Configuring the CUWN for the CMX Engage

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

Configuring the CUWN(CMX, WLC) for working with the CMX Engage

For CUWN, the following configurations are required to work with the CMX Engage:

1. Configuring Access Point Mode, SSIDs, ACLs, Splash URLs , and Virtual Interface in the WLC, page 15-1
2. Configuring the CUWN for Notifications and Reports, page 15-12
3. Configuring the CUWN for Internet Provisioning and Radius-Authentication, page 15-10(This configuration is required only if you need radius-authentication.)
4. Configuring the CUWN for Social-Authentication, page 15-15(This configuration is required only if you need social authentication for your portals.)

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.

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 15-5

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 restrict the Internet access for customers, and to allow access only to CMX Engage splash page URL when connected to the SSID, the CMX Engage IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the CMX Engage as an external URL, and results into multiple redirection for customer.

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. The wall garden ranges are listed under the caption "Creating the Access Control List".

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 8-32.

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.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

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

Note The Layer 2 security is to provide internet access without splash page. As we are already configuring splash page for CMX Engage, there is no need of Layer 2 security.

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

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

Note Web Policy is the Layer 3 security option that enables you to configure captive portal in the WLC.

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

Note If radius authentication is not required, you must 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.

Note Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The 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.

Note Enabling “overide global config” allows you to redirect the customer to the CMX Engage URL, which is an external URL.

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

Note The “Web Auth Type” must be “External” as the CMX Engage page is hosted in the external server, and not in the controller.

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. The splash page URL is displayed in step 7g under the caption “Creating the SSIDs in CUWN-CMX.

Note You must configure the splash page for the customer to be redirected to the CMX Engage web page during on-boarding.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter **1800**.

Step 10 **C**lick **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 Management > HTTP-HTTPS

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

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 The redirect URL field must be blank so that it won’t override the CMX Engage splash URL configured in Layer 3.

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 15-6
- FlexConnect Local Switch Mode, page 15-6

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

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 15-6
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 15-7
3. Create the SSIDs in the WLC for the FlexConnect Local Switch Mode, page 15-8
4. Configure the Virtual Interface, page 15-5

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 restrict the Internet access for customers, and to allow access only to CMX Engage splash page URL when connected to the SSID, the CMX Engage IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the CMX Engage as an external URL, and results into multiple redirection for customer.

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.The wall garden ranges are listed under the caption "Creating the Access Control List".

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 8-32.

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.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

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

Note The Layer 2 security is to provide internet access without splash page. As we are already configuring splash page for CMX Engage, there is no need of Layer 2 security.

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

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

Note Web Policy is the Layer 3 security option that enables you to configure captive portal in the WLC.

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

Note If radius-authentication is not required, you must 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 Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The 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.

Note Enabling "overide global config" enables you to redirect the customer to the CMX Engage URL, which is an external URL.

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

Note The "Web Auth Type" must be "External" as the CMX Engage page is hosted in the external server, and not in the controller.

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. The splash page URL is displayed in step 7g under the caption "Creating the SSIDs in CUWN-CMX".

Note You must configure the splash page for the customer to be redirected to the CMX Engage web page during on-boarding

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, 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

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

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.

Note The redirect URL field must be blank so that it won't override the CMX Engage splash URL configured in Layer 3.

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.

- Customer onboarding by captive portal,
- To seamlessly provision internet,
- Assign specific Internet bandwidth for a specific duration
- Deny internet connectivity to user

To configure radius authentication and seamless internet provisioning, perform the following steps:

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.To view the radius server IP address and secret key, in the CMX Engage dashboard, click the "Setup SSIDs in Meraki/ CUWN" link in the SSIDs section, and on the "Configure SSID in CUWN- CMX" tab, click the "Radius Server Configuration" section.

Step 8 Choose **Radius > Accounting.**

The Radius Accounting Servers page appears.

Step 9 From "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 can configure only the CMX Engage radius servers. To view the radius server IP address and secret key, in the CMX Engage dashboard, click the "Setup SSIDs in Meraki/ CUWN" link in the SSIDs section, and on the "Configure SSID in CUWN- CMX" tab, click the "Radius Server Configuration" section.

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 CUWN for Notifications and Reports

The configurations required for CUWN for notifications and reports depend on how the CUWN is connected to the CMX Engage. Access the respective link from the following based on your scenario:

- Configuring the CMX for Notifications and Reports, page 15-12
- Configuring the WLC for Notifications and Reports (without a CMX Installation), page 15-14
- Configuring the Mobility Express for Notifications and Reports (Location Updates), page 15-19

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 15-12
- Configuring CMX 10.0 or later for Notifications, page 15-13

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**- notifications/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 The "customerIdentifier" is customer-specific. To view your "customerIdentifier", in the CMX Engage dashboard, click the "Setup SSIDs in Meraki/CUWN" link the SSIDs page, and then click the "Configure SSID in CUWN-CMX" tab. The "customerIdentifier" will be displayed under the section "Configure CMX for Notifications > Configuring CMX 8.0 for Notifications". You can also contact the CMX Engage support team for "customerIdentifier.

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**.

Note If you select the DeviceType as "All", the CMX Engage gets the location updates for all the devices from the CMX.

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

Note If you select the Hierarchy as “All locations”, the CMX Engage gets the location updates from all the locations associated with the CMX.

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

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

Note Choosing the Receiver as “https” enables you to secure the location updates sent from your CMX.

Note The “customerIdentifier” is customer-specific. To view your “customerIdentifier”, in the CMX Engage dashboard, click the “Setup SSIDs in Meraki/CUWN” link the SSIDs page, and then click the “Configure SSID in CUWN-CMX” tab. The “customerIdentifier” will be displayed under the section “Configure CMX for Notifications > Configuring CMX 10.0 or later for Notifications”. You can also contact the CMX Engage support team for “customerIdentifier”.

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

Note If the MAC Scrambling is set to **ON**, the WLC will not send the actual MAC address, and the CMX Engage cannot identify the customers.

Note Even though the CMX Engage receives the location updates for the message format, “XML”, the CMX Engage will process the location update data only if the format is “JSON”.

Step 6 Click **Create** to create the notification.

Configuring the WLC for Notifications and Reports (without a CMX Installation)

If your wireless network is CUWN, and if you are not having a CMX installation, you have to use the wireless network option “CUWN-WLC” to work with the CMX Engage. For more information on configuring the wireless network as CUWN-WLC in the CMX Engage, see “Defining the Location Hierarchy for CUWN - without CMX Installation” section on page 3-9.

Note If you are using the CMX Engage with WLC (without a CMX installation), the WLC must be in “Foreign controller” mode.

For the wireless network, CUWN-WLC, the configurations required for notifications and reports will be done automatically when you connect the CMX Engage to the WLC, and import the WLC controller.

For more information on how to connect to the WLC and import the WLC controller for CUWN-WLC, see "Configuring the WLC to Import the WLC Controller and Access Points to the CMX Engage" section on page 3-15.

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.

Configuring Mobility Express for working with the CMX Engage

This section describes the configurations to be done in the Mobility Express Controller for using the CMX Engage.

The configurations required for various Mobility Express (ME) versions are different. The configurations for various ME versions are as follows:

- Configuring Mobility Express 8.7 or later for the CMX Engage, page 15-15
- Configuring Mobility Express 8.6 or Earlier for the CMX Engage, page 15-20

Configuring Mobility Express 8.7 or later for the CMX Engage

To configure the Mobility Express 8.7 or later for the CMX Engage, perform the following steps:

1. Creating SSIDs in the Mobility Express, page 15-16

Creating SSIDs in the Mobility Express

To create SSIDs in the Mobility Express, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

Step 4 To create a WLAN, click **Add new WLAN/RLAN**.

Step 5 In the window that appears, in the **General** tab, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 6 Click **Apply**.

The Add new WLAN/RLAN page appears.

Step 7 Click **WLAN Security**.

Step 8 Enable the **Guest Network** toggle Switch

Step 9 Enable the **Captive Network Assistan**t toggle switch.

Step 10 From the Captive Portal drop-down list, choose **External Splash Page**.

Step 11 From the Access Type drop-down list, choose **Web Consent**.

Step 12 In the Captive Portal URL field that appears, enter the CMX Engage splash URL.

To view the splash URL for your ME 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. The spalsh URL is displayed in step 7g under the “Creating the SSIDs in CUWN - CMX” section.

Step 13 Click **Apply**.

Step 14 To enable and broadcast the SSID, in the **General** tab, from the Admin drop-down list, choose “Enabled”, and enable the “Broadcast SSID” toggle switch.

Step 15 Execute the following command in the command prompt to disable the secure webauth mode. Then, restart the ME.

```
config network web-auth secureweb disable
```

Step 16 Execute the following command in the command prompt to change the webauth login success page from **Default** to **None**.

```
config custom-web webauth-login-success-page none
```

Configuring Radius-Authentication in the Mobility Express 8.7 or Later

To configure radius authentication in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the ME main window, click **Switch to Expert View** in the top right of the page.

Step 3 In the pop up window that appears, select **OK**.

Step 4 In the left pane, click **Management > Admin Accounts**

Step 5 In the page that appears, click the **Radius** tab.

Step 6 Click **Add RADIUS Authentication Server**.

In the “Add/ Edit Radius Authentication Server” window appears, enter the following radius server details:

a. In the “Server IP Address” text field, enter the IP address of the radius server.

b. In the "Shared Secret" text field, enter your radius secret key.

c. In the "Confirm Shared Secret" text field, re-enter the radius secret key.

Step 7 Click **Apply**.

Step 8 In the ME main window, click **Wireless Settings** in the left pane.

Step 9 Click **WLANs** .

The WLAN/RLAN Configuration page appears with the SSIDs list.

Step 10 Click the Edit icon for the “SSID ” created previously.

Step 11 In the Edit WLAN window that appears, click the **WLAN Security** tab.

Step 12 From the Access Type drop-down list, choose **Radius**.

Step 13 Click the Radius Server tab, and click **Add RADIUS Authentication Server**.

Step 14 From the “Server IP Address” drop-down list, select your Radius Server, and click **Apply**.

Step 15 In the Edit WLAN window, click **Apply**.

Now the Mobility Express 8.7 or later is configured for radius server authentication.

Creating Access Control Lists in the Mobility Express 8.7 or Later

To create Access Control Lists in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the ME main window, click the Wireless Settings in the left pane.

Step 3 Click **WLANs**.

The WLAN/RLAN Configuration page appears with the SSIDs list.

Step 4 Click the Edit icon for the “SSID ” created previously.

In the Edit WLAN window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, create rules with the following configuration

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	54.235.122.137/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	54.235.122.137/255.255.255.255	Any	Any	Any	Any
Permit	107.20.217.46/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	107.20.217.46/255.255.255.255	Any	Any	Any	Any

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

- Protocol : Any
- DSCP : Any
- Action : Permit

Step 8 Click **Apply**.

Configuring the Mobility Express 8.7 or Later for Social Authentication

To configure the Mobility Express for Social Sign authentication for captive portals, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the ME main window, click the Wireless Settings in the left pane.

Step 3 Click **WLANs**.

The WLAN/RLAN Configuration page appears with the SSIDs list.

Step 4 Click the Edit icon for the “SSID ” created previously.

In the Edit WLAN window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, configure the following two rules in addition to the existing ACL rules:

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPs	Any	Any
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any

White-listing the URLs in the Mobility Express 8.7 or Later

To white-list a URL in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the ME main window, click the Wireless Settings in the left pane.

Step 3 Click **WLANs**.

The WLAN/RLAN Configuration page appears with the SSIDs list.

Step 4 Click the Edit icon for the “SSID ” created previously.

In the Edit WLAN window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add URL Rules**.

Step 7 In the “Add/Edit URL ACLs” window that appears, configure the URL that you want to white-list.

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

- **URL**: domain
- **Action** : Permit

Step 8 Click **Update**.

Configuring the Mobility Express for Notifications and Reports (Location Updates)

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Step 1 In the WLC CLI mode, execute the following commands:

1. `config cloud-services cmx disable`
2. `config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}`
3. `config cloud-services server id-token {Customer JWT Token}`
4. `config cloud-services cmx enable`

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the CMX Engage dashboard, choose **SSIDs**, click the **Setup SSIDs in Meraki/CUWN** link, and then click the "Configure SSID in CUWN-WLC" tab. The {Customer Path Key}, {LB Domain}, LB IP Address}, and {Customer JWT Token} are displayed in step 1 under the caption "Configuring WLC to connect to CMX Engage". You can also contact the CMX Engage support team. Ensure that there are no trailing/leading spaces.

Step 2 Check the summary using the following command:

```
show cloud-services cmx summary
```

The result appears.

Now in the CMX Engage dashboard, when you choose "CUWN-WLC" in the "Add a Wireless Network" window, the WLC will be listed. So, you can import the APs of that WLC to the CMX Engage.

Sample Result

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.proximitymx.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... Active

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

Note If you are using Mobility Express with CMX Proxy, to configure the Mobility Express for location updates, in the CMX Engage dashboard, click the **Setup SSIDs in Meraki/CUWN** link, and then click the "Configure SSID in CUWN-WLC" tab. Follow the instructions in the "Configuring CMX Cloud Proxy to connect WLC with CMX Engage" section.

Configuring Mobility Express 8.6 or Earlier for the CMX Engage

To configure Mobility Express 8.6 or earlier for the CMX Engage:

- Creating SSIDs in Mobility Expres 8.6 or Earlier, page 15-21
- Configuring Radius-Authentication for Mobility Express 8.6 or Earlier, page 15-21
- Creating ACLs for Mobility Express 8.6 or Earlier, page 15-21
- Configuring the Mobility Express for Notifications and Reports (Location Updates), page 15-19

Creating SSIDs in Mobility Expres 8.6 or Earlier

The steps to create SSIDs in Mobility Express 8.6 or earlier are same as that for ME 8.7 or later. To know the configuration steps, see Creating SSIDs in the Mobility Express, page 15-16.

Configuring Radius-Authentication for Mobility Express 8.6 or Earlier

In Mobility Express 8.6 or earlier, you cannot configure radius servers individually.

To configure Mobility Express 8.6 or earlier for radius authentication, perform the following steps:

Step 1 Log in to ME with your credentials.

Step 2 In the ME main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs** .

The WLAN/RLAN Configuration page appears with the SSIDs list.

Step 4 Click the Edit icon for the “SSID” created previously.

Step 5 In the Edit WLAN window that appears, click the **WLAN Security** tab.

Step 6 From the Access Type drop-down list, choose **Radius**.

Step 7 To add the radius server, click **Add**.

Step 8 In the window that appears, enter the following radius server details:

d. In the “Server IP Address” text field, enter the IP address of the radius server.

e. In the "Shared Secret" text field, enter your radius secret key.

f. In the "Confirm Shared Secret" text field, re-enter the radius secret key.

g. Click **Apply**.

Step 9 In the Edit WLAN window, click **Apply**.

Now, the Mobility Express is configured for radius server authentication of the CMX Engage captive portals.

Creating ACLs for Mobility Express 8.6 or Earlier

Mobility Express 8.6 or earlier does not provide user interface to configure Access Control Lists. So for creating ACLs, and configuring social authentication, you must use the command prompt. For the commands to use for these ACL configurations, see “Cisco Mobility Express Command Reference Guide”.