Working with the WiFi Engage

This chapter describes the WiFi Engage features and how to create location-specific experience zones. It also describes the bandwidth requirements to deploy Enterprise Mobility Services Platform.

WiFi Engage Features

The WiFi Engage enables you to do the following:

- Develop location-specific experience zones.
- Create portals for the experience zones.
- Edit the portal from the Experience Zone Manager app.
- View reports that help in analyzing the usage, type of users, and performance of an experience zone.
- View details of users for various social network sites like Facebook and Linked In.

Pre-requisites to Deploy the Enterprise Mobility Services Platform

This section describes the port configurations and bandwidth requirements to deploy the Enterprise Mobility Services Platform.

Ports and IP Addresses

The Enterprise Mobility Services Platform is a cloud-based solution and there is no physical installation involved. However, there are certain instances, where the WiFi Engage needs to communicate with the MSE and vise versa. You can establish this connection through a public IP or vpn. In addition, you may have to white-list certain Enterprise Mobility Services Platform IP addresses.

The MSE must be publicly accessible (For a default MSE installation, the ports 80 and 443 must be open) for the following scenarios where the Enterprise Mobility Services Platform has to establish connection to the MSE:

- Connecting to MSE/CMX
- Importing access points
- Enabling maps
- Generating engagement report
- Generating user report
- Using location-based Enterprise Mobility Services Platform modules. For example, Micello WayFinder, Context Aware Container.

Enterprise Mobility Services Platform IP Addresses to White-list

To establish connection between the Enterprise Mobility Services Platform and MSE, you must white-list certain Enterprise Mobility Services Platform IP addresses. To view the IP addresses to white-list, in the WiFi Engage, click the Configuration Instructions link in the Configure > SSIDs window.

Note Contact Cisco for establishing a vpn connection.

Note You don't need to have a publicly resolvable domain name to connect to the Enterprise Mobility Services Platform.

Certain domains must be white-listed in the customer infrastructure so that the MSE instances deployed with in the customer network must be able to communicate to Enterprise Mobility Services Platform analytical and notification servers. To know the domains to be white-listed, in the WiFi Engage click the Configuration Instructions link in the Configure > SSIDs window.

Bandwidth Requirements to Deploy WiFi Engage

The following table lists the response received for various bandwidth and number of users.

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
1 Mbps	1	9.2
	2	10.41
	3	12.18
	4	13.5
	5	16.56
	6	17.84
2 Mbps	1	9.06
	2	9.15
	3	10.48
	4	11.28
	5	12.06
	6	12.34
	7	13.5
	8	15.5
	9	15.7
	10	16.85
	11	17.7
5 Mbps	5	9.34
	10	11.56
	11	11.92
	12	11.51
	13	12.5
	14	12
	15	13.82
	16	13.18
	17	14.91
	18	16.72
	19	15.96
	20	16.98
	21	17.41

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
7 Mbps	25	13.93
	30	15.41
	31	15.21
	32	15.64
	33	16.31
	34	18.92
9 Mbps	30	10.56
	35	12.11
	40	14.79
	41	14.7
	42	13.27
	43	13.93
	44	15.68
	45	16.81
	46	16.13
	47	19.25
11 Mbps	35	9.57
	40	10.07
	50	11.85
	55	13.51
	56	13.96
	57	14.67
	58	15.86
	59	16.36
	60	16.08
	61	17.11

Developing Location-Specific Experience Zones

The WiFi Engage enables you to create location-specific experience zones. Each experience zone provides visitors with a menu of services and content that is specific to the business and relevant to that location or area.

ABC is a leading hotel chain with many hotels around the globe. The hotel provides free WiFi access to all its customers. ABC is WiFi Engage enabled. Mr. White is a businessman and a regular customer of ABC who uses ABC's various hotels during his business trips. Mr. White has to visit New York and London as part of his business trip, and he has booked the hotels of ABC in both these places. When he is in New York, Mr White connects to the internet through ABC's Wi-Fi. Then, a portal is shown that has the tourist spots, shopping centers, local news, and local advertisements of New York. Mr. White travels

to London and accesses ABC's Wi-Fi. Now the portal shown to him has the tourist spots, shopping centers, local news, and local advertisements of London. Similarly, you can provide different experience zones to your customers when they access the same Wi-Fi ID from different locations.

Note The anchor controlled deployment model is not supported.

Note You need to have both the CUWN(MSE/CMX and WLC) and WiFi Engage accounts to create the experience zones. The CUWN properties are configured in the Wireless LAN Controller (WLC).

To develop a location-specific experience zone, perform the following steps:

1. Creating the Access Control and SSIDs in the Wireless LAN Controller, page 2-5
2. Accessing the WiFi Engage, page 2-5
3. Connecting to the MSE/CMX from the WiFi Engage, page 2-6
4. Manually Importing the SSIDs, page 2-7
5. Defining the Locations, page 2-7
6. Adding Access Points to a Location, page 2-8
7. Enabling the Maps for a Location, page 2-11
8. Creating the Portals, page 2-12
9. Developing the Experience Zones, page 2-12

Creating the Access Control and SSIDs in the Wireless LAN Controller

To use the WiFi Engage with the CUWN, you need to do some configurations in the WLC. To know the configurations required in the WLC, see the "Wireless LAN Controller Configurations" section on page 2-14.

Accessing the WiFi Engage

The WiFi Engage dashboard is available to the users through emsp.cisco.com. Cisco provides the user credentials to each customer of the WiFi Engage.

To access the WiFi Engage, perform the following steps:

Step 1 Go to emsp.cisco.com.

Step 2 In the Sign in window, enter the user credentials provided for your Enterprise Mobility Services Platform account, and click the arrow button to sign in.

Step 3 Click the **WiFi Engage** icon.

Note You can directly log in to the WiFi Engage using the URL https://emsp.cisco.com/wifiengage/.

Step 4 From the Select Customer drop-down list, choose the customer name, and click **Proceed**.

Step 5 The WiFi Engage dashboard appears.

Connecting to the MSE/CMX from the WiFi Engage

.You must connect to the MSE/CMX to add the access points to the locations and publish the experience zones.

To connect to the MSE/CMX, perform the following steps:

Step 1 In the WiFi Engage dashboard, click the icon for the Account Settings.

Step 2 In the MSE Settings dialog box that appears, click **MSE Account Settings**.

Step 3 Enter the server IP Address, username, and password for your MSE/CMX account, and click **Switch account**.

Note You need to provide the IP address of a server that is accessible publicly.

Note You can switch to a different MSE/CMX account using the MSE Account Settings button.

Manually Importing the SSIDs

The SSID refers to the network ID that you connect to access the internet through Wi-Fi. To create an experience zone for an SSID, you need to manually import that SSID from the 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 2-14.

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 **Configure > 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 Locations

The WiFi Engage enables you to provide different experience zones for various locations. A location can be defined as a logical grouping of the access points. So, when a Wi-Fi user connects to the internet using the same SSID from different locations, you can provide different experience zones for the user. Define the locations for which you want to create the experience zones.

To define a location, perform the following steps:

Step 1 Choose **Configure > Locations**, and click **Add Location**.

Step 2 In the Add Location window, enter the name of the location, and click **Add**.

The location added appears in the Locations window.

Searching for a Location

If you have a number of locations, you can use the Search option to locate the location. You can search for a location based on the location name or the name or Base Radio MAC address of the access points associated with that location.

To search for a location, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > Locations**.

Step 2 In the Search field, enter the name of the location that you want search for or the name or Base Radio MAC address of the access points that are associated with the location.

The locations are listed based on the search.

Adding Access Points to a Location

When you create an experience zone for a location, that experience zone is available for all of the access points associated with that location. You can add all of the access points in a MSE campus or only the selected access points to a location.

Note The access points added to a location are not available for another location.

Note You need to open the ports 80 and 443 in your firewall to import the access points. For more information, see the "Pre-requisites to Deploy the Enterprise Mobility Services Platform" section on page 2-2.

To add the access points for a location, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > Locations**.

The locations defined appear.

Note You can search for a location using the Search option. You can search for a location by the location name or the name or Base Radio MAC address of the access points associated with that location.

Step 2 Click the **Add access points** link corresponding to the location for which you need to define the access points.

Step 3 In the Access Points window, do the following:

a. From the Select Campus drop-down list, choose the MSE campus of which you want to add the access points.

b. From the Select Building drop-down list that appears, choose the building of which you want to add the access points.

c. From the Select Floor drop-down list that appears, choose the floor of which you want to add the access points.

The access points in that floor appear.

d. Select the access points that you want to add for the location.

e. Click **Add Access Points**.

The access points are added for the location. The total number of access points added appears against the location in the Locations window.

Note If there are no access points added to a location, the Key-In Access Point option appears against the location. You can use this option to add the access points to a location, if you know the name and Base Radio MAC address of the access point. For a location that has at least one access point associated with it, the Key-In Access Point button is available in the page that appears when you click the edit icon for a location.

Adding Access Points in Bulk to a Location

You can add the access points in bulk to the WiFi Engage without connecting to the MSE. You need to import the access point details in a csv file. You can download the csv template using the Export Template button available in the Locations window. After import, the access points get associated to the location that you have specified in the .csv template.

To add the access points in bulk to the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage Dashboard, choose **Configure > Locations**.

Step 2 In the Locations window that appears, click **Export Template**.

Step 3 In the Opening Access Points-Template.csv window that appears, click **Save** to save the template on your computer in the .csv format.

Step 4 Log in to Cisco Prime.

Note The configurations are done in the Cisco Prime 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.

Step 5 Choose **Reports > Report Launch Pad**.

Step 6 In the Report Launch Pad page that appears, choose **Device > AP Summary**.

Step 7 In the AP Summary page that appears, click **New**.

Step 8 In the New AP Summary page, do the following:

a. In the Report Title field, enter a name for the report.

b. From the Report By drop-down list, choose **Floor Area**.

c. In the Report Criteria field, define the criteria **All Campuses >All Buildings >All Floors**.

d. From the SSID list, choose **All SSIDs** or the SSIDs for which you want to generate the report.

e. Click **Run and Save**.

The AP summary report is generated.

Step 9 Click **Save and Export**.

Step 10 In the Export Report page that appears, do the following:

a. From the Export Format drop-down list, choose **CSV**.

b. Click **OK**.

Step 11 In the Export Results page that appears, click the .csv file in the Download column corresponding to the report name.

Step 12 Click **Save** to save the .csv file on your computer.

Step 13 Change the field captions in the .csv file as in the template downloaded earlier from the WiFi Engage.

Note Ensure to use the appropriate field captions for each column. You must change the Access Group Name to Location Name.

Step 14 Delete the additional rows or columns, if any, based on the WiFi Engage .CSV template.

Note Ensure that you associate an access point only with a single location.

Step 15 In the WiFi Engage dashboard, click **Import Template**.

Step 16 In the Import Access Points Template window that appears, click **Upload**.

Step 17 In the File Upload window that appears, choose the .csv file in which you have previously added the access point details, and click **Open**.

The uploaded file name appears in the Import Access Points Template window.

Step 18 Click **Done**.

The access points get added to the WiFi Engage and the “Successfully, access points are imported” message appears in the Locations window.

Deleting an Access Point from a Location

To delete an access point from a location, perform the following steps:

Step 1 In the WiFi Engage Dashboard, choose **Configure > Locations**.

The WiFi Engage locations appear.

Step 2 Click the edit icon adjacent to the location from which you want to delete the access point.

Step 3 In the page that appears, select the access point that you want to delete from the location.

Step 4 Click **Remove access points**.

Enabling the Maps for a Location

You can configure the maps that must appear for various locations. When the user accesses the WiFi Engage from various locations, the corresponding map appears.

To enable a map for a location, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > Maps**.

All of the locations that are added to the WiFi Engage appear.

Step 2 Expand the location for which you need to configure the map.

All of the access points associated with that location appear.

Note The locations with the arrow mark adjacent have access points associated with them.

Step 3 Click the **Change Map** link corresponding to the location for which you need to enable the map.

Step 4 In the Change Map window, configure the map for the location.

You can display the map from the MSE, Micello map, or an external source.

a. To display a MSE map, choose **Mse Map**. The map for this location in the MSE appears along with its name. Edit the name, if required, and click **Save**.

Note To display the MSE map for a location, you need to connect to the MSE and import the access points for that location. Based on the access points associated with a location, multiple maps may be displayed for a location.

b. To display a map from an external source, choose **Upload Map**. Upload the map using the **Upload** button, and enter a name for the map in the Map Name field, and click **Save**.

c. To display a Micello map, choose **Micello map**. Specify the Micello Map ID or Map URL of the map to upload. The map appears along with its name. Edit the name, if required, and click **Save**.

Note To upload a Micello map, you need to have a Micello account. For a Micello account, contact support@micello.com.

Searching the Map for a location

The WiFi Engage enables you to search the map that is configured for a location.

To search the map for a location, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > Maps**.

The Maps page appears.

Step 2 In the Search field, enter the name of the location.

The map for the location appears.

Creating the Portals

A portal is the user interface that appears when a Wi-Fi user is logged into an experience zone. 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 **Create > Portals**, and click **Create New**.

Step 2 Choose a template for the portal.

Navigate using the arrows highlighted in the window to choose the required template.

Step 3 In the Name field, enter a name for the portal, and click **Create**.

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

Step 4 Add features to the portal using the Portal Modules.

Step 5 Click **Save** to save the changes made to each module.

Developing the Experience Zones

An experience zone refers to the portal that appears to a user who accesses the WiFi Engage from a particular location with a specific SSID. The experience zones are created with respect to an SSID, portal, and locations.

To create an experience zone, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > Experience Zones**, and click **+Experience Zone**.

Step 2 In the Add Experience Zone window, add the following details, and click **Add Zone**.

a. From the SSID drop-down list, choose the SSID for which you want to define the experience zone.

b. From the Portal drop-down list, choose the portal that must appear for this experience zone.

c. From the Location area, choose **All Locations** if the experience zone is applicable for all of the locations, or choose **Choose Location**, and specify the locations for which you need to define this experience zone. Then, click **Add**.

d. In the Name field, enter a name for the experience zone, and click **Add Zone**.

Now, the users can view the captive portals on their devices.

Note Ensure that the splash page URL is configured for the SSID. For more information, see the "Create the SSIDs in the WLC" section on page 2-15.

Note Ensure that the Enterprise Mobility Services Platform IP addresses are white-listed in the Wireless LAN Controller. For more information on the Enterprise Mobility Services Platform IP addresses to be white-listed, see the"Enterprise Mobility Services Platform IP Addresses to White-list" section on page 2-2.

Note On an iPhone, within 3 seconds after connecting, the user is automatically taken to the portal for the experience zone.

Note On an Android phone, the user may require to open a browser to view the portal for that experience zone.

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 2-14
- FlexConnect Mode Configurations for Using the WiFi Engage, page 2-17

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 2-14
2. Create the Access Control Lists, page 2-14
3. Create the SSIDs in the WLC, page 2-15
4. Configure the Virtual Interface, page 2-17

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 WLC

Note The SSIDs are created in the WLC not in 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, uncheck 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 3-23.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**, and click **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 Portals" section on page 3-25.

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 2-18.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 2-18
3. Create the SSIDs in the WLC for FlexConnect Central Switch Mode, page 2-18
4. Configure the Virtual Interface, page 2-17

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 2-18
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 2-18
3. Create the SSIDs in the WLC for the FlexConnect Local Switch Mode, page 2-19

4. Configure the Virtual Interface, page 2-17

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 2-14.

Create the SSIDs in the WLC 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 WLC" section on page 2-15.

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 WLC 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 WLC 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 3-23.

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.