

Configuring Cisco Meraki for Cisco Spaces

This chapter describes the configurations required in Cisco Meraki for using Cisco Spaces.

- Enabling SSIDs in Cisco Meraki, on page 1
- Configuring Cisco Meraki for RADIUS Authentication, on page 2
- Configuring Cisco Meraki for Notifications and Reports, on page 4
- Configuring Cisco Meraki for Social Authentication, on page 5
- Manually Configuring SSIDs for Cisco Meraki, on page 5
- Configuring Scanning API in Cisco Meraki, on page 6
- Bluetooth Low Energy Device Support, on page 7

Enabling SSIDs in Cisco Meraki

To import the SSIDs to the Cisco Spaces to configure them for the Captive Portal Rules, you must enable those SSIDs in Cisco Meraki.

Note As Cisco Meraki is not a part of the Cisco Spaces, the menu path and menu names are subject to change.

To enable the SSIDs in Cisco Meraki, perform the following steps:

Procedure

Step 1 Go to https://meraki.cisco.com.

Step 2 Log in to the application using the login credentials for your Cisco Meraki account.

Step 3 Click the **Cisco Merkai Organization** in which you want to enable the SSIDs, and choose the required network.

Step 4 Choose **Wireless** > **Configure** > **SSIDs**.

The SSIDs available for the network appears.

Step 5 Rename the SSID and enable it.

Step 6 Click **Edit Settings**, and in the Splash page option, click the **Click-Through** radio button.

Step 7 Click **Save Changes**.

The SSID is successfully enabled in Cisco Meraki.

Configuring Cisco Meraki for RADIUS Authentication

To provide more security to your portals, the Cisco Spaces provides radius-authentication for the portals. Also, certain configurations are required in Cisco Meraki to manage the seamless internet provisioning that can be configured using the Captive Portal Rule.

The Radius Server Configurations required when configuring for the seamless internet provisioning is different from that of the standard radius server configuration.

Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations)

To configure Cisco Meraki for RADIUS authentication, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki with your Meraki credentials.

Step 2 Choose **Wireless Access Control**.

Step 3 Choose the SSID for the captive portal rule.

Step 4 In the **Association requirements** area, choose **Open**.

Step 5 In the **Splash page** area, choose **Sign-on with**, and from the drop-down list select **my RADIUS server**.

Step 6 In the **Radius servers**area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

Note You can configure only the Cisco Spaces RADIUS servers.To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 7 From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 8 In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port:1813

Note You can configure only the Cisco Spaces RADIUS servers. You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs page.

Step 9 Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 10 Save the changes.

Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning

To configure Cisco Meraki for RADIUS authentication and Seamless Internet Provisioning, do the following configurations in Cisco Meraki:

Procedure

Step 1 Log in to Cisco Meraki with your Meraki credentials.

Step 2 Choose **Wireless** > **Access** > **Control**.

Step 3 Choose the SSID for the captive portal rule.

Step 4 In the Association requirements area, choose **Mac-based access control (no encryption)**.

Step 5 In the Splash page area, choose **Click-through**.

Step 6 In the Radius servers area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually**link for a Meraki SSID in the SSIDs page.

Step 7 From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 8 In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port :1813

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 9 From the **Radius attribute specifying group policy name** drop-down list, choose **Filter-Id**.

Step 10 Save the changes.

Step 11 In the Cisco Meraki dashboard, click **Network-wide Group Policies**.

Step 12 Click **Add a Group**.

Step 13 In the **New group** window that appears, enter a name for the group.

Note You have to configure this name as the policy name in the Cisco Spaces dashboard. If you are specifying the group name as **CaptiveBypass**, this policy name will act as the default policy name for all the Captive Portal rules. That is, if you are not specifying a policy name for a Captive Portal rule for which the "Seamlessly Internet Provision" is opted, the policy name **CaptiveBypass** will be applied for that rule.

Step 14 From the **Bandwidth** drop-down list, choose the required option, and specify the Internet bandwidth to be provisioned for the customers.

Step 15 From the Splash drop-down list, choose **Bypass**.

Step 16 Click **Apply**.

Step 17 Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Configuring Cisco Meraki for Notifications and Reports

To send notifications using the Cisco Spaces and to view the Cisco Spaces reports, you must do certain configurations in Cisco Meraki.

Note When you import a Meraki network location to Location Hierarchy, the Notification URL automatically gets configured in Cisco Meraki. This support is not applicable for the Meraki networks added using Meraki API Key.

To manually configure Cisco Meraki for sending notifications using the Cisco Spaces or to view the Cisco Spaces reports, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki using the credentials for your Meraki account.

Step 2 Click the organization in which you want to enable SSIDs, and choose the required network.

Step 3 Choose **Network-wide** > **Configure** > **General**.

Step 4 In the **CMX** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics is enabled**.
b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.
c) Click **Add a Post URL**, and enter the post URL details in the respective fields.

To view the post URL details, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the **SSIDs** window.

Step 5 Click **Save Changes**.

Configuring Cisco Meraki for Social Authentication

For social authentication with Cisco Meraki, you must do some configurations in meraki.cisco.com.

To configure Cisco Meraki for social-authentication, perform the following steps:

Procedure

Step 1 In the Cisco Meraki dashboard, choose **Wireless** > **Configure** > **Access Control** .

The **Access Control**window appears.

Step 2 From the **SSID** drop-down list, choose the SSID for which you want configure the social authentication.

Step 3 In the **Wall Garden Ranges** field, enter the social networking domain names listed in the following table, and click **Save Changes**.

Social Authentication for Cisco Meraki is successfully configured.

Table 1: Social Networking Domain Names

Facebook	Twitter	LinkedIn	
*.facebook.com *.fbcdn.net *.akamaihd.net *.connect.facebook.net	*.twitter.com *.twimg.com	*.linkedin.com *.licdn.net *.licdn.com	

Manually Configuring SSIDs for Cisco Meraki

To manually configure an SSID in Cisco Meraki, you have to initially import that SSID in the Cisco Spaces. For more information, see the "Importing the SSIDs for Cisco Meraki section .

To configure the SSID manually in Cisco Meraki, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki using the credentials for your Meraki account.

Step 2 Choose the required Cisco Meraki organization and network from the respective drop-down list.

Step 3 Choose **Wireless** > **Access Control**.

Step 4 From the SSID drop-down list, choose the SSID that you want to configure for the Cisco Spaces.

Step 5 In the splash page area, choose **Click-through**.

Step 6 From the Wall garden drop-down list, choose **Wall garden is enabled**.

Step 7 In the **Wall garden ranges** field, enter the required wall garden ranges.

To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the **SSIDs** window.

Step 8 Click **Save Changes**.

Step 9 Choose **Wireless** > **Splash page**.

Step 10 For the previously selected SSID, in the **Custom Splash URL** area, choose **Or provide a URL where customers will be redirected**, and in the adjacent field enter the splash URL.

To generate and view the splash page URL for a Meraki SSID, follow the steps given below:

a) Click **Home** > **Captive Portals** > **SSIDs** to import the Meraki SSID to Cisco Spaces.
A splash page URL is generated in the Cisco Spaces Dashboard.

b) On the **SSIDs** page, click the **Configure Manually** link for the desired Meraki SSID.
The splash page URL for the selected Meraki SSID is displayed.

Step 11 In the **Splash Behavior**area, click the **The URL they were trying to fetch** radio button under **Where should users go after the splash page**.

Step 12 Click **Save Changes**.

Step 13 Repeat steps 3-12 for all the SSIDS that you want to use in the Cisco Spaces.

What to do next

Configuring Scanning API in Cisco Meraki

For using Meraki Camera, you must configure Scanning API in Cisco Meraki.

To configure a Scanning API in Cisco Meraki, perform the following steps:

Procedure

Step 1 Log in to the https://meraki.cisco.com using the login credentials for your Cisco Meraki account.

Step 2 Choose **Networkwide** > **General**.

Step 3 In the **Location and Scanning** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.

c) Add a post URL.

- In the **Post URL** field, enter the post URL .
- In the **Secret Key** field, enter the secret key that is used by your HTTP server to validate that the JSON posts that are coming from the Cisco Meraki cloud.

Note You can copy the post URL and secret key from the **Connect your Meraki Camera** window for **Setup** > **Camera** in Cisco Spaces dashboard.

- From the **API Version** drop-down list, choose the Location API version your HTTP server is prepared to receive and process.

Step 4 Configure and host your HTTP server to receive JSON objects.

Step 5 During the first connection, the Cisco Meraki cloud will verify the organization's identity as the Cisco Meraki customer.

The Cisco Meraki cloud will then begin performing JSON posts.

Bluetooth Low Energy Device Support

Support for Bluetooth Low Energy (BLE) devices are available on the Cisco Meraki network, in addition to the existing support on the Cisco Catalyst Wireless network.

This enhancement allows the Cisco Spaces platform to seamlessly integrate with BLE devices using Cisco Meraki. With this enhancement, Cisco Meraki BLE devices can now be accessed in various Cisco Spaces applications, including Firehose IoT Telemetry events, IoT Explorer, Signage, and Live Occupancy.

Note For this feature to work, you must perform specific configurations on the Cisco Meraki network to enable the data transmission to Cisco Spaces. We recommend that you contact Cisco Spaces support team for further assistance.