
# 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 internet 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.You can restrict the duration for which internet must be provided for each session. Also, you can define the bandwidth required for the internet for this captive portal rule.
- 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.

# Pre-requisites for Creating a Captive Portal Rule

- To specify the locations for which the captive portal rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the "Location Hierarchy" section on page 3-1.
- For CUWN-CMX, ensure that all the required APs are added to the CMX.
- To specify the SSID for which you want to display the captive portal, you must import the SSIDs created in your wireless network system to the CMX Engage. For more information on importing the SSIDs, see "Importing the SSIDs" section on page 4-2.
- To display a captive portal based on the captive portal rule, you must create the portal. For more information on creating the captive portal, see "Creating a Portal" section on page 8-1.
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see "Creating or Modifying Tags Using a Profile Rule" section on page 7-1.
- To send to an external API the details such as first name, last name, and so on of the customers who have signed into the captive portal, you must configure the Data Capture form in the captive portal. Without the Data Capture form, only the information such as device mac address will be sent to the external API. For more information on configuring a data capture form, see "Adding a Data Capture Form to a Portal" section on page 8-12.
- To manage internet provisioning and radius-authentication, do the required configurations in your wireless network.
  - If your wireless network is Meraki, do the configurations mentioned in "Configuring the Meraki for Radius-Authentication" section on page 3-2.
  - If your wireless network is CUWN, do the configurations mentioned in"Configuring the CUWN for Internet Provisioning and Radius-Authentication" section on page 15-8.

# Creating a Captive Portal Rule

Before creating a captive portal rule, ensure that all the pre-requisites are met. To know the pre-requisites for creating a captive portal rule, see "Pre-requisites for Creating a Captive Portal Rule" section on page 5-2.

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, first time or repeat user, 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 time with in a particular period, and only for certain days of a week. 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 a Captive Portal 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.

**Note** For CUWN-CMX, ensure that all the required APs are added to the CMX for the Captive Portal rules to function. After defining the location hierarchy, if you are adding new APs to the CMX, the newly added APs get automatically displayed in the location hierarchy.

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 apply the rule.

**Note** The SSIDs are available for selection only if you have imported/configured the SSIDs. If the required SSID is not imported/configured, you can import/configure it using the Configure SSID button listed in the drop-down list. When you select the Configure SSID button, you are redirected to the Import/ Configure SSID window. For more information on importing/configuring the SSIDs, see the "Importing the SSIDs" section on page 4-2.

**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 locations such as group, floor, or zone. You can add the locations of both Meraki and CUWN in a Captive Portal rule. For more information on creating the location hierarchy, see the."Defining the Location Hierarchy" section on page 3-2.

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 or Editing Metadata for a Location" section on page 3-20. You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the "Filtering by Location" section on page 5-9.

**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 the on-boarding status of the customer, 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 based on the on-boarding status of the customer, select the "Filter by On boarding Status" check box. If you want to filter the on-boarded customers (the customers who have completed the authentication process) for the rule, choose the **Onboarded Visitor** radio button. If you want to filter the customers who have not on-boarded (the customers who have not completed the authentication process) for the rule, choose the **Not Onboarded Visitor** radio button.

**b.** If you want to filter the customer by the Opt In Status, select the "Filter by Opt-In Status" check box, and choose whether you want to filter the opted in users or not opted in users. For more information on opted in users, see the"Opted In Users" section on page 7-6.

**c.** 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 7-4.

**d.** 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, specify 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 that you can configure, see the "Previous Visit Criteria" section on page 6-9.

**e.** If you want to filter the customers based on the customer's app status, select the **Filter by App Status** check box, and choose the app status for which the rule is applicable.

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

**f.** 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.

**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.** 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, configure 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 "Select Captive Portal" drop-down list, choose the captive portal that you want to show when the conditions defined in this rule are met.

  If you want to limit the period for which internet is to be provided for a session, select the "Session Duration" check box, and in the text field that appears enter the session duration. You can specify the session duration in minutes, hours, or days.

  If you want to restrict the bandwidth for the internet provided for the customers based on this captive portal rule, select the Bandwidth check box, and in the bandwidth bar that appears, specify the bandwidth. You can define the bandwidth within a range of 1 kbps and 1 tbps.

**Note** The portals that you have created for the chosen locations are available for selection. If you have not created the required portal, you can create it using the "Create Portal" button that is available in the "Select Captive Portal" drop-down list. When you select the "Create Portal" button, you are redirected to the Create Portal window. For more information on creating a portal, see the "Creating a Portal" section on page 8-1.

- **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 your wireless network such as CUWN or Meraki as mentioned in the "Pre-requisites for Creating a Captive Portal Rule" section on page 5-2. The text fields that is to be entered for this option depends on your wireless network.
  - In the Rule/Policy Name field, enter a name for the policy. You must specify the same name that you have defined in the Wireless Network.

**Note** This field is not required for the CUWN.

  - In the Session Duration field, mention the duration for which the you want to provide the internet access for each connection.
  - In the Bandwidth Limit field, choose the bandwidth to be provided. You can choose a maximum bandwidth of 1 tbps.

**Note** The bandwidth field is not required for Meraki as the bandwidth configured in the Meraki will be 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 "Filtering by Tag" section on page 7-4".

**c.** If you want to send to an external API the details such as first name, last name, mobile number, and so on of the customers who have signed up to the captive portal configured for this rule, select the Trigger API check box, and do the necessary API configurations. For more information on API configurations, see the"Trigger API Configurations" section on page 5-10.

**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.

# Use Case- Captive Portal Rule

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 users 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 WLC, define the mode for access points, create the ACLs, and create the SSID, XYZID. For more information on the WLC configurations, see the Configuring Access Point Mode, SSIDs, ACLs, Splash URLs , and Virtual Interface in the WLC, page 15-1.

**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 or Editing Metadata for a Location" section on page 3-20.

**Step 5** Create portal **C1** for super market and portal **C2** for mobile stores. For more information on creating the portals, see the "Creating a Portal" section on page 8-1.

**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 “Choose Location Metadata” window.

**Step 11** In the Identify area, select the **Filter by Opt-In Status** check box, and choose **Only for not opted-in Visitor**.

**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, choose **Show Captive Portal,** and from the “Select 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.

# Managing the Captive Portal Rules

You can pause a captive portal rule, and make it live again, whenever required. You can modify a captive portal rule, and delete it if required. You can also view the captive portal rules configured for a location.



## Pausing a Captive Portal Rule

To pause a captive portal rule, perform the following steps:

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

The captive portal rules created get listed.

**Step 2** Click the **Pause Rule** icon that appears at the far right of the captive portal rule that you want to pause.

The captive portal rule is paused.

**Note** To pause multiple captive portal rules, select the check box for the captive portal rules that you want to pause, and click the Pause button that appears at the bottom of the page.

# Restarting a Captive Portal Rule

To restart a captive portal rule, perform the following steps:

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

The captive portal rules created get listed.

**Step 2** Click the **Make Rule Live** icon that appears at the far right of the captive portal rule that you want to restart.

The captive portal rule is restarted.

**Note** To restart multiple captive portal rules, select the check box for the captive portal rules that you want to restart, and click the "Make Live" button that appears at the bottom of the page.

# Modifying a Captive Portal Rule

To modify a captive portal rule, perform the following steps:

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

The captive portal rules created get listed.

**Step 2** Click the **Edit Rule** icon for the captive portal rule that you want to modify.

**Step 3** Make necessary changes.

**Step 4** To save the changes, click **Save** or to publish the changes, click **Save and Publish**.

**Note** A live rule will have only the "Save and Publish" option. When you click the "Save and Publish" button, the rule gets published with the changes.

# Deleting a Captive Portal Rule

To delete a captive portal rule, perform the following steps:

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

The captive portal rules created get listed.

**Step 2** Click the **Delete Rule** icon that appears at the far right of the captive portal rule that you want to delete.

**Note** To delete multiple captive portal rules, select the check box for the captive portal rules that you want to delete, and click the Delete button that appears at the bottom of the page.

# Viewing the Captive Portal Rules for a Location

To view a captive portal rule for a location such as group, building, floor, and so on, perform the following steps:

**Step 1** In the CMX Engage dashboard, choose **Manage Locations**.

The Locations page appears with the location hierarchy.

**Step 2** Click the **Proximity Rules** icon for the location for which you want to view the captive portal rule.

**Step 3** Click the **Captive Portal Rule** tab.

The captive portal rules for the location gets listed.

**Note** The "Proximity Rules" link for a location is enabled only if atleast one proximity rule exists for that location.

## Filtering by Location

For the Proximity Rules such as Captive Portal Rule, Engagement Rule, and Profile Rule, you can filter the locations in which you want to apply a rule. You can also filter the locations by the metadata defined for the selected locations.

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 rule.

**c.** Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

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 choose 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 choose the value for the variable in the adjacent field.

d. Click **OK**.

## Trigger API Configurations

To configure to send notifications or customer details to an external API through the proximity rules, perform the following steps:

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

**Note** You can include the data such as first name, last name, and so on of the customer in the notification message or the customer details sent to the API by adding the smart link variables in the API URI or by adding variables in the method parameters.

  - Get- To send notification or customer details 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. You can add the request parameter keys defined in your API, and mention the values for them using variables. The value can be a hard-coded value or a variable. You can add a variable using the adjacent "Add Variable" drop-down list or by entering "$" in the value field. For more information on variables, see the"Smart Links And Text Variables" section on page 8-44. You can add more "get parameters" using the **add** button.
  - Post Form- To send notification or customer details to the API using the POST FORM method. If you choose this method, additional fields appear where you can mention the form parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the form parameter keys defined in your API, and mention the values for them. The value can be a hard-coded value or a variable. You can add a variable as a form parameter variable using the adjacent Add Variable drop-down list or by entering "$" in the value field. For more information on variables, see the"Smart Links And Text Variables" section on page 8-44. You can add more "form parameters" using the **add** button.
  - Post Json- To send notification or customer details 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 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 Variabl"e drop-down list, or by entering "$" in the text box. For more information on variables, see the"Smart Links And Text Variables" section on page 8-44.
  - Post Body- To send notification or customer details 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 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 or customer data sent to the API using the smart links. Click the “Add Variable” drop-down list or “$” in the text field to view the smart link variables that you can add. For more information on smart link, see the“Smart Links And Text Variables” section on page 8-44

**Note** Only those data that you have configured to capture using the Data Capture form in the portal are included.