Configuring Meraki for CMX Engage

This chapter describes the configurations required in Meraki for using CMX Engage.

Enabling the SSIDs in Meraki

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

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

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

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

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

Step 3 Click the Meraki 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, choose the **Click-Through** radio button.

Step 7 Click **Save Changes**.

The SSID is successfully enabled in Meraki.

Configuring Meraki for Radius-Authentication

To provide more security to your portals, the CMX Engage provides radius-authentication for the portals. Also, certain configurations are required in 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 Meraki for Radius-Authentication (Without Seamless Internet Configurations)

To configure Meraki for radius authentication, perform the following steps:

Step 1 Log in to 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 CMX Engage radius servers.To view the radius server IP address and secret key, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/ CUWN” link in the SSIDs section, and on the “Configure SSID in Meraki” tab, click the “Radius Server Configuration” section.

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

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 CMX Engage radius servers. You can configure only the CMX Engage radius servers.To view the radius server IP address and secret key, in the CM X Engage dashboard, click the “Setup SSIDs in Meraki/ CUWN” link in the SSIDs section, and on the “Configure SSID in Meraki” tab, click the “Radius Server Configuration” section.

Step 9 Configure the Wall Garden ranges. To view the wall garden ranges, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/CUWN” link in the SSIDs page, and click the “Configure SSID in Meraki” tab.

Step 10 Save the changes.

Configuring Meraki for Radius-Authentication and Seamless Internet Provisioning

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

Step 1 Log in to 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 CMX Engage radius servers. To view the radius server IP address and secret key, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/ CUWN” link in the SSIDs section, and on the “Configure SSID in Meraki” tab, click the “Radius Server Configuration” section.

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

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 CMX Engage radius servers.To view the radius server IP address and secret key, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/ CUWN” link in the SSIDs section, and on the “Configure SSID in Meraki” tab, click the “Radius Server Configuration” section.

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 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 CMX Engage 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 CMX Engage dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs page, and click the "Configure SSID in Meraki" tab.

Configuring Meraki for Notifications and Reports

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

In the CMX Engage dashboard, when you click a location in the location hierarchy for which the notification configurations are not done, a dialog box appears asking whether to configure the network. Click **Yes** to update Meraki with the configurations.

Manually also you can configure Meraki for notifications and reports. To manually configure Meraki for sending notifications using the CMX Engage or to view the CMX Engage reports, perform the following steps:

Step 1 Log in to 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 CMS 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 CMX Engage dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs window, and click the "Configure SSID in Meraki" tab.

Step 5 Click **Save Changes**.

Configurations Required in Meraki for Location Manager

Before using the CMX Engage dashboard for managing locations, the location Manager must do certain configurations in the Meraki dashboard.

To work as a location manager, in the Meraki dashboard, perform the following steps:

Step 1 Log in to Meraki.

Step 2 Choose **Organization > Configuration templates**.

Step 3 In the Configuration templates page that appears, click **Create a new template**.

Step 4 In the Create a new configuration template window that appears, enter the following details:

a. From the first drop-down list, click **Create New**.

b. In the Template name field, enter the name "**Location Manager Template**", and click **Add**.

The "Select networks to follow "Location Manager Template"" window appears.

Step 5 In the Target networks drop-down list, choose your primary network.

Note Group policies and other client-specific policies and authorizations on the target network(s) will be permanently removed upon binding. After creating the new template, configure those policies in the new template.

Step 6 Click **Bind**.

Step 7 In the "Configuration templates list > Location Manager Template" that appears, click **Save Changes**.

The newly created template, **Location Manager Template,** gets listed in the Configuration Templates page.

Configuring Meraki for Social-Authentication

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

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

Step 1 In the 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 Walled Garden Ranges text field, enter the social networking domain names listed in the following table, and click **Save Changes**.

Table 3-1 Social Networking Domain Names

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

The social-authentication for Meraki is successfully configured.

Manually Configuring the SSIDs for Meraki

To manually configure an SSID in Meraki, you have to initially import that SSID in the CMX Engage. For more information, see the "Importing the SSIDs for Meraki" section on page 4-2.

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

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

Step 2 Choose the required 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 CMX Engage.

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" text field, enter the required wall garden ranges.

To view the wall garden ranges, in the CMX Engage dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs page, and click the "Configure SSID in Meraki" tab.

Step 8 Click **Save Changes.**

Step 9 Go to **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.

Note When you import an SSID to the CMX Engage, the splash page URL for the SSID is generated in the CMX Engage. To view the splash URL for an SSID, in the CMX Engage dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs page, and click the "Configure SSID in Meraki" tab.

Step 11 Click **Save Changes**.

Step 12 Repeat steps 3-11 for all the SSIDS that you want to use in the CMX Engage.