Defining Captive Portal Rules

The Captive Portal Rule enables you to manage the captive portal display and internet provisioning for the customers connecting to your SSIDs.

Using a Captive Portal Rule you can manage the captive portal display and internet provisioning in the followings ways:

- **Show Captive Portal**: When a customer filtered for the rule connects to the SSID configured for the rule, a captive portal is displayed. The customer can access the interent by clicking any menu item in the portal, after completing the required authentication steps. You can configure to show different captive portals to the customers that suits them based on their location, number of visits, tags they belong to, number of visits made in your location, duration of their visits, and so on.
- **Direct Internet Access**: When a customer filtered for the rule connects to the SSID configured for the rule, the internet is provisioned immediately without any authentication process. The captive portal is not shown in this case.
- **Deny Internet Access**: When a customer filtered for the rule tries to connect to the SSID, connection cannot be established as internet is denied.

In addition, the Captive Portal rule enables you to do the following:

- Create tags or modify existing tags based on rule filtering.
- Send the details of the customers that are signed in to the captive portal to an external API.

In a Captive Portal rule, you can configure the actions to be performed, when the conditions defined are met.You can filter the customers for the rule based on various parameters such as locations, tags, number and duration of visits of the customers, app status, and so on.

This chapter describes how to create the captive portal rules.

Creating the Captive Portal Rule

To create a Captive Portal Rule, perform the following steps:

1. Enabling the SSIDs in the Meraki, page 4-2
2. Configuring the Meraki for Internet Provisioning and Radius-Authentication, page 4-2
3. Accessing the CMX Engage, page 3-2
4. Importing the SSIDs, page 4-4
5. Defining the Location Hierarchy, page 3-2
6. Creating the Portals, page 4-4

7. Creating Tags, page 4-5
8. Defining a Captive Portal Rule, page 4-5

Note You need to have the Meraki and CMX Engage accounts to configure the captive portals.

Enabling the SSIDs in the Meraki

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

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

To enable the SSIDs in the 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 the Meraki.

Configuring the Meraki for Internet Provisioning and Radius-Authentication

To provide more security to your portals, the CMX Engage provides radius-authentication for the portals. Also, certain configurations are required in the Meraki to manage the internet provisioning. To use the Captive Portal Rule option, do the following configurations in the 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 Spash 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. You must contact the Cisco CMX Engage support team for the radius server host and secret key.

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 must contact the Cisco CMX Engage support team for the radius server IP address and secret key.

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. For more information on configuring the wall garden ranges in the Meraki, see the "Manually Configuring the SSIDs" section on page 4-11.

Accessing the CMX Engage

The procedure to access the CMX Engage is described in the "Accessing the CMX Engage" section on page 3-2.

Connecting to the Meraki from the CMX Engage

To perform certain tasks such as importing the SSIDs, you must establish connection with the Meraki. The procedure to connect to the Meraki from the CMX Engage is described in the "Connecting to the Meraki Network" section on page 3-3.

Importing the SSIDs

The SSIDs refer to the network IDs that you connect to access the internet through Wi-Fi. To create the Captive Portal rules for an SSID of Meraki, you need to import that SSID from the Meraki network.

To import the SSIDs for a Meraki network, you need to enable the SSIDs in https://meraki.cisco.com. For more information, see the "Enabling the SSIDs in the Meraki" section on page 4-2. The enabled SSIDs are available for importing.

To import the SSIDs, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **SSIDs**.

The SSIDs page appears.

Step 2 Click **Import**.

The Please Select SSID to Import page appears.

Step 3 Select the SSIDs you need to import, and click **Import SSID**.

The imported SSIDs appear in the SSIDs window.

Step 4 Click the **Activate** button for the SSID to update the CMX Engage configurations for the SSID in the Meraki.

The SSID Configuration Sync window appears with the SSID updates that need to be configured in the Meraki.

Step 5 Click **Update**.

You can manually also configure the SSIDs in the Meraki. To know how to manually configure the SSIDs in the Meraki, see the "Manually Configuring the SSIDs" section on page 4-11.

Note As the CMX Engage needs to synchronize with the Meraki network to load the imported SSIDs, you may need to refresh the window to view the imported SSIDs.

For more information on updating the configurations in the Meraki, see the following:

- Synchronizing with the Meraki, page 4-11
- Advanced Configurations for the SSID, page 4-11

Defining the Location Hierarchy

To choose the locations for the rule, you must define the location hierarchy. The procedure to define the location hierarchy is described in the "Defining the Location Hierarchy" section on page 3-2.

Creating the Portals

A portal is the user interface that appears when a Wi-Fi user is connected to an SSID. You can create the captive portals and enhance the portals using the various portal modules provided by the CMX Engage.

When defining a portal, you can also configure the locations for which the portal must be available

Note This step is required only if you want to configure a portal for the Captive Portal Rule.

To create a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Portal**, and click **Create New**.

Step 2 In the Portal window that appears, enter a name for portal in the Name field,.

Step 3 If you want the portal to be available for all the locations, select the "This portal will be available in all locations" check box. Else, select the locations for which the portal must be available.

Step 4 Click **Create**.

The portal page appears with the portal modules on the left and portal preview on the right.

Step 5 Add features to the portal using the Creating a Portal.

Note To capture the customer details such as name, phone number, and so on, ensure that you add a Data Capture module in the captive portals. Before provisioning the internet, the data capture form is displayed to the customer. The captured customer details are stored in the CMX Engage database. The Data Capture module is available for the Hard SMS with Verification Code and E-mail authentication types.

Step 6 Click **Save** to save the changes made to each module.

Note A portal becomes live when you associate it with a Captive Portal Rule, and publish that rule.

Creating Tags

To use the tag filter in the Captive Portal Rule, you must create tags.The procedure to define tags is defined in the "Creating Tags or Including or Excluding the Customers from an Existing Tag Using a Profile Rule" section on page 6-1.

Note This step is required only if you want to use the tag filter in your captive portal rule.

Defining a Captive Portal Rule

After meeting the pre-requisites such as the Meraki configurations, location hierarchy, and so on, you can define the Captive Portal Rule. The pre-requisites depend on the filters that you want to use in the rule.

You can filter the customers for whom you want to apply the rule based on their location, whether the customer is an opted in or not opted in user, the tags the customers belong to, the number of visits made by the customer, the status of app in the customer's device, and so on.You can filter the locations in which the rule is to be applied based on the locations or the metadata associated with the locations. You can apply the rule based on the number of visits made by the customer to the specified locations during

the specified time. You can also configure to apply the rule only during a particular period, only for certain days of a week, and only during a particular time. The Captive Portal Rule also allows you to configure to provide direct internet connection when the customers filtered for the rule connects to your SSID. In this case, the captive portal is not displayed, but the customer will get access to the internet. You can also configure to deny the internet access to the customers filtered for the rule.

Using a Captive Portal Rule, you can create new tags or modify existing tags with the customers filtered for the rule. The Captive Portal Rule also allows you send the details of the customers connected to the SSID configured for the rule to an external API.

To create a captive portal rule to show a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Proximity Rules > Captive Portal Rule**.

Step 2 Click **Create a new rule**.

Step 3 In the Rule Name text field, enter a name for the captive portal rule.

Step 4 In the Sense area, perform the following steps:

a. From the drop-down list after "When a user is on", choose **WiFi**.

b. From the drop-down list after "and connected to", choose the SSID for which you want to show the captive portal.

Note The SSIDs are available for selection only if you have imported the SSIDs. For more information on importing SSIDs, see the "Importing the SSIDs" section on page 4-4.

Step 5 In the Locations area, specify the locations for which you want to apply the rule.

You can configure to apply the rule for the entire location hierarchy, or a single or multiple Meraki organization, group, network, floor, or zone. For more information on creating the location hierarchy, see the "Defining the Location Hierarchy" section on page 3-1.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the "Defining Metadata for a Location" section on page 3-7. You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata.

To specify the locations in which you want to apply the rule, perform the following steps:

a. Click the **Add Locations** button.

b. In the Choose Location window that appears, select the locations for which you want to apply the captive portal rule.

c. Click **OK**.

To apply the rule for locations with a particular metadata, perform the following steps:

a. Select the **Filter by Metadata** check box.

b. In the Filter area, click the **+Add Metadata** button.

The Choose Location Metadata window appears.

c. From the drop-down list, choose the metadata variable, and enter the value for the variable in the adjacent field.

d. Click **OK**.

To exclude the locations with a particular metadata, perform the following steps:

a. Select the **Filter by Metadata** check box.

b. In the Exclude area, click the **+Add Metadata** button.

   The Choose Location Metadata window appears.

c. From the drop-down list, choose the metadata variable, and enter the value for the variable in the adjacent field.

d. Click **OK**.

Step 6 In the IDENTIFY area, specify the type of customers for whom you want to apply the rule.

Note You can filter the customers for whom you want to apply the rule based on whether the customer is an opted in or not opted in user, the tags the customers belong to, the number of visits made by the customer, and the status of app in the customer's device. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the Captive Portal Rule is to be applied, perform the following steps:

a. If you want to filter the customers by the Opt In Status, select the Filter by OptIn Status check box, and from the Only for drop-down list, choose whether you want apply the rule for opted in users or not opted in users.

Note For more information on Opted In users, see the"Opted In Users" section on page 6-7.

b. If you want to filter the customers based on tags, select the **Filter by Tags** check box.

Note You can filter the tags in two different ways. Either you can specify the tags for which the rule must be applied or you can specify the tags for which the rule must not be applied. You can choose the best filtering method based on your requirement. For example, if you want to apply the rule for the customers in all the tags expect for one tag, it is easy to opt the exclude option, and mention that particular tag for which you do not want to apply the rule.

   – To include the tags so that the rule is applied to the customers in the selected tags, use the **Add Tags** button for "Include".

   – To not apply the rule to the customers in the tags that are excluded, use the **Add Tags** button for "Exclude".

   For more information on using the tag filter, see the "Filtering by Tag" section on page 6-6.

c. If you want to filter the customers based on the number of visits made by the customer in the selected locations, select the **Filter by Previous Visits** check box.

   Click the **Add Locations** button. In the Choose location window, select the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration for filtering. For more information on the visits and duration you can configure, see the "Notification Criteria" section on page 5-17.

d. If you want to filter the customers based on the customer's app status, select the **Filter by App Status** check box. From the "Filter by the users who" drop-down list, choose the status of the app users for which you want to apply the rule.

Step 7 In the Schedule area, specify the period for which you want to apply the rule.

a. Select the Set a time range for the rule check box and in the fields that appear, specify the time range for which you want to apply the captive portal rule.

b. Select the Set a date range for the rule check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the captive portal rule.

c. If you want to apply the rule only on particular days, select the Filter by days of the week check box, and from the list of days that appears, click the days on which you want to apply the rule.

Step 8 In the Actions area, configuration the actions to be performed when the preceding conditions are met:

a. To manage the internet provisioning for the customers filtered for the rule, choose the required option from the following:

- **Show Captive Portal**- Choose this option to display a captive portal when the customers filtered for the Captive Portal rule connects to the SSID configured for the rule. From the Show them Portal drop-down list, choose the captive portal that you want to show when the conditions defined in this rule are met. The portals that you have created for the chosen locations are available for selection. For more information on creating a portal, see the "Creating the Portals" section on page 4-4.
- **Seamlessly Provision Internet-** Choose this option if you want to provide internet to your customers immediately after they connect to your SSID. In this case, the customer does not have to complete any authentication steps. To use this option, you must do certain configurations in the Meraki. For more information on configurations required in the Meraki, see "Configuring the Meraki for Internet Provisioning and Radius-Authentication" section on page 4-2.
  - In the Rule/Policy Name field, enter a name for the policy. You must specify the same name that you have defined in the Meraki.
  - In the Session Duration field, mention the duration for which the you want to provide the internet access for each connection.

Note The bandwidth field is not required for your network. The bandwidth mentioned for the policy in the Meraki is considered.

- **Deny Internet-** Choose this option if you want to deny the internet to the customers filtered for the rule when they try to connect to your SSID. In this case, the customers are not allowed to connect to the SSID.

b. To create a tag for the customers who are filtered based on this Captive Portal rule or to add or remove the filtered customers from an existing rule, click the **Add Tags** button. For more information on using the tag filter, see the"Filtering by Tag" section on page 6-6.

c. If you want to send the notification to an external API, select the Trigger API check box.

- From the Method drop-down list, choose the method for triggering API.

Note You can add the customer details in the notification message, by adding the smart link variables in the API URI or in the method parameters.

  - Get- To send notification to the API using the get method. If you choose this method, additional fields appear where you can mention the request parameters, to include additional details such as first name, last name, mobile number, and so on of the customer in the notification. You can add the request parameter keys defined in your API and mention the values for them using smart links. The value can be a hard-coded value or a variable. You can add a smart link variable using the adjacent Add Variable drop-down list or by entering "$" in the value field. For more information on smart link, see the"Smart Link" section on page 7-44. You can add more "get parameters" using the **add** button.

  - Post Form- To send notification to the API using the post form method. If you choose this method, additional fields appear where you can mention the form parameters, to include additional details such as first name, last name, mobile number, and so on of the customer in the notification. You can add the form parameter keys defined in your API and mention the values for them.The value can be a hard-coded value or a variable. You can add a variable as a form parameter variable using the adjacent Add Variable drop-down list or by entering "$" in the value field. For more information on smart link, see the"Smart Link" section on page 7-44.You can add more "form parameters" using the **add** button.
  - Post Json- To send notification to the API using the post json method. If you choose this method, a text box appears where you can mention the json data that is to send as notification message to the API. You can mention the json values for various json fields defined in your API. The value can be a hard-coded value or a variable. You can add a variable as a json value using the adjacent Add Variable drop-down list or by entering "$" in the text box. For more information on smart link, see the"Smart Link" section on page 7-44.
  - Post Body- To send notification to the API using the post body method. If you choose this method, an additional field appears where you can mention the content that must be included in the notification sent to the API.

- In the URI text field, enter the URI for the API. You can include additional details of the customers in the notification message using the smart links. Click the Add Variable drop-down list or "$" in the text box to view the variables. For more information on smart link, see the"Smart Link" section on page 7-44.

Note Only those smart link variables that you have configured to capture using the Data Capture module in the portal are included in the notifications.

Note The summary of the rule is shown on the right side of the page.

Step 9 Click **Save and Publish**.

The rule gets published and listed in the Captive Portal Rules page.

Note If you do not want to publish the rule now, you can click the Save button. You can publish the rule at any time later by clicking the Save and Publish button. Also, you can publish the rule by clicking the Make Rule Live icon at the far right of the rule in the Captive Portal Rules page.

Example

XYZ is a business group that is engaged in different stream lines of business from mobile stores to super markets. XYZ has 5 mobile stores and 4 supermarkets at various locations in New York.The SSID of XYZ in New York is XYZID. XYZ wants to show a captive portal C1, that displays the offers available for various items in the super market, when the customers connect to XYZID from XYZ's super markets. Similarly, a captive portal, C2, must be shown to customers who connect to the XYZID from XYZ's mobile stores. The captive portal must be shown to the customers that are not opted in.

Locations with super markets: L1, L2,L3,L4, L5

Locations with mobile stores: L7, L8, L9, L10

To achieve the preceding scenario, perform the following steps:

Step 1 In the Meraki, enable the SSID, XYZID. For more information on enabling the SSID in the Meraki, see the Enabling the SSIDs in the Meraki, page 4-2.

Step 2 Log in to the CMX Engage.

Step 3 Add XYZID to the CMX Engage using the Import SSID option.

Step 4 Create the location hierarchy for XYZ. In the location hierarchy, all the supermarkets and mobile store of XYZ in New York must be defined as locations under the location, New York. Add a location metadata for the locations L1, L2, L3, L4, and L5 with key as **StoreType** and value as **SM**. Add a location metadata for the locations L7, L8, L9, and L10 with key as **StoreType** and value as **MS**. For more information on defining the location metadata, see the "Defining Metadata for a Location" section on page 3-7.

Step 5 Create portal **C1** for super market and portal **C2** for mobile stores. For more information on creating the portals, see the "Creating the Portals" section on page 4-4.

Step 6 In the CMX Engage dashboard, choose **Proximity Rules > Captive Portal Rule**.

Step 7 Click **Create a new rule**.

Step 8 In the RULE NAME field, enter the name, **R1**, for the captive portal rule.

Step 9 From the "When a user is on" drop-down list, choose **WiFi**, and from the "and connected to" drop-down list, choose **XYZID**.

Step 10 In the Locations area, perform the following steps:

a. Click the **Add Locations** button, and in the Choose Location window that appears, select the location for New York, and click **OK**.

b. Select the Filter by metadata check box, and click the **Add Metadata** button for Filter.

c. In the Choose Location Metadata window, choose the key, **StoreType**, and choose the value **SM**.

Note As the location metadata "StoreType" is defined for the locations that are under the location "New York", it will be available for selection in the Enter Location Metadata window.

Step 11 In the Identify area, select the Filter by OptIn Status check box, and from the Only for drop-down list, choose **not Opted In Users**.

Step 12 In the Schedule area, select the Set a date range for the rule check box, and specify the start date as today's date and end date as last date of this year.

Step 13 In the Actions area, from the Show Captive Portal drop-down list, choose **C1**.

Step 14 Click **Save and Publish**.

The rule gets published.

Step 15 Similarly, create another rule, **R2**, for the Mobile Group, with the location metadata key as **StoreType** and value as **MS**, and the captive portal, **C2**.

Now, when a customer visits XYZ's super market and connects to XYZID, **C1** is shown. When the same customer connects to XYZID from XYZ's mobile store, **C2** is shown.

Synchronizing with the Meraki

If there is any CMX Engage configuration update that is not synchronized with the Meraki network for an SSID, a red indicator appears against the SSID in the SSIDs window. Click the Sync link to synchronize. After synchronization, the indicator turns green.

Advanced Configurations for the SSID

The CMX Engage displays whether a radius server from the CMX Engage or a captive portal created using the CMX Engage Studio is configured for an SSID. If either of these, or both of these are configured for an SSID, then an Advanced Configuration With Meraki message appears against that SSID in the Actions column of the SSID window.

In addition, for the radius server configuration, the Radius Server Configuration message appears in the Remarks column. Similarly, for an CMX Engage Studio portal configuration, the details of the CMX Engage Studio Portal configuration appear in the Remarks column of the SSID. A green indicator is shown for each of these configurations.

If the Radius server or captive portal configured is not of the CMX Engage, the sync option appears in red.

You can revert the advanced configurations for an SSID by clicking the corresponding Revert to Basic Config button. Then, the CMX Engage captive portal gets configured for that SSID.

Manually Configuring the SSIDs

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

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

Step 1 Go to meraki.cisco.com.

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

Step 3 Choose the required Meraki organization and network from the respective drop-down list.

Step 4 Choose **Wireless > Access Control**.

Step 5 From the SSID drop-down list, choose the SSID that you want to configure for the CMX Engage.

Step 6 In the splash page area, choose **Click-through**.

Step 7 From the Wall garden drop-down list, choose **Wall garden is enabled.**

Step 8 In the Wall garden ranges text field, enter the required wall garden ranges.

To view the wall garden ranges, in the CMX Engage dashboard, choose SSIDs, and then click the Configure SSIDs Manually? link.

Step 9 Click **Save Changes.**

Step 10 Go to **Wireless > Splash page**.

Step 11 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 SSIDs, and then click the "Configure SSIDs Manually?" link.

Step 12 Click **Save Changes**.

Step 13 Repeat steps 4-12 for all the SSIDS that you want to use in the CMX Engage.