

Cisco Spaces: OpenRoaming Configuration Guide

First Published: 2026-09-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Cisco Spaces: OpenRoaming App** 1

Configure OpenRoaming 1

Deployment flow by platform 2

Create an OpenRoaming profile 3

Edit an OpenRoaming profile 5

Delete an OpenRoaming profile 6

CHAPTER 2 **Prepare Platform Integration** 7

Prepare Platform Integration 7

Controller-Based Deployments: Enable Hotspot on Cisco Spaces Connector 7

Verify hotspot-enabled connector 8

Controller-Based Deployments: View Connector Details 10

Controller-Based Deployments: View Hotspot Token 10

Controller-Based Deployments: Manage Connector 11

Meraki Deployments: Validate Meraki API Integration 12

CHAPTER 3 **Carrier Offload** 15

Carrier Offload 15

OpenRoaming Carrier Offload 16

Setup an AT&T account 17

Activate AT&T 20

Setup a T-Mobile Account 23

Activate T-Mobile 26

CHAPTER 4 **Configure Wireless Network** 29

Configure Wireless Network 29

Controller-Based Deployments: Configure Catalyst 9800 and AireOS 29

Apply Catalyst 9800 and AireOS CLI configuration 30

Configure Cisco Meraki Network 31

Review Cisco Meraki network configuration 32

Edit Cisco Meraki network 33

CHAPTER 5 **Check OpenRoaming Activation** 35

Check OpenRoaming Activation 35

CHAPTER 6 **Test your OpenRoaming network** 37

Test your OpenRoaming network 37

OpenRoaming client matrix 37

CHAPTER 7 **View OpenRoaming Reports** 39

View OpenRoaming reports 39

CHAPTER 8 **OpenRoaming firewall rules** 41

OpenRoaming firewall rules 41

Meraki RadSec IP allowlist 42

Domains to allowlist 42

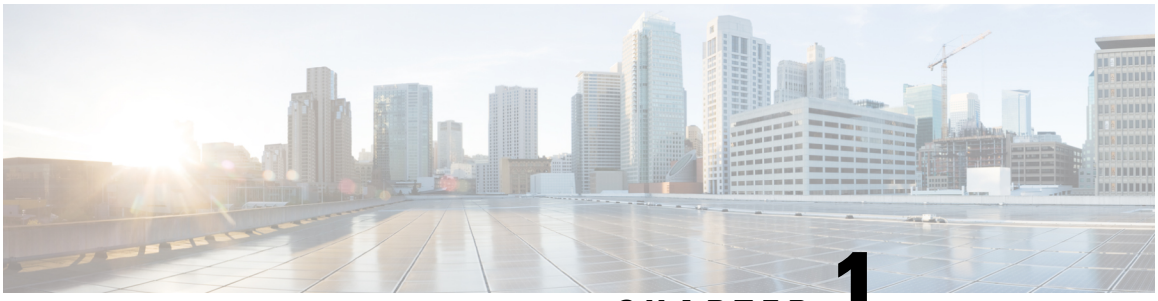
Carrier offload domain allowlist 43

CHAPTER 9 **Monitoring** 45

Monitoring 45

View OpenRoaming monitoring data 46

OpenRoaming monitoring data 47



CHAPTER 1

Cisco Spaces: OpenRoaming App

- Configure OpenRoaming, on page 1
- Deployment flow by platform, on page 2
- Create an OpenRoaming profile, on page 3
- Edit an OpenRoaming profile, on page 5
- Delete an OpenRoaming profile, on page 6

Configure OpenRoaming

Cisco Spaces: OpenRoaming Configuration Guide

Before you begin

Complete the prerequisites in this section before configuring OpenRoaming. To open the OpenRoaming app in Cisco Spaces, click the OpenRoaming tile on the Cisco Spaces dashboard.

Access and account readiness:

- Open OpenRoaming from **Cisco Spaces Home** > **Visitor Onboarding & Experience OpenRoaming**, or from **Feature Apps** > **OpenRoaming** > **Open App**.
- During first-time setup, the **Terms and Conditions** dialog appears when Setup is opened. Click **I Agree** to open the **OpenRoaming Setup** window.
- If OpenRoaming was configured earlier, the OpenRoaming app opens the home or reports page. If Terms and Conditions were accepted but setup is incomplete, the app opens the Get Started page.
- Confirm that the Cisco Spaces account is active and that the target wireless network is added to Cisco Spaces before starting OpenRoaming configuration.

Deployment and connectivity readiness:

- For controller-based deployments, confirm Cisco Spaces Connector is deployed and associated with the Catalyst 9800 or AireOS controller.
- For Meraki deployments, confirm the Cisco Meraki account is added to Cisco Spaces and the admin has read/write access in Meraki Dashboard.

- Confirm the administrator has read/write permissions in Cisco Spaces for OpenRoaming and Cisco Spaces, read/write access to the target Meraki Dashboard or WLC, and read access to the connector for verification.
- The Cisco Spaces Connector, controller, Meraki APs, and Meraki API path must reach Cisco Spaces and OpenRoaming services.
- If the deployment uses a firewall, DNS security service, proxy, or SSL inspection device, allowlist the required domains, ports, and Meraki RadSec HAProxy IP destinations before configuration.
- Bypass TLS inspection and proxy authentication for OpenRoaming service traffic.

Deployment flow by platform

Summary

Use the workflow that matches the wireless platform. Profile creation is common to all deployments. Activation and network configuration differ between controller-based and Meraki deployments.

Workflow

These stages describe the deployment flow by platform.

1. **Catalyst 9800 and AireOS Flow**
   - Create the OpenRoaming profile in Cisco Spaces.
   - Enable Hotspot service on the Cisco Spaces Connector and configure the hotspot token.
   - Confirm the connector hotspot status is Running and that the controller is visible in Cisco Spaces.
   - Generate the Catalyst 9800 or AireOS CLI configuration from Cisco Spaces.
   - Review and apply the generated CLI on the controller. For Catalyst 9800, select the Catalyst version option that matches the controller IOS XE release before copying the configuration.
   - Check OpenRoaming activation, then test with a supported client.
2. **Cisco Meraki Flow**
   - Create the OpenRoaming profile in Cisco Spaces with a new unique SSID name.
   - Validate that the Meraki API integration is connected and active in Cisco Spaces.
   - Select the Meraki organization and Meraki networks, then apply the OpenRoaming profile.
   - In the Meraki Dashboard, confirm that the SSID exists and is enabled with RADIUS, WPA2 or WPA3 encryption, no splash page, and Hotspot 2.0 enabled.
   - Check OpenRoaming activation, Meraki clients, and **Meraki Organization** > **Monitor** > **Change Log**, then test with a supported client.

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.

Before you begin

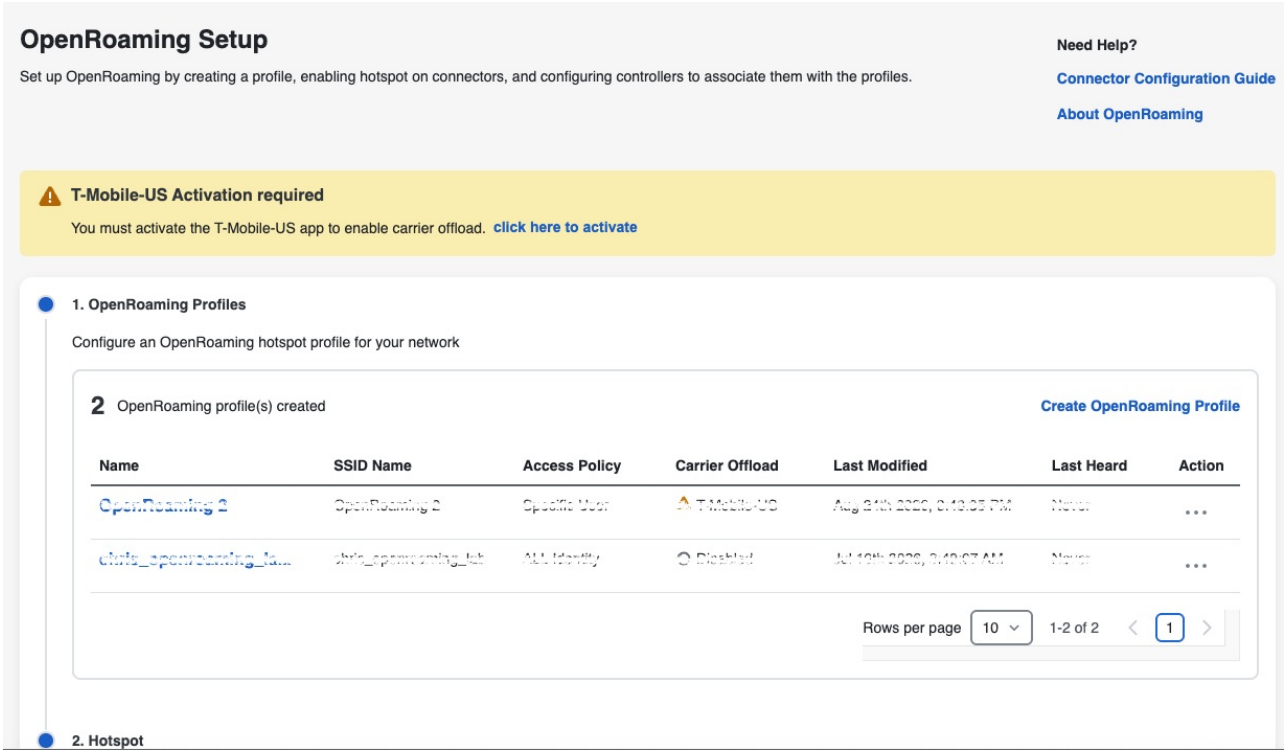
Before creating the profile, confirm SSID naming, access policy, identity requirements, carrier-offload scope, and firewall/domain readiness.

Procedure

Step 1 Choose an access policy.

a. On the **OpenRoaming** window, choose **Setup**. The **OpenRoaming Setup** window is displayed.

Figure 1: OpenRoaming Setup



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.

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

- **Accept only users who provide their identity**: Use when real identity such as an email ID is required.
- **Accept users with specified identity types**: Choose the desired identity types and enable Require real identity if needed.
- **Accept only your users**: Use only when the customer identity provider integration is ready.

e. Under **Preferred Credentials**, specify who can access your OpenRoaming.

- **I do not have preferred credentials**: This is the default option.
- **I have preferred credentials, which I want to use**: Select a domain from the drop-down list, click **Add**.

f. Click **Continue**. The **SSID Details** window is displayed.

Step 2 Configure an SSID.

a. In the **SSID Details** section, enter the SSID name. This is the secure SSID that will be broadcast for OpenRoaming and should be separate from captive-portal guest SSIDs.

b. In the **Advanced** section, choose Default Status as **Enable** or **Disable**. The default option is Enable.

c. For Fast Transition (802.11r), choose **Adaptive, Enable,** or **Disable**. The default option is Adaptive.

d. Click **Continue**. The **Carrier Offload** window is displayed.

Step 3 (Optional) Configure carrier offload.

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

b. Select from the available carriers.

Carrier offload enables mobile carrier subscribers to use the OpenRoaming SSID for carrier-integrated voice and data services. This configuration is optional.

Before configuring carrier offload, confirm the following prerequisites:

- You must have an existing relationship with a mobile carrier or service provider.
- The settlement provider must already be configured with the mobile carrier or service provider.
- Required carrier offload domains must be allowlisted if the customer enables carrier offload.

For more information, refer to the Carrier Offload Activation.

Step 4 Click **Continue**. The **Review your Configuration** window is displayed.

Step 5 Review and confirm the OpenRoaming profile configuration.

a. In the **Review Your Configuration** window, verify the access policy and SSID details.

b. If the configuration is correct, click **Done**. A success message appears briefly, and a confirmation window is displayed.

c. Confirm that the profile appears in the OpenRoaming Profiles section and that the access policy, SSID, and carrier-offload settings match the intended deployment.

Step 6 Click **Continue OR setup** to return to OpenRoaming Setup window.

Note Profile and SSID notes:

- If Accept only your users is selected, I do not have preferred credentials is disabled. Confirm IdP readiness before selecting this policy.
- For Catalyst and AireOS deployments, if the name entered is an existing SSID, ensure that the SSID name is an exact match of what is in the network.
- SSID broadcast must remain enabled.
- For Meraki deployments, use a new unique SSID name and ensure that an unused disabled SSID is available before applying the OpenRoaming profile.
- Use Adaptive for 802.11r unless another setting has been validated for the target client mix. Enable allows all clients to use Fast Transition, including clients that do not support it. Adaptive enables Fast Transition only for capable clients; other clients fall back to regular reauthentication.

Carrier offload notes:

- Partner App activation support in OpenRoaming is available for AT&T and T-Mobile. Partner App activation is required before associating a carrier-enabled OpenRoaming profile to a newly onboarded controller or Meraki network.
- If the required Partner App is not activated, Cisco Spaces does not allow the carrier-enabled profile to be configured on the newly onboarded network.

Edit an OpenRoaming profile

Procedure

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

Step 2 (Optional) To view the existing configuration, click the profile name.

Step 3 In the **OpenRoaming Profiles** section, click the three-dot icon for the profile that you want to update.

Step 4 Click **Edit profile**.

Step 5 Make changes and click **Continue** until the **Review your Configuration** window is displayed.

Step 6 Review the updates. If the changes are correct, click **Done**.

Step 7 Before editing a production profile, confirm the impact on assigned controllers, Meraki networks, carrier offload, and identity policy. Use a change window for production updates.

Delete an OpenRoaming profile

Procedure

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

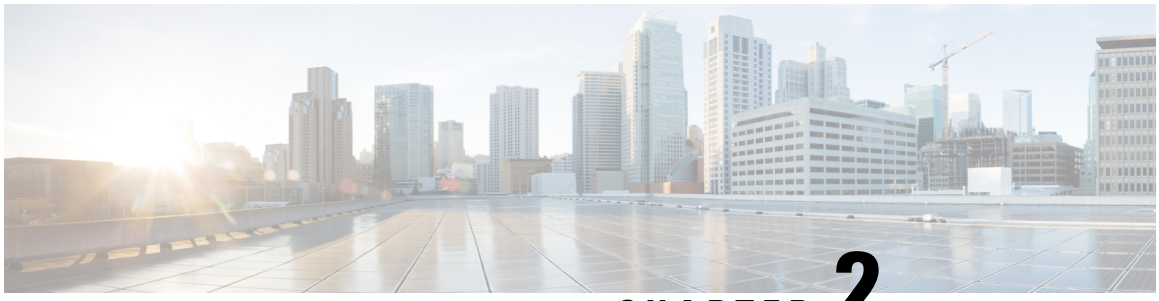
Step 2 In the **OpenRoaming Profiles** section, click the three-dot icon for the profile you want to delete.

Step 3 Click **Delete profile**.
A warning window is displayed.

Step 4 Click **Delete**.



Note Do not delete a profile that is still assigned to a controller or Meraki network unless rollback and customer impact are understood.



CHAPTER 2

Prepare Platform Integration

- Prepare Platform Integration, on page 7
- Controller-Based Deployments: Enable Hotspot on Cisco Spaces Connector, on page 7
- Controller-Based Deployments: View Connector Details, on page 10
- Controller-Based Deployments: View Hotspot Token, on page 10
- Controller-Based Deployments: Manage Connector, on page 11
- Meraki Deployments: Validate Meraki API Integration, on page 12

Prepare Platform Integration

Controller-based deployments and Meraki deployments use different activation paths. For Catalyst 9800 and AireOS networks, enable the Hotspot service on the Cisco Spaces Connector. For standard Meraki API deployments, OpenRoaming activation is handled through Meraki API integration; a Hotspot Connector is not required unless Cisco Support directs a connector-based Meraki activation.

Note

- The Cisco Spaces Connector requires direct outbound access to Cisco Spaces and OpenRoaming services.
- If the connector path crosses a firewall, DNS security service, proxy, or SSL inspection device, allowlist the required domains and ports in the OpenRoaming Firewall Rules section.
- Bypass TLS inspection or proxy authentication before enabling the hotspot service.

Controller-Based Deployments: Enable Hotspot on Cisco Spaces Connector

Before you begin

Controller, connector, and access point prerequisites:

- Catalyst 9800 WLC requires IOS XE 16.12.1 or later and a Cisco Spaces Connector.
- AireOS WLC requires AireOS 8.10.x and a Cisco Spaces Connector. AireOS 8.9, 8.8, 8.7, and earlier releases are EoL/EoS and are not supported for OpenRoaming.

- Deploy and activate Cisco Spaces Connector. Version 3.x is highly recommended for new deployments. Minimum supported version is 2.3.2 or above.
- Supported APs include all 9100 Series Access Points and Catalyst Wave 1 and Wave 2 Access Points.
- Review the WLC release notes to confirm AP support for the target controller release.

Unsupported deployment and connectivity prerequisites:

- Embedded Wireless Controller (EWC) on Catalyst 9100 and Embedded Wireless on Catalyst 9000 switches are not supported.
- CMX Tethering is not supported.
- Confirm that Hotspot Service is added to the connector.
- Configure and test connectivity between the connector and the wireless controller.
- Validate connector internet access or firewall/proxy allowlisting.
- HTTP/HTTPS proxy configuration on the Cisco Spaces Connector is not supported for the OpenRoaming hotspot path. Use the firewall allowlist and direct outbound access model described in OpenRoaming Firewall Rules.

Procedure

Step 1 In Cisco Spaces, go to **Setup** > **Wireless Networks**.

Step 2 In the **Connect your wireless network** flow, open the connector list and select the required Connector 3.x.

Step 3 Add Hotspot Service to the connector if it is not already enabled. Cisco Spaces adds the service-manager service by default.

Step 4 In the Connector GUI, configure the hotspot service token.

Step 5 Configure and test controller connectivity for the applicable controller type.

Step 6 After the hotspot service and controller connectivity are configured, return to **OpenRoaming** > **Setup**.

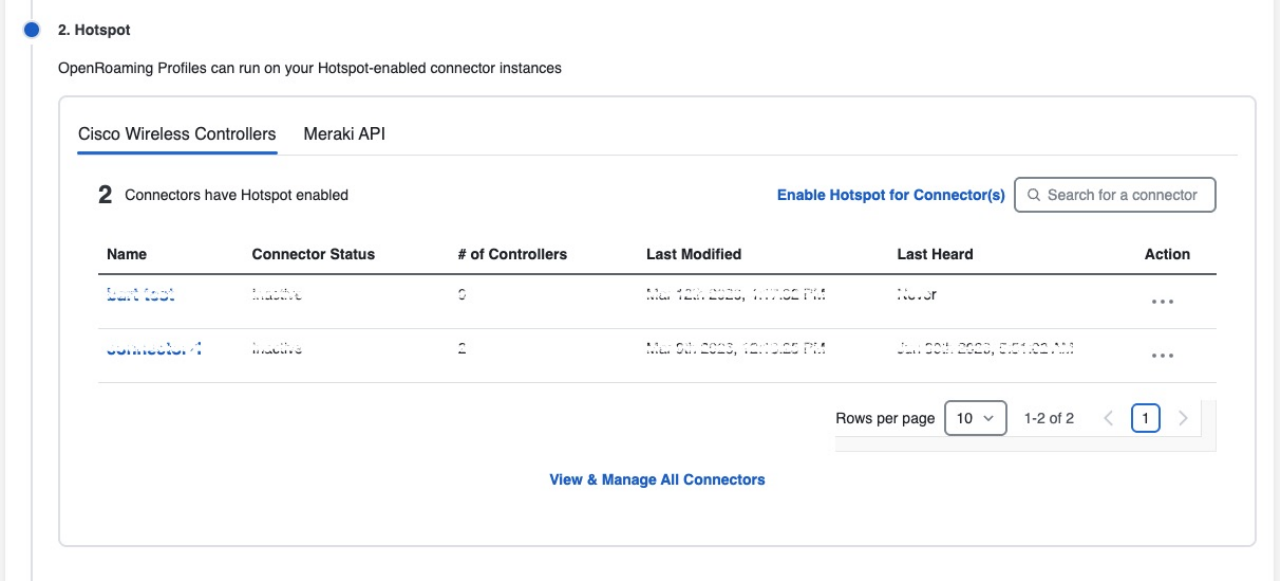
Verify hotspot-enabled connector

Continue this task after the hotspot service and controller connectivity are configured, and after returning to **OpenRoaming** > **Setup**.

Procedure

Step 1 In Section 2, **Hotspot-enabled Connectors**, verify that the connector is listed.

Figure 2: Hotspot-enabled Connectors



Step 2 In Section 3, verify that the associated controllers are displayed.

Step 3 In the **Connector Status** column, confirm that the status is **Running**. If status is not Running, check DNS, firewall or proxy logs, connector token, connector services, and controller reachability.

Note

- Starting December 2023, Connector 2.x entered software maintenance mode. Security updates continue through June 2024 and support for critical bug fixes continues through October 2024.
- Adding Hotspot Service installs the OpenRoaming hotspot container on the Cisco Spaces Connector.
- If the selected connector is already hotspot enabled, continue to the wireless network configuration section.
- Each hotspot token is intended for one Cisco Spaces Connector.
- For active-active or HA connector deployments, generate and configure a separate hotspot token for each connector.
- Reusing the same hotspot token on multiple connectors can prevent the hotspot-enabled connector from working.
- After the token is saved, the connector downloads and installs the Hotspot Connector image. Refresh the OpenRoaming Setup window before validating connector status.

Controller-Based Deployments: View Connector Details

Procedure

Step 1 On the **OpenRoaming** window, choose **Setup**.

Step 2 In **Hotspot-enabled Connectors** section, click **View & Manage All Connectors**.

Step 3 Under the **Cisco Wireless Controllers** tab, click a Connector name.

Step 4 Review Connector Details, then close the window and return to **OpenRoaming Setup**.

Controller-Based Deployments: View Hotspot Token

Procedure

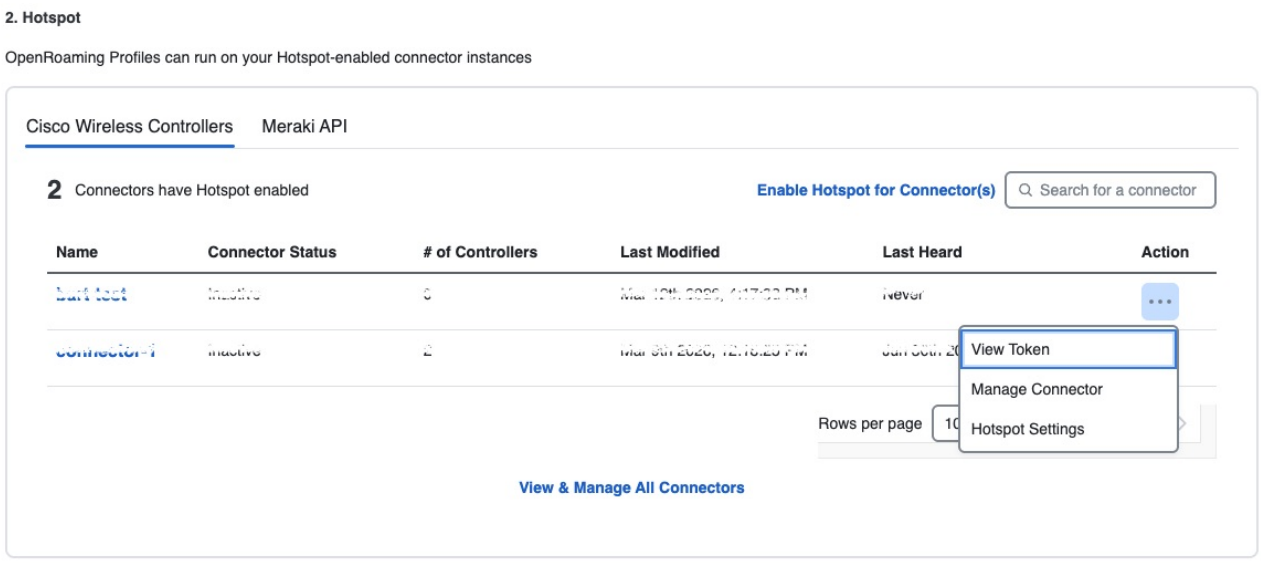
Step 1 On the **OpenRoaming** window, choose **Setup**.

Step 2 In **Hotspot-enabled Connectors** section.

Step 3 Under the **Cisco Wireless Controllers** tab, click the three-dot icon in the **Action** column for the connector.

Step 4 Click **View Token**.

Figure 3: View Token



Step 5 Click **Copy** to use the token for Connector setup.

Step 6 In the Cisco Spaces Connector GUI, paste this token in the Configure Token window.

Note

- After the token is saved, hotspot information is downloaded to the Connector.
- Refresh the window and verify that the Hotspot tab is present and status is Running.

Controller-Based Deployments: Manage Connector

Procedure

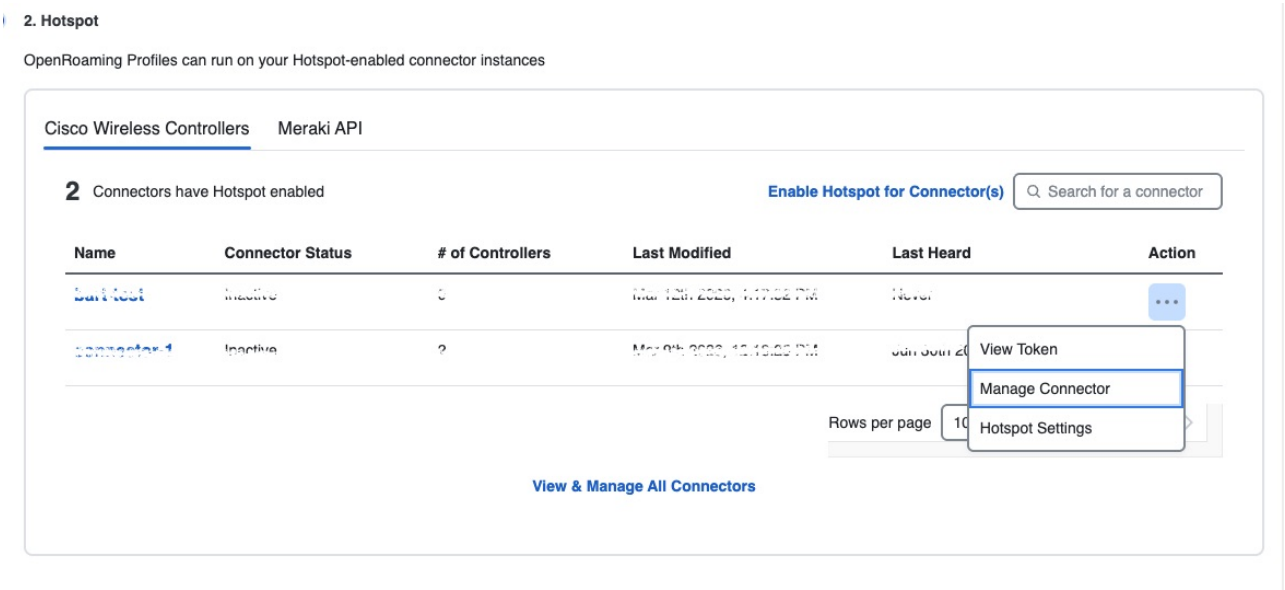
Step 1 On the **OpenRoaming** window, choose **Setup**.

Step 2 In **Hotspot-enabled Connectors** section, Click **View & Manage All Connectors**.

Step 3 Under the **Cisco Wireless Controllers** tab, click the three-dot icon in the **Action** column for the connector.

Step 4 Click **Manage Connector**.

Figure 4: Manage Connector



Step 5 Choose the required action: **Restart connector, Upload logs to cloud, Enable connector debug mode, Enable Hotspot debug mode**, or Automatically keep this connector up to date.

Note

- If the Connector Hotspot service must use specific DNS resolvers, click the three-dot icon for the connector and open Hotspot Settings. Add the required DNS server IP address.
- Dedicated DNS resolver configuration is optional and applies only when required for the connector/hotspot path.
- When a new hotspot container version is available, the connector displays the update in the Connector UI.
- Hotspot container updates do not require token reconfiguration. The connector downloads the new image, stops the old container, and starts the new container.
- Use debug mode during troubleshooting and disable it when no longer required.
- Collect logs before restarting a connector during an active issue.

Meraki Deployments: Validate Meraki API Integration

For Meraki deployments, Cisco Spaces uses Meraki API integration to discover organizations and networks before applying an OpenRoaming profile. Use this section to establish or verify the Meraki API connection. Assign the OpenRoaming profile in Configure Cisco Meraki Network.

Before you begin

- Use a Meraki administrator account with API permissions for the target organization.
- Confirm that Cisco Spaces can reach the Meraki API path through the customer firewall, proxy, or DNS security controls.
- For Meraki deployments, ensure the Meraki APs can reach the OpenRoaming RadSec endpoints over TCP 2083 as described in OpenRoaming Firewall Rules.
- Do not apply an OpenRoaming profile in this section. Profile assignment is covered in Configure Cisco Meraki Network.

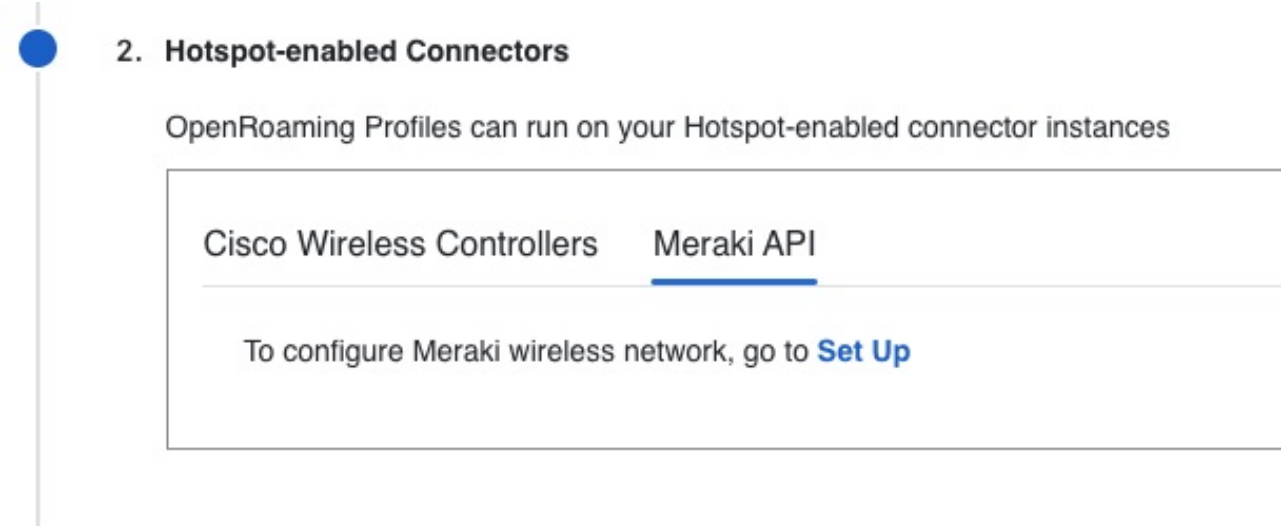
Procedure

Step 1 On the **OpenRoaming** window, choose **Setup**.

Step 2 In **Hotspot-enabled Connectors** section, click **Meraki API** tab.

Step 3 Under the **Meraki API** tab, click **Set Up** link.

Figure 5: Meraki API

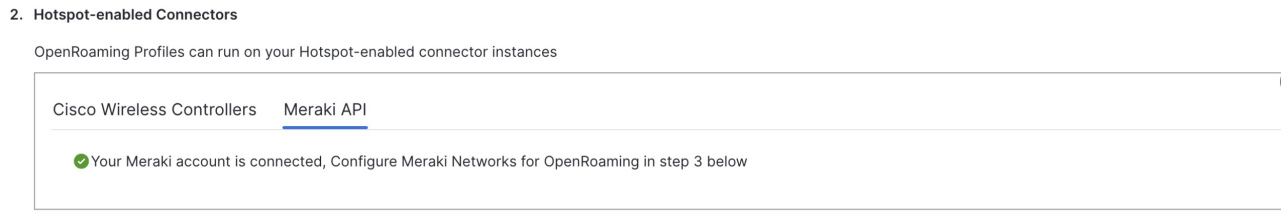


Step 4 Complete the Meraki account authorization prompts and select the required organization when prompted.

Step 5 Click **Next** to complete the Meraki API connection.

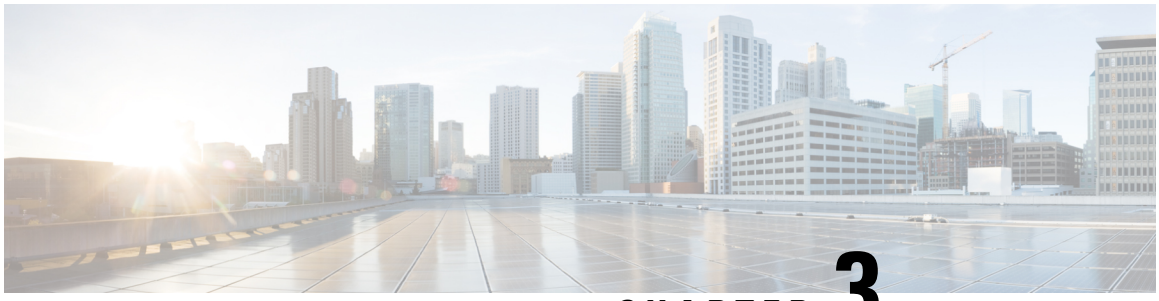
Step 6 Refresh the OpenRoaming Setup page and confirm that the Meraki API tab shows the Cisco Meraki account as connected.

Figure 6:



Note

- A green status indicator in the Meraki API tab confirms that the Meraki API connection is active.
- If the tab displays Set Up, complete the Meraki integration before configuring the Meraki network for OpenRoaming.
- Continue to Configure Cisco Meraki Network only after the account connection is active.



CHAPTER 3

Carrier Offload

Outlines the process for activating Carrier Offload with AT&T, including prerequisites, configuration steps, and troubleshooting procedures to ensure successful service deployment and reliable connectivity within your network environment.

- Carrier Offload, on page 15
- OpenRoaming Carrier Offload, on page 16
- Setup an AT&T account, on page 17
- Activate AT&T, on page 20
- Setup a T-Mobile Account, on page 23
- Activate T-Mobile, on page 26

Carrier Offload

Carrier offload enables supported mobile carrier subscribers to connect automatically to an OpenRoaming wireless network. The AT&T Auto-Attach and T-Mobile Auto-Attach Partner Apps in Cisco Spaces provide the carrier-specific onboarding and activation workflows required to enable carrier offload at approved locations.

The Partner Apps perform these functions:

- Automate the onboarding process between the customer access network and the mobile carrier, including the request to establish a carrier-offload agreement.
- Share supported service-level and network-health telemetry with the carrier through the Cisco Spaces Meta API so that the carrier can monitor the subscriber experience on the access network.

Before the Partner App can be activated, the carrier reviews the proposed locations and confirms that the access network meets its service requirements. The carrier also completes the applicable agreement and provides the credentials required to activate the application.

The account and activation process differs by carrier:

- AT&T provides a token after approving the customer account and locations.
- T-Mobile provides account credentials and requires the applicable tenant or account name during activation.

OpenRoaming Carrier Offload

Partner App activation does not replace OpenRoaming configuration. Configure and activate the OpenRoaming profile and wireless network before enabling the Auto-Attach Partner App.

Activate the Partner App only for locations that the carrier has reviewed and approved. Cisco Spaces shares the required network information for the selected locations with the carrier after the user grants the requested permissions.

Partner App activation is required before a carrier-enabled OpenRoaming profile can be associated with a newly onboarded controller or Cisco Meraki network.

The carrier-offload workflow consists of these stages:

- Configure an OpenRoaming profile for carrier offload.
- Configure the OpenRoaming wireless network and verify its activation.
- Submit an account request through the required carrier Partner App.
- Complete the carrier review and agreement process.
- Obtain the token or account credentials from the carrier.
- Grant Partner App permissions and select the carrier-approved locations.
- Authenticate to the carrier portal and complete activation.
- Confirm that the Partner App is active before applying the carrier-enabled OpenRoaming profile to a newly onboarded network.

Before you begin

Before configuring an Auto-Attach Partner App, verify the these requirements:

- The Cisco Spaces account is active, and you have administrator permissions to activate Partner Apps.
- The OpenRoaming app is enabled.
- An OpenRoaming profile is configured for carrier offload.
- The OpenRoaming wireless network is configured and its activation status is verified.
- The applicable locations are available in the Cisco Spaces location hierarchy.
- The required OpenRoaming and carrier-offload domains, addresses, and ports are allowed through the customer firewall.
- You are authorized to accept the Partner App terms and share the required location and network-health information with the carrier.
- You have the business and technical contact information required by the carrier.

Setup an AT&T account

Submit a request to AT&T to establish an Auto-Attach account and obtain the token required for application activation.

Before you begin

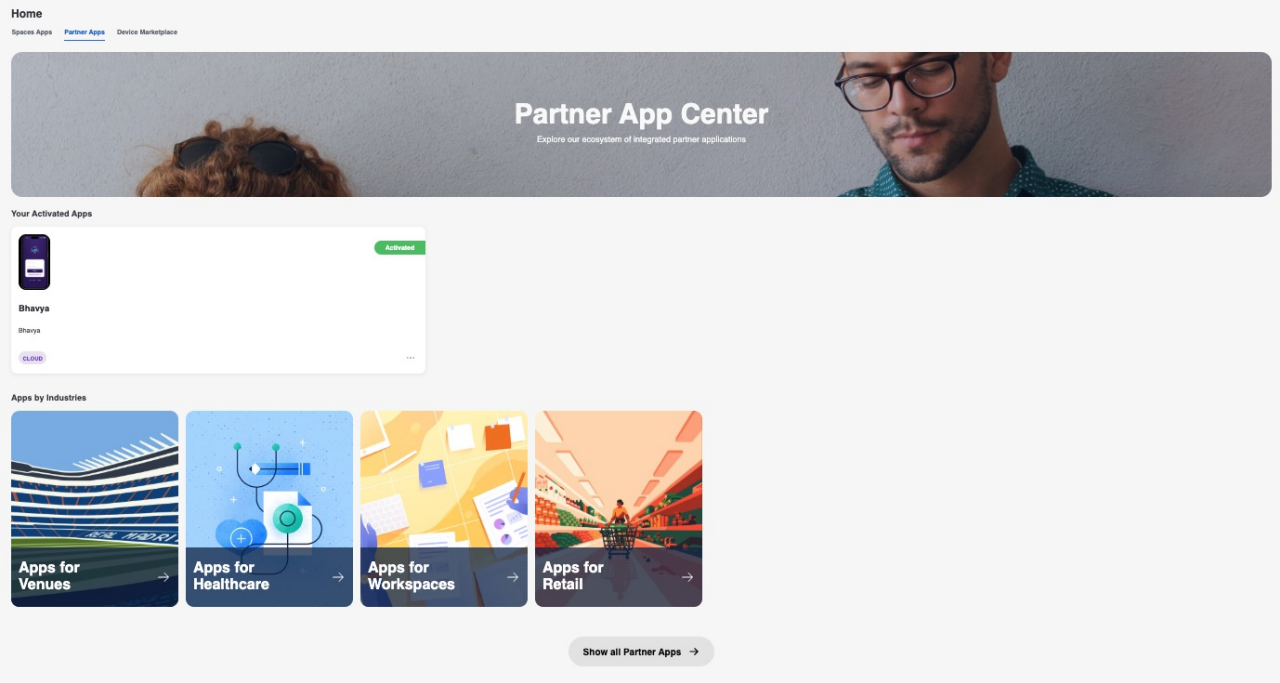
- Complete the carrier-offload prerequisites described in this chapter.
- Identify the locations where AT&T carrier offload will be enabled.
- Identify a business and technical contact who can work with AT&T during the location review and agreement process.

Note AT&T approval is external to Cisco Spaces. AT&T Auto-Attach activation cannot be completed until AT&T approves the account and locations and provides the required token.

Procedure

Step 1 Log in to Cisco Spaces.

Figure 7:



Step 2 Click the **Partner Apps** tab.

Step 3 Click **Show all Partner Apps**.

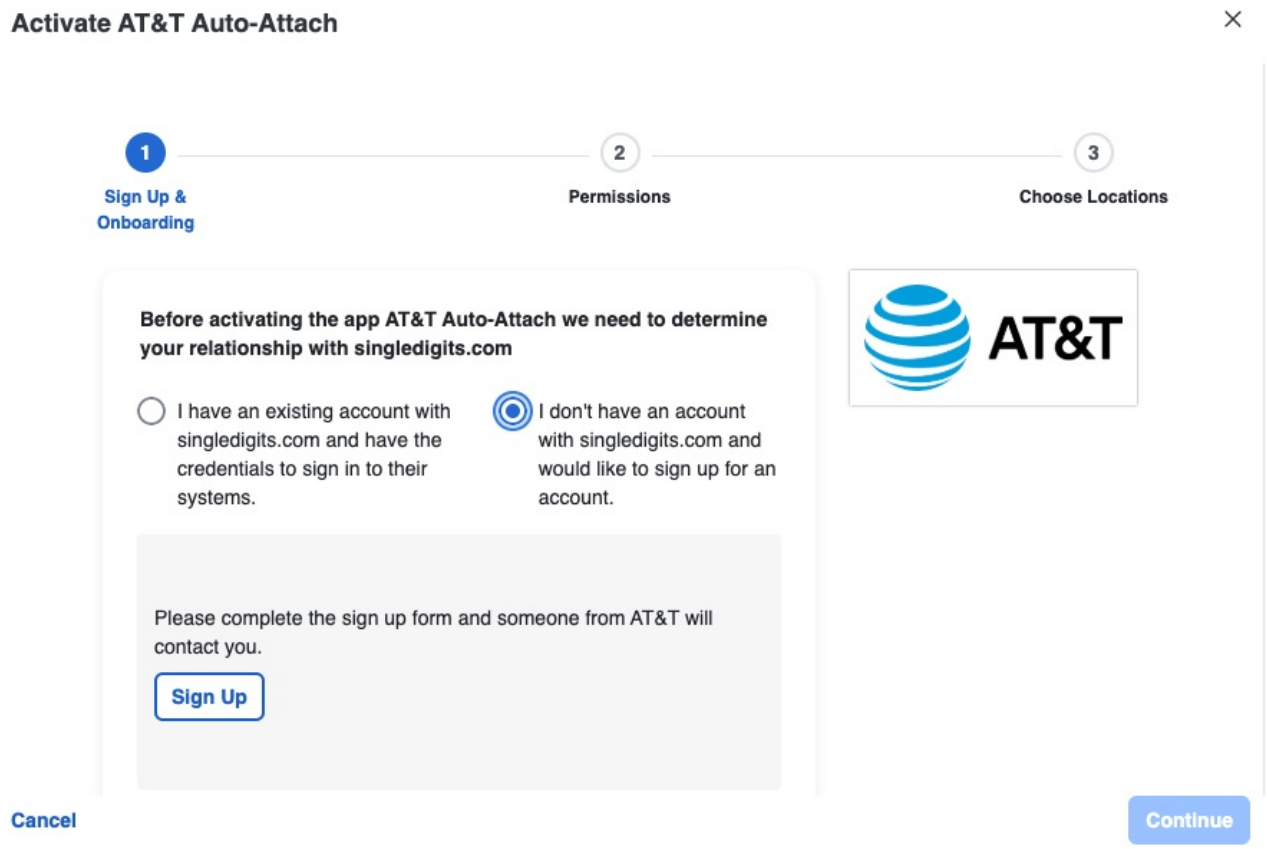
Step 4 Click **AT&T Auto-Attach**.
The **AT&T Auto-Attach** slide-panel appear.

Step 5 Click **Activate**.

Step 6 Review and accept the **Terms & Conditions**.
The account selection options appears.

Step 7 In the **Sign Up & Onboatding** section, choose the option to new account.

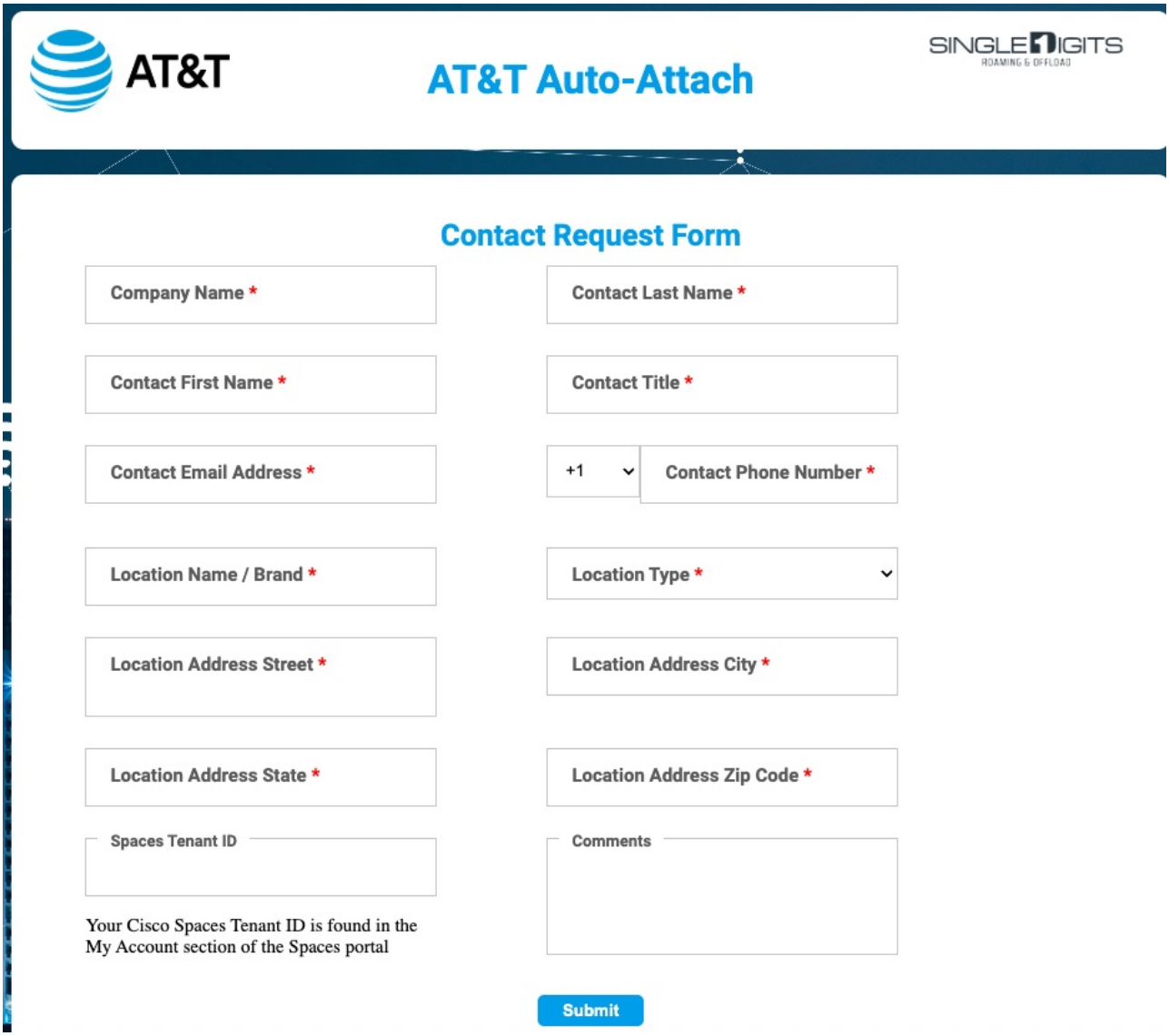
Figure 8:



The **Contact Request Form** appears.

Step 8 Enter these information in the **Contact Request Form**.

Figure 9:



- **Company Name**
- **Contact First Name**
- **Contact Email Address**
- **Location Name / Brand**
- **Location Address Street**
- **Location Address State**
- **Contact Last Name**
- **Contact Title**

- **Contact Phone Number**
- **Location Type**
- **Location Address City**
- **Location Address Zip Code**

Step 9 Click **Submit**.

AT&T receives the contact request. AT&T contacts the specified representative to review the proposed locations, confirm the expected subscriber experience, and complete the applicable agreement.

What to do next

After AT&T approves the request, it provides a token to the registered contact. Retain the token and use it to activate the AT&T Auto-Attach application.

Activate AT&T

Activate AT&T Auto-Attach for the locations approved by AT&T.

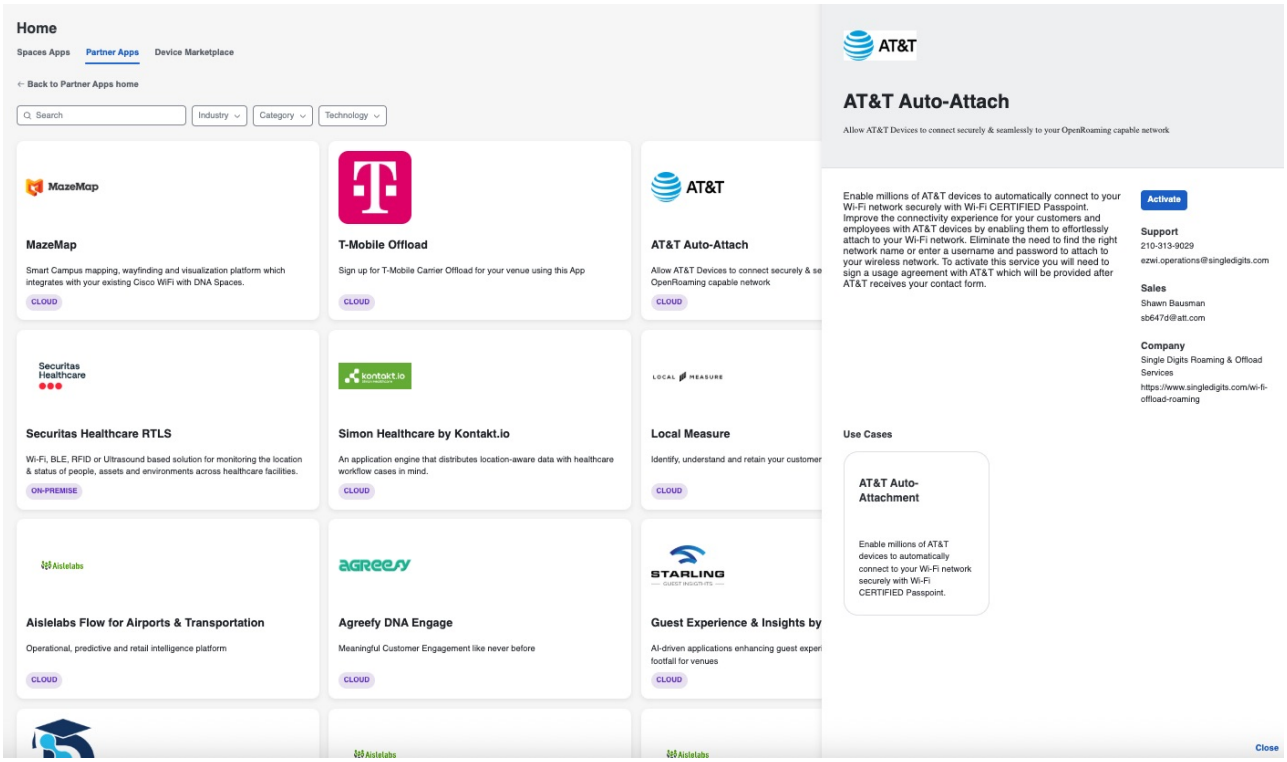
Before you begin

- AT&T has approved the customer account and locations.
- You have access to the email address used to register the AT&T account.
- You have the token provided by AT&T.
- The applicable locations are available in the Cisco Spaces location hierarchy.

Procedure

Step 1 Log in to Cisco Spaces.
Step 2 Click the **Partner Apps** tab.
Step 3 Click **Show all Partner Apps**.
Step 4 Click **AT&T Auto-Attach**.

Figure 10:



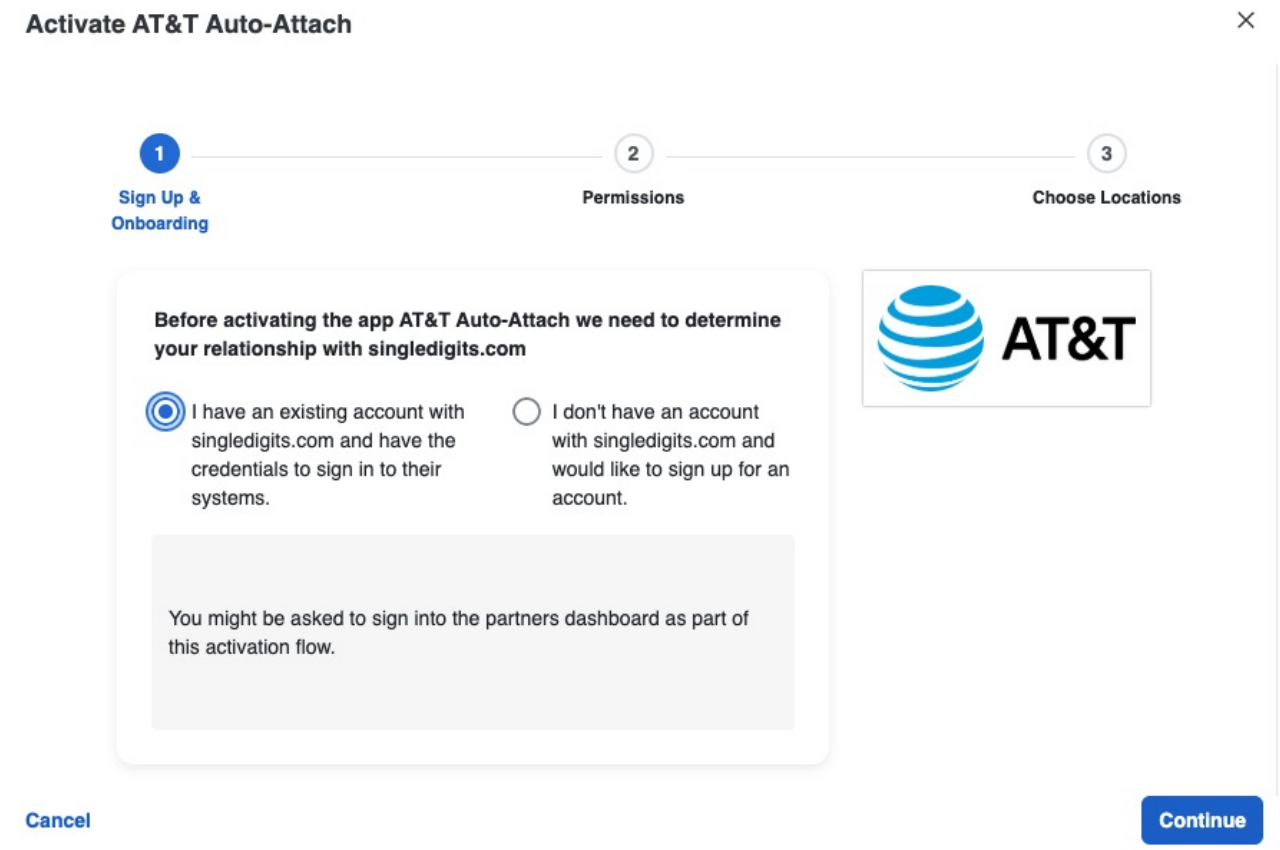
The **AT&T Auto-Attach** slide-panel appears.

Step 5 Click **Activate**.

Step 6 Review and accept the **Terms & Conditions**.
The account selection options appears.

Step 7 In the **Sign Up & Onboatding** section, choose the option to existing account.

Figure 11:



Step 8 Click **Continue**.

a) In the **Permission** section, click **Grant Permissions**.

b) In the **Choose Locations** section, select the locations where you want to activate AT&T Auto-Attach by using one of the these methods:

- To activate the application for every location, check the **Show all locations** check box.
- To activate the application for specific locations, select the required locations from the location hierarchy.

Step 9 Click **Next**.

a) Enter the email address used to register the AT&T account, click **Continue**.

b) Enter the token provided by AT&T, click **Sign in**.

The AT&T Auto-Attach application is activated for the selected locations.

What to do next

Verify that the registered contact receives the AT&T activation confirmation email. Confirm that the Partner App shows an active status for the intended locations before associating the carrier-enabled OpenRoaming profile with a newly onboarded network.

- After successful activation, supported AT&T subscribers can use the carrier-enabled OpenRoaming network at the approved locations.
- The Partner App can provide supported service-level and network-health telemetry to AT&T through Cisco Spaces.

Setup a T-Mobile Account

Submit a request to T-Mobile to establish an Auto-Attach account and obtain the credentials required for application activation.

Before you begin

- Complete the carrier-offload prerequisites described in this chapter.
- Identify the locations where T-Mobile carrier offload will be enabled.
- Identify a business and technical contact who can work with T-Mobile during the location review and agreement process.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 Click the **Partner Apps** tab.

Step 3 Click **Show all Partner Apps**.

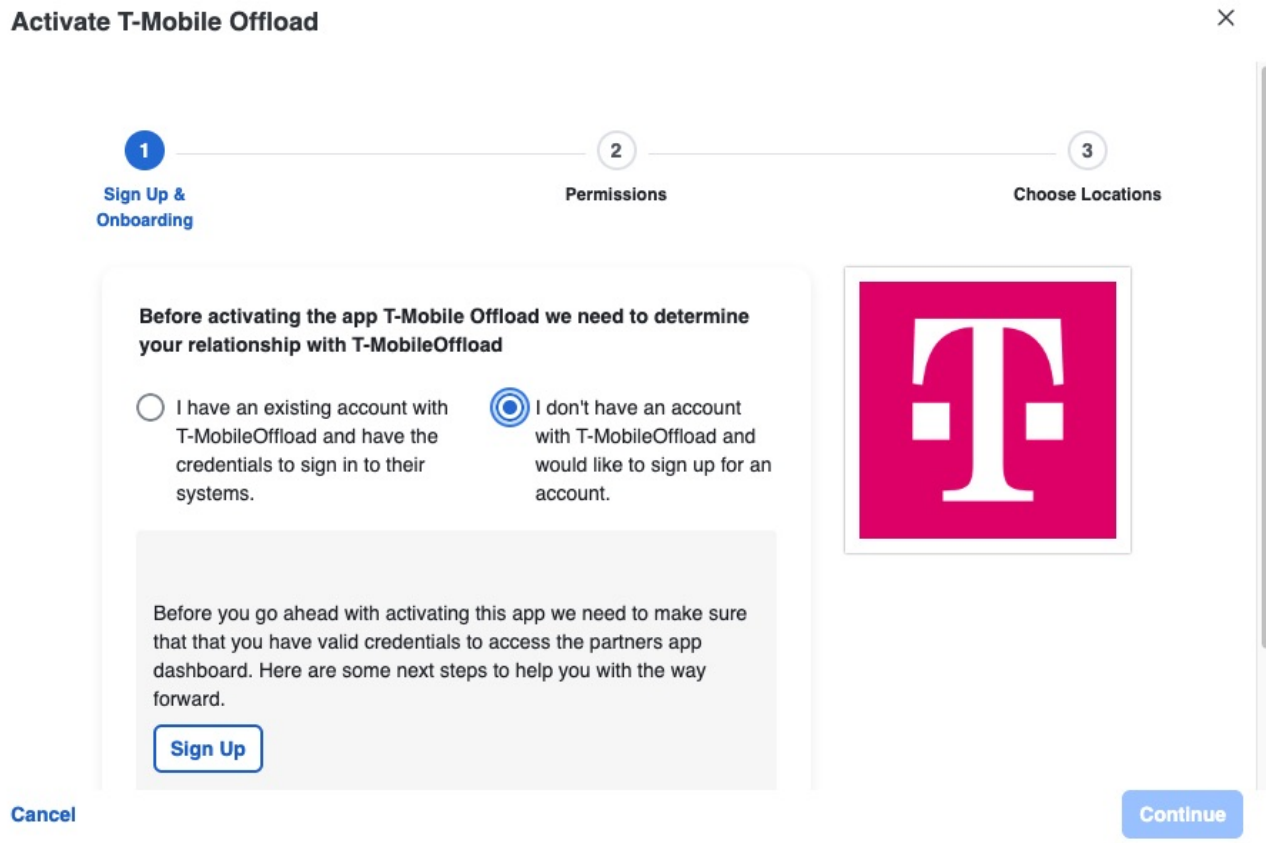
Step 4 Click **T-Mobile Offload**.
The **T-Mobile Offload** slide-panel appear.

Step 5 Click **Activate**.

Step 6 Review and accept the **Terms & Conditions**.
The account selection options appears.

Step 7 In the **Sign Up & Onboatding** section, choose the option to new account.

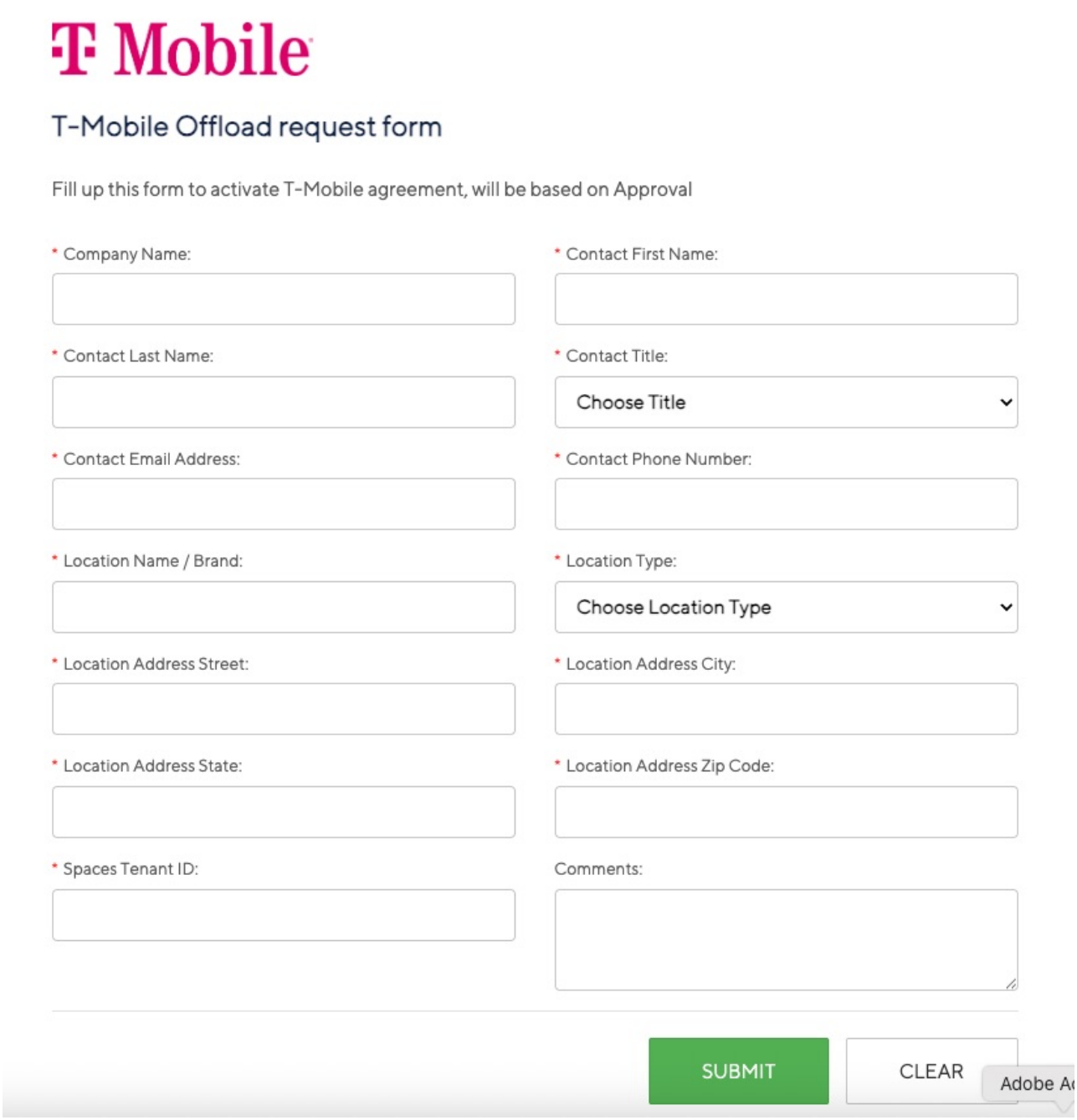
Figure 12:



The **Contact Request Form** appears.

Step 8 Enter these information in the **Contact Request Form**.

Figure 13:



- **Company Name**
- **Contact First Name**
- **Contact Email Address**
- **Location Name / Brand**

- **Location Address Street**
- **Location Address State**
- **Contact Last Name**
- **Contact Title**
- **Contact Phone Number**
- **Spaces Tenant ID**
- **Location Type**
- **Location Address City**
- **Location Address Zip Code**

Step 9 Click **Submit**.

T-Mobile receives the contact request.

T-Mobile contacts the specified representative to review the proposed locations, confirm the expected subscriber experience, and complete the applicable agreement.

What to do next

- After T-Mobile approves the request, it provides the account credentials required to activate T-Mobile Auto-Attach.
- Retain the credentials and confirm the tenant or account name to use during activation.

Activate T-Mobile

Activate T-Mobile Auto-Attach for the locations approved by T-Mobile.

Before you begin

- T-Mobile has approved the customer account and locations.
- You have the email address and password provided for the approved account.
- You have the applicable tenant or account name.
- The applicable locations are available in the Cisco Spaces location hierarchy.

Procedure

Step 1 Log in to Cisco Spaces.

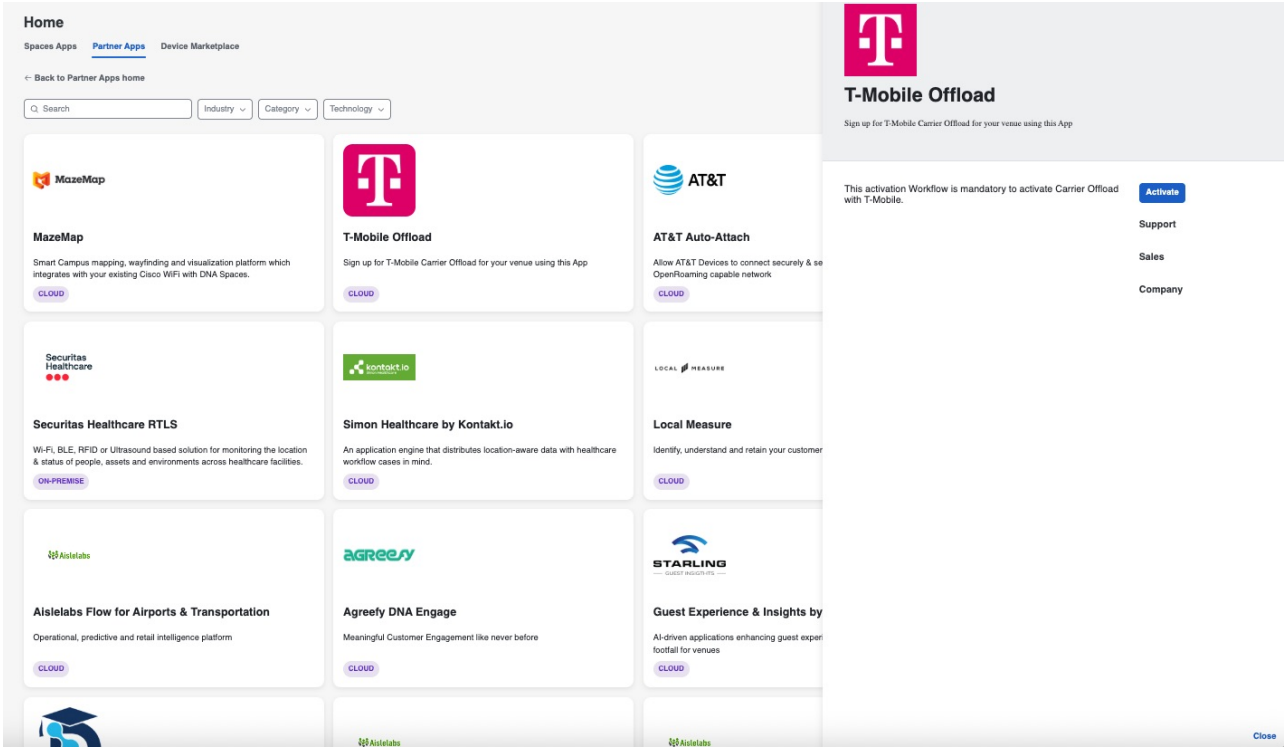
Step 2 Click the **Partner Apps** tab.

Step 3 Click **Show all Partner Apps**.

Step 4 Click **T-Mobile Offload**.
The **T-Mobile Offload** slide-panel appears.

Step 5 Click **Activate**.

Figure 14:



Step 6 Review and accept the **Terms & Conditions**.
The account selection options appears.

Step 7 Click **Continue**.

a) In the **Permission** section, click **Grant Permissions**.
b) In the **Choose Locations** section, select the locations where you want to activate T-Mobile Auto-Attach by using one of the these methods:

- To activate the application for every location, check the **Show all locations** check box.
- To activate the application for specific locations, select the required locations from the location hierarchy.

Step 8 Click **Next**.

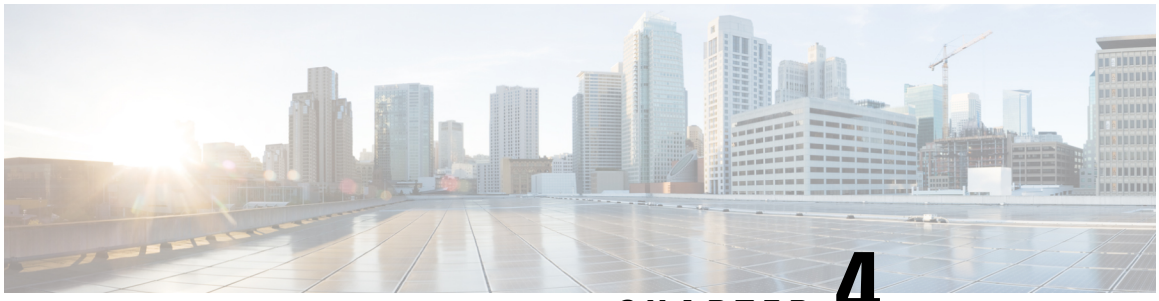
a) Enter the email address and password provided for the approved account, click **Login**.
b) Enter the applicable **Tenant/Account Name**.
c) Click **Proceed**.

The T-Mobile Auto-Attach application is activated for the selected locations.

What to do next

Confirm that the Partner App shows an active status for the intended locations before associating the carrier-enabled OpenRoaming profile with a newly onboarded network.

- After successful activation, supported T-Mobile subscribers can use the carrier-enabled OpenRoaming network at the approved locations.
- The Partner App can provide supported service-level and network-health telemetry to T-Mobile through Cisco Spaces.



CHAPTER 4

Configure Wireless Network

- Configure Wireless Network, on page 29
- Controller-Based Deployments: Configure Catalyst 9800 and AireOS, on page 29
- Configure Cisco Meraki Network, on page 31
- Edit Cisco Meraki network, on page 33

Configure Wireless Network

Select the procedure that matches the wireless platform to associate the OpenRoaming profile with the controller-based network or Meraki network.

Note If the selected OpenRoaming profile includes carrier offload, complete the required partner app activation before associating the profile with a newly onboarded controller or Meraki network.

Partner App activation support in OpenRoaming is available for AT&T and T-Mobile. Partner App activation is required before associating a carrier-enabled OpenRoaming profile to a newly onboarded controller or Meraki network.

If the required Partner App is not activated, Cisco Spaces does not allow the carrier-enabled profile to be configured on the newly onboarded network.

Controller-Based Deployments: Configure Catalyst 9800 and AireOS

Before you begin

Before configuring the Catalyst 9800 or AireOS wireless network, configure the SSID and AAA policy.

- Confirm that the controller appears under **Network configuration** > **Cisco Wireless controllers** with the expected controller status and associated connector.
- Confirm the Connector IP Address is available. If the value is not automatically populated in the Configure Controller window, enter the Cisco Spaces Connector IP address manually.

- For Catalyst 9800, identify the IOS XE version before generating configuration. Cisco Spaces provides separate Catalyst configuration options for IOS XE 17.2.1 or later and for 16.12.1/17.1.1.
- If a non-default policy profile or policy tag is used, copy only the ANQP server settings from the generated configuration and apply them to the correct wireless policy profile.

Procedure

Step 1 On the **OpenRoaming** window, choose **Setup**.

Step 2 Under **Network configuration** > **Cisco Wireless controllers** , click the three-dot icon for the target controller, then click **Configure Controller**.

Step 3 In the **Configure Controller** window, choose the required OpenRoaming profile for this controller and click **Continue**.

Step 4 Choose the controller type: **AireOS** or **Catalyst 9800**.

Step 5 Confirm the Connector IP Address. If it is not automatically filled, enter the Cisco Spaces Connector IP address.

Step 6 Confirm the WLAN Name. For Catalyst and AireOS, this value is automatically populated from the SSID name in the selected OpenRoaming profile. To change it, edit the OpenRoaming profile.

Step 7 Click **Show Configuration**.

Step 8 For Catalyst 9800, select the Catalyst version option that matches the controller IOS XE release: Catalyst (17.2.1/17.3.1) for IOS XE 17.2.1 or later, or Catalyst (16.12.1/17.1.1) for IOS XE releases earlier than 17.2.1.

Apply Catalyst 9800 and AireOS CLI configuration

Continue this task after selecting the Catalyst version option that matches the controller IOS XE release.

Procedure

Step 1 Review the generated CLI configuration. The generated configuration is for the Hotspot OpenRoaming ANQP server.

Step 2 Copy the generated configuration and paste it into the Catalyst 9800 or AireOS controller CLI.

Step 3 After applying the CLI configuration on the controller, click **Close** in Cisco Spaces.
The **OpenRoaming Setup** window is displayed.

Step 4 Confirm that the WLAN/SSID, AAA policy, ANQP/Hotspot settings, connector IP, wireless policy profile, policy tag, and controller association match the intended profile. For Catalyst 9800, confirm that the IOS XE version option used to generate the CLI matches the controller release.

Note

- Only CLI-based configuration is supported for Cisco AireOS and Cisco Catalyst controllers.
- Review the generated commands before applying them.
- The generated CLI assumes that the default wireless policy profile and policy tag are used.
- If the deployment uses a different wireless policy profile or policy tag, copy only the OpenRoaming Hotspot ANQP server settings from the generated configuration and apply them to the correct policy profile and policy tag.
- Ensure that the policy tag uses the WLAN configured for OpenRoaming and maps to the intended wireless policy profile.

Configure Cisco Meraki Network

Before you begin

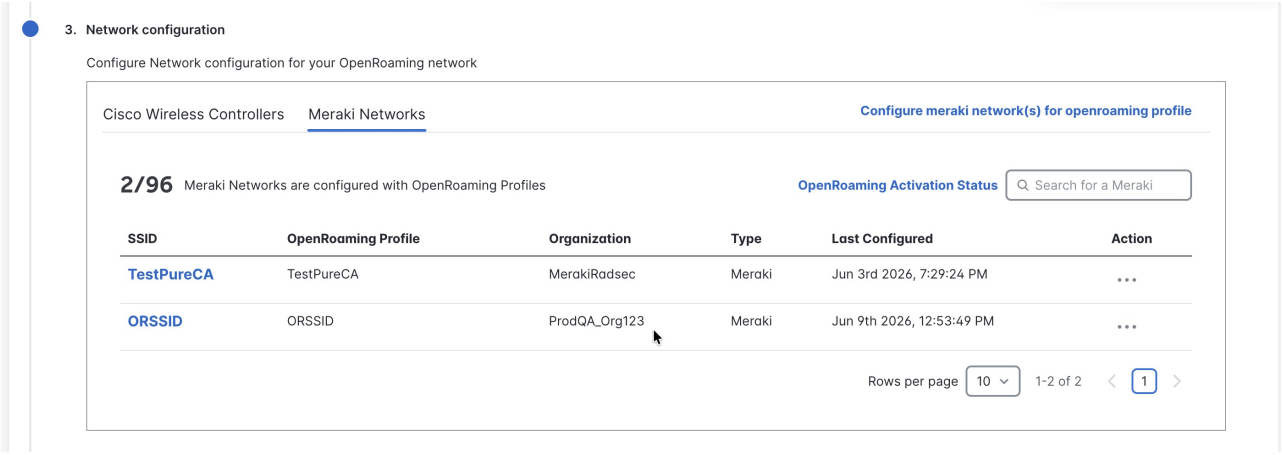
- For Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 APs, use R31.1.6 and above.
- For Wi-Fi 5, Wave 2 APs, use R30.7.2 and above.
- The Meraki account must have administrator access to activate the OpenRoaming SSID.
- At least one unconfigured SSID in Meraki Dashboard must be available in Disabled state.
- Supported Meraki APs include all MR Wi-Fi 5 Wave 2 APs that can be upgraded to at least MR 31.1.6, Wi-Fi 6 APs, and Wi-Fi 6E APs.
- Confirm Meraki API integration and Cisco Spaces permissions.
- Confirm Meraki AP outbound connectivity to the OpenRoaming RadSec endpoint over TCP 2083 as described in OpenRoaming Firewall Rules.

Procedure

Step 1 On the **OpenRoaming** window, choose **Setup**.

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

Figure 15: Meraki Networks



Step 3 Click **Set Up**.

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

Step 5 Click **Next**.

Step 6 Choose one or more Cisco Meraki networks for which you want to enable OpenRoaming. This step does not modify existing SSIDs.

Step 7 Click **Next**.

Review Cisco Meraki network configuration

Continue this task after choosing one or more Cisco Meraki networks for which you want to enable OpenRoaming.

Procedure

Step 1 From the drop-down list, select the OpenRoaming profile to apply to the Cisco Meraki network.

Step 2 Click **Next**.

Step 3 Review the **Configuration Summary**.

Step 4 Click **Configure**. Cisco Spaces configures the selected Meraki networks with a new SSID based on the OpenRoaming profile.

Step 5 In Meraki Dashboard, go to **Wireless** > **Configure** > **SSIDs** and confirm that the SSID created from the OpenRoaming profile is enabled. In the **SSID settings**, confirm Security is Enterprise with my RADIUS server, Encryption is WPA2 or WPA3, Splash Page is None (direct access), and RADIUS servers are configured. Navigate to **Wireless** > **Hotspot 2.0** and confirm Hotspot 2.0 is enabled. After client testing, client records appear in **Network-wide** > **Clients**, and Cisco Spaces API changes appear under **Organization** > **Monitor** > **Change Log**.

Note

- Configuration of Cisco Meraki networks that use templates is not supported.
- If one or more Meraki prerequisites are not met, OpenRoaming can be manually activated by installing a Cisco Spaces Connector. In this scenario, raise a support case for deployment support and describe the scenario. Support case reference: https://activate.dnaspaces.io/hubfs/Assets/CiscoSpaces-SupportUpdate.pdf
- Avoid weak encryption settings such as WPA1 or WPA1 and WPA2. Some clients may refuse to connect to OpenRoaming SSIDs configured with weak encryption.
- Use WPA2 Only or WPA3 under **Wireless** > **Configure** > **Access Control**.
- If required by the customer network design, configure VLAN tagging in the Meraki Client IP and VLAN settings after confirming the OpenRoaming SSID is created.

Edit Cisco Meraki network

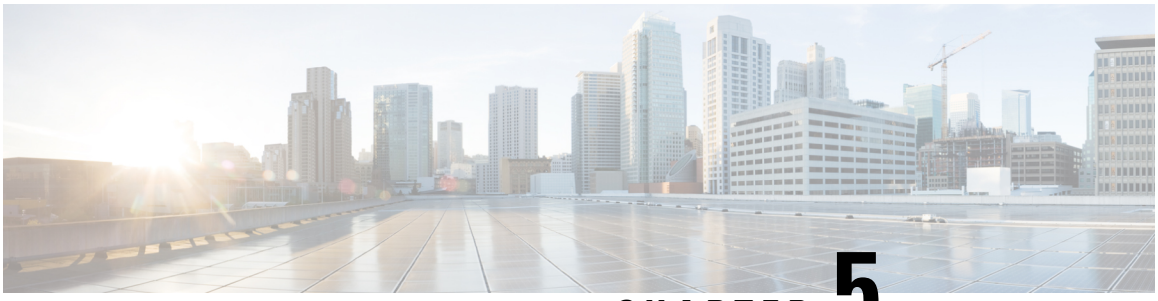
Procedure

Step 1 On the **OpenRoaming** window, choose **Setup**.

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

Step 3 Click the SSID for the Cisco Meraki network to update.

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



CHAPTER 5

Check OpenRoaming Activation

• Check OpenRoaming Activation, on page 35

Check OpenRoaming Activation

After configuring the controller-based network or Meraki network, confirm activation before client testing.

Procedure

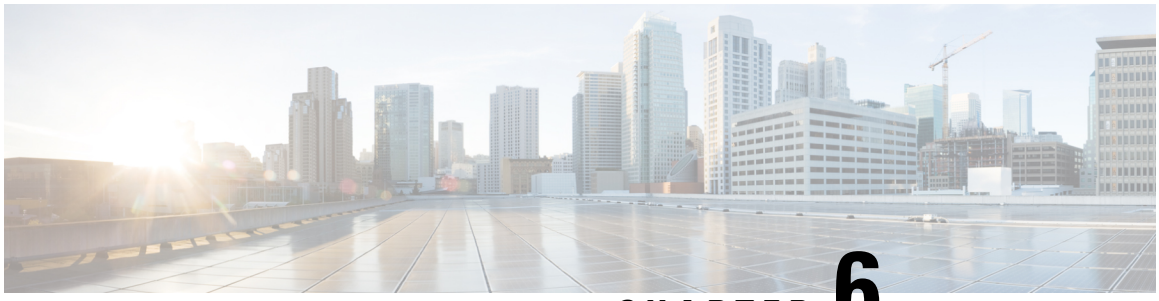
Step 1 In Cisco Spaces, check the OpenRoaming activation status on the **OpenRoaming** dashboard.

Step 2 For Catalyst 9800 and AireOS deployments, confirm that the hotspot-enabled connector remains **Running** and that the controller remains associated with the OpenRoaming profile.

Step 3 For Cisco Meraki deployments, confirm that pilot clients appear under **Network-wide** > **Clients** in Meraki Dashboard after testing.

Step 4 For Cisco Meraki deployments, verify that Cisco Spaces API changes were pushed to Meraki by reviewing **Organization** > **Monitor** > **Change Log**.

Check OpenRoaming Activation



CHAPTER 6

Test your OpenRoaming network

- Test your OpenRoaming network, on page 37
- OpenRoaming client matrix, on page 37

Test your OpenRoaming network

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

- Cloud/Social: Download the OpenRoaming mobile app from the iOS App Store or Google Play Store.
- Device Manufacturer: Test natively on a supported Samsung or Google mobile device.
- Carrier Offload: If carrier offload is configured, a mobile device from the supported carrier connects automatically to the OpenRoaming network.
- OpenRoaming SDK: If the brand mobile app integrates OpenRoaming SDK, a mobile device with the app connects automatically.

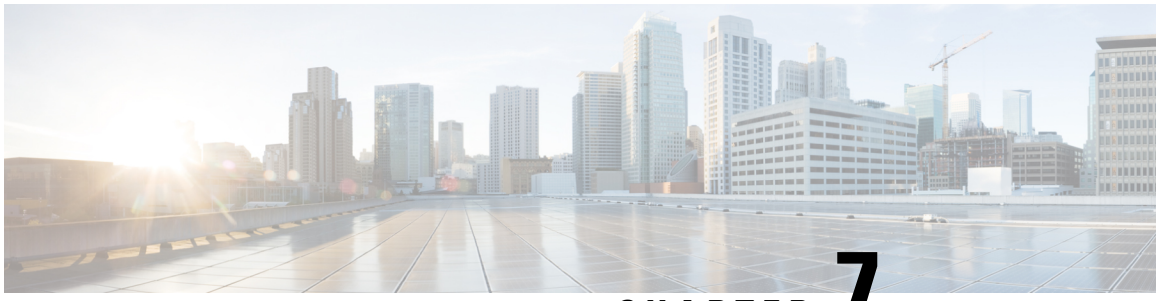
OpenRoaming client matrix

OpenRoaming Client Matrix

Table 1: OpenRoaming Client Matrix

Category	Support
Device Support	Samsung Devices: Android 10 or higher. Google Pixel: Android 11 or higher. Apple devices running iOS 13.3 or higher.
OS Support	Apple devices running iOS 13.3 or higher. Android phones running Android 9 or higher.

Category	Support
Cisco Spaces SDK	iOS 13.3 or higher. XCode version 12 or higher. Android 9 or higher.
Service Providers	T-Mobile. AT&T. Comcast.



CHAPTER 7

View OpenRoaming Reports

- View OpenRoaming reports, on page 39

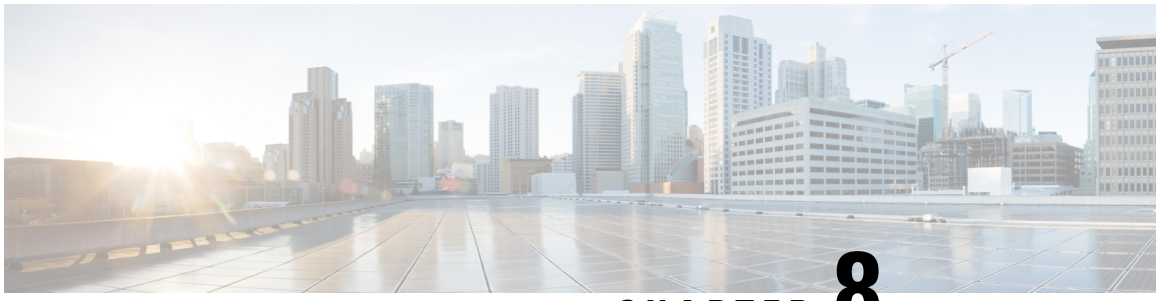
View OpenRoaming reports

Procedure

Click **Home** 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

Note Use reports after pilot testing to validate connection counts, device manufacturers, identity providers, data usage, and time-based connection patterns.



CHAPTER 8

OpenRoaming firewall rules

- OpenRoaming firewall rules, on page 41
- Meraki RadSec IP allowlist, on page 42
- Domains to allowlist, on page 42
- Carrier offload domain allowlist, on page 43

OpenRoaming firewall rules

The Cisco Spaces Connector and OpenRoaming integration path require reachability to OpenRoaming, OpenRoaming services, and RadSec endpoints. For controller-based deployments, allow controller-to-connector RADIUS traffic. For connector cloud access and Meraki RadSec, allow the required outbound paths. If direct internet access is restricted, configure the required ports, FQDNs, and Meraki RadSec HAProxy IP destinations on the firewall, DNS security service, proxy, or SSL inspection device.

Note

- Apply these allowlists before enabling the Hotspot service or associating an OpenRoaming profile with a controller or Meraki network.
- Validate DNS resolution and outbound connectivity from the same network path used by the connector, controller, Meraki APs, or Meraki API integration.

Table 2: OpenRoaming Firewall Rules

Traffic / service	Requirement
Cisco Spaces or OpenRoaming cloud	Allow HTTPS or TCP 443 to the regional Cisco and OpenRoaming domains.
Controller to Connector RADIUS	For controller-based deployments, allow Cisco AireOS/Catalyst controller traffic to the OpenRoaming Connector on UDP/TCP 1812 and 1813 for OpenRoaming RADIUS messages.
RADSec	Allow TCP 2083 where RADSec-secured authentication is used.

Traffic / service	Requirement
Meraki AP RadSec	For Meraki deployments, allow Meraki AP outbound TCP 2083 to the applicable OpenRoaming RadSec HAProxy IP destination listed in the Meraki RadSec IP allowlist.
RADIUS	Allow UDP 1812 and UDP 1813 where customer RADIUS flows are used.
DNS	Required FQDNs must resolve from the connector/controller/API egress network.
Proxy or SSL inspection	Bypass or explicitly trust required OpenRoaming service traffic. Proxy authentication, TLS inspection, or certificate substitution can prevent onboarding even when DNS resolution succeeds.

Meraki RadSec IP allowlist

For Meraki deployments, Meraki APs must have outbound connectivity over TCP 2083 to the applicable OpenRoaming RadSec HAProxy IP destination below. Allow the destination that corresponds to the Cisco Spaces environment used by the deployment.

Table 3: Meraki RadSec IP allowlist

Cisco Spaces environment	Meraki AP outbound HAProxy destination	Port
US or IO	184.73.46.220	TCP 2083
EU	63.33.180.45	TCP 2083
SG	54.169.186.118	TCP 2083

Domains to allowlist

Allow the FQDNs that apply to the Cisco Spaces tenant, connector, and OpenRoaming service path.

Table 4: Domains to allowlist

Domain allowlist
cisco.openroaming.org
cisco.openroaming.net
connector.dnaspaces.io
location.dnaspaces.io

Domain allowlist
idp.openroaming.net
sdk.openroaming.net
google.openroaming.net
apple.openroaming.net
samsung.openroaming.net
connect.ciscospaces.io
connector.dnaspaces.eu
location.dnaspaces.eu
eu-prod.openroaming.net
eu-sdk.openroaming.net
eu-google.openroaming.net
eu-apple.openroaming.net
connect.ciscospaces.eu
connector.ciscospaces.sg
location.ciscospaces.sg
sg-prod.openroaming.net
sg-sdk.openroaming.net
sg-google.openroaming.net
sg-apple.openroaming.net
connect.ciscospaces.sg

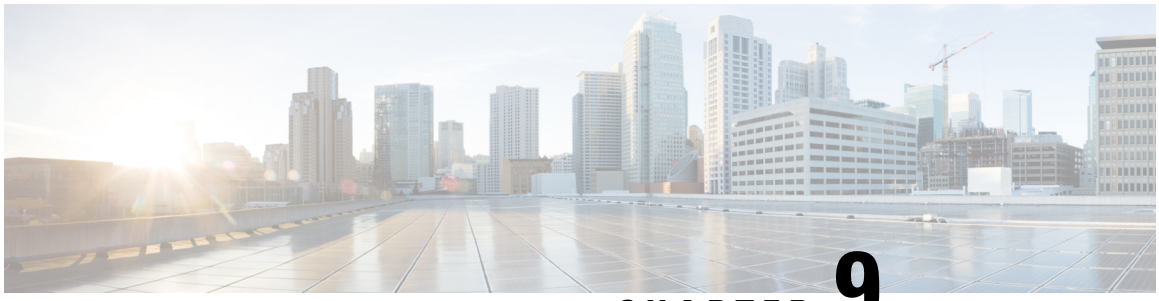
Carrier offload domain allowlist

Use this allowlist only when carrier offload is enabled in the OpenRoaming profile. These domains are not required for a standard OpenRoaming deployment without carrier offload.

Note Add only the carrier rows that match the enabled carrier offload providers to the firewall and DNS allowlists.

Table 5: Carrier Offload Domain Allowlist

Carrier	When to allowlist	Domains
AT&T-US	Required only when AT&T-US carrier offload is enabled.	wlan.mnc150.mcc310.3gppnetwork.org wlan.mnc280.mcc310.3gppnetwork.org wlan.mnc100.mcc313.3gppnetwork.org wlan.mnc410.mcc310.3gppnetwork.org
T-Mobile-US	Required only when T-Mobile-US carrier offload is enabled.	wlan.mnc120.mcc310.3gppnetwork.org wlan.mnc530.mcc312.3gppnetwork.org wlan.mnc490.mcc310.3gppnetwork.org wlan.mnc260.mcc310.3gppnetwork.org wlan.mnc160.mcc310.3gppnetwork.org



CHAPTER 9

Monitoring

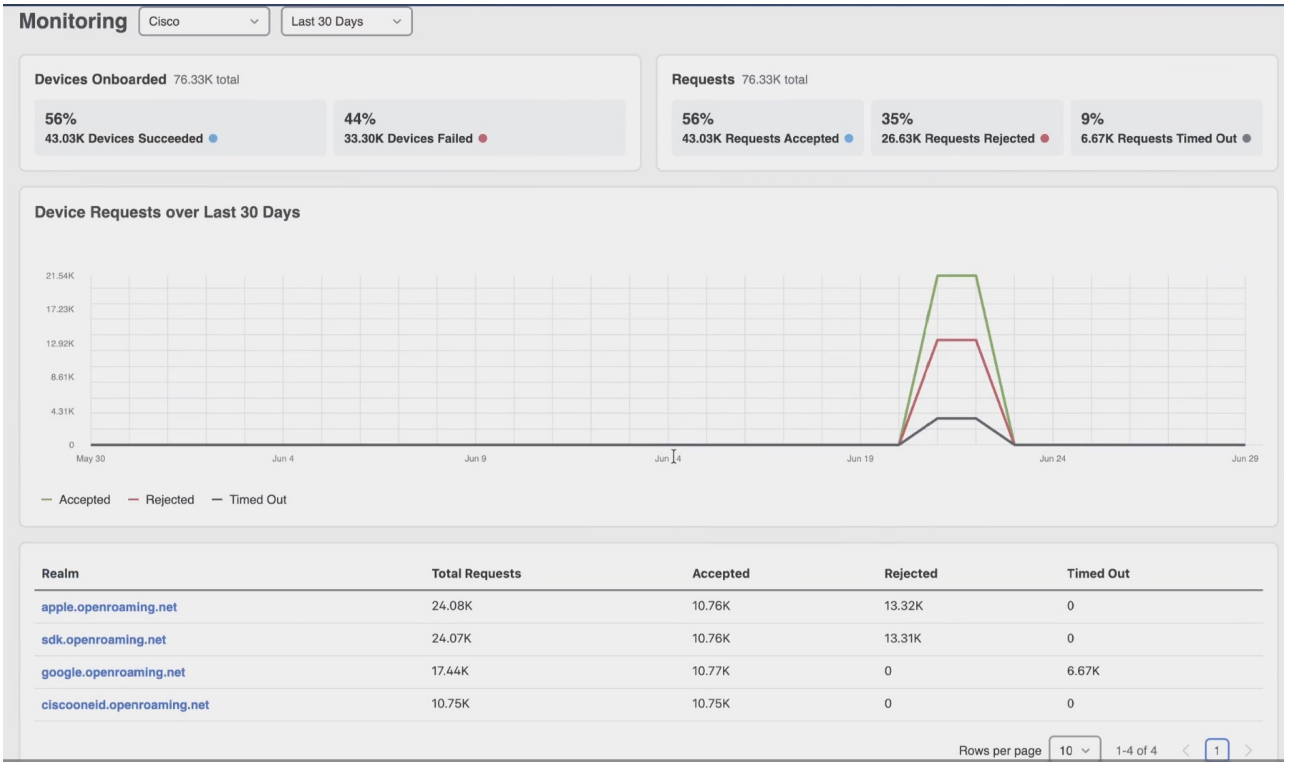
- Monitoring, on page 45
- View OpenRoaming monitoring data, on page 46
- OpenRoaming monitoring data, on page 47

Monitoring

The **Monitoring** dashboard provides visibility into OpenRoaming authentication activity. It enables administrators to monitor authentication trends, identify failures, and analyze Identity Provider (IdP) activity through a centralized dashboard. The dashboard presents authentication information through graphical and tabular views.

Note Monitoring uses the existing OpenRoaming configuration. You do not need additional configuration to view monitoring data after you configure OpenRoaming and controllers send authentication data.

Figure 16: Monitoring



View OpenRoaming monitoring data

Before you begin

Configure OpenRoaming.

Procedure

Step 1 In Cisco Spaces, choose **OpenRoaming** > **Monitoring**.

Step 2 To narrow the data to a specific identity provider, select an IDP.

Step 3 Select a time range.

You can view data for 8 hours, 24 hours, 1 week, or 30 days.

Step 4 Review **Devices Onboarded** to compare successful and failed onboarding activity.

Step 5 Review **Requests** to compare accepted, rejected, and timed-out authentication requests.

Step 6 Use the device requests graph to review request trends for the selected time range.

Step 7 In the **Realm** table, click a realm to view more details for that realm.

The details open on the page. Click **Close** to return to the monitoring dashboard.

Step 8 Use the **Network/Controller** table to review request activity by controller and network type.

OpenRoaming monitoring data

The **Device Onboarding** section displays the number and percentage of devices that successfully completed onboarding and those that failed.

The **Requests** section displays the following authentication request statistics as both numbers and percentages.

The **Device Requests** section displays graphical metrics that represent authentication activity over the selected time period.

Table 6: Realm

Realm	Total Requests	Accepted Requests	Rejected Requests	Timed-Out Requests
Domain or realm that generated authentication requests.	Total number of authentication requests from the realm.	Total number of accepted requests from the realm.	Total number of rejected requests from the realm.	Total number of timed-out requests from the realm.

Table 7: Network and Controller

Network and Controller	Total Requests	Accepted Requests	Rejected Requests	Timed-Out Requests	Network
List of network and controller	Total number of authentication requests from the controller.	Total number of accepted requests from the controller.	Total number of rejected requests from the controller.	Total number of timed-out requests from the network and controller.	Total number of network.