Configuring the CUWN for the CMX Engage

This chapter describes the configurations to be done in the CUWN for using the CMX Engage.

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 Access Point Mode, SSIDs, ACLs, Splash URLs , and Virtual Interface in the WLC, page 15-1
- Configuring the CUWN for Internet Provisioning and Radius-Authentication, page 15-8.
- Configuring the CMX for Notifications and Reports, page 15-9
- Configuring the CUWN for Social-Authentication, page 15-11

Configuring Access Point Mode, SSIDs, ACLs, Splash URLs , and Virtual Interface in the 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. You must also ensure that the splash URL for the SSID is configured in the WLC.

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

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

- Local Mode Configurations for Using the CMX Engage, page 15-2
- FlexConnect Mode Configurations for Using the CMX Engage, page 15-5

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.

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

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 dashboard, click the “Setup SSIDs in Meraki/CUWN” link in the SSIDs page, and click the “Configure SSID in CUWN - CMX” tab.

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 Wireless Network for Social-Authentication" section on page 8-29.

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 WLC

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 dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs page, and click the "Configure SSID in CUWN - CMX" tab.

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 15-5
- FlexConnect Local Switch Mode, page 15-5

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 15-5.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 15-5
3. Create the SSIDs in the WLC for FlexConnect Central Switch Mode, page 15-6
4. Configure the Virtual Interface, page 15-4

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 15-5
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 15-6
3. Create the SSIDs in the WLC for the FlexConnect Local Switch Mode, page 15-7
4. Configure the Virtual Interface, page 15-4

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 15-2.

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 15-3.

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 dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs window, and click the "Configure SSID in CUWN - CMX" tab.

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 Wireless Network for Social-Authentication" section on page 8-29.

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 WLC 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 dashboard, click the "Setup SSIDs in Meraki/CUWN" link in the SSIDs window, and click the "Configure SSID in CUWN - CMX" tab.

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.

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**.

The Radius Authentication Servers page appears.

Step 4 From the Auth Called Station ID Type drop-down list, choose **AP MAC Address:SSID**.

Step 5 From the MAC Delimiter drop-down list, choose **Hyphen**.

Step 6 Click **New**.

Step 7 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 8 Choose **Radius > Accounting.**

The Radius Accounting Servers page appears.

Step 9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

Step 10 From the MAC Delimiter drop-down list, choose **Hyphen**.

Step 11 Click **New**.

Step 12 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 13 In the WLC main window, click the **WLANs** tab.

Step 14 Click the WLAN of the SSID for the Captive Portal rule.

Step 15 Choose **Security**.

Step 16 In the Layer 2 tab, select the **MAC Filtering** check box.

Step 17 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 18 In the AAA Servers tab, in the Radius Servers area, do the following:

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

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

Step 19 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 20 Click the **Advanced** tab, and select the **Enabled** check box for Allow AAA Override.

Step 21 Click **Apply**.

Step 22 In the WLC main window, click the Security tab.

Step 23 Choose **AAA > Mac Filtering**.

Step 24 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 25 Ensure that the wall gardens are configured for the ACLs. To view the wall garden ranges, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/CUWN” link in the SSIDs page, and click the “Configure SSID in CUWN - CMX” tab.

Configuring the CMX for Notifications and Reports

To enable the CMX Engage to send notifications, you must do certain configurations in the CMX.

Note The CMX Engage supports CMX 8.0 or later.

If the CMX Engage cloud can communicate to your CMX instance, you can do this configurations automatically from the CMX Engage dashboard. In the CMX Engage dashboard, when you click a location in the location hierarchy for which the notification configurations are not done, a dialog box appears asking whether to configure the network. Click **Yes** to update the CMX with the notification configurations.

If the CMX Engage cloud cannot communicate with your CMX instance, then you have to manually configure the CMX for notifications. If you are manually configuring the CMX for notifications, the configurations required for various CMX versions are as follows:

- Configuring CMX 8.0 for Notifications, page 15-10
- Configuring CMX 10.0 or later for Notifications, page 15-11

Configuring CMX 8.0 for Notifications

To configure the CMX 8.0 for notifications, perform the following steps:

Step 1 Log in to CMX admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service > Notification > Subscriptions.**

The Notification Subscription page appears.

Step 4 Click **Add Subscription**.

Step 5 Enter the subscription name.

Step 6 Choose the subscription type as **Event Driven** from the drop-down list.

Step 7 Choose the data format as **JSON** from the drop-down list.

Step 8 Choose **HTTP** from the receiver transport drop-down list, and enter the following details:

a. **URL**- nnotifications/MSE/<customerIdentifier>.

b. Select the HTTPS check box if you want to use HTTPS protocol for secure access to the destination system.

Step 9 Enter the receiver host address as **livenotification.wifi-mx.com**.

Step 10 If you have selected the HTTPS check box, enter **443** as the port number of the receiver host. If HTTPS is not enabled, enter **80** as the port number.

Step 11 Ensure that the Scramble MAC addresses check box is not selected.

Step 12 Choose the notification trigger as **Presence Events** from the drop-down list, and click **Add**.

Step 13 Click **Save**.

Note For customerIdentifier, contact the CMX Engage support team.

Configuring CMX 10.0 or later for Notifications

To configure the CMX 10.0 or later for notifications, perform the following steps:

Step 1 Log in to Cisco CMX using the login credentials for your CMX account.

Step 2 Choose **Manage> Notifications**.

Step 3 Click **New Notification**.

Step 4 In the CREATE NEW NOTIFICATION window, perform the following steps:

a. In the Name text field, enter a name for the notification.

b. From the Type drop-down list, choose **Location Update**.

c. From the DeviceType drop-down list, choose **All**.

d. From the Hierarchy drop-down list, choose **All Locations**.

e. From the Receiver drop-down list, choose **https**, and in the text field enter the following details:

- **Host address**: livenotification.wifi-mx.com
- **Port No**: 443
- **URL**: notifications/MSE/<customerIdentifier>

Step 5 Ensure that MAC Scrambling is set to **OFF** and the message format is **JSON**.

Step 6 Click **Create**.

Note For customerIdentifier, contact the CMX Engage support team.

Configuring the CUWN for Social-Authentication

For social authentication with the CUWN, you must do some configurations in the Wireless LAN Controller.

To configure the CUWN for social-authentication, perform the following steps:

Step 1 Log in to Wireless LAN Controller using your credentials.

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

Step 3 In the Access Control List page that appears, click the Access Control List configured for the CMX Engage.

Click Add New Rule and add additional two rules with following information..

Table 1 ACL Rule - Wall Garden Range for Social Authentication

No	Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Direction
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any	Any

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