



Captive Portal Rule

- [Captive portal rule, on page 1](#)
- [Prerequisites for creating a captive portal rule , on page 2](#)
- [Create a captive portal rule to display captive portals, on page 2](#)
- [Use case: captive portal rule, on page 6](#)

Captive portal rule

A captive portal rule is a WLAN management feature that

- enables you to configure how the captive portal is displayed and how internet access is provisioned for customers connecting to specific SSIDs, and
- allows selection among different access modes such as Show Captive Portal, Direct Internet Access, or Deny Internet Access.
- **Show Captive Portal:** When a customer who meets the rule filters connects to the configured SSID, a captive portal appears. The customer can access the internet by selecting any menu item in the portal after completing the required authentication steps. You can configure different captive portals to suit customers based on their location, visit frequency, associated tags, visit duration, and other criteria. You can restrict internet access duration for each session and specify the bandwidth for the captive portal rule.
- **Direct Internet Access:** When a customer meeting the rule criteria connects to the configured SSID, internet access is provided immediately without authentication. The captive portal does not appear in this scenario.
- **Deny Internet Access:** When a customer who meets the rule criteria tries to connect to the SSID, the connection cannot be established because internet access is denied.

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

- Create tags or modify existing tags based on rule filtering.
- Send the details of customers 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.

Prerequisites 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, refer to the [Overview of Location Hierarchy](#) section.
- With the **CMX On Prem** option, add all required APs to Cisco 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 Cisco Spaces.
- To display a captive portal based on the captive portal rule, you must create the portal. For more information on creating the captive portal, refer to the [Create and manage portal](#).
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, refer to the [Creating or Modifying Tags Using a Location Personas App](#) section.
- 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, refer to the [Add a data capture form to a portal](#).
- RADIUS authentication is highly recommended for captive portals. RADIUS authentication is mandatory for **Seamlessly Provision Internet**, **Deny Internet**, and allowing users to define **Session Duration** and **Bandwidth**. Configure your wireless network to manage internet provisioning and RADIUS authentication.
 - If your wireless network is Meraki, do the configurations mentioned in [Configuring Cisco Meraki for RADIUS Authentication](#).
 - If your wireless network is CUWN (Cisco AireOS), do the configurations mentioned in [Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication](#).
 - If your wireless network is Cisco Catalyst 9800 Series Controller, do the configurations mentioned in [Captive Portal with RADIUS Server on DNA Spaces](#).

Create a captive portal rule to display captive portals

Enable administrators to define rules in Cisco Spaces that control captive portal behavior, allocate internet access, and trigger actions for specific user and location conditions.

Before creating a captive portal rule, ensure that all the prerequisites are met. To learn about the prerequisites for creating a captive portal rule, refer to the [Prerequisites for creating a captive portal rule](#) , on page 2.

You can filter the customers to whom you want to apply the rule based on their location, opt-in status, tag membership, whether they are first-time or repeat users, and the number of visits made by the customer. You can filter the locations to which the rule applies based on either the locations themselves or their associated metadata. You can also 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 the rule to apply only during specific times within a given period and only on certain days of the week.

The Captive Portal Rule also allows you to configure direct internet access when the filtered customers connect to your SSID. In this case, the captive portal is not displayed, but the customer will get access to the internet. You can configure the Captive Portal Rule to deny internet access to the filtered customers.

With a Captive Portal Rule, you can create new tags or modify existing tags for the filtered customers. 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 If Cisco Wireless Controller is connected through Cisco CMX, ensure that all the required APs are added to the Cisco CMX for the Captive Portal rules to function. After you define the location hierarchy and add new APs to Cisco CMX, they are automatically displayed in the location hierarchy.

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

Procedure

- Step 1** In the Cisco Spaces dashboard, click the **Captive Portal** app.
- Step 2** In the **Captive Portal** window that appears, click **Captive Portal Rule** in the left pane of the dashboard.
- Step 3** Click **Create New Rule** on the far right of the window. In the **Rule Name** field, enter a name for the captive portal rule.
- Step 4** In the Sense area, perform these steps:
- From the drop-down list after **When a user is on WiFi**, select **WiFi**.
 - From the drop-down list after **and connected to**, select the SSID for which you want to apply the rule.
- Note**
SSIDs are available for selection only if they have been imported or configured. If the required SSID is not imported or configured, you can import or 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.
- Step 5** In the Locations area, specify the locations where you want to apply the rule.
- You can configure the rule for the entire location hierarchy or for one or more locations, such as a group, floor, or zone. You can add the locations of both Meraki and CUWN in a Captive Portal rule. For details on creating the location hierarchy, see the [Overview of Location Hierarchy](#) section.
- 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, refer to the Defining or Editing Metadata for a Location section. 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, refer to the [Filter by location](#).
- 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, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.
- To specify the customers to whom the Captive Portal rule applies, complete these steps:
- To filter customers based on their onboarding status, check the Filter by Onboarding Status box. To filter by onboarded customers (those who have completed authentication), select the **Onboarded Visitor** option. If you want to filter the

customers who have not on-boarded (the customers who have not completed the authentication process) for the rule, click the **Not Onboarded Visitor** radio button.

- b) To filter customers based on opt-in status, check the **Filter by Opt-In Status** check box, and specify to include opted-in or not opted-in users. For more information on opted in users, see the "Opted In Option for Users" section on page 6-5.
- c) If you want to filter the customers based on tags, check the **Filter by Tags** check box.

Note

You can filter the tags in two different ways. You can specify either the tags to include in the rule or those to exclude from it. 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 exclude specific tags from the rule, use the **Add Tags** button for **Exclude**.

For more information on using the tag filter, refer to the Filtering by Tag section.

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

Click the **Add Locations** button. In the **Choose Locations** 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, refer the Previous Visit Criteria section.

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

- a) Check 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.
- b) Check 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.
- c) If you want to apply the rule only on particular days, check 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 internet provisioning for customers filtered by the rule, choose from these options:
 - **Show Captive Portal:** Select this option to display a captive portal when customers filtered by the Captive Portal rule connect to the configured SSID. From the **Select Captive Portal** drop-down list, select the captive portal to display when the rule's conditions are met.

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, refer to the [Create a portal](#).

- If you want to limit the period for which internet is to be provided for a session, check the **Session Duration** check box, and in the 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, check 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 session duration defined here overrides the session expiry configuration in your wireless network such as Cisco Wireless Controller or Meraki. This option allows you to set a longer session duration for a captive portal than the default in your wireless network.

- **Seamlessly Provision Internet:** Select this option to provide customers with internet access immediately after connecting 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 Cisco Wireless Controller or Meraki as mentioned in the [Prerequisites for creating a captive portal rule](#), on page 2. The data that is to be entered for this option depends on your wireless network.
 - In the Rule/Policy Name field, enter the name used in your wireless network. You must specify the same name that you have defined in the Wireless Network.

Note

This field is not required for the Cisco Wireless Controller or Cisco 9800 Series Wireless Controllers.

- To specify the session duration, check the Session Duration check box, and in the **Enter Session Duration** field, mention the duration for which the you want to provide the internet access for each connection.
- To specify the bandwidth, check the Bandwidth the Limit check box, and specify the bandwidth using the bandwidth bar that appears. You can specify a maximum bandwidth of 1 tbps.

You can also use the **Show Manual Configuration** option to manually enter the bandwidth allowed for a Captive Portal Rule. This option enables you to configure the exact bandwidth you want to set rather than the predefined values. You can specify the bandwidth in KBPS, MBPS, GBPS, or TBPS.

Note

The bandwidth field is not required for Meraki as the bandwidth configured in Cisco Meraki will be considered.

- **Deny Internet:** Select this option to deny internet access to customers filtered by the rule when they attempt to connect to your SSID. In this case, the customers are not allowed to connect to the SSID.
- To create a tag for customers filtered by this Captive Portal Rule, or to add or remove 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.
 - To send details (such as first name, last name, and mobile number) of customers who have signed up for the captive portal configured for this rule to an external API, check the **Trigger API** check box and complete the necessary API configurations. For more information on API configurations, refer to [Trigger API Configuration for Notification](#).

Note

The summary of the rule is shown on the right side of the window.

Step 9 Click **Save and Publish**.

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

Note

If you do not want to publish the rule now, you can click the **Save** button. To publish the rule later, open it and click the **Save and Publish** button. You can also publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the **Captive Portal Rules** window.

Use case: captive portal rule

Display targeted offers to visitors in XYZ's supermarkets and mobile stores by customizing captive portal rules based on location and store type.

XYZ is a business group engaged in various businesses, including mobile stores and supermarkets. XYZ has five mobile stores and four supermarkets at various locations in New York. The SSID name 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 supermarket, when the customers connect to XYZID from XYZ's supermarkets. Similarly, a captive portal, C2, must be shown to customers who connect to XYZID from XYZ's mobile stores. The captive portal must be shown to users who have 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 these steps:

Procedure

-
- Step 1** In the Cisco Wireless Controller, define the mode for APs, create the ACLs, and create the SSID, XYZID. Log in to Cisco Spaces and add XYZID to Cisco Spaces using the Import SSID option.
- Step 2** 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, refer to the [Adding Metadata for a Location](#) section.
- Step 3** Create portal **C1** for supermarket and portal **C2** for mobile stores. For more information on creating the portals, refer to the [Create a portal](#). In the Cisco Spaces dashboard, choose **Home**.
- Step 4** In the window that appears, choose **Captive Portal**. In the **Captive Portal** window, choose **Captive Portal Rule** in the left pane. Click **Create New Rule**.
- Step 5** In the **RULE NAME** enter the name, **R1**, for the captive portal rule. From the **When a user is on** drop-down list, select **WiFi**, and from the **add Connected to** drop-down list, select **XYZID**.
- Step 6** In the Locations area, perform these steps:
- Click the **Add Locations** button, and in the **Choose Locations** window that appears, select the location for New York, and click **Ok**.
 - Check the **Filter by metadata** check box, and click the **Add Metadata** button for Filter.
 - 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 is available for selection in the **Choose Location Metadata** window.
- Step 7** In the Identify area, check the **Filter by Opt-In Status** check box, and choose **Only for not opted-in Visitor**. In the Schedule area, check 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 8** In the Actions area, choose **Show Captive Portal**, and from the **Select Captive Portal** drop-down list, select **C1**. Click **Save and Publish**.

The rule gets published.

Step 9

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.
