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 a Captive Portal Rule

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

1. Configuring the Mode for Access Points, Create SSIDs ,and Create ACLS in the Wireless LAN Controller (WLC), page 4-2
2. Configuring the CUWN for Internet Provisioning and Radius-Authentication, page 4-2
3. Accessing the CMX Engage, page 3-2
4. Manually Importing the SSIDs, page 4-3
5. Defining the Location Hierarchy, page 3-2

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

Note You need to have the CUWN accounts (CMX and WLC) and CMX Engage accounts to configure the captive portals. The CUWN properties are configured in the Wireless LAN Controller (WLC).

Configuring the Mode for Access Points, Create SSIDs ,and Create ACLS in the Wireless LAN Controller (WLC)

To create a Captive Portal rule, you must initially define the mode for access points, and create the SSIDs and ACLs in the Wireless LAN Controller. For more information on the WLC configurations required to configure captive portals, see the "Wireless LAN Controller Configurations" section on page 4-10.

Configuring the CUWN for Internet Provisioning and Radius-Authentication

To provide an additional layer of security for your portal, the CMX Engage supports radius-authentication for the internet provisioning on the captive portals. Also, certain configurations are required in the CUWN to manage the internet provisioning.To use the captive portal rules, you must do the following configurations in the CUWN:

Step 1 Log in to WLC with your WLC credentials.

Step 2 In the WLC main window, click the **Security** tab.

Step 3 Choose **Radius > Authentication**.

Step 4 Click **New**.

Step 5 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

- Port Number:1812

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 6 Choose **Radius > Accounting**

Step 7 Click **New**.

Step 8 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

- Port Number: 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 In the WLC main window, click the **WLANs** tab.

Step 10 Click the WLAN of the SSID for the Captive Portal rule.

Step 11 Choose **Security**.

Step 12 In the Layer 2 tab, select the **MAC Filtering** check box.

Step 13 In the Layer 3 tab, ensure that the following is configured.

- In Layer 3 security drop-down list, **Web Policy** is selected, and the **On Mac Filter Failure** radio button is selected.

Note These configurations in the Layer 3 are done when creating the SSIDs.

Step 14 In the AAA Servers tab, in the Radius Servers area, do the following:

a. Select the **Enabled** check box for the Authentication Servers.

b. From the Server 1 drop-down list, choose the radius server you have previously defined.

Step 15 In the Authentication priority order for the web-auth user area, in the Order Used for Authentication box, set **Radius** as first in the order.

Note Use the Up and Down buttons to rearrange the order.

Step 16 Click the **Advanced** tab, and select the **Enabled** check box for Allow AAA Override.

Step 17 Click **Apply**.

Step 18 In the WLC main window, click the Security tab.

Step 19 Choose **AAA > Mac Filtering**.

Step 20 In the MAC Filtering page that appears, do the following:

a. From the RADIUS Compatibility Mode drop-down list, choose **Cisco ACS**.

b. From the MAC Delimiter drop-down list, choose **Hyphen**.

c. Click **Apply**.

Step 21 Ensure that the wall gardens are configured for the ACLs. For more information on configuring the wall gardens, see the "Wireless LAN Controller Configurations" section on page 4-10.

Accessing the CMX Engage

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

Manually Importing the SSIDs

The SSID refers to the network ID that you connect to access the internet through Wi-Fi. To create a Captive Portal rule for an SSID of the CUWN, you need to manually import that SSID from the Wireless LAN Controller (WLC).

Note For CUWN, you must manually import the SSIDs to the CMX Engage. The SSID name you specify in the CMX Engage must match with the SSID name configured in the WLC. You can view the SSID name in the WLC. To add an SSID to the CMX Engage, you must initially define that SSID in the Wireless LAN Controller (WLC). To know how to create the SSID in the WLC, see the "Wireless LAN Controller Configurations" section on page 4-10.

Note The SSIDs are configured in the WLC not in the CMX.

To manually import the SSIDs to the CMX Engage, perform the following steps:

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

Step 2 In the Please Select SSID To Import window, enter the name of the SSID you need to import, and click **Add SSID**.

The imported SSID appears in the SSIDs window.

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

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.

To know how to create a portal, see "Creating a Portal" section on page 7-1.

Note This step is required only if you want to configure a portal for the Captive Portal 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 CUWN 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 "Manually Importing the SSIDs" section on page 4-3.

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 campus, group, building, floor, or zone. 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 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 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**.

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

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 customer 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 to filter the 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 6-5.

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 5-18.

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 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.

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 a Portal" section on page 7-1.
- **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 the "Seamlessly Provision Internet" option, ensure that you have done the required configurations in the WLC. For more information on the configuration required in the WLC, see the "Configuring the CUWN for Internet Provisioning and Radius-Authentication" section on page 4-2.
  - 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 Rule/Policy Name is not required if your wireless network is CUWN.

- **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 6-5".

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 "$" in the value field. For more information on smart link, see the"Smart Link" section on page 7-45. You can add more "get parameters" using the **add** button.
  - Post Form- To send notification to the API using the post form method. If you choose this method, additional fields appear where you can mention the form parameters, to include additional details such as first name, last name, mobile number, and so on of the customer in the notification. You can add the form parameter keys defined in your API and mention the values for them.The value can be a hard-coded value or a variable. You can add a variable as a form parameter variable using the adjacent Add Variable drop-down list or by entering "$" in the value field. For more information on smart link, see the"Smart Link" section on page 7-45.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 7-45.
  - 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 7-45

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.

The captive portal rule is published.

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 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 Wireless LAN Controller Configurations, page 4-10.

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 4-5.

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 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.

Wireless LAN Controller Configurations

The CUWN configurations are done in the WLC. The WLC configurations for the local and flexconnect modes are different.

- Local Mode Configurations for Using the CMX Engage, page 4-11
- FlexConnect Mode Configurations for Using the CMX Engage, page 4-14

Note The configurations are done in the WLC that is not a part of the CMX Engage, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

Note The SSIDs and ACLs are created in the WLC and not in the CMX.

Local Mode Configurations for Using the CMX Engage

To configure the WLC to use the CMX Engage in the local mode, perform the following steps:

1. Configure the Local Mode for an Access Point, page 4-11
2. Create the Access Control Lists, page 4-11
3. Create the SSIDs in the CUWN, page 4-12
4. Configure the Virtual Interface, page 4-13

Configure the Local Mode for an Access Point

To configure a local mode for an access point, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials.

Step 2 In the WLC main window, click the **WIRELESS** tab.

All of the access points are listed.

Step 3 Click the access point for which you want to configure the mode to local.

Step 4 Click the **General** tab.

Step 5 From the AP Mode drop-down list, choose **local,** and click **Apply**.

Create the Access Control Lists

To create the access control list, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials.

Step 2 Choose **Security > Access Control Lists > Access Control Lists**.

Step 3 To add an ACL, click **New**.

Step 4 In the New page that appears, enter the following:.

a. In the Access Control List Name field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b. Choose the ACL type as **IPv4**.

c. Click **Apply**.

Step 5 When the Access Control Lists page reappears, click the name of the new ACL.

Step 6 In the Edit page that appears, click **Add New Rule**.

The Rules > New page appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the CMX Engage, click the Configuration Instructions link in the SSIDs window.

When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication.To know the wall garden ranges that you must configure for social authentication, see "Configuring the CUWN for Social-Authentication" section on page 7-31.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Create the SSIDs in the CUWN

Note The SSIDs are created in the WLC, not in the CMX.

To create the SSIDs in the WLC, perform the following steps:

Step 1 In the WLC main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.

Step 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The Edit "SSID Name" page appears.

Step 5 In the General tab, unselect the Broadcast SSID check box.

Step 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.

Step 7 In the **Layer 3** tab, do the following configurations:

a. From the Layer 3 security drop-down list, choose **Web Policy**.

b. Choose the **On Mac Filter Failure** radio button.

c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL previously defined.

d. Select the Enable check box for the Sleeping Client.

e. Select the Enable check box for the Override Global Config.

f. From the Web Auth Type drop-down list, choose **External (Redirect to External Server)**.

g. In the URL field that appears, enter the CMX Engage splash URL.

To view the splash URL for your CUWN account, in the CMX Engage, click the Configuration Instructions link in the SSIDs window.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**, and **c**lick **Apply**.

Step 10 In the General tab, select the Enabled check box for the Status and Broadcast SSID options, to enable the SSID.

Step 11 Execute the following command in the command prompt to disable captive bypassing. Then, restart the WLC.

config network web-auth captive-bypass disable

Step 12 Choose **Management > HTTP-HTTPS**.

Step 13 In the HTTP-HTTPS configuration page that appears, do the following:

a. From the HTTP Access drop-down list, choose **Disabled**.

b. From the HTTPS Access drop-down list, choose **Enabled**.

c. From the WebAuth SecureWeb drop-down list, choose **Disabled**.

d. Click **Apply**.

Step 14 Choose **Security> Web Auth> Web Login Page**, and ensure that the Redirect URL after login field is blank.

Note If you have made any changes to the Management tab, then restart your WLC for the changes to take effect.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose **Controller > Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the Interfaces > Edit page that appears, enter the following parameters:

a. In the IP address field, enter the unassigned and unused gateway IP address, if any.

b. In the DNS Host Name field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c. Click **Apply**.

Note If you have made any changes to the virtual interface, restart your WLC for the changes to take effect.

FlexConnect Mode Configurations for Using the CMX Engage

You can configure FlexConnect for central switch or local switch mode.

- FlexConnect Central Switch Mode, page 4-14
- FlexConnect Local Switch Mode, page 4-14

FlexConnect Central Switch Mode

To configure the WLC to use the CMX Engage in the FlexConnect central switch mode, perform the following steps:

1. Configure the FlexConnect Mode for an Access Point, page 4-14.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 4-15
3. Create the SSIDs in the CUWN for FlexConnect Central Switch Mode, page 4-15
4. Configure the Virtual Interface, page 4-13

FlexConnect Local Switch Mode

To configure the WLC to use the CMX Engage in the FlexConnect local switch mode, perform the following steps:

1. Configure the FlexConnect Mode for an Access Point, page 4-14
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 4-15
3. Create the SSIDs in the CUWN for the FlexConnect Local Switch Mode, page 4-16
4. Configure the Virtual Interface, page 4-13

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode.To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Step 1 In the WLC main window, click the **WIRELESS** tab.

All of the access points are listed.

Note For more details on the access points, see the Wireless LAN Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the AP Mode drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create the Access Control Lists for FlexConnect Central Switch Mode

Create the Access Control List using the same steps as outlined for the local mode. For more information, see the "Create the Access Control Lists" section on page 4-11.

Create the SSIDs in the CUWN for FlexConnect Central Switch Mode

Create the SSID using the same steps as outlined for the local mode. For more information, see the "Create the SSIDs in the CUWN" section on page 4-12.

Create the Access Control Lists for FlexConnect Local Switch Mode

To create the access control list for the FlexConnect local switch mode, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials.

Step 2 Choose **Security > Access Control Lists > FlexConnect ACLs**.

Step 3 To add an ACL, click **New**.

Step 4 In the New page that appears, enter the following:

a. In the Access Control List Name text field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b. Click **Apply**.

Step 5 When the Access Control Lists page reappears, click the name of the new ACL.

Step 6 In the Edit page that appears, click **Add New Rule**.

The Rules > New page appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the CMX Engage, click the Configuration Instructions link in the SSIDs window.

When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication.To know the wall garden ranges that you must configure for social authentication, see "Configuring the CUWN for Social-Authentication" section on page 7-31.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Create the SSIDs in the CUWN for the FlexConnect Local Switch Mode

Note The SSIDs are created in the WLC, not in the CMX.

To create the SSIDs in the CUWN for the FlexConnect local switch mode, perform the following steps:

Step 1 In the WLC main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.

Step 3 In the New page that appears, enter the WLAN details such as, Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The Edit "SSID Name" page appears.

Step 5 In the General tab, unselect the Broadcast SSID check box.

Step 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.

Step 7 In the **Layer 3** tab, do the following configurations:

a. From the Layer 3 security drop-down list, choose **Web Policy**.

b. Choose the **On Mac Filter Failure** radio button.

c. In the Preauthentication ACL area, from the WebAuth FlexACL drop-down list, choose the ACL previously defined.

d. Select the Enable check box for the Sleeping Client.

Note Clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e. Select the Enable check box for the Override Global Config.

f. From the Web Auth Type drop-down list, choose **External**.

g. In the URL field that appears, enter the CMX Engage Splash URL.

To view the splash URL for your CUWN account, in the CMX Engage, click the Configuration Instructions link in the SSIDs window.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**.

Step 10 In the FlexConnect area, select the Enabled check box for FlexConnect Local Switching, and click **Apply**.

Step 11 In the General tab, select the Enabled check box for the Status and Broadcast SSID options, to enable the SSID.

Step 12 Execute the following command in the command prompt to disable captive bypassing. Then, restart the WLC.

config network web-auth captive-bypass disable

Step 13 Choose **Management > HTTP-HTTPS**.

Step 14 In the HTTP-HTTPS configuration page that appears, do the following:

a. From the HTTP Access drop-down list, choose **Disabled**.

b. From the HTTPS Access drop-down list, choose **Enabled**.

c. From the WebAuth SecureWeb drop-down list, choose **Disabled**.

d. Click **Apply**.

Step 15 Choose **Security> Web Auth> Web Login Page**, and ensure that the “Redirect URL after login” field is blank.