrier, or if you click **Add Custom Carrier**, you must visit the **DNA Spaces Partner App Center** to first activate the offloading partner. Contact your carrier offloading partner for specific information that has to be entered in the custom fields.

c) Click **Next**.

The **Review Your Configuration** window is displayed.

Step 4   Review and confirm the OpenRoaming profile configuration.

After you have configured the access policy, SSID, and the optional carrier offload, you can review your OpenRoaming profile configuration and modify it if required before saving these settings.

a) In the **Review Your Configuration** window, verify the settings and do one of the following:

Note   By default, the OpenRoaming profile name is the same as the SSID name. You can choose to retain the OpenRoaming profile name as the SSID name or modify the profile name.

- If you are satisfied with the configuration, proceed with 4.b, on page 6.

- If you have to make changes, click the **Edit** link next to the section whose configuration has to be modified and make changes. Continue to click **Next** until you arrive at the **Review Your Configuration** window. On successful modification of the OpenRoaming Profile configuration, proceed with 4.b, on page 6.

b) Click **Done** to complete the creation of the OpenRoaming profile.
A success message appears briefly, and a confirmation window is displayed.

What to do next

If you want to continue the OpenRoaming configuration, click **Continue OR Setup** or close the configuration wizard.

Edit an OpenRoaming Profile

Step 1   On the **OpenRoaming** window, choose ☰ > **Setup**.
The **OpenRoaming Setup** window is displayed.

Step 2   In the **OpenRoaming Profiles** section, in the **Action** column, click the settings ⚙ icon corresponding to the profile that you want to update.

> **Note**   To view the existing configuration for a profile, click the profile name. A window displaying the configuration details for the selected OpenRoaming profile is displayed.

Step 3   Click **Edit Profile**.
The **Edit OpenRoaming Profile** configuration wizard is displayed.

Step 4   Make changes and click **Next**.

Step 5   Follow the prompts till the **Review Your Configuration** window is displayed.

A summary of the OpenRoaming profile modifications you made is displayed.

Step 6   Review the updates and do one of the following:

- If you are satisfied with the updates, go to .

- If you have to make further changes, click the **Edit** link next to the section whose configuration has to be modified and make changes. Continue to click **Next** until you arrive at the **Review Your Configuration** window. To confirm and save the updated OpenRoaming profile configuration, go to .

Step 7   Click **Done**.
A success message is displayed briefly followed by a confirmation window.

Delete an OpenRoaming Profile

Step 1   On the **OpenRoaming** window, choose ☰ > **Setup**.
The **OpenRoaming Setup** window is displayed.

Step 2   In the **OpenRoaming Profiles** section, in the **Action** column, click the settings ⚙ icon corresponding to the profile you want to delete.

Step 3   Click **Delete Profile**.
The **Delete OpenRoaming Profile** configuration wizard is displayed.

Step 4   Click **Done**.
A success message appears briefly, and a confirmation window is displayed.

Enable a Hotspot on the Cisco Spaces Connector

When you add a hotspot on the Cisco Spaces Connector, it leads to the installation of a new docker. You can enable a hotspot on the Cisco Spaces Connector either during the initial configuration of the connector or later using the procedure outlined here. For information on configuring a connector, go to the *Cisco Spaces Connector Configuration Guide*.

If you have already configured a connector, you can see it listed in the **Hotspot-enabled Connectors** section on the **OpenRoaming Setup** window.

| **Note** | You can upgrade the hotspot to the latest version from the **Hotspot** tab in the Cisco Spaces Connector GUI. The upgrade link appears only if a new version is available for upgrade. |

Depending on your wireless network, follow the corresponding procedure to enable a hotspot on a Cisco Spaces Connector after it has been created:

- Enable a Hotspot on the Cisco Spaces Connector (Cisco AireOS or Cisco Catalyst Network), on page 8
- Enable a Hotspot on the Cisco Spaces Connector (Cisco Meraki network), on page 11

Enable a Hotspot on the Cisco Spaces Connector (Cisco AireOS or Cisco Catalyst Network)

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

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

The **OpenRoaming Setup** window is displayed.

A list of all the Cisco Spaces Connectors, along with their status is displayed in the **Hotspot-enabled Connectors** section.

Step 2 Under the **AireOS/Catalyst** tab, click the **Enable Hotspot for Connector(s)** link.

The **OpenRoaming - Add Hotspot** window is displayed.

Step 3 Select the Cisco Spaces Connector for which you want to enable the hotspot and click **Continue**.

A token is generated, and a **Hotspot created successfully** message is displayed. This token is used by the Cisco Spaces Connector to download the hotspot connector container.

Step 4 Under **Token Generated**, click **Copy**.

Paste this token in the **Configure Token** window of the Cisco Spaces Connector GUI. Note that a token can only be used once for a single Cisco Spaces connector.

If a token is used more than once, the hotspot-enabled connector will not work. If the connectors are in active-active mode and share a connector token, you will need different hotspot tokens for each connector.

Step 5 Click **Close**.

Step 6 Refresh the **OpenRoaming Setup** window.

The new hotspot-enabled connector is now displayed in the listing in the **Hotspot-enabled Connectors** section.

View Connector Details (Cisco AireOS or Catalyst Network)

Step 1 On the **OpenRoaming** window, click **Set Up OpenRoaming** or ☰ > **Setup**.

The **OpenRoaming Setup** window is displayed.

A list of all Cisco Spaces Connectors with their status is displayed in the **Hotspot-enabled Connectors** section.

Step 2 Under the **AireOS/Catalyst** tab, click a Connector name.

The **Connector Details** window with details of the Connector's configuration is displayed.

Step 3 Close the window and return to the **OpenRoaming Setup** window.

View Hotspot Token for a Cisco Spaces Connector (Cisco AireOS or Catalyst network)

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

The **OpenRoaming Setup** window is displayed.

A list of all Connectors, along with their status, is displayed in the **Hotspot-enabled Connectors** section.

Step 2 Under the **AireOS/Catalyst** tab, click the settings ⚙ icon in the **Action** column corresponding to the connector you want to update.

Step 3 Click **View Token**.
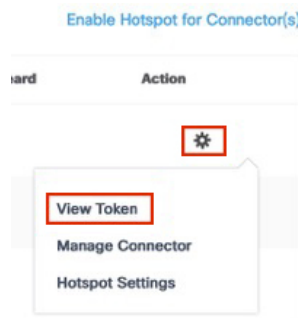
The **OpenRoaming – View Token** window is displayed.

Step 4   Click **Copy** to use the token for a Connector setup.

Step 5   In the Cisco Spaces Connector GUI, paste this token in the **Configure Token** window.

> **Note**   After the token is saved, the hotspot information is downloaded to the Connector. After you refresh the window, you will find a **Hotspot** tab next to the **Connector** tab. In the **Hotspot** tab, verify the status of the hotspot-enabled Connector. If the status is Running●, it indicates that the OpenRoaming hotspot has been successfully enabled for the Cisco Spaces Connector.

Step 6   Click **Close** to return to the **OpenRoaming Setup** window.

## Manage Connector (Cisco AireOS or Cisco Catalyst Network)

Step 1   On the **OpenRoaming** window, click **Set Up OpenRoaming** or ☰ > **Setup**.

The **OpenRoaming Setup** windows is displayed. A list of all Connectors, along with their status, is displayed in the **Hotspot-enabled Connectors** section.

Step 2   Under the **AireOS/Catalyst** tab, click the settings ✷ icon in the **Action** column corresponding to the connector you want to update.

Step 3   Click **Manage Connector**.
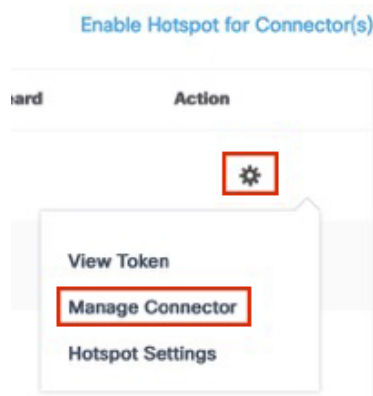
The **Manage Connector** window is displayed.

Step 4   Choose an action from the following options:

- **Restart connector**

- **Upload logs to cloud**

- **Enable connector debug mode**

- **Enable Hotspot debug mode**

- **Automatically keep this connector up to date**

Step 5   Close the window and return to the **OpenRoaming Setup** window.

Enable a Hotspot on the Cisco Spaces Connector (Cisco Meraki network)

Before you begin

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

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

The **OpenRoaming Setup** window is displayed.

A list of all the Cisco Spaces Connectors, along with their status is displayed in the **Hotspot-enabled Connectors** section.

Step 2   Under the **Meraki API** tab, click the **Set Up** link.

For information on configuring your Cisco Meraki setup, see the *Cisco Spaces Configuration Guide*.
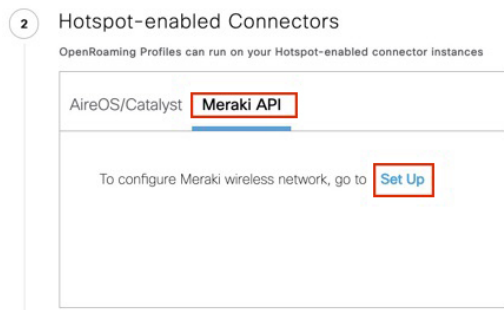
Step 3   Select the Cisco Spaces Connector for which you want to enable the hotspot.

Step 4   If you have a Meraki connector, click the **Meraki API** tab.
The **Configure OpenRoaming for Meraki** configuration wizard is displayed.

Step 5   Click **Next**.

Step 6   Choose the organization from the drop-down list.
A list of Meraki networks for the selected organization is displayed.

Step 7   Choose the Meraki network for which you want to configure OpenRoaming.

Step 8   Choose the OpenRoaming profile that you would like to apply for the selected Meraki networks.

Step 9   Click **Configure** to complete configuration.

A success message is displayed. Refresh the **OpenRoaming Setup** page.

A message is displayed under the **Meraki API** tab confirming your Cisco Meraki account is connected.

Configure Network Controller

Depending on your wireless network, follow the corresponding procedure to associate an OpenRoaming profile with the controller and configure the network:

Configure Cisco AireOS or Cisco Catalyst Network

Before you begin

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.

Configure Cisco Meraki Network

Before you begin

To use OpenRoaming on your Cisco Meraki network through Cisco Spaces, your network must meet the following prerequisites:

- All access points in the Cisco Meraki network need to be on R28.x or later versions of the Cisco Meraki firmware.

- There needs to be at least one unconfigured SSID and it should be disabled.

- Contact the Cisco Meraki support team to activate OpenRoaming on your network.

Note
- If you do not meet one or more of the above prerequisites, you can manually activate OpenRoaming on your Meraki network by installing a Cisco Spaces Connector. For more information, see the *Cisco Spaces Setup Guide for OpenRoaming*.

- Configuration of Cisco Meraki networks that use templates is not supported.

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

Step 2 In the **Network configuration** section, click the **Meraki Networks** tab.

Step 3 Click **Set Up**.

The **Configure OpenRoaming for Meraki** window is displayed.
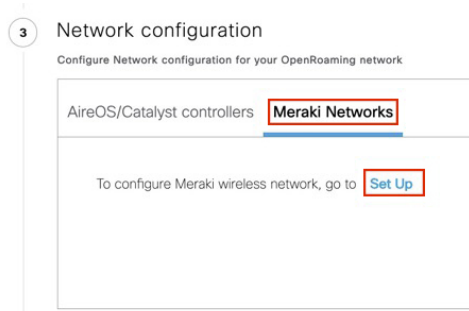
Note For information on configuring a Cisco Meraki network, go to the *Cisco Spaces Configuration Guide*.

Step 4 Choose an organization from the drop-down list.

Step 5 Click **Next**.

Step 6 Choose the Cisco Meraki networks for which you want to enable OpenRoaming.

> **Note** You can select multiple networks from the list.

Step 7 Click **Next**.

Step 8 From the drop-down list, select the OpenRoaming profile that needs to be applied on the Cisco Meraki network.

Step 9 Click **Next**.

Step 10 Review the **Configuration Summary**.

If you would like to make any changes, click **Back** to navigate to the previous windows.

Step 11 Click **Configure** to complete configuration of the OpenRoaming profile on the chosen Cisco Meraki networks. The **OpenRoaming Setup** page appears with a success message. Under the **Meraki Networks** tab, a confirmation message is displayed along with the count of Cisco Meraki networks configured with OpenRoaming profiles.

Edit Cisco Meraki Network

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

The **OpenRoaming Setup** window is displayed.

> **Note** Click **OpenRoaming Activation Status** to view the status of the configured Cisco Meraki networks.

Step 2 In the **Network configuration** section, click the **Meraki Networks** tab.

Step 3 Click the SSID corresponding to the Cisco Meraki network that you would like to update.

The **Edit Configuration** window is displayed.

Step 4 Click **Update** after making the needed updates.

The **OpenRoaming Setup** window is displayed with a success message.

Test Your OpenRoaming Network

You can test your OpenRoaming network configuration through the following methods:

Procedure

- **Cloud/Social**: To use this method, download the OpenRoaming mobile app from the iOS App Store or Google Play Store to your mobile device.
- **Device Manufacturer**: Use this method to test your OpenRoaming network natively on a Samsung or Google mobile device.
- **Other Methods**: In addition to the above two methods, you can also test your OpenRoaming network using the following two options:

> • **Carrier Offload**: If you have set up a Carrier Offload solution, a mobile phone from the supported carrier will automatically get attached to your OpenRoaming network.
>
> • **Cisco Spaces SDK**: If you have integrated your brand's mobile app with Cisco Spaces SDK, a mobile phone with your mobile app will automatically get attached to your OpenRoaming network.

For more information about Cisco Spaces SDK, see https://developer.cisco.com/docs/dna-spaces-sdk/. Log in using your Cisco credentials, if prompted.

View OpenRoaming Reports

To view your OpenRoaming reports, click ☰ > **Home**.

The following reports are available in the **OpenRoaming** dashboard:

- **Unique Devices**
- **Devices by IDP**
- **Devices by Manufacturer**
- **Data Usage**
- **Average Visit Duration**
- **Data Consumed per User**
- **Connections per Day**
- **Connections per Hour**

Related Documents

For more information about OpenRoaming in a Cisco Spaces setup, see the following documents:

- *Cisco Spaces OpenRoaming Setup Guide*
- *Cisco Spaces Connector Configuration Guide*
- *Cisco Spaces Configuration Guide*

For all Cisco Spaces documentation, see:

https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html

Cisco Support Community

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Join the forum at: https://supportforums.cisco.com/index.jspa .

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.