Defining Captive Portal Rules to Display Captive Portals

The WiFi Engage enables you to create captive portals and display them to the customers connected to a particular Wi- Fi ID (SSID). In the WiFi Engage, captive portals are displayed to the customers based on the captive portal rules defined.

This chapter describes how to create the captive portal rules that enable you to display the captive portals to the customers when they are connected to a particular SSID.

Configuring the Captive Portals Using the Captive Portal Rule

To configure the captive portal, 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. Accessing the WiFi Engage, page 3-2
3. Manually Importing the SSIDs, page 4-2
4. Defining the Location Hierarchy, page 3-2
5. Creating the Portals, page 4-3
6. Creating Tags, page 4-3
7. Creating a Captive Portal Rule, page 4-3

Note You need to have the CUWN accounts (MSE/CMX and WLC) and WiFi 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 configure the captive portals, 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 4-7.

Accessing the WiFi Engage

The procedure to access the WiFi Engage is described in the "Accessing the WiFi 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 WiFi Engage. The SSID name you specify in the WiFi 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 WiFi 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 4-7.

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

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

Step 1 In the WiFi 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 WiFi 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

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 enhance the portals using the various portal modules provided by the WiFi Engage.

To create a portal, perform the following steps:

Step 1 In the WiFi 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, and click **Create**.

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

Step 3 Add features to the portal using the Portal Modules.

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 WiFi Engage database. The Data Capture module is available for the Hard SMS with Verification Code and E-mail authentication types.

Step 4 Click **Save** to save the changes made to each module.

Creating 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.

Creating a Captive Portal Rule

The Captive Portal Rule refers to the conditions based on which a captive portal is displayed to the customers who is connecting to a particular SSID.

You can configure to show a captive portal for a combination of an SSID, locations, tags, number of visits, and duration.

You can filter the locations in which a captive portal is to be shown based on the locations or the metadata associated with the locations. You can show a portal based on the number of visits made by the customer to the specified locations during the specified time. You can also configure to show a portal only during a particular period, only for certain days of a week, and only during a particular time.

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

Step 1 In the WiFi 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 4-2.

Step 5 In the Locations area, specify the locations for which you want to show the portal.

You can configure to show the portal for the entire location hierarchy, or a single or multiple MSE, 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 also 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 Element" section on page 3-7. You can either show the portal for the locations with a particular metadata or exclude the locations with a particular metadata.

To specify the locations in which you want to show the captive portal, perform the following steps:

a. Click the **+** 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 **+** button.

The Enter 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 **+** button.

The Choose Location Metadata window appears.

c. From the drop-down list, choose the metadata variable.

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 show the captive portal 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 is to be shown, 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 show the captive portal for 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 portal must be shown or you can specify the tags for which the portal must not be shown. You can choose the best filtering method based on your requirement. For example, if you want to show the portal for all 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 show the portal.

- To include the tags so that the portal is shown only to the customers in the selected tags, use the + button for "Include".
- To not show the portal to the customers in the tags that are excluded, use the + 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 Visits** check box.

Click the + 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 customers for which you want to show the portal.

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, from the Show them Portal drop-down list, choose the captive portal that you want to show when the conditions defined are met.

The portals you have created are available for selection. For more information on creating a portal, see the "Creating the Portals" section on page 4-3.

Step 9 Click **Save and Resume**.

The captive portal rule is published.

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

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 4-7.

Step 2 Log in to the WiFi Engage.

Step 3 Add XYZID to the WiFi 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 location elements 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 Element" 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 4-3.

Step 6 In the WiFi 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 + 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 **+** button for Filter.

c. In the Enter Location Metadata window, select the key, **StoreType**, from the drop-down list, and enter 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 them Portal drop-down list, choose **C1**.

Step 14 Click **Save and Resume**.

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 WiFi Engage, page 4-7
- FlexConnect Mode Configurations for Using the WiFi Engage, page 4-11

Note The configurations are done in the WLC that is not a part of the Enterprise Mobility Services Platform, 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 not in the MSE/CMX.

Local Mode Configurations for Using the WiFi Engage

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

1. Configure the Local Mode for an Access Point, page 4-8
2. Create the Access Control Lists, page 4-8
3. Create the SSIDs in the CUWN, page 4-9

4. Configure the Virtual Interface, page 4-10

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 WiFi 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

Create the SSIDs in the CUWN

Note The SSIDs are created in the WLC, not in the MSE/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 **Passthrough** 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**.

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

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

Note You can also configure a Studio URL as the splash URL. For more information on configuring a Studio URL as a captive portal URL, see the "Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL" section on page 7-27.

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.

Radius-authentication Configuration

To provide an additional layer of security for your portal, the WiFi Engage supports radius-authentication for the internet provisioning on the captive portal sites. The radius credentials are autogenerated after the user completes the required workflow for the internet access. Then, the user credentials are passed to the CUWN for the radius-based internet provisioning. The radius server authentication can be enabled for SMS and social authentications. For more information on radius-authentication, see the "Radius-Authentication for the Portals" section on page 7-29.

Note You have to do this configuration only if you need the radius-authentication.

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 WiFi Engage

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

FlexConnect Central Switch Mode

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

1. Configure the FlexConnect Mode for an Access Point, page 4-11.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 4-11
3. Create the SSIDs in the CUWN for FlexConnect Central Switch Mode, page 4-12
4. Configure the Virtual Interface, page 4-10

FlexConnect Local Switch Mode

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

1. Configure the FlexConnect Mode for an Access Point, page 4-11
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 4-12
3. Create the SSIDs in the CUWN for the FlexConnect Local Switch Mode, page 4-12
4. Configure the Virtual Interface, page 4-10

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 4-8.

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 4-9.

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 WiFi 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

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

Note The SSIDs are created in the WLC, not in the MSE/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 **Passthrough** 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 WiFi Engage Splash URL.

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

Note You can also configure a Studio URL as the splash URL. For more information on configuring a Studio URL as a captive portal URL, see the "Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL" section on page 7-27.

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.